Messaging Security

Part of Hacking/Hustling Workshop with t4tech at Eyebeam

Liz Ectricity | September 20, 2018

Short language note

I use some computer security language in these notes.

Threat modeling is a process of determining what data is important to you, how much effort is worth it, what makes sense based on your situation. There is another full workshop on Threat modeling earlier from this series.

A common way to phrase setups is to call you Alice, the person you are trying to communicate with Bob, and to call the attacker Eve.

Goal

Text messaging is a common form of communication, where short pieces of information are sent either cellular networks or the internet. Attackers can be interested in text message data and metadata (who is being senst to, frequency of texts, size of texts) and can access this data from listening on these networks, or by accessing either Alice's or Bob's phone.

SMS and MMS

Short Message Service, and Multimedia Message Service are the standard messaging services. SMS is used for basic texts between two people, MMS is used for images, videos, audio, and for multiple recipients/group texts. Messages are sent to Short Message Service Centers, which attempt to forward the message to the recipient. Service Centers are managed by third parties, and phones default to whatever mobile network they are using. As a user, you have little control over what Short Message Service Centers do with your data. SMS is unencrypted, and most phone carriers will be default save messages. Hostile actors (Eve), can also place false Short Message Service Centers to intercept and store text messages. Other apps may use internet based messaging, including Imessage between iPhones, Whatsapp, Facebook messenger, and Signal. These apps provide various levels of defense, and require various levels of trust with their provider companies.

Listening

Situation Eve uses network to monitor communication between Alice and Bob.

Encryption defense Signal encrypts messages end-to-end. Metadata is still viewable to Listeners which means that recipient, number of texts, approximate message size (to nearest 256 characters) is viewable to a listener. Signal uses an open source encryption method, which means that it is likely a hole in their encryption method will be spotted in the public eye, with major news and changes.

Physical Attack

Situation Someone has your phone in their hand and is reading your texts.

Password defense A password can protect your texts from being read immediately. Passwords should be well chosen for the threat model. Passwords also require that the information being protected is properly encrypted, if the attacker is dedicated. Passwords may not be effective in situations where it is most advantageous to give up the password.

- With a warrant police may be able to demand a password.
- TSA agents, Immigration agents, Police etc. can use power to make giving your password advantageous to deescalating situations. Consider your threat model, what incriminating information is protected by your password, etc..

Disappearing messages defense Messages can be set to disappear after a set amount of time. This can make it difficult to find previous texts. An attacker who gains access to your phone will not see a history of texts. Consider your threat model in the length of time of texts. Signal does not store text messages externally. However a dedicated attacker could find metadata of texts forensically. Disappearing messages do not prevent Bob from recording your texts. They do not prevent other information from existing. They can deescalate encounters, but could escalate encounters depending on attacker's perception of you.

Person in the Middle

Situation Eve impersonates Bob, attempting to get information from Alice.

Private key notification Signal will notify you when the private key of someone you are texting changes. This can happen if the person gets a new phone, or reinstalls Signal. It can also occur if an attacker uses a different phone to impersonate the person you are texting. Keys are the way Signal establishes encryption. A "conversation" uses one key, until the key changes. When the key changes, messages are encrypted using a different mathematical formula, making the previous messages unreadable to a new phone.

Things to look at with Signal versus other Apps

EmThe most important feature of Signal is it uses a well known encryption method. This is important because well-known encryption methods are studied and attacked by academics, cryptographers, are constantly in industry use. A few other apps use proprietary encryption methods, which means they may have massive holes in their methods, which leave them vulnerable.

Other features for Signal

These features can be considered based on your threat model.

- *SMS and MMS* - Allows signal to send and receive unencrypted messages. Can be convenient, but may allow you to be confused about which messages are secure.
- *Screen Security* - Allows screen shotting of conversations. Can allow conversations to be recorded. May allow malware to record your screen.
- *Incognito Keyboard* - Requests your phone to use a keyboard that doesn't record keystrokes. Requires you to trust your keyboard provider.
- *Always relay calls* - Take all calls through Signal's encrypted calling service. Signal's service has fairly bad quality, but will provide similar defenses to its SMS service.
- *Read receipts* - Turns on read receipts. Increases metdata.
- *Blocked contacts* - Allows you to block contacts. Will show block contacts if you give up your password.
- *Registration Lock PIN* - Requires a PIN to use your phone number with Signal. This can reduce the chance of someone impersonating you using Signal.

Protonmail

Protonmail is an email client which can provide a method for secure email communication. In general, email communication is insecure. Emails are sent without encryption, which leaves them vulnerable to the attacks listed above (listening, person in the middle, etc.). Anything sent in an email is easily searched by Internet Service Providers (ISPs), Police Agencies, anyone with access to your local network, and anyone with access to your computer. Emails can be spoofed as well without much effort.

Protonmail is a end-to-end email encryption service. **The most important thing to keep in mind with protonmail is it will provide encryption to other protonomail emails**. Communication to other email providers such as gmail is insecure. Protonmail uses servers in Switzerland which prevents the seizure of its servers by EU or US police. Servers in EU or US jurisdiction could be searched for metadata or have encryption keys forcibly given by warrants.

Protonmail's site is here: https://protonmail.com/

PGP

PGP is a general suite of encryption methods for communication. PGP stands for "Pretty Good Privacy". PGP is mainly used for email. The advantage of PGP is that it can be used across email servers. The disadvantage is that is not straightforward to setup. Several email clients offer PGP add-ons. If both Bob and Alice and PGP tools, they can share keys (passwords) through a secure channel, and then send encrypted emails through an insecure channel (i.e. gmail), by decrypting emails via password. It is important to remember that once the email is decrypted, the text of the email should be handled securely and not stored. There are various methods for doing so, that are outside the scope of these notes.

OpenPGP lists various softwares that employ PGP protocol: https://www.openpgp.org

Over the Shoulder

Situation The attacker looks over your shoulder. Or records your screen using a camera. Or asks Bob what you said.

Defenses against this attack are largely using good security culture. Signal does not protect against this attack.

Quick note on Trusted OS

Signal, protonmail and PGP can only be trusted if you trust the OS (android, iPhone, Mac, Windows) you are running on. A *very dedicated* attacker (as in, if this in your threat model) may access your phone, replace your android OS with something that runs something that looks like Signal, but that does not secure your messages. This is just to say that nothing digital is truly secure.

Some Language you Might See

Encryption A mathematical process of making data difficult to read. Ideally encryption is difficult enough to take hundreds to thousands of years to decrypt.

Public/Private Key Encryption is often managed through public/private keys. Keys are essentially passwords. Private keys are held only by you, and are kept secret. Public keys are shown to everyone, and are especially of interest to who you are communicating with. A encryption protocol, such as used with HTTPS, PGP, Signal is often the RSA encryption method. This protocol will decrypt the message using either Alice's or Bob's private key and the shared public key.

End-to-End Encryption Encrypting messages through untrusted networks from Alice to Bob.

Zero Access Encryption Zero Access encryption refers to encrypting data where it is stored. Google or Facebook does not do Zero Access Encryption, they can and actively read your data. Protonmail claims Zero Access Encryption on its server, meaning your emails are encrypted while on their server, this reduces the ability for adversaries and for protonmail to read your data.