Cipherithm LLC

2013 PCI SSC North America Community Meeting Notes

A Cipherithm White Paper

Document Version 1.00

Publish date: Sept 30, 2013

2013 PCI SSC North America Community Meeting Notes

DISCLAIMER

This publication is proprietary and confidential to Cipherithm LLC and may not be used for any purpose other than communicating said information for the benefit of Cipherithm LLC its vendors, customers and to further its business interests.

NOTICE

Cipherithm LLC reserves the right to make changes at any time and without notice. The information furnished by Cipherithm LLC in this publication is believed to be accurate and reliable; however, no responsibility is assumed by Cipherithm LLC for its use.

2013 PCI SSC North America Community Meeting Notes

Revision Control

Version	Date	Editor	Change Description
1.0	9/30/13	SS	Initial release

2013 PCI SSC North America Community Meeting Notes

Purpose

This document provides the meeting notes taken by Scott Spiker at the 2013 PCI SSC North America Community meeting. The majority of the PCI SSC meetings are geared toward merchants and the PCI DSS. Cipherithm's interest in the PCI SSC meeting is more toward the device security requirements, you will find there are more details in that section of our meeting notes.

Thank you to Equinox for sponsoring my attendance to this annual meeting.

Feel free to submit comments, questions, and editorial suggests to info@cipheritm.com

Wednesday, September 25, 2013

PCI SSC Community Meeting

Mandalay Bay, Las Vegas, NV

1,400 attendees from 25 countries

Bob Russo Opening remarks

After 7 years of shared experience, top 10 list of where PCI is

10) Strength

- The PCI SSC has become a mature global forum
- Standards are being accepted globally
- Cash use is down 3.4%
- Check use is down 62%
- Card use is up 105%

9) Complexity

- 75% of data breaches are for financial gain
- Financial data breaches are being done by organized crime

8) Policy

- Cyber security is top priority for governments
- EU has new cyber policies
- USA has executive orders from the President for cyber security

7) EMV chip

- Being deployed globally
- EMV needs PCI standards to maintain security
- EMV helps reduce face to face fraud
- Other fraud is still possible, this is where PCI can help
- PCI has issued EMV guidance on its web site

6) Mobile

- Too early to place standards in this space
- Industry is moving too fast for effective standards

- PCI has issues mobile payments guidance on its web site

5) High Risk

- PCI is focusing on the risk areas
  - Small merchants
  - Retail and hospitality
- Qualified integrators and resellers (QIR)
- PCI is expanding global training

4) Technology

- P2PE update is coming soon
- Tokenization, PCI plans to produce a standard in 2014

3) Global

- Global card use is on the rise, therefore so is risk
- Huge card use growth globally

2) The Future?

1) "You are the Future"

- Indicating that the security experts represented in the PCI SSC membership and participation is the key to the future of PCI SSC.

Key Note Speaker

- Misha Glenny
  - Two books
    - McMafia
    - Dark Market

"Fireside Chat"

- Moderated by Misha Glenny
- Troy Leach (CTO, PCI SSC)
- NIST is supposed to provide guidance on Android O/S security, possibly in October 2013
- EMV migration to the USA conversation

DSS version 3.0

- Draft to be released in November 2013
- There was a lot of feedback received
- Not all feedback could be implemented
  - Some feedback reduced security
  - Some feedback conflicted with other feedback
- There was a lot of requests for scoping guidance
- Additional guidance requested:
  - Logging

  - Pre-authorization
  - Issuers
- Service provider attestations of compliance
  - Define service types
  - Identify service covered.
- Feedback groupings:
  - Require use of data discovery tools
  - Require web-malware scanning
  - Create a program for PCI approved penetration testing vendors
  - Password requirements are “out of touch”
  - Requirements are too vague
  - Requirements are too prescriptive
  - Sometimes the two above statements were addressed to the same requirement
  - Firewalls
  - Anti-virus
  - Many on requirement 12.8
- PCI DSS is designed to be technology agnostic
  - PCI DSS already supports
    - Cloud
    - E-commerce
    - Tokenization
- PCI DSS and PA-DSS 3.0 key themes
  - Education
  - Flexibility and consistency
  - Security as shared responsibilities
  - Emerging threats
- New section, Guidance
  - Best practices for implementing into “business as usual”
    - Focus on security, not compliance
    - PCI DSS is not a once a year activity
    - Don’t forget about the people involved (training and threats)
- Incorporated information from navigation guide to the DSS 3.0
- Feedback – promote consistent validation methods
  - Enhance testing procedures
  - Clarify what it means to verify a requirement
  - Improve reporting
  - Add new templates

PA-DSS version 3.0

- Volume of feedback as a lot less than received from DSS
  - Broader application eligibility
  - Simplify application listing process
  - Improve implementation guides
  - Move rigor needed for default passwords
- Greater flexibility
  - Allow use of wildcard in application passwords
  - Expand software development life cycle

    - Enhanced requirement for training
- Implementation guide feedback
- Default accounts
    - Payment application must not require use of default accounts
    - Application default password be changed during installation
    - Password rendered unreadable using one way cryptographic algorithms.

Open Forum for Questions

There were no PTS related questions.

Networking Reception

Discussed with Leon Fell, Jeremy King and Tim Cormier that many of us PED vendors did not like the reduced time for PTS updates to the vendors, especially when there is a brand new version to the requirements that is much more intense than version 3. The vendors feel they have shorted out of good discussion in all previous PCI SSC meetings and now it is worse. An idea was floated to provide a PTS vendor and lab meeting on the day before the SSC meeting, like what is done with the QSA's for DSS. PCI stated that they would consider this.

Thursday, September 26, 2013

Report on the Verizon Data Breach Report

- Threats
    - Small merchants are most vulnerable
    - 24% of incidents affect retail or food service
    - 72% driven by financial motives

PCI standards update

- P2PE
    - One solution is currently under review
    - Two payment applications are listed
- New hybrid requirements allows the use of non-SRED devices
- Tokenization / Mobile
- Mobile
    - PCI has provided guidance
    - Too early to apply standards to this technology
- Tokenization
    - In the process of developing a 4 document standard
        - General principles
        - Reversible tokens
        - Irreversible tokens
        - Implementation requirements
    - Released planned for 2014
    - Task force started August 2013

- PTS
    - ATM guidance put out 1st quarter of 2013
    - Card security guidance put out 2nd quarter or 2013
    - PTS version 4 requirements put out 2nd quarter or 2013
        - Re-ordered some requirements
        - New guidance for the labs
        - Re-organization of the Open Protocols
        - Combined the DTRs (Derived Test Requirements) with the DTPs (Derived Test Procedures)
    - Vendors must now provide a security policy to their customers and will be posted on the PCI SSC web site, this is a new requirement B20
    - A new program manual went up in Sept 2013
    - Estimated about 20% more tab testing is required for V4 testing
    - Much more robust testing is now required
    - MasterCard requires two devices be sent to MasterCard upon completion of an evaluation. The labs will not collect those devices and send them to MC. This is not a new requirement, but vendors were not doing this.
    - Prohibit use of wildcards in the model name
    - Expired devices will be listed on a separate page starting May 2014
    - Devices can submitted for V3 until Feb 28, 2014
    - Device report must be complete by April 30
    - Device report must be approved by June 30, 2014
    - For devices that are approved, continuation fees are billed May 1
    - To cancel renewing the listing fee must be more than 90 days prior to the invoicing. The cancelation request must be in writing. Copy of the End of Life letter must be provided
    - Canceled devices will be listed with a footnote showing they have been approved but are EOL
- PTS Device Expiration
    - PTS version 1 devices expire April 30, 2014.
    - Starting May 1, 2014, expired PEDs cannot be deployed
    - Deployed typically means purchased from the original manufacturer. (Visa's guidance is consistent with this.
    - Rumor has it that no expired devices can be newly deployed, meaning those companies that have new devices in inventory as of May 1, 2014, may not install these devices for new merchant locations. These devices could be used for replacments
    - More information is still to come on this
- PTS Sunset dates
    - There are discussions about when to sunset PTS version 1 devices. This means when they may no longer be used for PIN entry. The rumored data is 2017

PIN Security Requirements version 2

- PCI provides training material, intended for QSAs, that they can use for training clients. A license is required as well as a brand sponsor. There is a cost for the use of this material
- A working group has started for this effort
- Request for comments will be sent out the first quarter of 2014
- Plan to publish version 2 sometime May 2014

Open Forum for Questions

There were no PTS related questions.