PCI Updates: Securing the future of payments

Bob Russo, General Manager
2014
Everyone is Aware of Breaches!

Survey: Cyberattacks Greater Threat Than Physical Attacks
Evolution of Cyber Attacks

- Viruses
- Worms
- Trojan Horses
- Custom Malware
- Advanced Persistent Threats
Modern Malware Hides Itself

Guiding open standards for global payment card security
About the PCI Council

Founded in 2006 - Guiding open standards for payment card security

• Development
• Management
• Education
• Awareness
PCI Security Standards Suite
Protection of Cardholder Payment Data

Ecosystem of payment devices, applications, infrastructure and users

Guiding open standards for global payment card security
The Formula for PCI Success

Technology + Processes + People = Security

Guiding open standards for global payment card security
With version 3.0, PCI DSS is more mature than ever, and covers a broad base of technologies and processes such as encryption, access control, and vulnerability scanning to offer a sound baseline of security.

PCI DSS has made comprehensive security controls more commonplace in larger organizations. Therefore, the organizations become more difficult to compromise.

Source: 2013 Trustwave Global Security Report
The Standards Continually Evolve

Guiding open standards for global payment card security
Top Mistakes Revealed by Forensic Audits

Weak or default passwords

Lack of employee education

Security deficiencies introduced by third parties

Slow self-detection

Source: 2013 Trustwave Global Security Report

Guiding open standards for global payment card security
PCI DSS, PA-DSS 3.0 – Key Themes

Make PCI your compass, not your roadmap

Guiding open standards for global payment card security
Effective Dates for v3.0 PCI DSS

Version 3.0 was effective on 1 January 2014

Version 2.0 is valid until 31 December 2014

Different supporting documents

Check our website for the latest documents

Do not mix and match

Guiding open standards for global payment card security
EMV Chip in US – It’s Almost Here...
You May Have Heard...

EMV Chip will solve all security problems

Card payments will be revolutionized with EMV Chip

The payment landscape will be transformed, no need for PCI

PCI is on its way to extinction
EMV Chip Helps Reduce Face-to-Face Fraud
Even EMV Chip Needs PCI

Payment Card Industry (PCI)
Data Security Standard

PCI DSS Applicability in an EMV Environment
A Guidance Document
Version 1
Release date: 5 October 2010

Guiding open standards for global payment card security
Terminal Security

Guiding open standards for global payment card security
Don’t Forget About E-commerce!

View at
www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf
Looking Forward ...

PCI Standards will continue to evolve...

And will be applied as required, such as with EMV chip
Guiding open standards for global payment card security

Mobile

PCI Standards focus on merchant-acceptance

Mobile payment acceptance still evolving

Understand risk and use PCI SSC resources

PCI SSC is working with industry
Mobile Guidelines and Best Practices

Guidelines published 2012-2013

- PCI Mobile Payment Acceptance Guidelines for Developers
- PCI Mobile Payment Acceptance Guidelines for Merchants as End-Users
- Accepting Mobile Payments with a Smartphone or Tablet
Reducing the cardholder data footprint

More

efficient security

Less

complicated for PCI DSS

Guiding open standards for global payment card security
Where the Footprint Begins

66% of data breaches, the organization didn’t know the data was on the compromised system

VERIZON DATA BREACH INVESTIGATIONS REPORT

Guiding open standards for global payment card security
Ways to Reduce Footprint

**Reduce the need or ability to store or transmit cardholder data**

<table>
<thead>
<tr>
<th>Methods</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business process for retention</td>
<td>Reduce the need or ability to store or transmit cardholder data</td>
</tr>
<tr>
<td>P2PE</td>
<td></td>
</tr>
<tr>
<td>Tokenization</td>
<td></td>
</tr>
</tbody>
</table>
Point-to-Point Encryption

Guiding open standards for global payment card security

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>Version</th>
<th>Validated According</th>
<th>Certification Body</th>
<th>Date (Start)</th>
<th>Date (End)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>to P2PE Ver 1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solution Type:</td>
<td>Hardware/Hardware</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is a PCI P2PE Solution?

PCI PIN Transaction Security (PTS) approved devices with Secure Reading and Exchange of Data (SRED)

PCI P2PE validated applications and processes

Listed by PCI SSC
P2PE and Merchants

Only PCI-listed P2PE solutions are recognized as meeting requirements for reducing merchant PCI DSS scope.

Merchants and their acquirers accept the risk when using encryption solutions not listed by the Council.
Tokenization – Standard Expected in 2014

Work on tokenization standards has begun

Ensure that process of creating token from PAN doesn’t leak information about PAN
Ensure that a token or collection of tokens by themselves cannot feasibly allow discovery of PAN
Ensure that adequate controls exist over tokenization process
Ensure that token cannot be used in lieu of PAN for impermissible purposes

PAN

Tokenization
Industry Coordination

Continued cooperation to align tokenization efforts for the benefit of payment industry

EMVCo    ANSI X9    NIST
The Formula for PCI Success

Technology + Processes + People = Security

Guiding open standards for global payment card security
Preparation

What are your personal PCI education goals for the next three years?

For yourself

For your staff
People in Payment Chain Cause Most Internal Breaches!
Get Ready for the Future

Personal PCI training is essential to keep on top of emerging threats.

PCI training by the Council is the most effective, targeted way to accelerate mastery and stay current.

Validation proves your value to your employer and sets you apart from so-called “experts.”

Guiding open standards for global payment card security
Training Highlights

✓ Online Internal Security Assessor (ISA) Training
✓ P2PE Assessor Training
✓ Corporate Group Training – Let Us Come To You!
✓ Online Awareness Training in Four Hours
✓ Qualified Integrators and Resellers (QIR)™ Program
✓ PCI Professional Program (PCIP)™

To learn more, visit: www.pcisecuritystandards.org/training
New! Quick Resources for card security

- It’s time to change your password
- Stay Smart on Protecting Against Card Fraud!
- Increasing Security and Reducing Fraud with EMV Chip and PCI Standards

Windows XP Support is Ending

www.pcisecuritystandards.org/news_events/quick_resources.php

Guiding open standards for global payment card security
Get Involved – We Need Your Input

Join
Learn
Input
Network
Nominate
Vote
Share
Influence

Guiding open standards for global payment card security
Be Part of SIGs

Security Awareness

Penetration Testing Guidance

Guiding open standards for global payment card security
Save the Dates – 2014 Community Meetings

North America
9-11 September
Orlando, Florida

Europe
7-9 October
Berlin, Germany

Asia-Pacific
18-19 November
Sydney, Australia

Guiding open standards for global payment card security
Questions?

Please visit our website at www.pcisecuritystandards.org

Guiding open standards for global payment card security