Security Issues: Application Security and the Internet of Things

Wesley Simpson
Chief Operating Officer, (ISC)$^2$
About Me

» Chief Operating Officer (ISC)²
✓ 10 years in Operational Security in USAF
✓ 20 years in Software Development Lifecycle Management (Fortune 500)
  • IBM
  • Lotus Development Corporation
  • Fidelity Investments
  • Bank of America
  • Delta Air Lines
  • Time Warner
✓ Focus on Media & Entertainment
  • Digital Asset Management
  • Mobile Development
  • Product Development / PMO
✓ Certifications: ITIL v3, PMP, CSTE, CASQ, CSM, CSPO
It takes well-trained and certified personnel to recognize and mitigate threats and breaches.
The term “cybersecurity” is inconsistently applied around the world.

The term cybersecurity appears to get more attention for our profession is an attractive reason to start using the term in a broader context, but is it the right reason?

There are other terms that are inconsistently applied within the profession that take on different country-by-country terms, definition and usages.
Here is what we know...

» More infosec spend than ever...
» 2014 was the year of the breach
» Awareness is up – boards paying attention
» Jobs lost
Common Attacks

- Malware to steal credentials and abuse application
- Backdoor – command and control attacks
- SQL Injection
- Secondary attacks
Application Security Study

- Conducted by Osterman Research on behalf of (ISC)²
- 143 respondents
- Published March 2015
Role of Regulations in AppSec

Figure 1
Leading Regulations that Affect Security Decision-Making for Software Development
% of Organizations Reporting

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarbanes-Oxley Act (SOX)</td>
<td>67%</td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standard (PCI DSS)</td>
<td>50%</td>
</tr>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>47%</td>
</tr>
<tr>
<td>Electronic Fund Transfer Act</td>
<td>28%</td>
</tr>
<tr>
<td>The Health Information Technology for Economic and Clinical Health Act (HITECH)</td>
<td>20%</td>
</tr>
<tr>
<td>Gramm-Leach-Bliley Act (GLB) Act</td>
<td>19%</td>
</tr>
<tr>
<td>European Union Data Protection Directive; Safe Harbor Act</td>
<td>17%</td>
</tr>
<tr>
<td>Federal Information Security Management Act (FISMA)</td>
<td>15%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
Pitfalls of a Regulatory-Centric Approach

Heartland CEO on Data Breach: QSAs Let Us Down

Heartland Payment Systems Inc. CEO Robert Carr opens up about his company’s data security breach, how compliance auditors failed to flag key attack vectors and what the big lessons are for other companies.

Q&A

Heartland Payment Systems Inc. CEO Robert Carr, the year did not start off well, to say the least.

In January, the Princeton, N.J.-based provider of credit and debit processing, payment and check management services was forced to acknowledge it had been the target of a data breach — in hindsight, possibly the largest to date with 100 million credit and debit cards exposed to fraud.

In the following Q&A, Carr opens up about his company’s data security breach. He explains how, in his opinion, PCI compliance auditors failed the company, how informing
COTS vendors aren’t helping...

- 46% of respondents received packages that contained vulnerable versions of 3rd party components
- 45% encountered vendors that would not support a secure configuration of their product
- 38% encountered vendors who would not commit to addressing vulnerabilities that are reported
Apple’s Security Breach Should Scare You More Than Target’s Did

Feb. 24, 2014 10:44am | Elizabeth Kreft

Apple’s security protocol breach is nearly as bad as handing your credit card straight to a hacker rather than making them steal the information through the magnetic stripe readers.

The flaw in Apple’s iOS and OS X platforms essentially allows a hacker to get in between the initial verification “handshake” connection between the user and the destination server, enabling the adversary to masquerade as a trusted endpoint. This means the connection which is supposed to be encrypted between you and your bank, email server, healthcare provider and more is open to attack.

18.8K SHARES

Microsoft SCHannel Bug Latest in Long Line of Serious Crypto Flaws

by Dennis Fisher Follow @dennisf

November 12, 2014, 8:02 am

The critical vulnerability in the Schannel technology in Windows that Microsoft patched Tuesday is ripe for exploitation, experts say, and continues the long line of severe vulnerabilities in major SSL/TLS implementations in recent months.

Related: U.S., TECH, CYBER CRIME

U.S. hospital breach biggest yet to exploit Heartbleed bug: expert

BY JIM FINKLE AND SUPRIYA KURANE
...because the vendors don’t know how

- 33% of those surveyed have been forced to educate vendors/developers in basic security practice to obtain satisfactory results
- 35% have been forced to take mitigating action because vendors would not correct reported vulnerabilities.
Developer’s Motivation

- On Time
- On Budget
- Acceptable quality (more about functionality than security)
- What’s missing: resilience and follow up
...and that leaves us at risk

- 36% found vulnerabilities during our own testing that could compromise the integrity of the system or data
- 21% have implemented software we were not able to obtain security verification and validation results for
SECURITY HOLES
SECURITY HOLES EVERYWHERE
Our experience at (ISC)$^2$

» 2 types of software providers that will talk security with you:
  • The prepared and capable...
  • ..and the completely naive
What else runs on software?
OWASP Internet of Things Top 10

» 1. Insecure Web Interface
» 2. Insufficient Authentication/Authorization
» 3. Insecure Network Services
» 4. Lack of Transport Encryption
» 5. Privacy Concerns
» 6. Insecure Cloud Interface
OWASP Internet of Things Top 10

» 7. Insecure Mobile Interface
» 8. Insufficient Security Configurability
» 9. Insecure Software/Firmware
» 10. Poor Physical Security
What is the Internet of Things?

What we will cover...

- Mobile
- Wearables
- Connected Devices
Next Phase: Attacks on IoT

- Software is assembled – not written
- Flawed libraries
- Hard to update
- Minimal resources
- Remember developer motivation...
Mobile

- Mobile application risks
- Privacy issues
Wearables

- Smart watches
- GPS Watches
- Fitness sensors
- Smart glasses
Wearables in the Headlines

The scary truth about data security with wearables

By Teena Hammond July 3, 2014, 1:31 PM PST // @teena_hammond


Posted by James O’Brien on Tuesday, November 12, 2013 • 0 comments

---Back to SecureWorld Post

Chinese Army Bans Wearable Internet Gadgets Over Security Breach Concerns

Smart watches, glasses and other wearable internet gadgets have been banned among China’s armed forces over concerns of security breaches, according to state media reports.

The recent guideline is said to have been issued after a soldier tried to use a smartwatch to take a photo of his comrades stationed at the eastern city of Nanjing. He was stopped by his squad leader and the matter was reported to higher authorities, which ruled that such devices could harm military action and security.
Connected Devices

- Smart TVs
- Smart home devices
- Smart thermostats
- Medical devices
- Connected cars
Connected Device Headlines

Tech Insight: Hacking The Nest Thermostat
Researchers at Black Hat USA demonstrated how they were able to compromise a popular smart thermostat.

Congress, '60 Minutes' Exaggerate Threat Of Car Hacking

Red Button Flaw Exposes Major Vulnerability In Millions of Smart TVs

It's 9:30 p.m. on a Sunday in New York City. People in their apartments in the Inwood neighborhood of Manhattan have their air-conditioners blasting and don't hear the slight whirr of the two drones hovering 35 stories in the air outside. They're on the couch watching Family Guy, Duck Dynasty or the Good Wife on their new Web-connected flat-screen TVs.

DHS investigates 24 potentially deadly cyber flaws in medical devices
Five Star Automotive Safety Program

- Safety by Design
- Third Party Collaboration
- Evidence Capture
- Security Updates
- Segmentation and Isolation

» Source: iamthecavalry.org
The bottom line...

- Everybody needs an application security program of some kind!
- Program design will vary based on organizational needs and risk tolerance
What to do?

- Be proactive
- Be knowledgeable
- Be involved
- Demand better
- Live!
- Get trained
- Automate
Take Aways for Workplace

» Next 30 days
  • Go to lunch with someone from IT/Security/Development – ask how you can help them win (securely!).

» Next 90 days
  • Be mindful of what risks are there with your current set of applications. What role do you play in ensuring security?

» Next 6 months
  • Keep learning on your own. Be the knowledgeable resource that the organization needs.
Take Aways for Home

» Next 30 days
  • Look at the hardware you use. Are there firmware updates out there? Do they address security vulnerabilities?

» Next 90 days
  • When researching new technology purchases, car selections, etc. Write down what you think the risks might be. Research to see if those are or would be addressed by vendors

» Next 6 months
  • Educate family and friends on what is happening with smart devices and the risks.
Why Get Serious about AppSec?

- Less defects
- Better user experience
- Reduce risk
- Respond quickly
- Awareness
References

» Osterman Software Study
  • http://www.ostermanresearch.com/whitepapers/download230.htm

» Global Information Workforce Study
  • https://www.isc2cares.org/IndustryResearch/GISWS/

» Verizon Breach Report
  • http://www.verizonenterprise.com/DBIR/
INSPRING A SAFE AND SECURE CYBER WORLD.