Perspectives on Information Security

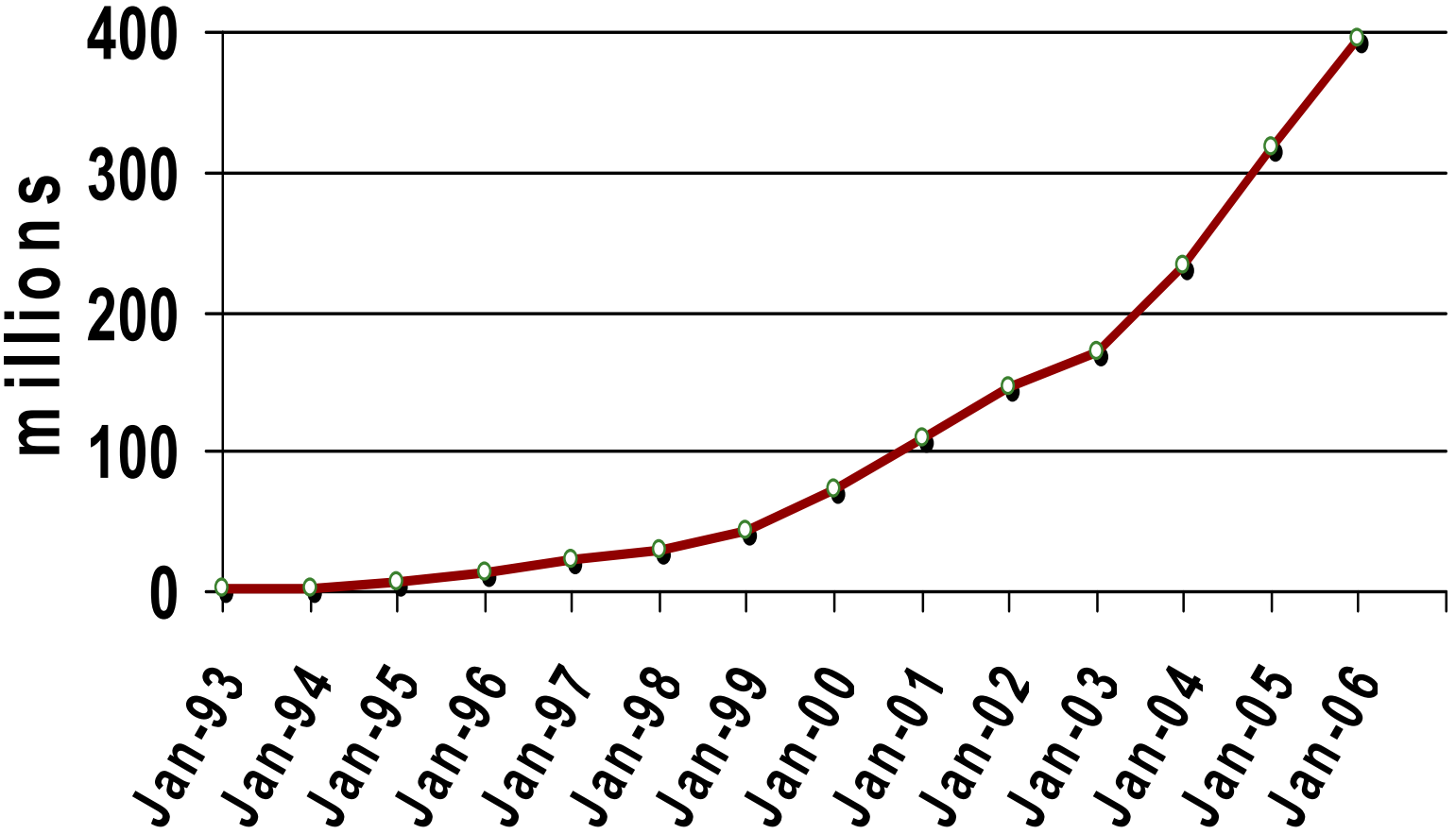
Stephen E Hansen

A Short History of the Internet and Cyber Naughtiness

… and why it matters

I know thy pride, and the *naughtiness* of thine heart. *1 Sam. xvii. 28.*

Internet Host Count †



† Source: Internet Software Consortium (http://www.isc.org/)

The Cold War drives research into resilient communications systems

- Need for attack/damage resistant communications systems
- ARPA research project leads to ARPANet

The system with a hard shell but a soft center

- The system succeeds in withstanding external damage.
- Poorly designed to withstand an internal attack.

An evolution of attack methodologies

- One-on-one attacks predominate until the late 1990s
  - Attacks require manual effort in real time
  - Some skill, training, and/or mentoring is required
- Exploit scripts and programs start to appear in the mid ’90s
  - Still one-on-one attacks
  - Less skill or training required. The rise of the Script Kiddies

An evolution of attack methodologies

- The appearance of the network vulnerability scanners in 1998 changes the threat model
  - Dramatically increases the ease and speed with which vulnerable systems can be found. Black Hats assemble huge lists of vulnerable systems but exploits still take time.
  - DSL and cable modem technologies start to replace dial-up modems in the home. Large numbers of vulnerable systems are now on-line 7x24.

An evolution of attack methodologies

- Automated exploit scripts were then coupled with the vulnerability scanners.
  - Large numbers of systems were compromised with no more effort than a few dozen keystrokes.
  - Many attacks were now completely automated.
- The resurrection of the worm
  - The exploit payload of the scanners are modified in some cases to download, install, and run copies of itself. Now it's a worm
  - The new code, once launched may run for months, or years.

An evolution of attack methodologies

- IRC gang channel wars have driven the development of bots and DoS techniques.
  - The usability of IRC as a communications medium has been severely degraded by the attacks on its server infrastructure.
  - Legitimate IRC Servers are now so unreliable that Bot Herders now set up their own IRC server networks.

The First Worm

- Was the 1988 Morris Worm the first DDoS attack?
  - Hundreds of affected systems each trying to infect their neighbors.
  - The out-of-control growth was due to a programming error. The network itself became the victim. Attacked from the inside it broke apart.

Followed by a decade of DoS

- Most attacks are one-on-one.
  - E-mail bombs (mailbox flooding) with multiple large files.
  - Host based resource exhaustion (memory, process tables, etc.)
  - Some OOB protocol stack exploits (the ping-of-death.)

Something new in ’95… Syn flooding

- Syn Floods
  - One of the first major use of low-level network protocol features as a DoS tool, and one of the most effective and hardest to defeat.
  - Other protocol based attacks also appear at about this time, sequence guessing, RST floods.
  - Still one of the more popular DoS attacks.

And the next new thing…

- Preceding the emergence of the large botnets, the next new thing in DDoS arrived in late 1997, the ICMP amplifier, or Smurf attack.
  - The attack makes use of misconfigured networks which allow incoming ICMP echo requests addressed to the network broadcast address.
  - A small number of attacking seed hosts can use this technique to bring down large hosts or networks.
  - Related attacks are UDP based Fraggle and chargen/echo mirrors.


I will not shut down major e-commerce sites
I will not shut down major e-commerce sites
I will not shut down major e-commerce sites
I will not sh commerce sites
I will not s pmmerce sites
I will not
Copyright 2000, The Halifax Herald Limited

Papa Smurf

- On Feb. 2000, large scale Smurf attacks disrupt access to several e-commerce sites, Yahoo, Ebay, Amazon, and others.
  - Smurf attacks are very difficult to trace.
  - Volunteers continually scan the Internet for networks capable of being used in smurf style attacks.

Attacking the Net

- October 2002, an attack is launched against the 13 DNS root servers.
  - ICMP flood attack.
  - It almost succeeded and it could have been much, much worse.

What makes a DDoS attack so dangerous and hard to defend against?

- Size and distribution.
  - Often thousands of hosts are brought to bear in a single attack.
  - The attacking hosts are often widely distributed around the Internet.
  - The attack mode itself may utilize spoofed source addresses.

If it's such a threat, why don't we see more attacks?

- One reason may be a lack of skill.
  - Use of generic attacks.
  - Use of inappropriate attacks.
  - Lack of understanding of basic network infrastructure and protocols.


OH, SURE. YOU CAN CRIPPLE THE INTERNET, BUT YOU CAN'T PUT YOUR DIRTY UNDERPANTS IN THE HAMPER...
MIKE LUCKOVICH

Why don’t we see more attacks?

- Another reason may be that it’s too risky.
  - Botnets are valuable commodities
  - Attacking botnets are vulnerable to discovery so attack durations are kept short intentionally.
  - The more damage done, the larger more dangerous the response. Just ask Mafiaboy.

Why don't we see more attacks? Remember MAD?

- The IRC gangs have multiple large botnets. Any attack is likely to result in a similar retaliatory attack.
- Attacks against the internet infrastructure would damage their own ability to work on-line, the one thing that most miscreants love to do more than almost anything else. It would be like blowing up your own house.

What can happen when the real world intrudes.

- What applies to a 16 year old in New Jersey is not likely to apply to the real world.
  - Power, money, politics, money, and hate.
  - Blackmail, money, cyberwar, and cyberterrorism.
  - Did I mention money?
  - These may not be your usual script-kiddies.

What can happen when the real world intrudes.

- Money, expertise, resources.
- Planning, research, and reconnaissance.
- Coordination and cooperation.

What if...
The November 2002 DNS attack redux

- What if the attack had been planned and executed by one of these groups?

The November 2002 DNS attack redux

- Select attack targets for maximum disruption and economic impact
  - The various DNS root servers are well hardened and difficult to attack successfully.
  - Attacks against selected financial and communications services would probably be easier to accomplish than an attack against DNS root servers.

The November 2002 DNS attack redux

- Mount a targeted attack using a flood of randomized service requests.
  - An example might be a flood of random DNS queries against the local DNS servers. This attack would be indistinguishable from valid queries.
  - Syn floods are still effective and more difficult to trace.

The November 2002 DNS attack redux

- Use multiple botnets, either each attacking for short periods, or start up a new one once the previous one is degraded.
- Prepare the attack for sustained service outages or for critical time points in the service activity.
  - A side-effect would be loss of confidence in Internet or reliability and suitability.

The Warhol Worm

- 0day exploit.
- Targeted, and distributed scanning.
- Destructive payload.

First described in **Warhol Worms: The Potential for Very Fast Internet Plagues** by Nicolas Weaver in 2001
http://www.iwar.org.uk/comsec/resources/worms/warhol-worm.htm
First implemented in the SQL Slammer Worm in January 2003 – Maximum growth obtained in approximately 3 minutes.

Next…

- Comparing Corporate vs. Academia
- Ramblings and thoughts on Information Security

Information Security in Industry and Academia

- Information as an asset
  - Value received when exchanged vs. shared.
- Perimeters
  - The campus vs. the castle
- Managing the hierarchy
  - The king vs. the nobles

Convergence

- Industry is seeing the collapse of the security perimeter.
- Academia is seeing the value in erecting check points, if not walls.
- Security zones

Information Security Management in a corporate environment

- Remain focused on the goal, minimize risk. In business this is most easily translated as “protect corporate assets from loss”. From an information security perspective this means protecting information assets. The keywords here are confidentiality, integrity, and availability (C.I.A.).
- Murphy ALWAYS wins. Shit happens. Failure is guaranteed so to be successful you must plan for failure.

The Myth of the Technical Solution

At the end of a thoughtful article on the future of nuclear war, J.B. Wiesner and H.F. York concluded that: "Both sides in the arms race are confronted by the dilemma of steadily increasing military power and steadily decreasing national security. It is our considered professional judgment that this dilemma has no technical solution. If the great powers continue to look for solutions in the area of science and technology only, the result will be to worsen the situation."

I would like to focus your attention not on the subject of the article (national security in a nuclear world) but on the kind of conclusion they reached, namely that there is no technical solution to the problem. An implicit and almost universal assumption of discussions published in professional and semi popular scientific journals is that the problem under discussion has a technical solution. A technical solution may be defined as one that requires a change only in the techniques of the natural sciences, demanding little or nothing in the way of change in human values or ideas of morality.

"The Tragedy of the Commons," Garrett Hardin, Science, 162(1968):1243-1248.

Policies and Procedures

- First policies, then procedures.
  - But it seldom works this way
- Document the why and review regularly
- There are always exceptions

Too many problems, never enough resources

- Absolute security requires infinite resources.
- Limited resources means that you must allocate them to where they will do the most good. Identify the area of maximum risk and allocate resources sufficient to reduce that risk so that is no longer the maximum (lather, rinse, repeat). Avoid the easy out or always addressing the vulnerability du jour.

Educating the masses

- Ignorance is not bliss and what people don't know will hurt them. Security education and awareness training is so important that is should be mandatory for all employees. Security, operations, and project development personnel should also be actively encouraged to obtain and maintain training in the latest security techniques.

Educating the Bosses

- C level education is needed to avoid “Management by Gartner”. Define your goals and publicize them. Make sure management understands why those goals were chosen and the benefits that will result from achieving them. If possible, frame the arguments in terms of benefits to be gained and not problems to be avoided.

Stephen Hansen

Information Security

CC & BW

Belowstairs.Org

Stephen.Hansen@Belowstairs.Org

This page intentionally left blank

The End