Manuscript Review

Payment System Security

Gaurish Korpal and Drew Scott

A. Summary

During a credit card transaction there are two devices: the credit card itself and the acceptance terminal. Data is passed between these devices in order to establish rules for the payment and in order to actually process the payment. There are two main sets of protocols and standards that govern a transaction: (1) EMV and (2) PCI, which was developed in response to weaknesses in EMV (including card cloning exploits, eavesdropping and more). When using EMV, there are several transaction models that can be agreed upon between the card and terminal, which can use different combinations of (a) being online or offline, (b) being contact or contactless, (c) using static, dynamic, or combined card authentication, (d) using PIN or not to verify the cardholder, and (e) having high or low transaction value. Different credit card companies have their own implementations of these models, and, for example, Mastercard's contactless protocol for high transaction values is secure, while many others aren't. Since many transaction models of EMV aren't secure, PCI was developed to include the entire scope of a transaction. PCI responds to the threats faced in credit card transaction systems by: using firewalls, not storing card data for long periods of time, doing frequent updates, using encryption, and more. The authors used Splunk to demonstrate the security of the firewall.

B. Strengths

- The abstract gives a strong summary of the manuscript and overview of the payment system industry.
- There is a good high level overview of the EMV protocol along with a good sampling of what options are available for a transaction to use.
- The visual aids have good content. They help contextualize the processes that are occuring, especially figure 1.
- A good sample of the exploits of both EMV and PCI were given, which provides the reader with context of why security research is required in this field.
- The responses to security threats that PCI implements have a wide breadth.

C. Weaknesses

- There are many typographical errors involving punctuations, capitalization, and table references.
- There are few very long sentences (section 1, second last line; section 5.C.2).
- Lack of explanation of some important topics like
  - man-in-the-middle attacks (section 3);
  - methodology for the study of 40 configurations of transaction models (section 4);
  - a list of differences between EMV and PCI (section 2 and section 5).

    - using Splunk to monitor incoming logs (section 5.D.1);
- The scaling of the figures included in the document is not appropriate. It is difficult to read their contents without zooming in.

D. Improvement recommendations

- Use a LaTeX editor that offers grammar and spell-check options. For example, Overleaf editor offers add-ons like Writefull and LanguageTool in addition to its in-built spelling checker.
- Use the `\label{}` and `\ref{}` in LaTeX to add table references (Overleaf guide).
- Since the paper has space to add more information (5-page limit), the paper quality can be improved by adding some explanation about the topic listed above in the weakness section.
- The Splunk dashboard screenshot can be split into three individual graphs to improve its readability.