BlueTeam presentation on Mock Banking System Cryptography & Network Security (`CSCI-4230`)

Brian Sheedy & Avi Weinstock

December 9, 2015

Protocol Overview

- Statically sized messages
- AES Encryption
- HMAC
- Nonces

Encryption

- 128-bit AES
- Applied to everything except the sender's name and HMAC
- Applied to every message, including nonce requests/responses
- Provides confidentiality and authenticity
- Keys statically set in bank, stored in cards for ATM

HMAC

- OpenSSL's HMAC function using SHA-256
- Applied to the encrypted data
- Applied in every message
- Provides integrity and authenticity
- 128-bit key set statically in bank and stored in cards for ATM

Nonces

- Prevent replay attacks
- Each message to the bank preceeded by requesting a new nonce
- Nonce included in the message
- If the nonce from the ATM does not match the one in the bank, the bank rejects the message
- If the nonce from the bank does not match the one originally sent to the bank, the ATM rejects the message
- Nonce is cleared from the bank after every message