



# Elizabeth Terry

---

## PCI DSS Roadmap – The Evolution of Payments

Chief Technology Officer, PCI Security Standards Council



# Growth of Payment Software





# Payment Security Themes for 2017

12A 32C20616E642070617463686513206F5590BF34121 6C62  
7 1076C6206C6974746C65 16E642074616C773192A3 B6C697AB  
E 0A16C20 Inter-Connectivity 1A07072216145A13C7573686  
8 12302E6F6163686573204C697474CC 5205265CB74AF8101F61636A  
1BA7 0 Authentication 486FAF64206 6E013921FC0 1FFC521  
1023 106564207368 206E61C F766 6C Encryption Attacks 7  
1 027 C6E207468652A 261736B60142E20480810D3F5A89C7B7C12AF  
00100 5368AF93010808B4FA017745C7A6 108B2C3FD5515708 0DF0161  
0F00F00AFFA33C08E00F2A5697D011A56AFE64 074686520601 772Data  
F1D01 02073 C732C20736852756B013A 0AA206336 5206E674616C6B  
6AD8 616E642001A 37 Agile Software Programming 1B2EC34B4  
16987 8E00F2A5694C028BE5BF7D011A0010A3BCE561AF87010FC2 616E74



## Attacking the Interconnected World



**World is becoming more connected every minute of every day with 30+ Billion Devices expected by 2020**

- Third-party services
- Third-party software
- Crime-as-a-Service
- IoT access to data



# Authentication

## The Evolution of Trust for Commerce

Multi-Factor

Card-not-Present

Enrollment credentials

Dynamic authentication

# Modern Payment Software

Code changing at a rapid pace

Extensive use of third-party software

Legacy code and modern threats

Newer security techniques





# Breadth of Opportunity for Encryption

## Good

Encryption used throughout a payment transaction

Data breaches have limited exposure of data

## Bad

Encryption leveraged by criminals for ransomware and obfuscation of activity

Migration from older cryptography a significant challenge for many



# PCI Themes for 2017

Better authentication

Better software design

Third party accountability

Improve education and collaboration

Technology and process to simplify compliance

More education on encryption and other technologies



# Better Authentication

PASSWORD

\*\*\*\*\*

# Better Authentication Using 3DS

Three-Domain Secure (3DS) is a messaging protocol which enables consumers to directly authenticate their card with the card issuer

Three domains consist of:



Merchant/Acquirer domain



Interoperability domain



Issuer domain

Reduces fraud by preventing unauthorized uses of cards

# Software Attack Surface Increasing in Payments

IoT

Malware in Memory

Cloud-based

Legacy code





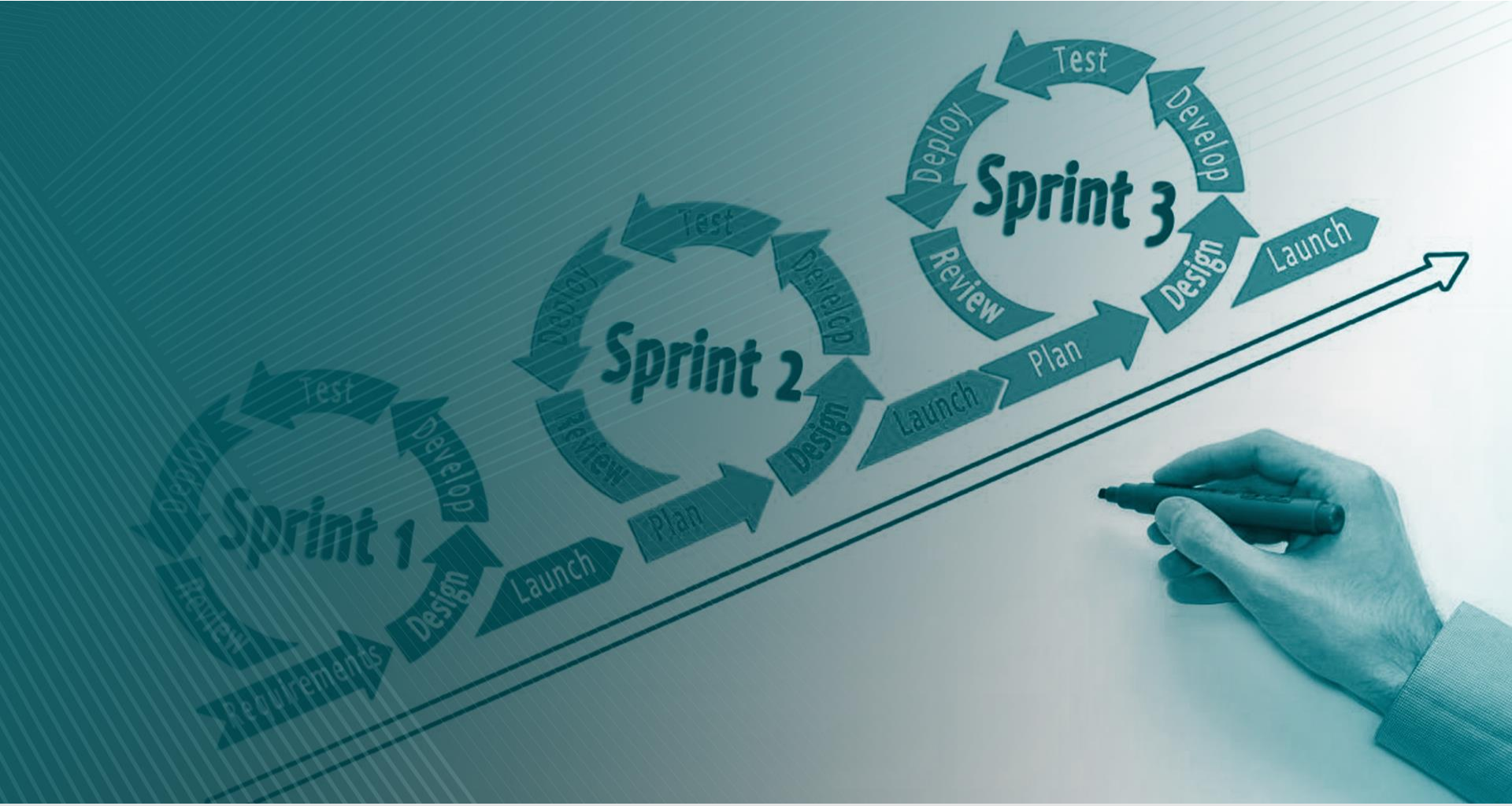
# Software Security Audit Challenges

Pace of change

Complexity

Transparency

# Secure Development Throughout Lifecycle





# App Developer Education



## New coding platforms and developers

Need for app developer education  
Accountability for due diligence

---

## More investment required for software

Network security doubles AppSec  
More incentive for good security



# Better Integration of Payment Technology



# Third Party Accountability

Qualified Integrator & Resellers (QIR)

DSS Service Provider Requirements

Third-party agreements

Software Developers

Third-party monitoring





# Importance of Automation

Ease security through automation for DSS

Machine learning advancements





# Security for Small Merchants



**Start protecting your business today with these security basics:**

-  Use strong passwords and change default ones
-  Protect your card data and only store what you need
-  Inspect payment terminals for tampering
-  Install patches from your vendors
-  Use trusted business partners and know how to contact them
-  Protect in-house access to your card data
-  Don't give hackers easy access to your systems
-  Use anti-virus software
-  Scan for vulnerabilities and fix issues
-  Use secure payment terminals and solutions
-  Protect your business from the Internet
-  For the best protection, make your data useless to criminals

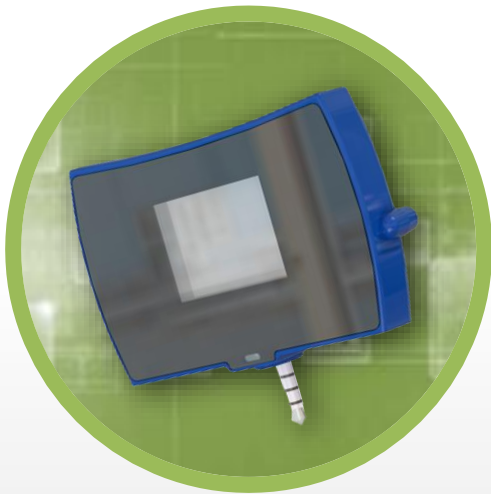
**PCI** Security Standards Council #PCISMB

Copyright 2016 PCI Security Standards Council, LLC. All Rights Reserved.

For more information on how you can protect your business, download the *Small Merchant Guide to Safe Payments*.  
[https://www.pcisecuritystandards.org/pdfs/Small\\_Merchant\\_Guide\\_to\\_Safe\\_Payments.pdf](https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf)



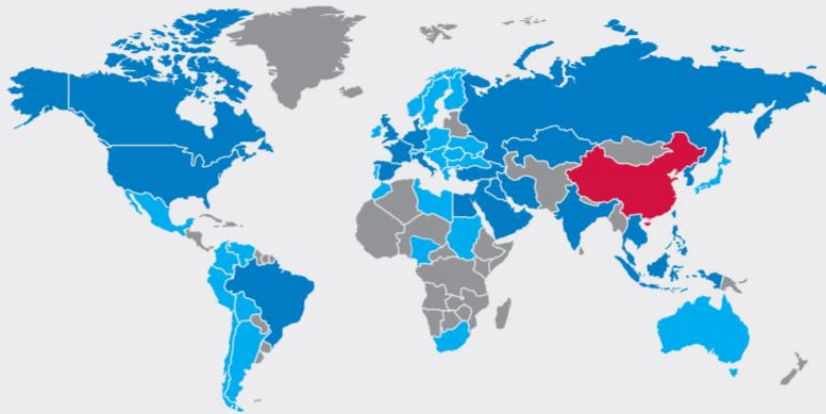
# Mobile Payments



Bring It All Together

# Mobile Technology Attacks

2016 Mobile Malware: What Happens in 1 Hour?



Intel Security: Malware detected from over 190 countries per hour.

■ > 6000      ■ 100 – 1000      ■ 10 – 100

Source: McAfee Labs 2016

As mobile becomes the new laptop and business access tool, it becomes “where the money is” for cybercriminals

25% of mobile devices were found to have some form of malware.  
– McAfee Labs

More CVEs registered in first half of 2017 for mobile OS than all of 2016

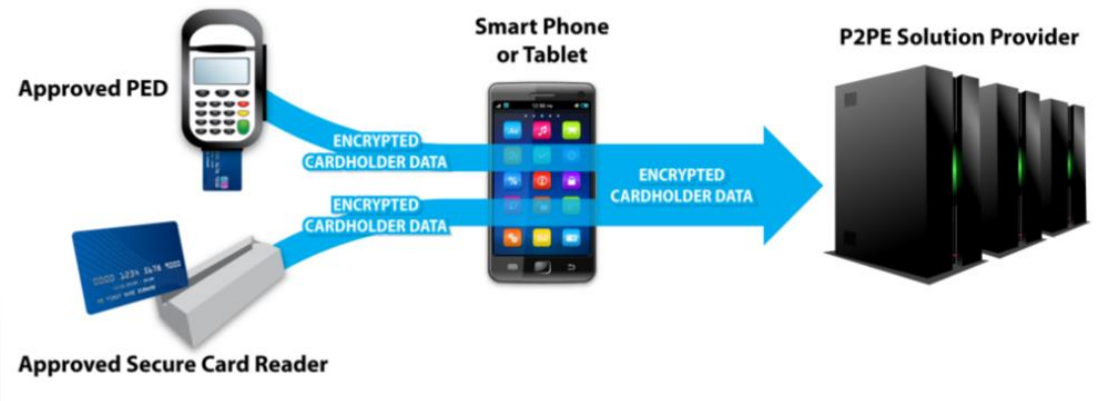


# Recent PCI Updates

Growth of SCRs listed  
that perform encryption  
before entry into COTS

Over-The-Air (OTA)  
Provisioning

Token Service  
Provider Security



## Updated Mobile Security Guidelines

PCI Mobile Payment Acceptance Security Guidelines for Developers (v2.0)

PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users (v2.0)

# How to Get Involved

PO members can contribute to:



—  
RFC for Software PIN-entry on COTS Devices

Cloud SIG

Software Taskforce

RFC for Standards (PIN, Card Production)

Feedback on existing standards (DSS, PA-DSS, P2PE)





# Bringing it Together



Holistic Security Integration

Improved Authentication

Leveraging technology to simplify

Security accountability for third parties

