**New Threats to Cyber-Security**

**Sherman /Mark S.**

Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213

Approved for public release, distribution unlimited.

The original document contains color images.

<table>
<thead>
<tr>
<th>SECURITY CLASSIFICATION OF:</th>
<th>17. LIMITATION OF ABSTRACT</th>
<th>18. NUMBER OF PAGES</th>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. REPORT</td>
<td>SAR</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>unclassified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. ABSTRACT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>unclassified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. THIS PAGE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>unclassified</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
New Threats to Cyber-Security

- Usual view of threat environment
- Looking backwards from today’s threats
- Looking forwards to future threats
- The need for prevention is pressing
Usual view of threat environment

47% of US adults had their personal information exposed by hackers

90% of US businesses report being hacked
59% report being hacked more than once

Nearly 250,000 malware artifacts by 1Q14

Sources: Poneman Institute, CNNMoney study, May 28, 2014; McAfee Quarterly Threat Report, June 2014; Wall Street Journal, Feb 26, 2014

retailcustomerexperience.com - 5_lessons_learned_from_recent_retail_data_breaches.pdf
Looking backwards from today’s threats

92% of the 100,000 incidents from the last 10 years can be described by 9 basic patterns

- Insider misuse
- DOS attacks
- Cyber-espionage
- Crimeware
- Web app attacks
- Physical theft and loss
- Payment card skimmers
- Point-of-sale intrusions
- Miscellaneous errors
Looking forwards to future threats

Cyber threats track evolution of technology

- Software is the new hardware
- Covering the next last mile
- Expanding endpoints
- Development is now assembly
Software is the new hardware

IT moving from specialized hardware to software, virtualized as
- Memory
- Storage
- Servers
- Switches
- Networks

Cyber-physical systems (CPS) evolving to a computer with interesting peripherals
- Airplane function in software moved from 8% to 80% since 1960
- Software defined radios drive communication
- Television evolved to digital signal processors

- Hardware security needs software analogs
- New programming models need secure coding guidelines
- Guard against side channel attacks enabled by virtualization
Covering the next last mile – securing the border and end points

The last mile has expanded to

- Cellular
  - Main processor
  - Base band processor
  - Secure element (SIM)

- Automotive
  - Intravehicular: more than 50 networked processors
  - Vehicle to infrastructure (V2I): congestion management, emergency services, law enforcement
  - Vehicle to vehicle (V2): safety, efficiency

- Industrial and home automation
  - SCADA
  - Bluetooth
  - Zigbee

- Aviation
  - Fly by wire
  - Next Gen air traffic control

- Smart grid
- Embedded medical devices
Development is now assembly

At least 75% of organizations rely on open source as the foundation of their applications.
Open source supply chain is vulnerable

- Security skills haphazard among developers
- No providence of code
- No process for updates

→ Transitive vulnerabilities from open source dependencies
An ounce of prevention is worth a pound of cure

“We wouldn't have to spend so much time, money, and effort on network security if we didn't have such bad software security.”

The need for prevention is pressing

19% fail to carry out security requirement definition
27% do not practice secure design
30% do not use static analysis or manual code review during development
47% do not perform acceptance tests for third-party code

More than 81% do not coordinate their security practices in various stages of the development life cycle.

Foresight leads to proactive defense

Tracking evolution of technology arms developers for securing the next generation of applications
Contact Information

Mark Sherman
(412) 268-9223
mssherman@sei.cmu.edu

Web Resources (CERT/SEI)
http://www.cert.org/
http://www.sei.cmu.edu/