Design Considerations

My chosen technology has been the end-to-end encrypted messaging which can be found today in many freely available applications. Common examples are Signal, which is especially known for encryption, or WhatsApp, which introduced end-to-end encryption a couple of years ago as a reaction to the rise of new, secure messaging apps.

Physical Attacks

I chose this card because this type of attack is especially easy and by far the most suitable attack on end-to-end encryption. In most cases it will be not possible to break the encryption of the communication between the endpoints, so the endpoints themselves provide the best attack vectors.

End points will most likely be mobile phones. People tend to leave their phones unattended. They also carry them with them all the time. The chance of being able to have physical access to a mobile phone for a certain amount of time without the victim noticing is high. Even if the victim notices the loss it will be most likely not be suspicious if it reappears again as if the victim just had lost the phone somewhere.

During this time of physical access, the attacker might be able to install malware on the phone to bypass the entire encryption and to dump the keys in use. He also has plain text access to all of the victim's past communication. People often exchange credentials for shared accounts or other confidential data on messaging apps, especially if they feel safe because of the end-to-end encryption. In this case, the presence of end-to-end encryption will therefore worsen the consequences of the attack.

Multi-Phase Attack

The multi-phase attack can begin with a physical attack on one of the endpoints which is why I have chosen the attack as the second card.

If the attacker has compromised one endpoint, he is able to read the entire conversations of the victim and to send new messages on his own. He even might be able to intercept replies and therefore communicate with contacts without the compromised victim knowing. He now can try to compromise more endpoints or even different communication channels.

From a social engineering perspective, impersonating the already compromised victim provides an extremely powerful starting point. The attacker is able to abuse the new victim's trust in the compromised victim and might even succeed in pushing the new victim into directly downloading and executing software with hidden malicious parts. He also can try to gather information about the endpoint users themselves: id, banking details, pictures, places and more. This even can lead to complete identity theft in the worst case. Even companies are in danger since people today often exchange business information of significant value on private communication channels.

Consequences

The consequences of the two attacks are difficult to foresee and can vary widely depending on the users' trust in the communication channel and awareness of the possibility of the attack. In general, worse consequences can be avoided by questioning the authenticity of messages. Most people today are aware of phishing e-mails, but most people are also not aware of similar attacks on different communication channels.

Also, despite the existence of biometrical access control on mobile phones, many people simply still don't lock their phone. The consequences can be disastrous, but people tend to not care about their phone as much as they do with their computers. Raising the awareness of the importance to secure the mobile phone and handling sensitive data with care would prevent many of the currently possible easy attacks on end-to-end encryption.