Information Systems Security: exercises on security of IP networks

Diana Berbecaru

< diana.berbecaru @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

AY 2023-2024

Outline

- **questions + discussion on:**
  - network authentication protocols
    - IEEE 802.1x
  - security attacks:
    - DHCP security
    - ICMP security
    - ARP (poisoning)
    - TCP (SYN flooding)
    - DNS
  - IPsec and VPN
  - firewalls

Question 1

- **Assume a big company uses a WiFi Access Point (AP) with support for 802.1x and RADIUS for user authentication. What is the main role of the AP and what needs to be done to allow it to work when a new EAP method appears?**
  - A. allow to perform authentication (through a virtual port) of the users connecting to the AP by encapsulating the EAP messages received from the users (supplicant) into RADIUS messages sent to the AS
  - C. must be updated if new user authentication protocols appear and are supported by EAP
  - D. no change is needed if new user authentication protocols appear and are supported by EAP
  - E. allows to derive session keys (for supplicant and AP) to be used for packet authentication, integrity, and confidentiality

Question 2

- **Assume a small company uses a WiFi Access Point (AP) enabled with support for 802.1x to authenticate its employees when getting access to the corporate network (via a password). What is the main role of the Wi-Fi AP?**
  - A. allows to perform authentication of the users connecting to the AP
  - B. allows to derive session keys (for supplicant and AP) to be used for packet authentication, integrity, and confidentiality
  - C. allows to perform port-based access control: employees will not get access to the network until they are correctly authenticated

Questions
(Security attacks)

Question 1

- **DHCP protocol is subject to attacks because:**
  - A. the client asking the network configuration is not authenticated
  - B. the client asking the network configuration sends the request in broadcast
  - C. the response of the DHCP server is not authenticated
  - D. the response of the DHCP server is not encrypted

Question 2

- **Assume an attacker knows that a company uses DHCP to provide network configuration. What kind of security attacks can he mount (from the ones explained in the course)?**
  - A. DoS attack (against the DHCP server)
  - B. DoS attack (against the DHCP client)
  - C. MITM attack
  - D. Replay attack
  - E. Sniffing attack
  - F. DNS attacks (malicious name-address translation)

Question 3

- **ICMP is a commonly used protocol. What kind of security attacks can be mounted by exploiting its features (from the ones explained in the course)?**
  - A. Smurfing (by exploiting echo request/reply)
  - B. Ping flooding (by exploiting echo request/reply)
  - C. MITM attack (by exploiting redirect)
  - D. Replay attack (by exploiting source quench)
  - E. DoS attack (by exploiting source quench)
  - F. MITM attack (by exploiting time exceeded for a datagram)

Question 4

- **ARP is a commonly used protocol. ARP poisoning attack is possible because:**
  - A. the ARP responses are not authenticated
  - B. the association between the MAC address to an IP address is changed by the attacker (e.g. by using attack tools)
  - C. no defense exists against ARP poisoning attack

Question 5

- **TCP SYN flooding is a:**
  - A. DoS attack in which the attacker floods the victim with multiple ACK messages in the 3-way TCP handshake so that the victim cannot respond
  - B. DoS attack in which the attacker sends multiple TCP connection requests with IP source address of a non-existing node, but never sends the ACK
  - C. DoS attack which is possible because the victim allocates entries in the TCP connection table when receiving a SYN, and then is waiting for the corresponding ACK
  - D. an attack against which it is very difficult to defend from

Question 6

- **Indicate (some of the) possible attacks against DNS:**
  - A. DNS shadow server
  - B. DNS cache poisoning (affecting the local NS)
  - C. wrong configuration of the resolver on the (DNS) client
  - D. data corruption (on the victim node) or on the zone files
  - E. replay of DNS requests
  - F. capture sensitive information from the DNS responses
  - G. user privacy problems for the queries

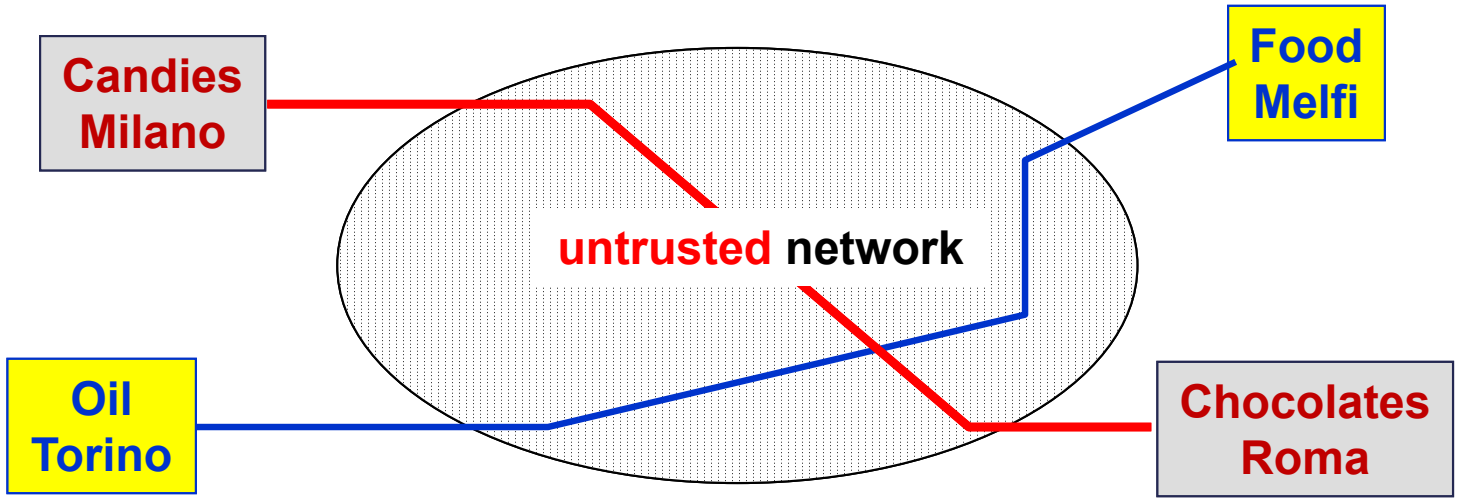
Questions
(IPsec and VPN)

Question 1

- **a VPN is:**
  - A. a technique to create a private network, typically uniting physically distant users or subnetworks through cryptographic protection of the network packets (secure IP tunnel)
  - B. a technique to create a private network, typically uniting physically distant users or subnetworks through the use of techniques such as:
    - private addressing,
    - protected routing (IP tunnel), or
    - via cryptographic protection of the network packets (secure IP tunnel)

Question 2

- assume that two companies (Oil Torino, and Food Melfi) decide to create a VPN via private IP addresses.

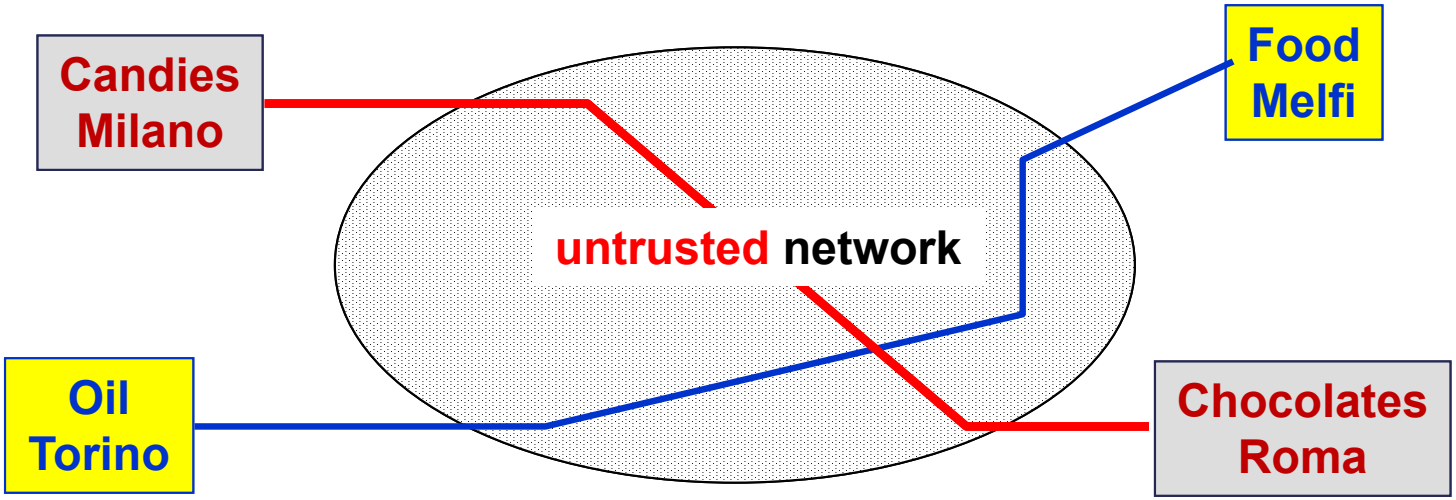


Question 2 - questions

- **which kind of attacks can be mounted by an attacker?**
  - A. assume an attacker in the network: inject fake packets by guessing or discovering the IP addresses used by the two companies
  - B. assume an attacker in the network: sniff the packets during transmission over the shared channels
  - C. assume an attacker inside telecom operator: get unauthorized access to the communication devices (routers) to intercept the transmission, replay, or inject new packets
  - D. assume an attacker (inside telecom operator or in the network): the DoS attack

Question 3

- **Assume two companies (Oil Torino and Food Melfi) decide to create a VPN via IP tunnel (IP in IP). Other two companies (Candies Milano and Chocolates Roma) also decide to create a VPN via IP tunnel (IP in IP).**

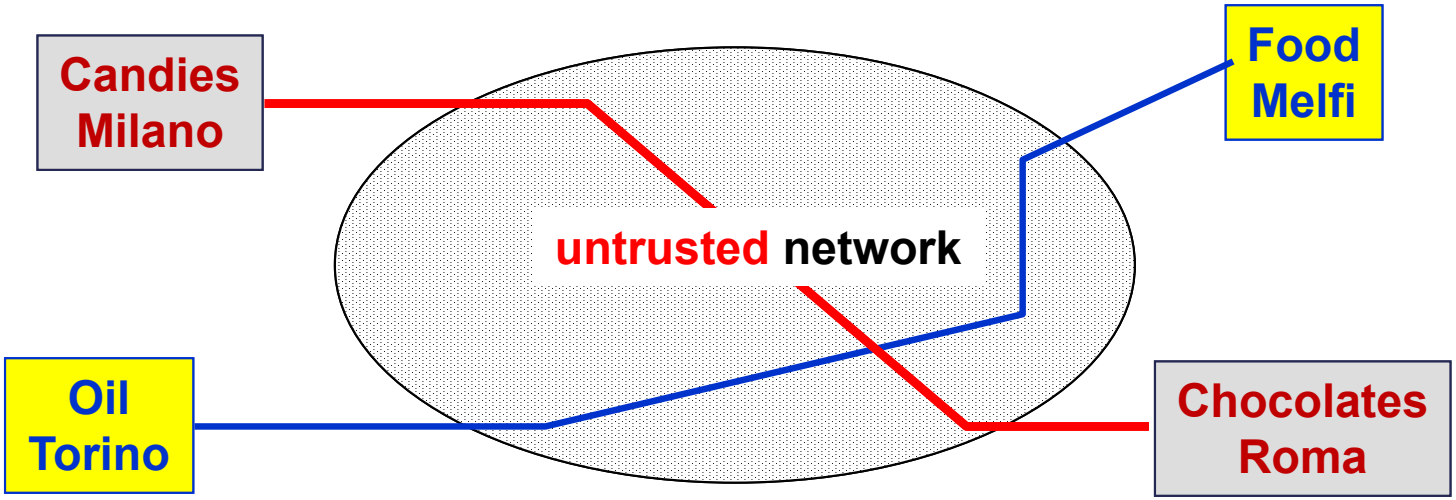


Question 3 - questions

- **Which kind of attacks can be mounted by an attacker?**
  - A. assume an attacker inside Candies Milano: he can inject fake packets by guessing or discovering the addresses used by Oil Torino
  - B. assume an attacker in the network: he can sniff (read the content of) the packets during transmission over the shared channels
  - C. assume an attacker inside telecom operator: if he can get unauthorized access to the communication devices (routers) then he can intercept the packets, replay, or inject new packets
  - D. assume an attacker (inside telecom operator or in the network): he can perform the DoS attack

Question 4

- **Assume two companies (Candies Milano and Chocolates Roma) decide to create a VPN via secure IP tunnel.**



Question 4 - questions

- **Which kind of attacks can be mounted by an attacker?**
  - A. an attacker inside Candies Milano: he can inject fake packets by guessing or discovering the addresses used by Oil Torino
  - B. an attacker in the network: he can sniff (read the content of) the packets during transmission over the shared channels
  - C. an attacker inside telecom operator: if he can get unauthorized access to the communication devices (routers) then he can intercept the packets, replay, or inject new packets
  - D. an attacker (inside telecom operator or in the network): he can perform the DoS attack

Question 5

- **the IPsec protocol provide security services:**
  - A. at application level
  - B. at transport level
  - C. at network level
  - D. at data link level

Question 6

- **the SPD in IPsec contains:**
  - A. list of active algorithms, keys, parameters to apply for the protection of the IP packets
  - B. list of rules that may depend on fields in the IP and transport-layer headers (e.g. destination address and port, source address and port, protocol) indicating whether IPsec need to be applied to the packet

Question 7

- **a company decides to adopt end-to-end security to protect communication between its end nodes. Moreover it decides each node must protect the IP packets both with AH and ESP. Assume two nodes A and B. Consider the node A: how many SAs and SPs does it need to configure in the IPsec module to communicate with the node B?**
  - A. one SA and one SP
  - B. two SAs and one SP
  - C. two SAs and two SPs
  - D. four SAs and two SPs

Question 8

- **Assume a company decides to adopt end-to-end security IPsec schema between all its nodes (placed at different locations). Which steps must be fulfilled to accomplish this task and which are the possible drawbacks?**
  - A. install (and configure) IPsec on all the nodes
  - B. in case ESP (with confidentiality) is used, then (internal) network monitoring, filtering of traffic based on the content, as well IDS will not be possible
  - C. install (and configure) IPsec only on the gateway
  - D. in case ESP is used, the IP header (original) is not protected when transmitted over the untrusted network
  - E. possible performance problems can be encountered at some hosts (e.g. ones acting as servers) due to IPsec load

Question 9

- **Assume a company decides to adopt Basic VPN IPsec schema between all its nodes (placed at different locations). Which steps must be fulfilled to accomplish this task and which are the possible drawbacks?**
  - A. install (and configure) IPSec on all the nodes
  - B. in case ESP (with confidentiality) is used, then (internal) network monitoring, filtering of traffic based on the content, as well IDS will not be possible
  - C. install (and configure) IPsec only on the gateway
  - D. in case ESP is used, the IP header (tunnel) is not protected when transmitted over the untrusted network
  - E. possible performance problems can be encountered at the gateway due to IPsec load

Question 9 - solution

- **Assume a company decides to adopt Basic VPN IPsec schema between all its nodes (placed at different locations). Which steps must be fulfilled to accomplish this task and which are the possible drawbacks?**
  - A. install (and configure) IPSec on all the nodes
  - B. in case ESP (with confidentiality) is used, then (internal) network monitoring, filtering of traffic based on the content, as well IDS will not be possible
  - C. install (and configure) IPsec only on the gateway
  - D. in case ESP is used, the IP header (tunnel) is not protected when transmitted over the untrusted network
  - E. possible performance problems can be encountered at the gateway due to IPsec load

Question 10

- **The (partial) protection against replay in IPsec is performed**
  - A. by a sequence number, inserted in the IP packet
  - B. by a sequence number, inserted in the AH or ESP headers
  - C. by counting how many packets have been received and confronting the number against a specific field in the AH or ESP headers
  - D. by exploiting a moving window (packets received that are outside the window are dropped)
  - E. by exploiting a moving window (packets received that are outside the window are accepted)

Question 10 - solution

- **The (partial) protection against replay in IPsec is performed**
  - A. by a sequence number, inserted in the IP packet
  - B. by a sequence number, inserted in the AH or ESP headers
  - C. by counting how many packets have been received and confronting the number against a specific field in the AH or ESP headers
  - D. by exploiting a moving window (packets received that are outside the window are dropped)
  - E. by exploiting a moving window (packets received that are outside the window are accepted)

Question 11

- **What is IKE in IPsec?**
  - A. an important component in IPsec that automates key establishment by using RSA
  - B. a combination of a protocol needed to negotiate, set-up, modify and delete a SA (ISAKMP) and a protocol for authenticated key exchange of symmetric keys (OAKLEY)
- **How IKE supports the negotiation of SAs?**
  - A. it creates first a SA to protect the ISAKMP exchange; then this SA is used to protect the negotiation of the SA needed by IPsec traffic
  - B. it creates directly a SA used to protect the IPsec traffic

Question 11 - solution

- **What is IKE in IPsec?**
  - A. an important component in IPsec that automates key establishment by using RSA
  - B. a combination of a protocol needed to negotiate, set-up, modify and delete a SA (ISAKMP) and a protocol for authenticated key exchange of symmetric keys (OAKLEY)
- **How IKE supports the negotiation of SAs?**
  - A. it creates first a SA to protect the ISAKMP exchange; then this SA is used to protect the negotiation of the SA needed by IPsec traffic
  - B. it creates a SA used to protect the IPsec traffic

Questions (Firewalls)

Question 1

- **Which are the design goals of a (network) firewall?**
  - A. only the ‘authorized’ traffic can traverse the firewall
  - B. the firewall must detect traffic that does not satisfy specific rules and raise alarms
  - C. the firewall must be a highly secure system itself
  - D. the firewall is a special purpose device which allows to creates secure tunnels with the internal trusted nodes
  - E. the firewall must be the only contact point between the internal network and the external one

Question 1 - solution

- **Which are the design goals of a (network) firewall?**
  - A. only the ‘authorized’ traffic can traverse the firewall
  - B. the firewall must detect traffic that does not satisfy specific rules and raise alarms
  - C. the firewall must be a highly secure system itself
  - D. the firewall is a special purpose device which allows to creates secure tunnels with the internal trusted nodes
  - E. the firewall must be the only contact point between the internal network and the external one

Question 2

- **Assume a company decides to adopt the default-deny (named also allowlist) authorization policy for its firewall configuration. What does it mean?**
  - A. by default, every network service is denied
  - B. by default, every network service is allowed
  - C. the administrator must create a list of few known services and configure the firewall to allow access only to those services
  - D. the adminsitrator must create a list of potentially dangerous services and configure the firewall to block access for that services

Question 2 - solution

- **Assume a company decides to adopt the default-deny (named also allowlist) authorization policy for its firewall configuration. What does it mean?**
  - A. by default, every network service is denied
  - B. by default, every network service is allowed
  - C. the administrator must create a list of few known services and configure the firewall to allow access only to those services
  - D. the adminsitrator must create a list of potentially dangerous services and configure the firewall to block access for that services

Question 3

- **Assume a company decides to adopt a packet filter (as firewall) placed at the border router between the external network and the internal one. What does it mean?**
  - A. the administrator must create a list of rules containing (typically) source IP address, source port number, destination IP address, destination port number, protocol (e.g., tcp, udp) and the action to be performed on the packet (allow, drop)
  - B. administrator must install a specific filter on the router, one for each application (e.g. FTP, SMTP, HTTP, TELNET)
  - C. the administrator may easily block attacks originating from IP addresses that are traced
  - D. the internal nodes are very well protected from external attacks (e.g. TCP SYN flooding or ping bombing)

Question 3 - solution

- **Assume a company decides to adopt a packet filter (as firewall) placed at the border router between the external network and the internal one. What does it mean?**
  - A. the administrator must create a list of rules containing (typically) source IP address, source port number, destination IP address, destination port number, protocol (e.g., tcp, udp) and the action to be performed on the packet (allow, drop)
  - B. administrator must install a specific filter on the router, one for each application (e.g. FTP, SMTP, HTTP, TELNET)
  - C. the administrator may easily block attacks originating from IP addresses that are traced
  - D. the internal nodes are very well protected from external attacks (e.g. TCP SYN flooding or ping bombing)

Question 4

- **Assume a company decides to adopt a 'dual-homed gateway' architecture to protect access to his web server (placed on the internal network). What does it mean?**
  - A. the administrator must create a list of rules for the packet filter containing (typically) source IP address, source port number, destination IP address, destionation port number, protocol and the action (allow, drop) to be performed on the packet
  - B. administrator must install a specific application filter on the GW for the web traffic (HTTP/S)
  - C. if the web server has a bug, the internal nodes are protected anyway
  - D. the administrator must configure two (filtering) systems instead of one

Question 4 - solution

- **Assume a company decides to adopt a 'dual-homed gateway' architecture to protect access to his web server (placed on the internal network). What does it mean?**
  - A. the administrator must create a list of rules for the packet filter containing (typically) source IP address, source port number, destination IP address, destionation port number, protocol and the action (allow, drop) to be performed on the packet
  - B. administrator must install a specific application filter on the GW for the web traffic (HTTP/S)
  - C. if the web server has a bug, the internal nodes are protected anyway
  - D. the administrator must configure two (filtering) systems instead of one

Question 5

- **Assume a company decides to adopt a 'screened host' architecture to protect access to his web server (placed on the same subnetwork of the gateway). What does it mean?**
  - A. the administrator must create a list of rules for the packet filter containing (typically) source IP address, source port number, destination IP address, destionation port number, protocol and the action (allow, drop) to be performed on the packet
  - B. administrator must install a specific application filter on the GW for the web traffic (HTTP/S)
  - C. if the packet filter has a bug, the internal nodes are protected anyway
  - D. the administrator must configure two (filtering) systems instead of one

Question 5 - solution

- **Assume a company decides to adopt a 'screened host' architecture to protect access to his web server (placed on the same subnetwork of the gateway). What does it mean?**
  - A. the administrator must create a list of rules for the packet filter containing (typically) source IP address, source port number, destination IP address, destionation port number, protocol and the action (allow, drop) to be performed on the packet
  - B. administrator must install a specific application filter on the GW for the web traffic (HTTP/S)
  - C. if the packet filter has a bug, the internal nodes are protected anyway
  - D. the administrator must configure two (filtering) systems instead of one

Question 6

- **Assume a company decides to adopt a 'screened subnet' architecture to protect access to his web server (placed on the same subnetwork of the gateway). What does it mean?**
  - A. the administrator must create a list of rules for two packet filter(s), possibly from different vendors, containing (typically) source and destination IP addresses and port numbers, protocol and the action (allow, drop) to be performed on the packets
  - B. administrator must install a specific application filter on the GW for the web traffic (HTTP/S)
  - C. if one packet filter has a bug, the internal nodes are protected anyway
  - D. the administrator must configure two (filtering) systems instead of one

Question 6 - solution

- **Assume a company decides to adopt a 'screened subnet' architecture to protect access to his web server (placed on the same subnetwork of the gateway). What does it mean?**
  - A. the administrator must create a list of rules for two packet filter(s), possibly from different vendors, containing (typically) source and destination IP addresses and port numbers, protocol and the action (allow, drop) to be performed on the packets
  - B. administrator must install a specific application filter on the GW for the web traffic (HTTP/S)
  - C. if one packet filter has a bug, the internal nodes are protected anyway
  - D. the administrator must configure two (filtering) systems instead of one