Point of Sale (POS) Device Security Measures

Grant Eckerson - Montana State University
Mentors: Dr. Clemente Izurieta & Yvette Hastings

Introduction

The Point Of Sale (POS) device is critical to the modern US economy. They are connected to the POS host's network to communicate with both their inventory systems inside the network and financial applications outside of the network. The information sent outside of the network contains highly critical personal information, such as a customer's name, address, DoB, and most importantly, their credit and/or debit card information. This sensitive personal information can be left vulnerable on the network and exploited through cyber-attacks. In addition to cyber-attacks made on the network, POS devices can be vulnerable to physical attacks when left unattended by their host. With how critical this information is, and how valuable it can be to those who exploit it, POS systems should be designed with sufficient security measures in place to prevent cyber and physical attackers from penetrating these devices. We conducted a thorough literature review to shed light on the various methods in place to safeguard our information. With information obtained from our literature review, we can start to identify where security measures can be improved to protect our sensitive personal information from POS device attacks.

Research Method

A literature review was conducted using the search string 'POS, security' on Google Scholar. Search criteria was: is the paper about POS devices- not mobile apps/ does the paper have multiple authors/ is it from the 2000s/ is the paper's topic directly related to POS security measures. After criteria was met, there were about 6700 papers, of which I read 20 abstracts and used 7 in this project.

Attack Methods[1,2,3,4,5,6,7]

- **Physical Attacks–**
  - False POS Devices (Skimming)/ Hidden Cameras/ Keyloggers
- **Cyber Attacks–**
  - RAM Scraping/ Network Sniffing/ SQL Injection/ Man-in-the-Middle Attacks/ Brute-Force
- **Human Attacks--**
  - Social Engineering/ Phishing/ Employee Complicity
- **Combination–**
  - False POS devices (Relay Attack)/ Backdoor Implementation

Physical Countermeasures[3,4,6]

- **Lock-up Servers/ Data Centers–**
  - As the hearts of a POS system- access to these would make an attacker's day.
- **Properly Store and Dispose of Documents–**
  - Items such at the network map can lead an attacker directly to what they want.
- **Properly Trained Alert and Trustworthy Attendants–**
  - Ensuring those who watch over POS devices can and will intervene in a physical attack would give attackers one less avenue to approach from.

Virtual Countermeasures[1,2,3,4,5,6,7]

- **Encryption–**
  - Encryption of multiple parts of the POS system- the wireless and local networks/ card information itself. If the attacker can not undo the encryption, the data is useless to them.
- **Separation of Data–**
  - Only store data required/ have most data stored off-site. If all data is stored in one place, the attackers only have to figure out one solution.
- **Firewalls–**
  - Blocks all network traffic not already allowed, a simple way to make an attacker's work more difficult. Still allows all traffic from approved sources, so an attacker could hijack the source or spoof the system into thinking they're the approved source.
- **Up-to-date Antivirus–**
  - Another simple way to limit the ways an attacker would have access to the system. Only works on already known viruses- new viruses require new antivirus software to be developed. Keeping up to date is critical.

Other Countermeasures[2,3,4,5]

- Guide and enforce users on security standards (Payment Application Data Security Standard/ Payment Card Industry Security Council)
- Constant updates to security standards/ rapid response and investigation to attacks
- Certified and trustworthy administrators for POS systems
- Further adoption of chip cards

Conclusion

The data within POS systems is worth millions of dollars, making them a very valuable target for would-be attackers. Being a defender, you have to be watching all possible avenues of attack. You have to defend 100% of the time. You prepare the best you can then react to what comes your way. As an attacker, you only need to succeed once and in one location to get what you want. By using the countermeasures listed here, as well as others, POS systems better their chances at successfully defending against attacks. A system administrator for a POS system should be vigilant in keeping their antivirus up-to-date. They should practice safe procedures for storage and separation of data- physical and virtual. They should be certified as a system admin in addition to being a trustworthy individual. The employees who attend to the POS systems should be properly trained as well as being alert and trustworthy individuals. All of this must be constantly true, as one slip and an attacker could access the valuable data within the system. All of this preparation and an attack could still get through, so it is imperative that administrators stay vigilant to quickly fix vulnerabilities. The security of the US's financial system is dependent on it.

References

[1] H.-J. Lee, Y. Lee, and D. Won, "Protection Profile for PoS (Point of Sale) System," *Lecture notes in electrical engineering*, pp. 495–500, Jan. 2014, doi: https://doi.org/10.1007/978-3-642-40675-1_74.
[2] B. A. Sassani Sarrafpour, R. Del Pilar Soria Choque, B. Mitchell Paul, and F. Mehdipour, "Commercial Security Scanning: Point-on-Sale (POS) Vulnerability and Mitigation Techniques," *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, doi: https://doi.org/10.1109/dasc/picom/cbdcom/cyberscitech.2019.00090.
[3] Sai, K. (2017). An Analysis of Point of Sale Systems Physical Configurations and Security Measures in Zimbabwean SMEs. *IRA International Journal of Education and Multidisciplinary Studies* (ISSN 2455-2526). 6(2), 181-190. doi:http://dx.doi.org/10.21013/jems.v6.n2.p5
[4] O. Avdeyuk, D. Kozlov, L. Druzhinina, and I. Tarasova, "Fraud prevention in the system of electronic payments on the basis of POS-networks security monitoring," *IEEE Xplore*, 2017. https://ieeexplore.ieee.org/abstract/document/8109597
[5] H. A. Rad, M. B. Tehrani, K. Samsucin and A. R. Ramli, "A Simple and Highly Secure Protocol for POS Terminal," 2009 *Second International Conference on Environmental and Computer Science,* Dubai, United Arab Emirates, 2009, pp. 204-207, doi: 10.1109/ICECS.2009.42.
[6] D. Smith and G. Megrath, "NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA THESIS Approved for public release; distribution is unlimited PREVENTING POINT-OF-SALE SYSTEM INTRUSIONS," 2014. Available: https://apps.dtic.mil/sti/pdfs/ADA607543.pdf
[7] M. Thesis, A. Pedersen, and A. Hedegaard, "Security in POS Systems QH igEpoint swwErisEPHHSESP Supervisor: Robin Sharp IMM, DTU," 2005. Accessed: Apr. 18, 2024. [Online]. Available: https://www2.imm.dtu.dk/pubdb/edoc/imm3965.pdf

Acknowledgements

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.