Google Wallet PIN Retrieval

Nikolaus Stemm

February 13, 2012

What is Google Wallet?

- Stores Credit Card information on your phone
- Near Field Communication (NFC) to pay
- PIN to make it "safer"

Security Element

- Designed for phones with Near Field Communication, currently only Samsung Nexus S 4G

- Such phones have a "Secure Element" to store and encrypt data
- SE is new, and highly tamper resistant (maybe self-destructing)
- Credit Card information stored here
- Currently, very secure

So what's the problem?

- Joshua Rubin and zveloLabs did some poking around on rooted phone
- Found data stored in database on phone
- "metadata" included lots of encrypted data likely used for storing SE information, like card info
- More importantly, contained easily parsed data:
  1. Unique User IDs

So what's the problem?

- Joshua Rubin and zveloLabs did some poking around on rooted phone
- Found data stored in database on phone
- "metadata" included lots of encrypted data likely used for storing SE information, like card info
- More importantly, contained easily parsed data:
  1. Unique User IDs
  2. Google account information

So what's the problem?

- Joshua Rubin and zveloLabs did some poking around on rooted phone
- Found data stored in database on phone
- "metadata" included lots of encrypted data likely used for storing SE information, like card info
- More importantly, contained easily parsed data:
  1. Unique User IDs
  2. Google account information
  3. Cloud to Device Messaging account info ("push" notifications)

So what's the problem?

- Joshua Rubin and zveloLabs did some poking around on rooted phone
- Found data stored in database on phone
- "metadata" included lots of encrypted data likely used for storing SE information, like card info
- More importantly, contained easily parsed data:
  1. Unique User IDs
  2. Google account information
  3. Cloud to Device Messaging account info ("push" notifications)
  4. Google Wallet Setup status

So what's the problem?

- Joshua Rubin and zveloLabs did some poking around on rooted phone
- Found data stored in database on phone
- "metadata" included lots of encrypted data likely used for storing SE information, like card info
- More importantly, contained easily parsed data:
  1. Unique User IDs
  2. Google account information
  3. Cloud to Device Messaging account info ("push" notifications)
  4. Google Wallet Setup status
  5. Secure Element status

So what's the problem?

- Joshua Rubin and zveloLabs did some poking around on rooted phone
- Found data stored in database on phone
- "metadata" included lots of encrypted data likely used for storing SE information, like card info
- More importantly, contained easily parsed data:
  1. Unique User IDs
  2. Google account information
  3. Cloud to Device Messaging account info ("push" notifications)
  4. Google Wallet Setup status
  5. Secure Element status
  6. The big one: PIN information

What kind of PIN information?

1. SHA256 hash string

What kind of PIN information?

1. SHA256 hash string
2. long integer salt

What kind of PIN information?

1. SHA256 hash string
2. long integer salt
3. A PIN is only 4 digits

What kind of PIN information?

1. SHA256 hash string
2. long integer salt
3. A PIN is only 4 digits
4. Only 10,000 possibilities

What kind of PIN information?

1. SHA256 hash string
2. long integer salt
3. A PIN is only 4 digits
4. Only 10,000 possibilities
5. Easy to brute force

Proof

- Created Google Wallet Cracker app to prove it
- Takes under 2 seconds to find PIN
- Video: http://www.youtube.com/watch?feature=player_embedded&v=P655GXnE_ic

How to fix it?

Just need to move the PIN to the Secure Element

- Need to get code digitally signed by manufacturer - takes time, but not difficult
- Moving PIN may be "change of agency" - banks now responsible for PIN security
- Banks may choose to allow security risk to continue to avoid liability

What to do in the meantime?

Slow bad guy down to give you time to call your bank!

1. Don't root phone

What to do in the meantime?

Slow bad guy down to give you time to call your bank!

1. Don't root phone
2. Lock Screens

What to do in the meantime?

Slow bad guy down to give you time to call your bank!

1. Don't root phone
2. Lock Screens
3. Disable debugging

What to do in the meantime?

Slow bad guy down to give you time to call your bank!

1. Don't root phone
2. Lock Screens
3. Disable debugging
4. Encrypt disk

What to do in the meantime?

Slow bad guy down to give you time to call your bank!

1. Don't root phone
2. Lock Screens
3. Disable debugging
4. Encrypt disk
5. Install updates!

The End

Questions?

http://nakedsecurity.sophos.com/2012/02/09/google-wallet-pins-easily-stolen-from-rooted-devices/

https://zvelo.com/blog/entry/google-wallet-security-pin-exposure-vulnerability

http://www.youtube.com/watch?feature=player_embedded&v=P655GXnE_ic

http://www.google.com/wallet/