XH Mobile - Green Belt Security

About Secure Software Development Training at Comcast

The TPX Security Learning Program is part of an effort to create a Secure Software Development mentality. The different levels of security training are provided to enable ownership of security at the development step. In following the Secure Development Lifecycle, DevOps becomes DevSecOps.

The TPX Security Learning Program follows a belt system, where the participant advances through the different colors as they progress through the levels. For description of the belt levels, see the TPX Belt System Brochure.

What is a Green Belt?

While the Yellow Belt session covers the basics of security topics and serves as a general introduction, the Green Belt is tailored to an employee's role within Comcast. There are different paths that can be followed while doing the Green Belt training: DB, software dev, or network engineer. The course is structured as a Learn, Share Do model.

The main benefit of participating in this program is gaining knowledge and acquiring skills on security topics. Comcast University does issue a certificate upon program completion and it looks good on a resume.

The TPX Security Learning Program is in the process of developing additional courses, with each offering content a bit more specialized than the previous one.

The TPX Security Learning Program has created a version of the Green Belt training available for contractors, called Green Lite Belt. See your manager for more information.

What did you learn?

I learned a lot! Not only during the Learn portion, but also while doing research for the Share and Do portions of the program. Some of the required and elective materials and courses are:

- Data privacy within Comcast
- Threat Modeling Overview
- Web Application Pen Testing Fundamentals
- Secure Coding Practices (Android)
- Cryptography overview
- Mobile Device Security
- HTTPS in depth
- Kali Linux and Ethical Hacking

The next part of this document is an overview of InfoSec and Cryptography concepts I studied during the training.

OWASP

Material from the Open Web Application Security Project (OWASP) organization was mentioned and used during the training. From their About page:

"OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security."

Among many other things, the organization publishes OWASP Top 10, a list of critical web application security risks.

The XH Wholesale App team has begun an exercise in evaluating security in the Wholesale App by following the OWASP Mobile Security Testing Guide.

CIA Triad of InfoSec

Information Security's primary focus is the balanced protection of the Confidentiality, Integrity and Availability of data. It seeks to protect these three attributes of systems and services.

Confidentiality, in Information Security, is ensuring that information is not made available or disclosed to unauthorized individuals, entities or processes.

Integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle.

Availability Ensuring that the information is available when it is needed. Therefore, the computing systems used to store and process the information, the security controls used to protect it and the communication channels used to access it must be functioning correctly.

https://en.wikipedia.org/wiki/Information_security

About Cryptography

- **Cryptography is an art**.
  It is the art of writing and solving codes. (Google)

- **Cryptography a science**.
  It is the science of encipherment and decipherment in secret code or cipher. (Merriam-Wester)

Cryptography helps keep information private while in transit and while stored and helps keep integrity, using digital signatures and hashes to verify no changes have been made to the information.

Caesar Cipher

The Caesar Cipher is one of the earliest known examples of cryptography and simplest of ciphers. It is a type of substitution cipher in which each letter in the plain text is “shifted” a certain number of places down the alphabet.

It is named after Julius Caesar, who is said to have used it with a shift of 3 to protect messages of military significance.

It is unknown how effective this form of communication was, but it is likely to have been reasonably secure since most of Caesar’s enemies would have been illiterate and others would have suspected the messages were in a foreign language.

https://en.wikipedia.org/wiki/Caesar_cipher#History_and_usage

Fast forward almost 2,000 years, maybe, to modern examples of cryptography, which include:

- SSL, TLS
- VPN
- hash on downloaded file
- digital signatures

Hashing Algorithms

So, let’s talk about hashing algorithms and how these have evolved to what is considered the standard today: SHA-256

Hash algorithms are one-way functions that take data and produce a unique hash value.

- take a file -> run it through a one-way hash

This produces a unique value that will be **the same** every time **the same file** is run through.

Hash functions originated from the need to compress data in order to reduce the amount of memory required to store large files. Today, common use of hash algorithms is for the verification of the integrity of downloaded files by using the singularly unique identifiers produced when running a file through a function.

https://coincentral.com/hashing-basics-history/

Hash algorithms are also used by SSL certificates to form digital signatures

https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/

Hashing Algorithms Vulnerabilities

Collisions – because hashes are a fixed length string, for every input we can imagine there are other possible inputs that will result in the same hash. An attacker is able to create collisions on demand and pass off malicious files or data as having a correct and proper hash.

https://medium.com/zkcapital/the-state-of-hashing-algorithms-the-why-the-how-and-the-future-b21d5c0440de

Birthday attack - If you put 23 people in a room, there is a 50% chance of two of them having the same birthday. If you put 70 people in a room, then the chance of two people having the same birthday goes up to 99.9%.

So, based on that probability and what we know about collisions, we can say that fixed output constraints mean there is a fixed degree of permutations upon which collisions can be found. It's bound to happen. All you need is a machine to run through the possibilities.

https://medium.com/zkcapital/the-state-of-hashing-algorithms-the-why-the-how-and-the-future-b21d5c0440de

Types of Hashing Algorithms - MD2, MD4 and MD5

MD2 and **MD4** are 128 bit hashing algorithms that have been considered vulnerable to collision attacks since 1989 and 1990.

MD5 is a newer version of MD4 that incorporates additional round of encryption for more security, but outputs a fixed, 128 bit string for every input. MD5 has also been found vulnerable, so no longer user in SSL or digital signatures (1992)

MD5 is so susceptible to a birthday attack that a 2.4 GHz Pentium Processor (remember those?) can compute artificial hash collisions within seconds.

https://medium.com/zkcapital/the-state-of-hashing-algorithms-the-why-the-how-and-the-future-b21d5c0440de

Types of Hashing Algorithms - SHA

SHA stands for Secure Hashing Algorithm. The SSL industry has picked SHA as its hashing algorithm for digital signatures.

Even though **SHA-1** produces a 160 bit hash and seeks to address the vulnerabilities of MD5, it has been found vulnerable since 2015. Google even created a SHA-1 collision.

https://z.cash/technology/history-of-hash-function-attacks#id111

Currently, **SHA-256** is considered to be the secure hash standard. It has been considered so since 2016.

SHA-256 produces a 256 bit hash, which results in a huge number of possible combinations. For more about this, read the **How Many Hashes** se ction here: https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/

Symmetric and Asymmetric Key Encryption and the Use of Public and Private Keys

Ok, so let's move to discussing the use of keys in cryptography. Remember how we discussed the Caesar Cipher and how it was based on a number of characters being "shifted"? The number for that "shift" is the key for the Caesar Cipher.

In cryptography a key is a piece of information (a parameter) that determines the output of an algorithm.

https://en.wikipedia.org/wiki/Key_(cryptography)

Symmetric key encryption

Symmetric key encryption uses the same key to encrypt and decrypt, so the key has to be shared between sender and receiver. The Caesar cipher is an example of shared key.

Symmetric key encryption's strength comes from the key size and algorithm. It is faster than asymmetrical key encryption and it is difficult to crack when the configuration has long enough keys. Current uses of symmetric encryption: Credit card transactions.

Symmetric key encryption standards:

> **DES** – key size of 56 bits became vulnerable to brute force attacks as computational power increased.
>
> **Triple DES** – Uses a key bundle that comprises three DES keys, each of 56 bits. Due to discovered vulnerabilities, OpenSSL does not include 3DES per default since August 2016. It is considered a weak cipher. https://en.wikipedia.org/wiki/Triple_DES
>
> **AES (Advanced Encryption Standard)** replaced DES and Triple DES. AES supports 128, 192 and 256-bit encryption keys. The theory is that a computer constructed today that could crack a DES key in one second, would take 149 trillion years for it to crack a 128-bit AES key.
>
> https://www.geek.com/news/aes-replaces-des-and-triple-des-544073/

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Asymmetric Key

Asymmetric Key encryption is also known as public key cryptography and uses two keys, one is public and the other private. In this case, the sender and receiver each generate two keys, a private and a public one, and the public key is made available to anyone who wants to send you a message. The sender encrypts with public key, and that message can only be decrypted with the receiver's private key.

Strengths:

- Secure key exchange and simplified key management (weakness of symmetric)
- Provides Authentication as well as encryption (protect from man-in-the middle attacks)
- Support for digital signatures

Weaknesses of Asymmetric Key encryption:

- Slower and less efficient than symmetric algorithm

Popular asymmetric key encryption algorithms include ElGamal, RSA, DSA, Elliptic curve techniques, PKCS

https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Resources

- Presentation Video (No Audio)
- Presentation Slides (PDF)
- About Comcast Security Training

  https://security.sys.comcast.net/How_Do_I/Services/Training/index.md
- Secure Development Lifecycle

  https://etwiki.sys.comcast.net/pages/viewpage.action?pageId=174311517
- TPX Belt System Brochure
  http://community.teamcomcast.com/i/CU/team/ecoeld/SiteAssets/security/tpxsecuritybeltsystem.pdf
- OWASP
  https://www.owasp.org/index.php/Main_Page
- OWASP Top 10 Report
  https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
- OWASP Mobile Security Testing Guide
  https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide