The Challenge of Secure Mobile Payments

Gauthier Van Damme

Katholieke Universiteit Leuven
ESAT/SCD/IBBT-COSIC

November 2010
Outline

1 Introduction
   - Issues with mobile payments
   - The online/offline dilemma

2 Existing deployments
   - Online Web Based
   - ID + Key Based
   - Mobile Network - based

3 The Way to the Future
   - Secure Element & NFC
   - Secure Payment Systems
Outline

1 Introduction
   - Issues with mobile payments
   - The online/offline dilemma

2 Existing deployments
   - Online Web Based
   - ID + Key Based
   - Mobile Network - based

3 The Way to the Future
   - Secure Element & NFC
   - Secure Payment Systems
Outline

1 Introduction
- Issues with mobile payments
- The online/offline dilemma

2 Existing deployments
- Online Web Based
- ID + Key Based
- Mobile Network - based

3 The Way to the Future
- Secure Element & NFC
- Secure Payment Systems
Outline

1 Introduction
   - Issues with mobile payments
   - The online/offline dilemma

2 Existing deployments
   - Online Web Based
   - ID + Key Based
   - Mobile Network - based

3 The Way to the Future
   - Secure Element & NFC
   - Secure Payment Systems
A difficult set-up

→ Shift of security from user control to system control
→ Users needs to accept this shift
A difficult set-up

→ Shift of security from user control to system control
→ Users needs to accept this shift
A difficult set-up

→ Shift of security from user control to system control
→ Users needs to accept this shift
It’s all about user trust

User trust is everything! Consider:

- System usability
- System reliability
- System security: make the best trade-off for your model
  - Know the technologies available
  - Know the security risks
  - Know the cost
- System failure: be prepared for breaches
  - Communicate openly about the risks
  - Compensate victims of fraud
  - Be aware today of future solutions/patches
It’s all about user trust

User trust is everything! Consider:

- **System usability**
- **System reliability**
- **System security**: make the best trade-off for your model
  - Know the technologies available
  - Know the security risks
  - Know the cost
- **System failure**: be prepared for breaches
  - Communicate openly about the risks
  - Compensate victims of fraud
  - Be aware today of future solutions/patches
It’s all about user trust

User trust is everything! Consider:

- System usability
- System reliability
- System security: make the best trade-off for your model
  - Know the technologies available
  - Know the security risks
  - Know the cost
- System failure: be prepared for breaches
  - Communicate openly about the risks
  - Compensate victims of fraud
  - Be aware today of future solutions/patches
It’s all about user trust

User trust is everything! Consider:

- **System usability**
- **System reliability**
- **System security**: make the best trade-off for your model
  - Know the technologies available
  - Know the security risks
  - Know the cost
- **System failure**: be prepared for breaches
  - Communicate openly about the risks
  - Compensate victims of fraud
  - Be aware today of future solutions/patches
It’s all about user trust

User trust is everything! Consider:

- **System usability**
- **System reliability**
- **System security**: make the best trade-off for your model
  - Know the technologies available
  - Know the security risks
  - Know the cost
- **System failure**: be prepared for breaches
  - Communicate openly about the risks
  - Compensate victims of fraud
  - Be aware today of future solutions/patches
Outline

1 Introduction
   • Issues with mobile payments
   • The online/offline dilemma

2 Existing deployments
   • Online Web Based
   • ID + Key Based
   • Mobile Network - based

3 The Way to the Future
   • Secure Element & NFC
   • Secure Payment Systems
The online/offline dilemma

Most payment systems are currently online:

- Accounts stored in central server
- ‘Value’ transfer safe & easy
- Straightforward user revocation & transaction control
- Easy integration of system updates/patches

But online systems can have different points of weakness:

- System security relies heavily on the authentication mechanisms
- Relies also on the network to be online all the time
- DoS attacks are a permanent thread
The online/offline dilemma

Most payment systems are currently online:

- Accounts stored in central server
- ‘Value’ transfer safe & easy
- Straightforward user revocation & transaction control
- Easy integration of system updates/patches

But online systems can have different points of weakness:

- System security relies heavily on the authentication mechanisms
- Relies also on the network to be online all the time
- DoS attacks are a permanent thread
Outline

1 Introduction
   - Issues with mobile payments
   - The online/offline dilemma

2 Existing deployments
   - Online Web Based
   - ID + Key Based
   - Mobile Network - based

3 The Way to the Future
   - Secure Element & NFC
   - Secure Payment Systems
Web Based Authentication

Classic username/password in a HTTP(S) connection to the server:

Pros:

- Point-to-point client-server encryption
  - No eavesdropping on the communication channel
  - Integrity check on exchanged data

- Easy set-up
Web Based Mobile Payments

Cons:

- It’s a weak security mechanism on classic computers
  - Passwords are not random
  - Passwords have to be typed
  - Passwords are shared over different applications
  - The communication is secure, not the system
  - Small flaws in SSL and its implementations recently appeared

- It’s even worse on mobile phones
  - Phone needs to be online
  - Typing is harder and slower
  - Username/Passwords can be stored on the phone
  - Anti-virus and -malware software in their infancy
Web Based Mobile Payments

Cons:

- It’s a weak security mechanism on classic computers
  - Passwords are not random
  - Passwords have to be typed
  - Passwords are shared over different applications
  - The communication is secure, not the system
  - Small flaws in SSL and its implementations recently appeared

- It’s even worse on mobile phones
  - Phone needs to be online
  - Typing is harder and slower
  - Username/Passwords can be stored on the phone
  - Anti-virus and -malware software in their infancy
Recent Mobile Banking Example

Recently, vulnerabilities have been found on different mobile banking applications:

- **Wells Fargo**: username, password & account data stored
- **Paypal**: server certificate not checked at client side
- **USAA**: website mirror images containing user data stored
- **Other** ...

http://news.cnet.com/8301-27080_3-20021874-245.html

Conclusion: security based only on what user knows is weak.
Recent Mobile Banking Example

Recently, vulnerabilities have been found on different mobile banking applications:

- Wells Fargo: username, password & account data stored
- Paypal: server certificate not checked at client side
- USAA: website mirror images containing user data stored
- Other ...

http://news.cnet.com/8301-27080_3-20021874-245.html

Conclusion: security based only on what user knows is weak.
Outline

1 Introduction
   - Issues with mobile payments
   - The online/offline dilemma

2 Existing deployments
   - Online Web Based
   - ID + Key Based
   - Mobile Network - based

3 The Way to the Future
   - Secure Element & NFC
   - Secure Payment Systems
Mobile payments with digital ID and Key

→ Security based on what you have!

- Need a unique physical object linked to an account: ID
- Its features should be hard to clone: Cryptographic Keys

→ Secure chip used!

- ‘Mobile’ usually refers to contactless cards
- Both online or offline payments possible
- Relatively easy, cheap and fast
- Tamper-resistant and unique
- User less involved in security
Mobile payments with digital ID and Key

→ Security based on what you have!

- Need a unique physical object linked to an account: ID
- Its features should be hard to clone: Cryptographic Keys

→ Secure chip used!

- ‘Mobile’ usually refers to contactless cards
- Both online or offline payments possible
- Relatively easy, cheap and fast
- Tamper-resistant and unique
- User less involved in security
Problems with digital ID and Key

No user interaction possible:
- No direct balance check, history, ...
- No direct user to user transfer possible
- Contactless ‘as is’ poses major security issues

Not all problems solved:
- Chip can be badly designed
- Full end to end security hard to implement
  - MITM attacks
  - Relay attacks
  - Data integrity problems
  - Denial of Service
The Mifare examples

- Mifare Classic
  - Bad cryptographic design
  - Hard coded UID only remaining security ‘feature’
- Mifare Plus
  - Many extra security features
  - Proprietary system: focus on closed-loop systems
- Mifare DESFire
  - Memory card with strong authentication
  - Compatible with the ISO-7816-4 ‘APDU’ standard

→ Hard to obtain global system security
The Mifare examples

- **Mifare Classic**
  - Bad cryptographic design
  - Hard coded UID only remaining security ‘feature’
- **Mifare Plus**
  - Many extra security features
  - Proprietary system: focus on closed-loop systems
- **Mifare DESFire**
  - Memory card with strong authentication
  - Compatible with the ISO-7816-4 ‘APDU’ standard

→ Hard to obtain global system security
Outline

1 Introduction
   - Issues with mobile payments
   - The online/offline dilemma

2 Existing deployments
   - Online Web Based
   - ID + Key Based
   - Mobile Network - based

3 The Way to the Future
   - Secure Element & NFC
   - Secure Payment Systems
Mobile Payments using the Mobile Network

- Based on authentication through the Subscriber Number (IMSI/TMSI)
- Usually payment through SMS or USSD on GSM network
- Widely deployable but potentially cumbersome
- Security based on GSM security
- Relies heavily on the MNOs
  - SMS is not a deterministic system
  - USSD talks to the MNO, not the payment system
  - The MNO does the authentication
  - The MNO implements the end to end encryption
GSM Networks: Authenticity & Integrity attacks

- Impersonate user through SIM cloning
  - Need SIM master key
  - Key used in weak default SIM A3/A8 algorithm to generate session key
  - With physical access to SIM, 150,000 chosen challenges suffice
  - In the air: use fake base station to challenge the SIM
  - A3/A8 proprietary: implementation can be chosen by provider

- Manipulate transactions using a MITM attack
  - Base stations are not authenticated to the SIM: use as MITM
  - Need to find session key used in weak A5/1 algorithm or force use of A5/0 or A5/2
  - Breaking A5/1: through ‘rainbow tables’ calculated in torrent project
    → 64 bit keystream mapped to A5/1 internal state ⇔ key

UMTS/3G Networks: base station authentication and stronger encryption algorithm (A5/3: KASUMI)
Outline

1 Introduction
   - Issues with mobile payments
   - The online/offline dilemma

2 Existing deployments
   - Online Web Based
   - ID + Key Based
   - Mobile Network - based

3 The Way to the Future
   - Secure Element & NFC
   - Secure Payment Systems
Some Considerations

- **Mid-1990s**: idea of SIM as a Secure Element (SE) accessible by external applications
  → The SIM Toolkit was born
- Why yet not widely adopted for payments?
  - SIM & SIM Toolkit development can get very complex
    → Use of Java Cards as a compatible platform
  - MNOs reluctant to see external parties access ‘their’ SIM
    → New SE’s popped up: embedded in phone or inside microSD card
  - Paying through GSM different from cash/card based payments
    → NFC technology was developed

But is the SE/NFC combinations payment security paradise?
And what exactly is a SE/NFC?
Some Considerations

- Mid-1990s: idea of SIM as a Secure Element (SE) accessible by external applications
  → The SIM Toolkit was born
- Why yet not widely adopted for payments?
  ▶ SIM & SIM Toolkit development can get very complex
    → Use of Java Cards as a compatible platform
  ▶ MNOs reluctant to see external parties access ‘their’ SIM
    → New SE’s popped up: embedded in phone or inside microSD card
  ▶ Paying through GSM different from cash/card based payments
    → NFC technology was developed

But is the SE/NFC combinations payment security paradise?
And what exactly is a SE/NFC?
Some Considerations

- Mid-1990s: idea of SIM as a Secure Element (SE) accessible by external applications
  → The SIM Toolkit was born
- Why yet not widely adopted for payments?
  - SIM & SIM Toolkit development can get very complex
    → Use of Java Cards as a compatible platform
  - MNOs reluctant to see external parties access ‘their’ SIM
    → New SE’s popped up: embedded in phone or inside microSD card
  - Paying through GSM different from cash/card based payments
    → NFC technology was developed

But is the SE/NFC combinations payment security paradise?
And what exactly is a SE/NFC?
Some Considerations

- Mid-1990s: idea of SIM as a Secure Element (SE) accessible by external applications
  → The SIM Toolkit was born
- Why yet not widely adopted for payments?
  - SIM & SIM Toolkit development can get very complex
    → Use of Java Cards as a compatible platform
  - MNOs reluctant to see external parties access ‘their’ SIM
    → New SE’s popped up: embedded in phone or inside microSD card
  - Paying through GSM different from cash/card based payments
    → NFC technology was developed

But is the SE/NFC combinations payment security paradise?
And what exactly is a SE/NFC?
Some Considerations

- Mid-1990s: idea of SIM as a Secure Element (SE) accessible by external applications
  → The SIM Toolkit was born
- Why yet not widely adopted for payments?
  ▶ SIM & SIM Toolkit development can get very complex
    → Use of Java Cards as a compatible platform
  ▶ MNOs reluctant to see external parties access ‘their’ SIM
    → New SE’s popped up: embedded in phone or inside microSD card
  ▶ Paying through GSM different from cash/card based payments
    → NFC technology was developed

But is the SE/NFC combinations payment security paradise?
And what exactly is a SE/NFC?
Some Considerations

- Mid-1990s: idea of SIM as a Secure Element (SE) accessible by external applications
  - The SIM Toolkit was born
- Why yet not widely adopted for payments?
  - SIM & SIM Toolkit development can get very complex
    - Use of Java Cards as a compatible platform
  - MNOs reluctant to see external parties access ‘their’ SIM
    - New SE’s popped up: embedded in phone or inside microSD card
  - Paying through GSM different from cash/card based payments
    - NFC technology was developed

But is the SE/NFC combinations payment security paradise?
And what exactly is a SE/NFC?
Some Considerations

- Mid-1990s: idea of SIM as a Secure Element (SE) accessible by external applications
  → The SIM Toolkit was born
- Why yet not widely adopted for payments?
  - SIM & SIM Toolkit development can get very complex
    → Use of Java Cards as a compatible platform
  - MNOs reluctant to see external parties access ‘their’ SIM
    → New SE’s popped up: embedded in phone or inside microSD card
  - Paying through GSM different from cash/card based payments
    → NFC technology was developed

But is the SE/NFC combinations payment security paradise?
And what exactly is a SE/NFC?
Some Considerations

- Mid-1990s: idea of SIM as a Secure Element (SE) accessible by external applications
  → The SIM Toolkit was born
- Why yet not widely adopted for payments?
  ▶ SIM & SIM Toolkit development can get very complex
    → Use of Java Cards as a compatible platform
  ▶ MNOs reluctant to see external parties access ‘their’ SIM
    → New SE’s popped up: embedded in phone or inside microSD card
  ▶ Paying through GSM different from cash/card based payments
    → NFC technology was developed

But is the SE/NFC combinations payment security paradise?
And what exactly is a SE/NFC?
Some Considerations

- Mid-1990s: idea of SIM as a Secure Element (SE) accessible by external applications
  → The SIM Toolkit was born
- Why yet not widely adopted for payments?
  - SIM & SIM Toolkit development can get very complex
    → Use of Java Cards as a compatible platform
  - MNOs reluctant to see external parties access ‘their’ SIM
    → New SE’s popped up: embedded in phone or inside microSD card
  - Paying through GSM different from cash/card based payments
    → NFC technology was developed

But is the SE/NFC combinations payment security paradise?
And what exactly is a SE/NFC?
The SE/NFC architecture

GSM, UMTS, GPS, WiFi, Bluetooth, ...

Secure Element
SIM microSD embedded

NFC

ESAT/SCD-COSIC (KUL) Mobile Payment Security November 2010
A SE at the heart of payment security?

- **NFC:**
  - Short distance communication: creates sense of control
  - No cryptography: no authentication, encryption, distance bounding, etc.

- **Secure Element:**
  - Secure data and key storage
  - Programmable: up to system architect to decide what to use
  - Different cryptographic libraries available

→ **Perfect security? NO!**

- Somehow user & OS always involved
- Advanced attacks possible
- Everything comes at a cost
A SE at the heart of payment security?

- **NFC:**
  - Short distance communication: creates sense of control
  - No cryptography: no authentication, encryption, distance bounding, etc.

- **Secure Element:**
  - Secure data and key storage
  - Programmable: up to system architect to decide what to use
  - Different cryptographic libraries available

→ Perfect security? NO!

- Somehow user & OS always involved
- Advanced attacks possible
- Everything comes at a cost
A SE at the heart of payment security?

- **NFC:**
  - Short distance communication: creates sense of control
  - No cryptography: no authentication, encryption, distance bounding, etc.

- **Secure Element:**
  - Secure data and key storage
  - Programmable: up to system architect to decide what to use
  - Different cryptographic libraries available

→ Perfect security? NO!

- Somehow user & OS always involved
  - Advanced attacks possible
  - Everything comes at a cost
A SE at the heart of payment security?

- **NFC:**
  - Short distance communication: creates sense of control
  - No cryptography: no authentication, encryption, distance bounding, etc.

- **Secure Element:**
  - Secure data and key storage
  - Programmable: up to system architect to decide what to use
  - Different cryptographic libraries available

→ Perfect security? NO!

- Somehow user & OS always involved
- Advanced attacks possible
- Everything comes at a cost
A SE at the heart of payment security?

- NFC:
  - Short distance communication: creates sense of control
  - No cryptography: no authentication, encryption, distance bounding, etc.

- Secure Element:
  - Secure data and key storage
  - Programmable: up to system architect to decide what to use
  - Different cryptographic libraries available

→ Perfect security? NO!
- Somehow user & OS always involved
- Advanced attacks possible
- Everything comes at a cost
Outline

1. Introduction
   - Issues with mobile payments
   - The online/offline dilemma

2. Existing deployments
   - Online Web Based
   - ID + Key Based
   - Mobile Network-based

3. The Way to the Future
   - Secure Element & NFC
   - Secure Payment Systems
It’s all about trade-offs

- Mobile payments imply many design choices: security is only one of them
- Find the trade-off that suits your mobile payment model
- Know the consequences of the choices on security
  → What can an attacker do with what effort?
It’s all about trade-offs

- Mobile payments imply many design choices: security is only one of them
- Find the trade-off that suits your mobile payment model
- Know the consequences of the choices on security → What can an attacker do with what effort?
Questions

?