Security - A Historical Perspective

Note Title 2/17/2011

Announcements

- Lab 2 (iptables) is due next Tuesday
- Second writeup - due next Thursday

1930s

- Alan Turing, Gordon Welchman & Harold Koen design the 'Bombe' to crack the Enigma code. (Essentially, they automate a brute force attack!)

(aren't any computers)

1960s

"Hackers" is the name given to people who master the mainframes and can push them beyond what they are designed to do.

("Bugs" came around this time also - but they were real.)

1970s

John Draper, aka "Captain Crunch", finds a way to fool payphones into allowing free calls.

found a whistle in a cereal box

The phone hacker, or "phreak" movement, begins to take off as organized groups like YIPL/TAP form.

As a side note;

Two members of the Homebrew Computer Club, "Berkeley Blue" and "Oak Toebark", begin constructing blue boxes, which are designed to hack into the phone system.

(You've heard of these guys, right?)

Steve Jops & Steve Woznick

1980's

More groups form:

- Warelords - based in St. Louis! (Mostly interested in piracy, but they also infiltrated The White House, Southwestern Bell, & others)

- the 414's: break into over 60 sensative systems, such as Los Alamos. (This results in a Newsweek article and the first computer security legislation)

- Cult of the Dead Cow
  - publish one of the first "ezines"
  - famous for later exploits
- Legion of Doom forms
  - one of the most famous, and a few years later, one of the most publicized after law enforcement raids begin

1980's

- In 1983-84, pop culture catches on
  - Wargames
  - William Gibson writes Neuromancer, which invents the term cyberspace (as well as the matrix & other terminology)
  - 2600, the Hacker Quarterly, begins publication
  - A year later, phrack begins its posting

Legislation - late 1980s

- 1986 - Computer Fraud and Abuse Act passes
  - First time it is made illegal to hack into a computer
  - Does not include juveniles

- In 1988, CERT is formed by DARPA (after Morris Worm)

The Hacker's Manifesto - 1986, in Phrack

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...

Worms

- 1987 - The Christmas Tree EXEC worm
- 1988 - The Morris Worm
- 1988 - The Father Christmas Worm

(plus many more costly attacks)

1990s

Operation Sundevil (in 1990):

The Secret Service raids prominent members of hacking BBSs in over 10 cities, including:

- Legion of Doom
- Steve Jackson games

This prompts the formation of the EFF - Electronic Frontier Foundation

1990s

- 1992:
  Sneakers comes out - gives the first "white hat" perspective

- 1993:
  - Defcon begins
  - AOL gives its users USENET access

Late 1990s:
- The BBSs disappear as WWW appears
- More exploits:
  - AOHell
  - Russian hackers steal $10 million

1995:

- *Hackers* is released
- Highly publicized Kevin Mitnick arrest
  - imprisoned without trial for 4 years
  - famous for social engineering - he did almost everything without ever exploiting vulnerabilities!
  - In 1999, he is eventually tried, gets 5 years sentence, & is almost immediately released.

Late 1990s

- 1996:
  - Hackers deface DOJ, CIA, & Air Force websites
  - US Gen. Accounting office reports over 250K attempts to break into DoD computers in 1995 alone (About 65% succeeded!)
  - mp3s come out, & are immediately pirated everywhere

- 1997 - 98
    - Windows NT, MS's answer to how insecure '95 & '98 are is released (& is immediately a giant target)
    - Super bowl add (!) by Network Associates
    - RIAA takes off & begins cracking down on ftp distributors (including teens)
    - Napster is released

<u>1999:</u>

- Banner year for security (& hacking). **Hundreds** of advisories & bug updates.
- L0pht testifies before Congress that they could shut down the internet in 30 minutes
- Legion of the Underground "declares war" against Iraq & Chinese governments

Major denouncement is released, signed by CDC, phrack, Lopht, & other major hacker groups

1999 cont;

- Melissa worm
  (first major macro exploit)
- Political hackings increase
- Clinton announces $1.46 billion initiative to improve computer security
- Civilization fails to crumble at midnight on Dec. 31, 1999

2000 and on:

2000:

- ILOVE YOU worm - first to use VBS. Infects millions in hours. (One of most damaging ever.)
- teenager serves jail time for the first time

2001:

- Microsoft DNS hack
- Russian programmer is arrested (at DEFCON) for violating DMCA
- several major viruses and worms

2002-2003:

- MS promises cleanup & more secure products
- DHS given jurisdiction over IT infrastructure
- US must update export laws (see Mac commercial)

From here:

What I'd call "modern" era of security.

What events do you all remember?