

UNIVERSITY OF TRENTO

## Security Engineering

### Lecture 16 – Network Security

Fabio Massacci  
(with the courtesy of W. Stallings)

19/11/14 Pacilabunets-Security Engineering ▶ 1

UNIVERSITY OF TRENTO

## Lecture Outline

- Network Attacks
  - Active Attacks
  - Passive Attacks
  - TCP Attacks
- Contermeasures
  - IPSec
  - SSL/TLS
  - Firewalls
  - Intrusion Detection Systems
  - Honeybots

19/11/14 Pacilabunets-Security Engineering ▶ 2

UNIVERSITY OF TRENTO

## Network Security


19/11/14 Pacilabunets-Security Engineering ▶ 3

UNIVERSITY OF TRENTO

## Where does Network Security sit?

19/11/14 Pacilabunets-Security Engineering ▶ 4


## Passive and Active attacks

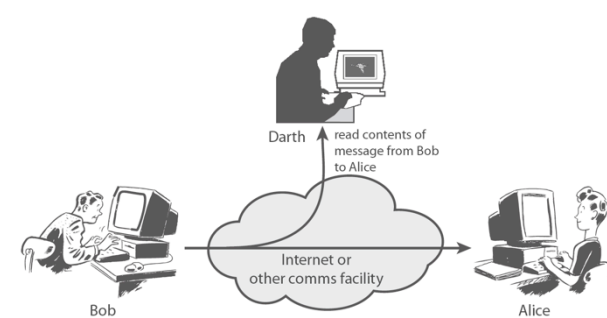
 UNIVERSITY OF TRENTO

- **Passive attacks**
  - **GOAL** : obtain information
  - No modification of content or fabrication
    - Release of message contents
    - Traffic analysis
- **Active attacks**
  - **GOAL** : modification of content and/or participation in communication to
    - Impersonate legitimate parties (Masquerade)
    - Replay or retransmit
    - Modify the content in transit
    - Launch denial of service attacks

19/11/14
Paci-Labunets-Security Engineering
▶ 5


## Passive Attack - Interception

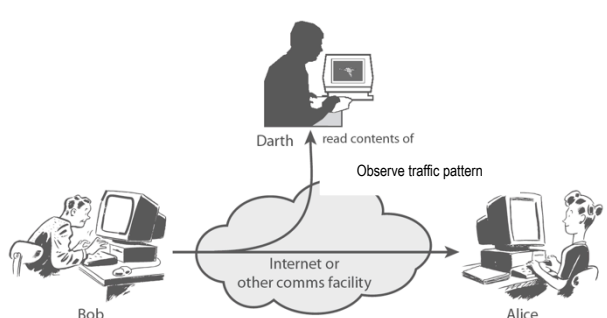
 UNIVERSITY OF TRENTO



19/11/14
Paci-Labunets-Security Engineering
▶ 6


## Passive Attack: Traffic Analysis

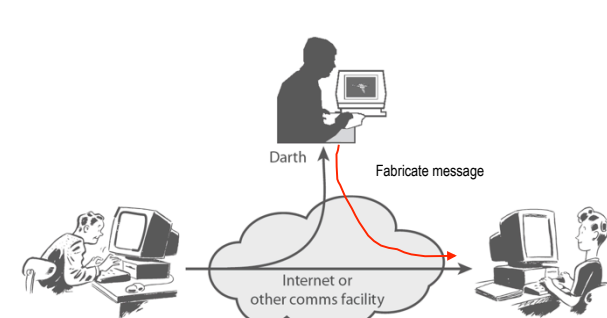
 UNIVERSITY OF TRENTO



19/11/14
Paci-Labunets-Security Engineering
▶ 7


## Active Attack: Masquerade

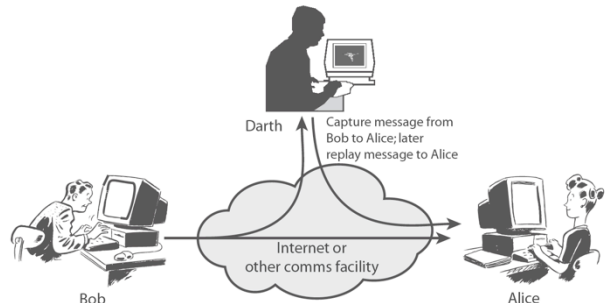
 UNIVERSITY OF TRENTO



19/11/14
Paci-Labunets-Security Engineering
▶ 8


### Active Attack: Message Replay

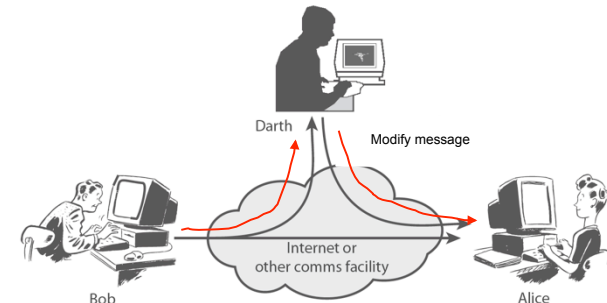
 UNIVERSITY OF TRENTO



19/11/14 Pacil-Labunets-Security Engineering ▶ 9


### Active Attack: Modification

 UNIVERSITY OF TRENTO



19/11/14 Pacil-Labunets-Security Engineering ▶ 10


### Active Attack: Denial of Service

 UNIVERSITY OF TRENTO

- an action that prevents or impairs the authorized use of networks, systems, or applications
- Attacks to
  - network bandwidth
  - system resources
  - application resources

19/11/14 Pacil-Labunets-Security Engineering ▶ 11

### Source Address Spoofing

 UNIVERSITY OF TRENTO

- use forged source addresses
  - given sufficient privilege to “raw sockets”
  - easy to create
- generate large volumes of packets with different, random, source addresses
- cause same congestion
- real source is much harder to identify

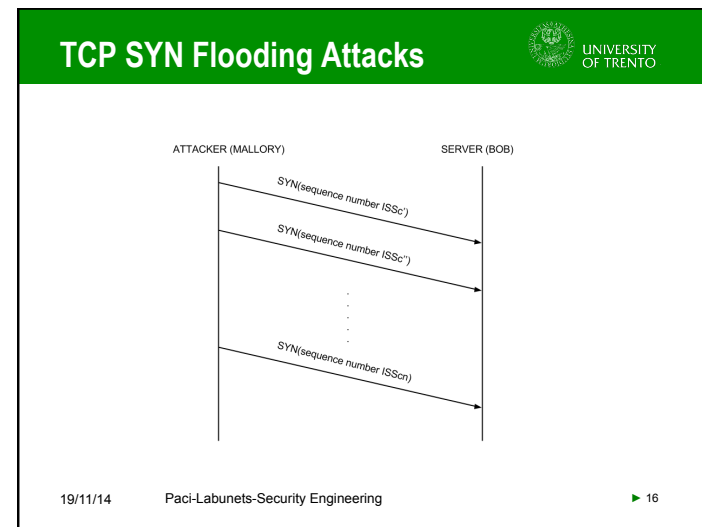
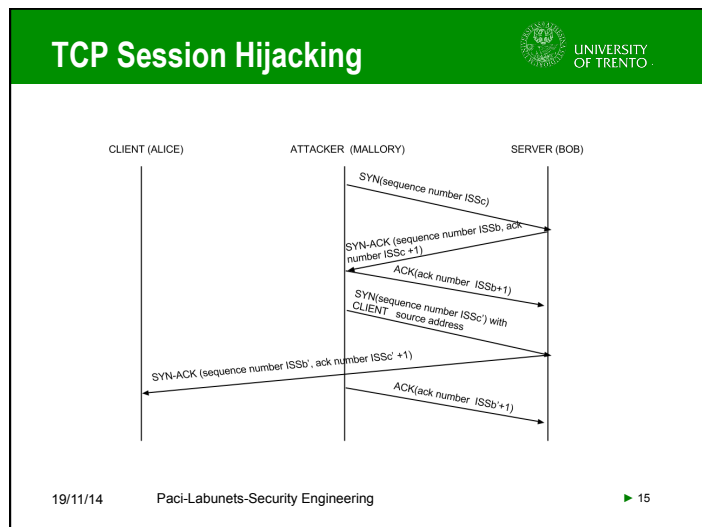
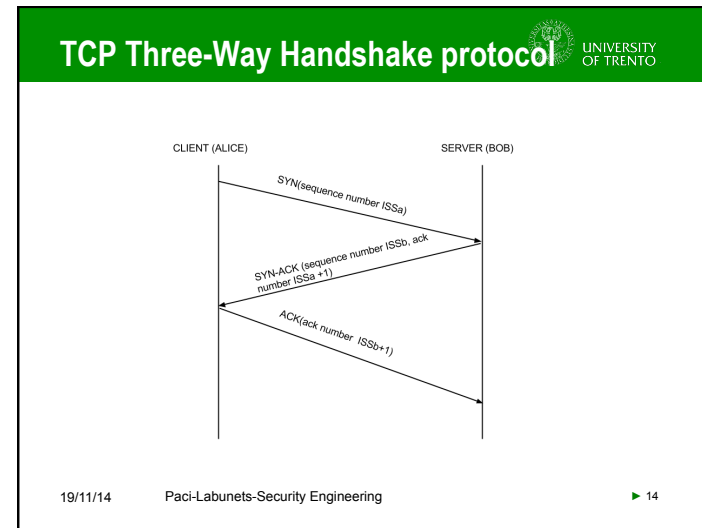
19/11/14 Pacil-Labunets-Security Engineering ▶ 12

### Active Attacks: TCP Attacks

UNIVERSITY OF TRENTO

- **TCP connections have associated state**
  - Starting sequence numbers, port numbers
- **Problem – what if an attacker learns these values?**
  - Port numbers are sometimes well known to begin with (ex. HTTP uses port 80)
  - Sequence numbers are sometimes chosen in very predictable ways

19/11/14
Paci-Labunets-Security Engineering
▶ 13



## Possible Countermeasures



- **Cryptographic security services**
  - IPSec
  - TLS/SSL
- **Non-cryptographic security services**
  - Firewalls
  - Intrusion Detection Systems
  - Honey pots

19/11/14 Pacì-Labunets-Security Engineering

▶ 17

## Building Secure Tunnels



- **Logical connections between two endpoints that crosses an insecure network**
- **Provide**
  - Data integrity, confidentiality and data origin authentication
- **Built as follows**
  - Authenticated key establishment protocol
  - Key Derivation
  - Traffic Protection using Derived Keys

19/11/14 Pacì-Labunets-Security Engineering

▶ 18

## IPSec



- **general IP Security mechanisms**
- **provides**
  - authentication
  - confidentiality
  - key management
- **applicable to use over LANs, across public & private WANs, & for the Internet**

19/11/14 Pacì-Labunets-Security Engineering

▶ 19

## IP Security Architecture



- **mandatory in IPv6, optional in IPv4**
- **have two security header extensions:**
  - Authentication Header (AH) (RFC 4302)
  - Encapsulating Security Payload (ESP) (RFC 4303)
  - Key Exchange function
- **VPNs want both authentication/encryption**
  - hence usually use ESP

19/11/14 Pacì-Labunets-Security Engineering

▶ 20

## Authentication Header (AH) UNIVERSITY OF TRENTO

- **provides support for data integrity & authentication of IP packets**
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- **based on use of a MAC**
  - HMAC-MD5-96 or HMAC-SHA-1-96
- **parties must share a secret key**

19/11/14      Paci-Labunets-Security Engineering      ▶ 21

## Encapsulating Security Payload (ESP) UNIVERSITY OF TRENTO

19/11/14      Paci-Labunets-Security Engineering      ▶ 22

## Security Associations UNIVERSITY OF TRENTO

- **a one-way relationship between sender & receiver that affords security for traffic flow**
- **defined by 3 parameters:**
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- **has a number of other parameters**
  - seq no, AH & EH info, lifetime etc
- **IP implementation has a database of Security Associations**

19/11/14      Paci-Labunets-Security Engineering      ▶ 23

## SSL / TLS UNIVERSITY OF TRENTO

- **Transport Layer Security protocol, ver 1.0**
  - De facto standard for Internet security
  - The primary goal of the TLS protocol is to provide confidentiality and data integrity between two communicating applications
  - In practice, used to protect information transmitted between browsers and Web servers
- **Based on Secure Sockets Layers protocol, ver 3.0**
  - Same protocol design, different algorithms
- **Deployed in nearly every web browser**

19/11/14      Paci-Labunets-Security Engineering      ▶ 24

## TLS Basics

UNIVERSITY OF TRENTO

- **TLS consists of two protocols**
- **Handshake protocol**
  - Use public-key cryptography to establish a shared secret key between the client and the server
- **Record protocol**
  - Use the secret key established in the handshake protocol to protect communication between the client and the server
- **We will focus on the handshake protocol**

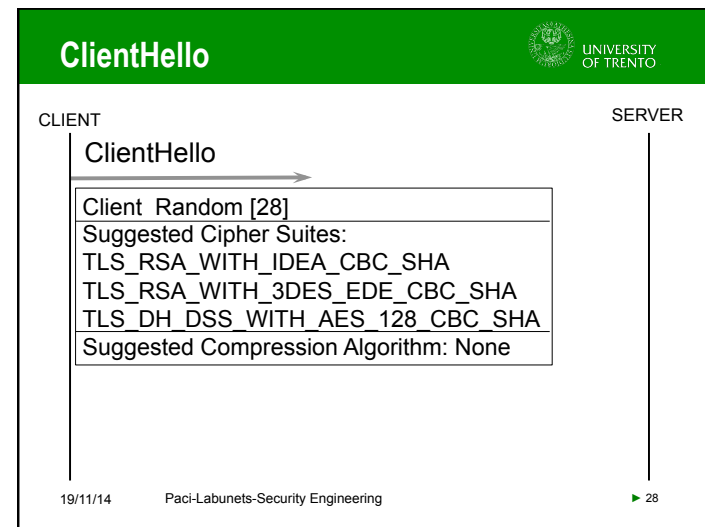
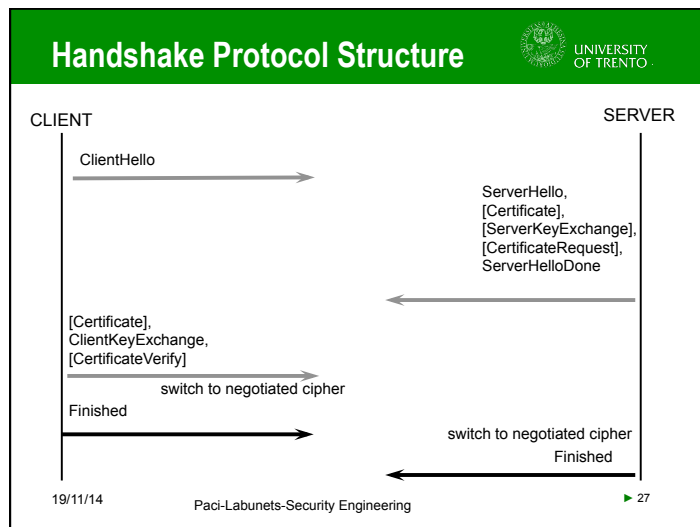
19/11/14
Paci-Labunets-Security Engineering
▶ 25

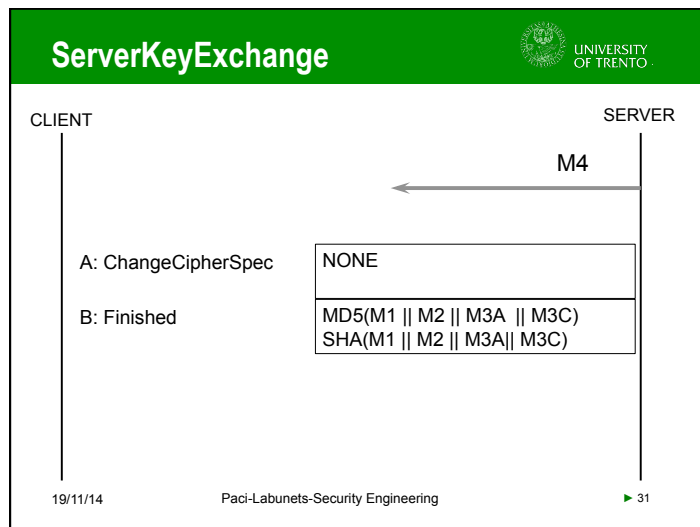
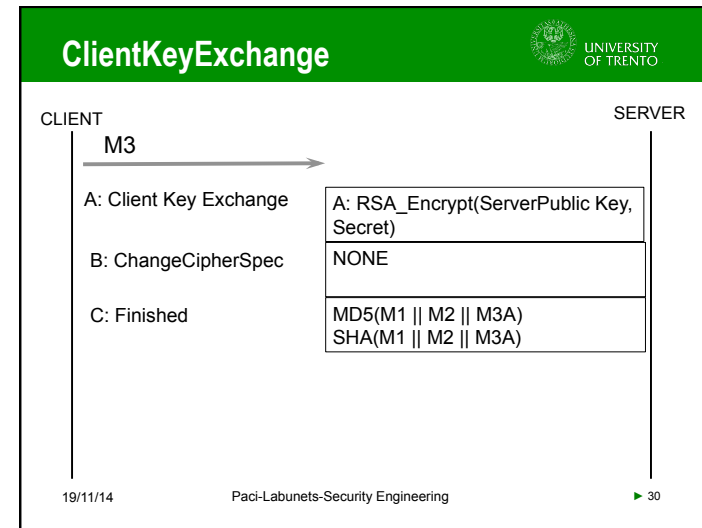
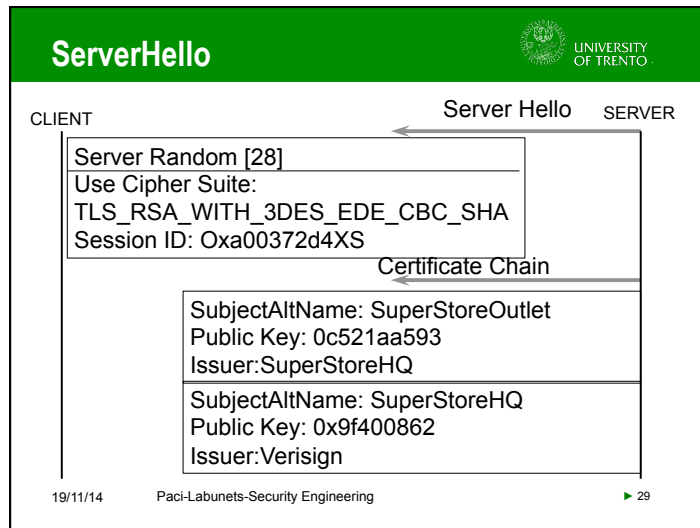
## TLS Handshake Protocol

UNIVERSITY OF TRENTO

- **Two parties: client and server**
- **Negotiate version of the protocol and the set of cryptographic algorithms to be used**
  - Interoperability between different implementations of the protocol
- **Authenticate client and server (optional)**
  - Use digital certificates to learn each other's public keys and verify each other's identity
- **Use public keys to establish a shared secret**

19/11/14
Paci-Labunets-Security Engineering
▶ 26





### Firewalls

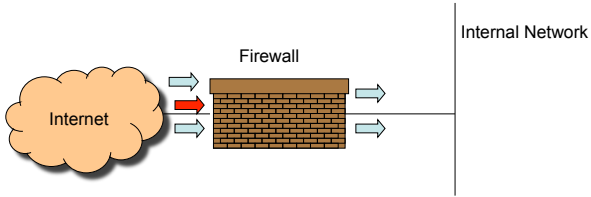
- **Lots of vulnerabilities on hosts in network**
- **Users don't keep systems up to date**
  - Lots of patches
  - Lots of exploits in wild (no patch for them)
- **Solution**
  - Limit access to the network
  - Put firewalls across the perimeter of the network

19/11/14
Paci-Labunets-Security Engineering
▶ 32



## Firewalls

- Firewall inspects traffic through it
- Allows traffic specified in the policy
- Drops everything else
- Two Types
  - Packet Filters, Proxies



19/11/14 Pacilabunets-Security Engineering 33

## Packet Filters

- Work at Network and Transport Layer
- Packet filter selectively passes packets from one network interface to another
- Usually done within a router between external and internal networks
  - screening router

19/11/14 Pacilabunets-Security Engineering 34

## Packet Filters

- Data Available
  - IP source and destination addresses
  - Transport protocol (TCP, UDP, or ICMP)
  - TCP/UDP source and destination ports
  - Packet options (Fragment Size etc.)
- Actions Available
  - Allow the packet to go through
  - Drop the packet (Notify Sender/Drop Silently)
  - Alter the packet (NAT)
  - Log information about the packet

19/11/14 Pacilabunets-Security Engineering 35

## Application-Level Proxies

- Implements the server and client part of the protocol on the firewall
- Proxy acts as a server for clients requests
  - Validate client requests
- Proxy act as a client and connects to the destination server

19/11/14 Pacilabunets-Security Engineering 36

## Firewall Rules

UNIVERSITY OF TRENTO

- **Permissive Policies**
  - Allow all traffic but block certain dangerous services
- **Restrictive Policies**
  - Block all traffic and allow only traffic know to meet a useful purpose such as HTTP, POP3, SMTP, SSH
- **An example:**
  - Allow from internal network to Internet: HTTP, FTP, SSJ, DNS
  - Allow from anywhere to mail server: SMTP
  - Allow from mail server to Internet: SMTP, DNS
  - Allow from inside to mail server: SMTP, POP3
  - Allow reply packets
  - Block everything else

19/11/14 Pacilabunets-Security Engineering
▶ 37

## Firewall Limitations

UNIVERSITY OF TRENTO

- **No protection against insider attacks**
- **No message content-based filtering**
- **No dection of protocol tunneling**
- **No encrypted messages filtering**

19/11/14 Pacilabunets-Security Engineering
▶ 38

## Intrusion Detection Systems

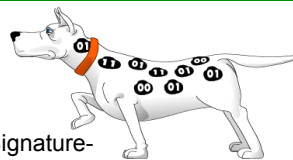
UNIVERSITY OF TRENTO

- **Firewalls allow traffic only to legitimate hosts and services**
- **Traffic to the legitimate hosts/services can have attacks**
- **Solution**
  - Intrusion Detection Systems
  - Monitor data and behavior
  - Report when identify attacks

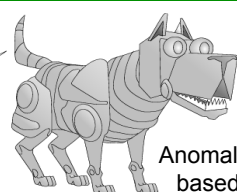
19/11/14 Pacilabunets-Security Engineering
▶ 39

## Types of IDS


UNIVERSITY OF TRENTO



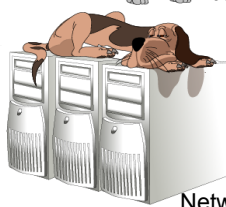
Signature-based



Anomaly-based




Host-based



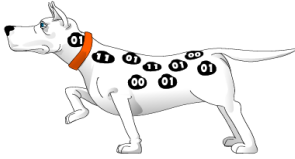
Network-based ▶ 40

19/11/14 Pacilabunets-Security Engineering
▶ 40

## Signature-based IDS


 UNIVERSITY OF TRENTO

- **Characteristics**
  - Uses known pattern matching to signify attack
- **Advantages**
  - Widely available
  - Fairly fast
  - Easy to implement
  - Easy to update
- **Disadvantages**
  - Cannot detect attacks for which it has no signature

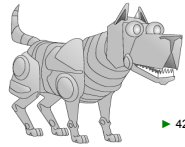


19/11/14
Paci-Labunets-Security Engineering
▶ 41

## Anomaly-based IDS


 UNIVERSITY OF TRENTO

- **Characteristics**
  - Uses statistical model or machine learning engine to characterize normal usage behaviors
  - Recognizes departures from normal as potential intrusions
- **Advantages**
  - Can detect attempts to exploit new and unforeseen vulnerabilities
  - Can recognize authorized usage that falls outside the normal pattern
- **Disadvantages**
  - Generally slower, more resource intensive compared to signature-based IDS
  - Greater complexity, difficult to configure
  - Higher percentages of false alerts




19/11/14
Paci-Labunets-Security Engineering
▶ 42

## Network-based IDS


 UNIVERSITY OF TRENTO

- **Characteristics**
  - NIDS examine raw packets in the network passively and triggers alerts
- **Advantages**
  - Easy deployment
  - Unobtrusive
  - Difficult to evade if done at low level of network operation
- **Disadvantages**
  - Different hosts process packets differently
  - NIDS needs to create traffic seen at the end host
  - Need to have the complete network topology and complete host behavior




19/11/14
Paci-Labunets-Security Engineering
▶ 43

## Host-based IDS


 UNIVERSITY OF TRENTO

- **Characteristics**
  - Runs on single host
  - Can analyze audit-trails, logs, integrity of files and directories, etc.
- **Advantages**
  - More accurate than NIDS
  - Less volume of traffic so less overhead
- **Disadvantages**
  - Deployment is expensive
  - What happens when host get compromised?




19/11/14
Paci-Labunets-Security Engineering
▶ 44

## Honeypots




- Information system resources whose value lie in their illicit use
- Systems to track attackers and learn about new attack techniques
- Low- interaction honeypots
  - Limited collection of an attacker's activities logs
  - Easy to be detected by an attacker
- High-interaction honeypots
  - Risk of being misused by the attacker



19/11/14 Pacil-Labunets-Security Engineering ▶ 45


## Network Security Standard



- ISO 27033:2009
- Part 1
  - Guidance on how to implement network security
  - Guidance and process on how to identify network security risks
  - Guidance on how to select security controls in ISO 27002
- Part 2
  - Guidance on how to implement a security architecture
- Part 3
  - Illustrates network specific security risks and threats

19/11/14 Pacil-Labunets-Security Engineering ▶ 46

## Reading Material



- Chapters 16 and 17. Dieter Gollman. Computer Security, Wiley.
- Chapters 6, 8, 9, 21. William Stallings and Laurie Brown. Computer Security: Principles and Practice, 3rd edition, Prentice Hall.

19/11/14 Pacil-Labunets-Security Engineering ▶ 47