Weekly Ethicacy
Joshua Higgins and Alicia Wade
CSCI 77800 Fall 2022

Breaking Encryption for Law Enforcement: Yet Another Security Hazard?

Background

In 2014 we had Riley v. California, which led to the requirement that law enforcement must have a warrant to search a suspect's phone upon arrest.

In both the San Bernardino (2015) and Pensacola Naval Station (2019) shootings, law enforcement obtained warrants to search the devices and from there ran into difficulties, relying on private companies and resources to try and gain access, costing tens of thousands of dollars at a time.

End-to-end encryption (E2EE) is not something that is foolproof, or even immune to government and law enforcement bypass. However, any and all suggestions that have been put forth to allow for government access (via backdoors) have been provably hazardous for secure implementations.

Pros

- Raises the speed at which law enforcement can obtain critical information for time-sensitive situations.
- Reduces the cost of encryption bypass for cases where the law has authority to search a device, but has no access key.

Cons

- Installing backdoors in encrypted systems creates technical vulnerabilities that could be exploited to commit cybercrime. This renders products and services that rely on encrypted systems vulnerable to cyber-attacks.
- Protocols that have technical vulnerabilities intentionally introduced into them, say free and open-source software, would not be adopted by organizations that want to build strong encrypted services.

Sources

- https://www.ucl.ac.uk/steapp/sites/steapp/files/encryption_pros_and_cons_pdf.pdf
- https://www.axel.org/2021/02/10/law-enforcement-is-already-breaking-into-encrypted-devices/
- https://www.american.edu/sis/centers/security-technology/encryption.cfm