A Preliminary M-Payment Model for M-Commerce in Kenya

Researchers: Ananda Fanon & Ismail Ateya, Dsc.

Important Terms

- E-Commerce – This is the purchasing and selling of goods and services over computer networks such as the internet. If payment for the good or service is handled over the network then it is referred to as an E-Transaction.
- M-Commerce – This is the purchasing and selling of goods, services and information through a mobile device such as a phone or PDA over a mobile network. If the payment for the transaction is handled electronically through the device, then it is referred to as an M-Payment.

Mobile usage in Kenya

- Mobile usage is on the increase because there are far less socio-economic barriers to acquiring a mobile handset.
- The table below presents the current mobile subscription statistics. The survey was conducted by the Communications Commission of Kenya and the results released in March 2008.

Year	1999	2000	2001	2002	2003	2004	2005	2006	2007	March 2008
Number of subscribers	15,000	114,000	585,131	1,325,222	1,590,785	2,546,157	5,263,676	7,340,317	11,440,077	11,986,007
Mobile penetration (%)	0.053	0.38	1.90	4.20	4.95	7.77	15.74	21.62	33.65	35.25

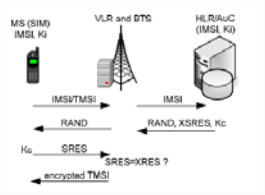
M-Commerce Opportunity

- The significant growth in mobile subscription presents an opportunity to further E-Commerce initiatives through mobile devices.
- Applications of M-commerce
  - **Entertainment** – book theatre tickets, book restaurants, place bets via WAP protocol.
  - **Shopping** – complete POS purchases in a supermarket.
  - **Money** – remote management of bank account details.
  - **Business Applications** – wireless access to enterprise systems.

GSM Security

- **GSM** (**Global System for Mobile communications**: originally from ***Groupe Spécial Mobile***) is the most popular standard for mobile phones.
- **GSM** is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity.
- GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800 MHz bands while others operate between 850 MHz or 1900 MHz.

Identification and authentication on GSM



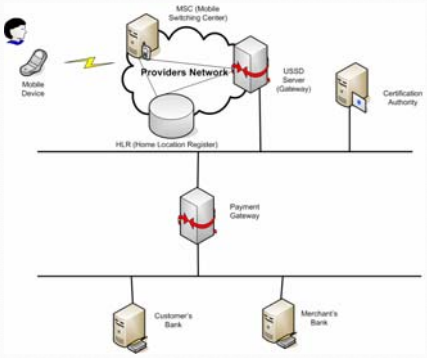
Problems with GSM Security

1. Most commonly used encryption algorithm COMP128, was broken by Wagner and Goldberg (Wagner, 1998) in less than a day.
2. Wagner and Goldberg further proved that it was possible to obtain the Ki value, therefore making it possible to clone a SIM card.
3. The A5 algorithm which is used to encrypt communications has 3 flavors (A5/1, A5/2, and A5/0).
   - A5/2 and A5/1 has been cracked by Wagner and Goldberg (Wagner, 1998)
   - These observations prove that eavesdropping during a communication session is possible.
4. Denial of service attacks is possible in GSM networks - the intruder modifies the RAND value that is sent to the MS by the AUC

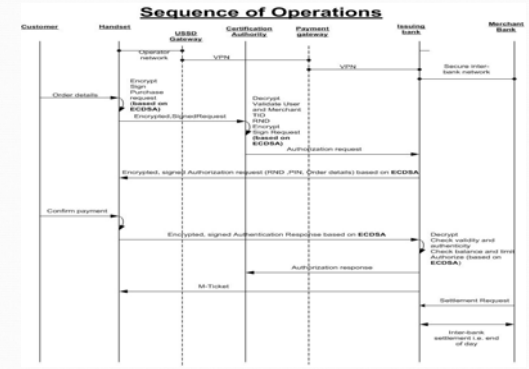
Observation

- You cannot rely only on GSM security for M-Transactions.
- Security issues that need to be addressed are;
  - Confidentiality
  - Integrity
  - Authentication
  - Non-repudiation

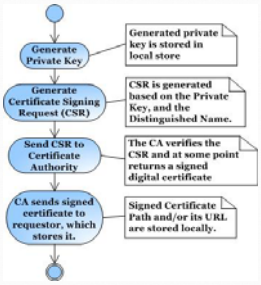
The Research Solution



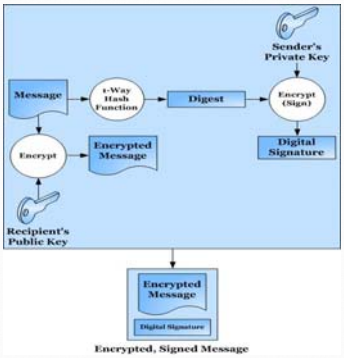
Research Solution Continued



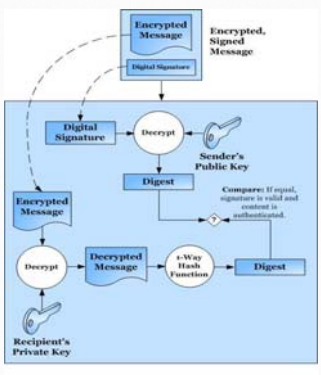
Registration for the service



Encrypting and Signing Transaction Details



Decrypting and Verification of Transaction Details



Conclusion

- Main issues affecting the development of M-Commerce applications are;
  - communication channel
  - security
  - mobile device resources
- The model is practically realizable and if implemented on a large scale, the M-Payment framework will significantly change how businesses transact.
- The market is ready for this development. So far M-PESA has over 2.3 million registered and over 18 billion has already been moved through person-person transfers.

Recommendations

- Optimization of the model
- Establishment of proper Legislation to protect electronic transactions.

Thank you!

Questions?