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

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	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**15**	

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.

DM-0001805

New Threats to Cyber-Security

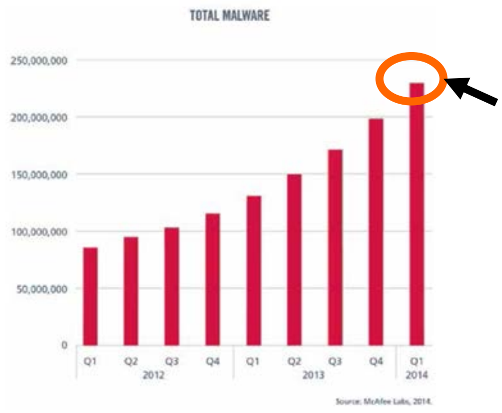
- Usual view of threat environment
- Looking backwards from today’s threats
- Looking forwards to future threats
- The need for prevention is pressing

Usual view of threat environment

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

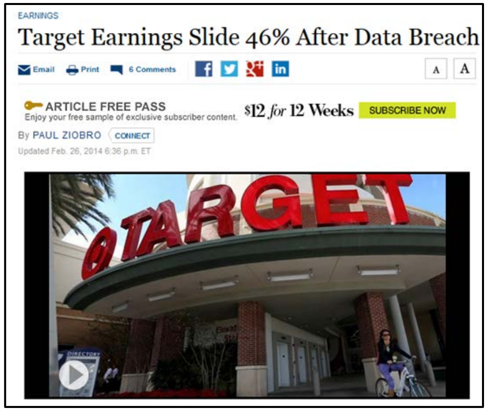
90% of US businesses report being hacked

59% report being hacked more than once



Source: McAfee Labs, 2014.

Nearly 250,000 malware artifacts by 1Q14



EARNINGS

Target Earnings Slide 46% After Data Breach

ARTICLE FREE PASS
Enjoy your free sample of exclusive subscriber content.

By PAUL ZIOBRO

Updated Feb. 26, 2014 6:36 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

verizon

2014 DATA BREACH INVESTIGATIONS REPORT

INSIDER MISUSE
MISCELLANEOUS ERRORS
DOS ATTACKS
PHYSICAL THEFT AND LOSS
CYBER-ESPIONAGE
CRIMEWARE
PAYMENT CARD SKIMMERS
WEB APP ATTACKS
POINT-OF-SALE INTRUSIONS

92%

THE UNIVERSE OF THREATS MAY SEEM LIMITLESS, BUT 92% OF THE 100,000 INCIDENTS WE'VE ANALYZED FROM THE LAST 10 YEARS CAN BE DESCRIBED BY JUST NINE BASIC PATTERNS.

Conducted by Verizon with contributions from 50 organizations from around the world.

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

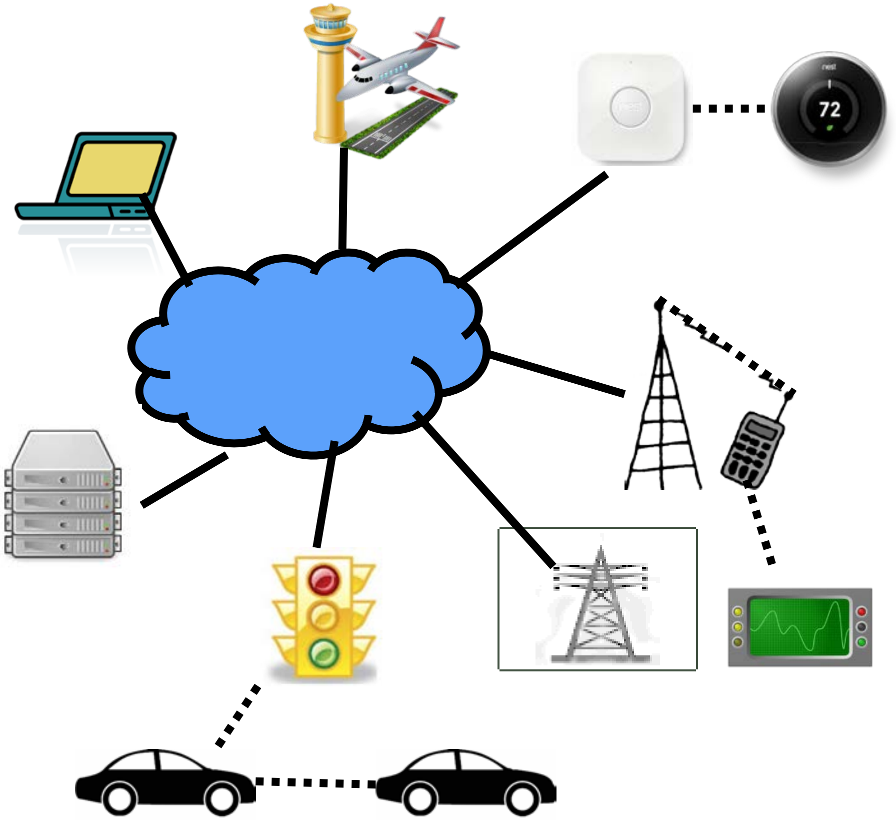
- Memory
- Storage
- Servers
- Switches
- Networks

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

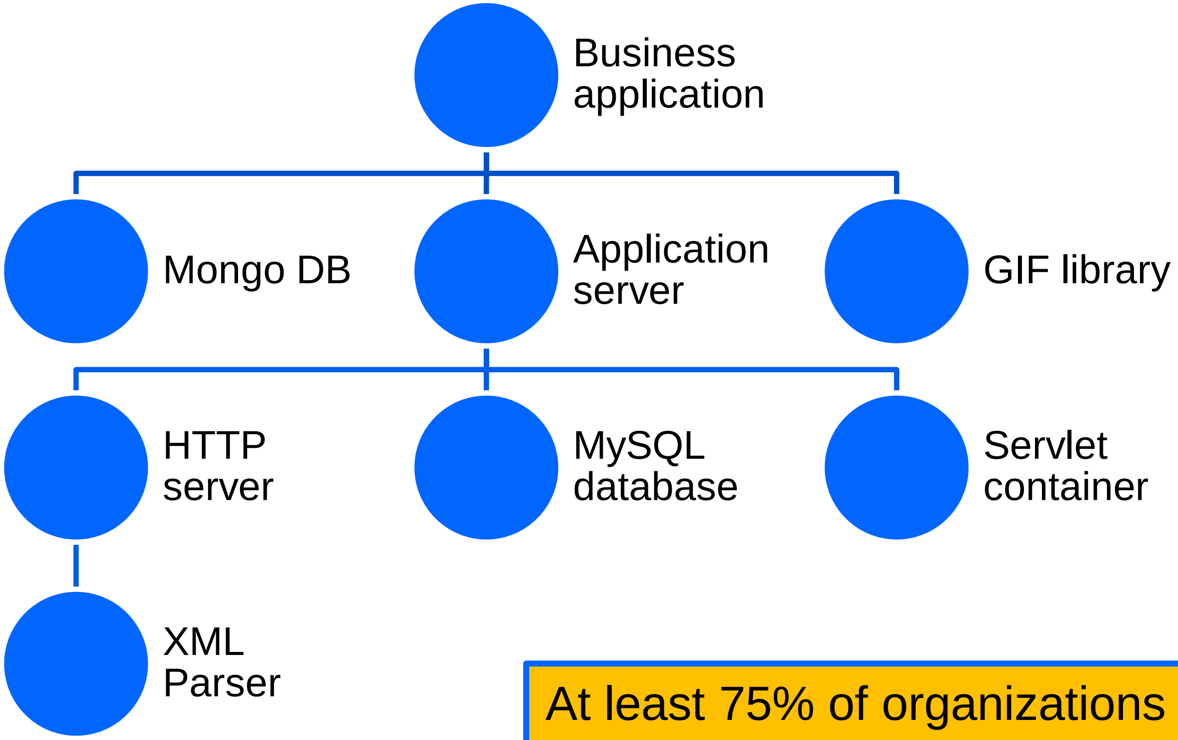
Covering the next last mile – securing the border and end points



The last mile has expanded to

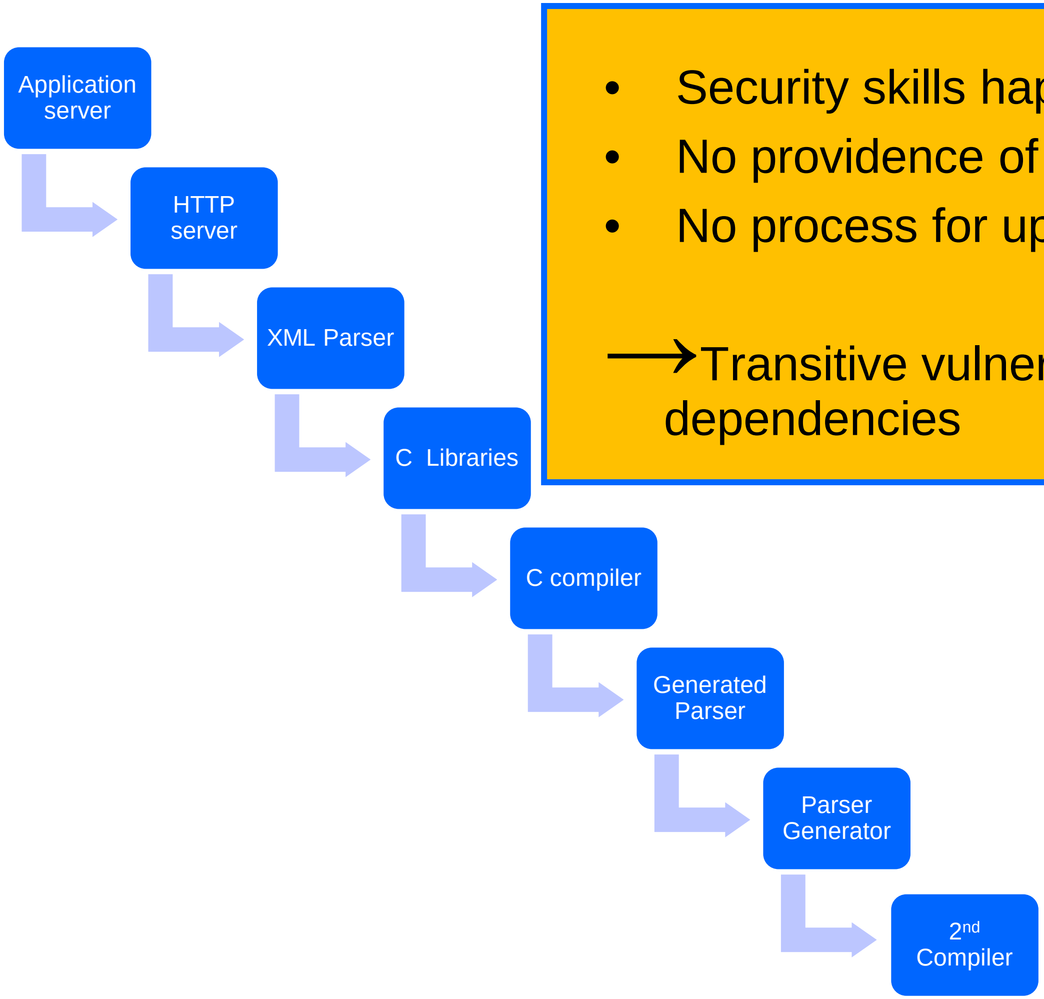
- Cellular
  - Main processor
  - Base band processor
  - Secure element (SIM)
- Automotive
  - Intravehicular: more than 50 networked processors
  - Vehicle to infrastructure (V2I): congestion management, emergency services, law enforcement
  - Vehicle to vehicle (V2): safety, efficiency
- Industrial 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

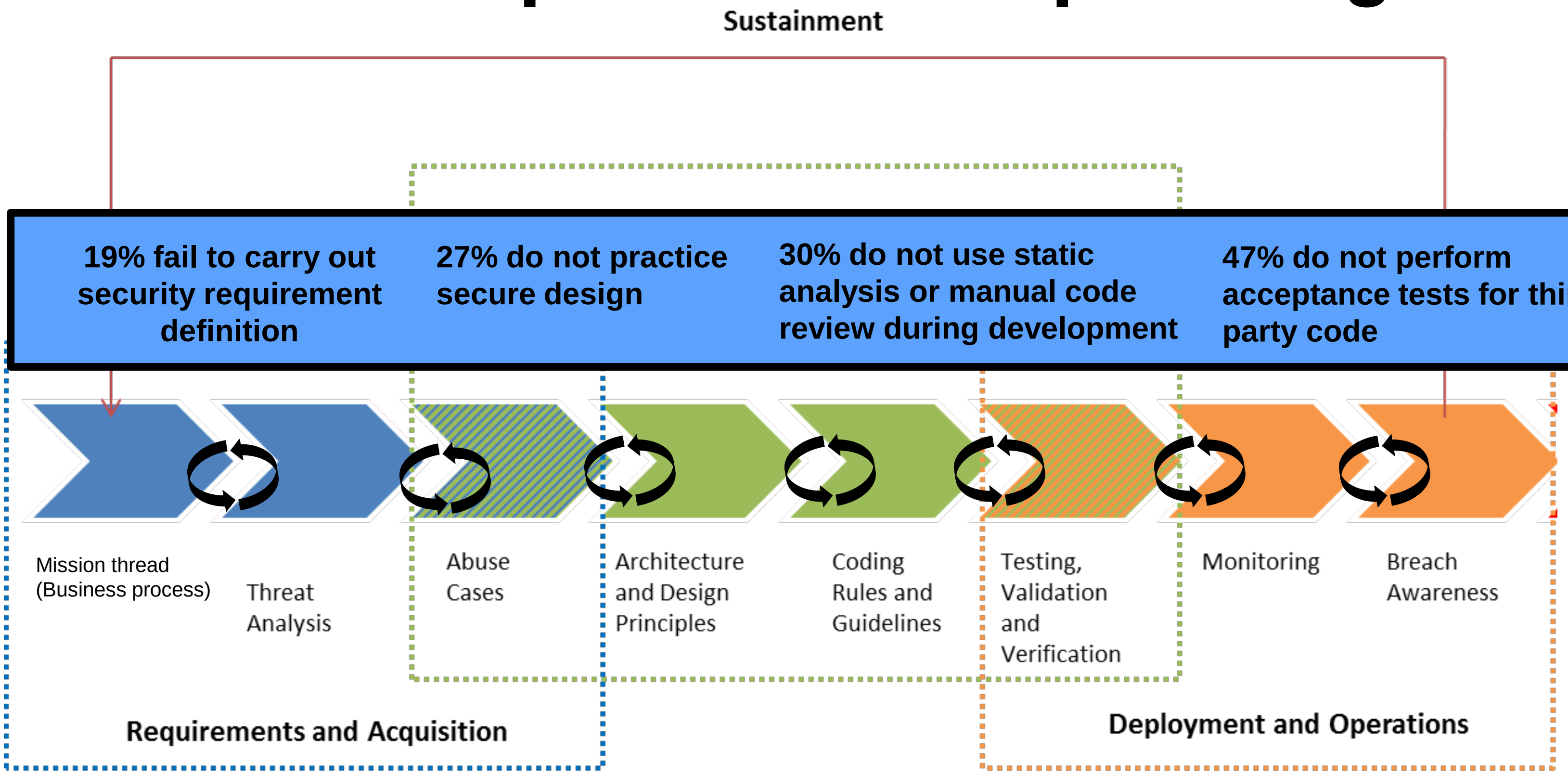
⟶Transitive vulnerabilities from open source dependencies

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.”

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

The need for prevention is pressing



Sustainment

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

Mission thread (Business process)

Threat Analysis

Abuse Cases

Architecture and Design Principles

Coding Rules and Guidelines

Testing, Validation and Verification

Monitoring

Breach Awareness

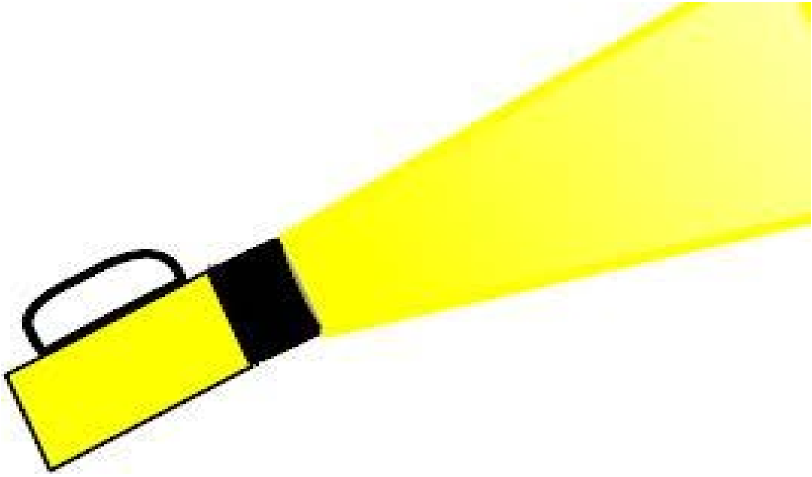
Requirements and Acquisition

Deployment and Operations

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

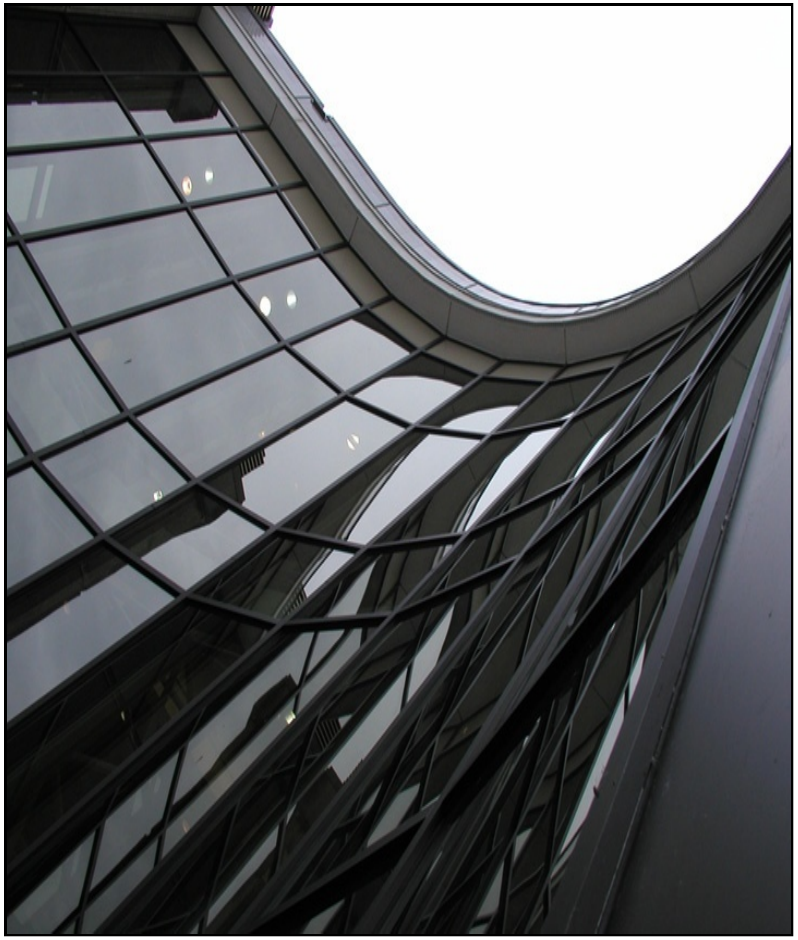
(412) 268-9223

mssherman@sei.cmu.edu

Web Resources (CERT/SEI)

http://www.cert.org/

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



Software Engineering Institute | Carnegie Mellon University