GDC Infosec 101: Information Security and Threat Modeling

Twin Cities Industrial Workers of the World General Defense Committee Local 14
Tech/Infosec Working Group
Version 1.1.1

0x00000000acab

What is this training?

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.

GDC Local 14 also has trainings for marshaling protests, picketing, copwatch, technology security, and more. 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

What is the IWW,? What is the GDC?

The General Defense Committee (GDC) is a body of the Industrial Workers of the World (IWW), a revolutionary anti-capitalist labor union founded in 1905. The early IWW was the first major union to welcome unskilled workers, women, and people of color into non-segregated locals. In 1917, the General Defense Committee was established to defend members of the IWW facing legal persecution for their beliefs and organizing. Today, the mission of the GDC has expanded beyond legal defense of members, and toward a more broad defense of the working class through community organizing and direct action.

The Twin Cities IWW General Defense Committee Local 14 has been active in political education, restorative justice for survivors of sexual assault, working in the police abolition and anti-fascist movements, and more.

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 infosec/tech 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

What makes this training relevant? What do you and others hope to learn?

What is **data**, and what is **meta-data**?

What is **security culture**? How does **security culture** help guide our actions?

What are some examples of good and bad security culture?

For further reading on social engineering: www.social-engineer.org/framework/general-discussion/

What is a v**ector**?

What is **social engineering**, and what are the core aspects of it? What is **elicitation**?

What are some persistent vectors we need to be aware of?

What is doxxing?

For further reading on online harassment:
www.crashoverridenetwork.com/resources.html

Attack Trees

Imagine you are an attacker, and you want to get at an item stored in a locker somewhere in public with an electronic lock. What **vectors** could someone use to get this item?

Build your **attack tree** (start with the physical item):

Who could want this? How do different adversaries approach this?

For further reading on attack trees: www.schneier.com/academic/archives/1999/12/attack_trees.html

Threat Modeling

What is a **threat model**?

How do we expand our attack trees concept into a **threat model**?

1.

2.

3.

4.

5.

6.

Remember: It's foolish to assume you can hide from or win against the highest levels of the state alone or with your small action group, and basing your security culture around this and/or every worst case scenario you can imagine is going to be a hamper on your overall effectiveness. Stay realistic for what threats you face, remember why it is that you do what you do, and focus on taking action over inaction!

A Very Short Primer on Cell Phones:

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

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 six 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!

Plan for Scenario ___

Plan for Scenario ___

After Action Reports

What is an **after action report**? Why are they helpful?

Should we keep them as written documents?

What elements should a good after action report have in it?

1.
2.
3.
4.
5.
6.
7.

8.

Encryption and Passwords

What is **encryption**? Recall the definition of **data**.

What are some qualities of good **encryption** or good implementations of encryption?

How can some of these qualities be implemented poorly?

Why are **strong passwords** important? What makes for a **strong password**?

Check https://haveibeenpwned.com/ as a group! How many of us have been breached?

Making a good password by definition runs contrary to typical human behaviors! There are 3 main ways to make **strong passwords**:

Mnemonic/reduction function + salt:

Passphrase/Diceware + salt:

Password Lockers -

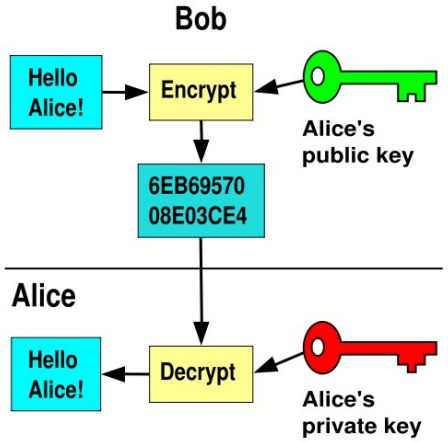
Where do you personally use passwords? Where do you need them changed?

I, _____, do solemnly swear to change my passwords to strong passwords, not to reuse them, and to be careful with letting them out. I understand that passwords are often the

first point of attack, and having strong passwords is perhaps the most important thing I can do to protect my encrypted data.

What is symmetric encryption? Where might we use it?

What is public key encryption?



Where might we use public key encryption?

Why is **encryption** not a magic bullet? How does this intersect with our mass orientation?

For further reading on public key encryption: ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp

Applications

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 v1.1 of this training (June 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, with a useful "bang" search feature to automatically go to other search engines. Disconnect.me is a go-between (proxy) for multiple search engines, including Google.
- 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.
- VPN: A "go-between" for your internet connection. Riseup email accounts can use a free VPN.
- TOR: An encrypted "onion routing" network designed to provide anonymity.
- 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 for multi-factor authentication.

For further reading on these and for a list of other secure projects: prism-break.org

Review

Speak with your neighbor and throughly answer these questions together in conversation. Write down further questions to ask the trainers about these topics if you have any!

What is **data**? What is **meta-data**? How does **encryption** relate to this?

What is a **vector**? What is **social engineering**? What is **elicitation**?

If there is a disagreement on the appropriate policy to implement as **security culture**, how can we resolve this?

How can **after action reports** inform future action? Should we keep them around?

Do you feel comfortable making a **strong password**? Are you going to change all your passwords?

Flip back to page two: were your initial questions answered? Do you have any other burning questions?

HTTP Error 204: No Content

[This page intentionally left blank.]

Evaluation	
What was your favorite part of the training? Why?	What was your least favorite part of the training? Why?
What was your favorite activity? Why?	What was the most difficult part of the training? Why?
In what sections could the trainers improve their knowledge?	In what ways could the trainers improve their teaching techniques?
Any final comments?	

Thank you for taking the time to provide us with valuable feedback. We hope this training was both entertaining and

enjoyable, but most of all, we hope you will join us in the work of organizing the defense of the working class!