Grand Challenges and Open Questions in Trusted Systems

Carl Landwehr (clandweh@nsf.gov)
Cyber Trust Coordinator
National Science Foundation

December 3, 2004
Megabytes of PC hard drive storage per retail dollar, 1980-2000
4.5 decimal orders of magnitude in 20 years

Data culled 11/2004 from:
http://www.littletechshoppe.com/ns1625/winchest.html
Estimated Internet Traffic
(Terabytes in December, log scale)

5 decimal orders of magnitude in 12 years

Source: A. M. Odlyzko, Internet traffic growth: Sources and implications.

But...
"Note:
Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks.

Therefore, as of 2004, we will no longer publish the number of incidents reported.” -- CERT
Spread of Spyware (U Washington)

Values indicate percentage of 872

Dates discovered for 872 out of the 1077 Gator Clients

From presentation by Siddhath Tharker at:
http://pollux.usc.edu/~ozden/599/slides/cs599_Siddharth_Spyware_Sybil_Sp04.ppt
“Since early October [2004], Corporate SpyAudit has been used to scan more than 10,000 computers in over 4,100 companies, said Stiennon. On average, it sniffed out 20 pieces of spyware per corporate computer, with about 5 percent of the systems harboring the most malicious kinds of spyware, such as system monitors (like keyloggers) and Trojan horses.”

Richard Stiennon, Webroot's vice president of threat research, as quoted by Greg Keizer, TechWeb.com, 1 December 2004
On the FBI's Wanted List (11/5/04)

JIE DONG

- for defrauding Internet auction site users out of approximately $800,000.

SAAD ECHOUDAFNI

- for allegedly hiring computer hackers to launch attacks against his company's competitors ... vendor based in Los Angeles reported a series of crippling denial of service attacks that effectively halted its business for nearly two weeks ... resulted in losses ranging from $200,000 to over $1 million.
There are LOTS of Research Agendas out there!

- 1998 NSF CIP workshop
- 2001: NSF Workshop on Information Technologies for Security
- 2002: CERIAS/Accenture Roadmap to Safer Wireless World
- 2002: PL 105-307 topic list
- 2002: NAS/CSTB IT for Counterterrorism: www.nap.edu
- 2003: I3P Research Agenda
- 2003: NSTAC R&D Exchange
- 2003: NITRD: LSN/NRT workshop on scalable cybersecurity
- 2003 CRA Conference on "Grand Research Challenges in Information Security & Assurance"
- 2004 PITAC cybersecurity subcommittee recommendations
- (2005) IRC updated Hard Problems List
From “IT for Counterterrorism” report - research priorities

- Improved Information and Network Security:
  - C3I for Emergency Response
  - Information Fusion
  - Privacy and Confidentiality
  - Planning for the Future

<table>
<thead>
<tr>
<th>Information and Network Security Area</th>
<th>Research Criticality</th>
<th>Difficulty</th>
<th>Progress and Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection and Identification</td>
<td>High</td>
<td>Difficult</td>
<td>5-9 Years</td>
</tr>
<tr>
<td>Architecture and design for containment</td>
<td>High</td>
<td>Difficult</td>
<td>5-9 Years</td>
</tr>
<tr>
<td>Large system backup and decontamination</td>
<td>High</td>
<td>Difficult</td>
<td>5-9 Years</td>
</tr>
<tr>
<td>Less buggy code</td>
<td>High</td>
<td>Very Difficult</td>
<td>5-9 Years</td>
</tr>
<tr>
<td>Automated tools for system configuration</td>
<td>High</td>
<td>Difficult</td>
<td>1-4 Years</td>
</tr>
<tr>
<td>Auditing functionality</td>
<td>Low</td>
<td>Difficult</td>
<td>10+ Years</td>
</tr>
<tr>
<td>Trade-offs between usability and security</td>
<td>Medium</td>
<td>Difficult</td>
<td>5-9 Years</td>
</tr>
<tr>
<td>Security metrics</td>
<td>Medium</td>
<td>Difficult</td>
<td>1-4 Years</td>
</tr>
<tr>
<td>Field studies of security</td>
<td>High</td>
<td>Easy</td>
<td>1-4 Years</td>
</tr>
</tbody>
</table>
CRA Grand Challenges 11/2003

CRA Conference on "Grand Research Challenges in Information Security & Assurance" yielded:

1) Eliminate epidemic-style attacks within 10 years
   - Viruses and worms
   - SPAM
   - Denial of Service attacks (DOS)

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

3) Within 10 years, quantitative information-systems risk management is at least as good as quantitative financial risk management.

4) For the dynamic, pervasive computing environments of the future, give end users security they can understand and privacy they can control.
PITAC Draft F&R, 11/2004 - Areas in need of research funding:

1. Computer Authentication Methodologies
2. Securing Fundamental Protocols
3. Secure Software Engineering
4. End-to-end System Security
5. Monitoring and Detection
6. Mitigation and Recovery Methodologies
7. Cyberforensics and Technology to Enable Prosecution of Criminals
8. Modeling and Testbeds for New Technologies
9. Metrics, Benchmarks, and Best Practices
10. Societal and Governance Issues
We built it – can we fix it?

• How **must** it be?
  - What are the limits?

• How **might** it be?
  - What are the possibilities?
Some Limits

- **Mathematical/logical**
  - Access control questions in some models are undecidable (HRU, 1976)
  - Obfuscation is impossible (BGIRSVY, 2001)
  - One time pads can support unbreakable ciphers
  - Shannon's theorem bounds channel capacity
- **Physical**
  - Reading a quantum-entangled photon alters its state
  - The speed of light limits the rate of information transmission
- **Economic**
  - Rational consumers don't spend money on undetectable properties
- **Social**
  - Perfection is not of this world

**Observation:** the economic and social limits have limited security more than the mathematical and physical ones
Some Challenges

- Create and deploy mechanisms to allow us to identify where a message originated with a fair degree of certainty
- Figure out how to build system interfaces that real people can understand and use
- Learn how to organize systems so that even when imperfect, they are not prone to catastrophic failure under attack
What’s the future of security relative to the networked world?

- **My opinions only:**
  - It’s going to get worse before it gets better
    - No obvious, readily deployable solutions to spam, virus woes
    - Even MS’s best efforts don’t seem to be helping that much
    - The attack community seems energized
    - VoIP may become a new target
  - It will get better eventually
    - Commercial pressures will mount
    - Technology will advance
      - Expect solutions that combine software and hardware
      - High assurance will be in the hardware, flexibility in the software
  - It will remain an interesting area to work because there are many possibilities and we are a long way from the limits
Thank you.

Questions?

Carl Landwehr
National Science Foundation
Program Director, Cyber Trust
CISE/CNS
E-mail: CLandwehr@nsf.gov
703-292-8950