PICKPOCKETING MWALLETS

A guide to looting mobile financial services

THE GRUGQ

- Info Sec researcher since 1999
- Experience
  - Telcoms Info Sec
  - Banking Info Sec
- Leads to
  - Mobile Financial Security

MOBILE FINANCIAL APPS

MOBILE FINANCE STAKEHOLDERS

MOBILE FINANCE STAKEHOLDERS

- Mobile Service Provider
  - Telco Operators

MOBILE FINANCE STAKEHOLDERS

- Mobile Service Provider
  - Telco Operators
- Financial Services Provider
  - Financial Institutes
    - Banks, etc.
  - Telco Operators

APPLICATIONS

- Mobile Banking
  - Operator provides channel to financial service
- Mobile Wallet
  - Operator provides financial services

MOTIVATORS

- Financial Institutions (FI)
  - Users configure mobile banking once
  - Reduce churn
- Operators
  - Increase value of relationship
  - Reduce churn

SECURITY GOALS

- Authenticate the customer
- Provide end-to-end security
  - Confidentiality
  - Integrity
  - Availability
- “At least as secure as an ATM”

RISKS

RISKS

- Identity
  - Lost / stolen phone
- Financial
  - Fraud
  - Non-repudiation

MORE RISKS

- Communications channel
  - Monitoring / Sniffing
  - Message Injection / Spoofing
  - Duplicates

NOT RISKS (YET?)

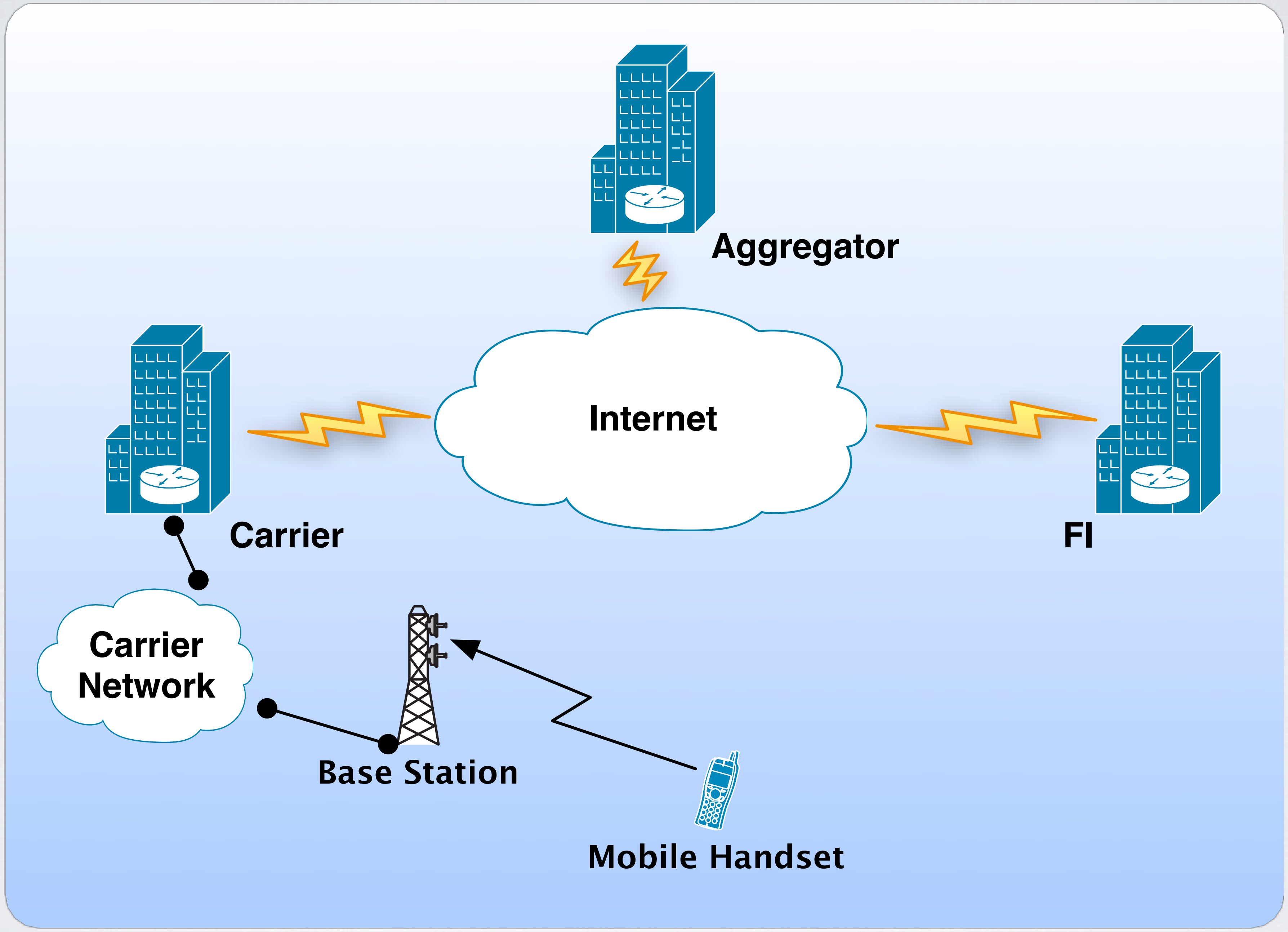
- Mobile Malware
  - Not prevalent
  - Fractured mobile platform landscape

COMPONENTS

MOBILE ELEMENTS

- Handset
- Over The Air (OTA)
- Carrier
- Aggregator
- Financial Institution (FI)

ELEMENTS


Aggregator
Internet
Carrier
FI
Carrier Network
Base Station
Mobile Handset

PLATFORMS

HANDSET PLATFORMS

- Web Application
- Thick Client
- SIM Card Application (STK)

WEB APP

WEB APP

- Easy to deploy

WEB APP

- Easy to deploy
- Easy to develop

WEB APP

- Easy to deploy
- Easy to develop
- Cross platform support

WEB APP

- Easy to deploy
- Easy to develop
- Cross platform support
- Limited control over look and feel

WEB APP

- Easy to deploy
- Easy to develop
- Cross platform support
- Limited control over look and feel

- Web app security
  - SQL injection, XSS

WEB APP

- Easy to deploy
- Easy to develop
- Cross platform support
- Limited control over look and feel

- Web app security
  - SQL injection, XSS
- Slow data link

WEB APP

- Easy to deploy
- Easy to develop
- Cross platform support
- Limited control over look and feel

- Web app security
  - SQL injection, XSS
- Slow data link
- Expensive data plans

WEB APP

- Easy to deploy
- Easy to develop
- Cross platform support
- Limited control over look and feel

- Web app security
  - SQL injection, XSS
- Slow data link
- Expensive data plans
- Subset of phones support browsers

THICK CLIENT

THICK CLIENT

- Complete control over look and feel

THICK CLIENT

- Complete control over look and feel
- Powerful operating environment

THICK CLIENT

- Complete control over look and feel
- Powerful operating environment
- Easy to develop*

THICK CLIENT

- Complete control over look and feel
- Powerful operating environment
- Easy to develop*

- Fractured handset platform landscape

THICK CLIENT

- Complete control over look and feel
- Powerful operating environment
- Easy to develop*

- Fractured handset platform landscape
- Vulnerable to local attacks

THICK CLIENT

- Complete control over look and feel
- Powerful operating environment
- Easy to develop*

- Fractured handset platform landscape
- Vulnerable to local attacks
- Hard to secure
    - Phone developers are not very security aware

SIM APPLICATION

SIM APPLICATION

- More secure (potentially)

SIM APPLICATION

- More secure (potentially)
- Works on all SIM cards

SIM APPLICATION

- More secure (potentially)
- Works on all SIM cards
- Mature development environment

SIM APPLICATION

- More secure (potentially)
- Works on all SIM cards
- Mature development environment
- Deployable OTA

SIM APPLICATION

- More secure (potentially)
- Works on all SIM cards
- Mature development environment
- Deployable OTA
- Secure against malicious phone

SIM APPLICATION

- More secure (potentially)
- Works on all SIM cards
- Mature development environment
- Deployable OTA
- Secure against malicious phone

- Cumbersome interface

SIM APPLICATION

- More secure (potentially)
- Works on all SIM cards
- Mature development environment
- Deployable OTA
- Secure against malicious phone

- Cumbersome interface
- Looks terrible
  - No multimedia

SIM APPLICATION

- More secure (potentially)
- Works on all SIM cards
- Mature development environment
- Deployable OTA
- Secure against malicious phone

- Cumbersome interface
- Looks terrible
  - No multimedia
- Restricted operating environment
  - Low power
  - Low memory

MBANKING ARCHITECTURE

- SMS input
  - Operator
- HTTP(S) input
  - Aggregator
- XML input
  - Financial Institution

MWALLET ARCHITECTURE

- SMS input
  - Operator
- HTTP(S) input
  - Operator - application
- Database manipulation

BACKEND PLATFORMS

- Problems
  - Lack of verifiable audit trail
- Single entry book keeping

CONCERNS

HANDSET CONCERNS

- Identity
    - Lost / Stolen
- Monitoring / Spoofing
- Malicious (e.g. hackers)
- Infected (not yet…)

OTA CONCERNS

- Monitoring
  - GSM encryption is cracked
  - GSM monitoring equipment < €1000

OPERATOR CONCERNS

- Monitoring
  - SMS processing is unencrypted
- Injection
  - Spoofing SMS from SMSC is trivial

OPERATOR CONCERNS, CONT.

OPERATOR CONCERNS, CONT.

- Mobile Banking is Value Added Service (VAS)
  - Ringtones, wallpaper, $10 tetris clones, all your financial data

OPERATOR CONCERNS, CONT.

- Mobile Banking is Value Added Service (VAS)
  - Ringtones, wallpaper, $10 tetris clones, all your financial data
- Security awareness is limited
  - Toll fraud: will this result in revenue leakage?

OPERATOR CONCERNS

- Poor understanding of financial risk management

AGGREGATOR

- Monitoring
  - Malicious employees
  - Other customers
- Injection
  - See above.

FINANCIAL INSTITUTIONS

- Poor understanding of Operator concerns

RECOMMENDATIONS

RECOMMENDATIONS

- Identify customers via a unique mFin PIN + phone
- Transmit the PIN hashed with the message data
- Add a unique message ID (timestamp) per customer per request

- Require customer notification for dangerous operations, e.g. transfers
- Signup process should include in-branch application
- Require secure audit trails for all transactions

FINANCIAL REGULATIONS

- Require the Carrier to follow financial regulations regarding access and control over the messages
- Require the Aggregator to follow financial regulations regarding access and control over the messages

- Use an STK application on the handset
  - Require code review before it goes live
- Require security reviews over major components of the environment
  - Mobile app
  - Carrier environment
  - Aggregator environment

- Develop a clear customer service management plan for lost / stolen handsets
  - Work with the carrier
  - Ensure it doesn’t automatically cancel CC/ATM

ENCRYPTION KEYS

- Manage the encryption keys/certificates used by the application
  - Work with the Carrier on SIM keys
  - Work with the Aggregator

CONCLUSION

- mFin Apps present unique challenges
- Trust relationships with third parties
- Difficult application environments
- No existing "best practices"
- Vendors have immature products