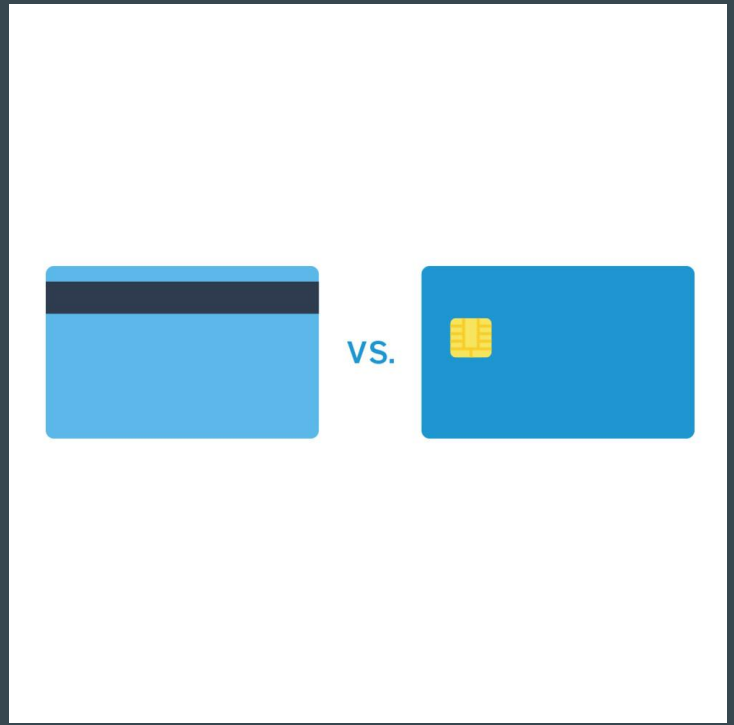
Smart Card Technology

Kelly Heaney

Background

- Successor to magnetic stripe cards
- Contains microprocessor, memory, and I/O interface
- Performs authentication on microprocessor, rather than terminal



Applications

- Credit/Debit Cards
- ID Verification and Access
- SIM cards

Security

- MAC - message authentication codes
- Supports SHA-1, MD2, MD4, MD5 hashing algorithms
- Supports DES, 3DES, AES, blowfish, or IDEA secret key algorithms

Vulnerability

- Flaw in RSA library by German chipmaker Infineon
- Obtain private key via public key
- Generating keys since 2012

Project

- Answer to Reset (ATR) - first response from smart card
- Application Protocol Data Units (APDU)
- Send APDU command to get card information

References

- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-157.pdf
- https://pyscard.sourceforge.io/user-guide.html#the-answer-to-reset-atr
- https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/
- https://www.openscdp.org/scripts/tutorial/emv/reademv.html