Some thoughts on iMessage

Gabriel Kaptchuk

National Security

Johns Hopkins researchers poke a hole in Apple's encryption

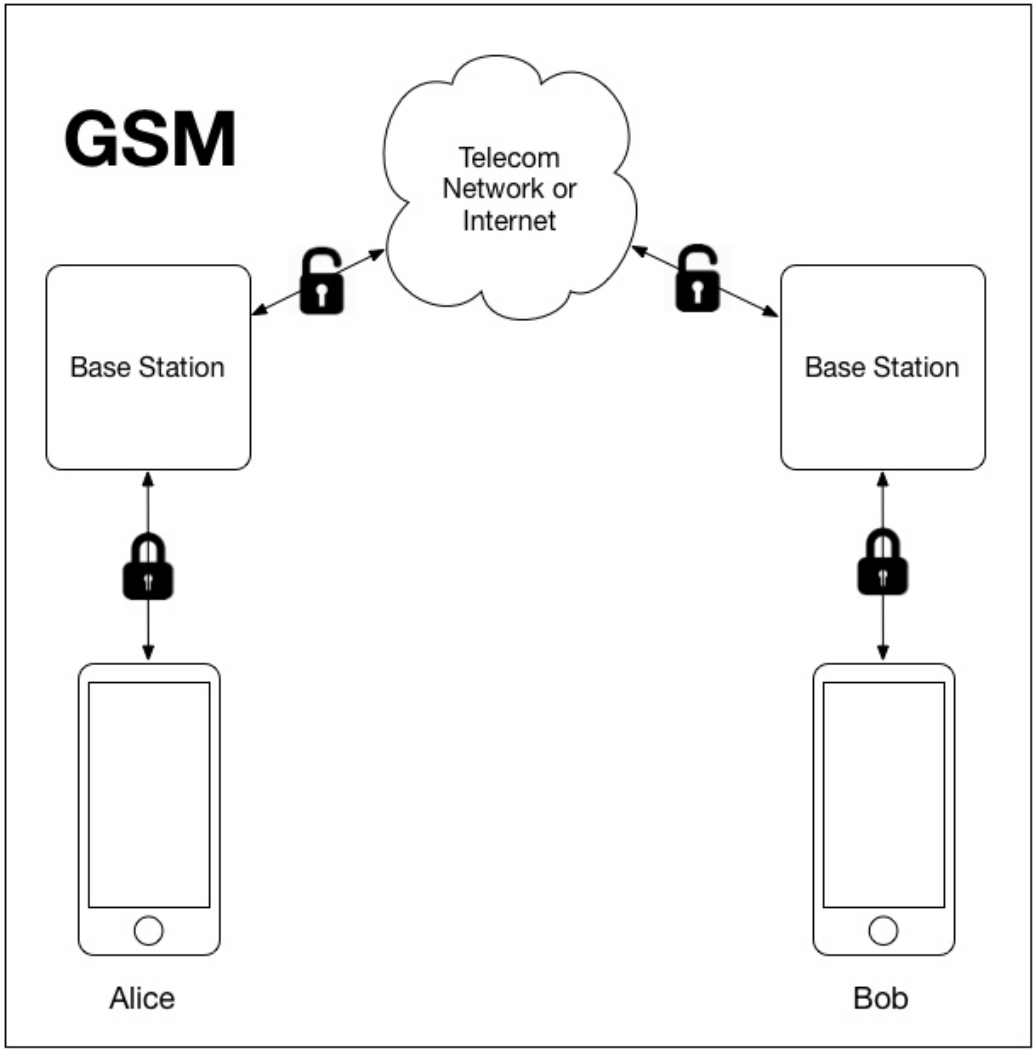
A group of Johns Hopkins University researchers found a bug in Apple's encryption that would let a skilled attacker decrypt photos and videos that were sent as secure instant messages. (Matthias Schrader/AP)

By Ellen Nakashima March 21

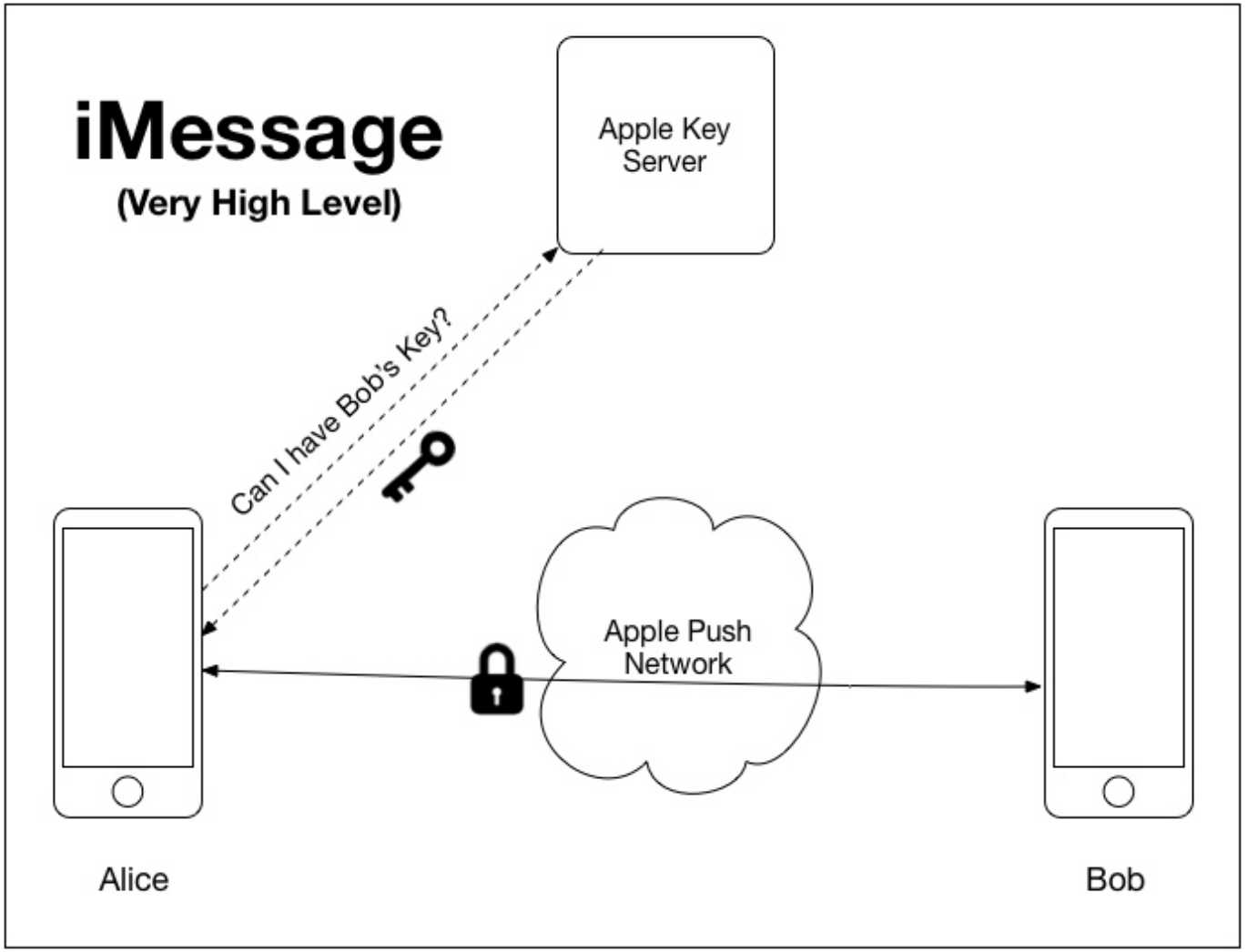
Why is iMessage Important?

- SMS has virtually no real security
  - Current realization of SMS in GSM which uses A5/1 or A5/2
  - Once traffic hits base station, it is decrypted for relay
- There is no public key infrastructure for GSM
  - It is actually a stateless protocol
- iMessage was introduced in 2011 and was the first widely adopted “end-to-end secure” messaging system
  - More secure than SSL/TLS!

How does SMS/GSM Work?



How does iMessage Work?



iMessage has a LOT of parts

- Public Key infrastructure for encryption
- Public Key infrastructure for authentication
- Multiple devices registered to a single account
- Sending more than just text
  - Attachment messages
- Logging into a new device
  - Turned on but not logged in?
- Push Notifications
- Phone number Identity and icloud identity
- Messages must remain secure to Apple
- …

What's Interesting from a Networking Perspective?

- How do you securely send a message such that the communications infrastructure itself is untrusted?
- What about untrusted Public-Key infrastructure?
- Tradeoff between utility and security
- Any Thoughts?

What about the Attack?

- Its pretty complicated and requires a strong background in security
- Attacker mauls ciphertext 200,000 time and watches the phones reaction to each change
- Each query leaks a tiny piece of information, and over a large number of queries we can recover information about plaintext
- Have to overcome lots of practical problems to make this work