Payment Application - Don't Secure Sh!t

cmlh

Shmoocon 2K10 - Firetalks

Last Updated 28 February 2010

whoami

Not QSA and/or PA-QSA i.e. End User therefore **Unbiased**.

PCI-DSS

- Energy Australia (.nsw.gov.au Critical Infrastructure)
  - "Should I Black Your PC I/Eyes Again?" Presentation to .nsw.gov.au
- eWay (.au ASP Payment Gateway)
- FOXTEL (.au Subscription Television)

PA-DSS

- OWASP AU 2009 Presentation with Darren Skidmore (FNIS)

PA-DSS - History

Payment Application Best Practice (PABP) from VISA

PCI Security Standards Council Publications:

- Accepted PABP v1.4 until 15 October 2008
- v1.1 - 15 April 2008
- v1.2 - 15 October 2008

Rumoured that PA-DSS is more through then PABP

- No way to verify as PABP has ceased publication

PA-DSS - Diff PCI-DSS

PCI SCC list Validated Payment Application (VPA)

- Not QSA like PCI-DSS

PA-DSS Implementation Guide

VISA are the only Card Brand mandating PA-DSS

- Conformance by 1 July 2012

Diff from PCI DSS (.com) or PCI PTS (Hardware /dev)

PA-DSS Implementation Guide (i.e. PCI DSS Conformance)

Economics of INFOSEC

Identify Political and/or Technical Deficiencies in:

- PA-DSS
  - Including Dependencies on PCI DSS
- PA-QSA

Intend to audit specific Validated Payment Application (VPA) at a later date

PA-QSA

QSA -> PA-QSA

CI$$P (ISC2) and/or CISA/CISM (ISACA)

- ISC2 recently launched the C$$LP

Security Researchers with these quals???

<sarcasm>I mistakenly put $$ which does represent the not for profit agenda of ISC2</sarcasm>

Out of Scope

Due to their PCI-DSS (lack of) effort

- Single Implementation (Custom /dev Software)
- Payment Gateway (ASP or SaaS)
- Implementation (DB, OS, etc)

Attack Surface of PCI DSS

In Scope

Payment Applications which process VISA only

“Payment” Module within COTS is In Scope

- Attack Surface of other “Modules”

PCI DSS Dependency

1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data

Attacks are similar to those of PCI DSS

- Masked on Screen yet read /dev
- Commodity Hardware

Commodity i.e. not restricted

PCI DSS Dependency

2. Protect stored cardholder data

Attacks are similar to those of 3.4 of PCI DSS

- No reference to Cryptographic Modes
  - Hence "Broken" Modes used e.g. ECB

Root Cause "Applied Crypto" as "Reference"

Cryptographic Modes are mentioned in "Applied Cryptography"

PA-DSS

5. Develop secure payment applications

Cites *OWASP "Guide"* - WTF!!!

- OWASP Top Ten 2007 -> 2010 RC1
- TANDEM, Mainframe and AS/400 based
  - www Server on LPAR

MITRE CWE has > 700 Type of Vuln

PCI DSS Dependency

- *6. Protect wireless transmissions*
- WEP - WTF!!!
- Joshua Wright on Not Broadcasting SSID
  - Contacted PCI DSS 1.0
  - Implemented PCI DSS 1.2

Quotes from http://www.networkworld.com/chat/archive/2008/022608-josh-wright-wireless-security-chat.html

Q. “Joshua, please let me know your thoughts on disabling broadcasting your router’s SSID.
A. It’s a bad idea. I know the PCI specification requires you to do this, and I’ve told them they need to remove this requirement from the specification.”

PA-DSS

7. Test payment applications to address vulnerabilities

Root Cause is Maturity

- Pen Test is Point in Time

PCI DSS Dependency

10. Facilitate secure remote software updates

Should be implemented but consider other vendors e.g. Evilgrade

- ARP Spoofing,
- DNS Cache Poisoning,
- DHCP Spoofing

PCI DSS Dependency

12. *Encrypt sensitive traffic over public networks*
13. *Encrypt all non-console administrative access*

Recent attacks against SSL not considered.

Payment Specific

There is no security advice specific to payment transaction types, i.e. Chargeback, etc

Root Causes

Elitism

- Financial Security is “Smoke and Mirrors”
- Compounded by Blowing Smoke up their (_o_)

Root Causes

"Hitting the Celling" due to:

- CI$$P and CISA/CISM
- Reading "Applied Cryptography"/etc only

Conclusion

christian.heinrich@cmlh.id.au

Thanks

- Kyle Osborn @kposborn for rego code
  - Don’t forget your RUXCON shirt
- Bruce @gdead and Heidi Potter for late rego
- @grecs for scheduling this firetalk
- All other shmoocon staff