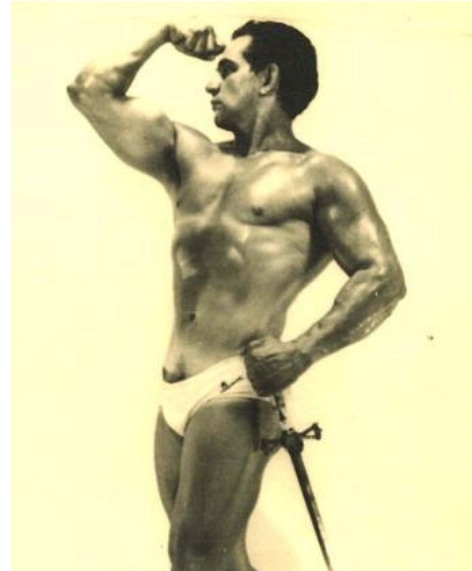


PCI SSC Summary 2011

A review of the insights and antics from Arizona

As summer came to its official close, the Payment Card Industry Security Standards Council (PCI SSC) descended on Scottsdale, Arizona, for its annual North American Conference. The conference opened with Bob Russo and Eduardo Perez taking the stage to deliver the “State of PCI Address” (the state of PCI is Strong!). Over the past five years, PCI has evolved from the management of a single standard to the management of multiple security standards (PCI Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA DSS), PCI Pin Transaction Standard (PCI PTS)), management of the inventory of validated payment devices and applications, and has taken on the oversight and training for Qualified Security Assessors (QSA), Approved Scan Vendor (ASV) and Payment Application (PA) QSAs, as well as the relatively new Internal Security Assessor (ISA) and PCI Forensic Investigator (PFI) programs. Wow, that certainly is a lot of progress for five years!



After the rousing state of the union, Frank Abagnale (of “Catch Me if You Can” fame) took the stage and emphasized the challenge we have in our battle to secure cardholder data, both from the aspect of the risk-vs-reward society that we have become (it doesn’t matter if it’s wrong as long as I don’t get caught; only then am I sorry). He also discussed the inherent challenges that technological advancement brings to security (just because you can doesn’t mean you should!).

Next up was the daily “Ask Bob” session. We all asked Bob if it was okay to store cards in the clear and he said no..!

The PCI SSC has been very busy lately with the release of new guidance documents on:

- Wireless
- Tokenization
- Virtualization

All of these of documents can be found at the PCI SSC website so read them for yourself!

https://www.pcisecuritystandards.org/security_standards/documents.php



At this point, the council was feeling pretty bold so they took on all comers during a PCI DSS and PA DSS Q&A session. Key observations for this session include:



- EuroPay, MasterCard, and Visa (EMV) sometimes referred to as “chip and PIN” or “smartcard” is coming. It reduces risk, but does not remove the merchant from PCI scope.
- Telephone recordings with Cardholder Data (CHD) are in scope and may put some Multi-Protocol Label Switching (MPLS) and Voice over IP (VOIP) systems into scope as well.
- Virtualization—no one-size-fits-all so check with your QSA (make sure the QSA you ask has experience with virtualization).
- Tokenization does not remove the merchant from PCI scope. Look at the white paper for guidance.
- Wireless is still a challenge. The council wants wireless scanning even if there is no wireless in the CDE to prevent and validate rogue devices.
- Mobility—the council is publishing mobility requirements and will be putting mobile payment applications on the PA DSS list shortly. Until then, you will have to rely on either your professional judgment or your QSA’s.
- For a Point-to-Point Encryption (P2PE) implementation to be effective in reducing scope, everything must be validated:
 - Hardware from the acquirer, processors and/or gateway
 - Point-of-Interaction (POI) terminal and all of its applications, communications and encryption/decryption methodology
 - Solution provider documentation, including inventory management
 - Solution provider manages all updates
 - Merchant can’t have access to encryption keys or be able to inject terminals
 - Merchants can’t have access to the data

Note: There is no Self-Assessment Questionnaire (SAQ) for P2PE environment (though it is under development). Until one exists, merchants need to work with their acquirer for direction.



With a night of stimulating security conversation and bull riding behind us, it was time to tackle a new day of payment security fun! After a brief recap by Mr. Russo, Chris Novak took the stage to review what our friends, the hackers, are up to, and to discuss some of the more interesting trends related to their bad behavior. The net-net of the presentation is that while hackers are becoming more and more organized and skillful, most

hacks do not require a significant amount of skill to pull off and most can be prevented with limited effort. It is also important to note that the vast majority of hacks are captured in the network logs, but are not acted upon until a third party notifies the merchant that they have been identified as a Common Point of Purchase (CPP). Lastly, it's generally an outsider who is exploiting the system and they are most likely using our favorite exploit (SQL Injection).



If you have not read the Verizon 2011 Data Breach Investigations report, you should. Here is the link: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

As with all conferences, you learn as much from the “unofficial” sessions as you do from the “official” sessions. Here are a few observations from the unofficial portion of the conference:

- Mobility is here and everyone is working hard to secure it (P2PE will play a big part in this).
- P2PE is gaining popularity, but is far from a silver bullet. Not all solutions are the same and implementation is key (devil is in the details).
- The council will be focusing on PA DSS application implementation guides this year as we have had a significant problem with the misconfiguration of validated applications over the past few years.
- Some really exciting Special Interest Groups (SIGs) have been submitted for this upcoming year. My personal favorites are the cloud computing, Level 3 – 4 Ecommerce, and Merchant Risk Assessment

All in all, it was a great conference. It was nice to see old friends, meet new ones, and have in-depth conversations regarding the technologies and events that are shaping our payment world. If you didn't make it this year, I highly recommend that you put it on the schedule for next year.



Jim Bibles leads the Business and Product Development teams for ComplyGuard Networks. He is widely recognized as an expert in the development and implementation of risk-based compliance programs. His focus for the past 10 years has been in the payment space where he has implemented information security and merchant PCI DSS compliance programs for such companies as Visa Inc. and Wells Fargo Merchants Services. His current focus is developing merchant network vulnerability and risk management tools for small to medium-sized businesses and their service providers, so that they are in a better position to make intelligent risk based decisions on how they secure their network. Jim is a QSA and is an active thought leader within the payments community. www.ComplyGuardNetworks.com

