

S5: New Threats to Cyber-Security

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Mark Sherman, PhD
Technical Director, CERT
mssherman@sei.cmu.edu

29-Oct-2014



Report Documentation Page

*Form Approved
OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 29 OCT 2014	2. REPORT TYPE N/A	3. DATES COVERED	
4. TITLE AND SUBTITLE New Threats to Cyber-Security		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Sherman /Mark S.		5d. PROJECT NUMBER	
		5e. TASK NUMBER	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.			
13. SUPPLEMENTARY NOTES The original document contains color images.			
14. ABSTRACT			
15. SUBJECT TERMS			
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified	
			SAR
			15
			19a. NAME OF RESPONSIBLE PERSON



Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0001805



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

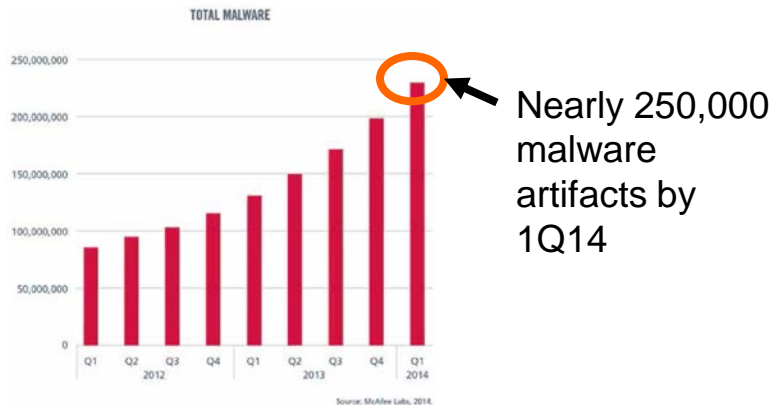


Usual view of threat environment

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



EARNINGS

Target Earnings Slide 46% After Data Breach

ARTICLE FREE PASS
Enjoy your free sample of exclusive subscriber content. \$12 for 12 Weeks [SUBSCRIBE NOW](#)

By PAUL ZIOBRO [CONNECT](#)

Updated Feb. 26, 2014 6:26 p.m. ET



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

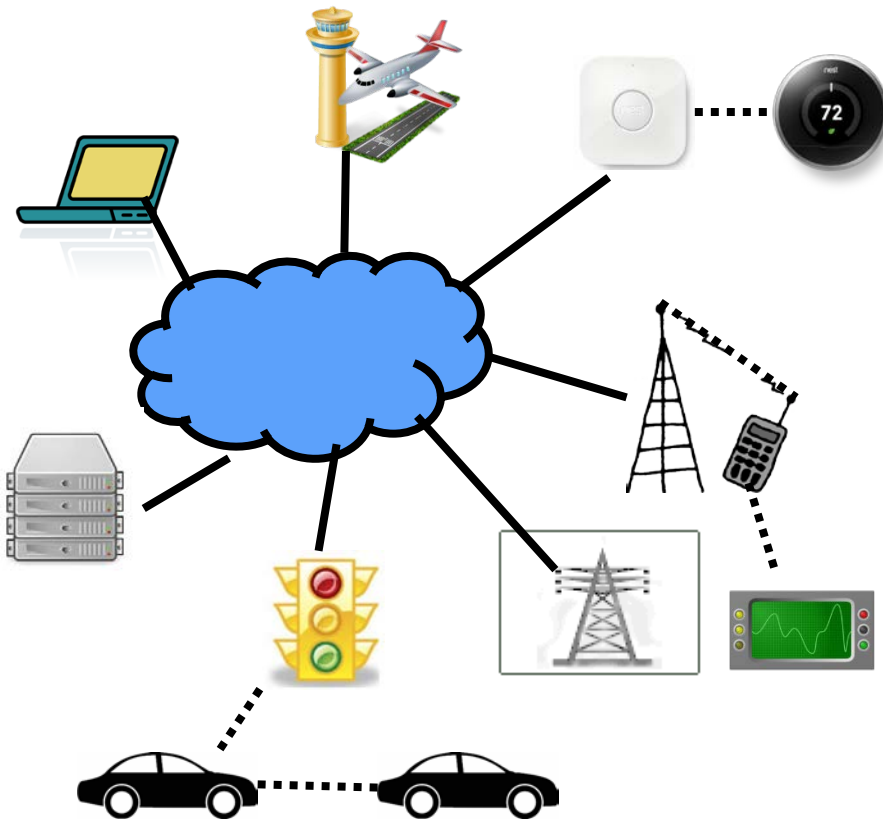
Cyber-physical systems (CPS) evolving to a computer with interesting peripherals

- 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



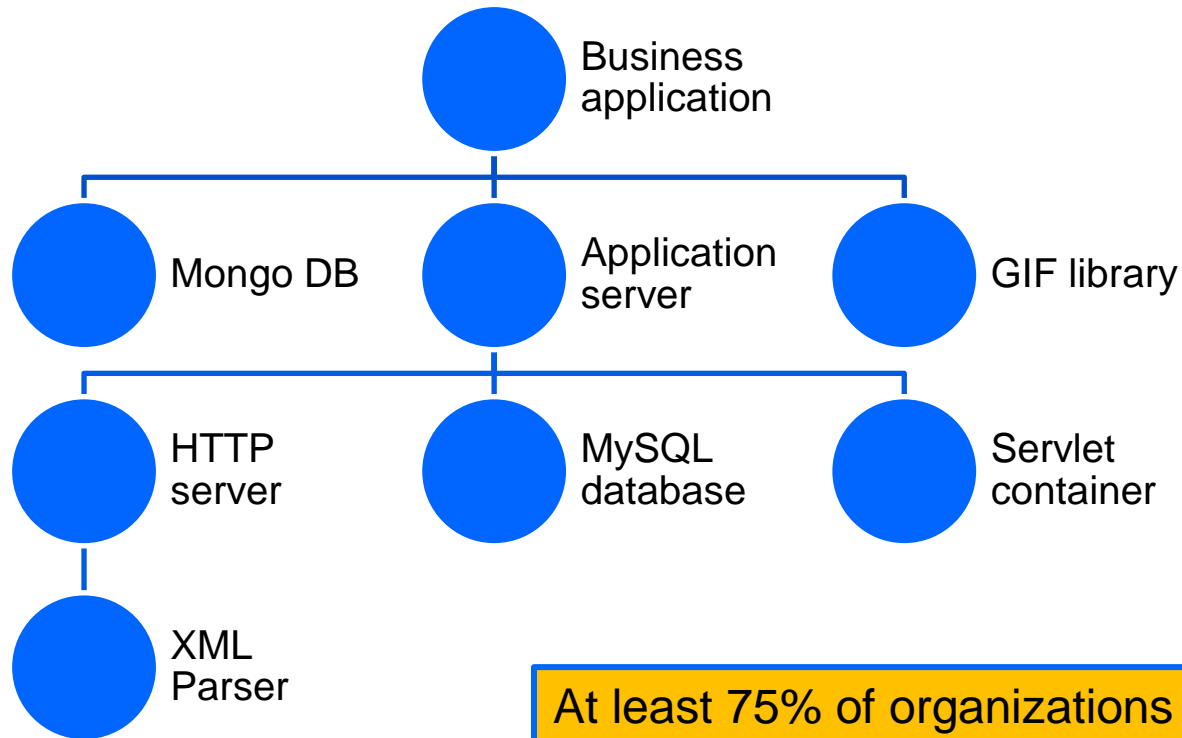
The last mile has expanded to

- 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 (V2V): safety, efficiency
- Industrial and home automation
 - SCADA
 - Bluetooth
 - Zigbee
- Aviation
 - Fly by wire
 - Next Gen air traffic control
- Smart grid
- Embedded medical devices





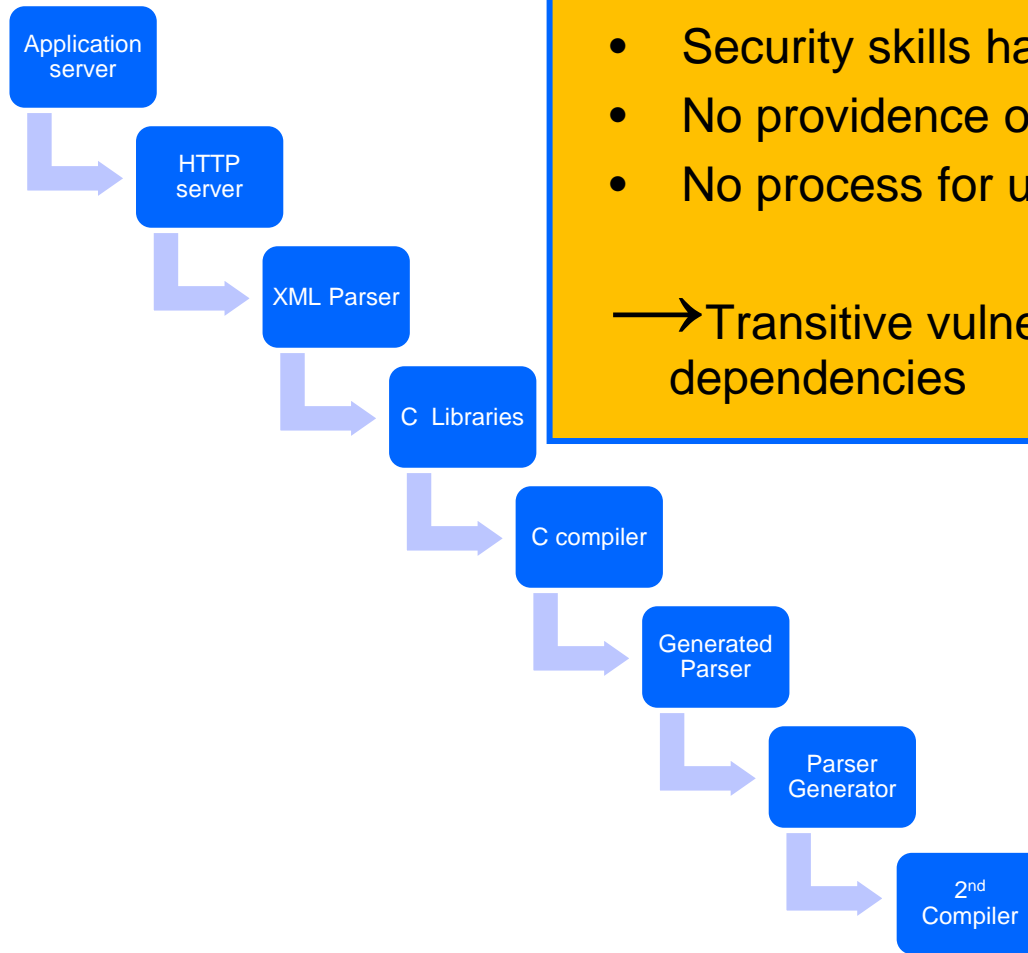
Development is now assembly



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.”

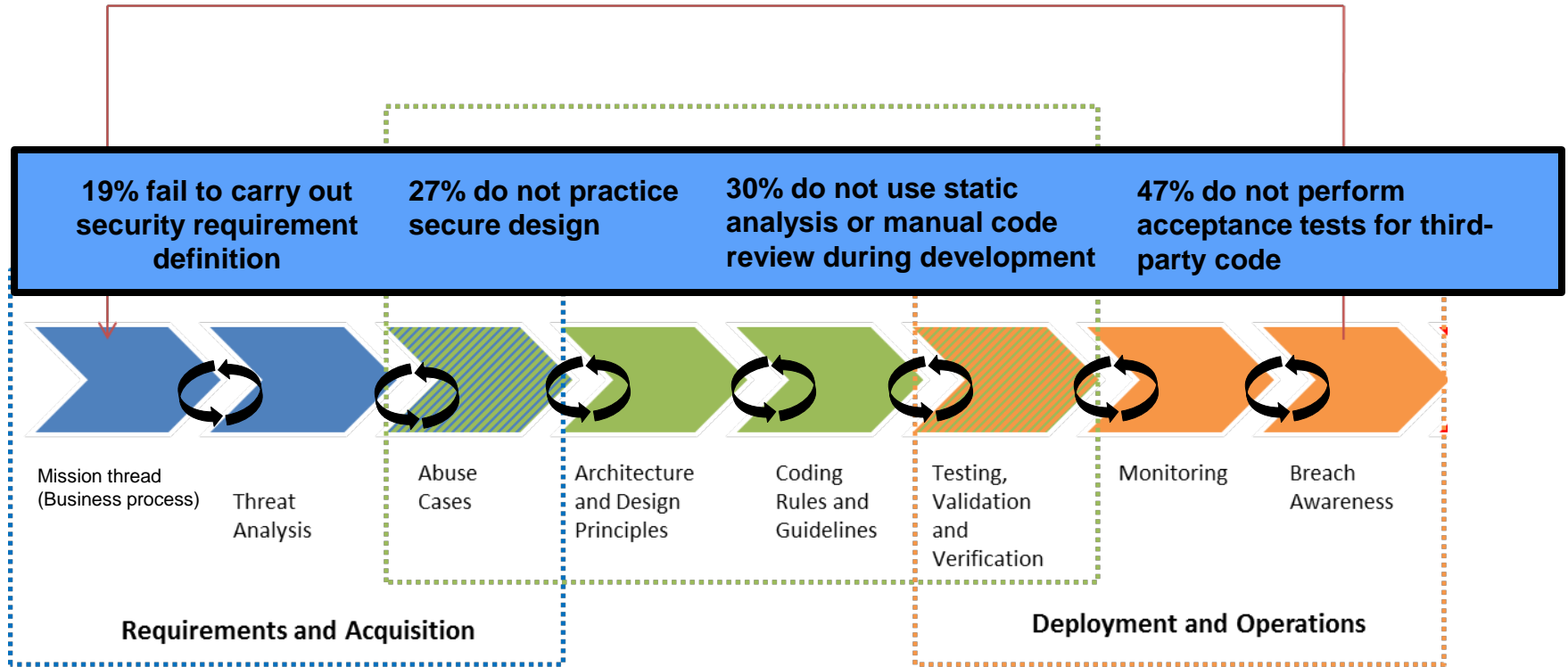
Bruce Schneier in Viega and McGraw,
“Building Secure Software,” 2001





The need for prevention is pressing

Sustainment



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

Source: Forrester Consulting, "State of Application Security," January 2011





Foresight leads to proactive defense



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





Contact Information

Mark Sherman

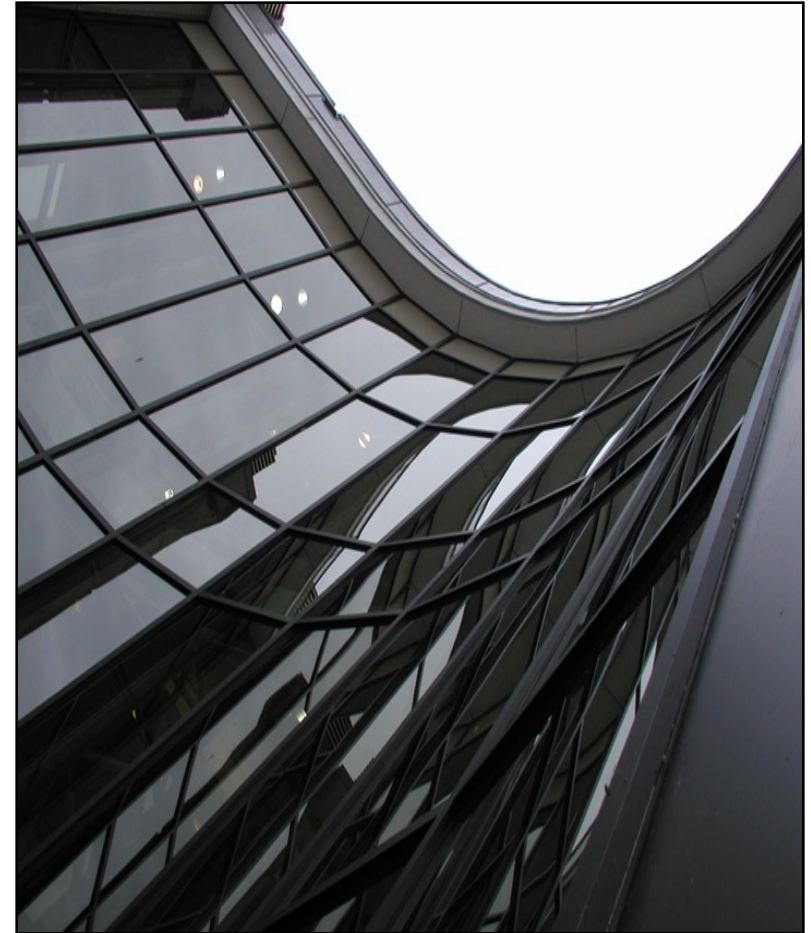
(412) 268-9223

mssherman@sei.cmu.edu

Web Resources (CERT/SEI)

<http://www.cert.org/>

<http://www.sei.cmu.edu/>





Software Engineering Institute

Carnegie Mellon University



Software Engineering Institute

Carnegie Mellon University

Mark Sherman
S5: New Threats to Cyber-Security
© 2014 Carnegie Mellon University