Ethics of Device Backdoors

April Seliger

Quick overview/refresher of Encryption

- End-to-End encryption only the sender and receiver of a message can see it
- Both parties have a public and private key (essentially passwords)
- Sender encrypts the message with the receiver's public key and then sends it
- Receiver gets the message and decrypts using their private key
- Only the Receiver knows their private key.

Should this be allowed?

Could be used nefariously, i.e. terrorism

Video

San Bernardino

On December 2nd, 2015 a terrorist attack was carried out in San Bernardino California

- Both the shooters were killed.
- One of the shooter’s phones was seized but it was locked
- The FBI attempted to compel Apple to introduce a backdoor to the phone, Apple refused.
- Eventually the phone was cracked using a zero-day bug.

Should Apple have complied with the FBI?

Pro sides of the argument

- Can be used to stop terrorists
- Warrants can already be issued for physical property, why not digital?
- Can stop more than just massive terrorist threats (Child porn, pirating, ect)

Con sides of the argument

- The government cannot be trusted to be “good” for all time
- A bad actor could abuse this power individually
- Cannot be restricted to just “good” countries, countries abusive to their citizens would gain access too
- Already contains evidence of abuse through fear mongering

Utilitarian Ethics

- The greatest amount of happiness
- Backdoor could/would stop terrorists = GOOD
- Backdoor could/would be used to spy on things legal in the US (i.e. being gay in say Egypt) = BAD

Thank you

Questions?