Effects of Mobile Payment Systems on Privacy, Identity, and Security

{ Aayush Upadhyay and Naicheng Wangyu
CS 457/557: Sensitive Info in a Wired World
November 14, 2013

Overview

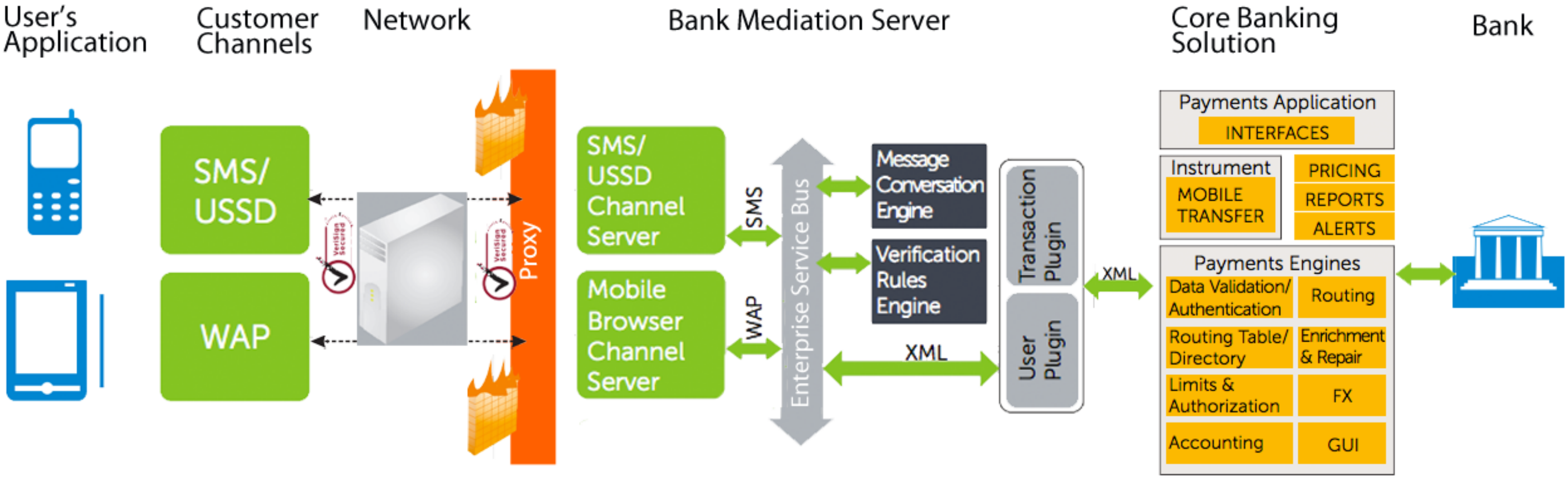
1. What are mobile payment/banking systems?
2. Technological structure

   How does it work? How should it work?
3. Security vulnerabilities and responses
4. Impact on privacy, identity, and security
5. Solutions under ideal conditions

What is a M-Payment system?

- A payment system (branched vs. branchless) in which agents are enabled to complete financial transactions
- Specifically, we focus on M-Payment systems in the developing world where these are common characteristics:
  - Lack of physical banks
  - Lack of capital
  - Low value transactions

Mobile Banking Architecture



-Discussion-

- At which layer do you need to implement security in mobile banking?

Why are M-Payment systems relevant?

A study of the significance of Kenya's MPESA payment system

- 2.6 billion in the developing world are w/o a bank account
- Branched banking infrastructure is not applicable for large populations with small deposit/withdrawal amounts
- 3/4ths of households in Kenya use M-PESA to save
  - ~15M active users as of March 2012
- Accurate identification is lacking because customers often lack proper identification

Register FREE at any Authorised M-PESA Agent*
M-PESA
Send pesa by phone
M-PESA is the new, easy and affordable way to send money home.
* Please see following advertisement for a list of Authorised M-PESA Agents.

Why are M-Payment systems relevant?

Three case studies that demonstrate m-payment presence internationally

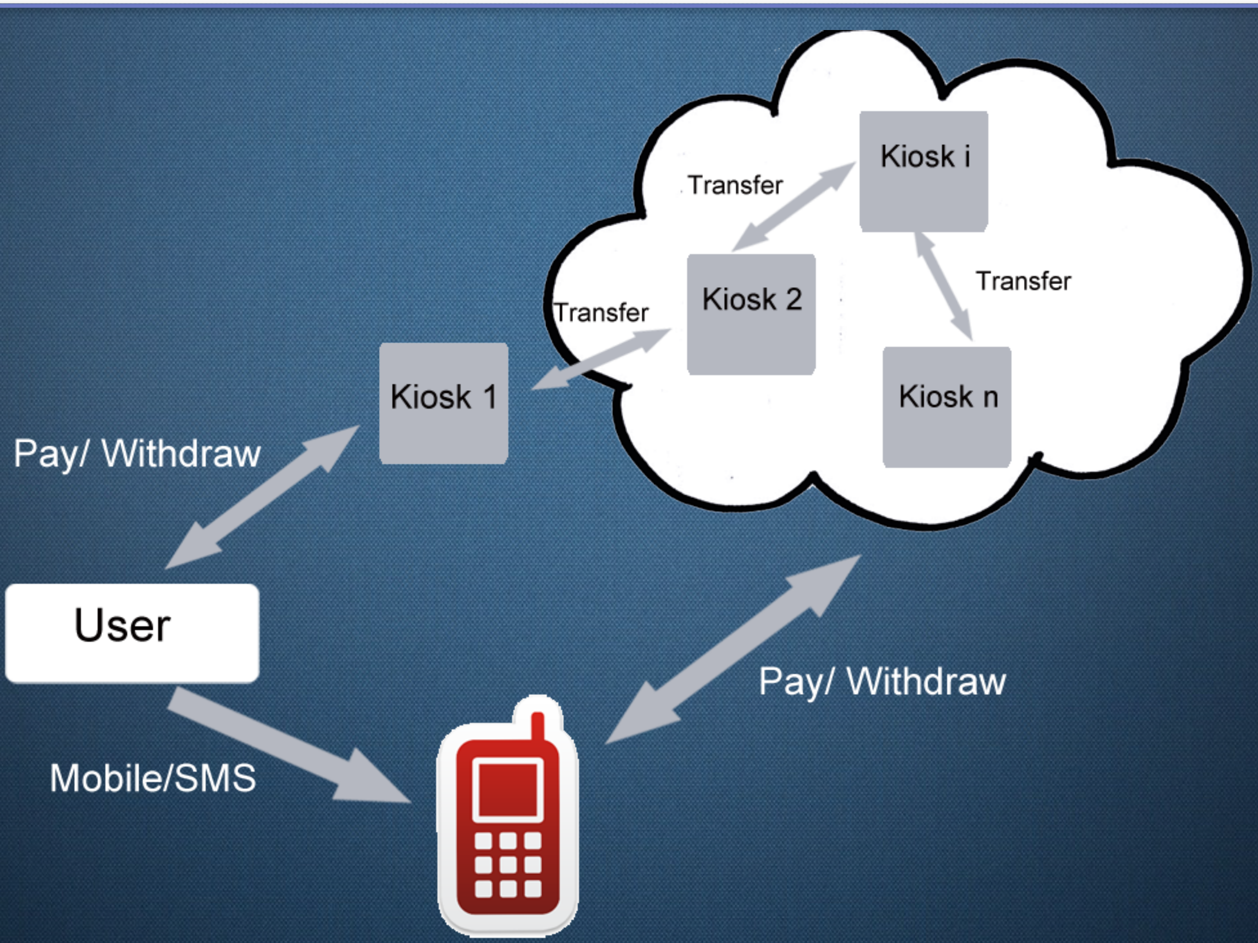
- Uganda (MTN)
  - "The next Kenya", 9M users; 25M transactions/ month
  - Not heavily regulated in terms of identification
- Philippines (GCASH)
  - Allows for bank transactions from outside of Philippines, transaction limits ($895), tiered customer due diligence
  - 80% (75M) of population have mobile phones
  - 20M of them do not have a bank account
- Afghanistan (M-Paisa)
  - Security concerns are high due to fear of terrorists
  - ~97% of Afghanis without access to banking infrastructure

Why are M-Payment systems relevant?

A study of the goals and concerns from a global perspective

- Development vs. Security
  - Ex: Maximizing financial inclusion vs. needing to have formal forms of identification (often not available in developing countries)
- USAID, US Treasury
  - Seeking a balance between maximizing socioeconomic development while minimizing money-laundering and terrorist financing risks
- If this works, why not simply use this over a traditional banking system?

MPESA's technical architecture



What are some of the vulnerabilities?

A list of already-exploited aspects of early stage mobile technology

- Outdated Infrastructure: Newer technologies can attack vulnerabilities of existing cryptography
- Replay: Interception of SMS
- Spoofing: Cloning of SIM cards
- Denial of Service: Jamming GSM frequencies
- Man in the Middle: Listen to transmitted traffic

What are some of the vulnerabilities?

Outdated infrastructure: weak encryption protocols

- Newer technologies can attack vulnerabilities of existing cryptography.
- Traffic between mobile equipment and base station encrypted using A5 ciphers. A5/1 used in Europe/NA, A5/2 is weaker and used in more of the developing world.
- Wagner and Goldberg have shown serious flaws in the entire family of ciphers, allowing real time traffic interception.
- COMP128 is another cipher that has flaws that enable SIM cloning.

What are some of the vulnerabilities?

Spoofing: SIM Cloning

- SIM cards are copied by placing a device between the SIM and handset, operating until K_i is extracted
- Even if extra authentication such as a PIN is required, doesn't mean much if traffic can be intercepted/decoded
- Although updated algorithms have been circulated to GSM providers, it is unclear whether these updated versions are currently in use
- This is particularly true in regimes which may wish a blanket regulation to prevent strong encryption.
  - India's IT Act of 2000

What are some of the vulnerabilities?

Denial of Service: Jamming GSM Frequencies

- Approach:
  - Build a USRP with a valid MNC/MCC
  - Boost signal to convince local devices that USRP is valid operator
  - Once device switches from valid MNO to the USRP, drop packets
- Can also jam the network with false control requests, such as causing the phone to deactivate itself
- Cost effective. USRP can be set up for under $100 to jam GSM frequencies

What are some of the vulnerabilities?

Man in the middle

- Universal Software Radio Peripheral (USRP) can be configured to spoof a carrier using high-power transmitters to capture genuine traffic
- Particularly effective in rural/developing areas that have sparse coverage
- USRP can capture traffic, alter it, and send it to the base station as if it came from the phone
- Leads to identity theft/illegal access, and can also make it easier for replay or spoofing attacks

-Discussion-

- What are some of the real-world consequences if such vulnerabilities are exploited?

Example: GCASH was vulnerable to attack

- Using any phone with a field testing mode, e.g. Nokia S60, one can ascertain the level of encryption used for SMS
- However, using a Universal Software Radio Peripheral, the handset can be negotiated down to A5/0, not knowing that connection is unencrypted
- User is then easily fooled into providing his PIN via SMS
- An attacker can rig a handset with the legitimate user's International Mobile Subscriber Identity (IMSI) and send a transaction using the captured IMSI and PIN of an arbitrary amount to an arbitrary number

The potential effect of such vulnerabilities

Impacts range across privacy, security and identity

- Privacy: Maintenance of personal financial records
- Security: 2-fold: Personal and Systemic
  - Any victims of theft or fraud in the context of these systems would have little recourse to legal assistance.
  - Different forms of security attacks noted previously
- Identity: SIM copying and spoofing

What are some of practical solutions?

A list of attempts in addressing the security concerns

- Short Term:
  - Have more employees reviewing transactions
  - Review access points in person to ensure legitimacy

- Long Term:
  - Use AES/3DES, up-to-date crypto
  - Improve wireless coverage, continue to build infrastructure
  - Use statistical learning for scalable fraud detection

Concluding thoughts

- M-Payment systems provides banking services to large populations that don't have access to traditional services
- Branchless banking improves access but the lack of built-in security and authentication leads to several privacy, security and identity concerns
- In the future, better technology and improved infrastructure can alleviate these problems and continue to revolutionize the lives of many