Komrabai Kargbo

Security of Transactions Performed Using Credit Card Readers for Smartphones and Tablets

1.Introduction and Motivation

In the past, clunky credit card readers were needed. They are clunky and cost hundreds of dollars. To be competitive, small businesses needed them to let their customers use their credit cards instead of using cash. With the introduction of credit card readers for smartphones and tablets, small companies can buy credit card readers for $10 that they can plug into cellphones.

With the introduction of mobile credit card readers, many security weak points are introduced. We want to analyze the the smartphone credit card reader and check to see if it is actually secure and if there are any weak points that we might find. We want to know if credit card readers can be compromised by a fake buyer, a fake seller, a fake manufacturer, or someone on the network. We also want to compare the security differences of a traditional credit card reader and one that is attached to smartphones.

This is a topic worth exploring because more small businesses are starting to use plug-in credit card readers and a lot of personal digital information is being sent over the internet. This is an important study to see if small businesses and consumers are safe.

2.List of Alternative Solutions(protocols/ algorithms/ implementations)

- Credit card data encryption within credit card readers at point of swipe
- Meeting the Payment Card Industry Data Security Standards(PCI-DSS)
- Cryptographic protocols and message formats(SSL and PGP) when transferring data
- Requiring cryptographic keys be at least 128 bits long. Asymmetric keys must be at least 2048 bits long
- Card Authentication
- Tokenization once data reaches servers
- Device/host Authentication
- Purchase tracking
- Monitor each transaction to detect suspicious behavior from swipe to settlement
- Algorithms to spot and freeze malicious or suspicious activity
- Risk Visualization
- Security updates to software (patches on servers and equipment)

3.Tentative List of Evaluation Criteria

Security, trust, and privacy are the requirements needed in order for electronic payments via credit card readers to work efficiently and securely.

4.Mutual Dependencies among various Evaluation Criteria

- network security
- integrity

5.Problems/Hypotheses Planned to Investigate

- Identity Theft
- Card Fraud/Counterfeits
- Wireless network security of the system
- Difference between traditional credit card reader and plug-in credit card readers

6.Questions Seeking Answers

How can we make sure that the manufacturer cannot steal credit card information?
Is there any way to steal the credit card information?
Can another application on the device monitor the coming and going of transactions?
Can credit card information be compromised over wireless network?
What steps make sure that the credit card information secured?
Are certain credit card readers more secure than others?
Is there a security difference between a traditional credit card reader and one for smartphones?

7.Procedure/Experiments used for Verifying Results of Investigation

Utilizing a skimming application in order to receive unencrypted data from credit cards.
Using credit card reader applications and look for malfunctions
Make a payment using credit card reader and document results

8.Time Schedule. Goal Dates

10/16 - obtain credit card reader and see how they work
11/4 - evaluate the differences between different credit card readers
11/18 - run tests to see if can compromise information from any side
12/2 - finish testing and write final report

9.A list of possible areas, where the specification can change depending on the progress of the project

- Solutions and alternatives to security issues

- Problems and Hypothesis planned to investigate

10.Tentative Table of Contents for Final Report

- Abstract
- Introduction
- Materials and methods
- Data and tests
- Results
- Conclusion
- References

11. List of Literature

- S. Karnouskos et al. 3rd international conference on mobile business 2004. “Security, Trust and Privacy in the Secure Mobile Payment Service.” http://www.semops.com/uploadfiles/SE MOPS_SEC_mBusiness2004.pdf

- W. Frisby et al. “security analysis of smartphone point-of-sale system.” University of Wisconsin-Madison. Available: http://pages.cs.wisc.edu/~rist/papers/pos.pdf

- F. Biship and P. Saunders “RF payment via a mobile device.” US Patent # US 7493288 B2.

- RAMON P. DEGENNARO, “Merchant Acquirers and Payment Card Processors: A Look inside the Black Box,” University of Tennessee and a visiting scholar at the Federal Reserve Bank of Atlanta.

- Square, “Secure Data Encryption.” Available: https://help.squareup.com/customer/portal/articles/7764-secure-data-encryption

12. Additional Information

- Most of the skimmer apps and the information needed to use them are accessible in the open web
- smartphone app downloaded that decodes the audio of credit card swipes as received from the reader