Carnegie Mellon®

Computing Infrastructure Risk

Issue, Analysis, and Recommendation

Lynn Robert Carter

2008-12-23

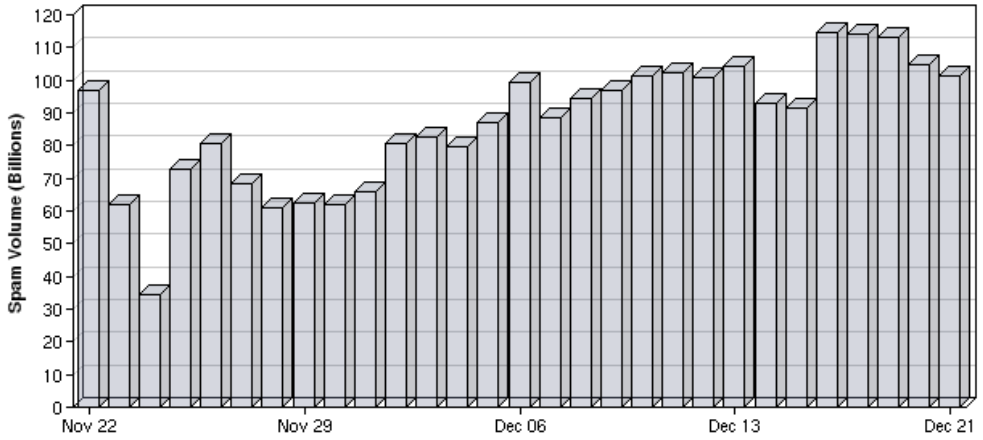
Agenda

- Computing infrastructure at risk
- The root cause
- Solution elements are known
- Barriers to implementing the solution
- Recommendation

Infrastructure Risk

- Our computing infrastructure is at risk
- Numerous botnets have compromised millions of machines around the world
- Denial of service attacks are the very visible tip of the “iceberg” of what is possible
- The SPAM load on the internet is near 90%

Spam load approaching 90%



Date	Spam Volume (Billions)	% of Global Email Volume	Spam Volume Change
2008 Dec 21	101.3	88.1%	-3% ↓
2008 Dec 20	104.6	86.8%	-8% ↓
2008 Dec 19	113.3	86.5%	-1% ↓
2008 Dec 18	114.1	86.4%	-0% ↓
2008 Dec 16	114.6	86.6%	25% ↑
2008 Dec 15	91.7	87.8%	-2% ↓
2008 Dec 14	93.2	88.4%	-10% ↓
2008 Dec 13	104.0	86.6%	3% ↑
2008 Dec 12	101.0	86.1%	-1% ↓
2008 Dec 11	102.4	86.2%	1% ↑
2008 Dec 10	101.5	86.1%	5% ↑
2008 Dec 09	96.8	86.4%	2% ↑
2008 Dec 08	94.6	87.4%	7% ↑

http://www.senderbase.org/home/detail_spam_volume?displayed=lastmonth&action=&screen=&order=

Distributed computing threat

- The SETI network has borrowed over 3.4×10^6 years of compute power from its donors
- Such compute power can be used to solve any number of problems, many to our detriment
  - Denial of service attacks and extortion
  - Discover access methods to secure systems
  - Find and compromise more machines

The rise of botnets

- Known botnets have compromised many millions of machines
  - A Dutch botnet of 1.5 million reported in 2005
    http://www.informationweek.com/shared/printableArticle.jhtml?articleID=172303265
  - FBI: a botnet of 1 million US machines in 2007
    http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm
- New “rootkits” make it harder to tell that a machine is compromised or repair the system short of initializing the hard drive

New targets of opportunity

- Personal computers are just one target that the bad guys can hit
- Any computing device that can access the internet is potentially at risk
  - Cell phones, PDAs, and media players
  - Entertainment systems
  - Navigation and control systems

Impact analysis-1

- The banking industry has been hit hard
- Identity theft through phishing is just one path
- Compromised computers can provide a wealth of valuable information
  - Anything the user sees or types can be stolen
  - Data on the hard drive can be read or altered
  - Built in cameras and microphones can be used, even when the device appears to be off

Impact analysis-2

- Denial of service attacks have caused firms to pay to avoid future attacks
- Most attacks appear to have been for monetary gain or to prove capabilities, but the attack on former Soviet Block Georgia hints at what can be done
- The full potential of their capabilities is not clear; many options are not easily profitable

Impact analysis-3

- Technology exists to falsify anything digital
  - The entertainment industry has shown us what is possible (The Curious Case of Benjamin Button)
  - Morphing still images, voices and videos is known technology and can be used to prompt potentially inappropriate action
- Many systems can be remotely controlled; the latest “Die Hard” movie is not totally fiction

Impact analysis-4

- Private networks and custom systems have the potential to avoid many of these risks
- All it takes to compromise such a solution is to have one weak link… humans are notoriously weak links in any security system
- Every aspect of business, government, and part of our military computing infrastructure is at risk and the exposure is growing

Agenda

- ✓ Computing infrastructure at risk
- ➢ The root causes
- Solution elements are known
- Barriers to implementing the solution
- Recommendation

The root causes

- Root cause: security was not a fundamental design criteria
- The so called von Neumann architecture can be easily misused to change a program so it performs completely unrelated functions
- The internet was designed to connect trusted researchers with the assumption that if you were on the net, you must be a good guy

von Neumann architecture

- While not actually von Neumann's creation, his computer architecture paper, where data and code are stored in the same memory, was the one that became popular
- Programs can alter their own code as easily as they alter data; some software depends on this
- File systems can also be easily compromised in much the same way

Buffer overflow

- Mitre reported that 85% of vulnerabilities in 2005 were application exploits
- Buffer overflow has been a common method employed to attack applications along with "design errors" and "exceptional conditions"
- Both operating systems and the applications provide pathways to compromise systems

Source: Buffer Overflow Attacks: Detect, Exploit, Prevent, by James C. Foster, *et al*

Security was not a design goal

- Computers, operating systems, programming languages, applications, and many internet protocols and systems were not designed to be secure
- More than 20 years has passed since the first major computer virus and we are still in an escalating game of “cat and mouse” or maybe more accurately, “whack a mole”

Agenda

- ✓ Computing infrastructure at risk
- ✓ The root causes
- ➢ Solution elements are known
- ■ Barriers to implementing the solution
- ■ Recommendation

Other architectures

- The “Harvard” architecture is similar to the “von Neumann” architecture, in that it uses both “stored program and data”; but they are not stored in the same memory
- Memory management schemes to separate data from instructions have existed
- Operating systems have existed that separate the operating system from the application

An unfortunate failure

- The iAPX 432 was a 1980s era microprocessor designed to support object orientation and segmented memory in hardware
- Replacing pointers with “protected object” references (called capabilities) that can only be created by privileged instructions is a way to design security into the hardware
- We need a hardened “security” processor

Virtualization

- Isolating the application and its environment from the real operating system and file system is another known solution
- Each time an application is launched, create a virtual machine, operating system instance, and application instance from a read-only file system employing independent checksums
- A “security” processor can host a mini-cloud of “security enabled” application processors

Trusted computing

- Security depends upon secure foundations
- Processors must be uniquely identified
- Authentication of message sender and source is a crucial element of secure computing
- Key elements of security must be implemented in the hardware so physical security can be used to guarantee cyber security

Trusted communication

- Authentication of pushed messages and similar checking for pulled messages is crucial
- Randomness and multiple-independent agents must be at the heart of authentication
  - The authentication agents used must be random
  - All agents must return the same message is key

Computing antibodies

- We must change the way systems are built so they are aware of attacks and respond to them
  - From notifying authorities to locking down certain key capabilities, a system should not just patiently endure an attack until the attacker succeeds
  - The new secure internet protocols must be able to track attacks back to its source via hardware
- Attacking others must have consequences

Agenda

- ✓ Computing infrastructure at risk
- ✓ The root causes
- ✓ Solution elements are known
- ➢ Barriers to implementing the solution
- ■ Recommendation

Barriers-1

- The bad guys will not just sit around idle while we implement our solution if they know what we propose to do
- Many users want anonymity and yet they want to deal with a trusted-known supplier
- Current computing/networking marketplace does not have enough true competition for normal market forces to work effectively

Barriers-2

- Many governments and corporations are in a conflict of interest; many might perceive that changing the *status quo* could cost them
- Changing internet equipment and all of the key infrastructure computers with be very costly
- A system is only as secure as its weakest link; people can still compromise aspects of this solution, even if only temporarily

Agenda

- ✓ Computing infrastructure at risk
- ✓ The root causes
- ✓ Solution elements are known
- ✓ Barriers to implementing the solution
- ➢ Recommendation

Recommendation-1

- The cyber equivalent of the Manhattan Project
- A black program must be launched to build a new set of foundational cyber building blocks upon which to build a secure infrastructure
- The solution must allow the current insecure implementations to run atop it as legacy until market forces and conditions dictate they be replaced with secure solutions

Recommendation-2

- Reuse of current computing assets is key, but it will not take precedence over security
- Asymmetric security is key; a trusted agent must be able to provide trusted copies of data to insecure users
- Parallel operation and proven protection of key national assets must be ensured before the existence of the project is made public

Recommendation-3

- Programs to quickly and fairly move the technology into the market are crucial
- Significant effort to prepare for education, training, skill, and behavior change programs must be developed in preparation for the program coming out of the black
- Preparation for political, legal, business and social issues must be a priority

Closing thoughts

- The cost of recovering from the damage to New Orleans has far exceeded what would have been required to protect it from Katrina
- The cost of effective financial oversight would have been several orders of magnitude less than the wealth that has been lost this year
- We cannot continue to play this cyber security game when so much is at stake

Carnegie Mellon®

Computing Infrastructure Risk

Issue, Analysis, and Recommendation

Lynn Robert Carter

2008-12-23