Bypassing Security Mechanisms to Comply with Legal Orders

Case Study

You are the lead security engineer for a company that manufactures mobile devices. Your team has received a court order to create a mechanism that law enforcement will use to gain access to a suspect's device without their permission. How do you respond?

Case narrative

Your company manufactures a popular line of smart phone devices that are used by millions worldwide. For years, your company has been criticized for inadequately protecting user's private data stored on the device. Specifically, whenever a device was lost or stolen, anyone who recovers the device can extract credit card information, usernames and passwords to social networks, pictures, and other sensitive information.

Taking these concerns to heart, your team recently designed and implemented a full-disk encryption system to protect user data. The data could only be decrypted and retrieved from the device with the user's password or fingerprint. Your team identified a possible weakness to brute-force attacks: By connecting the phone to a computer via USB cable, an attacker could run a program that automatically tries all possible passwords. Each attempt takes 80 ms to run, allowing for over 1,000,000 automated attempts in one day.

To prevent brute-force attacks, your code built in an exponential back-off: After 10 failed login attempts, the phone would be locked for 5 minutes before the password could be tried again; another failed attempt produced a 30-minute lock-out; one more and the phone would be locked for a day. By the 15th failed login, the phone would be locked for years.

Your manager has informed you that your company has received a court order to create a program to bypass the exponential back-off mechanism. Members of a law enforcement agency have seized a phone from a suspect and have presented sworn testimony to a judge that this phone likely contains evidence of a crime that has already been committed or one that may be forthcoming. The court order requires your company to produce a firmware update that law enforcement can install on this phone. The requirements stipulate that the update is to run only on this particular phone, disable the exponential back-off, then remove itself.

Historical context and additional discussion

In the aftermath of a 2015 mass shooting in San Bernardino, CA, police sought evidence that the shooter had information on his phone about prior contacts with some of the people killed. The U.S. FBI were granted a search warrant of the shooter's phone, but were unable to access the phone due to the lock mechanism. The Department of Justice then filed a motion in court to order Apple to produce a firmware update that would disable the exponential back-off as described; Apple responded by refusing to cooperate with the request, and the Department of Justice eventually dropped the motion.

1. Does the introduction of this firmware upgrade constitute a "back door" into an encryption mechanism? In either way, what are the implications of this classification?
2. How will creation of this firmware upgrade affect consumer confidence in computing systems, as the new code is designed to bypass other mechanisms that were put in place to protect consumers with an increasingly trusted boot sequence?
3. With few exceptions, there is generally no mechanism to bind a piece of software to one particular device, suggesting at least part of the court's request is not possible technically. How would you explain this to a non-technical audience?
4. If you comply, what risks are presented to other users who have purchased your phone? Are these risks acceptable?
5. Does it matter if the suspected evidence relates to a criminal action that has already occurred versus a potential future crime?
6. If Apple complied with this request, on what grounds would it be acceptable to refuse future requests?
7. What are the implications of a large corporation refusing to cooperate with law enforcement and legal court orders in relation to cases of public safety? What does this suggest about the power of large technology companies?
8. How do you think the public's perception of Apple contributed to the outcome of this case? Would a smaller company or one that lacked a devoted user base be able to commit to such a stance?
9. In the San Bernardino case, the exponential back-off was implemented in software. The next generation of iPhone used a different processor that had this mechanism integrated into the hardware security system; upgrading the firmware to bypass the back-off (if possible) would require Apple engineers to break the security of a separate company's product. How would this design change affect the previous questions, if at all?