Security

Gianluca Dini

Dept. of Information Engineering
Faculty of Engineering, Univ. of Pisa

dini@iet.unipi.it

http://www.iet.unipi.it/g.dini/

0

Topics

- Applied cryptography
  - Main crypto primitives
    - Symmetric encryption, Public key encryption, Hash functions, Secure (pseudo-)random generators
  - Black-box view
- Services
  - Key management
  - Authenticity, Authorization, Auditing
- Case studies
  - WEP, IpSEC, SSL, KERBEROS, SET, Phishing, DDoS…

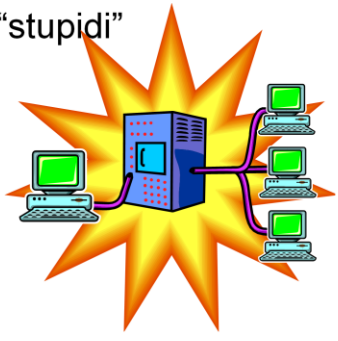
I meccanismi crittografici sono i building block per costruire protocolli e sistemi sicuri.

Topics

- Design and implementation of secure protocols
  - Application level
  - C/C++ or Java
  - OpenSSL, JCA/JCE

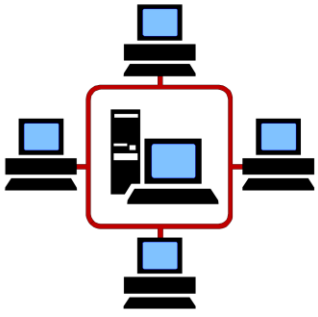
Centralized system

- Features
  - Centralized processing
    - E.g., Information System
  - Access through dumb terminals “stupidi”
  - Single administrative domain
  - Physical protection
  - Known and trusted users
- Objective
  - System integrity
- Security mechanisms
  - Hw mechanisms (user/system space); O.S. (VM)



Local Area Network

- Features
  - Information system, sw development
  - Resource sharing
  - Workstations
  - Single administrative domain
  - Physical protection
  - Known and trusted users
- Objective
  - System integrity
- Security mechanisms
  - address-based authentication



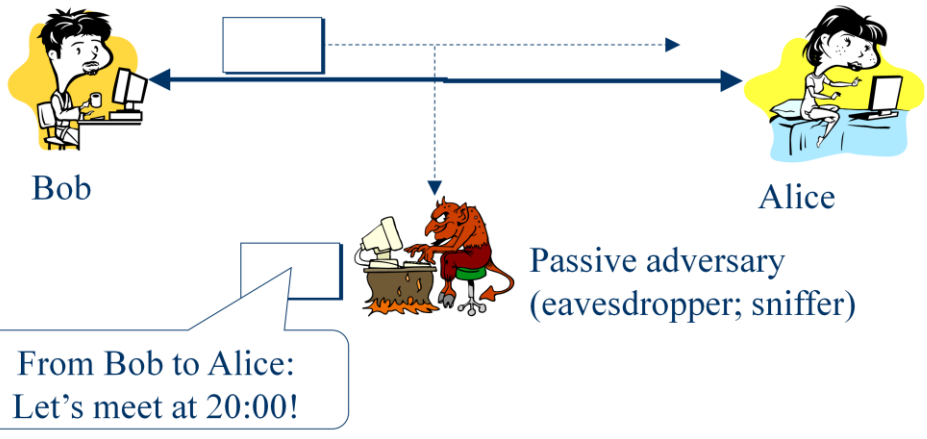
Wide Area Network

- Features
  - Sensitive applications: e-comm; e-health…
  - Different application domain
  - Unknown and/or untrusted users/domains
- Objectives
  - Confidentiality, authenticity, integrity, non-repudiation
- Mechanisms
  - Ciphers, hash functions, digital signature

Attacks against security

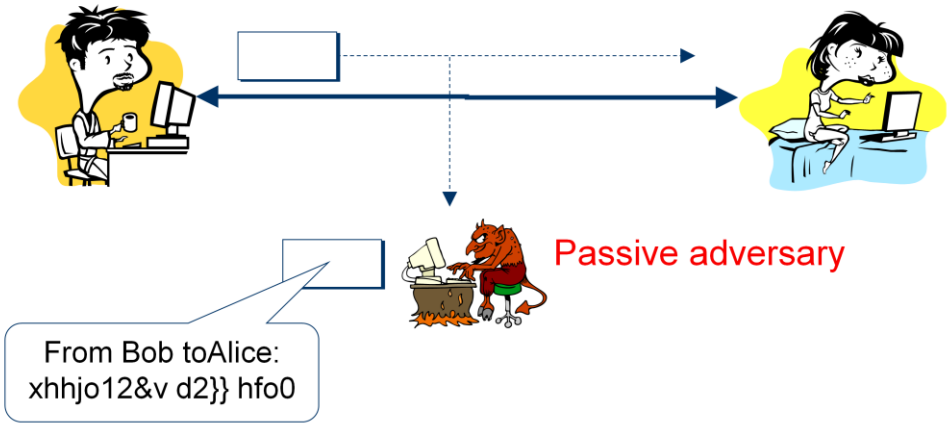
- Eavesdropping
- Traffic analysis
- Spoofing, masquerade
- Message modification
- Message deletion
- Message replay

Eavesdropping



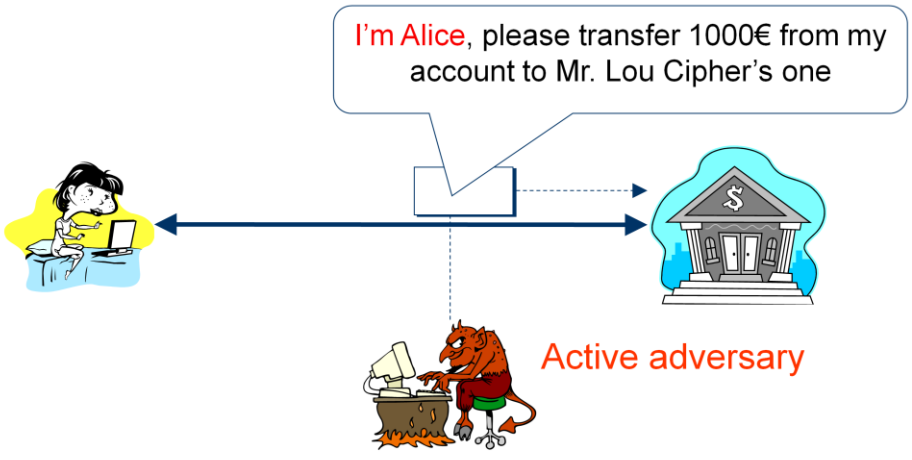
The adversary (unauthorized party) reads the contents of transmission

Traffic analysis



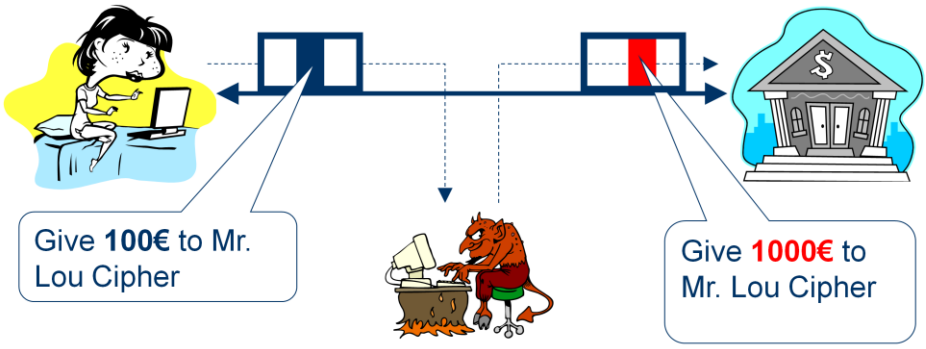
The adversary determines: the existence of a communication; identity of communicating parties; frequency and size of messages…

Spoofing, masquerade



The adversary pretends to be someone else

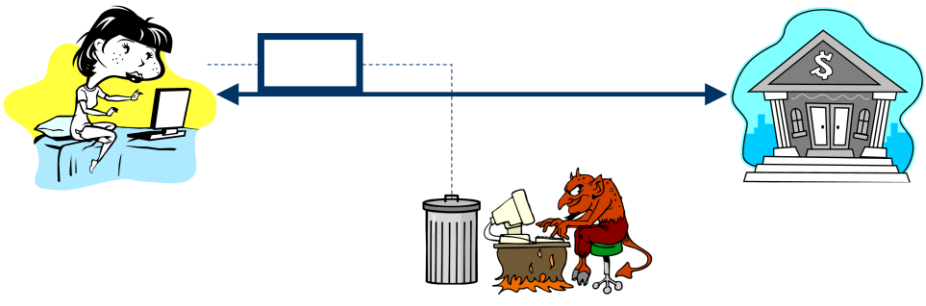
Message modification



Active adversary

The adversary modifies messages without being detected

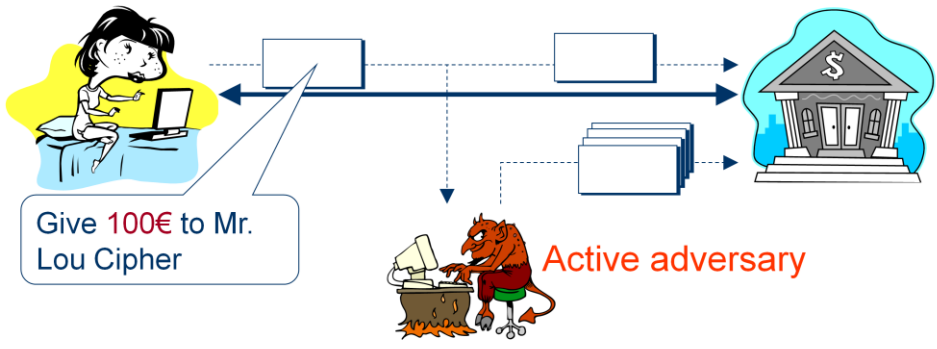
Message deletion



Active adversary

Denial of Service (DoS)

Message replay



The adversary intercepts a message and replays it several times

Attacchi alla sicurezza

Types	Attack	Detection/Counter measures
Passive	• Eavesdropping • Traffic analysis	• Difficult to detect • Easy to contrast
Active	• Masquerade • Message modification • Replay • Denial of Service	• Easy to detect • Difficult to contrast

Requirements

- Confidentiality
  - secrecy
  - privacy
- Data integrity
- Authenticity
  - Identification
  - Message origin
- Non-repudiation

Cryptography and crypo-primitives

- Cryptography s the practice and study of mathematic techniques for secure communication in the presence of third parties (called adversaries)
- Cryptographic primitives are
  - Ciphers (symmetric and asymmetric)
  - Hash functions
  - Digital signatures
  - Secure (pseudo-)random bit generators

Two messages

- To invent a crypto algorithm is a mathematician's tas but to use it correctly is a computer scientist/engineer's oneInventare un algoritmo crittografico è compito
- Cryptography is not equal to security

  "*Whenever anyone says that a problem is easily solved by cryptography, it shows that he doesn't understand it*"

  (Roger Needham/Butler Lampson)

I meccanismi crittografici sono i building block per costruire protocolli e sistemi sicuri.

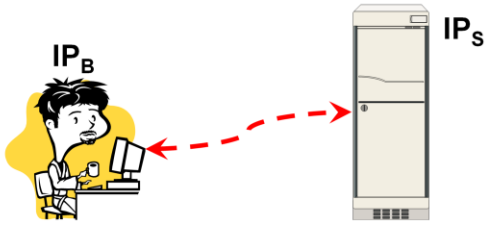
An example: IP spoofing

Overview

Problems with the TCP/IP protocol suite

- Address-based authentication
- No-use of authentication

Trust relationship in the Unix world



`~/.rhosts`
…
`ip`$_s$ `bob`
…

`~/.rhosts`
…
`ip`$_b$ `bob`
…

- Server *S* ***trusts*** *Bob* when he talks from host *B*
- Server *S* trusts host *B*'s ability to identify its users

- Bob can use any of the **r*** commands without the annoying hassle of password authentication
- The **r*** commands are based on ***address-based authentication***

TCP 3-way handshake

Handshake for connection establishment

S: server (target host);
C: client (trusted host);
ISN: initial sequence number;

M1 C -> S: SYN(ISN_C), SRC = C
M2 S -> C: SYN(ISN_S), ACK(ISN_C)
M3 C -> S: ACK(ISN_S)
data transmission

Sequence numbers allow TCP to implement data sequencing and acknowledging for communication reliability

TCP spoofing: basic idea

If an adversary X is able to "guess" ISN_S, then he can impersonate the trusted host C

X impersonates *C*

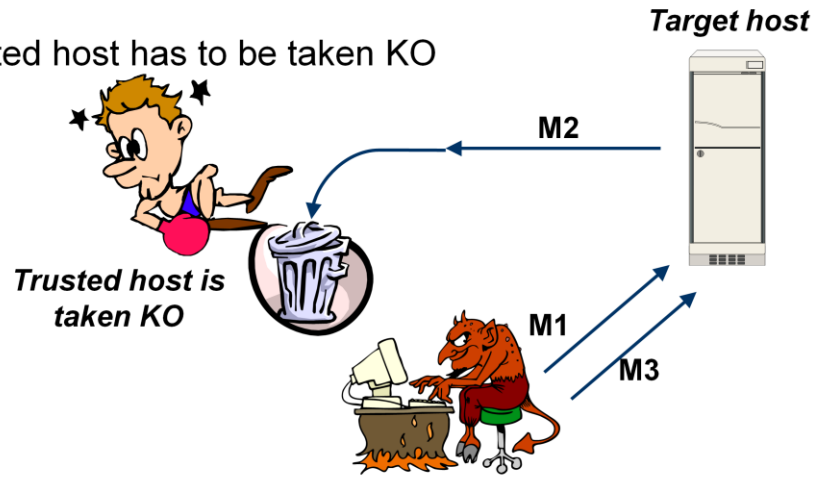
M1 X -> S: SYN(ISN_X), SRC = C
M2 S -> C: SYN(ISN_S), ACK(ISN_X)
M3 X -> S: ACK(ISN_S)
M4 X -> S: ACK(INS_S), *malicious payload*

- X does not receive M2 but he is able to guess ISN_S and thus generate M3
- *S* ***believes*** that the connection is with *C*

TCP spoofing: basic idea

Problem

- Upon receiving M2, the trusted host C would send the **RST command**
- The trusted host has to be taken KO



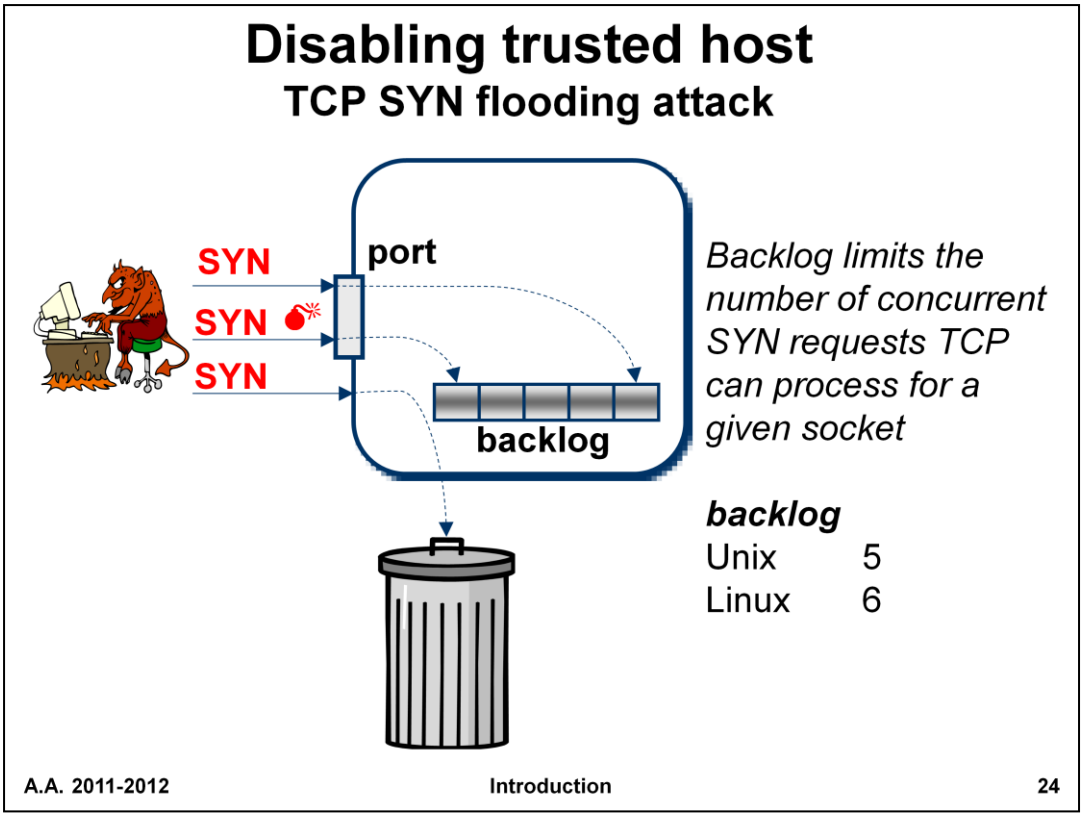
The attacker has to take the trusted KO. Otherwise, upon receiving message M2 (SYN/ACK), the trusted host would send a **RST** (Reset command) packet to the target host since the trusted host does not know anything of the current connection establishment.

TCP spoofing: attack planning

- Choose the **target host (S)**
- Discover a pattern of trust and a **trusted host (C)**
  - ***background information is known***
  - ***try neighbouring IP addresses***
- Disable the trusted host
- Impersonate the trusted host
  - sample sequence numbers
  - make connection attempt
- Leave a backdoor, if the attack succeeds

After a target is chosen the attacker must determine the patterns of trust.

Figuring out who a host trusts may be or may not be easy. A **`'showmount -e'`** may show where filesystems are exported, and **`rpcinfo`** can give out valuable information as well. If enough background information is known about the host, it should not be too difficult. If all else fails, trying neighboring IP addresses in a brute force effort may be a viable option.

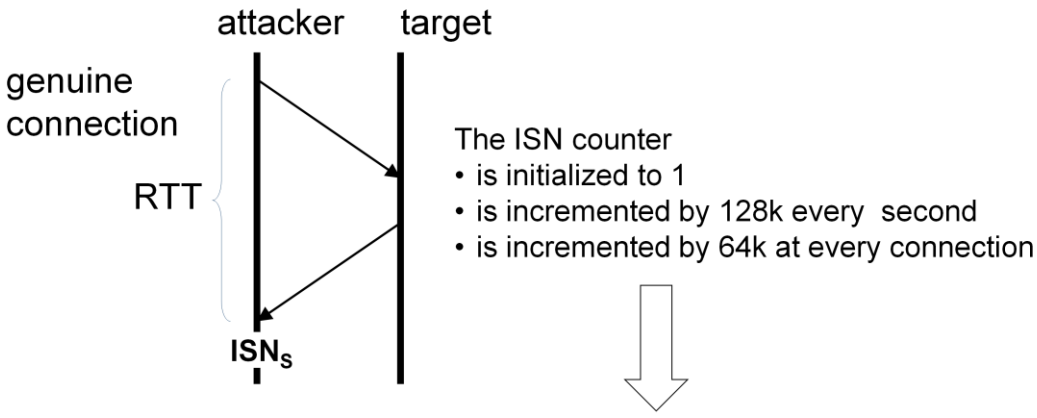


The trusted host can be disabled by means of a SYN flooding attack.

Even in this case, the attacker must use a spoofed address. Otherwise, this host would receive a SYN/HOST from the target host and send a RST packet, thus foiling the attack.

ISN sampling and prediction

RTT: Round Trip Time



ISN_S and (an estimation of) RTT allow the attacker to estimate the next value for ISN_S to be used in the spoofing attack

A.A. 2011-2012 Introduction 25

After the attacker has estimated ISN, she immediately proceeds to the next phase of the attack (if another TCP connection were to arrive on any port of the target before the attacker was able to continue the attack, the ISN predicted by the attacker would be off by 64,000 of what was predicted).

PREDICTED ISN and THE SLIDING WINDOW MECHANISM

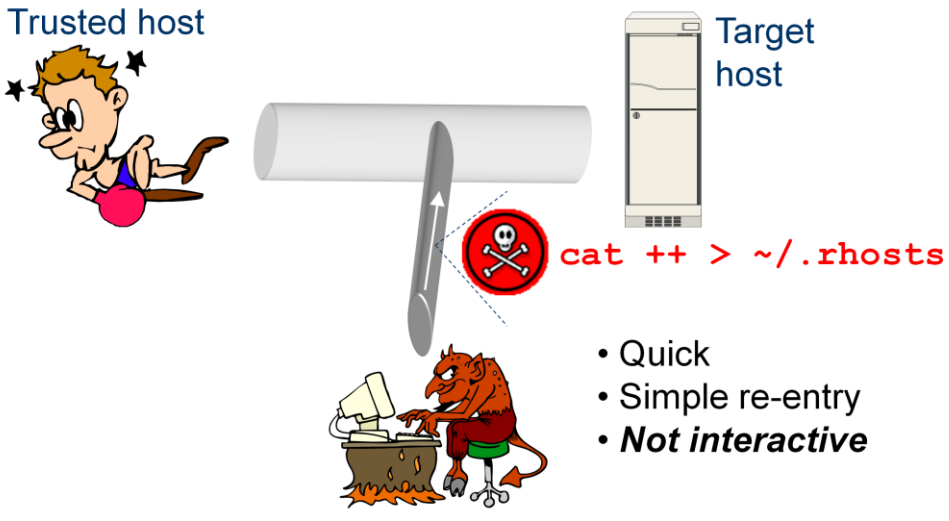
When the spoofed segment makes it's way to the target, several different things may happen depending on the accuracy of the attacker's prediction:

•If the sequence number is EXACTLY where the receiving TCP expects it to be, the incoming data will be placed on the next available position in the receive buffer.

•If the sequence number is LESS than the expected value the data byte is considered a retransmission, and is discarded.

•If the sequence number is GREATER than the expected value but still within the bounds of the receive window, the data byte is considered to be a future byte, and is held by TCP, pending the arrival of the other missing bytes. If a segment arrives with a sequence number GREATER than the expected value and NOT within the bounds of the receive window the segment is dropped, and TCP will send a segment back with the *expected* sequence number.

Insert a backdoor



- Quick
- Simple re-entry
- ***Not interactive***

Preventive measures (I)
(not unique)

- ***Be un-trusting and un-trustworthy***
  - **Disable all r* commands**
  - **Remove all .rhosts**
  - **Empty /etc/equiv (host wide trust relationships)**
  - **Force users to use other means of remote access**
    - e.g. **ssh**
- ***Packet filtering***
  - Impose trust relationships only among internal hosts
    - ***No internal host should trust and external host***
    - ***Filter out all traffic from the outside that purports to come from the inside***

Preventive measures (II)

- ***Cryptographic methods***
  - Require all network traffic to be authenticated and/or encrypted
  - ISN Randomizing
    - *Sequence numbers are chosen randomly and unpredictably*
    - **ISN = Clock + (upon every new connection)**

      hash(localhost, localport, remotehost, remoteport, s),

      where **s** is secret material