CS2107 Intro Information Security

AY23/24 Sem 2, github.com/gerteck

0. Introduction

CS2107: Introductory module, illustrates fundamentals of how systems fail due to malicious activities and how they can be protected.

Lecture Notes notation

- **Textbook:** Security in Computing (5th ed). Prentice Hall. Reference [PFx.y] refer to chapter x section y of this book.
- Links with "read": Part of lecture, required.
- Links with "see": Optional good to browse references.

Internet Security Threat Report Exc. Summary

Persistent threats are threats that often operate within the shadows, outside of attention focused.

- Highly targeted, often use combination of social engineering and software vulnerabilities to establish footholds within the targeted enterprise.
- Network protection not enough to migitgate threats, comprehensive monitoring program required to scan all internal and external network traffic. Identifying, securing data is also key to protecting assets.
- Recent attack types: Formjacking, Ransomware, Living off the Land (LotL),

Introduction to Computer/Info Security

Systems may fail due to operator mistakes, hardware failures, poor implementation etc. Many systems robust against typical noise. Security is about intentional failures inflicted by deliberate human actions.
Security Definitions: C-I-A triad

- **Confidentiality**: Prevention of unauthorized disclosure of information.
- **Integrity**: Prevention of unauthorized modification of info / processes.
- **Availability**: Prevention of unauthorized withholding of info / resources.
- Other requirements may include (Confidentiality: anonymity, covert channel), (Integrity: Non-repudiation (digital signature)), (Other: Accountability, traitor-tracing (printout w hidden watermark)) etc.
- Importance of understanding security requirements before adopting mechanisms. Do not adopt mismatched protection mechanisms.

Difficulties in achieving Security

- **Security not considered** (in early design stage).
  Lack of adverarial thinking in design / trade-off in security with ease-of-use, performance / cost.
- Difficult to formulate requirements /design / implementation bugs.
- Difficult to operate/manage (Human error).
- **Known Vulnerabilities: CVE (Common vulnerabilities & Exposures**. Repository of discovered vulnerabilities. Significant portion considered "implementation bugs".
- **Zero-day Vulnerabilities**: Unpublished vulnerabilities. If attackers deploy attacks on zero-day v., victims have "zero-day" to react. Not easy to get.

1. Encryption

Key Summary & Takeaways

- **Encryption designed for confidentiality.** (Not necessarily integrity).
- Formulate attack scenario by defining attacks it can prevent.
- Notions of "Oracle": Encryption, Decryption, Padding Oracle.
- **Key strength**: Quantifying security by equivalence of best-known attack to exhaustive search.
- No known efficent attacks on modern schemes under "original" threat models, but there are pitfalls. Such as implementation error (wrong mode, wrong random source, mishandle of IV), side channel attack, implicity require integrity, padding oracle attack.
- Design of various symmetric key encryption schemes:
  - One-time pad, stream cipher (xor'ing with "pseudo-random" string)
  - Block cipher (mode of operations: CBC, ECB, CTR, GCM)
- **Crucial role of IV**. (Need randomness for indistinguishability). Make encryption probabilistic, how it is deployed, why it is important.

Definitions

- **Symmetric Key Encryption Scheme**: Two algorithms: encryption and decryption. Meets correctness property, and must be secure.
- **Correctness:** $(D_k(E_k(x)) = x)$. **Security**: Informally, "difficult" to derive useful info of the key k, and plaintext x. Ciphertext resemble random sequence of bytes.
- **Cryptography**: Study of techniques in securing communication in present of adversaries with access. Encryption just a primitive (other includes crypto hash, digital signature etc. Common placeholders: Alice, Bob, Eve ("eavesdroppper"), Mallory (malicious, modify message), etc.

Attack Model

Aka: Threat / Adversary / Security Model, Attack Scenario.
Measuring **security of a system**: Through attack classes it can prevent. Secure w.r.t these classes of attacks. Attack models are application-dependent. Attack models described by:

- Attacker's knowledge (info / service exposed) and computing resources
- Attacker's goal

Types of information we assume access to: (Access to info can be formulate to accesses to an **"Oracle"**).

- **Ciphertext only attack:** Adversary given collection of ciphertext c. May know some properties of the plaintext, for e.g. the plaintext is an English sentence. (adv. can't choose plaintext).
- **Known plaintext attack:** Adversary given collection of plaintext m and corresponding ciphertext c. (adv. can't choose plaintext.)
- **Chosen plaintext attack (CPA):** Access to blackbox (i.e. the oracle). Can choose, feed any plaintext m, obtain corresponding ciphertext c (all encrypt with the same key), reasonable large number of times. Can see ciphertext and choose next input. *(black-box called encryption oracle).*
- **Chosen ciphertext attack (CCA2)**: Same as chosen plaintext attack, but adv. chooses ciphertext and blackbox outputs plaintext. *black-box called decryption oracle*.
  Note: (strange to assume attacker has power to decrypt, but good reason is that in some practical scenario, attacker does have some but not full decryption capability, e.g. *padding oracle*. To cater for all scenarios, in formulation and design of encryption, we consider oracle with full decryption capability.)

Adversary's Goals

- **Total Break**: Attacker wants to find the key.
- **Partial Break**: Few definitions, e.g. decrypt ciphertext, determine coarse information about plaintext, etc.
- **Indistinguishability (IND)**:) Attacker may satisfy with distinguishability of ciphertext: with some "non-negligible" probability more than ½, the attacker is able to distinguish the ciphertexts of a given plaintext (say, "Y") from the ciphertext of another given plaintext (say, "N"). (Equivalently, unable to distinguish the ciphertext and a randomly sequence).
- **Note**: total break most difficult goal, since achieves all. Distinguishability weakest goal, design cryptosystem preventing weakest goal.

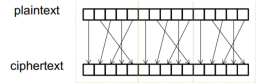
Classicial Ciphers

1. Substitution Cipher

- **Plaintext, ciphertext**: String over a set of symbols U.
- **Key**: Subsitution table S, 1-1 onto function from U to U.
- **Key space**: Set of all possible keys (e.g. 27). **Space Size** is total number of possible keys (factorial, 27!). **Key Size** is number of bits required to represent a key. (log 2 (27!), since 27! unique)
- **Exhaustive Search (Brute-force): Can be infeasible in worst case**
- **Known-plaintext-attack**: Access to pairs of ciphertext and corresponding plaintexts: *Sub. cipher "not secure / totally broken under known plaintext attack"*. (Possible in practice, e.g. certain words in header of email "From, Subject", protocols bytes fixed header information etc.)
- **Ciphertext only attack**: Vulnerable to frequency analysis attack, when plaintexts English sentences.

2. Permutation Cipher (aka transposition cipher)

- Groups plaintext into blocks of t characters, applies secret permutation (1-1 onto function). Fails miserably on known-plaintext attack.



- S & P cipher not secure, performing substitution multiple times no use. However, by interlacing them (S&P), attacks become more difficult. Many modern encryption scheme (e.g. AES) designed using rounds of S & P.

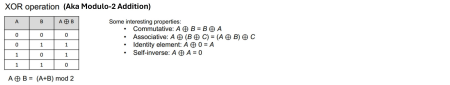
Perfect Secrecy

- **Definition**: A cryptosystem has perfect secrecy if for any distribution X, for all x, y:
$$Pr(X = x|Y = y) = Pr(X = x)$$.
- For any ciphertext y and plaintext x, the chances attacker correctly predicts x before knowing y, and after knowing y, are the same.

3. One Time Pad

One-time pad (OTP) is an encryption technique that requires the use of a single-use pre-shared key that is larger than or equal to the size of the message being sent.

- Plaintext is paired with a random secret key (known as one-time pad).
- Each bit or character of the plaintext encrypted by combining it with corresponding bit/character from pad using modular addition.[1]



One-Time-Pad:

Encryption:

Given n-bit Plaintext: $x_1, x_2, ..., x_n$ and n-bit key: $k_1, k_2, ..., k_n$

ciphertext C= $(x_1 \oplus k_1), (x_2 \oplus k_2), (x_3 \oplus k_3), ..., (x_n \oplus k_n)$

Decryption:

Given n-bit ciphertext: $c_1, c_2, ..., c_n$ and n-bit key: $k_1, k_2, ..., k_n$

plaintext $X = (c_1 \oplus k_1), (c_2 \oplus c_2), (c_3 \oplus k_3), ..., (c_n \oplus k_n)$

Encryption: plaintext ⊕ key → ciphertext

Decryption: ciphertext ⊕ key → plaintext

Correctness (decrypting the ciphertext give back the plaintext)∴

For any x, k, $(x \oplus k)_{\text{ciphertext}} \oplus k = x \oplus (k \oplus k) = (x \oplus 0) = x_{\text{plaintext}}$

- **Requirement**: Key cannot be re-used, used only once. Hence, 1GB plaintext would need 1GB key to encrypt.
- From pair of ciphertext & plaintext, key can be derived. However, key useless, as only used once.
- **Security**: OTP leaks no information of plaintext, sometimes called ”unbreakable”.

Modern Ciphers

Generally refers to schemes that use computer to encrypt / decrypt. E.g:
- DES [Data Encryption Standard 1977]
- RC4 [Rivest’s Cipher 4 1987]
- A5/1 [used in GSM 1987]
- AES [Adv. Encrypt. Std.], RSA).

- Designs take into consideration of known-plaintext-attack, freq. analysis and other known attacks.
- Supposed to be secure, so any successful attack does not perform noticeably better than exhaustive search.

1. DES / Exhaustive Search

2. Block Cipher & Mode-of-Operations

3. Stream Cipher and IVs

Types of Attacks

Triple DES & Meet-in-middle Attack

Padding Oracle Attack