Basic Internet Security & Privacy

David Papp, P.Eng.

CISA, CISSP, MCSE, CCNP, CCDA, CWNA, NSCA

Last Modified
20 minutes ago ☺

The Business Link

October 25, 2005

A bit of history

The Rogue Gallery of Hackers…

Rogue Gallery of Hackers

- CIRCA 1971
  - John Draper, a Vietnam vet, discovers that a Cap'n Crunch whistle produces a tone activating AT&T's free calling.
- CIRCA 1983
  - A Milwaukee hacking group called the 414's break into computers at Los Alamos Labs and the Memorial Sloan-Kettering Cancer Center.

Rogue Gallery of Hackers

- 1984
  - The Legion of Doom (LOD) hacking group formed by “Lex Luthor” targets telecommunications companies and 911 emergency telephone services.
- 1988
  - Student Robert Morris unleashes a worm on the Internet that crashes 6,000 computers. Morris becomes the first person convicted under the US Computer Fraud and Abuse Act.

Rogue Gallery of Hackers

- 1988
  - Kevin Mitnick is arrested and convicted. At the time, Mitnick had broken into Digital Equipment Corp.’s computer systems.
- 1990
  - The “Great Hacker War” begins as LOD and Masters of Deception (MOD) cyberwar jams many phone lines and results in multiple break-ins of computers.

Rogue Gallery of Hackers

- 1990
  - Kevin Poulsen takes over all the phone lines going into KIIS-FM in Los Angeles to guarantee that he'd be the 102nd caller and win a Porsche. Poulsen is later convicted.
- 1992
  - Four members of MOD are convicted of various computer crimes, Phiber Optik, a.k.a. Mark Abene, is sentenced to a year in prison.

Rogue Gallery of Hackers

- 1994
  - Russian mathematician Vladimir Levin leads a break-in of Citibank computers to steal $10 million. All but $400,000 was recovered and Levin was later arrested.
- 1995
  - Kevin Mitnick, also known as Condor, is arrested again, this time for illegal use of stolen cellular telephone numbers. He spends five years in jail.

Rogue Gallery of Hackers

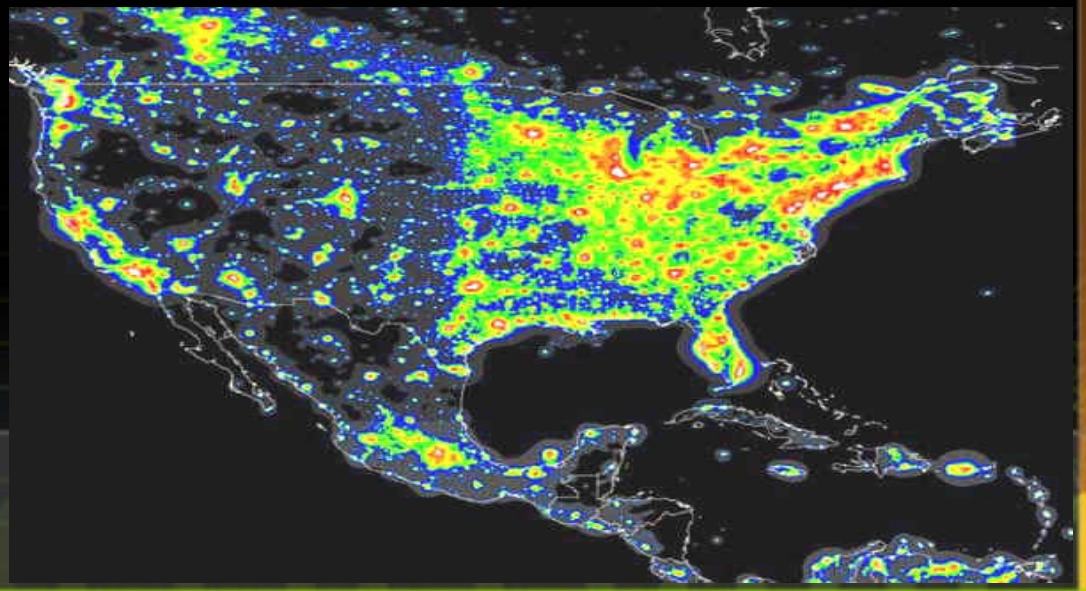
- 1999
  - The Melissa Virus is released by David L. Smith. It replicates by sending itself to people listed in the victim's address books.
- 2000
  - DDoS attacks all but shut down Web sites, including Amazon, CNN, eBay, and Yahoo. A recorded online chat session later fingers a Montreal teenage hacker.

Rogue Gallery of Hackers

- 2000
  - A variant of Melissa called the Love bug or ILoveYou virus is traced to a Philippine computer science student. The estimated damage caused by the virus: $6.7 billion.
- 2000
  - Wireless phones in Europe are targeted by a cell phone virus called Timofonica, signaling what may be a new capability for hackers.

Recently

Today we have a proliferation of email spam, viruses, and many more computer users & devices connected to the Internet.



Spam

April 2004

- 67% of all worldwide email = spam
- 83% of all US email = spam

Viruses

1990 – 200 to 500
1991 – 600 to 1,000
1992 – 1,000 to 2,300
1994 – 4,500 to 7,500
1996 – 10,000+
1998 – 20,000+
2000 – 50,000+

Confusion due to mutations (polymorphic viruses)

Worms

- February 2004 – **MyDoom** worm
  - *Over 1,000,000 infected*
- August 2003 - **Blaster** worm
  - *300,000 to 350,000 infected*
- January 2003 – **Slammer** worm
  - *200,000 to 250,000 infected*
- September 2001 – **Nimda** worm
  - *150,000 to 200,000 infected*
- July 2001 – **Code Red** worm
  - *350,000 to 400,000 infected*

Slammer Worm

-Fastest computer worm in history. As it began spreading, it DOUBLED IN SIZE EVERY 8.5 SECONDS!

-It achieved full scanning rate of over 55 million scans per second after only 3 minutes.

-It infected more than 90% of vulnerable hosts within 10 minutes. Code Red was 14 hours.

-Two orders of magnitude faster than Code Red which has a “leisurely” doubling time of 37 minutes.

-Slammer was so aggressive that it quickly interfered with its own growth due to completely using up all the bandwidth of many Internet connections.

-The weakness was discovered and a patch was released on July 24/02. The worm broke out Jan25/03, 6 months later!!

Virus Gangs

- Starting in January 2004, a “war” began between MyDoom, Beagle, and Netsky.
- These viruses placed backdoors in your system

- As of March14/04, MyDoom.H (8), Beagle.N (14), Netsky.M (13)
- As of Feb10/05, MyDoom.AU(47), Beagle.BA(53), Netsky.AE(31)

- Netsky = Skynet = Terminator Movie ☺
- Embedded messages in viruses:
  - Bagle.J: “Hey, Netsky… don’t ruine our business, wanna start a war?”
  - Netsky.F: “Skynet Antivirus – Bagle – you are a looser”
  - MyDoom.G: “to netsky’s creator(s): imho, skynet is a decentralized peer-to-peer neural network etc etc… not your XXXX app.”

Categorizing Security

- Exploits
  - Audits, penetration tests, vulnerabilities
- Methodologies
  - Certifications, documentation, reports, experience
- Countermeasures
  - Firewalls, VPNs, Encryption, Disaster Recovery Plans

whois

- Domain Names and IP Addresses

- www.abc.com = hostname
- abc.com = domain name
- 216.239.57.99 = IP Address (www.arin.net)

  - www.onewhois.com or www.allwhois.com
  - www.dnsstuff.com
  - www.samspade.org
  - **network-tools.com/help/**

Email – General Delivery

Go to post office	= Connect to **POP3 server**
Ask for mail	= Poll for mail
Show ID	= Authenticate with username/pwd
Receive Mail	= Receive email

POP3 = Post Office Protocol v3

Email Delivery

Drop mail in red box	= Connect to **SMTP server**
Send mail to depot	= Send mail
Sort by postal code	= Resolve DNS
Deliver to correct mailbox	= Deliver mail to correct POP server

SMTP = Simple Mail Transfer Protocol

DNS records are like postal codes

DNS servers are like phone books

Email Headers

- Outlook (right click on email in Inbox, then Options, then read the Internet Headers)
- Read from bottom up
- Excellent information about reading email headers at
  http: / /www.stopspam.org/email / headers.html

Sample Email Header

```
Received: from mail.isp.com (mail.isp.com
[22.22.22.22]) by mailhost.company.com (8.8.5/8.7.2)
with ESMTP id LAA20869 for ; Tue, 18 Mar 2003 14:39:24
-0800 (PST)
Received: from mycomputername.bogus.com (ip-
host.isp.com [11.11.11.11]) by mail.isp.com (8.8.5) id
004A21; Tue, Mar 18 2003 14:36:17 -0800 (PST)
From: jane.doe@isp.com (Jane Doe)
To: someperson@company.com
Date: Tue, Mar 18 2003 14:36:14 PST
Message-Id: <rth031897143614-00000298@mail.isp.com>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Sample Email Header

```
Received: from mail.isp.com (mail.isp.com
[22.22.22.22]) by mailhost.company.com (8.8.5/8.7.2)
with ESMTP id LAA20869 for ; Tue, 18 Mar 2003
14:39:24 -0800 (PST)
Received: from mycomputername.bogus.com (ip-
host.isp.com [11.11.11.11]) by mail.isp.com (8.8.5)
id 004A21; Tue, Mar 18 2003 14:36:17 -0800 (PST)
From: jane.doe@isp.com (Jane Doe)
To: someperson@company.com
Date: Tue, Mar 18 2003 14:36:14 PST
Message-Id: <rth031897143614-00000298@mail.isp.com>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Sample Email Header

```
Received: from mail.isp.com (mail.isp.com
[22.22.22.22]) by mailhost.company.com (8.8.5/8.7.2)
with ESMTP id LAA20869 for ; Tue, 18 Mar 2003
14:39:24 -0800 (PST)
Received: from mycomputername.bogus.com (ip-
host.isp.com [11.11.11.11]) by mail.isp.com (8.8.5)
id 004A21; Tue, Mar 18 2003 14:36:17 -0800 (PST)
From: jane.doe@isp.com (Jane Doe)
To: someperson@company.com
Date: Tue, Mar 18 2003 14:36:14 PST
Message-Id: <rth031897143614-00000298@mail.isp.com>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Sample Email Header

```
Received: from mail.isp.com (mail.isp.com
[22.22.22.22]) by mailhost.company.com (8.8.5/8.7.2)
with ESMTP id LAA20869 for ; Tue, 18 Mar 2003
14:39:24 -0800 (PST)
Received: from mycomputername.bogus.com (ip-
host.isp.com [11.11.11.11]) by mail.isp.com (8.8.5)
id 004A21; Tue, Mar 18 2003 14:36:17 -0800 (PST)
From: jane.doe@isp.com (Jane Doe)
To: someperson@company.com
Date: Tue, Mar 18 2003 14:36:14 PST
Message-Id: <rth031897143614-00000298@mail.isp.com>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Hotmail Email Header

- Received: from hotmail.com (bay16-f55.bay16.hotmail.com [65.54.186.105]) by mail.remote.net (8.12.8p1/8.12.8) with ESMTP id i4I1cVsS025191 for <david@remote.net>; Mon, 17 May 2004 19:38:31 -0600 (MDT) (envelope-from hacker___52@hotmail.com)
- Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC; Mon, 17 May 2004 18:38:28 -0700
- Received: from 24.64.82.142 by by16fd.bay16.hotmail.msn.com with HTTP; Tue, 18 May 2004 01:38:28 GMT
- **X-Originating-IP: [24.64.82.142]**
- **X-Originating-Email: [hacker___52@hotmail.com]**
- From: "Mr. E" <hacker___52@hotmail.com>
- To: david@remote.net
- Subject: Guess Who?
- Date: Mon, 17 May 2004 21:38:28 -0400
- Message-ID: <BAY16-F55fVwcdZ06YO00020f9d@hotmail.com>
- X-OriginalArrivalTime: 18 May 2004 01:38:28.0434 (UTC) FILETIME=[D1A6FB20:01C43C78]

Whois IP Address

WWW.ARIN.NET / WHOIS
24.64.82.34

```
OrgName:     Shaw Communications Inc.
OrgID:       SHAWC
Address:     Suite 800
Address:     630 - 3rd Ave. SW
City:        Calgary
StateProv:   AB
PostalCode:  T2P-4L4
Country:     CA

NetRange:    24.64.0.0 - 24.71.255.255
CIDR:        24.64.0.0/13
NetName:     SHAW-COMM
NetHandle:   NET-24-64-0-0-1
NetType:     Direct Allocation
NameServer:  NS2SO.CG.SHAWCABLE.NET
NameServer:  NS1SO.CG.SHAWCABLE.NET

Comment:
RegDate:     1996-06-03
Updated:     2003-06-20

OrgAbuseHandle: SHAWA-ARIN
OrgAbuseName:   SHAW ABUSE
OrgAbusePhone:  +1-403-750-7420
OrgAbuseEmail:  internet.abuse@sjrb.ca

OrgTechHandle: ZS178-ARIN
OrgTechName:   Shaw High-Speed Internet
OrgTechPhone:  +1-403-750-7428
OrgTechEmail:  ipadmin@sjrb.ca
```

Trivia

There is no industry standard for an acceptable number of bugs, but a sometimes-quoted figure is one bug per 10,000 lines of code – a lot of bugs when you consider than Windows 2000 reportedly contains some 40 million lines of code. XP has even more…

Why? How? Yikes!

- Lack of people applying Microsoft updates
- Lack of AntiVirus software present
- Lack of updating AntiVirus definitions
- Lack of firewalls in place

Your computer is not a “toaster”. You cannot just plug it in and take it for granted that it works. Regular maintenance must be performed. Just like a car with oil & filter changes, break pads, etc.

Countermeasures Protect You & Your Computer

(see handouts)

- Apply Windows and Office Updates
- Software firewall
- Hardware firewall
- AntiVirus
- Encryption
- VPN
- Passwords
- Backups
- Surge Protection, UPS
- Destroy deleted files
- Wipe hard drives
- Protect Internet privacy
- Spyware blocker
- Spam blocker
- Be skeptical

Trivia

Average Time for Exhaustive Key Search

At 1,000,000 encryptions per second:

32-bit key length requires ~ 2 milliseconds
56-bit key length requires ~ 10 hours
128-bit key length requires
~5,000,000,000,000,000,000 years

Trivia

- The American Dialect Society voted the verb Google the “most useful” word for 2002.
- The term itself is a play on googol – same pronunciation – which is the number 1 followed by 100 zeroes. It was coined in 1938 by nine-year-old Milton Sirotta, after his uncle, mathematician Edward Kasner, asked him for a word to describe a really big number. ☺

PIPEDA / PIPA

- **Federal:**
  PIPEDA: Personal Information Protection and Electronic Documents Act
- **Provincial (Alberta):**
  PIPA: Personal Information Protection Act

- Organization engaged in commercial activity that collects, uses, or discloses personal information need to know about PIPEDA (Federal) and PIPA (Provincial – Alberta).
- **It's the law!** PIPA takes precedence over PIPEDA.
- Both laws in full effect January 1st, 2004
- Organizations must protect personal information, regardless of format, against unauthorized access, disclosure, copying, use, or modification. The degree of protection should be commensurate with the sensitivity of the information.

- PIPEDA Schedule 1, Section 4.7 – Safeguards:
  Methods of protection should include locked filing cabinets, locked offices, "need to know", passwords, encryption, privacy policies, care in destruction and disposal of personal information, …

Questions to ask a security consultant

- Is this your day job?
- How long have you been doing this?
- What certifications/training do you have?
- Do you or any of your staff have a criminal record?
- Do you have any ties or associations with a particular vendor?
- Do you offer any guarantees?
- Do you offer support for emergency situations?
- Do you have any references or a client list?

Security Certifications

- **CISSP** – Certified Information Systems Security Professional, www.isc2.org
- **SSCP** – Systems Security Certified Practitioner, www.isc2.org
- **CISA** – Certified Information Systems Auditor, www.isaca.org
- **CPP** – Certified Protection Professional, www.asisonline.org
- **GIAC** – Global Information Assurance Certification, www.giac.org
- **Security Certified Program** – www.securitycertified.net
- **Cisco certifications** – www.cisco.com
- **Microsoft certifications** – www.microsoft.com

Contact Info

David Papp
david@remote.net
780.951.4869