Fondamenti di Cybersecurity
Appunti

Giovanni "Qua' Qua' dancer" Palma
e
Alex "Morbidelli WhatsApp" Basta

Contents

Ci sara' una domanda sul lab

Example 0.0.1

Quali opzioni ho per crackare una password?

Chapter 1

Key Exchange

1.1 Introduction to Cryptography

Definition 1.1.1: Cryptography

Art and science of using mathematics to obscure the meaning of data by applying transformations to the data thta are impractical or impossible to reverse without the knowledge of some key

Definition 1.1.2: Cryptoanalysis

Art/science of breaking encryption without knowing the key

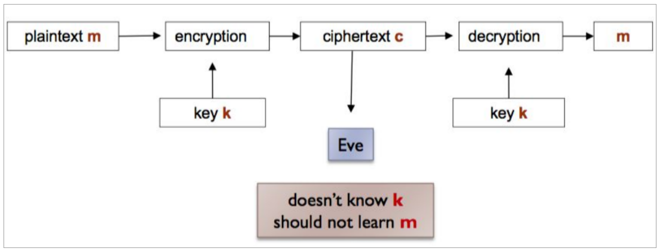
Used for:

- **Communication**: web traffic, wireless, vpn
- **Files on disk**
- **User authentication**

For secure communication, we also want to ensure no eavesdropping or tampering. Possible approaches are:

- **Steganography**: we 'hide' the existance of the message
- **Cryptography**: we instead hide the meaning of the message

1.1.1 Encryption Terminology



1.1.2 Goals and Protocols

The basic goals are:

- **Privacy**
- **Authenticity**

- **Integrity**
- **Non-repudiation**: no disclaming of authorship (guarantees Authenticity and Integrity)

The *protocols* need to guarantee these goals by understanding:

- The parties and the context
- The goals
- The **trusted computing base**
- The capabilities of the ... (**Threat Model**)

1.1.3 Kerchoff's Principle and the Threat Model

Important rule regarding the safety of cyber systems

> **Theorem 1.1.1**
> The security of a protocol shouldn't assume that the underlying methods/algorithms of the encryption are secret, as only the secrecy of the keys can be guaranteed.
> **Security by obscurity does not work.**

So the encryption functions need to remain secure even with the attacker knowing how the function works.
The attacker threat model consists of:

- Knowledge about the cipher (Kerchoff)
- Interaction with the messages and the protocol
- Interaction with the encryption algorithm
  - **Ciphertext-only**
  - **Chosen-plaintext attack (CPA)**
  - **Chosen-ciphertext attack (CCA)**
  - CPA and CCA may be *adaptive* (previous requests may change choices)
- Available resources (storage/computation)

1.1.4 Symmetric Encryption

Lowkey l'abbiamo fatta gia' due volte, aggiungo solo roba che dice in piu' (sta letteralmente leggendo le slide come il guerriero)

- **Single-use key**: the key is regenerated for each transmitted file
- **Multi-use key**: the key is used with a "nonce" in order to be used for multiple transmissions

1.1.5 Asymmetric Encryption

Private and public key. La pubblica e' salvata in una **public repo** gestita da un'autorita' trusted

1.1.6 Secure Communication

Una volta SSL ora TLS, poi RCS per end-to-end security (sono la stessa cosa??)

1.1.7 Boh

Criptography is a rigorus science that follows three main steps:

- Specify Threat Model
- Propose a construction
- ...

un po di storia, va veloce (manca la post-quantum criptology)
vabbe' sto scrivendo tutot in italiano facciamolo in italiano
la brodez sta davvero ripetendo il cifrario di Cesare.... e' ez da battere provando tutte le chiavi (non ce ne stanno molti) -¿ bruteforce/exhaustive-search criptanalysis

Monoalphabetic cipher

Come chiave prende una permutazione dell'alfabeto sono $2^8$8 non possiamo fare brute force possiamo fare criptanalysis con metodi statistici, ovvero usando la frequenza di ogni lettera

Affine cipher

Caso specifico del sub-cipher1

Example 1.1.1 (2 di un esame 17 gen 25)

Chapter 2

Modular Arithmetic

Chapter 3

Asymmetric Criptography

Chapter 4

IPsec and TLS

Chapter 5

Access Control

Chapter 6

Exploits and Patches