Perspectives from the L0pht

To: DakotaCon

From: Joe Grand aka KINGPIN

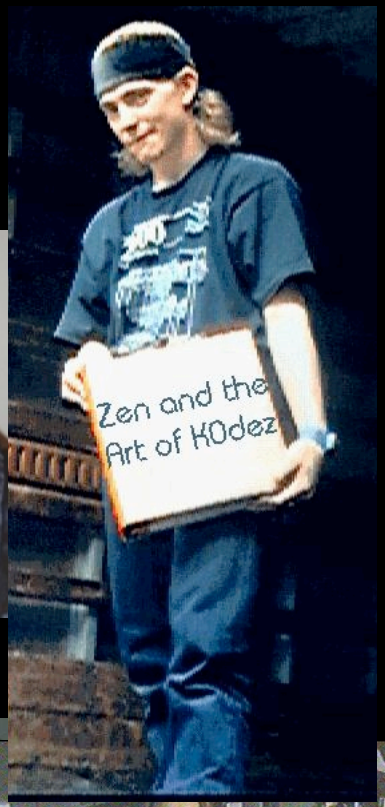
Perspectives from the L0pht

- A look back at growing up in the early days of the computer security industry
- How things have changed (or stayed the same)
  - What we had to face as hackers then
  - How different the security community is now
  - Are we any better off?

Back in the Day...

- If you were involved in computers, you were in the minority
  - It was not a "cool" or "sexy" thing to do
- Being a hacker was at your own risk
- Computer security was not often in mainstream media

The Security "Industry" Before



The Security Industry Now

- Started in the early 1990s as a clubhouse for local hackers
  - Store computer equipment
  - Tinker w/ projects
  - Experiment with new and old technologies
  - Just hang out
- Turned into tight-knit friends changing the face of computer security vulnerability research and disclosure

The L0pht

- All met online through local Boston, MA BBSes
- One of the first "hacker spaces"
- Early membership changes, with the core group solidifying around 1996
- In the late 90s, decided to try and become self-sufficient
  - Focus more on researching and disclosing vulnerabilities
  - No holds barred, tell it like it is
  - Cover rent and expenses w/ t-shirt, electronic kit, hacker CD, and flea market sales

The L0pht

- Anticlimactic ending in January 2000
  - Joined forces with VC to start security consulting firm @stake (now part of Symantec)
  - Original members all went their separate ways (some still involved in security)
- Played a very important role in my life and shaped me in many ways

The Early Days (~1994)

The Early Days (~1994)

The Early Days (~1994)

The Early Days (~1994)

Unauthorized Access by Annaliza Savage, 1994

www.youtube.com/watch?v=EUiWzwmDSx8

The Heyday (1996-1999)

The L0pht

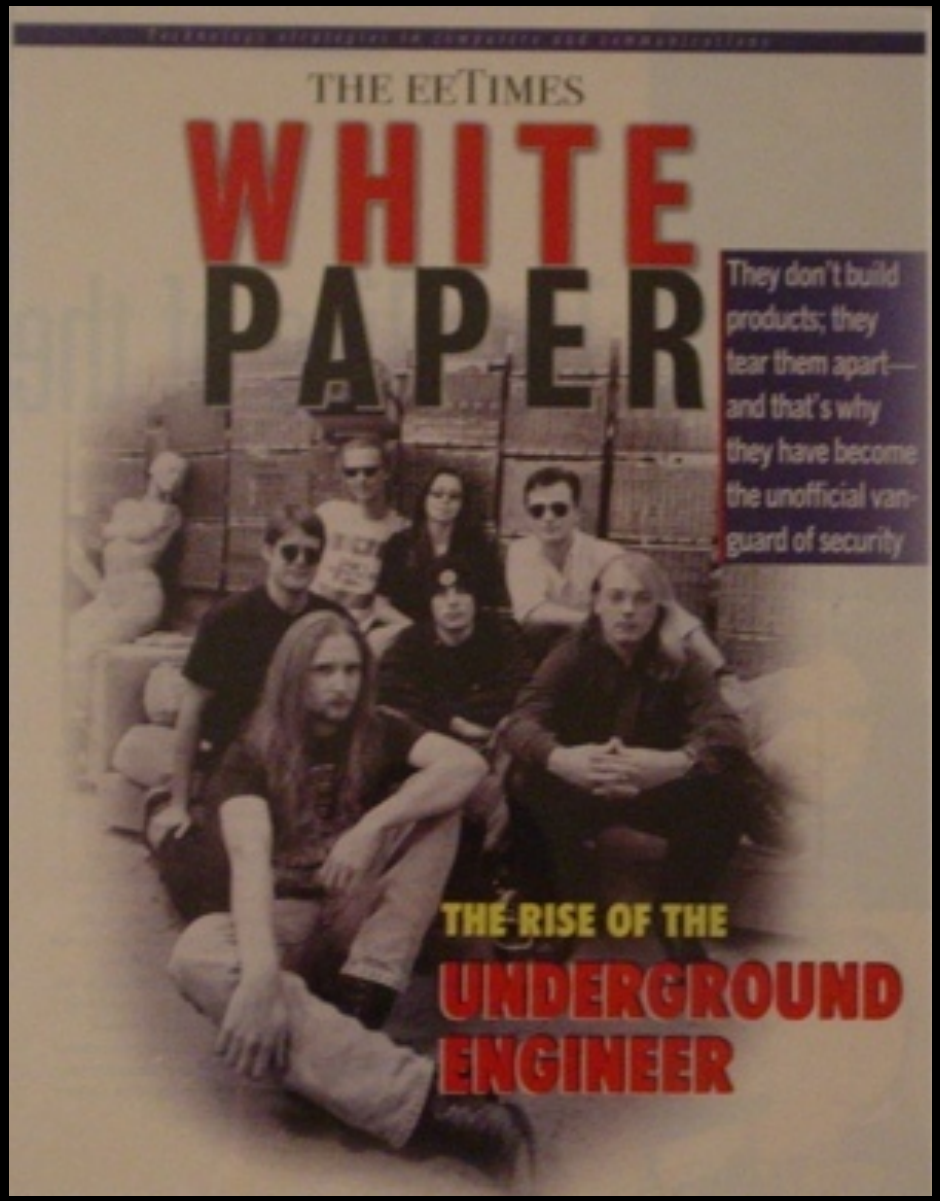
What do a group of hackers do when the equipment they've accumulated over years of dumpster diving no longer fits in their apartments? They get a l0pht. Since 1993, a core group of seven Boston-based hackers have rented a loft space for hacking, trading information about cellular phone security, and building things like a wireless Internet service using discarded microwave equipment. All strictly for educational purposes, of course.

"It's a sort of hacker think tank" says Mudge (front), l0pht member and a familiar name to Apple II software crackers. Today, l0pht is stuffed with old PDPs, Sun Workstations, and even a small supercomputer.

Now that all of them have day jobs in the industry, why do they keep at it? "For the girls and the text files, of course," says Mudge. – *Steve G. Steinberg*

Wired Magazine, August 1996

The Heyday (1996-1999)

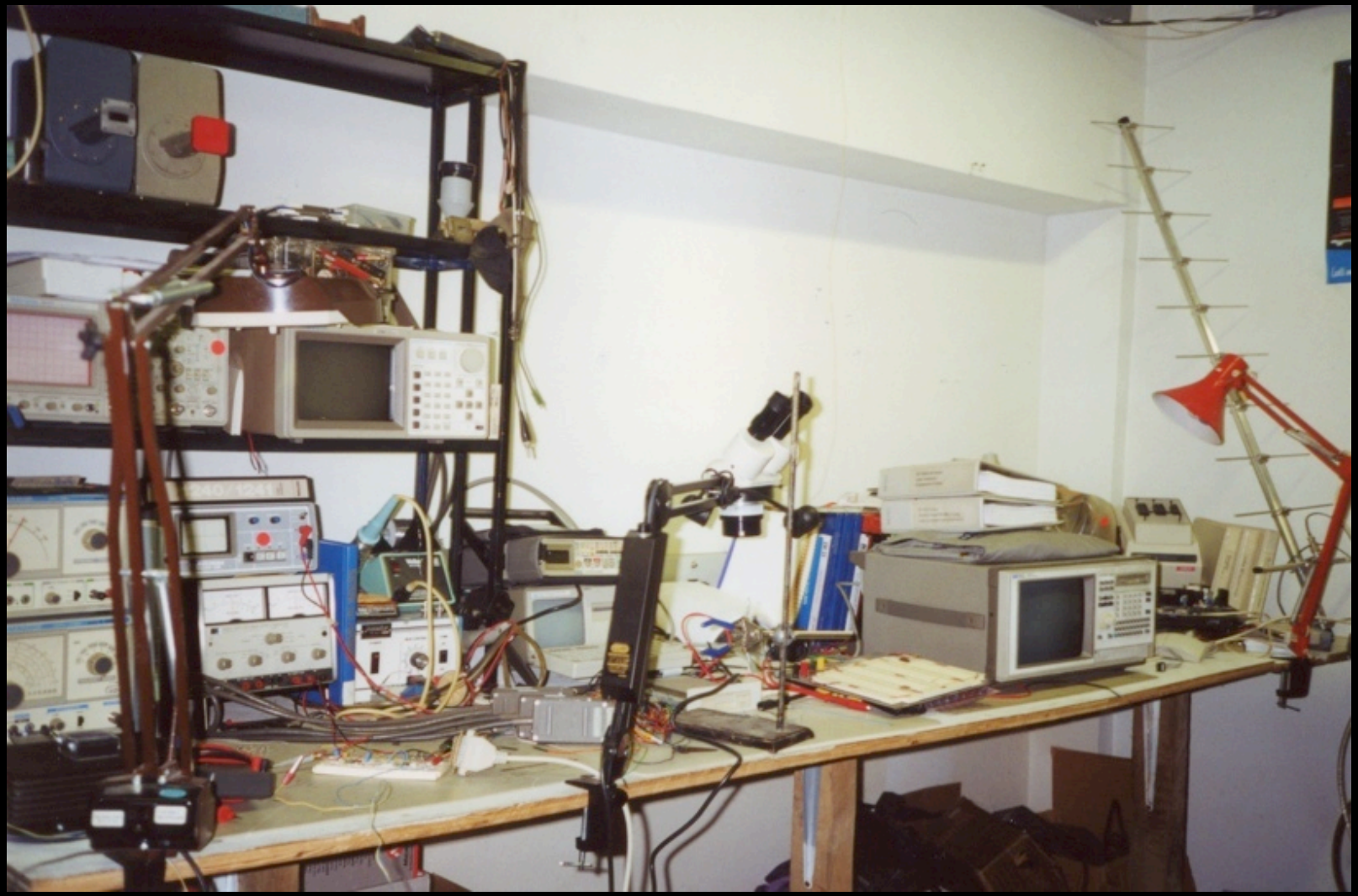


EETimes, Sept. 22, 1997

The Heyday (1996-1999)

The Heyday (1996-1999)

The Heyday (1996-1999)



The Heyday (1996-1999)

Advisories

- Full disclosure of our discovered vulnerabilities, starting ~1996
- We didn't play favorites
  - No corporate backing
  - No greased palms
  - We wanted to force the vendor to fix the problem
- We weren't looking to make $

Advisories

- Now, the landscape is completely different
  - Vendor pressure to prevent release of information
    - Threatened legal action
    - Talks pulled from major conferences
  - Advisories used as marketing by consulting companies to gain more clients
  - Corporate interests determine what is publicly released

Advisories

Release	Application	Platforms	Severity	Author
4/11/97	Microsoft NT Passwords	L0phtCrack the Microsoft NT cracker	L0phtcrack will recover passwords from Windows NT registries in a variety of fashions, including exhaustive keyspace attacks.	mudge@l0pht.com weld@l0pht.com

Recently several NT password crackers have emerged. We offer this one with the belief that it offers some features and functionality that the current ones do not have.

L0phtcrack will recover passwords from Windows NT registries in a variety of fashions.

By feeding in the output from PWDump [by Jeremy Allison, jra@cygnus.com] and a dictionary file, L0phtcrack rev 1 will attempt to retrieve:

1) only the LANMAN plaintext password
2) only the NT Dialect MD4 plaintext password [see reasoning below]
3) Both the LANMAN and MD4 plaintext passwords (by deriving the MD4 password from the LANMAN output and running through up to 2 to the Nth power permutations)

Release	Application	Platforms	Severity	Author
1/14/97		Filter Fresh Coffee Machines	Users can gain access using a factory default backdoor.	/dev/null@l0pht.com

Scenario: Suppose you don't work at Microsoft, Sun, or any of the companies that provide free hot caffinated beverages to their employees. It's a sad day when you find yourself at work (or scrounging around someone elses place of employment... I dunno, perhaps leaving a portable sniffing laptop up in the acoustic ceiling tiles) around 2am and the only coffee available is from a FILTER FRESH vending machine. It's even sadder when you are being asked to deposit .55 cents for an 8oz. cup of really poor java.

How to scam coffee from FILTER FRESH coffee vending machines.

Release	Application	Platforms	Severity	Author
9/96	Sendmail 8.7.5	All	Any local user can gain root privileges	mudge@l0pht.com

Due to a problem with the code in sendmail a buffer overflow condition exists that allows a user to overwrite the information in a saved stack frame. When the function returns, the saved frame is popped off of the stack and user code can be executed.

An exploit script will be made public upon the actual release of Sendmail 8.8 which fixes this particular exploitable code segment.

Full L0pht Advisory
CERT issued it's own advisory in response.

L0pht Heavy Industries web site archive

http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/l0pht/l0pht.html

Advisories

- There were no "accepted practices" like there are now
  - No full v. responsible disclosure debate
  - We were making it up as we went along
- If we were able to figure it out, chances are other people have figured it out, too
  - ...and potentially using it for illegitimate purposes

Advisories

- If we didn't push the issue and publicly release information, nobody would have paid attention
- Most times, the vendor would keep stretching the time needed to fix the problem or just blow it off
  - Microsoft: "That research is purely theoretical."
  - L0pht: "Making the theoretical practical!"

Advisories

- Mudge on Exploits...
  - "We made tools. Give Jimmy Carter a hammer and he's going to build a new house for somebody. Give it to somebody with a little less ethics, they might go break a window with it or beat somebody over the head."
- Some people disagree(d) with our approach
  - We were doing things in a way that had never been done before
  - Ex.: `www.theregister.co.uk/2010/04/23/verizon_narcissistic_vulnerability_pimps/`

Senate Testimony (May 1998)

05/06/98 WED 15:00 FAX

United States Senate

COMMITTEE ON
GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

May 5, 1998

L0pht Heavy Industries Technologies, Inc.
P.O. Box 990857
Boston, MA 02199-0857

Dear L0pht:

On Tuesday, May 19, the Senate Committee on Governmental Affairs will hold a hearing to assess the information and computer security vulnerabilities in the Federal government.

Seven members of your organization are invited to appear before the Committee to present:

- Information on computer and communication system hacking;
- Specific security weaknesses in computer and communication systems which enable hackers to exploit information on these systems;
- Recommendations for improving system security in terms of software, hardware, and physical devices.

Senate Testimony (May 1998)

Weld Pond, Space Rogue, Tan, Kingpin, Mudge, Brian Oblivion, Stefan Von Neumann

Senate Testimony (May 1998)

- Discussed multiple threat vectors and worst-case scenarios against computer and communication systems
  - Software/application, network, hardware, wireless/satellite
  - Imagine what could happen with a dedicated, focused team (foreign government, military, intelligence agencies, organized crime, overseas competitors, etc.)
- Internet (and other technologies) not designed for security, but being used and trusted in that manner
  - Originally designed to *share* information

Senate Testimony (May 1998)

- Senator Lieberman: "Modern day Paul Reveres" for our warnings
- But, the media needed a sound bite...

Senate Testimony (May 1998)

L0PHT HEAVY INDUSTRIES

United States Senate
Committee on Governmental Affairs
Senator Fred Thompson, Chairman

Nation's elite hackers tell Congress what they're capable of doing to computer systems

Hackers: We could bring down Internet

Terrorists could add Internet to hit list

LOpht Heavy Industries, a Boston-based hackers club, and other experts warned the Senate Governmental Affairs Committee that lax protection of government and private sector computer systems could allow terrorists to:

- ▶ Redirect commercial flights by hacking onto the Federal Aviation Administration's air traffic control system.
- ▶ Manipulate State Department data so terrorists would be able to enter the country.
- ▶ Cause panic on Wall Street by shifting large sums of money around.
- ▶ Disrupt electricity, water and cellular services for large sections of the country.

They're not kidding — unfortunately

Seven hackers from the LOpht (www.LOpht.com) hacking community told a Senate committee last week that they could take down the Net in 30 minutes.

A band of seven hackers from Boston told a Senate Committee yesterday that they could bring down the foundations of the Internet in 30 minutes.

Hackers could crash Internet in 30 minutes

Washington

A Senate committee heard seven of the nation's top computer hackers claim yesterday that they could make the entire Internet crash in a half hour and boast that given more time and money, they could interrupt satellite transmissions or electricity grids and snoop on the president's movements.

AS SEEN ON TV

The hearing's focal point was the testimony of seven Boston-area computer specialists, described by Senator Fred Thompson (R-Tenn.), chairman of the committee, as belonging to the nation's leading "hackers think tank," known as LOpht (pronounced "loft").

Testifying under their Internet aliases — Mudge, Brian Oblivion, Space Rogue, Kingpin, Weld Pond, John Tan and Stefan Von Neumann

United States Senate
COMMITTEE ON
GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

Hackers Say Net Attack Could Be Devastating

It would take half an hour, they tell Senate

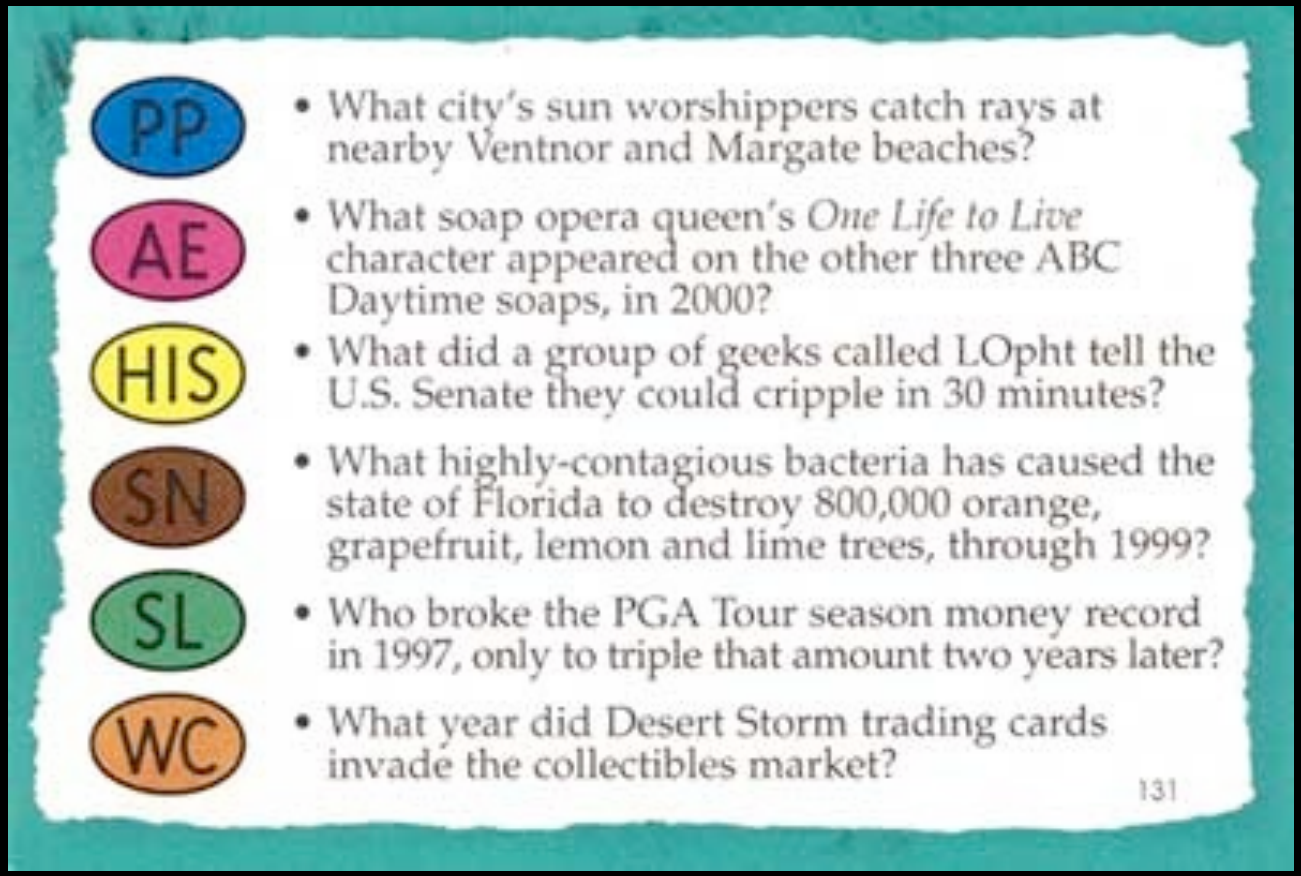
Pros: Net could be trashed in 30 minutes

Hackers claim serious weaknesses in US computer networks

Senate Testimony (May 1998)

Late Night with Conan O'Brien, May 20, 1998

Senate Testimony (May 1998)



Trivial Pursuit: Genus 5 (circa 2000)

Senate Testimony (May 1998)

Trivial Pursuit: Genus 5 (circa 2000)

The Sellout (2000)

Into the light: *Once shadowy computer code warriors like Kingpin are going legit*

Using Good Hackers to Battle Bad Hackers

IF YOU HAVE A MURKY PAST AND DOUBT you could become a dot-com millionaire, think again. Last week a scraggly band of hackers known as "L0pht Heavy Industries" joined with some straitlaced tech execs to form @Stake, an Internet-security consulting firm.

Newsweek, January 17, 2000

The Sellout (2000)

Has Anything Really Changed?

- Wireless
  - 1997: Intercepting POCSAG/Mobitex pager traffic (Kingpin)
  - Now: Insecure wireless networks, out-of-band authentication via text messaging, cellphone baseband hacking
  - Wireless was never fixed, but everyone jumped onto it, anyway
- Buffer Overflows/Browser Exploits
  - 1995: "How to Write Buffer Overflows" (Mudge)
  - ~1997: First IE buffer overflow (Dildog)
  - Now: Code is still written poorly and people/corporations/governments are getting 0wned all over the place!

Has Anything Really Changed?

- Consumer Watchdog
  - 1999: Cyberspace Underwriters Laboratories (CyberUL) (Tan)
    - Consumer Reports-like reviews and warnings of tech. products
    - `http://dl.packetstormsecurity.net/docs/infosec/cyberul.html`
  - Now: Still no accountability
    - Who is responsible for design/creation/release of insecure products?
    - Vendors can freely make erroneous claims
    - Users pay the price

Has Anything Really Changed?

- Things have arguably gotten worse
  - The online presence of people, companies, and organizations has grown larger
    - The entire world is connected now.
  - Users and vendors are not learning from history
  - Many companies now involved in this industry selling security products that give us a false sense of security
  - We rely on technology for every aspect of our daily lives
  - Exploits being developed on a daily basis...
    - ...and lots of script kiddies out there using them!

Has Anything Really Changed?

- People assume someone else is looking out for the technology we use and is keeping track of problems
  - Not verifying and validating for themselves
- Vulnerability/attack response
  - Many SW vendors are more accepting of security issues
    - security@*.com
    - Some even paying bug bounties (Google, Mozilla)
  - But, HW vendors are stuck in the 90s
- We still have a long way to go...

The End!

[joe @ grandideastudio.com]