Request for Feature Enhancement (RFE)
PCI-DSS – Requirements and Security Assessment Procedures

Author
Kamala Narasimhan
kamala@manasv.com

Table of Contents

Scope

This document makes a case for adding a new requirement to PCI-DSS "Requirements and Security Assessment Procedures" specification. It describes the proposed requirement and explains its need. It then makes a comparison of the proposed requirement with existing requirements. It also describes how to enforce the requirement. It then dwells into industry report on statistics, references to technical research, affected parties, its cost etc., all pertaining to the infraction this requirement help solve. It concludes by appealing to the PCI-DSS council to consider amending the current specification to include the proposed requirement.

It should be noted that any reference to PCI-DSS specification implies PCI-DSS "Requirements and Security Assessment Procedures"[1] version 3.1 of the specification, the latest as of this writing.

Requirement

Card holder data held in-memory must be protected.

Card holder data held in memory by payment and other relevant applications should be protected while in memory. Irrespective of the amount of time in memory, the card holder data is vulnerable during the time it is in memory. The same data is otherwise protected as stipulated by PCI-DSS requirements during other stages of its handling in the payment process.

Reason

Existing advancements do not close all the gaps in card holder data handling process. While EMV, point-to-point encryption etc. reduces the points of vulnerability at varied stages in the chain of responsibility, it does not make all stages of payment information handling impenetrable. Thus the investment made to protect card holder data at several stages could be defeated by exploiting a vulnerable point at a stage open to weakness. To get closer to a comprehensive card holder data protection solution, gaps in the process need to be identified and closed. This requirement help close one such gap.

Card Holder Data Protection Requirements Comparison

PCI-DSS specification currently has a section “Protect Cardholder Data” with two requirements clearly stated under it. Requirement 3 outlines how stored card holder data, that is, data at rest must be protected and requirement 4 describes how the same data must be protected while in-transit . However, that data also exist in memory at one or varied points in time and there is no requirement governing that. It opens a gap during which the card holder data is vulnerable. Adding a new requirement to include in memory protection, under the same “Protect Cardholder Data” section would help close that gap.

How to Enforce the Requirement?

While requirements 3 & 4 in the PCI-DSS specification can be enforced by way of encryption, there is more than one way to enforce in memory card holder data protection. It should be suggested that the payment industry adopt one of the existing in memory protection technology to confirm with the proposed requirement.

Under detailed guidelines for the proposed requirement, it should be suggested that access to card holder data in memory be allowed just to the authorized payment applications and within that to specific modules. It should be recommended that additional checks be put in place to ascertain that those applications and modules aren't tampered with in memory or during its load. It should also be recommended that sanity checks like the state of registers and stack be done during the time card holder data is accessed by authorized code. Lastly, it should be suggested that any access by unauthorized applications be rejected and logged for auditing needs.

Industry Report – In-memory Data Infractions

In-memory Data Breach Statistics

According to “Verizon 2014 Data Breach Investigations Report”[2], memory scraping was the 4th top most threat action in 2013, a significant change from the year before! Also, per the same document, 85% of threat actions carried out as part of POS intrusion are memory scraping attacks. Verizon's 2015

report[3] on the same topic further reiterates the growth of memory scraping attacks that affect the POS systems. Sophos report[4] on memory scraping provides data on infections by sector and country.

In-memory Data Breach Technical Research

On the technical research front, TrendMicro researcher Numaan Huq created a very detailed report[5] explaining the different PoS memory scraping families of infections along with how and what is exploited by each of those malwares. Blogger Xylibox[6] has done a wealth of research on this topic as well.

Businesses Affected

Among others, following are some of the businesses whose payment system were affected by memory scraping attacks -

- Target[7]
- Home Depot[8]
- Neiman Marcus[9]
- Michael's[10]
- TJ Maxx[11]
- Albertsons[12]
- SuperValu[12]
- Heartland Payment Systems[13]
- Viator[14]

Cost of Industry Infractions

Target's data breach cost $148 million per NY times report[15]. Home Depot's breach cost the company $62 million per Bizjournal[16]. Ohio credit unions were hit with a $1.3 million fraud losses because of Home Depot data breach as reported by The Blade[17]. And these data doesn't begin to describe the staggering loss incurred by the industry because of attacks directly pertaining to in-memory data breach and as a consequence or ripple effect there after.

PCI-DSS – Industry Criticisms

Dark Reading's article[18] makes a particular comment that PCI DSS does not go far enough to address memory scraping attacks. A Gartner analyst[19] as well points out PCI-DSS's short comings in this area. An article[20] by “Heat Security Blog” specifically targets the lack of PCI-DSS rules around card holder data in memory.

Conclusion

Looking at the staggering cost of memory scraping attacks, which at its core is made possible by lack of in-memory protection of card holder data, it is reasonable for the PCI-DSS council to act towards adding a new requirement to better protect card holder data in-memory. After all, it has already done that for the same data at rest and in-transit.

Also, by carefully looking at the gaps that still exist in payment system processing and fixing it by mandating more requirements to PCI-DSS specification, PCI-DSS could get closer to becoming the

most holistic standard to help protect payment card data. The requirement proposed in this document is one such requirement that would get PCI-DSS closer to that goal!

References

1. PCI-DSS “Requirements and Security Assessment Procedures” - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf
2. Verizon 2014 Data Breach Investigations Report - http://www.verizonenterprise.com/DBIR/2014/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR
3. Verizon 2015 Data Breach Investigations Report - http://www.verizonenterprise.com/DBIR/2015/
4. Sophos - https://nakedsecurity.sophos.com/2013/07/16/a-look-at-point-of-sale-ram-scraper-malware-and-how-it-works/
5. TrendMicro PoS RAM Scraper Malware - http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf
6. Xylibox - http://www.xylibox.com/2012/12/point-of-sale-and-memory-scrappers.html
7. Target Intrusion - http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/
8. Home Depot Breach - http://www.itsecurityguru.org/2014/09/03/home-depot-suffers-major-card-breach-industry-views/
9. Neiman Marcus Breach - http://www.darkreading.com/attacks-and-breaches/target-breach-8-facts-on-memory-scraping-malware/d/d-id/1113440
10. Michael's Breach - http://www.darkreading.com/attacks-and-breaches/michaels-stores-investigates-data-breach/d/d-id/1113587
11. TJ Maxx Breach - http://www.direnzic.co/blog/great-article-by-cyberheist-news-today/
12. Albertson and SuperValu Breaches - http://www.wired.com/2014/09/ram-scrapers-how-they-work/
13. Heartland Payment Systems Breach - http://www.bankinfosecurity.com/heartland-payment-systems-forcht-bank-discover-data-breaches-a-1168
14. Viator breach - http://www.net-security.org/secworld.php?id=17391
15. Target breach cost - http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=1
16. Home Depot breach cost - http://www.bizjournals.com/atlanta/news/2014/09/18/home-depot-breach-cost-62m-exposed-56m-cards.html?page=all
17. Ohio credit union's losses - http://www.toledoblade.com/Retail/2014/11/01/Ohio-s-credit-unions-hit-hard-by-national-retailers-data-breach.html
18. Dark Reading article - http://www.darkreading.com/attacks-breaches/ram-scraper-malware-why-pci-dss-cant-fix-retail/a/d-id/1297501
19. Gartner article - http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/
20. Heat Security Blog - https://heatsoftware.com/security-blog/8285/what-does-the-target-breach-tell-us-about-dss-and-pos/