Attack Tree for Modelling Unauthorized EMV Card Transactions at POS terminals

Dilpreet Singh, Ron Ruhl and Hamman Samuel
Information System Security and Management Department,
Concordia University College of Alberta, 7128 Ada Blvd NW, Edmonton, AB, Canada
dsingh2@student.concordia.ab.ca, {ron.ruhl, hamman.samuel}@concordia.ab.ca

Keywords: EMV, EMV transaction process, attack, attack tree methodology, point of sale terminal, PCIDSS.

Abstract: Europay, MasterCard and Visa (EMV) is a dominant protocol used for smart card payments worldwide, with over 730 million cards in circulation. One goal of the EMV protocol is to secure debit and credit transactions at a point-of-sale (POS) terminal, but still there are vulnerabilities, which can lead to unauthorized disclosure of cardholder data. This research paper will provide the reader with a single document listing the vulnerabilities leading to various possible attacks against EMV payment card transaction process at a POS terminal. Attack tree methodology will be used to document these vulnerabilities. This research will also provide the countermeasures against various possible attacks**.**

1 INTRODUCTION

For 25 years, EMV has implemented payment cards which initially used a magnetic stripe only but now contain a chip microprocessor which processes payments at POS devices. This research examines when the card is present at a POS terminal and will use attack tree methodology to describe the security of dynamic data authentication and combined data authentication (DDA/CDA) EMV cards.

2 EMV TRANSACTION PROCESS

EMV developed common protocol standards (Murdoch et al.,2010) which are published at emvco.com. General core requirements are also augmented by card specific standards of each party. The EMV card issuing bank is responsible for selecting specific subsets including authentication and risk management. The EMV transaction process can be categorized into three phases: card authentication, card verification and transaction authorization.

2.1 Card Authentication

The card authentication assures the card and the card issuer authenticity to the terminal. Card authentication involves a sequence of sub-steps.

2.1.1 Application Selection

EMV cards may contain multiple applications (Debit/Credit/ATM) and files supporting the applications. On inserting the EMV card into the POS terminal, the terminal requests to read the EMV file "1PAY.SYS.DDF01" listing the applications that the chip card contains. After successful application selection, the card sends the Processing Options Data Object List (PDOL) to the terminal. This lists the data elements that the card will require from the terminal to execute the next commands in the process. If high priority application selection fails, the terminal switches to the next priority application.

2.1.2 Read Application Data

After application selection, the terminal need to know the functionalities supported by the EMV card and the location of the information related to these functionalities. The terminal then issues, the Get Processing Options (GPO) command. In response, the card issues the Application Interchange Profile (AIP) and the Application File Locator (AFL). AIP indicates the functions that the card supports while AFL is a list of application data records for the supported functions by the card. These records contain cardholder information (e.g. primary account number, start and expiry date) which can be read by

the terminal using the read record command (Murdoch et al.,2010). These records have RSA digital signatures linked with a certificate authority (CA) known to the terminal. Depending upon the variant of the EMV, RSA crypto-graphic operations can be performed. Both DDA and CDA cards contain RSA private keys specific to the customer's card intended for use for asymmetric cryptographic operations such as digital signatures and encryption. The certificate for DDA and CDA public keys is created for the card and this is chained to the issuing bank and a CA. The CA public key is stored on all POS terminals.

2.1.3 Data Authentication

EMV specification for DDA and CDA is defined below (EMV,2008):

- DDA uses asymmetric cryptography to create a card-specific public-private key pair assigned to the card. The private key is securely stored and inaccessible to the terminal. The DDA certificate with the card public key is verified using challenge response (Breekel et al.,2016).
- CDA authenticates the transaction and the card by Message Authentication Code (MAC) with a key that the bank knows.

The type of data authentication method depends upon the terminal and the card capabilities.

2.1.4 Processing Restrictions

The terminal determines application compatibility supported by the card and the terminal. It involves matching the application version number, checking the type of allowed transactions, card validity and application validity and the current transactions allowed by the Application Usage Control (AUC).

2.2 Cardholder Verification

Cardholder verification uses the CVM list which specifies the card`s policy and when to use encrypted PIN, plaintext PIN, signature or No-CVM. It also specifies the steps to be taken if the verification fails (Murdoch et al.,2010). Most transactions today are PIN verified.

DDA and CDA cards send a PIN from the terminal to the chip encrypted with the public key of the card. The PIN verification process could be either 'offline' or 'online'. In offline PIN verification, the cardholder enters the PIN in the PIN Entry Device (PED) which is sent to the card (encrypted or unencrypted) (Murdoch et al.,2010). In case of "Offline Encrypted PIN" the chip transforms the PIN one-way according to the issuing banks specifications and then compares the result with the one which was previously stored on the card using the same one-way process. Based on the terminal capability it might send the "Offline Plain-text PIN" to the card which is not a secure way of communication thus making it susceptible to attacks. If the PIN matches, the transaction is processed further. If not correct, the PED asks for the PIN again (unless the retry counter stored on the EMV chip has reached its maximum). In "Online PIN" at an ATM the PIN is sent directly to the issuer over the payment network. Although most transactions are PIN verified, there are still terminals that do not have PIN entry devices and only accept magnetic stripe. In United Kingdom (UK) there exists a type of EMV card known as "Chip and Signature" card, which does not support PIN verification (Murdoch et al.,2010). These cards are issued to visually impaired customers or who have memory loss.

Unsigned CVM lists allow someone to modify the list and downgrade the card from one that requires a PIN verification to `signature` or `nothing` (i.e. no authentication at all).

2.3 Transaction Authorization

After successful cardholder verification, the terminal requests the card to generate a MAC over the transaction details which will be sent to the issuing bank (Murdoch et al.,2010). The transaction authorization can either be offline or online depending upon the card and terminal compatibility.

2.3.1 Terminal Risk Management

Terminal risk management is to safeguard the payment system against fraud. The risk of fraud can be reduced by online authorizing the transaction. Whether a transaction should be authorized online or offline depends mainly on three factors: offline floor limit; random selection of the transaction to be processed online; and lastly, if the card has not undergone an online transaction in a long time.

2.3.2 Terminal Action Analysis

In this step, the terminal makes the decision whether to online or offline authorize or to decline the transaction. For this, the terminal analyses the previous verification and authentication results. Irrespective of the terminal decision, it must request confirmation from the card and uses a Generate Application Cryptogram (generate AC) command.

2.3.3 Card Action Analysis

This step is the same as terminal action analysis. The difference is that the card makes the decision to authorize the transaction online or offline or to decline the transaction. The card may perform its own risk management (for example, in a Near Field Communication or NFC "tapped" transaction the risk limit for tapped transactions is held on the card). The card decision of authorising the transaction may differ from the terminal but is subjected to certain logic rules (e.g. the card is not permitted to request offline acceptance if the terminal proposed online authorization). The card communicates its decision to the terminal using a cryptogram. The card will then generate: transaction approved (Transaction Certificate - TC); request online approval (Authorization Request Cryptogram - ARQC); or, transaction declined (Application Authentication Cryptogram - AAC).

2.3.4 Offline/Online Decision

If the terminal receives a TC or AAC that means the transaction is completed with an offline authorized or offline declined. But if the terminal received an ARQC that means the transaction needs to be online authorized and the transaction authorization request is sent to the issuer. The cryptogram sent to the bank includes a type code, a sequence counter identifying the transaction (ATC – application transaction counter), a variable length field containing data generated by the issuer application, and a MAC, which is calculated over the rest of the message including a description of the transaction (Murdoch et al.,2010). The MAC is computed, typically using 3DES, with a symmetric key shared between the card and the issuing bank (Murdoch et al.,2010). The issuing bank performs several checks and then returns a ARC (authorization response code), indicating how the transaction should proceed and places this in an ARPC (authorization response cryptogram) (Murdoch et al.,2010). The card validates the computed MAC contained with ARPC and if successful it means the issuer authorized the transaction (Murdoch et al.,2010). Now the card issues a TC that the terminal sends to the issuing bank and stores a copy of it for record purposes.

2.4 Transaction Completion

In offline transaction approval, the card generated TC is sent to the issuer right away or later as a part of the transaction settlement process. If the transaction is approved or declined online the terminal will request a final transaction cryptogram using the Generate AC command. After the final card processing the card can be removed from the terminal. An EMV card transaction can be made contactless if the POS allows. For contactless payments, the card needs to be in range of the terminal so that information exchange takes place**.** For contact type cards, the card needs to be inserted in the terminal. Contactless EMV card transactions have a similar transaction process with a few exceptions in the protocol as follows:

- EMV contactless transaction have two modes: EMV mode and Mag-Stripe mode.
- Contactless involves only one cryptogram exchange and not two.
- A new CVM method is added known as consumer device CVM. It applies when the contactless transaction uses a NFC phone (Breekel et al.,2016).

Contactless transactions start with the terminal choosing the high priority application from the list specified in the Proximity Payment System included in the 1PAY.SYS.DDF01 (Breekel et al.,2016). Then the terminal specifies the mode of operation. Mag-stripe mode is often in older infrastructure where the terminal cannot process chip data nor authenticate static data on the card (Breekel et al.,2016). Instead of the normal GENERATE AC command it uses the COMPUTE CRYPTOGRAPHIC CHECKSUM command and an Unpredictable Number is included as a parameter (Breekel et al.,2016). For EMV mode a new CVM called on-device cardholder verification is used. If both terminal and card have high priority for this CVM method, the transaction is performed with this CVM (Breekel et al.,2016). The terminal then passes the argument that offline plain text PIN is used and how the device verifies the cardholder identity is not specified. The rest of the transaction process flow is like the contact transaction process flow. In contactless transaction, there is only one cryptogram involved so it has a different meaning from the contact transaction described above:

- Contact EMV transactions generated TC indicates the offline or online transaction approval, whereas for contactless transactions it indicates offline approval.
- A generated ARQC in a contactless transaction is not followed by a TC or AAC. This indicates that the card or terminal requires issuer authorization for the transaction (Breekel et al.,2016).

- If a transaction is declined, an AAC is generated just like contact transactions.

3 PCI DSS STANDARD OVERVIEW

The Payment Card Industry Data Security Standard (PCI DSS) sets the technical and operational requirements for merchants to protect cardholder data. This standard applies to any entity that stores, transmits or processes cardholder data and the standard is enforced by EMV. The important PCI DSS goals related to this research are: Protect cardholder data; and Implement strong access control measures. The detailed document is available online (PCI DSS quick reference guide, 2009).

4 THE ATTACKS

The various types of attacks possible on DDA/CDA EMV cards, but not limited to, are given below:

4.1 Man-in-the-middle Attack (MITM)

The central fault in the EMV protocol is that the PIN verification step is never clearly authenticated (Murdoch et al.,2010). A man-in-the-middle device can easily perform this attack if it can intercept and modify the communication between card and terminal. This attack makes the terminal believe that PIN verification took place and was successful whereas it makes the card believe PIN verification was not attempted and another mechanism (e.g. signature) was used. The entered dummy PIN never gets to the card and therefore the PIN retry counter on the card is not changed. If the transaction is processed offline there is less ability to detect the attack as the issuer will not be contacted during the transaction process. If the transaction is processed online, the man-in-the-middle can change the cryptogram type thus turning an ARQC or AAC into a TC (Murdoch et al.,2010). This may cause cryptogram verification to fail and by the time it will be detected the attacker would have left the POS.

This attack execution has been demonstrated on live terminals (Murdoch et al.,2010). The illustration shows that the man-in-middle circuit has a fake card that will be inserted into the legitimate terminal. The fake card is connected to an interface chip ($2 Maxim 1740 [8]) through thin wires used for voltage shifting (Murdoch et al.,2010). This is connected to a FPGA board ($189 Spartan-3E Starter Kit [9]) that converts between the card and PC interface. FPGA is then connected to a laptop through a serial link which is then connected to smart card reader from Alcor Micro (11) in which the stolen genuine card is inserted (Murdoch et al.,2010). A python script running on a laptop relays the transaction while waiting for the verify command being sent by the terminal (Murdoch et al.,2010). It then suppresses it to the card and responds with a verify command (Murdoch et al.,2010). The rest of the communication is unchanged. The attack could be easily miniaturised.

The cardholder could prevent this attack if the cardholder were notified after every transaction the card makes. The cardholder would deactivate the stolen card if unauthorized transactions occurred. Merchants could prevent this attack by giving proper training to their employees. In addition, the bank could prevent the attack by digitally signing the CVM list so that the attacker cannot modify them.

4.2 Pre-Play Attack (PPA)

Michael Roland and Josef Langer demonstrated an attack scenario to forge the magnetic stripe information for contactless payment cards using skimming. This PPA is used to obtain dynamic card verification codes (CVC) required for authorising payments. They further described a weakness in credit cards by downgrading its CVM list to magnetic stripe mode. Mike Bond et al. (2014) demonstrated a type of PPA where he predicted the unpredictable number (UN) for the automated teller machine (ATM) but for this attack the target is limited to an EMV contactless protocol in mag-stripe mode. The limit of the attack is the maximum amount that can be authorized with a contactless card transaction (Vila and Rodrıguez). There are four kernel specification (1,2,3,4) variants for the EMV contactless payment systems (Vila and Rodrıguez). For this attack scenario, Kernel 2 specifications were used in that the protocol interacts with payment cards supporting the MasterCard Pay Pass or similar cards. In the mag-stripe implementation, the UN used in the COMPUTE CRYPTOGRAPHIC CHECKSUM command is weakened by the protocol design itself. The UN is a 4-byte value limited by a BCD-encoding numeric value in the kernel 2 specification in which UN ranges from 0 to 99,999,999. In the magnetic stripe protocol, the UN is reduced to 0 to 999. This set of UN was predicted in a minute using the Android App running on a Google Galaxy Nexus S (Vila and Rodrıguez). An attacker communicating for one minute with the EMV mag-stripe card can generate enough information required for a successful

payment transaction. The CVC is obtained using the UN, the card secret key and Application Transaction Counter (ATC). The ATC increases for each EMV transaction which prevents against replay attacks. However, an attacker can use only one ATC+ CVC set per transaction. The attacker overwrites AIP clearing the flag containing EMV mode downgrading it to mag-stripe. Mag-stripe mode data returned in GET PROCESSING OPTIONS is not authenticated. With this data, the attacker can create a functional contactless clone with pre-played data.

To demonstrate a successful combined pre-play attack and downgrade to mag-stripe attack scenario, the system involves a Java card application and an Android app. The Android app running on Galaxy Nexus is used to collect mag-stripe data and pre-play data from a genuine card through its contactless interface which later can be transferred to a Java card with the same application.

The simplest fix against this attack is a cryptographically secure random number generator. The cardholder could also prevent this attack by placing the card in an aluminum box. Banks could prevent this by digitally signing the CVM list so the attacker cannot modify the list.

4.3 NFC Relay Attack

Jose Vila and Ricardo J. Rodrıguez showed implementation alternatives to achieve relay attacks in Android devices and to demonstrate practical implementation of the attacks using NFC-enabled phones (Kfir and Wool). This attack is a type of passive relay attack. In this attack, the attacker can trick the reader into communication with a victim that is very far away. An attacker can use a pick-pocket system to use the victim's contactless card data without the victim's knowledge. In near-field communication (NFC), there are three modes of operation (i.e. peer-to-peer mode, read/write and card-emulation mode). In peer-to-peer mode, NFC devices communicate with each other directly. In read/write mode, NFC devices communicate with the NFC tag. In card-emulation mode, the NFC device emulates as a contactless smartcard (Kfir and Wool). The NFC relay attack is achieved by: a peer-peer communication channel; a malicious verifier (i.e. fake terminal) communicating with the legitimate contactless payment card; and, a malicious prover (i.e. fake card) communicating with the legitimate POS terminal.

The communication is relayed from the legitimate card to the legitimate terminal without the cardholder knowing about a malicious verifier and malicious prover. The limitations of this attack are that the NFC-enabled device acting as a malicious verifier must be in read/write mode (Kfir and Wool); and, the card must be in host-card emulation (HCE) mode, which is natively supported from Android KitKat onward (Kfir and Wool).

To successfully perform this attack, two off-the-shelf Android NFC-enabled mobile devices executing an Android application were developed for testing purposes (about 2000 Java Lines of Code Counter (LOC) and able to act as dishonest verifier/prover, depending on user's choice), having a single constraint: The dishonest prover must execute, at least, an Android KitKat version (Kfir and Wool). The POS device used is Ingenico IWL280. The experiment has been successfully tested (Kfir and Wool) on several mobile devices, such as Nexus 4, Nexus 5 as dishonest provers, and Samsung Galaxy Nexus, Sony Xperia S as dishonest verifiers (Kfir and Wool).

This attack can be prevented by using a Faraday-cage approach as well. Another countermeasure is to control the activation of the card (i.e. the card gets activated only with the PIN entry by the cardholder).

4.4 Shim-in-the-middle Attack

Shim-in-the-middle attacks involve inserting a thin, flexible circuit board into the card slot between the reader and the card chip. A circuit that transmits the signal to a nearby receiver is hard to detect in the PED. An attacker can also attach a shim to the card and insert it into the PED. The shim stays in place in the machine and the card is removed by the attacker. A nearby receiver records card details and PINs. The cardholder PIN can be intercepted if the PIN was sent in the plain-text (Bond,2006). The intercepted information related to PINs or accounts enables counterfeiting magnetic stripes which can be later used for unauthorised transaction purposes at terminals accepting magnetic stripe. This attack does not need employee participation. Therefore, corrupt merchants prefer it as they can easily deny any knowledge of the shim existence in their PED.

This attack can be prevented by merchants obeying to the PCI DSS goals stated earlier. The cardholder could prevent this attack if they know how to detect the presence of shimmer in the terminal. Merchant could also train their employees and use tamper-resistance terminal to prevent this attack. POS clerks could also identify modification to the terminal during daily inspection routine.

4.5 Eavesdrop Attacks

During an EMV transaction process at a POS terminal, account details or a PIN can be eavesdropped to forge the magnetic stripe for fraudulent activates.

4.5.1 Camera and Double-swipe Method

This approach involves a camera facing the PIN pad and a fraudulent merchant who secretly swipes the customer's card through his own device to intercept information needed to counterfeit the magnetic stripe. The fraudulent merchant keeps two terminals: one genuine terminal and one fraud merchant terminal since modifying a working terminal requires bypassing a tamper resistant device. Tampering with the POS is complicated and requires considerable manual effort (Bond, 2006).

4.5.2 Counterfeit Terminal

This approach constructs a counterfeit terminal which captures data to forge the magnetic stripe. The counterfeit terminal may require the cardholder to enter the PIN which is intercepted using sensors or software key loggers (Bond, 2006).

4.5.3 Signal Eavesdropping Attack

This attack is used to tap the data line in the PED to get the unencrypted information required to create a fake magnetic stripe card. This attack was demonstrated on two widely deployed PEDs in the UK (i.e. the Ingenico i3300 and the Dione Xtreme) (Drimer, Murdoch and Anderson, 2008). Ingenico PED was defeated easily with a simple 'tapping attack' (due to design flaws in the Ingenico PED). This PED has a user accessible compartment in its rear which is not tamper-proof (Drimer, Murdoch and Anderson, 2008). This compartment leads to the circuit board and many signals routed at the bottom layer. The PED's designers opted to provide 1mm diameter holes and other holes through the printed circuit board (PCB) (Drimer, Murdoch and Anderson,2008). The holes are used for positioning optional surface mount sockets. If the PED has one of these holes, it can be easily used to tap a metal hook to a data line. The tap can be placed between the card chip and the microprocessor. However, in the given case, this attack was easily achieved using a bent paperclip placed through the hole (Drimer, Murdoch and Anderson,2008).

In the Dione Extreme PED there is no concealed compartment that helps to hide the wiretap but it is still vulnerable. However, a 4cm needle can be inserted into a flat ribbon connector socket through a 0.8 mm hole from rear (Drimer, Murdoch and Anderson, 2008). A thin wire connected to a FPGA board can translate the data and send it to a laptop that will show an answer to reset (ATR) initial exchange intercepted using the tap (Drimer, Murdoch and Anderson, 2008). In Ingenico PED, a small FPGA board can easily be inserted into the compartment without anyone's knowledge from where the attacker can easily record transaction details. In the case of Dione PED, a small FPGA board can be hidden under the counter and cannot be easily detected unless the cardholder knows what to look for (Drimer, Murdoch and Anderson, 2008).

Eavesdropping attacks can be prevented by merchants complying to the PCI DSS goals "Protect Cardholder Data and Implement Strong Access Control Measures" (PCI quick reference guide,2009). In some of the eavesdrop attacks, the merchants themselves can be an attacker. To protect against this, the cardholder should be given tips on how to detect the modifications in the terminal.

4.6 Fall-back to Magnetic Stripe and Cross-Border Fraud

The weakness that current EMV cards are facing is fallback to the magnetic stripe whenever the Chip and PIN is not used. This enables the attackers to skim a customer`s credit card and record the PIN as well. An attacker can then create a new card with the skimmed data and the observed PIN (Anderson, Bond and Murdoch). This is a widely faced problem with countries accepting PIN's along with magnetic stripe technology for EMV transactions. Thus, an attacker can use the card stolen from one country in another country using the magnetic stripe technology. This attack is an international version of the fallback to magnetic stripe attack and therefore known as cross-border fraud.

Encrypted PIN and use of 'iCVV' (card verification value for integrated circuit cards) is a countermeasure for fallback to magnetic stripe based attacks. The previously stored CVV is replaced by iCVV in the chip cards. When using iCVV during the chip based transactions the CVV from the magnetic stripe can be recovered by swiping the card into a separate reader (Drimer, Murdoch and Anderson, 2008).

4.7 Active Relay Attack

In this attack, a victim initiates the EMV transaction process with an attacker installed reader which the victim is unaware of. A victim thinks he is paying a

small amount at the malicious reader but the reader relays the card response to a remote legitimate reader to pay for more expensive items (Mehrnezhad, Hao and Shahandashti, 2017). The relayed wirelessly communication allows a real POS purchase. The victim thinks they paid a small amount but instead they would eventually be billed for a much larger amount. Since the malicious reader is not connected to the bank, the victim will never be charged for the small amount and will show only one large transaction (Drimer and Murdoch, 2013). This attack is possible for both contact and contactless EMV transactions depending on the POS and the card compatibility.

Attack requirements for this attack include a fake terminal and a fake card. A FPGA board is used in the fake terminal (Saar and Murdoch,2013). Two laptops are needed to relay signals. The FPGA code and PC software written in python and Verilog requires programming skills (Drimer and Murdoch, 2013).

This attack can be prevented by either using a distance-bounding protocol or using a user-interface. For a user-interface, the customer inserts the card into an interface and then the interface into the terminal. If the amount shown on the interface is satisfactory to the cardholder he/she can carry on with the transaction. This interface will protect against magnetic-stripe forging. For distance-bounding protocol, the card and terminal must support the protocol (Drimer, Murdoch and Anderson, 2008).

5 ATTACK TREE METHODOLOGY

Attack tree methodology can be used to demonstrate different ways in which a system can be attacked and to design countermeasures thwarting the attacks (Schneier,1999). Various attacks against a system are represented with the goal as root node and how to achieve it in different ways as leaf nodes.

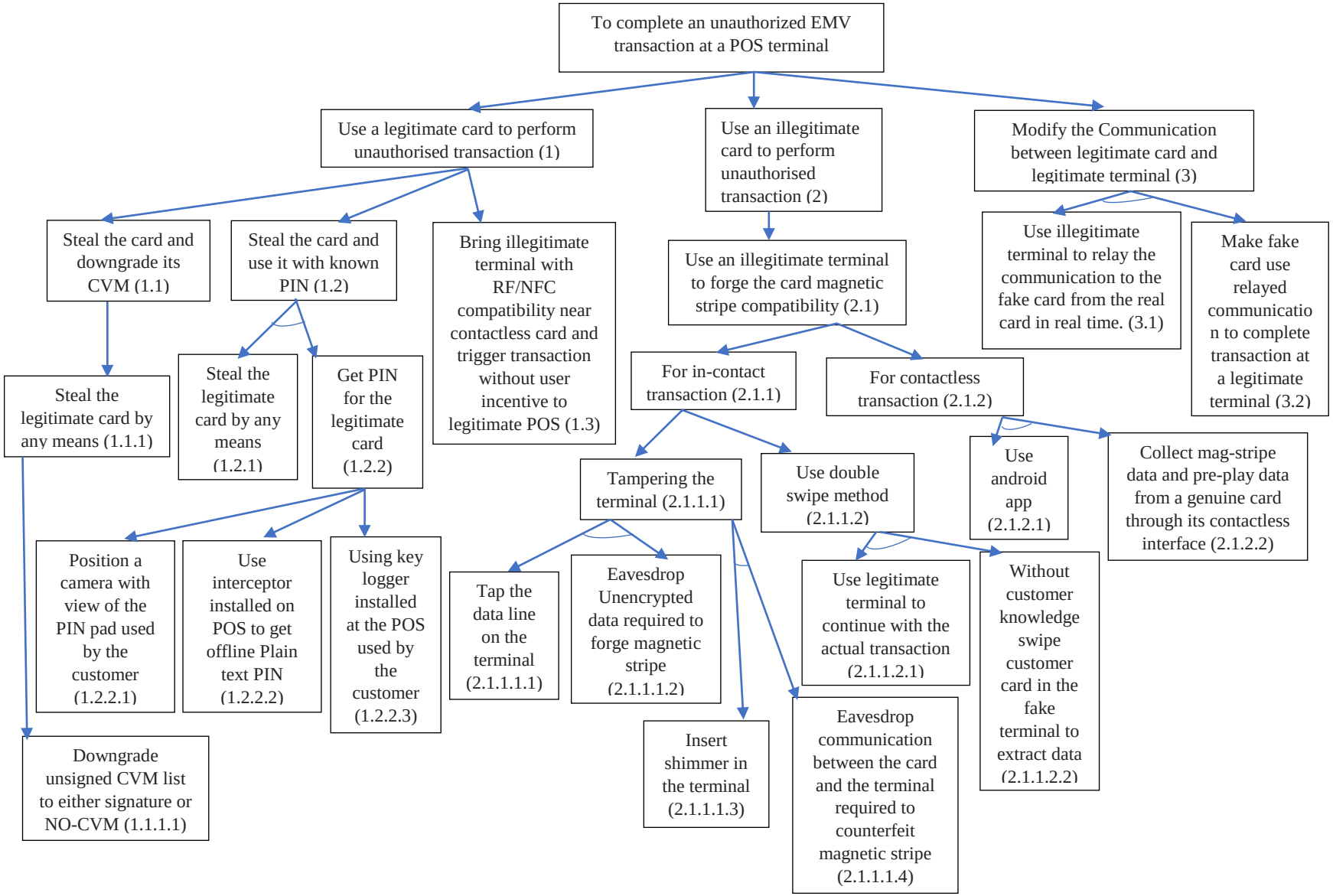
Each leaf node becomes a sub-goal and children of those leaf nodes are ways to achieve that sub-goal (Schneier,1999). The attack tree structure is refined using AND or OR logical connections. In AND logical connections, all sister node conditions should be met to achieve the sub-goal, whereas OR logical connection acts as alternative methods. In the attack tree, AND logical connection is represented as **'ن'** in between the line connectors whereas OR logical connections are simple line connectors.

The table below list EMV attacks. An arrow vector is used to represent the down hierarchy of the attack tree nodes (i.e. the sequence an attacker can follow to achieve an attack). The AND logical connection from the attack tree configuration is represented as '&' whereas OR logical connection is represented as '-'. The attack tree follows Table 1.

Table 1: Attack tree nodes mapping various attacks and countermeasures against those attacks.

ATTACKS	ATTACK TREE NODES	ATTACK MITIGATION STRATEGY
Man-in-the-middle attack	1→1.1→1.1.1 → 1.1.1.1	Cardholder gets real time notification of the transactions made. Merchants inserting cards into the terminal by themselves. Card issuing bank signing the CVM list.
Pre-play attack	2→2.1→2.1.2 →2.1.2.1&2.1 .2.2	Cryptographically secure random number generator. Faraday-cage approach. Signed CVM list.
NFC-Relay Attack	1→1.3	Faraday-cage approach and controlling the card activation.
Shim-in-the-middle attack	2→2.1→2.1.1 →2.1.1.1→ 2.1.1.1.3& 2.1.1.1.4	Tamper-resistance terminal. Daily routine inspections by merchants. Cardholder detection of changes to the terminal.
Camera and Double-swipe method	2→2.1→2.1.1 →2.1.1.2→ 2.1.1.2.1& 2.1.1.2.2	The cardholder having adequate knowledge about how to detect the modification in the terminal and to determine suspicious activities.
Counterfeit Terminal	1→1.2→1.2.1 &1.2.2→1.2.2 .1-1.2.2.2- 1.2.2.3	Encrypted PIN and use of 'iCVV' (i.e. ensure the transaction if chip based)
Signal eavesdropping attack	2→2.1→2.1.1 →2.1.1.1→2. 1.1.1.1& 2.1.1.1.2	PCI DSS requirement: Encrypt transmission of cardholder data across open, public network and restrict physical access to cardholder data. The cardholder able to detect the modification in the terminal.
Active relay attack	3→3.1 & 3.2	Distance-bounding protocol of card and terminal and/or user-interface method.

Attack tree modelling an unauthorised EMV transaction at a POS terminal



6 CONCLUSIONS

This paper studied various attacks producing unauthorized EMV card transaction at POS terminals using an attack tree. Countermeasures against those attacks are also provided. EMV card industry participants can use this to understand the risk to various parties during EMV transactions at a POS terminal. This research adds to the existing attack trees for ATM and browser EMV exploits.

REFRENCES

Bruce Schneier, "Attack Tree" [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html [Accessed 11 May 2017].

EMV – Integrated Circuit Specifications for Payment Systems, Book 2: Security and Key Management, version 4.2 ed., LLC, June 2008.

Ezeude, Kingsley Anayo " The Modeling of An Identity Catching Attack on The Universal Mobile Telecommunication system (UMTS) Using Attack Tree methodology" [Online]. Available: https://www.scribd.com/document/243982400/The-Modeling-Of-An-Identity-Catching-Attack-On-The-Universal-Mobile-Telecommunication-System-UMTS-Using-Attack-Tree-Methodology [Accessed 14 May 2017].

How EMV (Chip and PIN) Works - Transaction Flow Chart [Online]. Available: https://www.level2kernel.com/flow-chart.html.

Joeri de Riuter and Erik Poll, Formal Analysis of EMV Protocol Suite, Digital Security Group, Radboud University Nijimegen, Netherlands. 2011 [Online] Available; http://www.cs.ru.nl/E.Poll/papers/emv.pdf

Jordi van den Breekel, Diego A. Ortiz-Yepes, Erik Poll, and Joeri de Ruiter, "EMV in a nutshell" [Online]. Available:https://www.cs.ru.nl/E.Poll/papers/EMVtechreport.pdf [Accessed 18 May 2017].

Jose Vila and Ricardo J. Rodrıguez," Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited"[Online]. Available: https://conference.hitb.org/hitbsecconf2015ams/materials/Whitepapers/Relay%20Attacks%20in%20EMV%20Contactless%20Cards%20with%20Android%20OTS%20Devices.pdf [Accessed 28 May 2017].

M. Bond. Chip and PIN (EMV) interceptor, March 2006.http://www.cl.cam.ac.uk/research/security/banking/interceptor/ [Accessed 28 May 2017].

Maryam Mehrnezhad, Feng Hao, and Siamak F. Shahandashti, " Tap-Tap and Pay (TTP): Preventing the Mafia Attack in NFC Payment "[Online]. Available:https://www.researchgate.net/publication/300132931_TapTap_and_Pay_TTP_Preventing_the_Mafia_Attack_in_NFC_Payment [Accessed 12 June 2017].

Maxim Integrated Products, Inc., MAX1740, MAX1741 SIM/smart-card level translators in μMAX, January 2001, [Online] Available http://datasheets.maxim-ic.com/en/ds/MAX1740-MAX1741pdf

Michael Roland and Josef Langer," Cloning Credit Cards: A combined pre-play and downgrade attack on EMV Contactless "[Online]. Available: https://www.usenix.org/system/files/conference/woot13/woot13-roland.pdf [Accessed 04 June 2017].

Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, Ross Anderson" Chip and Skim: cloning EMV cards with the pre-play attack," 2014 IEEE Symposium on Security and Privacy

Ogundele Oludele, Zavarsky Pavol, Ruhl Ron and Lindskog Dale, "Implementation of a Full EMV Smartcard for a Point-of-Sale Transaction", World Congress on Internet Security (WorldCIS), 2011, Publication Year: 2012, Pages(s): 28 – 35.

Oludele Ogundele, Pavol Zavarsky, Ron Ruhl, Dale Lindskog" Fraud Reduction on EMV Payment Cards by the Implementation of Stringent Security Features" International Journal of Intelligent Computing Research (IJICR), Volume 3, Issues 1/2, Mar/Jun 2012

PCI Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 1.2 [Online] Available:https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf [Accessed 02 October 2017]

Ross Anderson, Mike Bond, and Steven J. Murdoch" Chip and Spin" [Online]. Available: http://www.chipandspin.co.uk/spin.pdf [Accessed 15 March 2017].

Saar Drimer and Steven J. Murdoch," Chip and PIN (EMV) relay attacks"[Online]. Available: https://www.cl.cam.ac.uk/research/security/banking/relay/ [Accessed 08 June 2017].

Saar Drimer, Steven J. Murdoch, Ross Anderson" Thinking Inside the Box: System-Level Failures of Tamper Proofing" 2008 IEEE Symposium on Security and Privacy

Step by step: How does a EMV contact card payment work? [Online]. Available: https://www.quora.com/Step-by-step-How-does-a-EMV-contact-card-payment-work.

Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond " Chip and PIN is Broken," 2010 2010 IEEE Symposium on Security and Privacy.

Visa Expands Technology Innovation Program for U.S. Merchants to Adopt Dual Interface Terminals. [Online]. Available: http://usa.visa.com/download/merchants/bulletin-tip-us-merchants-080911.pdf

Xilinx Inc., "Spartan-3E starter kit," November 2009. [Online]. Available: http://www.xilinx.com/products/devkits/ HW-SPAR3E-SK-US-G.htm

Ziv Kfir and Avishai Wool," Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems" [Online]. Available: http://ieeexplore.ieee.org/document/1607558/ [Accessed 24 May 2017].