Cybersecurity BootCamp
week 1

ZERNA Lesly

October 2017

1 Introduction

Cybersecurity BootCamp by CyberWayFinder SPRL consists in a four week training in topics to be introduced into the cyber security field. This training is mainly focused on women.

This document contains my personal notes and extra info about the topics involved during the 4 weeks.

2 Class 1 - Introduction to Cybersecurity

Interesting points related to security in the internet:

- DOS
- IoT
- Cyberweapons
- Cybercriminal organizations
- Ethical standards

Brief intro

"Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide. Cyber security includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection.[2] Also, due to malpractice by operators, whether intentional, accidental, IT security is susceptible to being tricked into deviating from secure procedures through various methods."[wikipedia]

Overview

- what to consider when trying to secure something?
- what is risk management?
- what about 2-factor ID for email?
- Thinking about security:
    1. all stack should be secured
    2. users authentication
    3. data encryption
    4. levels of access (what is allowed to do?)
    5. application security
- The real interests is "data"
- Set up "protection levels" [top secret ... basic]
- "you cannot protect things that you don't valuate"
- application of GDPR
- differences among data security - data protection - data privacy ???

"The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU."[wikipedia]

Meeting compliance and Managing threats

- think as criminal -> find the attack patterns
- how to protect with a limited budget?
- encryption of all the data?
- understand the threats and predict the future
- actions again threats
- auditors' job
- define the critical infraestructure

NIST Cyber security framework

- identity
- protect
- detect
- respond
- recover

3 Class 2 - Physical security

(Video ->Hittler and Cloud Computing Security)

Asset Security

Asset -> a major application, general support system, ...
lifecycle: Create -> Store -> Use -> Share -> Archive -> Destroy (recycle?)

- who is allowed to use that info?
- is the usage being monitoring?
- when sharing -> distribution (is it encrypted?)

Lines of Defense (Audit, Risk, Ops)

- **1st line of defense** -> internal control measures, management control (operate controls)
- **2nd line of defense** -> financial controller, security, risk management, quality, inspection, compliance (perform controls)
- **3rd line of defense** -> internal audit

Important in security C.I.A.

- **Confidentiality**
- **Integrity**
- **Availability**

Physical (environmental) Security

- layered defense model
- medieval castle and moat defense
- core enterprise zone
- DMZ

Physical security

- detect (camera)
- control in data center
- design of data center
- computer room location
- physical controls (too dry/too hot)

4 Class 3 - Crypto analysis

Applied crytologie and PKI

Caesar cipher

- substitution cipher
- **break it** -> find the pattern
- frequency analysis

Vigenere cipher

- tabula recta -> mapping or matrix
- improve of caesar

Enigma machines

Ready to break the encrypted code. "The Enigma machines were a series of electro-mechanical rotor cipher machines developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. Enigma was invented by the German engineer Arthur Scherbius at the end of World War I.[1] Early models were used commercially from the early 1920s, and adopted by military and government services of several countries, most notably Nazi Germany before and during World War II.[2] Several different Enigma models were produced, but the German military models, having a plugboard, were the most complex. Japanese and Italian models were also in use."[wikipedia]

Digital era

- AES

Threads:

- integrity
- non-repudiation
- key generation

Quantum cryptography

It is based on physics (google <- quantum computers)
Interesting -> http://gva.noekeon.org/QCandSKD/QCandSKD-introduction.html
Qubit -> quantum bit
"In quantum computing, a qubit or quantum bit (sometimes qbit) is a unit of quantum information—the quantum analogue of the classical bit. A qubit is a two-state quantum-mechanical system, such as the polarization of a single photon: here the two states are vertical polarization and horizontal polarization. In a classical system, a bit would have to be in one state or the other. However, quantum mechanics allows the qubit to be in a superposition of both states at the same time, a property that is fundamental to quantum computing."[wikipedia]

Binary math concepts

- binary numbers
- 1 byte = 8 bits
- XOR operator (contributes to perfect secrecy -> unbreakable)

Cryptographic services

- confidentiality
- data integrity
- authentication
- non-repudiation
- source authentication

Crypto policies and standards

ISMS -> Information security management system

Symmetric ciphers:

- IDEA
- 3DES
- AES

Key stream generator:

- key (128 bits in lenght)
- key stream
- plain text
- cipher text

Stream cipher

"A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent on the current state of the cipher, it is also known as state cipher. In practice, a digit is typically a bit and the combining operation an exclusive-or (XOR)."[wikipedia]

Asymmetric key algorithm

public and private key

"Public key cryptography, or asymmetrical cryptography, is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. This accomplishes two functions: authentication, which is when the public key is used to verify that a holder of the paired private key sent the message, and encryption, whereby only the holder of the paired private key can decrypt the message encrypted with the public key."[wikipedia]

Cryptographic hash functions

"A cryptographic hash function is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value', 'message digest', 'digital fingerprint', 'digest' or 'checksum')."[wikipedia]

References

Computer security, https://en.wikipedia.org/wiki/Computer_security [cited October 2017].

GDPR, https://en.wikipedia.org/wiki/General_Data_Protection_Regulation [cited October 2017].

NIST, https://www.nist.gov/cyberframework [cited October 2017].

Enigma machine, https://en.wikipedia.org/wiki/Enigma_machine [cited October 2017].

Quantum bit, https://en.wikipedia.org/wiki/Qubit [cited October 2017].

Stream cipher, https://en.wikipedia.org/wiki/Stream$_cipher[citedOctober2017]$.

Asymmetric key, https://en.wikipedia.org/wiki/Public-key_cryptography [cited October 2017].

Cryptographic hash functions, https://simple.wikipedia.org/wiki/Cryptographic$_hash_function[citedOctober201$