1) Team Members

Matthew Carter and Brienne Douglas

2) Project Title

Securing Card-Not-Present Transactions Through EMV Authentication

3) Introduction

EMV chip payment cards are widely accepted throughout the world, but the United States has yet to fully adopt the technology. Many of the retailers in the United States will accept EuroPay, MasterCard, and VISA (EMV) chip card transactions by October 2015 according to [11]. This shift in accepted payment methods intends to limit the occurrences of fraudulent transactions enabled by the knowledge of the magnetic stripe's weaknesses. However, this shift will not improve the security of "card-not-present" (CNP) transactions.

Fraudulent CNP transactions have increased substantially in correlation with the EMV implementation for "card-present" (CP) transactions as shown in [7]. This paper describes one possible framework to provide CP transactions with EMV payment cards for Internet purchases. The authentication data generated with secret keys tied to the payment cards may provide the same level of card verification protections to purchases from a remote vendor.

4) Motivation

Criminals adapted during EMV's deployment period by moving to fraudulent CNP transactions that bypass security measures in EMV as shown in [7]. Improvements in the EMV protocol will continue as researchers identify potential problems and issuers rectify them. The focus of organizations reliant on purchase methods such as CNP needs to be the application of EMV security to CNP transactions. This type of framework accounts for future enhancements to the EMV protocol and applies them to both CP and CNP.

MasterCard proposed using existing EMV technology to provide authentication for online banking in an initiative known as the Card Authentication Procedure (CAP). This process requires a card reader that generates a one-time password for online transactions provided the user has the EMV payment card and pin, demonstrated by [12]. The framework proposed in this paper requires the use of a similar card reader, but provides a procedure to perform the EMV protocol with remote vendors.

5) Development Procedure

The technical research on this project will prototype a framework for performing EMV payment card transactions with a remote vendor. The research will include the analysis of the EMV protocol through the use of EMV payment cards and the Smart Card Detective hardware mentioned in [7]. The hardware has the ability to emulate a terminal for an EMV transaction, enabling a user to exercise the protocol. The design for EMV transactions with a remote vendor will use knowledge gained from the analysis in the previous step. The components of the framework will include a smart card reader driven by software on a computer or other device and a test EMV payment card. Demonstration of an active attack on an encrypted card-not-present transaction will highlight shortcomings of the cryptography employed by card-not-present transactions. Running the same attack with the addition of the EMV authentication will determine the impact of the added layer of verification.

6) Hardware Requirements

The following is a list of hardware components required for the development.

a. Smart Card Detective (or other test payment card)
b. Smart card reader
c. Personal computer

7) Alternative Solutions

Alternative solutions to current payment cards include digital wallet services and EMV protocol improvements. This project will focus on the digital wallet services Apple Pay and PayPal due to their wide acceptance. Evaluation of these alternatives will better assess the need for improvements in electronic transactions.

8) Evaluation Criteria

The evaluation criteria for the framework are as follows.

a. Extensible design for protocol enhancements
b. Verification of authentication
    i. Is it possible to impersonate the card?
    ii. Is it possible to impersonate the remote vendor?
c. Remaining security concerns
d. Hardware requirements

9) Mutual Dependencies

Mutual dependencies amongst the evaluation criteria are as follows.

a. Verification of authentication and hardware requirements depend upon:
    i. The type of cardholder verification method (CVM) used for EMV
b. Remaining security concerns and hardware requirements are interrelated because:
    i. The hardware design will directly affect the security concerns
        1. Pin input method
c. The design for remotely executing the protocol and the impersonation of the remote vendor are mutually dependent through:
    i. The design, if based upon card-present transactions, will not authenticate the vendor

10) Hypotheses

a. Incorporating the EMV protocol into online transactions will reduce fraud due to:
    i. Difficulty in cloning EMV chip payment cards
    ii. The EMV protocol provides a level of card verification with a secret key
b. The EMV protocol vulnerability research reveals areas that require enhancements
    i. Providing a modular framework for EMV with remote vendors allows protocol changes and replacements

11) Questions

a. What are the steps of the EMV protocol required to provide authentication?
    i. What data needs to be provided for each step?
b. What hardware requirements are there to support the card reader?
    i. Smart Card Detective
    ii. Smart Card Reader
c. Is the pin required for the card to generate an authentication message?

12) Procedure and Time Schedule

The following list represents the steps involved in the investigation.

a. October 16-17
    i. Review authentication procedures for Internet purchases with payment cards

ii. Research known vulnerabilities and mitigation techniques for these authentication methods

b. November 4-6
   i. Reproduce no card present attack via man in the middle (MITM) for existing payment methods
c. November 18-20
   i. Develop infrastructure to support remote EMV transactions
d. December 2-4
   i. Attempt to reproduce known MITM attack with enhanced authentication

13) Areas of Specification Prone to Change

The following list includes areas of the project that are most likely to change.

a. Hardware interface to card
b. Timeline will change based on progress made

14) Table of Contents

15) Literature

[1] C. Brzuska, N. P. Smart, B. Warinschi, and G. J. Watson, "An analysis of the EMV channel establishment protocol," in *Proc. ACM CS*, 2013, pp. 373-386.
[2] J. de Ruiter and E. Poll, "Formal analysis of the EMV protocol suite," in *Theory of Sec. and Appl.*, 2011, vol. 6693, pp. 113-129.

[3] How EMV (chip and PIN) works – Transaction flow chart. (n.d.) Creditcall Ltd. [Online]. Available: https://www.level2kernel.com/flow-chart.html. Accessed Sept. 22, 2015.
[4] S. Watts. (2010, Feb. 11). New flaws in chip and pin system revealed. [Online]. Available: http://www.bbc.co.uk/blogs/newsnight/susanwatts/2010/-02/new_flaws_in_chip_and_pin_syst.html
[5] A. Johnson. (2008, Oct. 1). U.S. credit cards becoming outdated, less usable abroad. [Online]. Available: http://www.creditcards.com/credit-card-news/outdated-smart-card-chip-pin-1273.php
[6] "EMV and encryption + tokenization: A layered approach to security," First Data Corp., Atlanta, GA, 2012.
[7] M. Bond, O. Choudary, and S. Murdoch, "Chip and skim: Cloning EMV cards with the pre-play attack," in *Proc. IEEE S&P,* 2014, pp.1-15.
[8] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond, "Chip and PIN is broken," in *IEEE Symp. On Sec. and Privacy*, 2010, pp. 433-446.
[9] M. Yang. (2014, Sep. 15). Security enhanced EMV-based mobile payment protocol. [Online]. Available: http://www.hindawi.com/journals/tswj-/2014/864571/
[10] M. Schulz. (2014, Sep. 8). The unfortunate truth about your new chip credit card. [Online]. Available: http://www.huffingtonpost.com/creditcardscom/the-dirty-little-secret-y_b_5572081.html
[11] Will retailers be ready for EMV by Oct 15? (n.d.). Payments Leader. [Online]. Available: http://www.paymentsleader.com/will-retailers-be-ready-for-emv-by-oct-2015/. Accessed Oct. 4, 2015.
[12] "MasterCard authentication solutions: Two-factor solutions designed to enhance security for online banking and e-commerce," MasterCard Int. Inc., Purchase, NY, 2006.