MOBILE POINT OF SCAM: ATTACKING THE SQUARE READER

Alexandrea Mellen, John Moore
almell@bu.edu, jmoore15@bu.edu
WHO ARE WE?
AGENDA

- Mobile P.O.S.
- Square Reader
- Software Vulnerabilities
- Hardware Vulnerabilities
- Countermeasures
- Disclosures
MOBILE P.O.S.

black hat
USA 2015
A NEW P.O.S.

- 3 C’s: compact, cheap, compatible
  - Yet still sophisticated
- Food trucks, coffee shops, salons, taxis...
- Square, PayPal, Intuit, Groupon, Amazon...
WHY DO I CARE?

New software & hardware,
WHY DO I CARE?

New software & hardware, from lots of providers,
WHY DO I CARE?

New software & hardware, from lots of providers, with rapid adoption...
WHY DO I CARE?

New software & hardware, from lots of providers, with rapid adoption... handling sensitive info!
“We protect your data like our business depends on it—because it does.” [1]

Square, Inc.
SQUARE, INC.

- $20b in transactions in 2013 [2]
- $30b in 2014 (estimated) [2]
- $100m in single day [3]
- $50m → $5b valuation in 5 years (100x) [4]
- >1 billion transactions [5]
HOW IT WORKS

- Magnetic head moves over stripe
- Varying voltage is decoded to bits
- Earlier models are passive
- Later models encrypt and amplify
THE SQUARE READER - MODELS

S2  S3  S4
INCOMPLETE DEPRECATION

- June ‘14: S3 “no longer supported,” but...
- June ‘15: all Readers still successfully complete transactions
  - Including unencrypted ones!
“All previous readers continue to be secure for daily use.” [6]

Square, Inc.
PLAYBACK ATTACK

- Replay attacks not possible for S3 and S4
  - Protected by transaction counter
- But playback of swipes is possible
  - Monotonically increasing count not enforced
- Stockpile swipes
  - Initiate delayed transactions
  - Use social engineering as necessary
SWORDPHISH

- Proof of concept iOS/web app assists with attack
  - Records extra swipes
  - Transmits to server
  - Server provides interface for playback
DEMO
HARDWARE VULNS
HARDWARE ENCRYPTION

- Ribbon cable connections
- Chip **not** located for **point-of-swap** encryption
HARDWARE ENCRYPTION BYPASS

- Tamper-resistant casing
- Jumper connection
- Crush encryption chip
  OR disable encryption chip connections
HARDWARE ENCRYPTION BYPASS
HARDWARE ATTACK VECTOR

- Malicious merchants
- Credit card skimmer
  - Cheap
  - Small
  - Easy
Proof of concept

- Records swipe
- Transmits audio to our external server
- Server decodes audio and stores info
DEMO
COUNTERMEASURES
SOFTWARE

- Remove claims of old models’ security
- Enforce deprecation of old models
- Implement risk signals as appropriate
- Decline stale swipes based on counter
HARDWARE

- Enforce deprecation
- Move chip directly to magnetic head for point-of-swipe encryption
SOFTWARE

- Reported playback attack in December ‘14
- Square triages issue in January ‘15
- Deployment of fix proves troublesome
  - Database synchronization
  - Offline transactions
- Marked as resolved in May ‘15
SOFTWARE (cont.)

✓ Remove claims of old models’ security
✓ Enforce deprecation of old models
✓ Implement risk signals
✗ Decline stale swipes based on counter
HARDWARE
“We’re already aware of the possibility that someone might tamper with our readers in this way.”

Square, Inc.
Square Readers are susceptible to SW and HW attacks that leave users vulnerable.

The growing mobile P.O.S. market faces unique challenges.

It is worth exploring (and securing) this relatively new attack surface!
Thank you!

Please complete the speaker feedback surveys!

Alexandrea Mellen, John Moore
almell@bu.edu, jmoore15@bu.edu
CITATIONS

2. http://techcrunch.com/2014/10/05/square-closes-150-round-at-6-billion-valuation/
3. https://squareup.com/townsquare/100m-day/
5. https://venturebeat.com/2014/11/05/jack-dorsey-square-has-processed-1-billion-payments-to-date/