Bare Demo of IEEEtran.cls for IEEE Conferences

Michael Shell
School of Electrical and
Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332–0250
Email: http://www.michaelshell.org/contact.html

Homer Simpson
Twentieth Century Fox
Springfield, USA
Email: homer@thesimpsons.com

James Kirk
and Montgomery Scott
Starfleet Academy
San Francisco, California 96678–2391
Telephone: (800) 555–1212
Fax: (888) 555–1212

Abstract—**Near Field Communication(NFC) has expanded rapidly and is set to be the new big thing in communication. Contact-less payment processing being its biggest beneficiary, there are many other uses of NFC technology like passport identification, security access etc.The growth in NFC technology does not come without any security vulnerabilities. Malicious attackers can carry out many attacks like Eavesdropping,Man in the middle attack and Relay attacks on this type of communication.Among all these types of attacks relay attack is currently not detectable and cannot be predicted in most scenarios.Relay attacks can be carried out on un-encrypted data and is much more dangerous when compared to man in the middle attack.In this paper we give an overview of security issues in NFC communication, describe the relay attack in detail, present our timing based solution to the problem and its implementation, and give results of our evaluation of timing based relay prevention.**

I. Introduction

Near field communication is a type of wireless radio communication designed for a very short range, usually up to 10 cm.It was originally based on RFID (Radio-frequency identification) and operates at 13.56 MHz communicating very small amounts of data, at rates between 106 and 424 kbps. NFC is primarily designed for communication between a tag and a reader using these radio frequency waves. When NFC is used for communication of secure and confidential data, security is always going to be an issue that has to be dealt with priority.Secure transactions, such as financial, the need for security is even higher. Credit card in its natural form is prone to fraud and is rapidly moving to a contact-less medium for conducting business which adds more complexity. The security of NFC is a significant concern and as the use of this technology grows, that concern grows with it.One of the inherent security structures built into NFC technology is the proximity for communication.Because tags are only able to communicate over about 10 cm eavesdropping on the communication can prove to be challenging. It has previously been shown that distance can actually be increased to at least 50 cm. While any attack involving the transfer of secure information is a concern, the relay attack is one of the most critical because there is not a lot of hardware that is required to carry out this attack and the user would not have an idea when the attack takes place.

II. Relay attacks on NFC Communication

The intruder launches a relay episode by putting a malicious reader close to the label owners genuine label and a malicious tag close to the genuine reader. The malicious tag as well as the malicious reader are connected as well as form an url to pass all activity forth and back between the authentic tag as well as authentic reader. The relay may be attached over any medium including the Bluetooth or Internet, and all visitors in between the genuine tag and genuine reader is transferred straight to the opposite end. Figure 1.3 illustrates a relay strike. Right here we are able to observe the malicious tag C comes into selection of the authentic reader D what requests communication. This particular request is passed from the relay to the malicious person B as well as the petition is created to the genuine tag A. Tag A responds and that information is transferred again throughout the link on the authentic reader D. The authentic tag as well as authentic reader both believe they're speaking directly to the genuine unit in close proximity. This particular confidence of proximity is bypassed by the relay, and the inherent security feature breaks. Since tags are made to be activated with no user interaction they're especially susceptible to this particular attack. A malicious party may just provide one end of the relay of theirs up to a geniune label while it's in a pocket or perhaps a bag.

III. Existing work

Several of the more promising work done in relay attack prevention use distance bounding protocols, which set an upper bound to the distances allowed. This is actually attained by requiring a cryptographic challenge response mechanism to measure the proximity to the authentic device. This approach is able to present challenges, such as time for processing such responses, elimination of time extensions for responses, and dealing with noisy channels. The more error resistance is actually incorporated into them the far more open to attacks these bounding protocols can become. A few promis- ing work incorporates a full duplex secret key agreement scheme into the distance bounding [twenty nine]. This would hopefully help with computation and power consumption demands as a result of the cost of cryptographic operations. Even when proper encryption strategies are actually used the protocols still remain vulnerable to relay attacks [twenty eight]. Without authentication of the reader, an attacker could query the tag in the beginning and replay the info at a later time, which is sometimes called terrorist fraud. Eavesdropping, or perhaps listening in on such conversations, has been identified as a problem. Unless encryption of information is needed in some form this remains an issue. The ECMA even state in one of their documents that users must plan implementations carefully around possible vulnerabilities. As encryption isn't built into NFC, security is actually left up to the application developer, or perhaps the end user of the technology, which isn't a comforting prospect. Even encryption schemes may be ineffective without prior sharing of device authentication. With the relay attack in case we could keep the information from the tag and send it to the proxy to emulate the tag then detection in this manner becomes impossible. There would be no additional timing delays in such a setup. This's also not accurately Fifteen described as a relay attack however. This's much more of a true man-in-the-middle or perhaps just store and replay attack. This particular kind of security vulnerability has already been seen in attacks such as ticket cloning [seven]. Even a replay attack for passport control was discussed and is actually vulnerable, but again, this is a replay, not a relay attack.

A. *Countering relay attacks*

An effective countermeasure solution against the relay attack addressed here will be an implementation that will work within the operating constraints of the existing ECMA and ISO standards. By giving a little change to the software program at the reader or initiator we are able to in essence provide a solution with a software program or perhaps firmware update. This wouldn't create changes to any of the existing tags, which have already been manufactured and distributed. Rather changes will remain limited to the readers, and could produce an an easy-to-implement and affordable solution to our issue. We don't propose a change to any of the standards, to the communication techniques or anything to compromise alternate tag type compatibility, but rather a warning mechanism to detect and counter possible relay attempts. This remedy has been implemented and tested with Type two Mifare Ultralight A tags. It's consistent and functional. We just used Mifare Ultralight A tags in this project, but if alternate tag types not tested here were to present additional timing artifacts, such as anomalies in the time readings, then at probably the worst warnings will be generated. The implementation could allow for disabling such warnings if necessary. In a situation where those other cards types were seldom seen, the occasional warning may actually be acceptable. We will advise against allowing a system to present warnings constantly as users could tend to be unaware and complacent when real problems occurred [twenty]. If different tag types were to be used additional research into timing for those tags should be evaluated. We want this particular solution to be robust against attacks and consistent in its warnings. In devices that are Android for instance a quick code update could create the warning and verification system needed to protect against relay attacks and could be pushed out to the devices as any normal software update would be.

IV. Contactless Payment System

From new form factors like watches and phones, to new acceptance locations - like vending machines - contactless payment technology is actually fueling innovation in the payments industry. Issuers and payment brands have introduced a variety of form factors including fobs, mini cards, stickers, mobile phones and wearables (jewellery, wristwatches and wristbands) - all enabled with contactless payment. As a result, consumers now view contactless as an established payment method for low value general retail transactions, ticketing and transport, and toll or perhaps parking transactions. And contactless is actually happening on the mobile in a huge way. Already available in the US, Canada and Australia, Apple Pay - Apple's mobile payment and digital wallet service - will soon launch in China, Hong Kong, Spain and Singapore. Apple isn't alone. Google, Samsung and others are actually looking at extending contactless mobile payment to the users of theirs. Indeed, Samsung is actually taking things even more with plans to extend service beyond payment to transit passes, coupons and membership cards - an approach also possible on today's multi application contactless payment cards.

A. *Devices in Contacless Payments*

Almost any device capable of making payments using radio frequency identification (RFID) technology is actually using contactless payment technology. The device doesn't have to be a smartphone though this's by far the most commonly used device for contactless payments. An antenna and chip embedded into the device lets the customer wave their smartphone over a card reader to create a purchase.

Security for contactless payments is actually the same as for charge card. Fraud protection laws all apply, and secure channels and encryption are actually used for sending credit card info and PIN numbers. For several purchases or high priced purchases within a very short period of time, the user is actually asked to manually enter her PIN number to ensure theft hasn't occurred. Typically contactless payments are faster because the PIN number or even a signature is not necessary. It also, nonetheless, can result in the customer to spend much more since paying is very quick and easy.

The very first example of contactless payment came in the form of Speedpass in 1997. Mobil gas stations offered contactless payment devices that clipped onto a key ring. The customer waved the device over a labeled square at the gas pump and paid instantly. Today ExxonMobil still offers this service, and other gas stations are actually incorporating contactless payment technologies into their payment choices.

1) Subsubsection Heading Here: Subsubsection text here.

V. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.