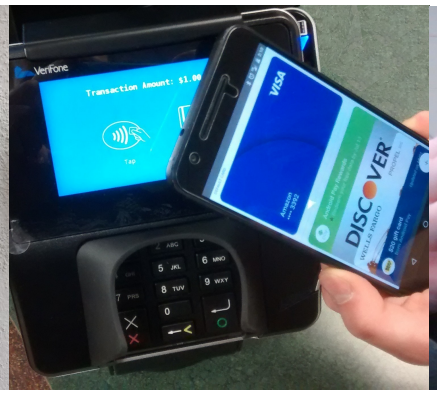
Security of Near Field Communication: Does My Phone Need A Tinfoil Hat?

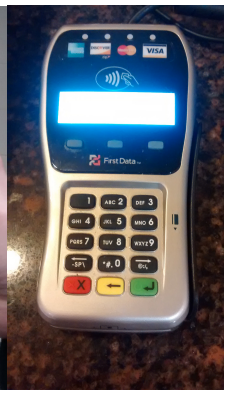
Thomas Harren

University of Minnesota, Morris

April 30, 2015

Have you used NFC?

Note: The communication standard used in UCard was not verified

Definition

Near Field Communication or *NFC*

is a short-range contactless communication technology.

Definition

Near Field Communication or *NFC*

is a short-range contactless communication technology.

- 1 meter range
- Quick setup
- Line of sight not required

Motivation

Questions about NFC

- What is NFC and how does it work?
- Is it secure and should I trust it?
- Is NFC the future?

Outline

Background

Introduction to RFID

- NFC is based on *radio frequency identification* (RFID) technology

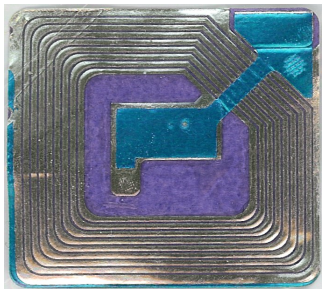
Introduction to RFID

- NFC is based on *radio frequency identification* (RFID) technology
- Range depends on frequency, size of antenna, power, and interference

Introduction to RFID

- NFC is based on *radio frequency identification* (RFID) technology
- Range depends on frequency, size of antenna, power, and interference
- Communication happens between tags and readers

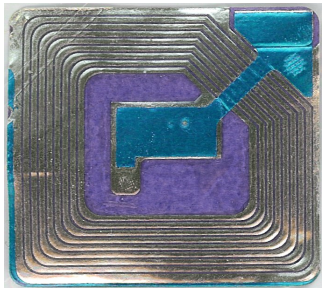
Tags & Readers



Tag

- A tiny circuit with an antenna coil
- Stores limited information
- Can be powered or passive
- Passive tags are smallest and cheapest

Tags & Readers



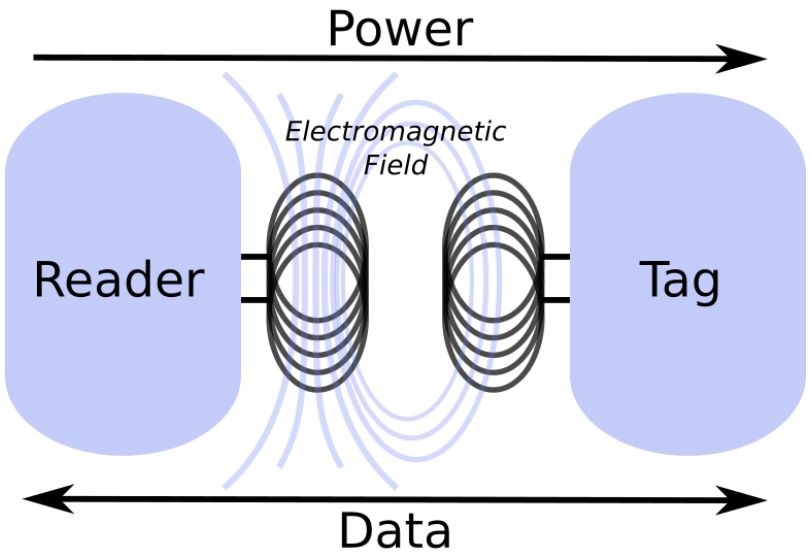
Tag

- A tiny circuit with an antenna coil
- Stores limited information
- Can be powered or passive
- Passive tags are smallest and cheapest

Reader

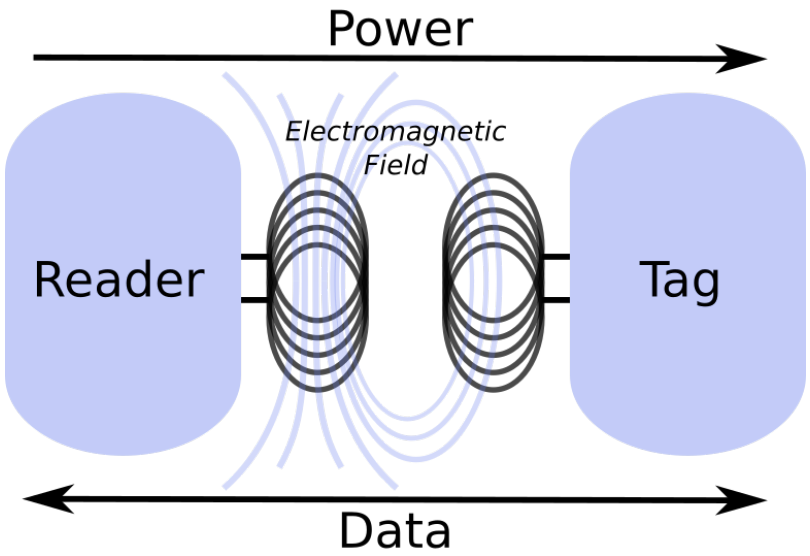
- Reader generates an electromagnetic field using an antenna coil
- The tags coil receives power from the field
- Initiates communication

Contactless Communication



RFID Communication

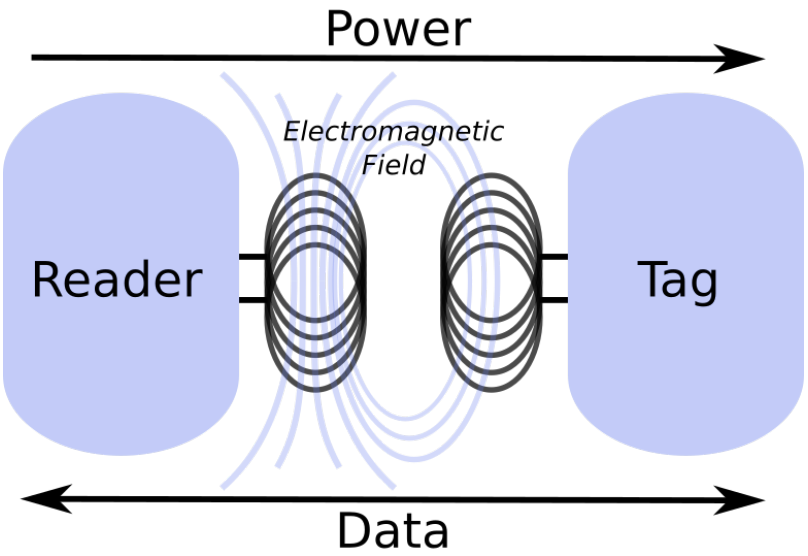
Contactless Communication



RFID Communication

1. Reader generates a field

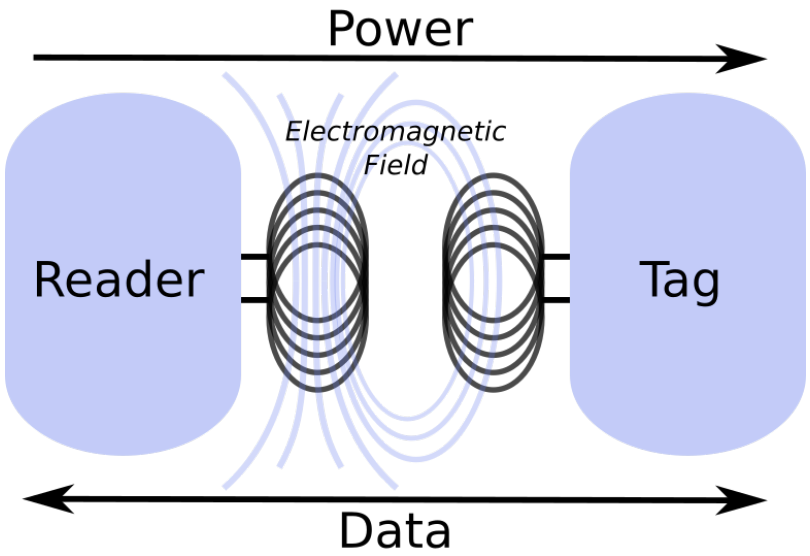
Contactless Communication



RFID Communication

1. Reader generates a field
2. Tag is activated by induced power

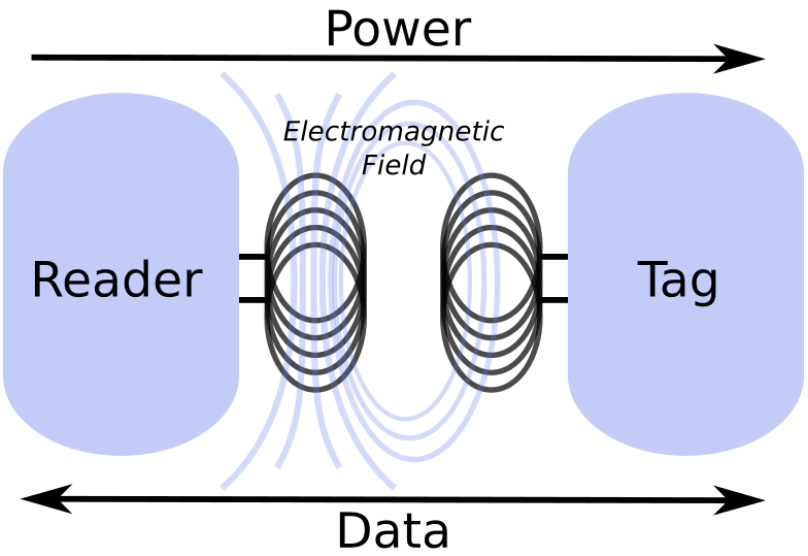
Contactless Communication



RFID Communication

1. Reader generates a field
2. Tag is activated by induced power
3. Reader runs discovery protocol, selecting tag by unique ID

Contactless Communication



RFID Communication

1. Reader generates a field
2. Tag is activated by induced power
3. Reader runs discovery protocol, selecting tag by unique ID
4. Communication ensues

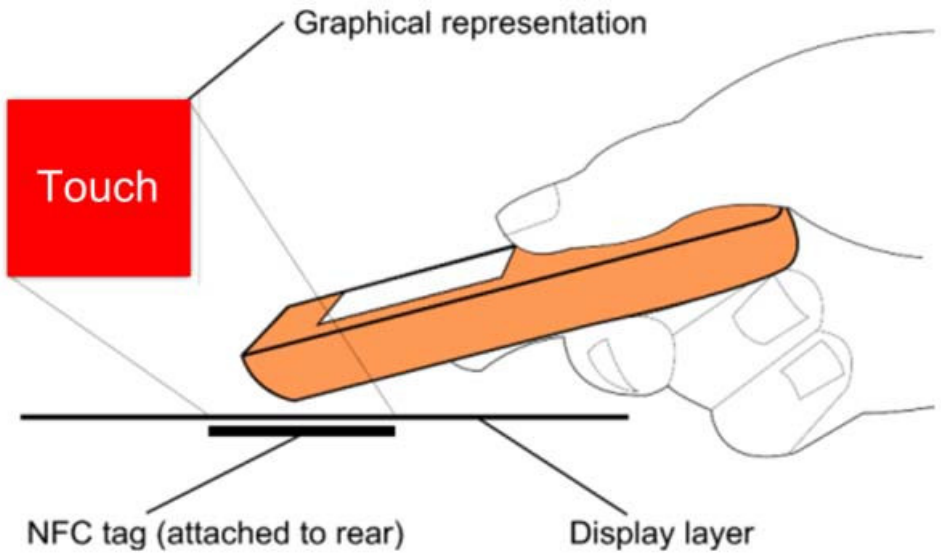
NFC on Mobile Phones

NFC extends RFID:

1. Phones can act as readers
2. Phones can emulate tags
3. Phones can communicate peer-to-peer

NFC on Mobile Phones

1 Phones can act as readers

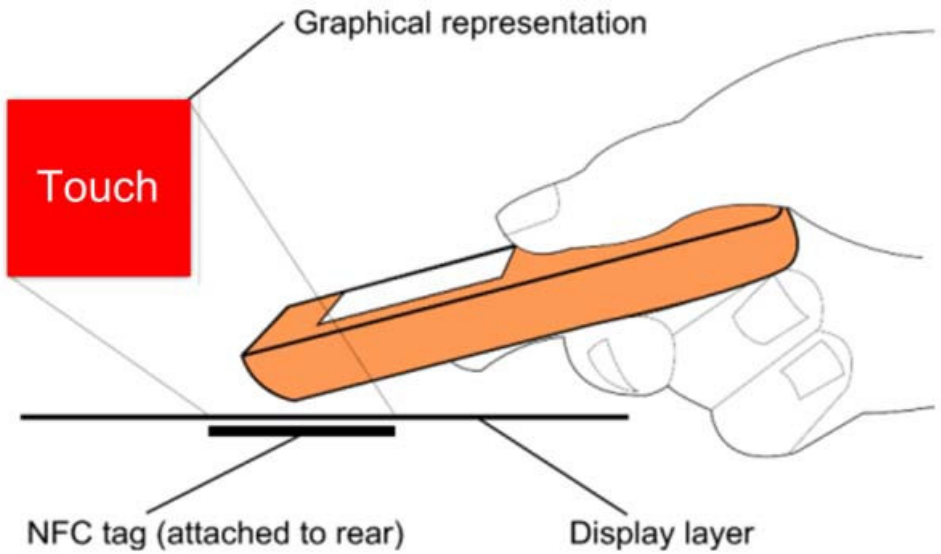


- Phones read NFC tags as if they were QR codes

Image from Hardy 2010

NFC on Mobile Phones

1 Phones can act as readers

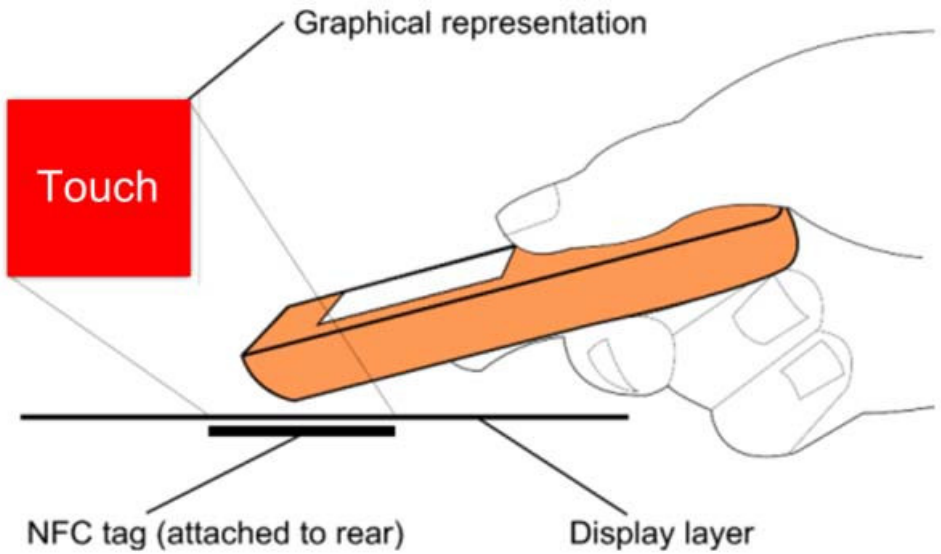


- Phones read NFC tags as if they were QR codes
- Touching a tag mounted to a map could bring up tourist information

Image from Hardy 2010

NFC on Mobile Phones

1 Phones can act as readers



- Phones read NFC tags as if they were QR codes
- Touching a tag mounted to a map could bring up tourist information
- Research into using tags as a user interface

Image from Hardy 2010

NFC on Mobile Phones

2 Phones can emulate tags

- Phones acts as if it were a passive tag

Image Note: Thank you Evan

NFC on Mobile Phones

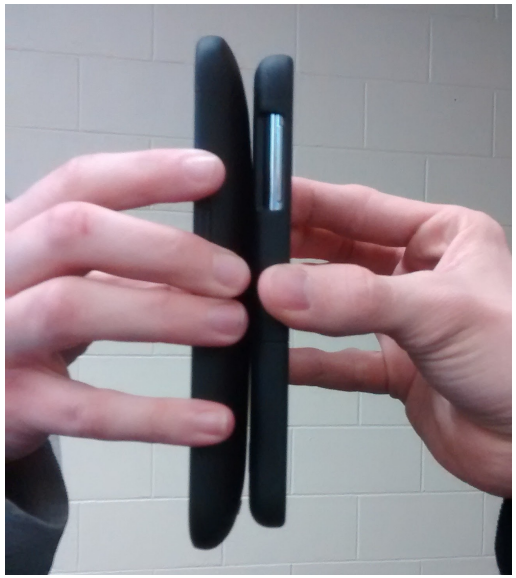
2 Phones can emulate tags

- Phones acts as if it were a passive tag
- A possibility for payments or ticketing applications

Image Note: Thank you Evan

Phones can communicate peer-to-peer

3 Phones can communicate as peers

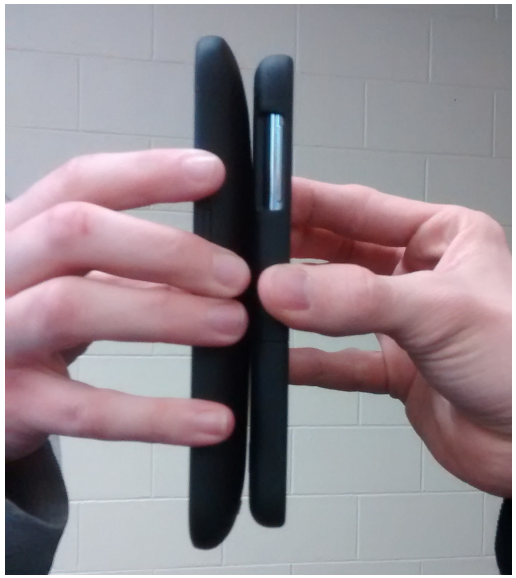


- Phones take turns switching between reader and tag-emulation mode

Image Note: Thank you Jacob and Maggie

Phones can communicate peer-to-peer

3 Phones can communicate as peers

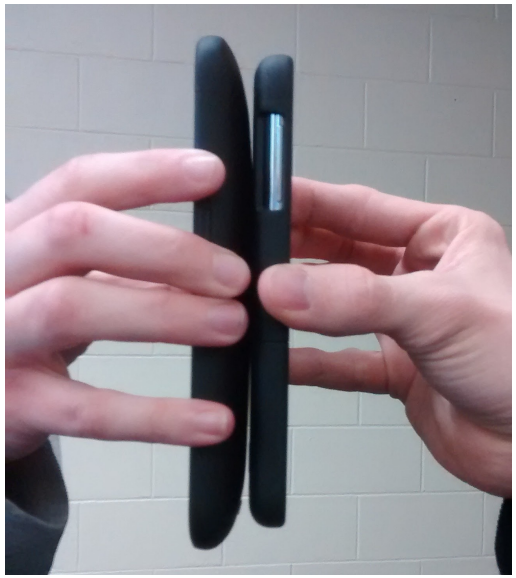


- Phones take turns switching between reader and tag-emulation mode
- Highest NFC communication throughput

Image Note: Thank you Jacob and Maggie

Phones can communicate peer-to-peer

3 Phones can communicate as peers



- Phones take turns switching between reader and tag-emulation mode
- Highest NFC communication throughput
- Can be used as a basis for stronger security or file transfers

Image Note: Thank you Jacob and Maggie

Security for NFC

NFC is not inherently secure

1. NFC's limited range makes attacks difficult, but not impossible
2. Features like confidentiality, integrity, and authentication need to be implemented as an extension of NFC

Contactless Credit Cards

Contactless Credit Cards

- Some credit cards contain passive NFC tags

Contactless Credit Cards

- Some credit cards contain passive NFC tags
- We focus on Jensen, Gouda, and Qiu's [1] work on securing such cards in this section

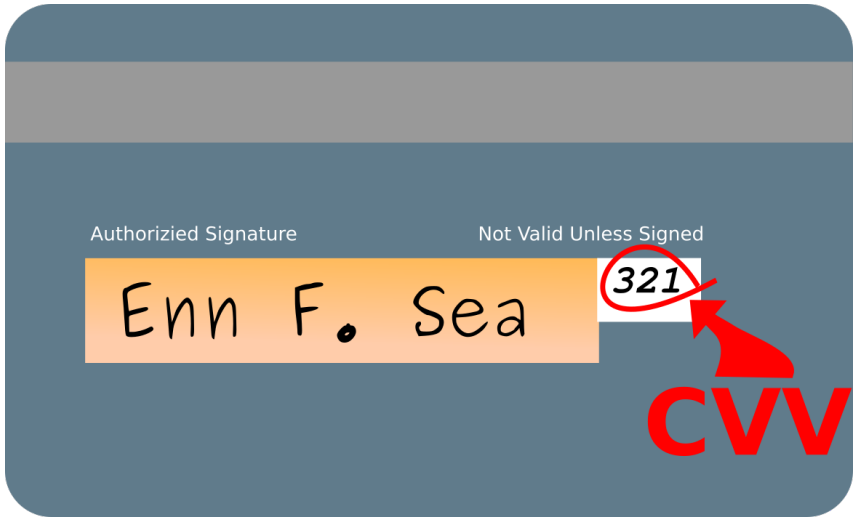
Contactless Credit Cards

Contactless Credit Cards

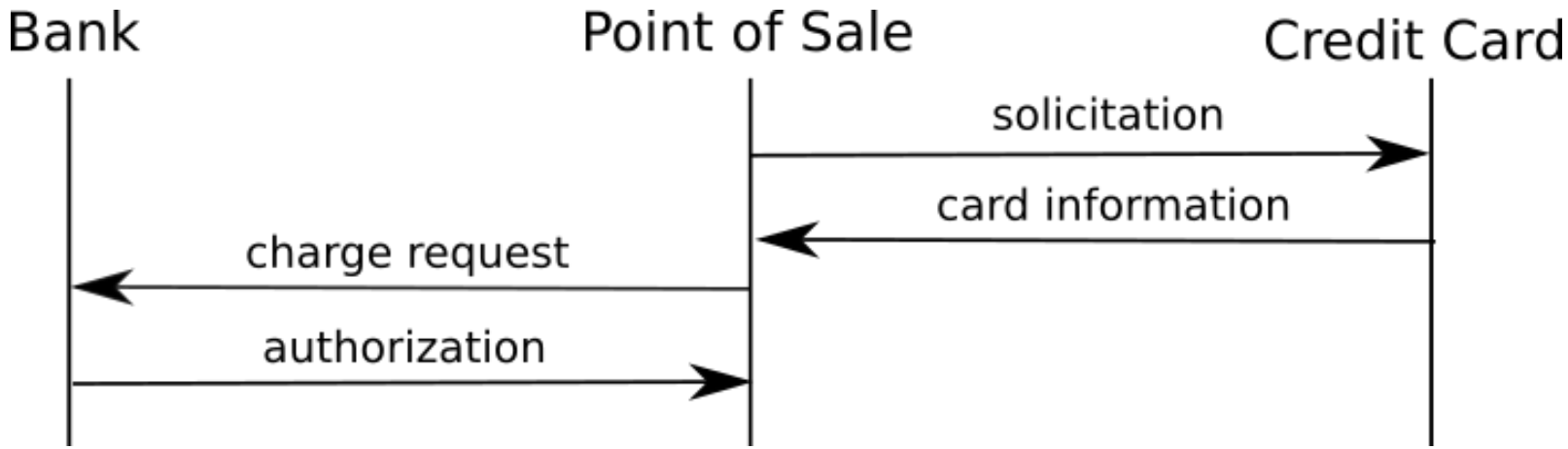
- Some credit cards contain passive NFC tags
- We focus on Jensen, Gouda, and Qiu's [1] work on securing such cards in this section
- Security solutions must be computationally inexpensive to run on passive tags

Contactless Credit Cards

- Card generates a pseudo-random *Dynamic Card Validation Value* (iCVV) for each transaction
- The iCVV is sent to point of sale and then validated by bank



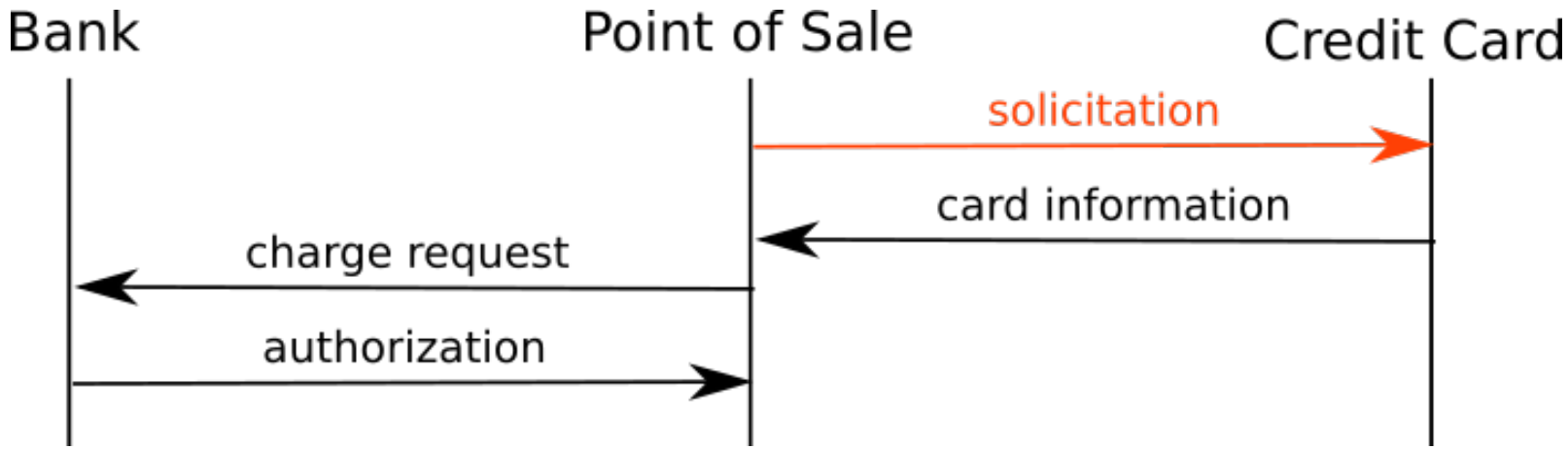
Current Credit Protocol



Security depends upon

- Each transaction's card generated iCVV
- The limited range of NFC

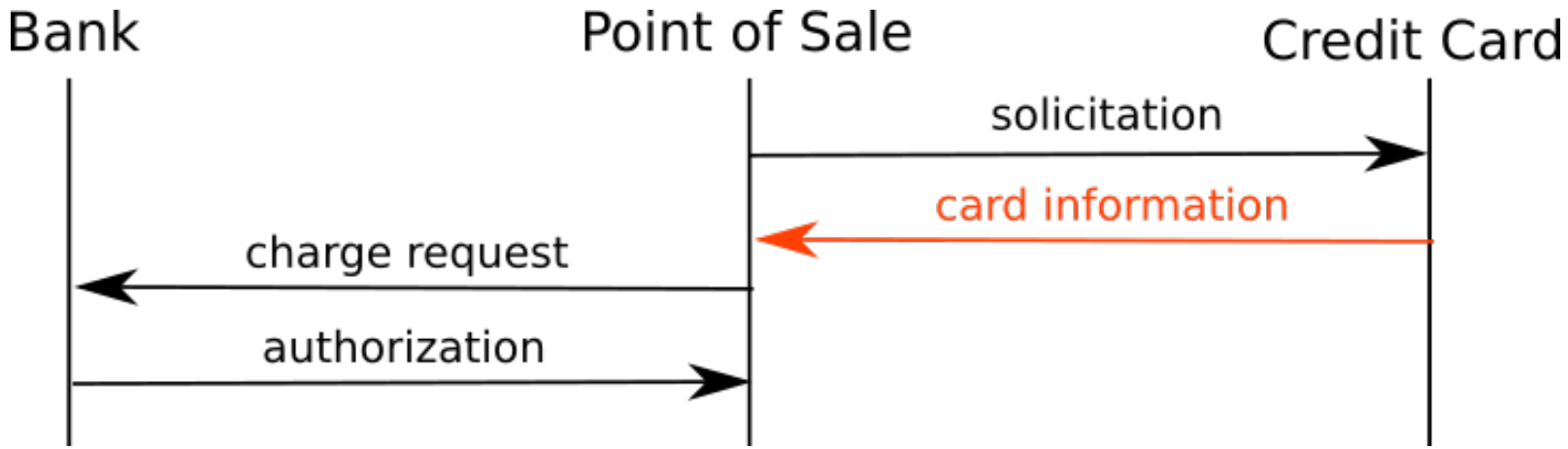
Current Credit Protocol



Solicitation

- Point of Sale and Credit card exchange static messages
- For example, card may identify itself as `VISA CREDIT`

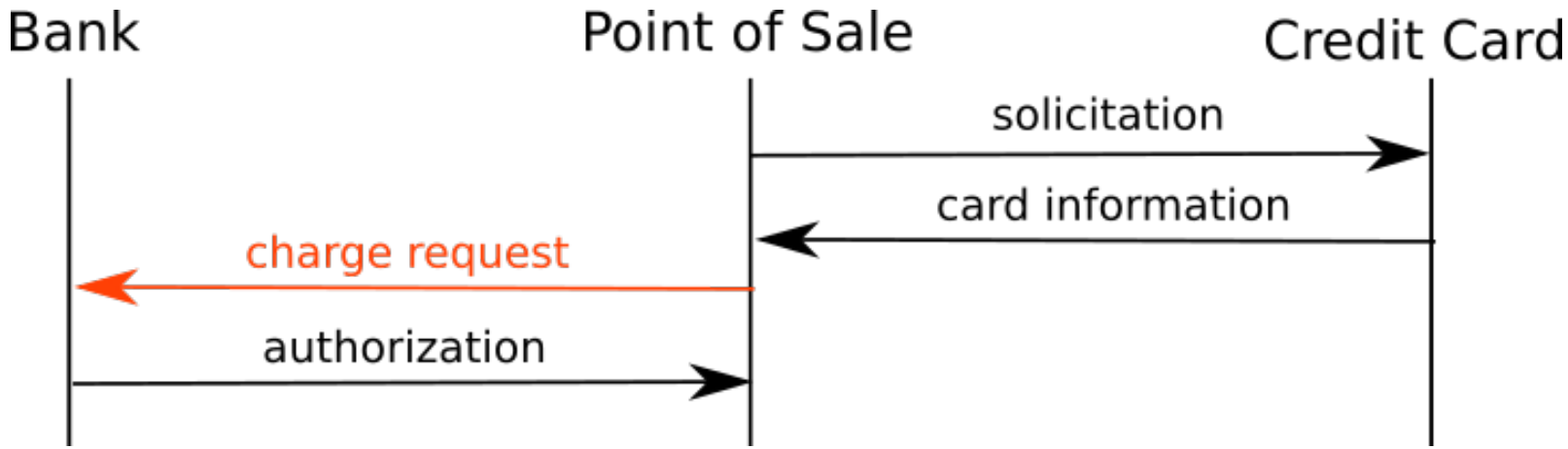
Current Credit Protocol



Card Information

- Credit card transmits card information, including: **card number, expiration, bank name, and iCVV**
- Unfortunately, this transmission is in plain text

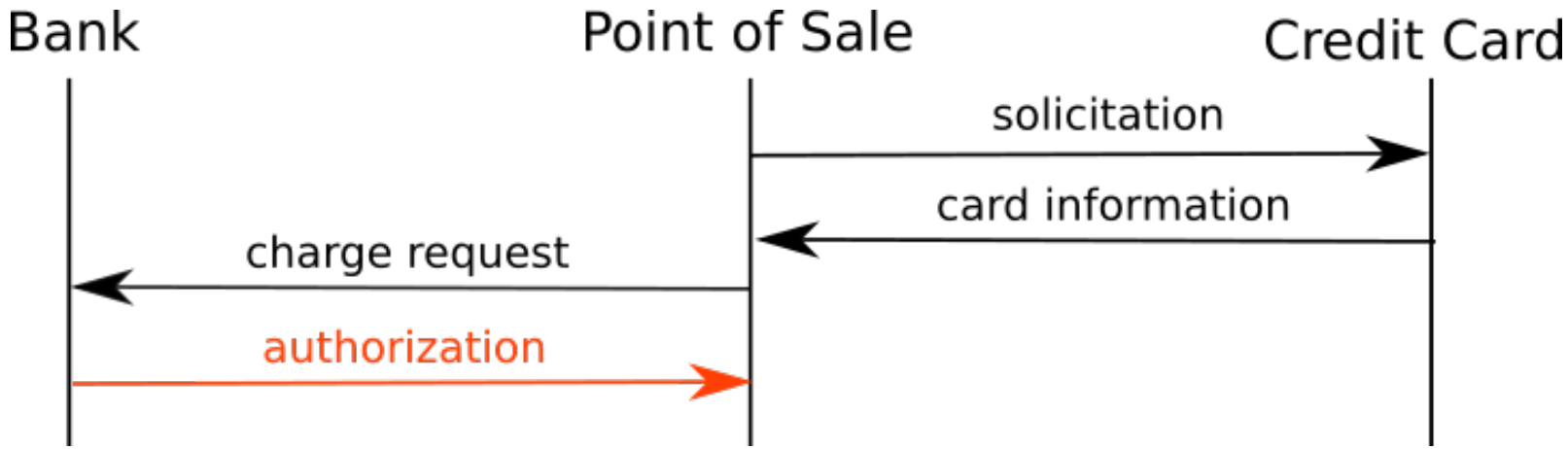
Current Credit Protocol



Charge request

- Card number, expiration, and iCVV are sent to the indicated bank

Current Credit Protocol



Authorization

- Bank verifies transaction by checking iCVV, location information, and other bank information

Eavesdropping

Eavesdropping

- A third party captures sensitive information sent between Point of Sale and Credit Card

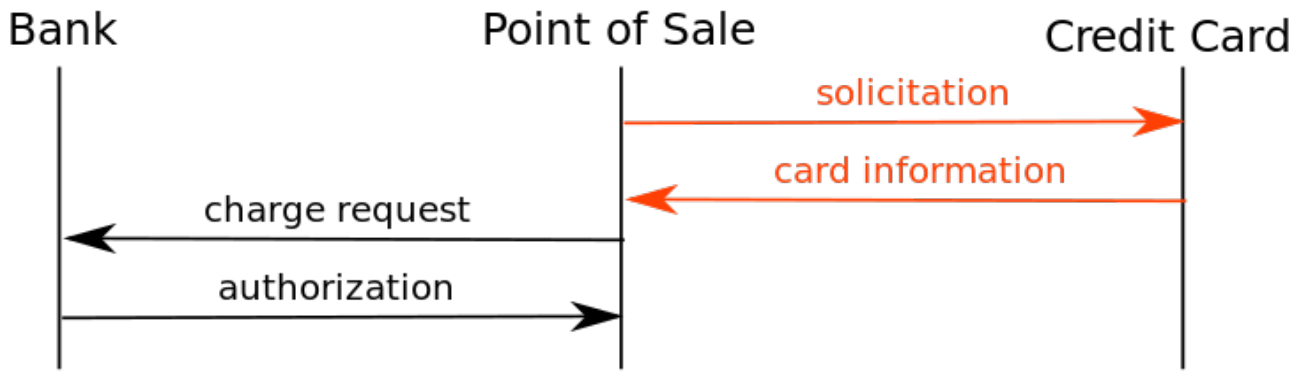


Photo of eavesdropper from Flicker

Eavesdropping

Eavesdropping

- A third party captures sensitive information sent between Point of Sale and Credit Card

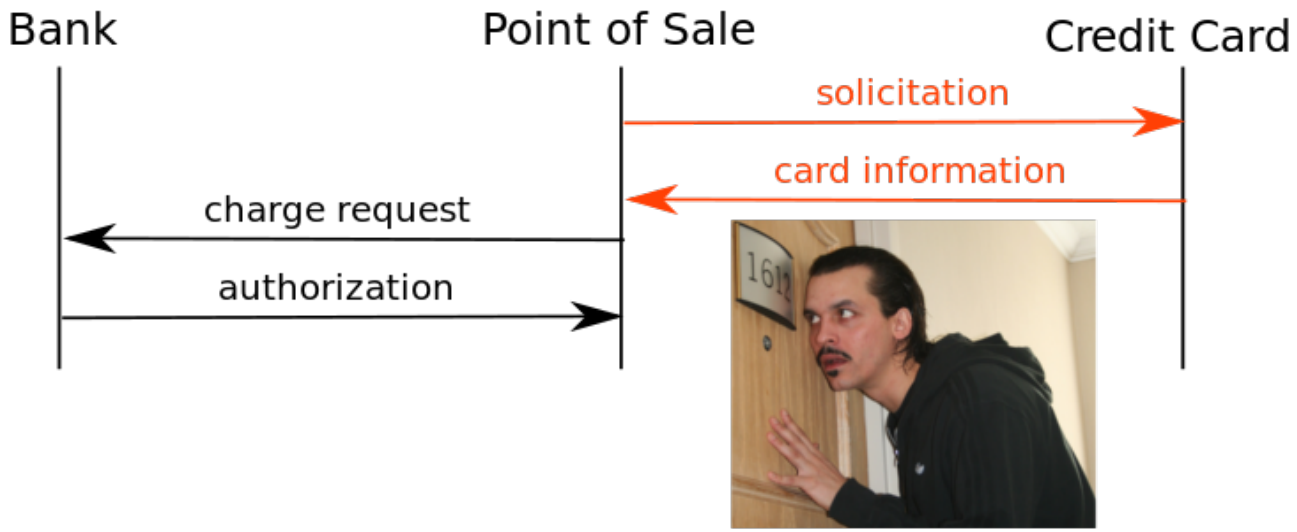


Photo of eavesdropper from Flicker

Eavesdropping

- A third party captures sensitive information sent between Point of Sale and Credit Card
- Card number, expiration, bank name, and *used* iCVV can be obtained

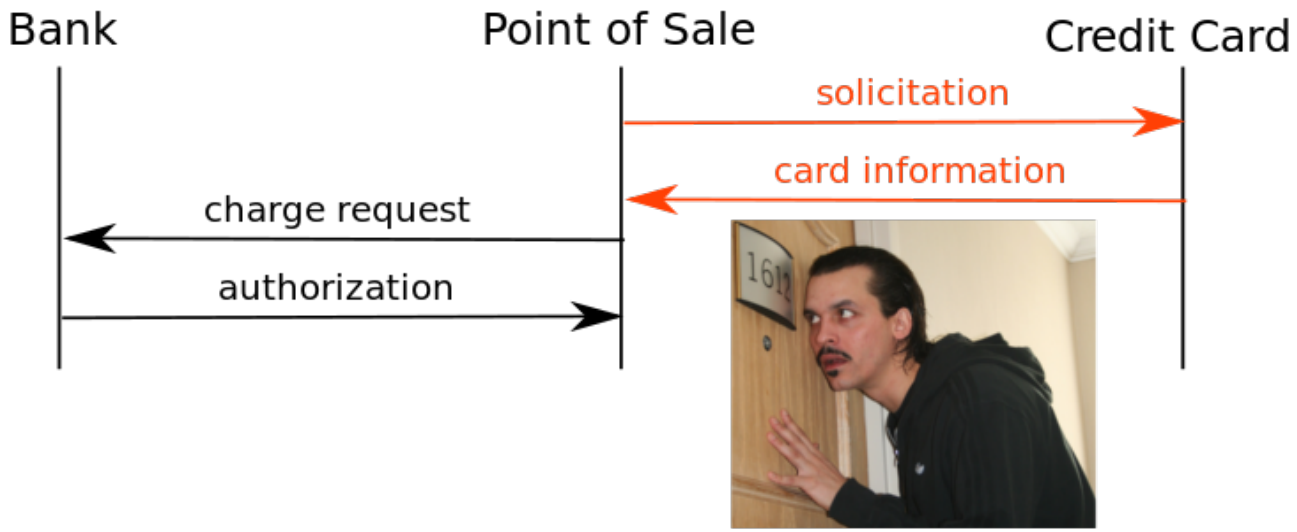
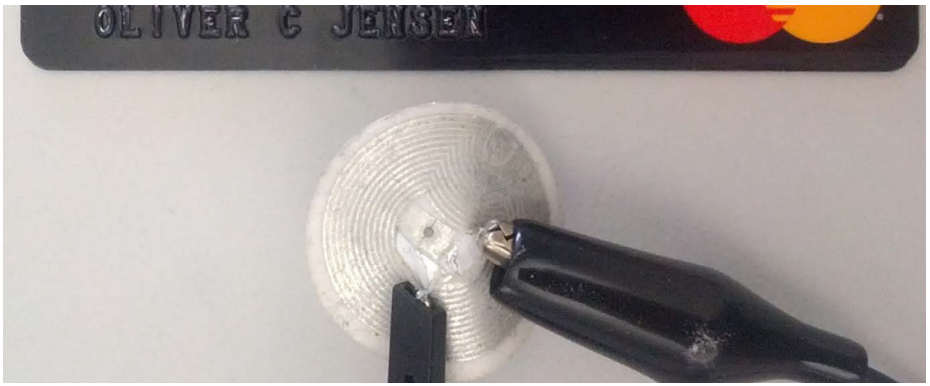


Photo of eavesdropper from Flicker

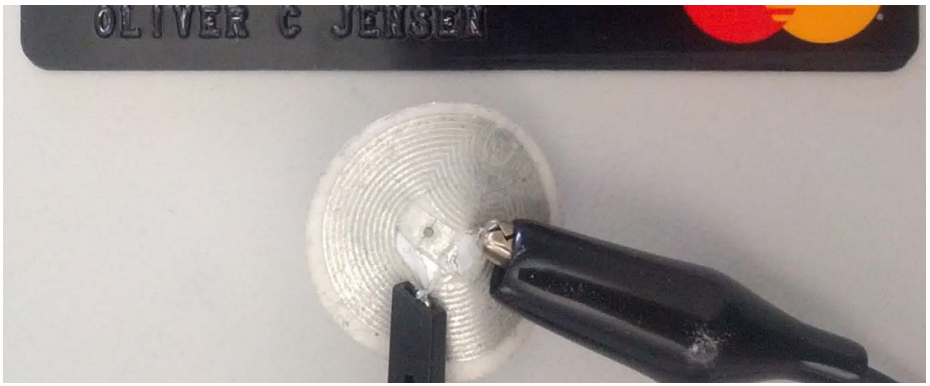
Eavesdropping

The eavesdropping attack is feasible, requiring only an inexpensive tag and radio



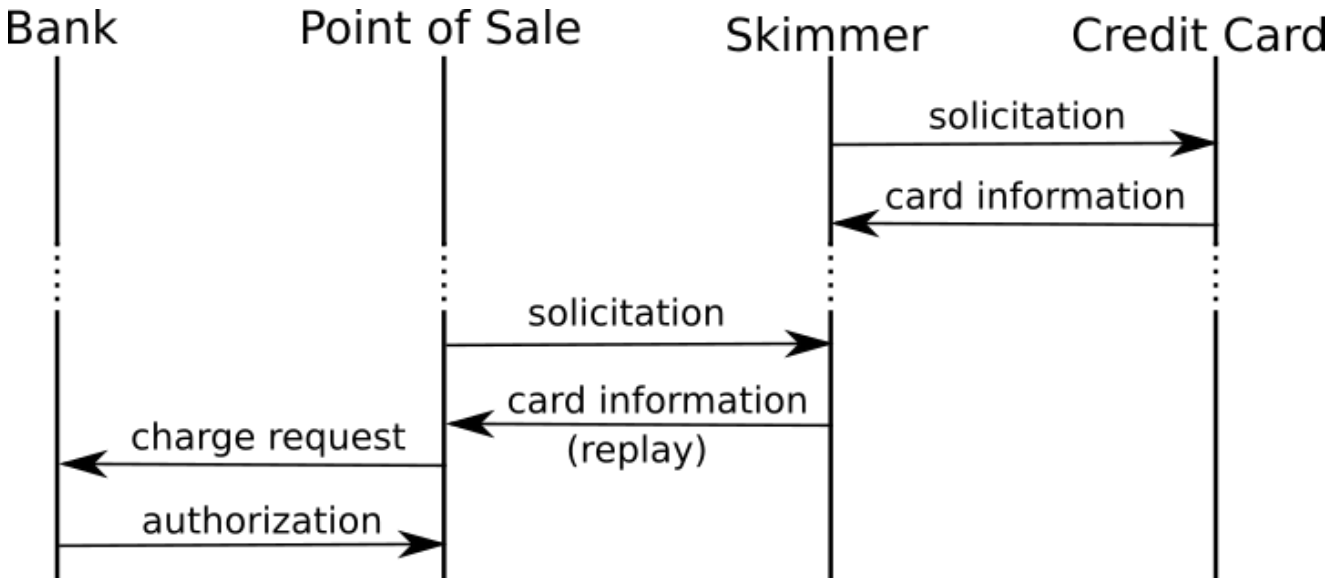
Eavesdropping

The eavesdropping attack is feasible, requiring only an inexpensive tag and radio



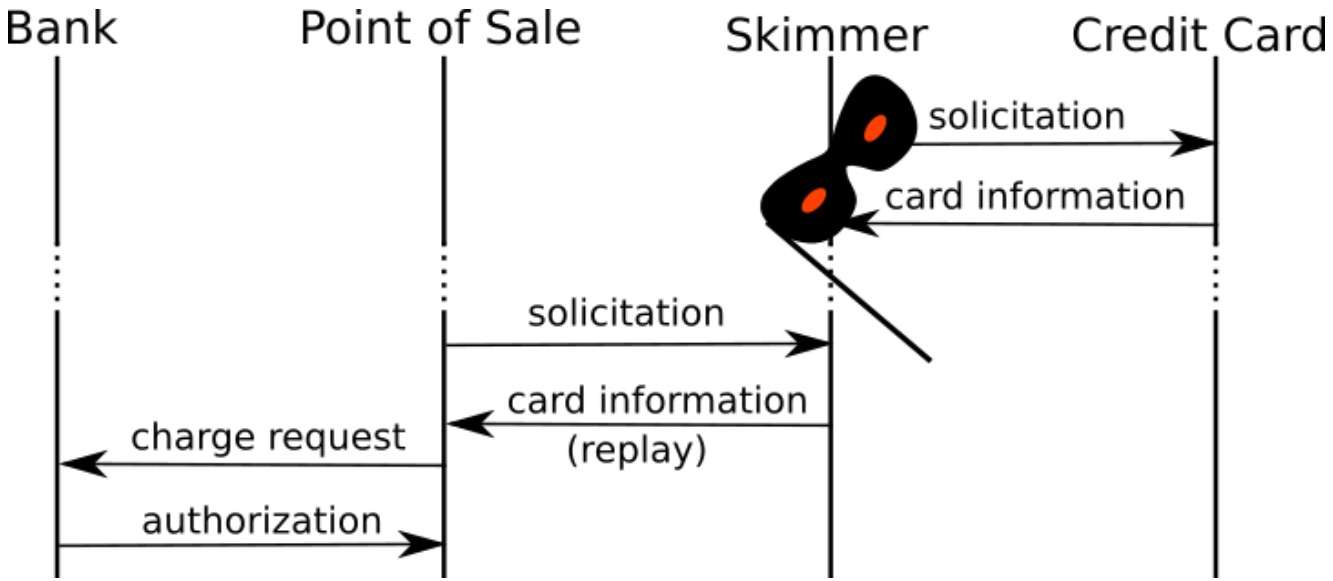
- A small antenna could easily be concealed near a terminal

Skimming & Relay Attacks



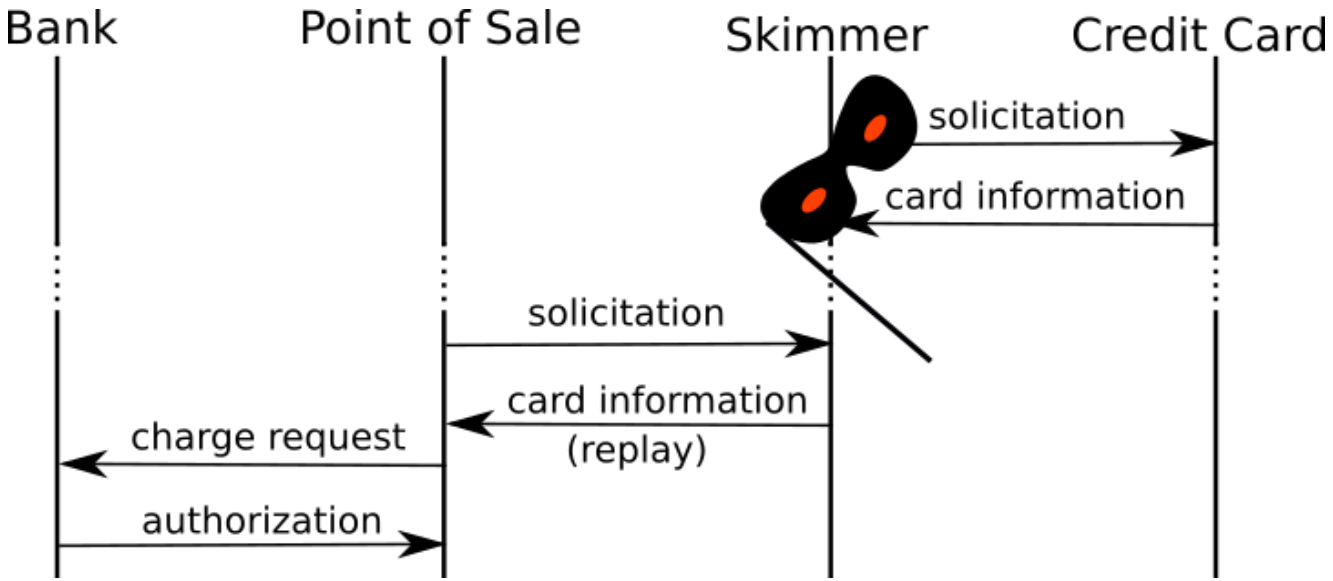
The attacker masquerades as a card reader

Skimming & Relay Attacks



The attacker masquerades as a card reader

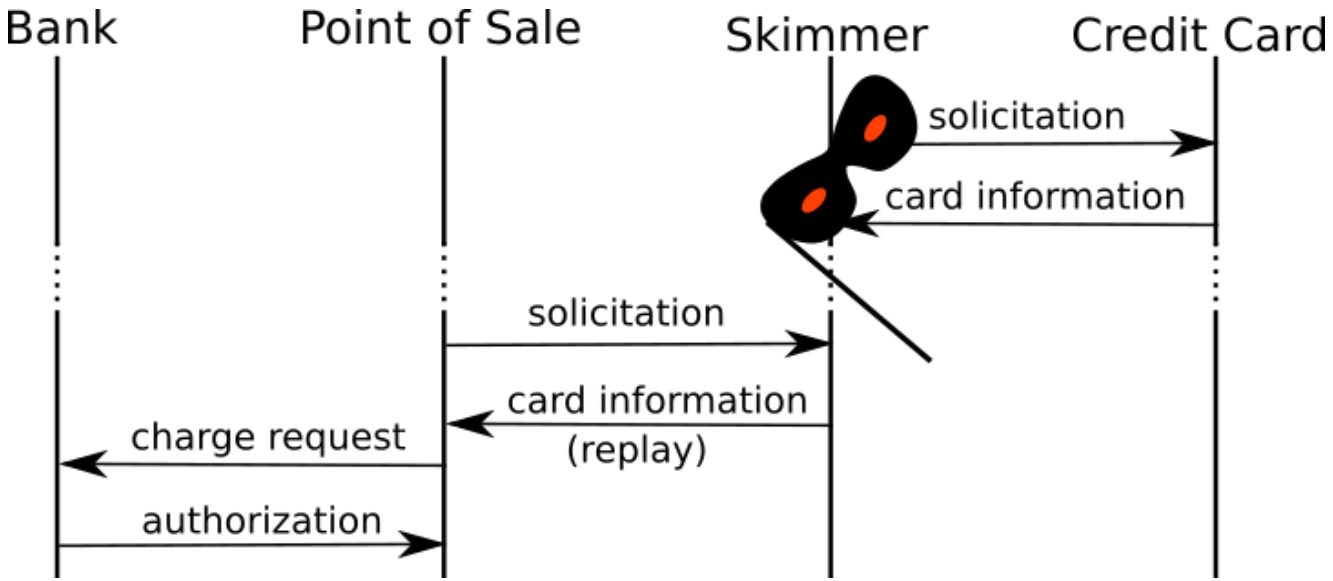
Skimming & Relay Attacks



The attacker masquerades as a card reader

- An unused iCVV can be *skimmed* from the card

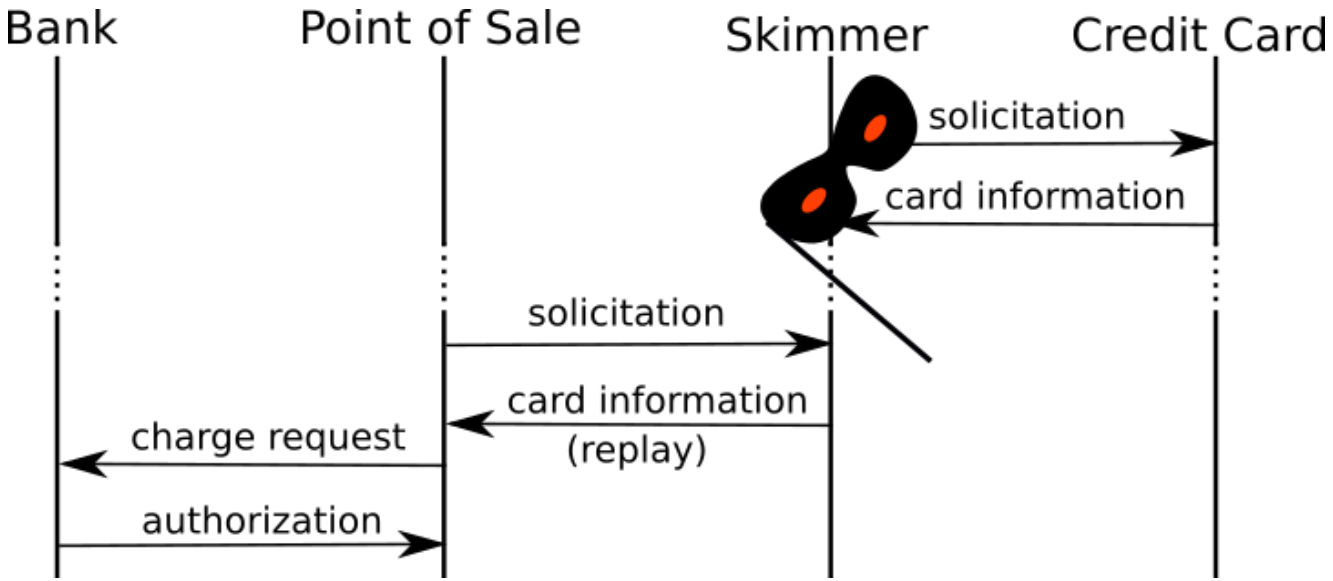
Skimming & Relay Attacks



The attacker masquerades as a card reader

- An unused iCVV can be *skimmed* from the card
- Then, a fraudulent purchase can occur at a real point of sale

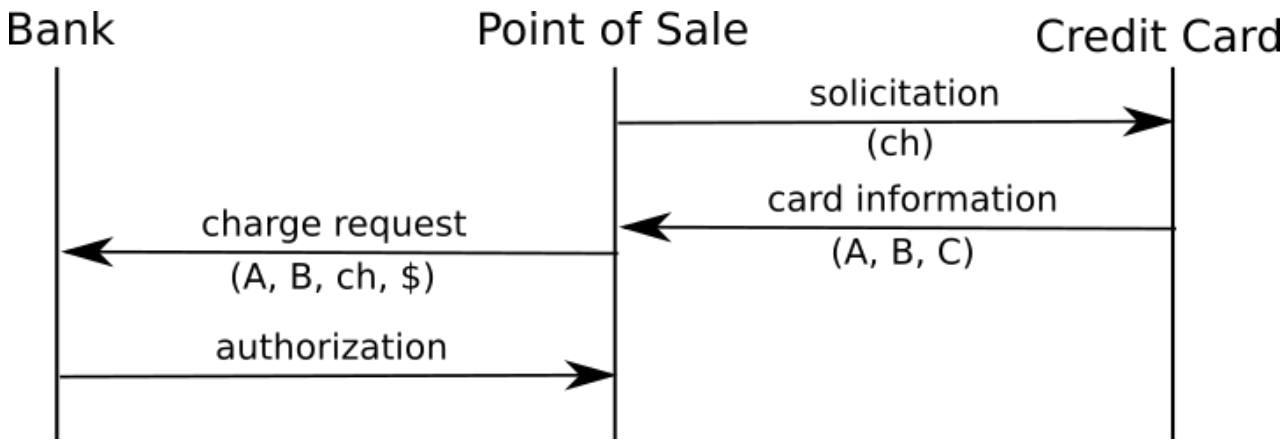
Skimming & Relay Attacks



The attacker masquerades as a card reader

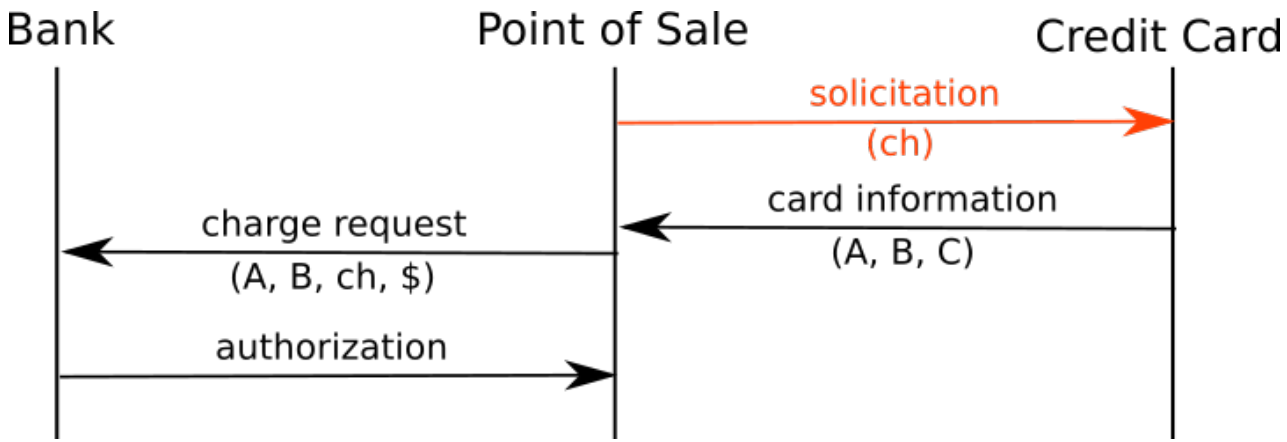
- An unused iCVV can be *skimmed* from the card
- Then, a fraudulent purchase can occur at a real point of sale
- In a relay attack, two devices execute the skimming attack in concert

Proposed Secure Credit Protocol



A credit card protocol restructured

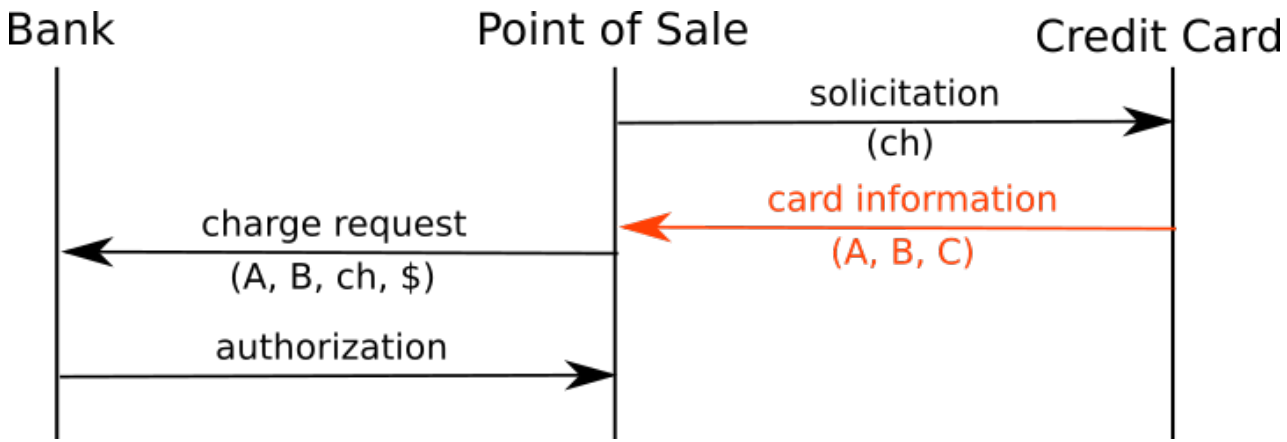
Proposed Secure Credit Protocol



Solicitation

- Point of Sale now sends a challenge

Proposed Secure Credit Protocol



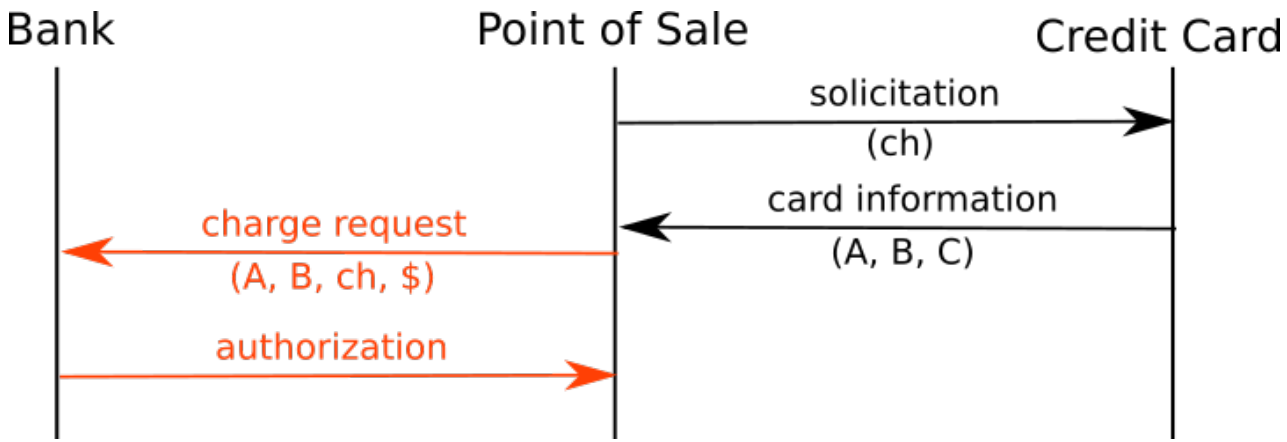
Restructured Card Information

(A) ***UUID***, a static Universally Unique Identifier is used to identify the credit card.

(B) ***H(card info, ch, iCVV)*** is a hash-like function used to authenticate the card's identity.

(C) ***bank name*** is used to route the charge request.

Proposed Secure Credit Protocol



Charge request

- Card information is sent to the indicated bank

Authorization

- Bank verifies transaction

Hash-like function H

Requirements of H

1. **Output appears random**
2. **Output cannot be used to derive components**

So that attackers cannot

- Glean useful information
- Build a new hash output using the components and a new challenge

Hash-like function H

Requirements of H

1. **Output appears random**
2. **Output cannot be used to derive components**

Bank-generated hash	1011 0110
Challenge	1110 1110
Values kept when ch=1	1010 0111

Hash-like function H

Requirements of H

1. **Output appears random**
2. **Output cannot be used to derive components**

Bank-generated hash	1011 0110
Challenge	1110 1110
Values kept when ch=1	1010 0111
iCVV	1010 1010
Result of XOR	0000 1101

NFC and Mass Transit Ticketing

NFC and Mass Transit Ticketing

- Presently, contactless cards widely used for mass transit ticketing

NFC and Mass Transit Ticketing

- Presently, contactless cards widely used for mass transit ticketing
- Three Nokia reseachers investigate NFC phone based ticketing

NFC and Mass Transit Ticketing

- Presently, contactless cards widely used for mass transit ticketing
- Three Nokia reseachers investigate NFC phone based ticketing
- Tamrakar, Ekberg, and Asokan's [2] work is the focus of this section

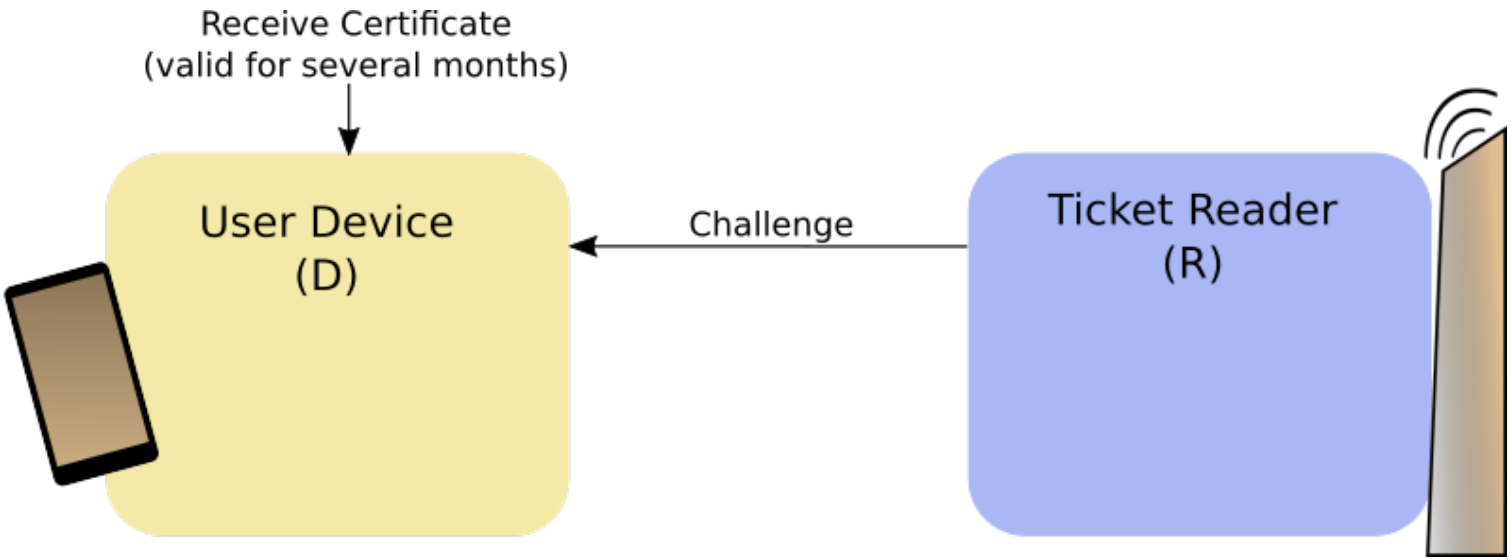
NFC and Mass Transit Ticketing

- Presently, contactless cards widely used for mass transit ticketing
- Three Nokia reseachers investigate NFC phone based ticketing
- Tamrakar, Ekberg, and Asokan's [2] work is the focus of this section
- Their goal is to build a secure ticketing scheme while keeping transaction time below the 300ms industry standard

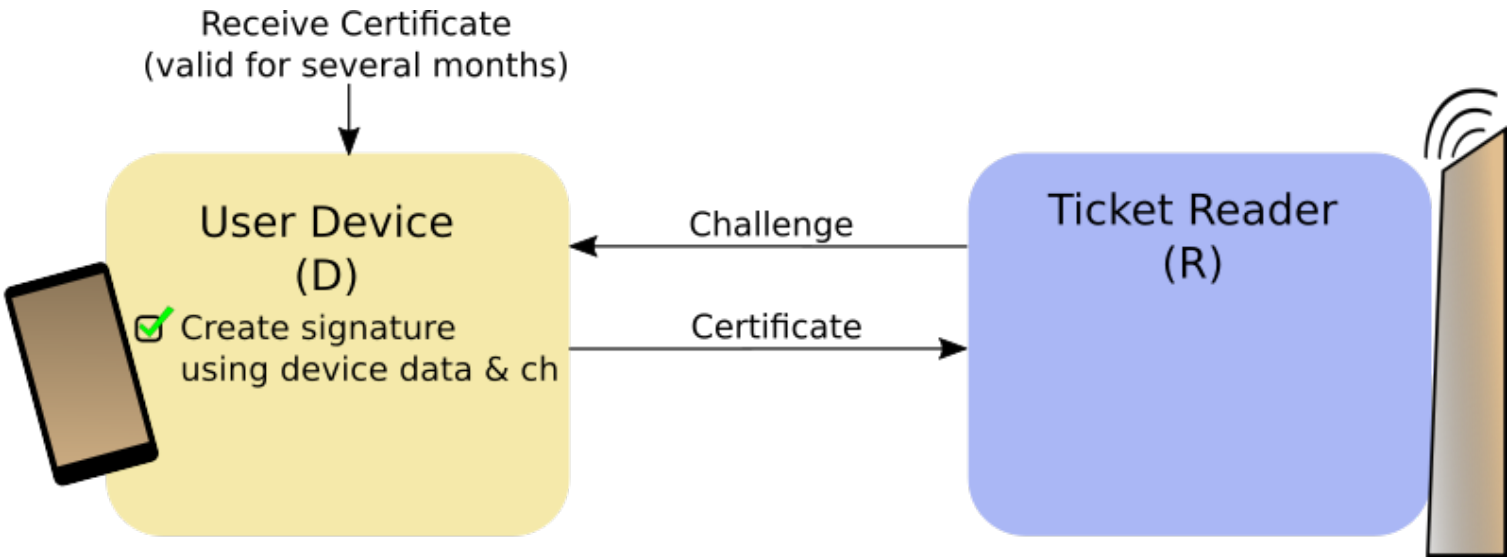
Proposed Ticketing Protocol

Proposed Ticketing Protocol

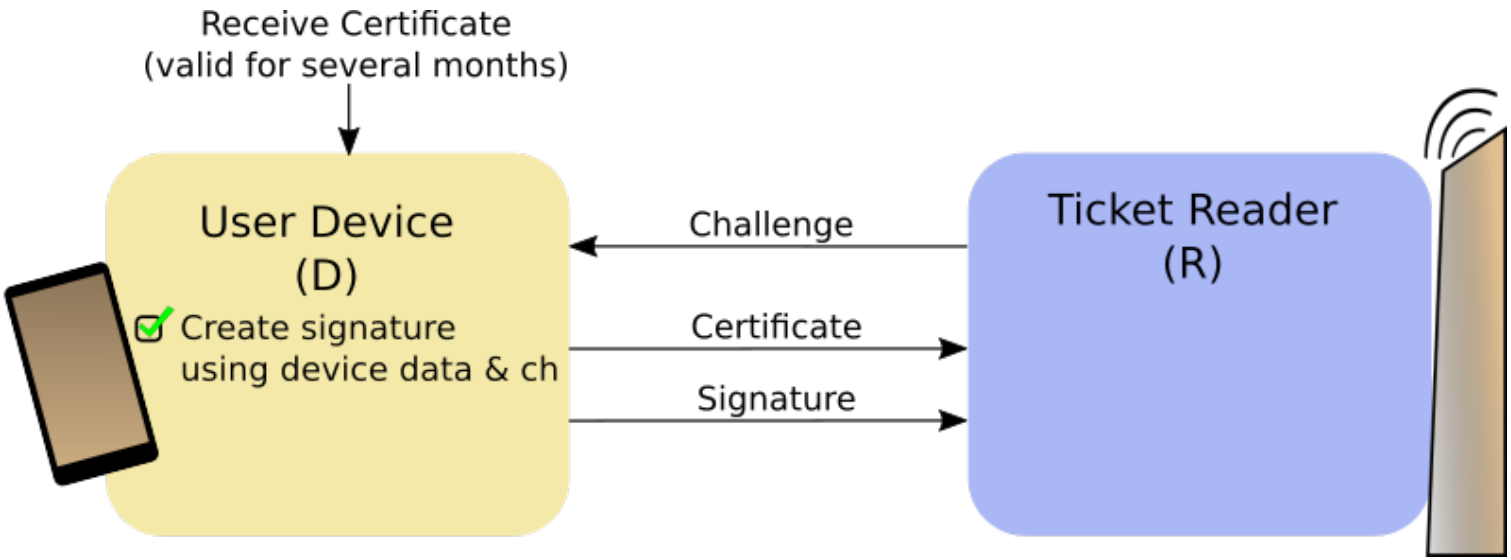
Proposed Ticketing Protocol



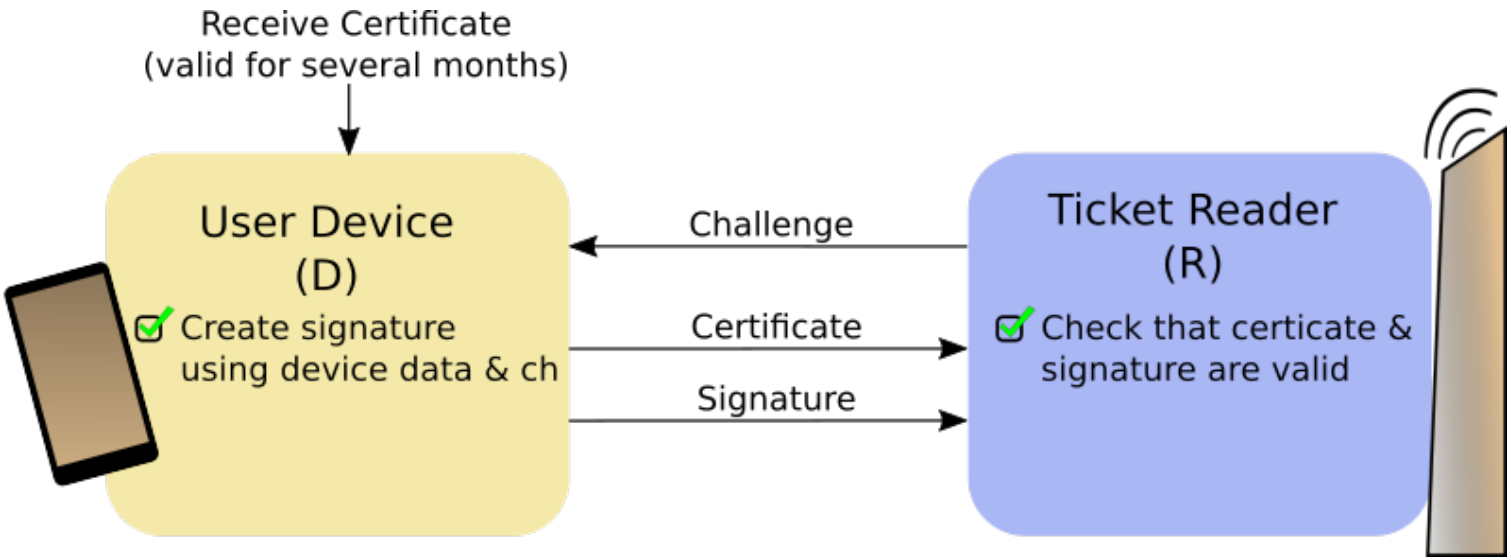
Proposed Ticketing Protocol



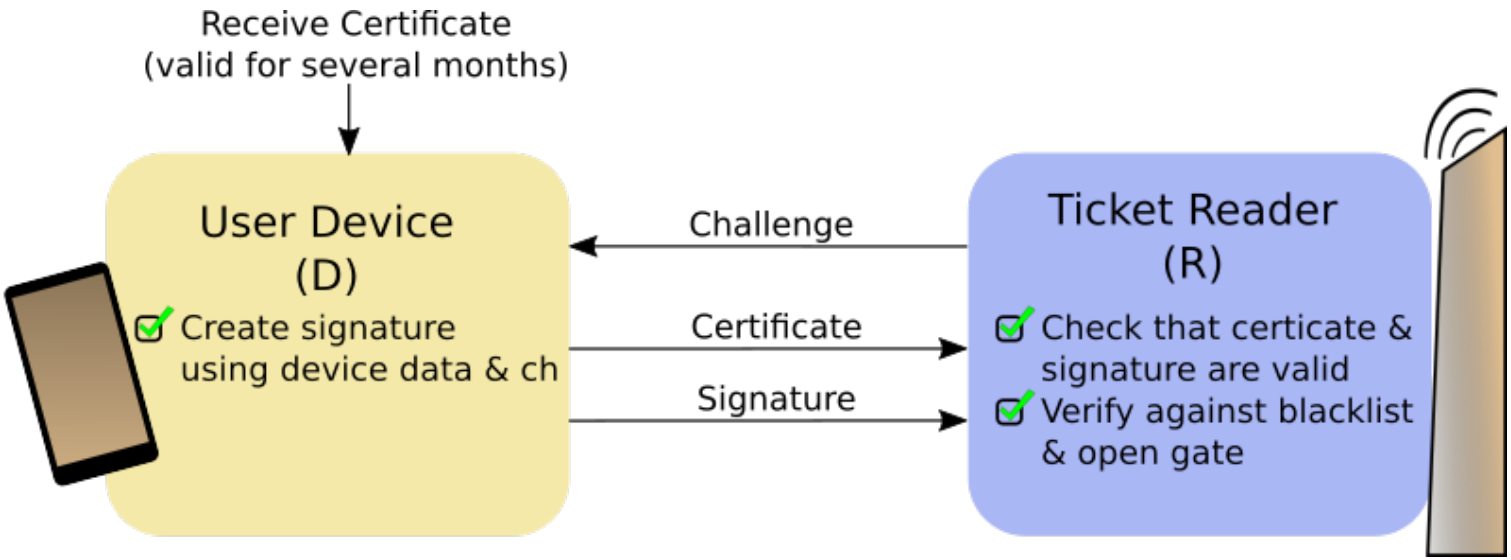
Proposed Ticketing Protocol



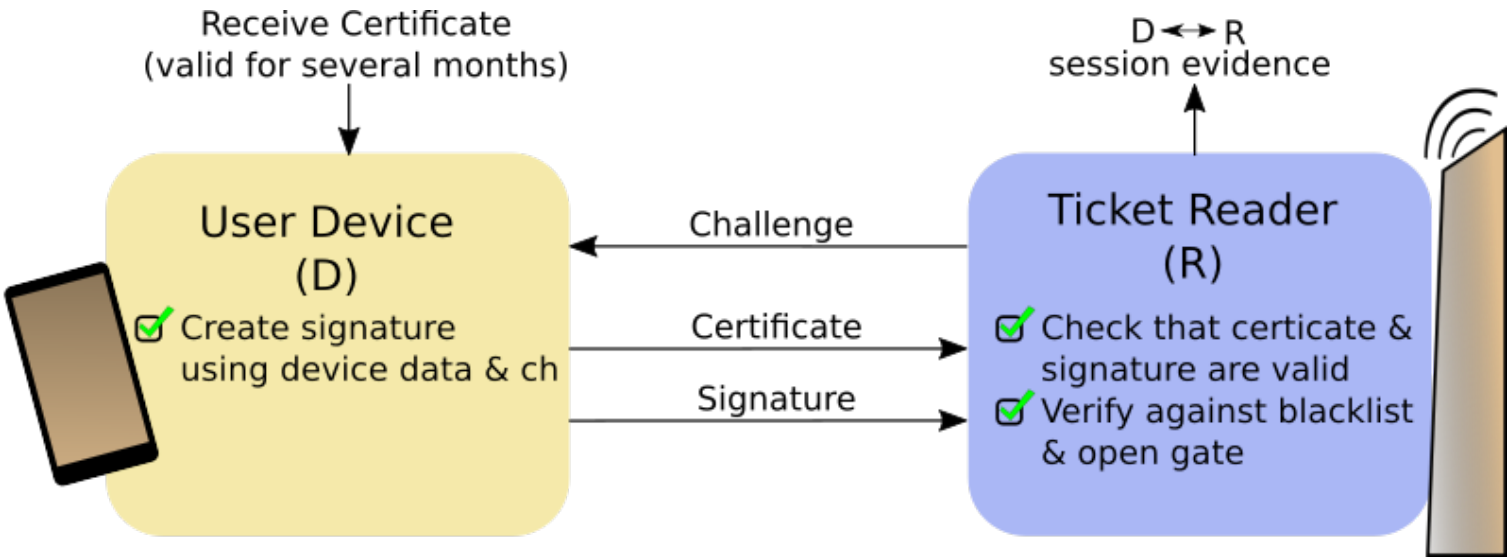
Proposed Ticketing Protocol



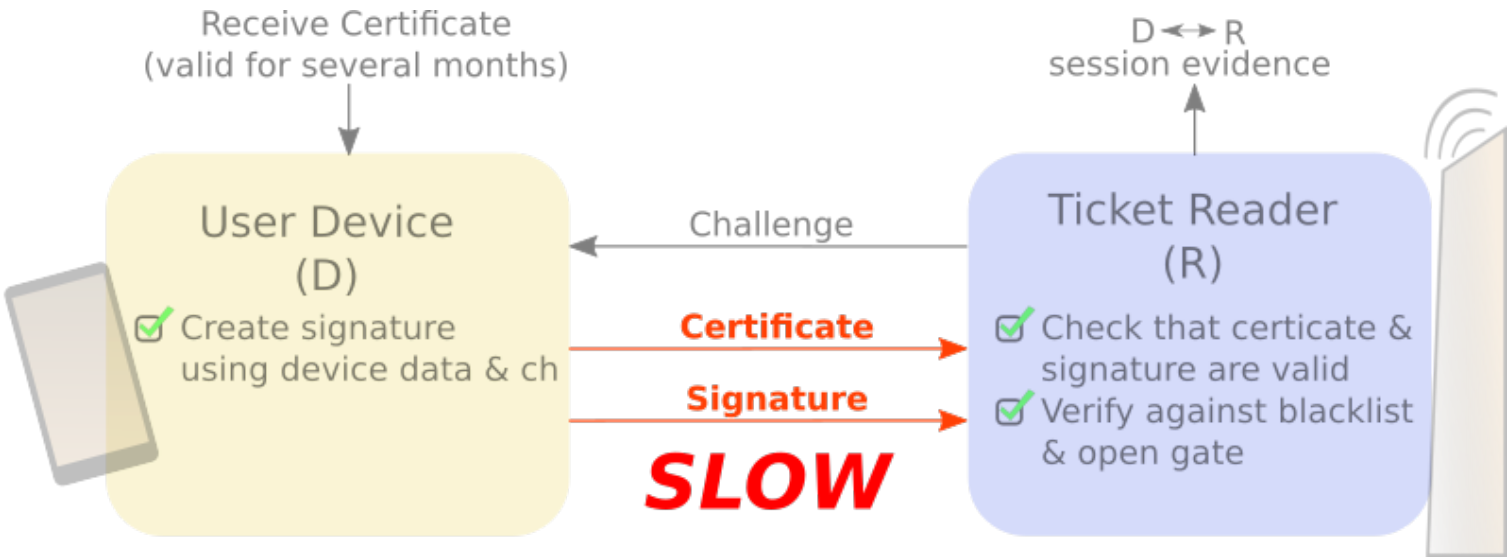
Proposed Ticketing Protocol



Proposed Ticketing Protocol



Proposed Ticketing Protocol



Protocol Variant 1

Use a lighter authentication method

Protocol Variant 1

Use a lighter authentication method

- Switching from a signature to a MAC (*message authentication code*) substantially reduces overhead

Protocol Variant 1

Use a lighter authentication method

- Switching from a signature to a MAC (*message authentication code*) substantially reduces overhead

Use tokens instead of certificates

Protocol Variant 1

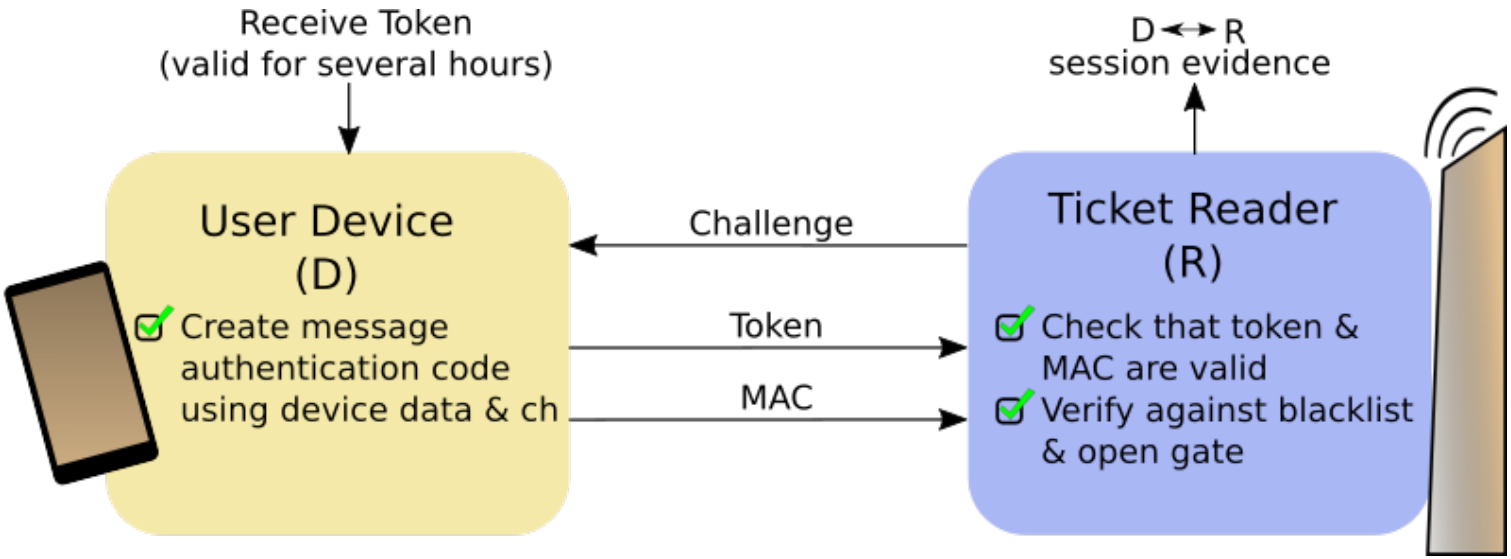
Use a lighter authentication method

- Switching from a signature to a MAC (*message authentication code*) substantially reduces overhead

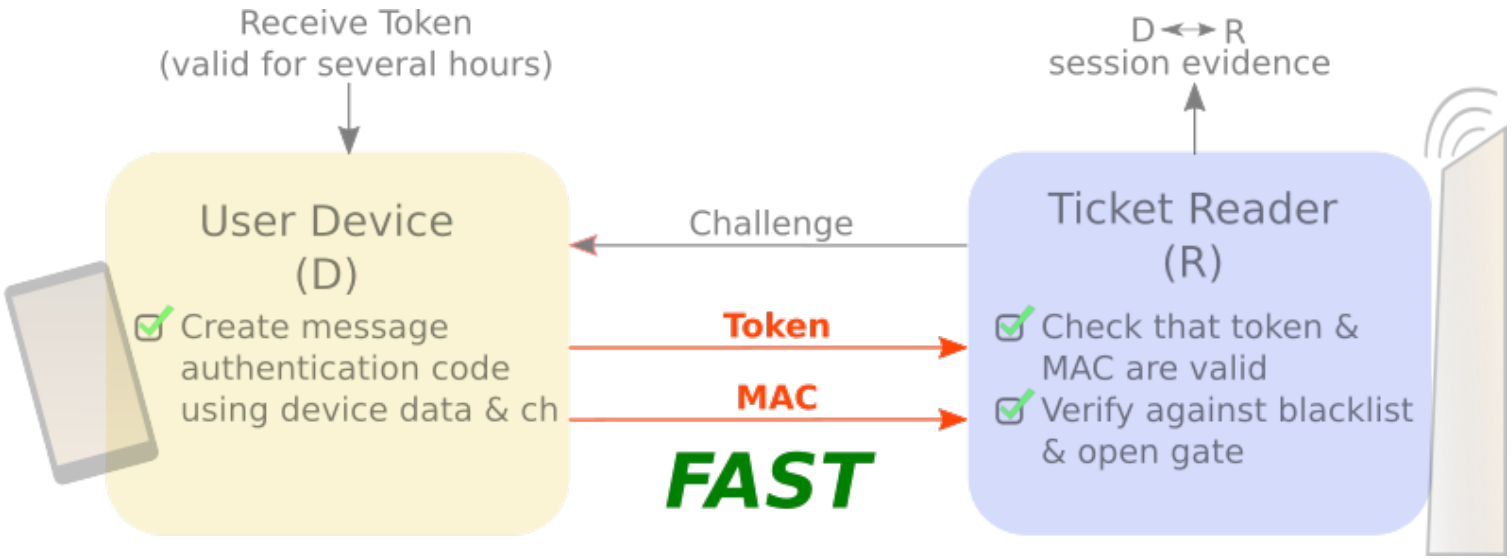
Use tokens instead of certificates

- Send a small token that the reader can validate
- For security, the token should be refreshed often

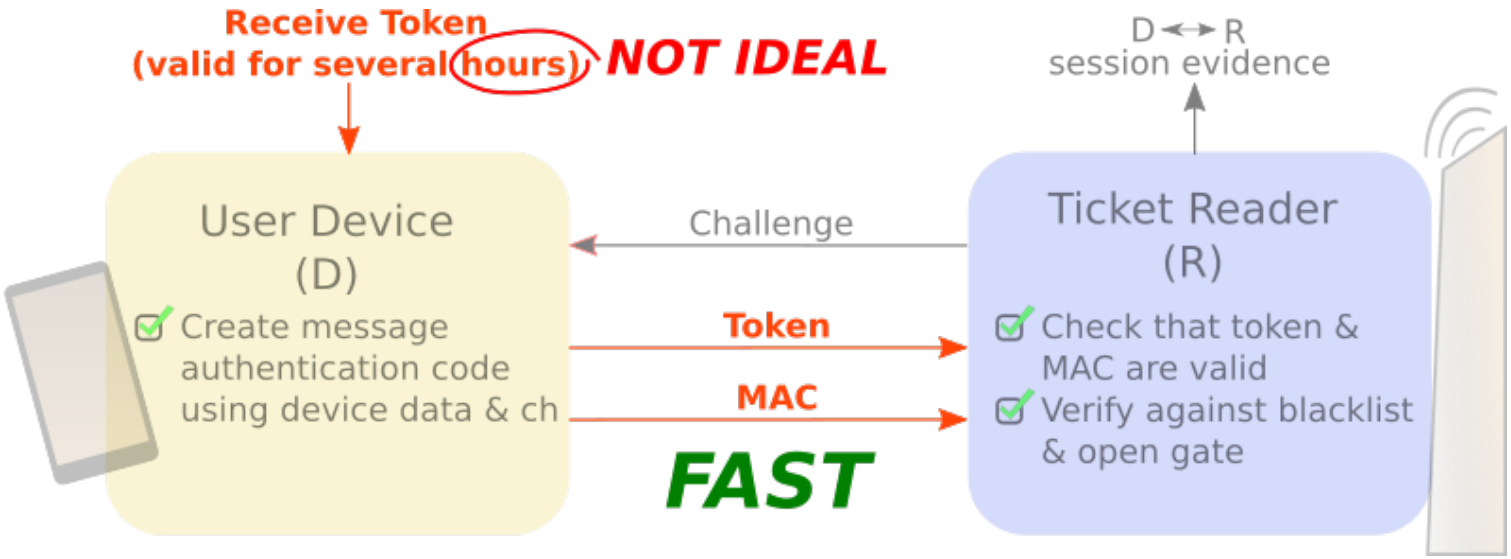
Protocol Variant 1



Protocol Variant 1



Protocol Variant 1



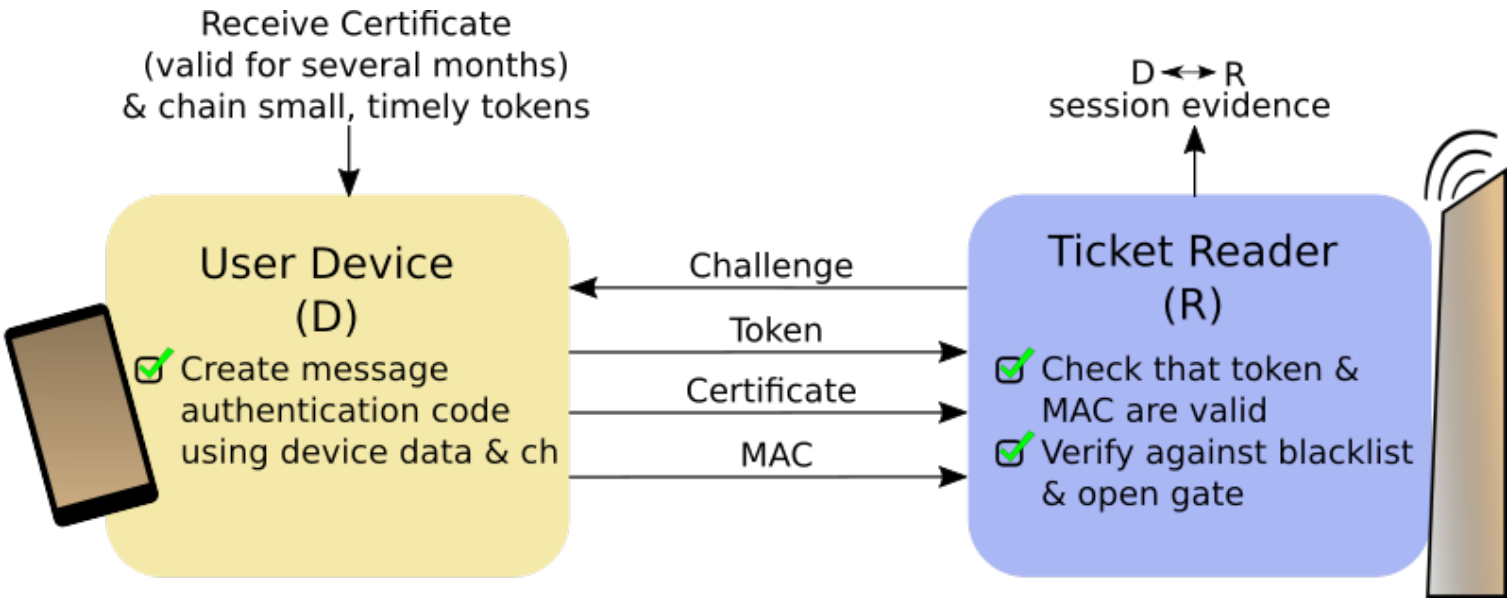
Protocol Variant 2

Use small, timely tokens AND a long-term certificate

Protocol Variant 2

Use small, timely tokens AND a long-term certificate

- This is implemented using a reverse hash chain



Viability of Mobile Ticketing

Viability of Proposed Protocols

Encryption Key Size	Standard	Variant 1	Variant 2
1024 bits	296 ms	164 ms	182 ms
1152 bits	314 ms	172 ms	190 ms
2048 bits	482 ms	228 ms	246 ms

Viability of Mobile Ticketing

Viability of Proposed Protocols

Encryption Key Size	Standard	Variant 1	Variant 2
1024 bits	296 ms	164 ms	182 ms
1152 bits	314 ms	172 ms	190 ms
2048 bits	482 ms	228 ms	246 ms

- NFC transfer speeds were the biggest bottleneck

Viability of Mobile Ticketing

Viability of Proposed Protocols

Encryption Key Size	Standard	Variant 1	Variant 2
1024 bits	296 ms	164 ms	182 ms
1152 bits	314 ms	172 ms	190 ms
2048 bits	482 ms	228 ms	246 ms

- NFC transfer speeds were the biggest bottleneck
- The authors noted that smaller two key sizes have been deprecated in the payment industry

Viability of Mobile Ticketing

Viability of Proposed Protocols

Encryption Key Size	Standard	Variant 1	Variant 2
1024 bits	296 ms	164 ms	182 ms
1152 bits	314 ms	172 ms	190 ms
2048 bits	482 ms	228 ms	246 ms

- NFC transfer speeds were the biggest bottleneck
- The authors noted that smaller two key sizes have been deprecated in the payment industry

Viability of Mobile Ticketing

Viability of Proposed Protocols

Encryption Key Size	Standard	Variant 1	Variant 2
1024 bits	296 ms	164 ms	182 ms
1152 bits	314 ms	172 ms	190 ms
2048 bits	482 ms	228 ms	246 ms

- NFC transfer speeds were the biggest bottleneck
- The authors noted that smaller two key sizes have been deprecated in the payment industry
- The industry recommended transaction time is 300ms. After taking this into account, only two options are viable

Viability of Mobile Ticketing

Viability of Proposed Protocols

Encryption Key Size	Standard	Variant 1	Variant 2
1024 bits	296 ms	164 ms	182 ms
1152 bits	314 ms	172 ms	190 ms
2048 bits	482 ms	228 ms	246 ms

- NFC transfer speeds were the biggest bottleneck
- The authors noted that smaller two key sizes have been deprecated in the payment industry
- The industry recommended transaction time is 300ms. After taking this into account, only two options are viable

Viability of Mobile Ticketing

- Using mobile ticketing offers convince and a richer user interface

Viability of Mobile Ticketing

- Using mobile ticketing offers convince and a richer user interface
- The Nokia researchers grant that relay attacks are possible in all protocols, but that there is a short opportunity windows and low monetary gain

Viability of Mobile Ticketing

- Using mobile ticketing offers convince and a richer user interface
- The Nokia researchers grant that relay attacks are possible in all protocols, but that there is a short opportunity windows and low monetary gain
- The researchers state that these protocols are meets performance and security needs better than the current contactless card system

Viability of Mobile Ticketing

- Using mobile ticketing offers convince and a richer user interface
- The Nokia researchers grant that relay attacks are possible in all protocols, but that there is a short opportunity windows and low monetary gain
- The researchers state that these protocols are meets performance and security needs better than the current contactless card system
- While mobile ticketing is an imperfect, it is valid path forward that offers value

EnGarde: Physical NFC Security

EnGarde: Physical NFC Security

- Commercial payments systems are bringing NFC to phones

EnGarde: Physical NFC Security

- Commercial payments systems are bringing NFC to phones
- As a result, there may be new risks in both payment and non-payment applications of NFC

EnGarde: Physical NFC Security

- Commercial payments systems are bringing NFC to phones
- As a result, there may be new risks in both payment and non-payment applications of NFC
- EnGarde is a semi-permanent phone attachment, designed to act as a hardware-based firewall

EnGarde: Physical NFC Security

- Commercial payments systems are bringing NFC to phones
- As a result, there may be new risks in both payment and non-payment applications of NFC
- EnGarde is a semi-permanent phone attachment, designed to act as a hardware-based firewall
- Gummeson et al's [3] work on the EnGarde prototype is the focus of this section

EnGarde Prototype

EnGarde Prototype

EnGarde Prototype Features

EnGarde Prototype

EnGarde Prototype Features

- Small form factor for semi-permanent mounting to a mobile phone

EnGarde Prototype

EnGarde Prototype Features

- Small form factor for semi-permanent mounting to a mobile phone
- Independent battery, memory, and processor from phone

EnGarde Prototype

EnGarde Prototype Features

- Small form factor for semi-permanent mounting to a mobile phone
- Independent battery, memory, and processor from phone
- Software can be updated to combat current and future threats

EnGarde Expectations

EnGarde should defend against all NFC modes

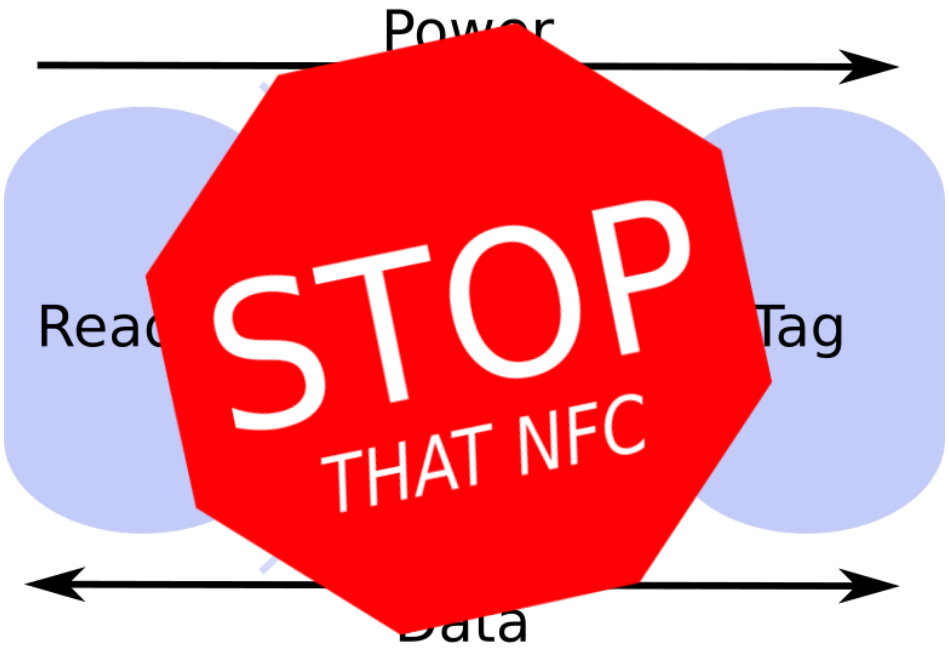
- Malicious tags
- Malicious readers
- Malicious peers
- Malicious software installations

NFC Decoding and Jamming

How does EnGarde detect and stop unwanted transmissions?

NFC Decoding and Jamming

How does EnGarde detect and stop unwanted transmissions?



NFC Decoding

NFC Decoder

- When there is an incoming or outgoing transmission, EnGarde will listen in

NFC Decoding

NFC Decoder

- When there is an incoming or outgoing transmission, EnGarde will listen in
- EnGarde scans transmissions and determines if they are worthy using a set of blocking rules

NFC Decoding

NFC Decoder

- When there is an incoming or outgoing transmission, EnGarde will listen in
- EnGarde scans transmissions and determines if they are worthy using a set of blocking rules
- The blocking rules can be updated for robust handling of current and future attacks

Jamming Communications

Reflective Jamming

- This jamming method is used against low-powered tags

Jamming Communications

Reflective Jamming

- This jamming method is used against low-powered tags
- By broadcasting on the same frequency, EnGarde can block out messages from malicious tags

Jamming Communications

Reflective Jamming

- This jamming method is used against low-powered tags
- By broadcasting on the same frequency, EnGarde can block out messages from malicious tags
- The field the phone is using to activate the tags also powers EnGarde's defense

Jamming Communications

Pulse Jamming

- This jamming method is used against high-powered readers or peers

Jamming Communications

Pulse Jamming

- This jamming method is used against high-powered readers or peers
- Since a reader is sourcing a considerable amount of power, Engarde can only corrupt rather than completely block messages

Jamming Communications

Pulse Jamming

- This jamming method is used against high-powered readers or peers
- Since a reader is sourcing a considerable amount of power, Engarde can only corrupt rather than completely block messages
- The field from the reader sustains EnGarde's defense

Experimental Evaluation of EnGarde

Results

- EnGarde was able to successfully block all malicious test cases using one of the jamming methods

Experimental Evaluation of EnGarde

Results

- EnGarde was able to successfully block all malicious test cases using one of the jamming methods
- Decoding was also successful in decoding a malicious tag to the URL *http://www.malware*

Experimental Evaluation of EnGarde

Results

- EnGarde was able to successfully block all malicious test cases using one of the jamming methods
- Decoding was also successful in decoding a malicious tag to the URL *http://www.malware*
- EnGarde's defense seems strong, but we note that its defense is only as strong as the blocking rules it has

Conclusion

Conclusion

- Now we have a better idea of how NFC works. Is it secure? Is it the future?

Conclusion

- Now we have a better idea of how NFC works. Is it secure? Is it the future?
- Clever solutions can mitigate security concerns

Conclusion

- Now we have a better idea of how NFC works. Is it secure? Is it the future?
- Clever solutions can mitigate security concerns
- NFC data transfer speed appears to be the biggest bottleneck

Conclusion

- Now we have a better idea of how NFC works. Is it secure? Is it the future?
- Clever solutions can mitigate security concerns
- NFC data transfer speed appears to be the biggest bottleneck
- NFC is young and will likely act as platform for future applications

Conclusion

- Now we have a better idea of how NFC works. Is it secure? Is it the future?
- Clever solutions can mitigate security concerns
- NFC data transfer speed appears to be the biggest bottleneck
- NFC is young and will likely act as platform for future applications
- In the end, security relies on vigilance and on understanding risks

Questions

Questions?

Stop by the NFC enabled pop machine near the bookstore for a neat demonstration.

Sources

Primary Research Sources

1. Oliver Jensen, Mohamed Gouda, and Lili Qiu. 2016. A secure credit card protocol over NFC. In Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN '16). ACM, New York, NY, USA, Article 32 , 9 pages.
2. Sandeep Tamrakar, Jan-Erik Ekberg, and N. Asokan. 2011. Identity verification schemes for public transport ticketing with NFC phones. In Proceedings of the sixth ACM workshop on Scalable trusted computing (STC '11). ACM, New York, NY, USA, 37-48.
3. Jeremy J. Gummeson, Bodhi Priyantha, Deepak Ganesan, Derek Thrasher, and Pengyu Zhang. 2013. EnGarde: protecting the mobile phone from malicious NFC interactions. In Proceeding of the 11th annual international conference on Mobile systems, applications, and services (MobiSys '13). ACM, New York, NY, USA, 445-458.

Sources

Additional Sources

- Personal photos
- Wikipedia Articles: Near Field Communication, Radio-frequency identification, Card Security Code, Intermodal Container
- Robert Hardy, Enrico Rukzio, Paul Holleis, and Matthias Wagner. 2010. Mobile interaction with static and dynamic NFC-based displays. In Proceedings of the 12th international conference on Human computer interaction with mobile devices and services (MobileHCI '10). ACM, New York, NY, USA, 123-132.