End-to-End Encrypted Communications: Phone Apps (beginning)

Learning Objectives

Learners will:

- Explore what “private communication” might mean.
- Be familiar with encryption as an idea.
- Be able to explain why end-to-end encryption is useful when communicators don’t trust intermediary third-parties and companies.
- Know where to find more information about end-to-end encrypted communication and downloading related messaging apps, such as Signal.
- Be able to identify that SMS is an insecure communication method.

Prerequisites

- Participants must have a mobile device with them if doing an install.
- Trainer has already done threat modeling with this group.

Ratio

Instructor: Learners
1:5 (One instructor to five students)

Suggested Materials

- Projector
- If planning an install, participants should bring their smart phones with them.

GOTCHAS AND PROBLEMS YOU MIGHT HIT

- What if participants don’t have their mobile devices?
- What if participants don’t own their mobile devices, or feel that their devices are already compromised by malware?
- What if participants don’t want to give their phone number? Do you have a backup activity, or a practice phone number they can contact?
- What if participants feel uncomfortable with other people in the room? What if people don’t know each other?

Recommended Reading

- How to: Use WhatsApp for Android and for iOS
- Communicating with Others
- Our OTR guides may be relevant depending on how the Q&A goes and the needs of the group you are teaching.
- Our PGP guides (for Linux, Windows, and Mac OS X) may be relevant. However, if you decide to teach PGP, that is a separate training and requires quite a bit of time and explanation..

Lesson Content

WARMUP

Facilitator splits up the group into two teams.

Facilitator: “Please introduce yourself to the people next to you by your preferred names. After, I’d like you to address the following prompt over the next five minutes. Your ideas can be as wild and imaginative as you want them to be. I’d like you to come up with as many ideas as you can in the next five minutes.”

To Team 1: “Your team is the Communicators. Let’s say you want to send a secret message to a friend. You don’t mind that others can see the fact that you and your friend are communicating, but you want to make sure the message’s content stays between you and your friend. How would you do it?”

To Team 2: “Your team is the Interceptors. Your group will be trying to intercept the secret message that the communicators are sending. You very badly want to read that secret message. What are the options you have? What kind of capabilities do you have? How might you get around the Communicators’ cleverness?”

“Go!”

Facilitator can encourage wild ideas in their responses. Team 1 Participants may say things like: passing a note that’s carefully folded and written in invisible ink, sending a SMS text message, using an obscure game chat channel to communicate, physically running and meeting to pass the note in person at a different location each time, writing in a made-up language that only you and your friend know, using an encrypted messaging app, etc.

Team 2 Participants may say things like: they imagine they are the government, and they have capabilities and resources like lawyers, system administrators, law enforcement, and three letter agencies. They can hire someone to help them crack the message or put malware on devices. Or, they may imagine they are a team of technically skilled hackers. Or, they might be a cell phone company, and intercept SMS messages. The hope is that they are able to come up with lots of roles of who may be involved in wanting to get this message.

After the five minutes are up, pose questions like the following. Depending on the participants’ responses, the facilitator can spend five minutes having the group go over each answer.

- What are the benefits of using invisible ink? Could someone crack how to read the invisible ink, once they identify that invisible ink is being used?
- What are the benefits of sending a SMS? Could someone crack how to read a SMS? How easy or hard might that be?
- What are the benefits of meeting in person at a secret location? Could someone figure out where you are meeting? How easy or hard might that be?
- What are the benefits of using an obscure tool, like a video game chat system? Could someone figure out where you are meeting, or are they unlikely to look?
- What are the benefits of writing in a made-up language? Could someone crack a made up language? What would happen after the made up language is

translated and figured out?

Discussion points may vary on participants' ideas of what might be secure or insecure.

Facilitator can then discuss: "Did anyone bring up using encryption? What examples of encryption do you know? What does encryption allow us to do?"

Facilitator should wait for responses, and guide participants toward an explanation like: "Encryption allows us to scramble messages into meaningless gibberish, and back into readable information."

KNOWLEDGE SHARE: SMS vs. End-to-End Encrypted Messages

(Facilitator can show the gif of SMS passing through a cellphone network.)

Facilitator: "This is a SMS, or text message, going through a cellphone network. What kinds of computers might have access to this text? How many people might have access to these computers?"

Guide participants to an answer along the lines of: Cell phone companies and others with access to cell towers. And since these companies share their data with each other across borders depending on business partnerships, possibly thousands and thousands of people.

Facilitator can lead a raise of hands and call and response portion.

Q: Who here has an iPhone?

Q: iPhone users, have you noticed that messages you send to other iPhone users are a different color than those you send to non-iPhone users? What color are they?

A: Blue!

Q: Does anybody have any idea what that color might indicate?

A: Apple iPhones use end-to-end-encryption for iMessage.

Q: What happens when you send messages to someone who has an Android phone?

A: Messages are green. They are sent unencrypted.

Transition:

Q: But what if the person you want to chat with doesn't have an iPhone, and you still want an end-to-end encrypted communication?

(Participants may already know of end-to-end encrypted apps that people can download.)

Facilitator: "One thing you should note is that both parties need to have end-to-end encryption tools downloaded in order to communicate privately with each other."

Facilitator: "Telecommunication networks and the Internet have made communicating with people easier than ever, but have also made surveillance more prevalent than ever. Without taking extra steps to protect your privacy, every phone call, text message, email, instant message, voice over IP (VoIP) call, video chat, and social media message may be vulnerable to eavesdroppers.

Often the safest way to communicate with others is in person, without computers or phones being involved at all. Because this isn't always possible, the next best thing is to use end-to-end encryption."

Facilitator: "What might this phrase, end-to-end encryption, mean?"

(Facilitator should guide participants toward the answer of: "End-to-end encryption ensures that a message is turned into a unreadable, scrambled message by its original sender, and decoded only by its final recipient," or "It scrambles messages between devices into gibberish, and is useful when you don't trust the service providers or companies who are helping to pass along the message.")

Facilitator: "What are some examples of third parties be that may interact with your SMSes and voice calls?"

(Participants may say some company names like ISPs or cell carriers, or the names of the phone manufacturers themselves.)

KNOWLEDGE SHARE:

Talking points:

- Most end-to-end encrypted messaging apps we recommend are free!
- They're great for use over Wi-Fi and over data plans.
- Many work internationally.

- Many allow you to do video chats, group chats, disappearing messages.

You can also share some more in-depth points:

- **Metadata matters.**

Phone service carriers know that you are using an end-to-end encrypted messaging app because they have access to your phone's' metadata. Companies that host app download stores (e.g. the Apple App Store or Google Play Store) also know you are using these apps. They are able to see the information *about* your messages, or metadata, and that includes details like when you downloaded the app. Depending on the app, metadata may be limited to this fact, or can be far more detailed. For instance, an app may also log who you have been contacting, when, and for how long, though the contents of the message itself aren't seen except by you and your intended recipients.

- **Before choosing a phone app, check what user information the app developers keep.**

Picking the right tool for you depends on your level of comfort.

- **Check that the end-to-end encrypted messaging app that you are using is end-to-end encrypted *by default*.**

- **Know the app's way of notifying you about an unencrypted message.**

There's a risk of someone misunderstanding a message as encrypted, because they may be confused about the app interface. For example, some apps will let you know when you are contacting someone who is not on the end-to-end encrypted app, and there will be some text that says something like: "Unencrypted SMS" or "Unencrypted text". Look out for this text!

- **Many encrypted messaging and phone apps require you to give your phone number and this may be a concern for some people.**

There are also ways to tie your account to a proxy phone number for apps like Signal and WhatsApp.

There are alternative apps that let you choose a username instead, like Wire. If being identified easily is a concern of yours, pick a username that's not the same as your usernames for other accounts or affiliated with your actual interests or identity.

- **Your country might not allow some encrypted messaging apps. Follow current events about restrictions on the Google Play Store and the Apple App Store.**

- **Many end-to-end encrypted messaging apps let you verify the identity of the device of your friend, which mitigates against eavesdroppers who may try to pretend to be your friend:**

This practice is called “key verification”, which is also known as checking the “safety number” in an app like Signal.

This helps you really make sure that you are talking to who you think you are! When sending messages, there’s a risk of something called a “machine-in-the-middle attack,” or MitM attack which is just when someone pretends they’re the person you’re trying to communicate with and is able to intercept your messages. The way you can prevent this is through a practice called “key verification.”

By verifying keys, you and the person with whom you’re communicating add another layer of protection to your conversation by verifying each other’s identities, allowing you to be that much more certain that you’re talking to the right person. Key verification allows your contact to confirm that the person they’re communicating with is really you, and you to confirm that the other person is really them, by checking with each other in-person or over a different, secure channel.

In practice, it usually looks like using your phone’s camera to scan your friend’s phone’s QR code, and having them do the same for you. That way their phone is confirmed as theirs.

The facilitator can then move onto the Q/A portion, followed by a guided install.

ANTICIPATED QUESTIONS & ANSWERS

Q: Why do you recommend these apps over [insert other app here]?
A: *The facilitator should refer to this piece about how EFF makes its decisions on tools.*

They’re end-to-end encrypted by default.

They’re free and they work on both Android and IOS phones.

These apps also have great security features. Apps like Signal, WhatsApp, and Wire use something called forward secrecy. A short summary is that the app encrypts each

message with a new set of encryption keys. It protects past messages against future compromises, like if someone was to somehow acquire your secret keys. This is different than something like end-to-end encrypted email, where the encryption keys stay with the user indefinitely until they choose to generate new keys (perhaps years later). If a bad actor gets ahold of their private key, that bad actor can decrypt all their previously sent messages.

(Note to the facilitator: If you've already explained public key cryptography and the person asking seems to be fairly technical, this explanation might make sense to them: https://whispersystems.org/blog/asynchronous-security/)

(Some of the latest additional features that are exciting in Signal include private contact discovery. Like the above, you can provide this link for a participant to read further: https://signal.org/blog/private-contact-discovery/)

Q: Isn't WhatsApp owned by Facebook? What does that mean?
A: Yes. WhatsApp initially promised to not share data with Facebook, and then changed its stance. WhatsApp is still end-to-end encrypted, but they are sharing metadata with Facebook, like who is contacting whom. A benefit, however, is that WhatsApp is a mainstream app, so it depends on the concerns you have, and the concerns of the people you are trying to communicate with. To read more about EFF's materials regarding Whatsapp, see the SSD guides for how to use WhatsApp for Android and for iOS.

Q: What if I want to anonymously communicate?
A: This is a different series of concerns than just wanting to have the content of your communications remain private. Do you prefer not to be associated with the person you are chatting with? This might be important for a journalist chatting with a source, a whistleblower, etc. The metadata of you chatting with a sensitive person (and vice versa) has a different set of risks and considerations. None of the tools we've talked about provide anonymous communication.

If anonymity is a concern for you, we can chat after the workshop.

Q: Does Signal really not retain that information? How can you know?
A: You can refer participants to this grand jury subpoena letter from the FBI in 2016: https://whispersystems.org/bigbrother/eastern-virginia-grand-jury/)

However, they should know that if Signal were to receive a U.S. court order, they may be forced to collect this kind of information going forward.

Q: I heard that people can hack into Signal. Is that true?
A: No, that method of compromise is from malware on your device. Malware can infect your device through methods like downloading a malicious file or by clicking on a phishing link. No end-to-end encryption tool can protect your messages if the endpoint (your device) is compromised by malware. This doesn't mean that the end-to-end encryption provided by the tool doesn't work.

Q: What if I don't want to use my real phone number?
A: You have several options. You can use Wire. Or, if you're based in the US, you can get a Google Voice phone number or a Twilio phone number to pseudonymously communicate. You can also replace your SIM card.

Q: Can I use end-to-end encryption for things aside from communication?
A: Yes! You can use it for file sharing as well. SpiderOak has a service for this. OnionShare is available for anonymous file sharing

Q: Can I use end-to-end encryption for instant messaging?
A: Yes. You can use a protocol called Off the Record (which many of these end-to-end encrypted messaging apps also incorporate). EFF has a guide for how to use Tor Messenger.

Q: Why don't you recommend encrypted email *or* End-to-end encrypted phone apps sound great! Is there an equivalent for email?
A: We don't usually recommend it in a training because it takes a lot of time for participants to set up and understand. The apps are far easier to teach because people are more comfortable with downloading an app on their phones, and the messaging interface feels familiar. Encrypted email has a few unique constraints that make it a bit more complex than end-to-end encrypted apps to explain to beginners.

One notoriously time-consuming and nuanced option is called Pretty Good Privacy (PGP, also used interchangeably with the free and open source implementation, GPG, or GNU Privacy Guard). There are some in-browser implementations of PGP that take less time to set up. For example, there is Mailvelope, a browser add-on/extension that's compatible with Gmail, and encrypts with other Mailvelope users. That being said, it is in-browser, rather than on your own computer.

EFF *does have* guides on SSD for setting up PGP directly on your computer. However, there are many ways to misunderstand or click on the wrong service. You're more in control using the PGP Thunderbird and Enigmail settings. You can read through our guides for Linux, Windows, and Mac OS X

OPTIONAL CLOSING ACTIVITIES

Survey the audience and check for understanding:

- What information can companies and service providers and telephone companies see when you communicate?
- What can a company see when you are using encryption on their platform? *(The answer is not “nothing.” The answer is gibberish or scrambled content, and they still see you communicating with someone.)*
- What information can service providers and telephone companies see when you communicate with someone using end-to-end encryption? *(Guide answers toward metadata.)*
- What are some popular services that don’t use end-to-end encryption?
- What does end-to-end encrypted communication help you do?
- What is a man/machine-in-the-middle attack?
- Let’s say you have malicious software on your device. Are your end-to-end encrypted communications still private?