Infosec 101: Information and Threat Modeling Trainer's Manual - General Defense Committee N... - groups - Crabgrass

Infosec 101: Information and Threat Modeling Trainer's Manual

Trainers manual for Infosec 101 training.

Administration

Training Purpose and Philosophy

This master training document (eg. Trainer's manual) is one half of a training that was originally developed by members of the Twin Cities IWW General Defense Committee Local 14. The original purpose of this training was to address some of the bad habits among members of GDC Local 14 regarding information security during the occupation of Minneapolis's 4th precinct in late 2015, and to present it while still staying true to our organization's commitment to explicit outward organizing, direct democracy, and direct action. This training has since evolved to accommodate general information security practices that any group of beginners could find useful, while more technical aspects have been moved into another training. We also have trainings for marshaling protests, picketing, technology security, and more. To read more about some of the topics discussed in this training, please see the cache of reference materials available. To hear more about our other projects, please visit us at https://www.facebook.com/TC.GDC/, http://twincitiesgdc.org/, or contact us at tc-gdc@iww.org.

While it's true that there are lots of specific infosec/tech trainings out there, but this one fulfills a particular niche in both its audience and its political orientation. This training has been written in a way that is encouraging of action over absolute security, and is written to address a crowd that may not be into cryptographic-lifestylism. I realize that a lot of interest in "tech security" really comes that crowd – people really interested in the form of cryptography and novel concepts regarding data, and perhaps advancing these ideas, but not particularly interested in the functional work of this: organizing resistance. It's not that advancing our ideas isn't important, but the purpose of this training is not to address this lifestyle crowd, but rather those who are actively organizing resistance on a grassroots level. Similarly, since this training is written for a mass-movement orientation, some of the specific types of security that you can really only address in cadre style or affinity group organizations isn't really well developed in this training, and I think might need their own module or perhaps training to address.

Housekeeping and how to implement the training:

Good trainings do not occur by accident, and good planning makes for good experiences. Keep in mind the following:

- Find a space: A free space you can reserve for the entire length of the training with tables, chairs, power strips, some kind of whiteboard/presentation system, and other smaller amenities.
- Consider the context of the event: Is the space you have friendly to this kind of training? Do the attendees have an appropriate political and technical background?
- Consider attendance: advertise on multiple platforms (social media, word of mouth, email lists, etc). Will you have enough participants to make the event worthwhile?
- Consider time: You may need about 3 hours to complete this training.
- Consider the needs of your participants and hurdles for them to come to the event: Does the event need childcare? Will you have enough refreshments for the participants? Do you need to arrange transportation? Do you need computers?
- It may be appropriate to collect donations or secure funding to cover the costs of the event.

Abstract and Promotional Materials

For use in promotional materials:

GDC Infosec 101: Information Security and Threat Modeling
The GDC Information Security and Threat Modeling training (the 101 section of the information security training) was developed during the occupation of Minneapolis's 4th precinct in late 2015 in order to address some bad habits among members regarding information security while still staying true to our organization's commitment to explicit outward organizing, direct democracy, and direct action. The Infosec 101 was designed to be accessible to those who are not computer-literate, and does not require participants to bring computers. It includes sections on security culture, threat modeling, postmortems, and the theoretical side of encryption. After the training, participants should have a solid understanding of why we use security culture, and how to build, grow, and implement policies appropriate for whatever threats they face.

Vocabulary Words

As a trainer, try to emphasize these words when explaining concepts:

Security Culture – Security Culture is a set of customs and practices for those engaging in sensitive activity which minimizes the risks inherent to those activities.
Data – Data is an abstraction of information that needs interpretation.
Meta-Data – Meta-Data is data about data.

Vector – A **Vector** is a avenue of exploitation or attack.
Social Engineering – A vector that relies on human interaction.
Threat Modeling – Threat modeling is a process by which potential threats can be identified, enumerated, and prioritized – all from a hypothetical attacker's point of view
Attack Tree – Attack trees are conceptual diagrams showing how an asset, or target, might be attacked.
Postmortem – A postmortem is a reference, either spoken or written, made after an action to determine and analyze elements of the action that were successful or unsuccessful, created for use in future planning.
Encryption – Encryption is data that is written in such a way that only authorized parties can interpret it.

Time Guide

Write these on the corner of the whiteboard:

+0:00 Introduction
+0:15 Data & Security Culture
+0:30 Vectors
+0:50 Attack Trees & Threat Modeling
+1:40 Break
+1:50 Postmortems
+2:00 Encryption & Passwords
+2:45 Applications
+2:50 Review and Feedback

Intro

Introductions – 5 Minutes (0:00)

Begin by introducing the Industrial Workers of the World (and maybe Work People's College?), the General Defense Committee, and our philosophy (particularly around explicit outward organizing) and purpose for this training. Then go around the room and introduce everyone, starting with the trainers. Everybody should give their name and pronouns, group affiliation(s), and how/why they came to this training.

If anybody genuinely feels that the deep state is directly going after them, let's save that talk for after the training. We can get you to the Ecuadorian embassy for asylum, but most people aren't operating under that threat model. Let's not focus our whole training on threats from the deep state.

Policies – 5 Minutes (0:05)

Read as a group:

IWW Safer Spaces policy:

The Industrial Workers of the World is a union committed to the emancipation of the working class. The working class is diverse, and as a union we recognize that oppression is many layered. As such, we strive to keep our common places free from oppressive action, behavior, and language. If anybody feels harassed, unsafe, or otherwise impeded from participating in this training by any such behavior or action, they are encouraged to discuss the matter with either the offending party or the trainer, either by themselves or by proxy. If the behavior does not improve, trainers may ask the offending party to leave.

Tech Space Guidelines:

The GDC 14 tech/infosec working group is made up of nerds, and as nerds talking about the things we're passionate about, we recognize that nerd culture is not always welcoming to newcomers. We strive to make this training as constructive and inclusive as possible. Try to keep these guidelines in mind during this training:

Do collaborate: There is more information on every level to share than a single teacher could ever give, and working together is the best way to share knowledge. This is different from a blanket "there are no wrong answers", but more related to "the best answers come from working together".
Do learn by action: Poking around is really the first method to get a foothold, especially when you feel lost. If you make a mistake, others are here to help.
Do NOT shame others or feign surprise: We all started somewhere, and we need to focus on creating a constructive culture instead of a culture of competition with your fellow defenders.
Do NOT "um, ACTUALLY…": Constructive suggestions are okay, but one-upsmanship without recognition of prior work or explanation behind your criticism is not constructive.
Do NOT blurt out answers: Ask if someone needs help first, and become part of the process instead of handing out an answer.

Introduction and Security Culture

Experiences – 5 Minutes (0:10)

We strive to make our trainings as interactive and tailored to the recipients as possible, so asking your audience what they need and what they are familiar with can really help address this common oversight.

Ask: Has anybody in this room had some level of understanding with any of the following (raise your hands)

- Security Culture
- Threat Modeling
- Social Engineering
- Strong Passwords
- Encryption
- Cell Phone Security

Ask: Does anybody have any deeper relevant knowledge to information security? What is it that people hope to learn from this training?

What is data? What is meta-data? – 5 Minutes (0:15)

Read: One of the primary goals of this training is to give everybody the knowledge and tools that they need to be able view their situations in an abstract way, then analyze and improve their own methods for controlling information. In order to get a baseline for this, we need to ask the question of "What is **data**?".

Take questions and shape the conversation: Data is an abstraction of information that needs interpretation. Meta-Data is data about data (who? where? when? how?) that can sometimes be just as important as data itself. How does this relate to the concept of information security?

What is Security Culture? – 10 Minutes (0:20)

Situational awareness is key in all sensitive contexts, and information security is no different. Security Culture is a set of customs and practices for those engaging in sensitive activity which minimizes the risks inherent to those activities. Security culture is NOT a set of practices that prevent activity from occurring in totality, and security culture is NOT monolithic in nature. Building security culture is always about addressing the question "Can we do this better for our current situation?". Good security culture is acutely aware of the points of interest it needs to protect, and adjusts the practices and behaviors of all involved appropriately to the threats currently faced by the group.

Ask and take examples from the group on

1. Relaxed or smooth experiences with good security culture – eg. When we say don't talk to cops, it's easy to

remember, and beneficial.
2. Rough or near miss experiences that good security culture saved you from – eg. I told my friends not to talk to cops when they were about to, and it saved us from being arrested.
3. Bad experiences with badly designed or implemented security culture. – eg. Somebody said we can't talk to anybody we don't already know when we're organizing a canned food drive. It was inappropriate.

Trainer note: The question of "how do we develop these practices for our activities?" will be addressed in the threat modeling section – introduce the concept as an adaptable and fluid system.

Sometimes having strong group procedures, protocol, or bylaws can prevent group drama and set the tone for your security culture – particularly around membership joining and leaving. If this training is not for a GDC group, this may be even more important to discuss.

Vectors and Social Engineering – 5 Minutes (0:30)

A **Vector** is a avenue of exploitation or attack. Not all vectors need be physical – many are explicitly social, and we call these vectors **Social Engineering**: eg. "Why pick the lock if they'll open the door for you?".

Ask: Does anybody have any good stories about social engineering? How do you get information out of people when they don't necessarily want to give it to you?

Trainer note: Teaching people how to use social engineering is a topic covered in the 102.

Persistent Vectors – 15 Minutes (0:35)

We are all only human: we all have wants, needs, and networks to support our every day lives and activities. What are some persistent threat vectors we need to be aware of in general, and how much resources would someone need to discover/exploit them? Who would be harmed from exploits like this?
Take suggestions from the group and STAY GENERAL.

Ask: How many of you have: (raise of hands)

- A Public Facebook Account
- A blog or journal
- Have ever had a personal website (re: both whois and internet archive)
- A LinkedIn
- Info on a school/university site

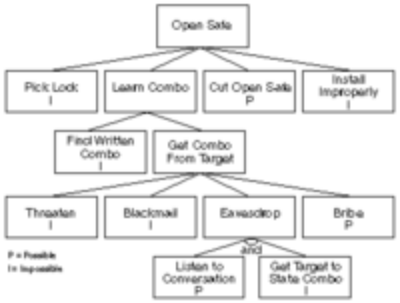
Certain information may not seem like an issue at first, but a concerted social engineering campaign can actually be very effective at hampering the activities of the target. Naiveté about how these campaigns work is a serious problem, and it's an important to be able to put yourself in the mindset of an attacker completely uninterested in following "the rules", be they legal, social, or anything else. It's not that these campaigns exist outside of morality, but their general functioning places the contempt for the target above these other systems. The methods in targeted harassment isn't always necessarily a bad thing either: sometimes these campaigns can target bad groups like Chanology targeted Scientology, but the exact same tactics can be used against innocent groups like #gamergate (a precursor to the fascist alt-right movement) targeted women in games and tech.

The Crash Override network was created by a female game developer as a defense center for women and feminists during the #gamergate campaign, and have a lot of resources for people looking to prevent and people already facing targeted harassment, especially online. One of the most common and low effort methods of attack is called doxxing, and it works by digging up skeletons in the closet/exposing any personal information publicly in a way that could be seen as, but does not legally constitute threatening. There are many massive data-broker firms that collect this information on everybody in the north america, and removing yourself from these sites can prevent attacks before they happen. Crash Override has many excellent deeper pieces on preventing doxxing and how to reclaim your data from data-brokers, and I would highly recommend looking into them.

As a rule of thumb even beyond the public eye, we should only be keeping data around as long as it's relevant – how that is applied is up for you to decide.

Attack Trees – 10 Minutes (0:50)

Shifting gears: Imagine you are an attacker, and you want to get at an item stored in a locker somewhere in public. What vectors could you use to get this item?
Take suggestions from the group on all the ways you could get into this safe, from the simplistic to secret agent level.
Now write them all down in a tree with the safe entry at the top, and each vector listed as a sub item in the tree, with all relevant equipment and work as sub-sub items.



Then, pretend that you are:

1. A well meaning but snooping family member
2. An Internet troll
3. A common burglar level adversary
4. A committed and skilled fascist
5. The Police
6. The NSA/CIA/“State Level Actors”

Using different color markers here is helpful!

Discuss: Which of these methods make the most sense given the time, resources, and potential backlash involved upon failure when each of these groups are the attackers using these vectors? Not every action will upset all of these groups in real life obviously, but this should illustrate the differences between different levels of threat.

How to build a threat model – 5 Minutes (1:00)

Building one tree is great, but if we are to model our actions and find the ways we need to be careful about what we’re doing, we need to build an overall system that addresses these questions. You probably won’t have to do this exhaustively every time, but if there is disagreement in your group about what your security culture should look like, writing it out should help guide you to an appropriate model for the actions you are taking.

1. Create a plan, and list items/structures/systems to be protected
2. List reasonable attackers
3. Create an exhaustive attack tree for these items
4. Apply these attackers to the tree, and rate the feasibility of these attacks.
5. Rate the inherent risks and payoffs of this plan overall.

6. Repeat for other plans, and compare and contrast plans of action.

Read: Remember: It's foolish to assume you can hide from or win against the highest levels of the state, and basing your security culture around this is going to be a hamper on your overall effectiveness as a group. Stay realistic for what threats you face, and focus on taking action!

A short primer on cell phones – 5 Minutes (1:05)

Read as a group: Lots of scary things have been both written about and done to cell phones before, and we want everybody who takes this training to be aware of what these things are. We include this section not to prevent action, but to shape action in a way that keeps people informed and operations secure. Action is better than inaction, and as always, at the end of the day, having and building comrades within a vibrant social movement that have your back is more effective than a paranoid security culture. Strong relationships fight power in ways that physical tools can not, and security culture alone cannot defend on every front or make powerful actions lasting and relevant.

All that being said, consider the following:

If your phone was stolen today, what would that mean to you? Some of the things your phone probably has on it locally right now include (but are definitely not limited to):

- Statistically speaking, a weak password or no password on your lock screen.
- An extensive collection of your communications via email and text message.
- A record of phone calls you have made.
- Your internet history.
- Accounts that are already logged in to websites, and whatever data may be on those accounts.
- Personal photographs you have taken.
- Possibly GPS coordinates of where these photos were taken.
- A record of locations you have been when searching for things in your GPS.
- Possible credit card information.

Some of the things that can be accessed by attackers with vast amounts of resources (such as when the state is agitated and/or prepared) may include:

- Possible retrieving of data stored on your phone that you have deleted.
- Meta-data of texts and emails you have deleted via cell tower records.
- A record of where your phone has been via triangulation of cell towers, a GPS signal being recorded and reported, or other methods.

- The ability to power on or off your phone, sometimes even for a short while to send out location if the battery is removed.
- The ability to record audio and video from your phone at any time.
- The ability to identify your phone and intercept any data coming from or going to your phone if there is a fake cell tower.

Again, this isn't meant to scare you, but rather to make sure that the threats that cell phones represent to our privacy and security are accurately represented. Remember: sometimes meta-data can be just as important as data itself, so please keep all of this in mind when building threat models. If any of these warnings are serious concerns, maybe moving away from phones is a good idea. And finally, always be aware of the information you're recording, whether that be audio, video, text, or anything else! No scheme to protect that information is perfect!

Assessing Plans of Action Activity – 30 Minutes (1:10)

THIS IS THE MOST IMPORTANT PART OF THE TRAINING

Exercise: Operational security is more important than technical security, even though it's less exciting to talk about. Learning how to build an appropriate threat model for scenarios that you face is the most important part of this training and should not be overlooked! Good security culture starts here.

Now that we have a way to systematically create threat models, let's practice on one or two of the following generic situations, all of which are based on situations GDC 14 has actually dealt with in the past. Your trainer will select which ones you will work on in your small group. Think like an attacker, and remember the steps to building a threat model!

1. Your group learns of a public social event of high class right wing intellectuals, business leaders, and other community leaders (possibly law enforcement and political figures). It is a dinner party with a $25 entry fee plus food and drinks sold individually. The event will be held in a venue normally reserved for wedding receptions. What action do you take, and how would you prepare?
2. Your group learns of a house show featuring one out-of-town, explicitly neo-nazi band as well as two other local bands which are seemingly apolitical. Your group has a few members in this particular music scene. What action do you take, and how would you prepare?
3. We are planning a rally and picket of a city-owned store where a marginalized person was recently murdered by police, as a way to hurt the city financially. We have gotten word that a far right group is threatening to attack your event. You expect 150 people or more to attend your action. How do you prepare for this action?
4. Your group is planning a speaking event about a recent struggle at a friendly venue. There have been attempts by far right elements to disrupt your activity and there are rumours that they are planning to do so here as well. You are expecting 30-40 people to attend your event, and there is one entrance to the venue. How do you prepare?

5. Your group is planning to disrupt a public event of a far right wing speaker. A pacifist group is planning a rally outside the venue and are expecting 50 to 100 attendees. Another activist group in town is also planning to disrupt the event and have told your group not to show up. This group is notoriously difficult to work with, are often unwilling to hear criticism from outsiders, and individual members of this group have threatened members of your group with violence. You also expect for police to be heavily present. How do you defend your disruption, and how do you prepare?

The next two pages in this manual have space to work these scenarios out!

After the exercise: on an organizational level, it's also important to have protocol or plans to respond to actions or reactions you have not foreseen. Much of this kind of response modeling is more throughly explained in our marshal/direct action training, but it is important to note here.

Break Time – 10 Minutes (1:40)

Trainer note: Give a 10 minute break.

Postmortems – 10 Minutes (1:50)

If we don't learn from our mistakes or recognize our successes, our organizations are doomed to failure. A debrief meeting should be set up as part of planning actions, and a postmortem should come out of them. A postmortem is a reference, either spoken or written, made after an action to determine and analyze elements of the action that were successful or unsuccessful, created for use in future planning. Postmortems are best done by those who participated in the action, and done soon after the action was completed.

Take questions and shape the conversation: If keeping a record, what parts of an event should we record and which ones should we get rid of?

Depending on your threat model this advice may change, but as a general rule of thumb, do not retain anything in your report that you would not like to hear repeated back to you in a court of law, or anything unique that could be used as a direct vector against you or comrades. Keep relevant information that could be useful as a learning tool – the point of a postmortem is to inform future actions and iterate on techniques and tactics, not be a grand unedited history of everything you've ever done in your life.

Take questions and shape the conversation: What should a good postmortem have in it?

Generally, a good postmortem should have:

1. A relevant title and an abstract overview, no more than a few sentences.
2. Situation: What was the situation/opposition's intent, and what was the plan of action?
3. Intelligence: What relevant info and techniques were studied and discussed prior to the action?
4. A summary of events
5. Discussion of key issues
6. Skills to be improved upon
7. Lasting/unresolved issues
8. Closing Comments

Exercise: Do a hypothetical verbal postmortem with your partner over one of your planned actions. Don't let it be all sunshine and rainbows though!

Encryption

What is encryption and what makes for good encryption? – 10 Minutes (2:00)

Ask: Does anybody have a good definition of encryption? Remember: Data is an abstraction of information that requires interpretation.
Encryption is data that is written in such a way that only authorized parties can interpret it.

Take questions and shape the conversation: Not all encryption is created equal though. What are some qualities of good encryption and implementations of encryption that separate it from bad encryption and bad implementations?

Generally, we can ask:

1. Can they find it? The message should be available for those who need it, yet difficult to find for those who seek to intercept it. (Obfuscation, Secret Sharing)
2. Does a message even exist given a blob of data? Or is this just random jibberish laying around? (Deniability)
3. What can they find out about the circumstances of this message? It ought to be difficult to glean information about the purpose of the message, including sender/receiver, date/time, etc. (Metadata encrypted or removed)
4. What does the message say? It should be very difficult to glean information from the message itself. (Strong Cryptography on the Data, Strong Passwords)
5. Is it tamper proof? If intercepted by an adversary, the message should be hard to tamper with and replace. (Signing, asymmetry)

Very strong cryptographic protocols exist, but in the real world, often times many of these methods falter due to shoddy implementation. What kinds of bad implementation could we imagine for each of these qualities?

Strong Passwords and Password Guessing – 25 Minutes (2:10)

THIS IS THE 2ND MOST IMPORTANT PART OF THE TRAINING

The first point of entry to any kind of encryption breaking is generally the password. Having a strong password is essential if you expect your data to be secure. Again, this is not very exciting to talk about, but it's essential and should not be overlooked.

Take an attacker's perspective: It's possible to try and type in all possible passwords up to a given length, but beyond 12 characters or so, this becomes very expensive in resources. However, most human beings don't use completely random passwords – they make passwords from a human perspective. There are lists of human readable words out there that are far more common than random strings of letters, and more often than not, passwords contain personal information related to the user.

A good password should have:

- 12 or more characters
- Both lower and upper case letters
- Numbers
- Special characters (punctuation)
- No human readable words
- No common substitutions for human readable words (pa55word)
- No easily obtained personal information (date of birth, pet/maiden names, etc)
- No easy keyboard pattern (qwerty) or repetition
- One use: no reused passwords
- Multiple factor authentication (if possible)

Exercise: Check haveibeenpwned as a group. Know that your password, either hashed or plaintext, may be floating out there in the internet while connected to your email/username/other login credentials. Not every site has the best security, and all it takes is that one instance if you use the same password.

All of this may seem very overwhelming, and that's because by definition a good password runs contrary to typical human behaviors. Don't fret however! That doesn't mean there aren't trick methods to make and remember good passwords! The three most common methods to make and remember good passwords are:

- Mnemonic/Reduction Function (personal favorite) – Pick a specific phrase that you will remember, and then reduce it to a combination of characters by specifically choosing parts of them. “It’s 12:30 PM. I am getting hungry!” could be reduced to:

  ```
  "I1230P.Iagh!"
  ```

  Foreign language speakers can use non-english constructions as well! Salting your password with a few letters somewhere from the site you’re using it can prevent reused passwords, like

  ```
  "I1230P.Iagh!"goo
  ```

  for google.
- Passphrase/Diceware – Diceware is a method of creating a password by rolling dice, and then using the numbers that you rolled to look up words in a table of words. The passwords (or in this case “passphrases”) created by this method are generally easy to remember, virtually immune to brute force attacks, and sufficiently strong to resist dictionary attacks when done correctly. The only reason this is not my preferred method is that some very bad websites do not allow passwords longer than 32, 16, or sometimes even 8 characters, making this difficult. Salting is also an option with this method.
- Password Lockers – A password locker is a program that uses a master password to create a list of passwords for different uses that you can always look up. The downside is the clear point of entry at the master password, but if you have many accounts you need to remember passwords for, this can be a useful way to generate strong and unrelated passwords for the paranoid.

Use 2 factor authentication if supported!

Exercise: List common places people use passwords, and make people solemnly swear to use good passwords and change all their current passwords.

Common encryption methods – 10 Minutes (2:35)

Beyond passwords and logins, there are a lot of common applications of encryption that you may not see. When you know you need it though, there are a few different encryption tools that I would recommend for different uses:

Symmetric

Symmetric encryption uses one password for both encryption and decryption of data. The support for some of the other good cryptographic qualities beyond “strong cryptography” may be mixed or limited.

- Files and volumes – 7Zip is a file compression tool (like a zip file) that has support for encryption. It's not very good with metadata, as you can see all the files and their sizes, but for many purposes, the ease of use factor trumps over the more specific "encrypted volume" projects like Veracrypt. Veracrypt would be the next suggestion if you need something even more secure.
- Full Disk – LUKS is a standard Linux encryption tool to encrypt your entire hard disk so that you need a password to log into it when you turn it on. Veracrypt can do this for older versions of Windows – some new editions of Windows and iOS have this built in. I usually have this option as standard, because once you do it, it's out of the way, and it's not particularly invasive. Newer versions of android have LUKS.

Public key

Public Key encryption is a complex approach to cryptography to implement almost all of the features we discussed earlier. It uses different "keys" for encryption and decryption, and provides a way to verify you are sharing messages with someone that you mean to. The exact workings of public key encryption are beyond the scope of this training, but if you are really interesting in knowing more about them and how to use them, I would suggest you take the Information Security 102 training.

- Email – PGP/GPG are methods to encrypt and decrypt messages over email. They are however, difficult to use even in 2016, and there is a large cultural adoption problem. If you need secure email though, this is the way to go. Trusting centralized systems like lavabit is difficult because they always end up as targets. Protonmail is also supposedly end to end, but all keys are still centrally managed.
- OTR – OTR was based on PGP, and is public key encryption over generic messaging protocols. It's also hard to implement for the average user, but it exists if you need it.
- Signal – Signal was based on OTR, and is the recommended public key encryption messaging platform of choice. There are a lot of design elements that are intuitive and easy to understand for the average user, it encourages cultural adoption by being a simple replacement for text messaging, and having it contained to one app that needs very little configuration makes installation painless and a low bar of entry.

Refrain: Encryption is not a magic bullet

Remember the attack trees? Certain types of attacks can be prevented by using strong encryption, but not every attack. If your attacker can look over your shoulder as you're typing in your password, or steal your cell phone while it's open to read your emails and texts, no amount of encryption will prevent those kinds of attacks. Knowing the length you need to go to balance usability and protection will only be brought to you though the use of appropriate threat modeling. This also needs to intersect with our political orientation of explicit outward organizing.

Applications – 5 Minutes (2:45)

Read as a group: Now that we have a base understanding of security culture, data, meta-data, threat modeling, encryption, and more, it's okay to make some recommendations for tools appropriate to this level of understanding. Many more tools exist, but these are aimed at those new to information security or those who don't have the time or understanding to be able to play with tools all day.

As per standard with recommending software, this is the most up to date information as of v1.0 of this training (Feb 2017); those looking for recommendations in the future are encouraged to read up on any changes made to these projects or projects like them since this list was made.

Browser Plugins

- HTTPS Everywhere: This plugin sets the default data transmission in your browser to use TLS encryption if the website supports it.
- uBlock Origin: This low profile and efficient adblocker helps prevent intrusive and deceptive advertisements from getting in the way of your browsing.
- Privacy Badger: A more sophisticated blocker designed specifically to learn which connections are tracking you, and prevent them from accessing your machine.

Replacements for Common Applications and Services

- Google Search → DuckDuckGo/Disconnect.me: DuckDuckGo gives you free, anonymous, unlogged web searches. Also has a very good "bang" search feature to automatically go to other search engines. Disconnect.me is a go-between (proxy) for multiple search engines.
- Gmail/Hotmail/etc →Riseup/openmailbox/ProtonMail/Autistici: Email is notoriously complex, and hosting your own server is beyond the scale of even many tech savvy people. Riseup, openmailbox, ProtonMail, and Autistici all have free accounts with varying degrees of privacy and security attached. Others exist as well – these are just some of the most popular alternatives.
- Text messsages→Signal Private Messenger: Signal uses public key encryption for text messaging, and is well known for being user friendly. Highly recommended.

Advanced Users

There are LOTS of more advanced tools out there, but how these work is beyond the scope of this training. If you're interested in really digging deep into information and technology, here are a few interesting points to jump off at:

- uMatrix/NoScript: Advanced firewalls for your browser, with many privacy-enhancing tools.

- PGP/GPG: Public Key encryption for email.
- TOR: An encrypted “onion routing” network designed to provide anonymity, more powerful and robust than proxy servers.
- Freenet and GNUnet: Both projects were designed to shift the web away from the client-server paradigm and into a more complex peer to peer topology.
- TailsOS: An entire live operating system designed with privacy in mind, to be carried around with you on a flash drive and used when a secure OS is necessary.
- Yubikey: A physical usb encryption key.

Conclusion

Review – 10 Minutes (2:50)

Participants fill out review sheet with neighbors, and bring back the questions. Recall our definitions:

Security Culture – Security Culture is a set of customs and practices for those engaging in sensitive activity which minimizes the risks inherent to those activities.
Data – Data is an abstraction of information that needs interpretation.
Meta-Data – Meta-Data is data about data.
Vector – A **Vector** is a avenue of exploitation or attack.
Social Engineering – A vector that relies on human interaction.
Threat Modeling – Threat modeling is a process by which potential threats can be identified, enumerated, and prioritized – all from a hypothetical attacker’s point of view
Attack Tree – Attack trees are conceptual diagrams showing how an asset, or target, might be attacked.
Postmortem – A postmortem is a reference, either spoken or written, made after an action to determine and analyze elements of the action that were successful or unsuccessful, created for use in future planning.
Encryption – Encryption is data that is written in such a way that only authorized parties can interpret it.

Survey (3:00)

Please take some time to fill out and return surveys! The more notes we get about this training, the better we can make this for next time.