

Seminar 5

Digital Security

Table of Contents

Seminar Five: Overview	3
Instructor Advance Reading.....	3
Digital safety overview for journalism students by the Electronic Frontier Foundation.....	3
Tactical Tech’s Security in a Box project	3
Freedom of the Press Foundation	3
Searchable archive of listserv posts by “Internet Freedom”	3
OpenNews.....	3
Instructor Advance Work.....	3
Student Advance Reading, Viewing, and Homework	4
Threat Modeling, Part One	4
Threat Modeling, Part Two	4
Threat Modeling, Part Three.....	4
Threat Modeling, Part Four.....	4
Optional: install Signal and Tor Browser, open a Gmail or Protonmail account	4
Seminar 5: Power Point Presentation.....	4
PowerPoint, Slide 1: Intro	5
PowerPoint, Slide 2: Why Digital Safety?.....	5
Digital Hygiene Lecture by Instructor	7
PowerPoint, Slide 3: Digital Hygiene.....	7
PowerPoint, Slide 4: Make a Strong Passphrase.....	8
PowerPoint, Slide 5: Comparing Passphrases.....	8
Social Media Hygiene Lecture by Instructor	10
PowerPoint, Slide 6: Keeping Safe on Social Media.....	10
PowerPoint, Slide 7: Social Media Hygiene	10
PowerPoint, Slide 8: Security and Privacy on Facebook	10
PowerPoint, Slide 9: Scenario One Simulation	11
PowerPoint, Slide 10: Scenario One (cont.).....	11
PowerPoint, Slide 11: Scenario Two Simulation	11
PowerPoint, Slide 12: Scenario Two (cont.).....	11

Threat Modeling Lecture by Instructor	12
PowerPoint, Slide 13: Threat Modeling – Basic Questions	12
PowerPoint, Slide 14: Threat Modeling – Additional Questions	12
Instructor Lecture on Creating a Toolbox	13
PowerPoint, Slide 15: Toolbox	13
PowerPoint, Slide 16: Email	13
PowerPoint, Slide 17: Tor: The Onion Routing	14
PowerPoint, Slide 18: Virtual Private Networks	14
PowerPoint, Slide 19: Encryption at Rest.....	15
PowerPoint, Slide 20: Scenario Simulation	15
PowerPoint, Slide 21: Scene 1: In the Journalist’s Hotel	15
PowerPoint, Slide 22: Scene 2: Café where journalist & source agree to meet.....	16
PowerPoint, Slide 23: Scene 3: In the Journalist’s Hotel	16
PowerPoint, Slide 24: Scene 4: At the Airport	16
PowerPoint, Slide 25: List of Resources	16

Seminar Five: Overview

This seminar illuminates the serious need for journalists to ensure the security of personal and work-related data stored on electronic devices and to keep themselves from being tracked through traces left on the internet.

Through lectures, exercises, and discussions, students will gain a heightened awareness of how to protect their data, navigate the growing number of data security tools, and determine the level of security needed in different situations.

Instructors are provided with background to help inform their teaching as well as readings for students to review in advance of the session. The instructors are also given bullet points to explain technology issues and promote discussion. A PowerPoint presentation and role-playing scenarios also will help the instructors guide the class.

Keep in mind that *nothing digital is ever completely safe*. The safest way to get information is to meet face-to-face. All the encryption tools only lower the risks and mitigate danger, they do not prevent them.

Instructor Advance Reading

[Digital safety overview for journalism students by the Electronic Frontier Foundation](#) presents basic aspects journalists should consider when it comes to digital safety and offers manuals for using certain tools.

[Tactical Tech's Security in a Box project](#) offers a more rigorous rundown on what tools are available and how to use them. It complements EFF's guide on the hands-on aspect.

[Freedom of the Press Foundation's](#) blog provides practical details on safety, e.g. how to set a safe passphrase.

[Searchable archive of listserv posts by "Internet Freedom"](#) technologists where journalists find the latest thoughts about any particular tool or concern.

[OpenNews](#), a project funded by non-profit Community Partners, has assembled a GitHub repository of useful information when it comes to organizing a training session about digital safety, such as expectation management and facilitating class discussions on the topic. The instructor can apply ideas the material offers in class as needed.

Instructor Advance Work

Install WhatsApp and play with it. Set up PGP using one of the ways introduced here <https://ssd.eff.org/en/module/how-use-pgp-mac-os-x> or use Mailvelope <https://www.mailvelope.com/en/help>

To try out WhatsApp and PGP, the instructor needs to communicate with another person who also use WhatsApp and PGP.

Install Tor <https://www.torproject.org/projects/torbrowser.html.en>

Add all the students' WhatsApp numbers into one broadcasting list.

Student Advance Reading, Viewing, and Homework

Here's a short video on how the internet works; assign students to think about how communications can be intercepted: "[How the Internet Works in 5 Minutes.](#)" (video)

How to create a strong password: "[Surveillance Self-Defense: Creating Strong Passwords.](#)"

Threat modeling assignment:

Read this introduction to threat modeling: "[Surveillance Self-Defense: Assessing Your Risks.](#)"

Then, watch the following four video lectures about threat modeling:

- [Threat Modeling, Part One](#)
- [Threat Modeling, Part Two](#)
- [Threat Modeling, Part Three](#)
- [Threat Modeling, Part Four](#)

Video Lecturer Bio: Jason Reich is the Director of Global Security at BuzzFeed. Before joining BuzzFeed, Reich led a team of crisis response experts working in the Middle East and North Africa. Reich is consulted regularly as an expert on issues of information security, online harassment and other media safety issues.

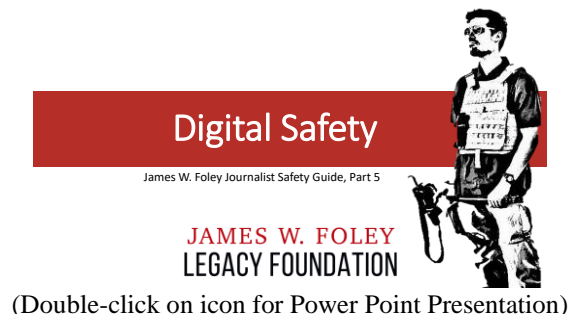
Write the [answers for the five risk model questions listed on the Electronic Frontier Foundation page](#) for one country where you hope to report. Submit your responses to your instructor the day before class.

Install [WhatsApp](#)

Save instructor's WhatsApp number.

Optional: install [Signal](#) and [Tor Browser](#), open a [Gmail](#) or [Protonmail](#) account.

Seminar 5: Power Point Presentation



(Double-click on icon for Power Point Presentation)

PowerPoint, Slide 1: Intro

The instructor starts the seminar by telling students they are going to hear from an expert to introduce the course. Then, the instructor reads Paul Rosenzweig's bio:

Paul Rosenzweig is the founder of Red Branch Consulting PLLC, a homeland security consulting company, and a Senior Advisor to The Chertoff Group. Rosenzweig formerly served as Deputy Assistant Secretary for Policy in the Department of Homeland Security in the George W. Bush administration. He is a Distinguished Visiting Fellow at the Homeland Security Studies and Analysis Institute. He also serves as a Professorial Lecturer in Law at George Washington University, an Adjunct Professor at the Near East South Asia Center for Strategic Studies at the National Defense University, a Senior Editor of the Journal of National Security Law & Policy, and as a Visiting Fellow at The Heritage Foundation. In 2011 he was a Carnegie Fellow in National Security Journalism at the Medill School of Journalism, Northwestern University, where he is an adjunct Professor.

Play the video of Paul Rosenzweig: [Importance of Digital Video](#). Rosenzweig uses the case of James Rosen and Jin-Woo Kim. Password for all videos: **foley17**

PowerPoint, Slide 2: Why Digital Safety?

The instructor then discusses how the internet works and how communication can be compromised based on the Instructor Advance Readings, followed by a role-playing exercise.

IN-CLASS EXERCISE

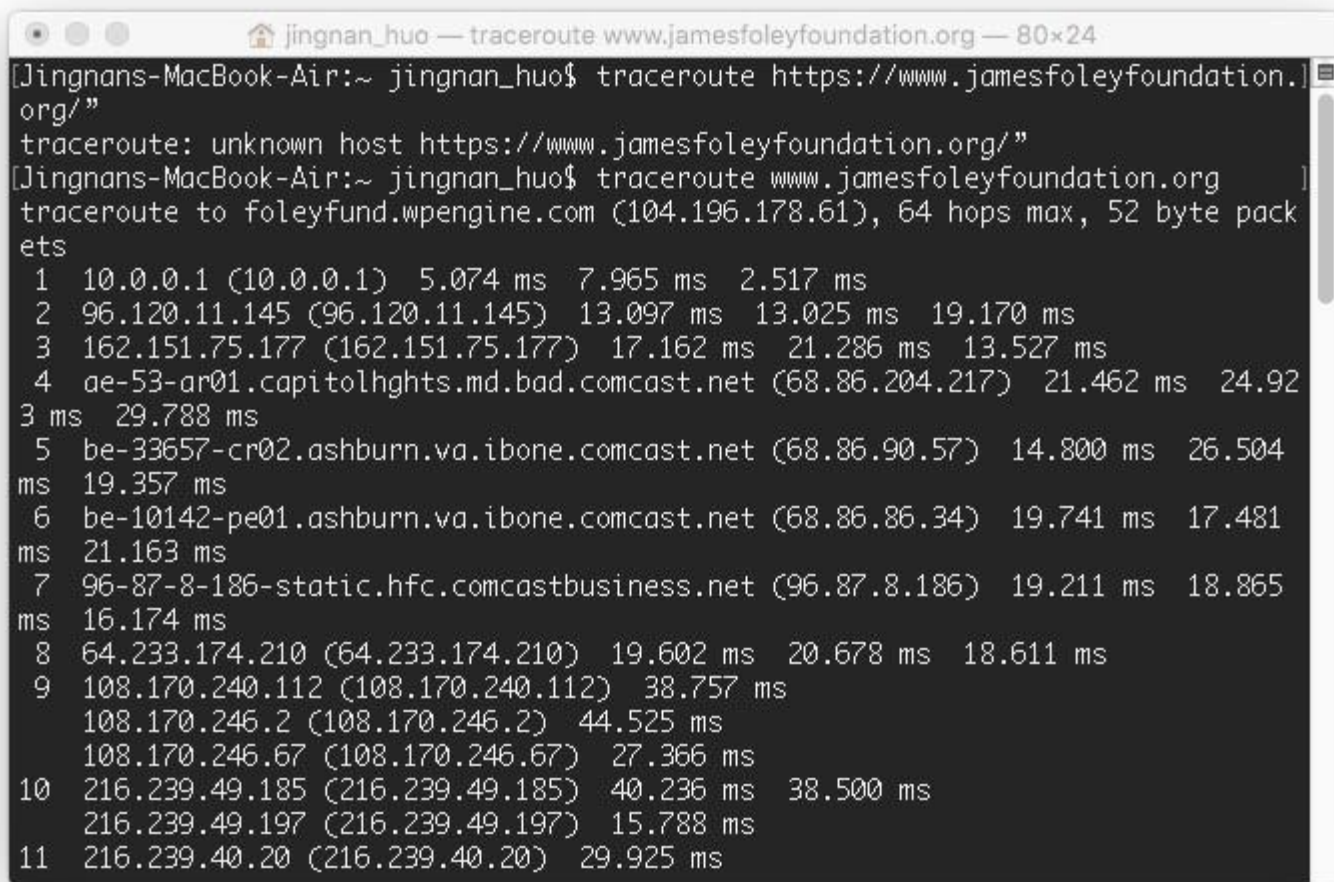
Each student plays the role of a server connected to the internet, and each server may be controlling computers at various entities such as universities, corporations and government agencies.

Student A plays a computer sending information – give the student a small picture and instruct Student A to put the picture into an envelope, write Student B on the outside of the envelope to indicate the intended recipient. Student A leaves the envelope unsealed, then passes the envelope to Student C, who passes it to Student D, who passes on to Student E. In advance, tell student C, D, and E that they can choose to look or not look inside the envelope. The instructor explains that this is what happens if information is sent without being encrypted.

Replay the scenario, but first have A seal the envelope (which would symbolize encrypted information). C, D, and E cannot see what's inside the envelope. The instructor notes that the students weren't able to look inside the envelope, keeping that information safe, but they know that A has sent the envelope to B at this point in time. AND they know that the envelope is sealed, that the traffic is encrypted. This could be a red flag in nations like Ethiopia, Pakistan, Vietnam or China, as entities monitoring Internet traffic including government authorities might believe any encrypted information means it is information the government would want to know.

Do a traceroute demonstration

If using an Apple computer, the instructor should click cmd+space to get the Spotlight search, type “terminal” into the search box, hit enter, and a black box with white letters on it will pop up. Type “traceroute www.jamesfoleyfoundation.org” in the black box and hit enter. The instructor will see lines of numbers and names start popping up one line after another. The lines represent the servers that are relaying this computer’s request, which is to visit the website “https://www.jamesfoleyfoundation.org/”. The servers are all the Cs, Ds and Es that the information is going through. This process happens when one visits a website, and also when one sends an email. Information is relayed through different servers, often located in different places. If the email was not encrypted, each of these nodes is an opportunity for someone to intercept and see the email’s content.



```
jingnan_huo — traceroute www.jamesfoleyfoundation.org — 80x24
[Jingnans-MacBook-Air:~ jingnan_huo$ traceroute https://www.jamesfoleyfoundation.org/]
org/"
traceroute: unknown host https://www.jamesfoleyfoundation.org/"
[Jingnans-MacBook-Air:~ jingnan_huo$ traceroute www.jamesfoleyfoundation.org ]
traceroute to foleyfund.wpengine.com (104.196.178.61), 64 hops max, 52 byte pack
ets
 1  10.0.0.1 (10.0.0.1)  5.074 ms  7.965 ms  2.517 ms
 2  96.120.11.145 (96.120.11.145)  13.097 ms  13.025 ms  19.170 ms
 3  162.151.75.177 (162.151.75.177)  17.162 ms  21.286 ms  13.527 ms
 4  ae-53-ar01.capitolhghts.md.bad.comcast.net (68.86.204.217)  21.462 ms  24.92
3 ms  29.788 ms
 5  be-33657-cr02.ashburn.va.ibone.comcast.net (68.86.90.57)  14.800 ms  26.504
ms  19.357 ms
 6  be-10142-pe01.ashburn.va.ibone.comcast.net (68.86.86.34)  19.741 ms  17.481
ms  21.163 ms
 7  96-87-8-186-static.hfc.comcastbusiness.net (96.87.8.186)  19.211 ms  18.865
ms  16.174 ms
 8  64.233.174.210 (64.233.174.210)  19.602 ms  20.678 ms  18.611 ms
 9  108.170.240.112 (108.170.240.112)  38.757 ms
   108.170.246.2 (108.170.246.2)  44.525 ms
   108.170.246.67 (108.170.246.67)  27.366 ms
10  216.239.49.185 (216.239.49.185)  40.236 ms  38.500 ms
   216.239.49.197 (216.239.49.197)  15.788 ms
11  216.239.40.20 (216.239.40.20)  29.925 ms
```

If using a PC, type “cmd” in the search box of the start menu, and a black box would pop up. The instructor would type “tracert jamesfoleyfoundation.org”, and hit enter. The same lines will pop up.

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\JN-Huo>tracert jamesfoleyfoundation.org

Tracing route to jamesfoleyfoundation.org [104.196.178.61]
over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms   10.0.0.1
  1  2 ms    2 ms    2 ms   96.120.11.145
  2 12 ms   12 ms   34 ms  162.151.75.177
  3 23 ms   38 ms   21 ms  ae-53-ar01.capitolhghts.md.bad.comcast.net [68.8
6.204.217]
  4 15 ms   21 ms   16 ms  be-33657-cr02.ashburn.va.ibone.comcast.net [68.8
6.90.57]
  5 19 ms   19 ms   19 ms  be-10142-pe01.ashburn.va.ibone.comcast.net [68.8
6.86.34]
  6 15 ms   14 ms   19 ms  96-87-8-186-static.hfc.comcastbusiness.net [96.8
7.8.186]
  7 19 ms   20 ms   20 ms  Request timed out.
  8 *      *      *
  9 15 ms   26 ms   19 ms  216.239.51.36
 10 43 ms   14 ms   18 ms  108.170.246.67
 11 37 ms   20 ms   24 ms  216.239.49.197
 12 32 ms   50 ms   63 ms  209.85.255.252
 13 63 ms   66 ms   31 ms  108.170.238.49

```

Now ask Student A to seal the picture in the envelope and put it on a table; then A tells Student B to fetch it, skipping all the Cs, Ds and Es. Explain to students that they can open an email account in which only they and their correspondent have the password – no one else – and they can just upload documents to the email account for viewing by both without having to hit “Send.”

Instructors should tell students that what they just did is called a “dead drop” in the virtual sense, and that it avoids interception caused by having the information passed by servers.

But also point out that there is a trade-off between securing their emails from surveillance and attracting the unwanted attention of intelligence agencies by using encryption. The fact that authorities see that your email is encrypted can make you a “person of interest.”

Digital Hygiene Lecture by Instructor

Play the video of Paul Rosenzweig: [Importance of Digital Hygiene \(video\)](#)

The instructor, using knowledge from the advance instructor readings, should tell the students about basic digital hygiene. These are the things that should be done in all circumstances.

PowerPoint, Slide 3: Digital Hygiene

- **Update software.**

Regardless of operating systems, software must be updated with periodic security patches to remain secure.

Why? Because information about system vulnerabilities that are unknown to the vendor, also known as “zero days or 0-day,” are traded on black markets and bought by those who want to exploit them. An ill-intentioned actor can purchase a zero day, design a virus that exploits the vulnerability, and then spread the virus to infect all computers that have the vulnerability.

An old, well-known and well-exploited XP vulnerability can be bought for \$10, because most computers would have patches for this vulnerability. An Android 6 loophole may cost \$500,000, because it tends to be newer, less well known, and most phone would probably not have patched it up yet, so the potential return of exploiting the vulnerability would be much larger. If you have a vulnerability, the best you can hope for is that it is very expensive and/or time-consuming to find and exploit, making it unattractive to most hackers.

Most computers around the world that get infected are vulnerable because they are using pirated versions of Windows

- **Keep strong passphrases or use a password manager.**

PowerPoint, Slide 4: Make a Strong Passphrase

Play video of Paul Rosenzweig: [Passwords and Password Managers \(video\)](#)

Passwords should be between 12 to 16 characters, including UPPER case and lower case, numbers and symbols. You should have a unique password for each online account.

Some recent research indicates that password length matters more than cases and symbols.

There is an easy way to create strong passwords – think of a random sentence and then transform it.

Example: make up something that includes things students can see in the classroom, a student’s favorite animal, a strange occurrence, and name of a fruit, then transform that sentence in a random way.

Tactical Tech developed the following form to show how long it takes to crack a password depending on complexity:

PowerPoint, Slide 5: Comparing Passphrases

Sample password	Time to crack with an everyday computer
Bananas	Less than 1 day
Bananalemonade	2 days
BananaLemonade	3 months, 14 days
B4n4n4L3m0n4d3	3 centuries, 4 decades

Sample password	Time to crack with an everyday computer
We Have No Bananas	19151466 centuries
W3 H4v3 N0 B4n4n45	20210213722742 centuries

Another option is to use a password manager such as LastPass or 1Password. You can store all of your website passwords in a password manager and just remember the master password. The password manager will assign a near-random, hard-to-crack password for all your websites; you access your sites through the password manager. However, if you forget the password for the password manager, it cannot be reset and you cannot access the passwords.

- **Be very careful about attachments and links.**

Most penetration attacks occur from opening an attachment or clicking a link that includes a virus or malware. In other words, the computer user has opened the door to let the hackers in.

One good way to open an email without infecting a computer is to view it on Google Drive because it stays on the cloud and doesn't infect the computer.

- **Use two-factor or multi-factor verification.**

If you have activated two-factor verification for your email, every time you log on to your email on a machine that you have not used before, you will receive a prompt – it can be an SMS, an internet-based message on your phone such as “someone attempted to log onto your account at this place at this time – is this you?” or an actual phone call. It will give you a code to enter on your computer to log on. This is two-factor authentication at work.

There are also internet-based phone apps like DuoApp that are even more secure. DuoApp generates a new code on your phone that you can enter into your account, whether you are using a phone or computer. You can also use a USB security key to verify your identity upon login. If a snoop guesses your email password and wants to log on to your email account, you will receive the same prompt, then you can say “no”, and reset your password. You also are then aware that someone is trying to log into your email account.

- **Don't use USB ports without a filter.**

If you charge your phone at a public USB port without a filter, the USB port can download all the information on your phone. A USB filter is a small device that goes into the USB port before the phone is plugged in. It makes sure that the phone only gets electricity from the port, and does not transmit information.

- **Keep machines nearby, do not leave them unattended**

Maintain the physical integrity of all of your digital equipment including computers, tablets and phones. Don't leave them unattended. It would take a hostile actor only seconds to install spyware via a USB port on your machine. Do not let your machine out of your sight. Carry all of your equipment with you at all times. If they are too heavy, switch to lighter machines or leave

some at home. The decision to leave your equipment somewhere will depend on the threat modeling you would have conducted in advance.

Lock the screens when you must leave them momentarily.

Social Media Hygiene Lecture by Instructor

PowerPoint, Slide 6: Keeping Safe on Social Media

Play introduction video lecture, given by Jason Reich: “[Keeping Safe on Social Media](#)” (video)

Social media helps you spread your work and engage with your audience, but social media also attracts harassment and trolling. In some countries, adversaries can follow your social media posts to find out more about you, your location and family.

When you do threat modeling, consider discontinuing the use of social media accounts. If you do need them, then consider the following general rules:

PowerPoint, Slide 7: Social Media Hygiene

Be aware of what you share, and with whom you share it.

Pay particular attention to sharing your location publicly when you are sharing Facebook updates, tweeting or providing a Snapchat map entry. Use the **audience selector** to choose who can view your posts; your audience does not have to be public.

PowerPoint, Slide 8: Security and Privacy on Facebook

Facebook has a list of social media safety how-to’s. Highlights include:

- You have the power to control your presence on Facebook. You can use Privacy Settings to specify audiences for your posts, and use Timeline Review to control what is posted on your timeline.
- Whether you maintain a Facebook Page for yourself or for your newsroom, use two-factor authentication.
- You can use encrypted communication via WhatsApp or Secret Conversations on Messenger to have secure conversations with contacts and sources.
- Manage tagging – decide where you want to be tagged, where you can be seen, and who can tag others in posts. Use [the audience selector](#) to adjust who you share posts with.
- Report harassment – [tell Facebook when you think something violates the Community Standards](#)
- Check your privacy settings – make sure that your personal information is private to the extent that you want it to be
- You can manage how you are tagged in photographs. You can choose to review the photos you are tagged in, and you can remove the tags if you want. The person tagging you won’t receive a notification that you have removed the tag.

- Find out more about security and privacy on Facebook at www.facebook.com/journalists

When encountering harassment, you should:

- Report everything.
- Take screenshots.
- Save the URL.
- If you feel threatened, reach out to local law enforcement.
- If you manage a page, ban people from contributing to the page and hide or block the content.

To guard against account impersonation, you should:

- Make your friends list private so an impostor doesn't reach out to your friends pretending to be you.
- Hide pages you like/follow, so impostors don't have as much material to emulate.
- For the same reason, hide the groups of which you are a part.

Claiming to be another person on Facebook violates its Community Standards. A Facebook team works to detect and block these kinds of scams through special techniques it has developed. Facebook says it continually works to improve this area so users can have a safe experience.

PowerPoint, Slide 9: Scenario One Simulation

You're a journalist using social media to report on local politics. One person frequently makes comments about your "biased" stories, but you leave the comments up to encourage discussion. One day, you post a story about a dispute over a reduction in public transit funding and the person comments with your address explaining that he is coming to talk to you. What do you do?

PowerPoint, Slide 10: Scenario One (cont.)

- Take a screen shot of the comment
- Delete the comment
- Notify employer/security/ police
- Block or ban the person
- Check your privacy settings on social media to make sure personal information is not public

PowerPoint, Slide 11: Scenario Two Simulation

Someone sends you several messages about being a huge fan of your journalism. They message your social media profile and you reply, "Thanks!" Following this, you start receiving messages everyday about how much they love you, their personal life, and when you don't respond, they get angry and start harassing your friends on social media. What do you do?

PowerPoint, Slide 12: Scenario Two (cont.)

- Don't respond and stop reading their messages

- Let your employer know, if possible
- Block the person and report their activity to the social media company
- Check your privacy settings on social media so they can't reach out to more friends or contact you elsewhere

Threat Modeling Lecture by Instructor

Tell students that when they have learned how communication can be intercepted and data compromised, they may want to use all of the tools available to them. But security comes at the cost of convenience, and in some countries, the use of encryption tools can attract the attention of authorities and get journalists into trouble. In some countries, using popular tools that are also encrypted, like iMessage and WhatsApp, can be better than using Signal, which, although acclaimed for privacy, can make one stand out. Besides basic digital hygiene, all other encryption tools are optional, and you should think strategically before you use them. The thinking process is called risk or threat modeling.

PowerPoint, Slide 13: Threat Modeling – Basic Questions

The instructor asks students to share the threat model that they wrote in advance of the seminar and their thought process in making it. If students have picked the same threat or same country, comparing their models can be interesting.

Tell students that there are a few things to consider when it comes to threat modeling in addition to the frameworks in advance reading.

- Are you trying to counter the threat of being targeted by a nation's government versus some opportunist actor who wants to steal your bank information? If you are dealing with a nation, then carefully consider if you can counter these attacks.
- Consider country-specific information – for example, Signal can keep your phone conversations private except in Mexico because the Mexican government uses a spyware called Pegasus. This example is tied into one of Jason Reich's lectures.
- When it comes to dealing with threats, one general guideline is to compartmentalize – don't keep all your information in one place, machine, or account.

PowerPoint, Slide 14: Threat Modeling – Additional Questions

Other things to consider when it comes to threat modeling:

- What kind of footprint are you leaving on the ground? How will your ground activities match up with your available online profile?
- Are you reporting on a high-profile, a middle-profile or a low-profile assignment? If you are on a high-profile assignment, you could attract attention if anything happens to you so adversaries may hesitate before attacking you. If you are low-profile, under the radar, adversaries may not notice you. What is the most dangerous is the middle-profile – adversaries notice you, but you may not have a lot of means to get attention when you are in trouble. Avoid acting on a middle-profile in a hostile environment.

- Make it hard for adversaries to connect the dots – use one phone on a part of the journey and another phone on the next leg so adversaries, even when monitoring your phone, do not have a full track of where you are going.
- Again, it is important to keep in mind that *nothing digital is ever completely safe*. The safest way to get information is to meet face-to-face. All the encryption tools only lower the risks and mitigate danger, they do not prevent it.

Instructor Lecture on Creating a Toolbox

Instructor plays video of Paul Rosenzweig: [Encrypting Communications \(video\)](#)

PowerPoint, Slide 15: Toolbox

WhatsApp and Signal (an encrypted messaging app)

- WhatsApp and Signal both use encryption protocols developed by Open Whisper Systems. They use end-to-end encryption, which prevents interception.
- WhatsApp offers two-step verification. It can be enabled under Settings > Account > Two-step verification > Enable.
- Backup Caveat- in the case of WhatsApp, you or the person you are talking with may backup your conversation on the cloud. So your data may end up in the hands of a third party. Signal does not have a cloud backup option so there's no such risk.
- Signal's Android version has a local backup feature – you can export your messages to a file and then import it in another smart phone. Signal's iOS version doesn't have this feature.
- Note that most phone-base apps will require access to your contact list to function properly.
- Facebook Messenger has “secret conversation” if your source prefers Facebook – it's not automatic encryption as in the case of WhatsApp and Signal. You need to individually set conversations to “secret.”

PowerPoint, Slide 16: Email

Gmail, Protonmail, PGP

- Gmail has automatic encryption that prevents non-government prying eyes. Governments can subpoena your emails.
- Protonmail has its servers in Switzerland, which so far hasn't yielded to subpoenas from any country, so it's a good option as well.
- Caveat: both you and your correspondent need to use the same email service or something with a similar security protocol for the security to work.
- When you can't ensure that both you and your correspondent use the same security protocol, you can use PGP, which stands for Pretty Good Privacy; it allows you to encrypt your email using asymmetric authentication.

Demonstration of the concept of public-private key encryption:

Asymmetric authentication involves a public key and a private key. You can generate public and private keys from several websites. They are pseudo-random numbers that the system uses to encrypt your data.

Here's what you'd want to say to students:

“So when I get a public and private key, it's as if I have a key [show a key], and an infinite number of locks [show several open locks]. The key represents the private key and the lock represents the public key. I can post my public key for anyone to see, and anyone who wants to send me an encrypted message copies my public key- [showing a open lock], and encrypts their message [click the lock]– like locking their own safe with my lock. Once it's locked, even the sender of the message cannot see the original information, only the one holding the private key can open the lock – which is me, holding the private key.”

Check out EFF's page or Mailvelope if you want to learn how to set up PGP

PGP, when properly used, offers strong protection against communication being intercepted in transit. Some experts say it's the most secure means of digital communication. Others warn that private keys can be compromised-unlike messaging tools-or be subpoenaed. But its use can also attract unwanted attention from government and other including criminal surveillance entities.

PowerPoint, Slide 17: Tor: The Onion Routing

Tor browser

History of Tor: Tor is the acronym for The Onion Routing. It was first developed by the United States Naval Research Laboratory, largely funded by the Department of Defense. The aim at that time was to create communications that cannot be intercepted – something for spies. Now it's used by all kinds of people, including the military, drug traffickers, activists, and journalists.

- If you don't want adversaries to know what sites you are visiting on the internet, Tor browser is a good choice. It hides your traces on the internet by bouncing your communications around different points of the internet, so someone watching your internet traffic won't understand where the traffic went, and the sites you visit won't know your physical location.
- Although it's very good, it doesn't keep your browsing activities 100 percent untraceable. The NSA has found ways to track Tor traffic. And the fact that you use Tor can be detected on the network, raising a flag. Don't use Tor on a government computer.

PowerPoint, Slide 18: Virtual Private Networks

- VPN services channel your internet traffic from and to a server that's not based at your location. Some VPN services are designed to only bypass censorship, while others also encrypt your traffic – you would want these if you would like to keep your internet traffic from prying eyes.
- Be aware that VPN does not mask the metadata, and different VPNs use different

encryption methods. You should check out the VPN provider's log policy – what information do they collect about your internet activities? The country of jurisdiction is also important. Pick a provider that's based in a country that's not likely to cooperate with your adversary, especially when your adversary is the government of another country.

PowerPoint, Slide 19: Encryption at Rest

- Play video of Paul Rosenzweig: [Encryption at Rest \(hard drives, USB disks\) \(video\)](#)
- Most importantly – get updated information as to whether the tools you use are still safe at <https://mailman.stanford.edu/pipermail/liberationtech/> (Note: the anti-hacker community consensus on software is simple: if it's no longer safe, don't use it.).

PowerPoint, Slide 20: Scenario Simulation

- **Students' role:** Journalists – can be a group or several journalists acting on their own.
- **Tools:** cards with the words “burner phone”, “smartphone installed with Signal and VPN”, and “laptop installed with VPN” written on them. Each student should have one set of cards.
- **Facilitation:** everyone should install WhatsApp. The instructor should save everyone's number in a broadcast list, everyone should have the instructor's number (the instructor plays the role of the source).

Plot (version for instructor)

Overall Mission: the journalists report in a foreign country, then leave but want to ensure they are protecting the materials they have gathered and their sources.

PowerPoint, Slide 21: Scene 1: In the Journalist's Hotel

Journalist tries to interview a source about Russia in Ukraine. The journalist tries to reach the source. Assume that the journalist is not being physically followed and the authorities only know him/her by digital traces.

Message for the instructor to broadcast to each student via WhatsApp: “I have materials showing the government torturing people. I have a friend who has been tortured, and he agrees to be interviewed on condition of anonymity. We can call or meet. What do you prefer?”

Question to discuss: Should they meet in person or should they telecommunicate?

The journalist should assess the situation, including the country's laws, precedent cases, and security for both the journalist and the source. While telecommunication runs the risk of interception in some countries, meeting a foreign national may be riskier for your source in other countries.

When choosing an app to communicate with, journalists should “blend in.” If journalists in certain countries are one of a few using a certain encryption app, it raises a flag for adversaries.

PowerPoint, Slide 22: Scene 2: Café where journalist & source agree to meet

The source does not show up at the time agreed.

Message to broadcast: “I think we are being followed. Not safe to meet. How about I send you the files on Google Drive? The file is pretty large. You need wifi.”

Talking point: How to send files? Do you use VPN in a public wifi? Talk about things to note when choosing VPNs.

Talking point: Educate your source about cybersecurity up front.

PowerPoint, Slide 23: Scene 3: In the Journalist’s Hotel

Journalist has received the source’s materials, and receives information that they need to leave the country, and they are going to fly out from the airport tomorrow.

Talking point: Encrypt your hard drive, log out from your email, social media, clear your browsing history, and disable passwords and usernames in your browser settings.

PowerPoint, Slide 24: Scene 4: At the Airport

Reporter’s waiting in the airport talking with the source. The phone goes out. There are phone charging portals in the airport.

Talking point: Should you plug your phone in? Don’t charge without USB filter. No charging from unknown computers.

At border control, the journalist’s computer was confiscated.

Talking point: Did you encrypt your computer?

PowerPoint, Slide 25: List of Resources