DSA Cybersecurity Workshop Worksheet - Part 1 - Dec 3, 2024

Security Mindset

Key Principle: Security is a process, not a product.

> Think of cybersecurity as a continuous cycle of assessing threats, implementing safeguards, and adapting to new challenges. It's not a one-time fix or a software solution you can buy and forget. The digital world constantly evolves, and your security measures must keep pace. Regularly updating your software, changing passwords, and staying informed about new security threats are all part of this ongoing process.

Action Items

- **Create strong, unique passwords for all accounts.** Consider using a password manager (Bitwarden or 1Password).
- **Enable two-factor authentication (2FA) wherever possible.** Use an authenticator app (Aegis or OTP Auth) for TOTP codes.
- **Compartmentalize your online activities.** Use different browsers for different purposes.
- **Install Ublock Origin** to block ads/malicious scripts, and **restart your phone regularly.**
- **Regularly review and update your security practices.**

Personal Security Plan

Threat Modeling

> **Definition:** Threat modeling is a structured approach to identifying, assessing, and mitigating potential threats to your digital assets and personal information.
> **Purpose:** To gain a clear understanding of your cybersecurity landscape and prioritize your security efforts.
> **Key Questions:**
>
> - What assets/data are worth protecting?
> - Who are the potential attackers?
> - What is the likelihood of an attack?
> - What are the potential consequences of a security breach?
> - What level of inconvenience am I willing to tolerate to enhance security?
> - Who and what can be trusted?

1. What assets/data are worth protecting?
    - **Devices:** Smartphones, laptops, tablets, smart home devices, etc. Consider the data stored on each device and its potential value to attackers.
    - **Personal information:** Social Security number, financial data, addresses, phone numbers, medical records, etc. This information can be used for identity theft, financial fraud, or even blackmail.
    - **Important files:** Photos, documents, videos, etc. These files may hold sentimental value, contain sensitive information, or be used for extortion.
    - **Online accounts:** Email, social media, banking, shopping, etc. Access to these accounts can allow attackers to impersonate you, steal your data, or spread misinformation.
2. Who are the potential attackers?
    - **Law enforcement/government agencies:** May target activists, journalists, or individuals deemed a threat to national security.
    - **Malicious individuals:** Motivated by personal grudges, financial gain, or the desire to cause harm.
    - **Organized attackers (with resources and motives):** Cybercrime groups, hacktivists, or even foreign governments.
    - **Tech companies (and their potential ties to government agencies):** May collect and share your data without your consent or be compelled to hand it over to authorities.
3. What is the likelihood of an attack?
    - Consider your online activities, affiliations, and the sensitivity of your data.
    - **Example:** If you regularly participate in online activism or handle highly sensitive information, you may face a higher risk of targeted attacks.
4. What are the potential consequences of a security breach?
    - **Doxxing (public release of private information) and harassment:** Can lead to reputational damage, emotional distress, and even physical harm.
    - **Financial loss or identity theft:** This can result in significant monetary losses, difficulty obtaining credit, and damage to your financial reputation.
    - **Legal repercussions or arrest:** May occur if your data is used for illegal activities or if you are targeted by law enforcement.
5. What level of inconvenience am I willing to tolerate to enhance security?
    - Consider the trade-off between convenience and security.
    - **Example:** Using a password manager may be slightly less convenient than reusing the same password everywhere, but it significantly improves your security.
6. Who and what can be trusted?
    - Evaluate the trustworthiness of individuals, organizations, and online services.
    - **Example:** Consider the privacy policies of online services, the security practices of organizations you interact with, and the trustworthiness of individuals you share information with.

Exercise: Reflect On Your Threat Model

- **List Your Digital Assets:** Take an inventory of all your devices, accounts, and types of sensitive information.
- **Identify Potential Threats:** Consider who might be interested in your data and what their motives might be.
- **Assess Risk Levels:** Determine the likelihood and potential impact of each threat.
- **Prioritize Security Measures:** Focus on the most critical assets and the most likely and impactful threats.

Don't worry if you're not completely sure, we'll be covering threat modeling more in-depth in a future workshop!

Commonalities in Everyone's Threat Model

- Secure Authentication/Authorization
- Compartmentalization: Separation of Contexts & Identities
- Defense Against "Drive By" and "Watering Hole" Malware

1. ## Secure Authentication/Authorization

Passwords:

- The first line of defense for your accounts.
- **Characteristics of strong passwords:**
  - At least 12-16 characters long
  - Mix of uppercase, lowercase, numbers, and symbols
  - Unpredictable and not based on personal information
  - Unique for each account.

Password Managers:

- **Purpose:** To generate, store, and manage strong passwords.
- **Benefits:**
  - **Convenience:** Automates password generation and entry, reducing the need to remember complex passwords for each account.
  - **Security:** Enforces strong password practices, making it harder for attackers to guess or crack your passwords.
  - **Organization:** Centralizes password storage, eliminating the need for multiple spreadsheets or sticky notes.
  - **Simplicity:** Requires remembering only one master password to access all your other passwords.
- **Recommendations:**
  - **Bitwarden:**
    - Generous free tier, affordable paid plans
    - Independently security audited
    - Open-source
    - Download: https://bitwarden.com
  - **1Password:**
    - More advanced features
    - Paid plans only
    - Independently security audited
    - Closed-source
    - Download: https://1password.com

MultiFactor/2 Factor Authentication: Method Comparison

- **SMS/Email One-Time-Password (OTP)**
  - Least secure
  - Better than nothing, but not by much
  - SIM swapping; email account takeover, etc.
- **Push Notifications**
  - Already logged-in devices can receive the approval notification

        - Not all services offer this
    - **Time-based One-time Password (TOTP)**
        - Time-limited code is derived from a shared secret (created during setup) and the current time.
        - The short duration of code working makes it extremely difficult for attackers to intercept and use it
        - Most secure for the majority of people
    - **Hardware Security Keys**
        - A physical USB key that can be used to authenticate with something you physically must have
        - Interception is impossible without physically robbing you

Recommendation: Use Time-based One-time Password (TOTP) Authenticator app

- Best to use one separate from a password manager
- Can be backed up and restored on a new device in case of phone breakage, loss, etc.
- Open source (so code is auditable) is always preferred
- Can be used while the device is offline (no wifi, no data connection, etc necessary)

- **Android:** Aegis Authenticator
    - https://getaegis.app/

- **iOS:** OTP-Auth: OTP Auth
    - https://cooperrs.de/otpauth.html

Exercise: Set Up a Password Manager & Multi-Factor Authentication

Step by Step Guide: Bitwarden Setup

1. **Choose a Password Manager:** Select a recommended option or another reputable provider.

2. **Create an Account:** Follow the provider's instructions to set up your account.

3. **Generate Strong Passwords:** Use the password manager to create new, unique passwords for your accounts.

4. **Export & Import Existing Passwords:** If you have existing passwords saved in your browser, export them, then import them securely into the password manager.
   Exporting passwords from the browser:
   Chrome:

- ***Settings > Passwords & Autofill > Google Password Manager > Settings*** (Alternatively, enter: ***chrome://password-manager/settings*** into the URL bar)
- Then click ***Export Passwords*** button to download a file

Firefox:

- ***Settings > Privacy & Security > Logins and Passwords > Saved Logins > Export***

Safari:

- ***File > Export > Passwords*** in Safari menu bar
- or **System Preferences > Passwords > click three-dots icon > Export Passwords** (on macOS Monterey)

Importing to Password Manager: General Instructions

- ***Settings > Import > Select file type > Upload file > Import***

5. **Install Browser Extension:** Add the password manager extension to your web browser for seamless password entry.

   Chrome/Chromium/Vivaldi:
   - https://chromewebstore.google.com/
   - Search for your password manager. Make sure it is the official one created by the same company!

   Firefox/Librewolf/Mullvad:
   - https://addons.mozilla.org/en-US/firefox/extensions/
   - Search for your password manager. Make sure it is the official one created by the same company!

6. **Enable Two-Factor Authentication (2FA):**
   - Choose a TOTP Authenticator app like Aegis or OTP-Auth.
   - Install the app on your mobile device.
   - Open the app and scan the QR code provided by the account you are setting up 2FA for.
   - Enter the verification code displayed in the app to complete the setup.

2. Compartmentalization/Separation of Contexts

- **Purpose:** To isolate different online activities and minimize the risk of cross-contamination.

        - **Enhanced privacy:** Prevents websites/trackers from building a comprehensive profile of your online behavior by separating browsing activities.
        - **Improved security:** Limits the impact of a security breach in one context. If one browser is compromised, your other activities remain protected.
        - **Better organization:** Keeps your digital life organized by separating work, personal, and sensitive activities into different browsers.
    - **Recommended Browsers:**
        - **Chromium:** The open-source foundation for Google Chrome, offering a balance of performance and privacy with the familiarity of Chrome.
            - Download: https://www.chromium.org/getting-involved/download-chromium/
        - **Firefox:** A privacy-focused browser with a strong emphasis on user control and customization.
            - Download: https://www.mozilla.org/en-US/firefox/new/
        - **Librewolf:** A fork of Firefox with pre-configured privacy and security enhancements.
            - Download: https://librewolf.net/
        - **Mullvad Browser:** Developed in collaboration with the Mullvad VPN team and TOR Browser developers, this browser prioritizes privacy and security.
            - Download: https://mullvad.net/en/browser
        - **Vivaldi:** A highly customizable browser with built-in features for note-taking, task management, and more.
            - Download: https://vivaldi.com
        - **Tor Browser:** Routes your internet traffic through a network of volunteer-operated servers, providing a high degree of anonymity.
            - Download: https://www.torproject.org/download/

Exercise: Implement Browser Compartmentalization

- **Choose Different Browsers:** Select two or more browsers from the recommended list or other privacy-focused options.
- **Assign Activities:** Dedicate each browser to a specific type of online activity (e.g., work, personal, sensitive transactions).
- **Configure Privacy Settings:** Adjust the privacy settings of each browser to align with the sensitivity of the activities it's used for.

3. Protection from “Drive-by”/”Watering Hole” Malware

- **Ublock Origin:**

- **Purpose:** A powerful browser extension that blocks ads and malicious scripts. [cite: 55]
- **Benefits:**
    - **Enhances privacy:** Prevents websites and ad networks from tracking your browsing activity. [cite: 55]
    - **Improves security:** Blocks malicious code that can be embedded in ads or on compromised websites. [cite: 56]
    - **Speeds up browsing:** Eliminates ads, reducing page load times and bandwidth consumption. [cite: 56]
- **Download:**
    - Chrome/Chromium/Vivaldi: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en
    - Firefox (Librewolf and Mullvad come with it preinstalled):: https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/
- **More Information:** https://ublockorigin.com

Exercise: Install and Configure Ublock Origin & Restart your phone

1. **Download Ublock Origin:** Use the appropriate link above to download the extension for your chosen browser.
2. **Install the Extension:** Follow your browser's instructions to install the downloaded extension.
3. **Configure Settings (Optional):** Explore Ublock Origin's settings to customize its behavior if desired.
4. **Restart Your Phone**
    - Malicious or obnoxious scripts/code you may have come across while browsing on your phone generally isn't persistent and can't survive a reboot, so reboot your phone at least once a week to clear out anything you might have encountered
    - Note: That doesn't apply if you've installed a malicious app; if that's the case, the only solution is to uninstall the app.
        - Check all your app's permissions to see what it's able to do, and if it should have access to that permission. Does that game *really* need permission access to view all your files? Does that flashlight app need full network internet access?