Computer Networks (part 6)

Rémi Emonet – 2021
Université Jean Monnet – Laboratoire Hubert Curien

Computer Networks: global overview

1. Introduction to computer networks
2. Networking application layer (HTTP, FTP, DNS, ...)
3. Data transfer layer (UDP, TCP, ...)
4. Network layer (routing, IP, ICMP, NAT, ...)
5. Lower layers, wireless and mobile (Ethernet, ARP, ...)
6. Security (SSL, ...)

Computer Networks 6: Plan

- Goal: get some notions of security
  - basics on cryptography
  - using cryptography for security
  - other security aspects
- Overview
  - Risks and objectives
  - A story about passwords
  - Symmetric cryptography
  - Asymmetric cryptography
  - Cryptography and security
  - Firewall and intrusion detection

Computer Networks 6: Plan

- Goal: get some notions of security
  - basics on cryptography
  - using cryptography for security
  - other security aspects
- Overview
  - Risks and objectives
  - A story about passwords
  - Symmetric cryptography
  - Asymmetric cryptography
  - Cryptography and security
  - Firewall and intrusion detection

Security

- A and B wants to communicate in a secure manner
- Somebody with bad intents may want to
  - listen to the network
  - delete messages
  - alter messages
  - add messages
- Example of A and B
  - people (mails, IM, etc)
  - a browser and a web server (online shopping, etc)
  - a mobile application and a bank
  - some DNS servers
  - some routers
- Reminder: all internet layers are unsecure

Security

- A and B wants to communicate in a secure manner
- Goals
  - confidentiality
    - avoid people to read their messages
  - authentication
    - be sure who sent a message
  - integrity
    - knowing if the message has been altered
  - accessibility and availability
    - all users must have access to the service

Importance of security

- Traditional web
  - online shopping
  - online banking
  - online privacy
  - the network stack is unsecured : IP, DNS, ARP, …
- Mobile devices
  - smartphones
  - tablets
- Internet of Things
  - connected devices, web of things
  - smart and personal devices
  - home automation (appliances, blinds, light bulbs, …)
  - smart cars

Encryption

- A wants to send a message to B
- Elements
  - : message to be send by A
  - : A's encryption function
  - : encrypted message
  - : B's decryption function
  - : decrypted message
- What to choose for and ?

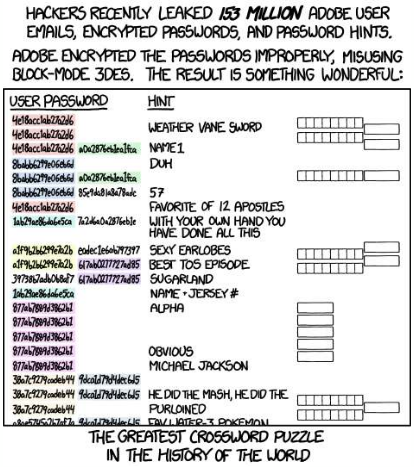
Computer Networks 6: Plan

- Goal: get some notions of security
  - basics on cryptography
  - using cryptography for security
  - other security aspects
- Overview
  - Risks and objectives
  - A story about passwords
  - Symmetric cryptography
  - Asymmetric cryptography
  - Cryptography and security
  - Firewall and intrusion detection

Passwords should be stored properly!

Forgotten Password? What happen when you hit "I forgot my password"?

Example: 2013 Adobe's leak …



What may happen if I directly store passwords?

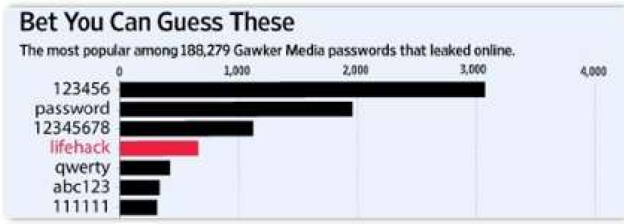
What Adobe Stored

- username for some users only
- the true "user name" is the email
- varying-length "**encrypted**" password
- password hint

Why storing this is, this way is wrong?

Some statistical analysis

8-byte data value	Prevalance in first ciphertext block (linear scale)
110edf2294fb8bf4	1.6%
8fda7e1f0b56593f	0.45%
2fca9b003de39778	0.44%
e5d8efed9088db0b	0.13%
ecba98cca55eabc2	0.11%



Statistics are too hard?

Adobe password data		Password hint	
110edf2294fb8bf4	->	numbers 123456	❶ 123456
110edf2294fb8bf4	->	==123456	
110edf2294fb8bf4	->	c'est "123456"	
8fda7e1f0b56593f e2a311ba09ab4707	->	numbers	❷ 12345678
8fda7e1f0b56593f e2a311ba09ab4707	->	1-8	
8fda7e1f0b56593f e2a311ba09ab4707	->	8digit	
2fca9b003de39778 e2a311ba09ab4707	->	the password is password	❸ password
2fca9b003de39778 e2a311ba09ab4707	->	password	
2fca9b003de39778 e2a311ba09ab4707	->	rhymes with assword	
e5d8efed9088db0b	->	q w e r t y	❹ qwerty
e5d8efed9088db0b	->	ytrewq tagurpidi	
e5d8efed9088db0b	->	6 long qwert	
ecba98cca55eabc2	->	sixxone	❺ 111111
ecba98cca55eabc2	->	1*6	
ecba98cca55eabc2	->	sixones	

Never store a password!

- Hash it
- Add Salt
- Add Pepper
- More explanations
  - https://crackstation.net/hashing-security.htm [en]
  - http://www.victorkabdebon.net/archives/117 [short][fr]

Analyzing Adobe's leak

Resources and recommended read from
https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

Computer Networks 6: Plan

- Goal: get some notions of security
  - basics on cryptography
  - using cryptography for security
  - other security aspects
- Overview
  - Risks and objectives
  - A story about passwords
  - Symmetric cryptography
  - Asymmetric cryptography
  - Cryptography and security
  - Firewall and intrusion detection

Symmetric Cryptography: example

- Principle: given a known key K
  - $c = f_A(m) = F(K, m)$
  - $m_o = f_B(c) = G(K, c)$
- Shuffling letters
  - `abcdefghijklmnopqrstuvwxyz`
    ↓
  - `klpoiuytrewqmnbvcxzasdfghj`
- Encryption key: the correspondence for the 26 letters
- Encrypted message: `mbxi vrjjk`

What are the limits/problems of this simple symmetric approach?

- A same message is always encoded in the same way!
  - easy to replay a sequence of recorded messages
  - easy to extract statistics (occurrence of some letters, ...) ⇒ key
- How to exchange the encryption key?

Improving Symmetric Cryptography

- Using a different parts/variations of a key for each message
- AES Advanced Encryption Standard
  - key size: 128, 192 or 256 bits
  - brute force attack: millions of years
  - ok to use today

Computer Networks 6: Plan

- Goal: get some notions of security
  - basics on cryptography
  - using cryptography for security
  - other security aspects
- Overview
  - Risks and objectives
  - A story about passwords
  - Symmetric cryptography
  - Asymmetric cryptography
  - Cryptography and security
  - Firewall and intrusion detection

Asymmetric Cryptography: principle

- Principle: two keys (one public, one private)
  - $c = f_A(m) = F(K^+, m)$
  - $m_o = f_B(c) = G(K^-, c)$
- RSA: Rivest, Shamir, Adelson algorithm
  - 2 keys, each is an integer
  - message to encode: an integer

RSA: "reminder" about modulus

- Rest of the integer division: $12 \% 5 = 2$
- $[(a \% n) + (b \% n)] \% n = (a + b) \% n$
- $[(a \% n) - (b \% n)] \% n = (a - b) \% n$
- $[(a \% n) \times (b \% n)] \% n = (a \times b) \% n$
- $(a \% n)^d \% n = a^d \% n$ (generalization of the product)
- ex: $a = 17, n = 10, d = 2$
  - $a^d \% n = 17^2 \% 10 = 289 \% 10 = 9$
  - $(a \% n)^d \% n = (17 \% 10)^2 \% 10 = 7^2 \% 10 = 9$
- ex: $a = 16, n = 10, d = 2$
- ex: $21^{27} \% 10 = ?$

RSA: key generation procedure

- Select two prime numbers p et q (1024 bits each)
- Compute $n = p \cdot q$ and $z = (p-1)(q-1)$
  - n is called the the "key length", it is the max size of a message
  - as n and z are coprime, by Fermat-Euler theorem, we have: $\forall x, y : x^y \% n = x^{y \% z} \% n$
- Select e ($< z$) such that e and z are coprime
- Select d such that $e \cdot d - 1$ is a multiple of z, i.e., $(e \cdot d) \% z = 1$
- Public key: the pair (n, e)
- Private key: the pair (n, d)

RSA: using generated keys

- Message m
- Encryption: $c = m^e \% n$
- Decryption: $m_o = c^d \% n$
- Magic!? $m_o = c^d \% n = (m^e \% n)^d \% n = m^{e \cdot d} \% n$
- Reminder: $\forall x, y : x^y \% n = x^{y \% z} \% n$
- Reminder: $e \cdot d \% z = 1$
- $m_o = m^{e \cdot d} \% n = m^{e \cdot d \% z} \% n = m^1 \% n = m$

RSA

- Example: $p = 5, q = 7, e = 5, d = 29, m = 12$ (00001100)

RSA: approach's security and advantages

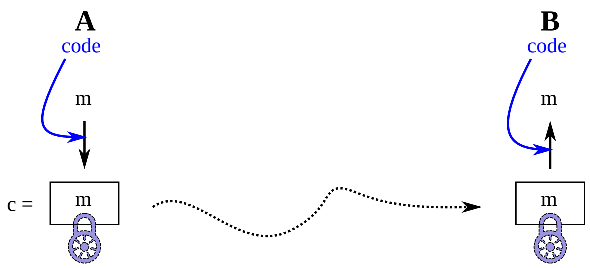
- Supposing a known public key (n, e)
- How to find d (to have the private key (n, d))
  - find the factors of n
  - these are p and q (each 1024 bits)
- Factorization of big numbers is difficult
- Key pair
  - the *public key* is published to all
  - the *private key* is never published
- Symmetry in the asymmetry
  - d and e are completely swap-able in the equations
  - we can encrypt with a public key

Computer Networks 6: Plan

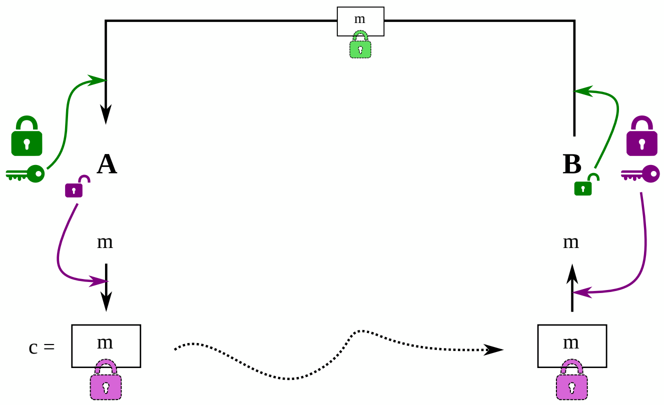
- Goal: get some notions of security
  - basics on cryptography
  - using cryptography for security
  - other security aspects
- Overview
  - Risks and objectives
  - A story about passwords
  - Symmetric cryptography
  - Asymmetric cryptography
  - Cryptography and security
  - Firewall and intrusion detection

Reminder and Notations for key-based cryptography

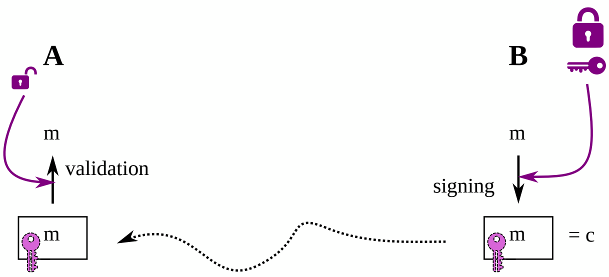
Exchange with symmetric cryptography



Exchange with asymmetric cryptography



Signing with asymmetric cryptography



Practical Example: Secure Shell (SSH)

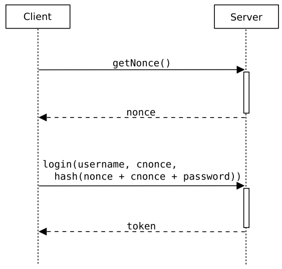
- Secure remote login
  - client-server architecture (default server port 22)
  - temporary key pairs …
  - setup a common shared secret
  - authenticate the user
- Generation of user authentication keys
  - `ssh-keygen`
  - → `$HOME/.ssh/id_rsa`
  - → `$HOME/.ssh/id_rsa.pub`
- SSH usage
  - remote login, authenticated by key
    - adding the public key in `$HOME/.ssh/authorized_keys` on the target machine
  - tunneling: TCP forwarding, X11 forwarding, SOCKS
  - file transfer: SSH file transfer (SFTP), secure copy (SCP)

Cryptography and Security

- E-mails, OpenPGP
  - confidentiality
  - signature and integrity
- CA: certificate authorities
  - signing certificates/keys
- WEP, WPA, ...
- IPSec
- SSL/TLS

SSL/TLS

- Transport Layer Security (TLS)
  - (was SSL, *secured* socket layer)
- Stateful connection
  - handshake (client hello, server hello, negocication)
  - using asymmetric crypto (RSA)
  - communication using symmetric crypto (e.g., AES)
- NB: Principles of a secured handshake
  - nonce
  - cnonce
  - padding



SSL/TLS Session

Example Attack: POODLE

- Use negotiation to downgrade to SSL 3.0 (known unsafe)
- Use SSL 3.0 problem

The Question of Forward Secrecy

- Forward secrecy?
  - if we break the key at some point in time
  - are past communications compromised?
- Use Diffie-Hellman algorithm
  - build a shared secret over a public channel
  - derive key-pairs for each session
- Principle ...
  - one-way function (difficult to undo)
  - e.g. mixing colors
  - problem of “discrete logarithm”

Browsers and Certificates

- Principle
  - your browser or system trusts some “Certificate Authorities” (CA)
  - CA validates the identity of domain name owners
  - CA sign owners certificates (and keys)
  - your browser does validation via this chain of trust
  - schema, demo...
- Additional security:
  - certificate pinning (db of hashes of known certificates)
  - DNSChain, ...
- Having your own certificates
  - buy from a certificate authority
  - or use “Let's encrypt”

Computer Networks 6: Plan

- Goal: get some notions of security
  - basics on cryptography
  - using cryptography for security
  - other security aspects
- Overview
  - Risks and objectives
  - A story about passwords
  - Symmetric cryptography
  - Asymmetric cryptography
  - Cryptography and security
  - Firewall and intrusion detection

Firewall: packet filtering

- Objective
  - avoid denial of service (e.g., SYN flooding)
  - avoid illegal access
  - limit access to the outside
- Examples
  - block port UDP 666 or port TCP 80
  - block all connections from the outside
  - block broadcast
  - block traceroute (block ICMP "TTL expired")

Intrusion Detection and Protection

- Goal
  - do not limit rules to packet headers (IP, port, etc)
  - detect attacks
- Types of attacks
  - port scanning
  - denial of service
  - network mapping (via ICMP)
- Principles of intrusion detection
  - deep packet analysis (look at the actual content)
  - analysis of packet correlation
  - modeling normal traffic to detect anomalies
- Network protection
  - DMZ: demilitarized zone
    - sub-network for external-facing services, firewall(s)
  - honeypot
    - fake system to detect and log attacks

- Hash it, add Salt and Pepper
- More explanations
  - https://crackstation.net/hashing-security.htm [en]
  - http://www.victorkabdebon.net/archives/117 [short][fr]

Reminder: Never store a password!

Computer Networks 6: Plan

- Goal: get some notions of security
  - basics on cryptography
  - using cryptography for security
  - other security aspects
- Overview
  - Risks and objectives
  - A story about passwords
  - Symmetric cryptography
  - Asymmetric cryptography
  - Cryptography and security
  - Firewall and intrusion detection

End Of Part