Cyber Security 2018

Ensuring Message Freshness in A Multi-Channel SMS Steganographic Banking Protocol

Omego Obinna, Eckhard Pfluegel, Martin Tunnicliffe, Charles Clarke

Kingston University,

Penrhyn Rd, Kingston upon Thames KT1 2EE

Background

- Online banking is a huge success story
- In 2014, there were 133.5 million digital banking users in the U.S. and this figure was projected to increase to 161.6 million in 2019
- Mobile banking is increasingly the most preferred online banking approach
- SMS banking is an attractive solution due to its simplicity and cost-effectiveness
- However there are concerns about the security

SMS Banking Security

- However the following security attacks might take place:
  - An unauthorised external entity (adversary) performing passive or active attacks:
    - Eavesdropping
    - Man-in-the-middle attack
    - Replay attack
  - The government, the mobile service provider and external adversaries can eavesdrop on the communication, or modifying message content
- How could we design a secure SMS mobile banking protocol?

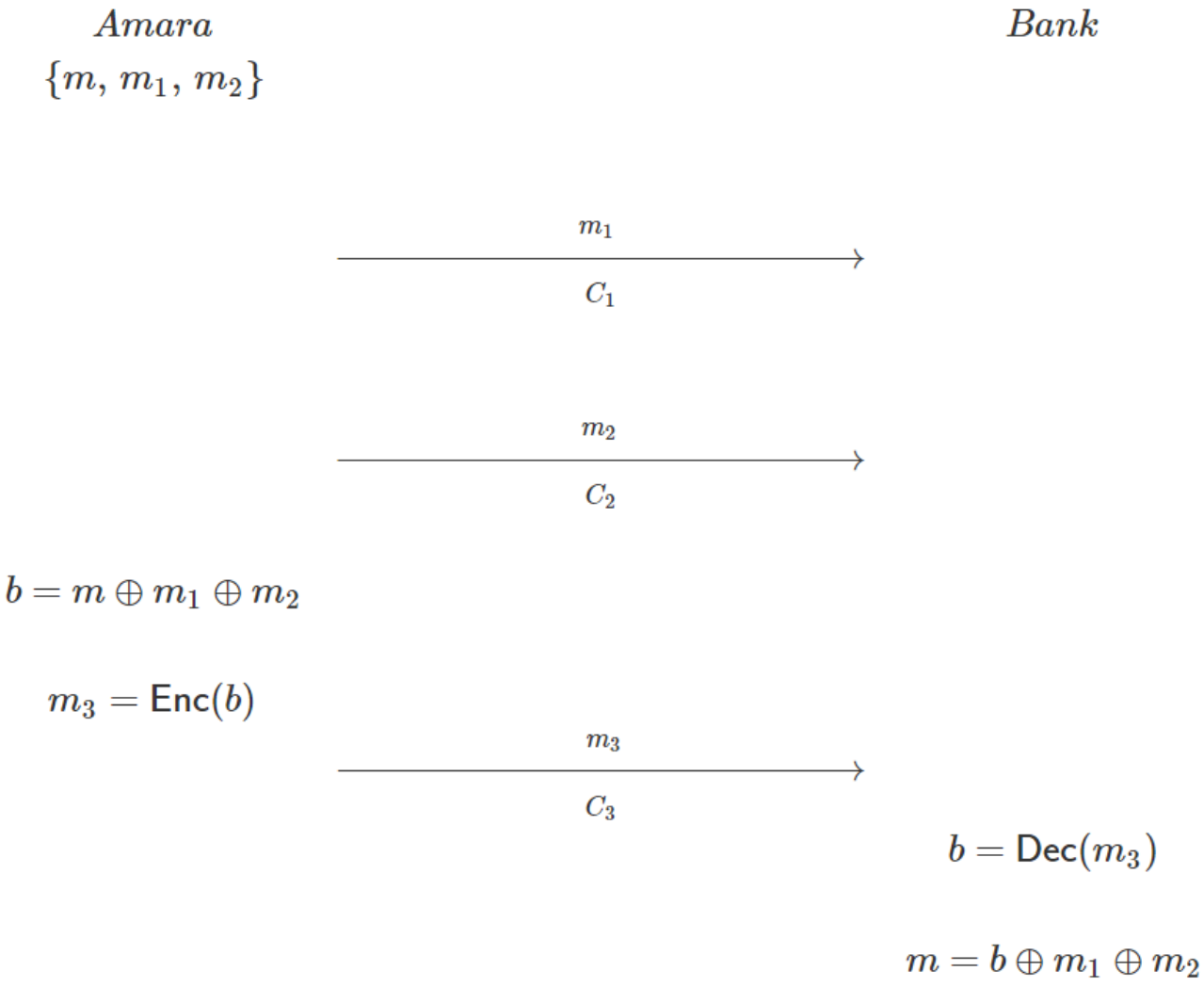
Security Assumptions

- The bank can be trusted
- The cybercafé, government and the mobile operator(s) cannot
  - They could carry out passive or active attacks (eavesdropping, man-in-the-middle, steganalysis)
  - Attacks could be done on their own, or by working together (collaborative attack)

Main Idea

- We want to avoid encryption, as it attracts suspicion due to the socially constrained SMS channel
- Instead, we use a combination of low-entropy and high-entropy steganography
- The use of three communication channels further increases attack resistance

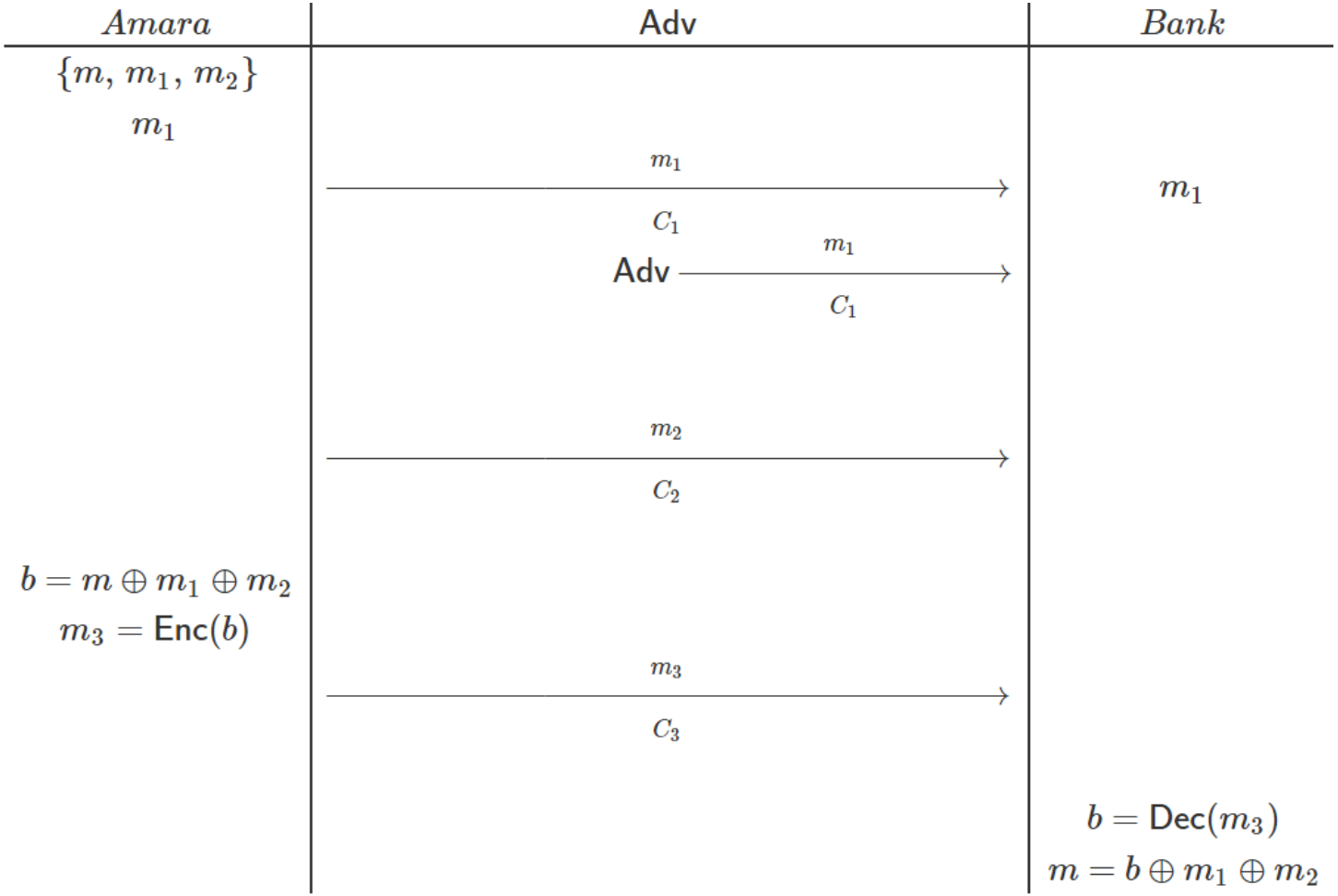
Previous Approach: Three-Channel Steganographic Protocol



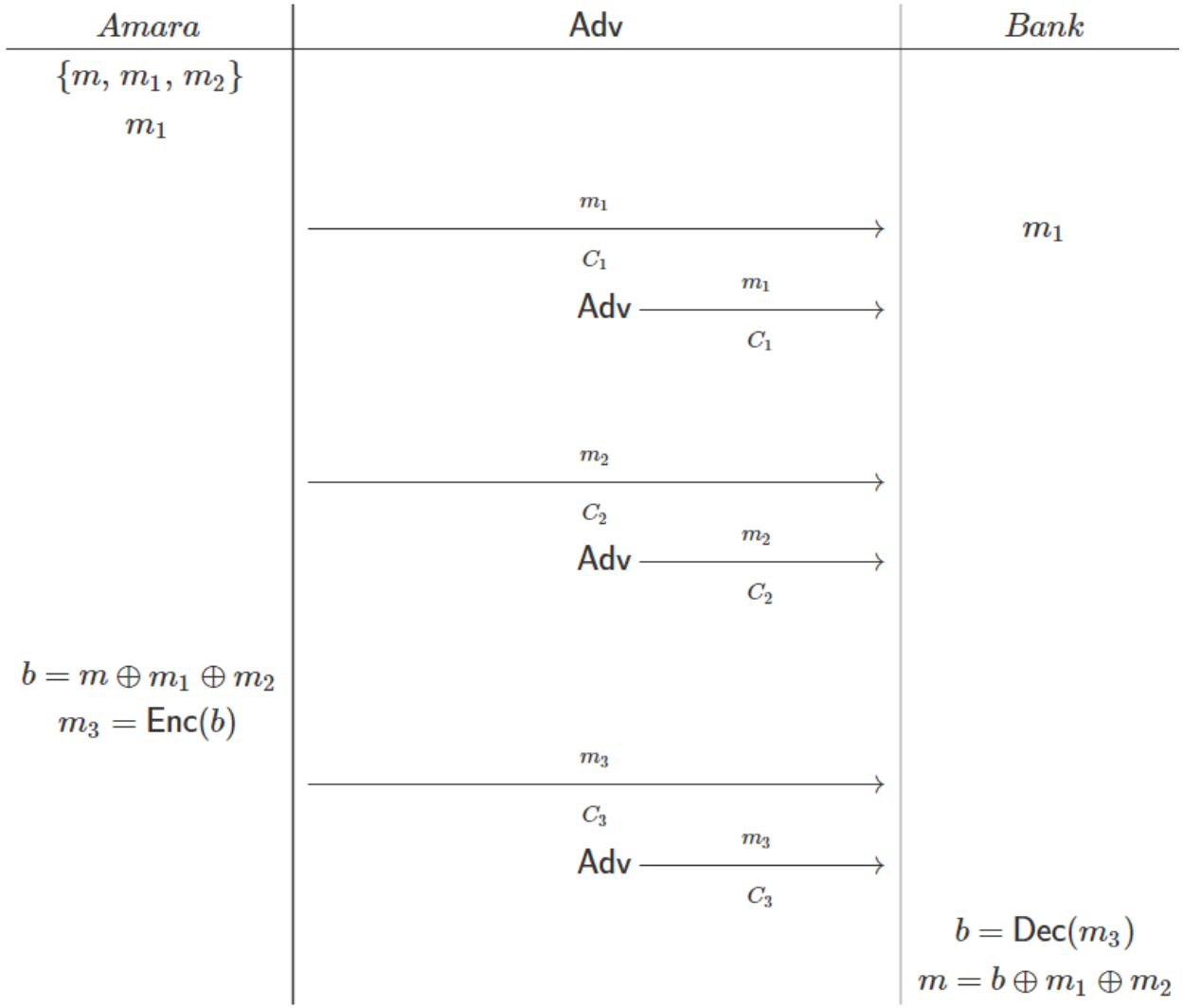
Vulnerabilities and Threats

- Problem: this protocol cannot establish message integrity
- Resulting Threats:
  - Replay attack (passive and active attack)
  - This attack is a form of network attack on a security protocol in which a valid data transmission is maliciously repeated or delayed.
  - This is carried out by a range of adversaries.
  - Fools the honest participant(s) into thinking they have successfully completed the protocol run.

Attack model 1



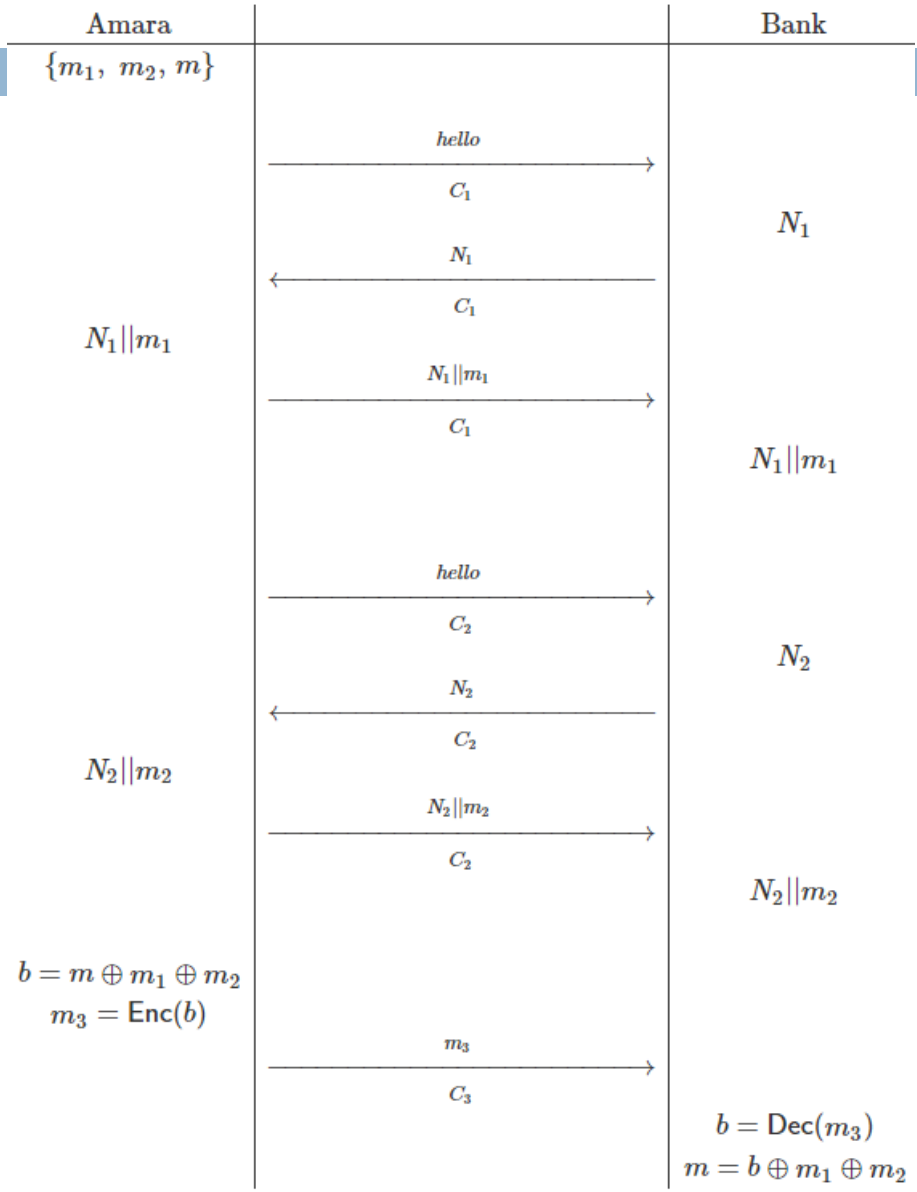
Attack model 2



Goals

- Make the Protocol robust against:
  - The multi-channel replay attack
- Including a nonce
  - A nonce is valid only once. The purpose of a nonce is to make each transaction unique so that an adversary is unable to replay old communications or an unauthorized transaction in a different context. A cryptographic nonce should have the following characteristics
    - unpredictability or pseudo-randomness.
    - could include a time-stamp to ensure exact timeliness, although this requires clock synchronization between communicating entities.

New Approach: Protocol Architecture



Conclusion

- We have designed a secure SMS banking protocol with distinct novel features:
  - The protocol employs three channels
  - It is based on a hybrid steganography model
  - It provides security against a range of adversaries
- We are working towards a robust design and implementation for real-world use