Overview
Four Grand Challenges in Trustworthy Computing

Reformatted from the presentation created and given by Dr. Gene Spafford, Purdue University.
Why Grand Challenges?

♦ Inspire creative thinking
  – Encourage thinking beyond the incremental

♦ Some important problems require multiple approaches over long periods of time

♦ Big advances require big visions
  – Small, evolutionary steps won’t take us everywhere we need to go
Why Trustworthy Computing?

♦ Identified as important in first Grand Challenges conference
♦ Clear and increasing public needs
♦ Poses significant research challenges
♦ Synergistic with current industry and government initiatives
  – e.g., NSF Cyber Trust
Challenge 1

Elimination of epidemic-style attacks by 2014

– Viruses and worms
– SPAM
– Denial of Service attacks (DOS)
Why is this a Grand Challenge?

♦ Epidemic-style attacks can be fast
  – Slammer worm infected 90% of vulnerable hosts in less than 30 minutes
  – Attacks exploit Internet’s connectivity and massive parallelism

♦ Price of entry is low for adversaries
  – Very easy for “uneducated” to launch the attack

♦ Unpredictable attack techniques and sources
  – Polymorphic worms and viruses
  – Anonymous attackers

♦ No organized active defense
  – Poor visibility into global Internet operations
  – No emergency global control
Current Trends

CERT-reported Attacks

Computer Viruses

Regular viruses, Macro viruses
Growth in Worms/Viruses

Unauthorized Use

Graph showing the percentage of respondents who had unauthorized use of their systems.

2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute
Types of Attacks

2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 481 Respondents
Amount of Losses by Type

- Sabotage: $871,000
- System penetration: $901,500
- Web site defacement: $958,100
- Misuse of public Web application: $2,747,000
- Telecom fraud: $3,997,500
- Unauthorized access: $4,278,205
- Laptop theft: $6,734,500
- Financial fraud: $7,670,500
- Abuse of wireless network: $10,159,250
- Insider Net abuse: $10,601,055
- Theft of proprietary info: $11,460,000
- Denial of service: $26,064,050
- Virus: $55,053,900

Total Losses for 2004 — $141,496,560

CSI/FBI 2004 Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents
Security Technologies Used

- Biometrics: 11%
- Public key infrastructure systems: 30%
- Smart cards/other one-time password tokens: 35%
- Encrypted files: 42%
- Intrusion prevention systems: 45%
- Reusable account/login passwords: 56%
- Encryption for data in transit: 64%
- Intrusion detection: 68%
- Server-based access control lists: 71%
- Firewalls: 98%
- Antivirus software: 99%

2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute
2004: 483 Respondents
Importance of Security Technologies

![Bar Chart showing the percentage of respondents who believe in the importance of various security technologies.

- Cryptography: 28%
- Investigations and legal issues: 43%
- Security systems architecture: 48%
- Economic aspects of computer security: 51%
- Security management: 63%
- Access control systems: 64%
- Network security: 70%
- Security policy: 70%

2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 480 Respondents]
Qualitative Trends

♦ Commoditization – rapid assimilation and dissemination of attack methods/code
♦ Convergence – integration of attack modes (e.g., worms that deposit remote access Trojans)
♦ Social engineering – adopting new enticements for unwary users
♦ Additional propagation vectors – including P2P systems, chat systems
♦ Technical vulnerabilities – exploiting known technical vulnerabilities causes most damage
♦ Speed of propagation – infection occurs before human intervention possible (need for automated defenses)
♦ Countermeasure awareness – malcode authors test against popular defenses and use active countermeasures (disable anti-virus software, act benign in simulated environment)
♦ Common platforms – attacks mounted against widely deployed systems

## Worm Taxonomy

<table>
<thead>
<tr>
<th>target discovery</th>
<th>scanning, lists (pre-generated, externally generated, internal), passive</th>
</tr>
</thead>
<tbody>
<tr>
<td>carrier</td>
<td>self-carried, second channel, embedded</td>
</tr>
<tr>
<td>activation</td>
<td>human, activity-based, scheduled processes, self</td>
</tr>
<tr>
<td>payloads</td>
<td>none, remote control, spam-relay, html-proxies, dos, data collection, access for sale, data damage, physical world (control, dos, reconnaissance, damage), maintenance</td>
</tr>
<tr>
<td>attackers</td>
<td>curiosity, power, commercial advantage, criminal gain, protest, terrorism, cyber warfare</td>
</tr>
</tbody>
</table>

Challenge 2

Develop tools and principles that allow construction of large-scale systems for important societal applications that are highly trustworthy despite being attractive targets.

– e.g., patient medical record databases
– e.g., electronic voting systems
– e.g., law enforcement databases
Why is This a Grand Challenge?

♦ Worldwide, computing technology is being adopted to support critical applications
♦ We do not know, in general, how to build systems that resist failures and repel attacks with high confidence
♦ We do not understand how to compose systems into networks of trustworthy systems
Elements of a Secure System

♦ Specification/Policy
  – secrecy
  – integrity
  – availability
  – accountability

♦ Implementation/Mechanism
  – isolation (impractical)
  – exclusion (code signing, firewalls)
  – restriction (sandboxing)
  – recovery
  – punishment

♦ Correctness/Assurance
  – trusted computing base
  – defense in depth
  – usability
  – theory

“Gold Standard” Issues

• Authentication
• Authorization
• Audit

(Au = gold)

aka: AAA

Reference Monitor Model

Chains of Trust

- need for end-to-end access control in distributed environments
- based on creating evidence for identities of principal
- delegation via “speaks-for” principle
- connecting “chain” of reasoning end-to-end

Challenge 3

Within 10 years, develop quantitative information-systems risk management that is at least as good as quantitative financial risk management.
Why is This a Grand Challenge?

♦ We do not understand the full nature of what causes IT risk
♦ We do not understand emergent behavior of some vulnerabilities and systems
♦ Failures in networked systems are not independent
Why Does it Matter?

♦ We cannot manage if we cannot measure: If you don’t have a measure you will either under-protect or over-spend

♦ What you measure is what you get
  – Measuring the wrong thing is as bad or worse than not measuring anything at all
  – The measures ultimately need to be consistent, unbiased, and unambiguous
Challenge 4

For the dynamic, pervasive computing environments of the future, give computing end-users security they can understand and privacy they can control.

- Technology can easily outrun comprehensibility.
  Security implementation must not make this worse
- Must not lose control of my information, my privacy, my location
Barriers to Overcome?

- User needs are much broader than traditional security models
  - Bridge the gap from user to mechanism
  - Privacy doesn’t always fit in traditional security models
- Dynamic environments are challenging
- Device heterogeneity is challenging
- Multiple competing stakeholders
- It’s difficult, in general, to make things usable
- Real-life user security requirements and policies are hard to express in terms of current mechanisms