CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2023-10-06, 14:00 – 18:00

No extra material **is allowed** during the exam except for an English language dictionary in paper form.

The last page of this exam contains pictures of some protocols and headers that *may* be useful in some questions.

Write in a clear manner and motivate (explain, justify) your answers. If an answer is not explained/justified, it will get significantly lower or zero marking. If you make any assumptions in your answer, do not forget to clearly state what you assume.

A good rule-of-thumb for how much detail to provide, is to include enough information and explain so that a person who has not taken this course can understand the answer.

Questions must be answered in English.

Teacher: Tomas Olovsson, 031 – 772 1688
Dept. of Computer Science and Engineering

CTH Grades:	30-38 → 3	39-47 → 4	48-60 → 5
GU Grades:	30-47 → G		48-60 → VG

1. Attacks and DoS

a) In the Smurf attack, ICMP echo or UDP is used to do *packet magnification*. How does such an attack work? How can this problem be addressed? (2p)

It sends ICMP echo messages to a broadcast address with a victim as the sender. All hosts on the network will then send an ICMP echo reply message to the victim, thus one packet generates a storm of packets to the victim. Firewalls should block all external traffic to broadcast addresses to avoid its hosts to be used as senders of the traffic.

b) The possibility to fragment IP datagrams has been shown to be problematic. Describe two different problems or attacks which exploit fragmentation and explain how they work! (4p)

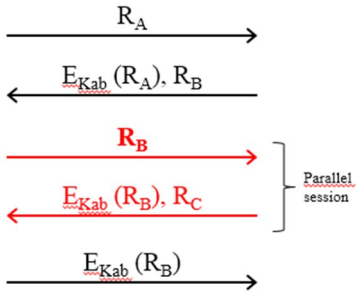
* Reassembly can be done in different ways for end-hosts, hard for IDS or FW to know.
* Fragment reassembly (DoS): send only one fragment per datagram making the receiver allocate buffer space for the full datagram.
* Fragment ID reveals information (OS fingerprinting).
* IDLE or Dumb scanning using a trusted system to check available resources (see slides).
* Send oversized datagrams (> 65,535 bytes) using fragments.

Etc.

c) UDP scanning is harder to do than TCP scanning. Why? What is the problem? How can operating systems, at least to some degree, protect themselves against leaking information about open UDP ports? (2p)

It is hard to know whether a UDP message is accepted or silently dropped. However, if a host responds with an ICMP (port unreachable) message, it is not open. Protection can be to limit the number of transmitted ICMP messages to, for example, one per second.

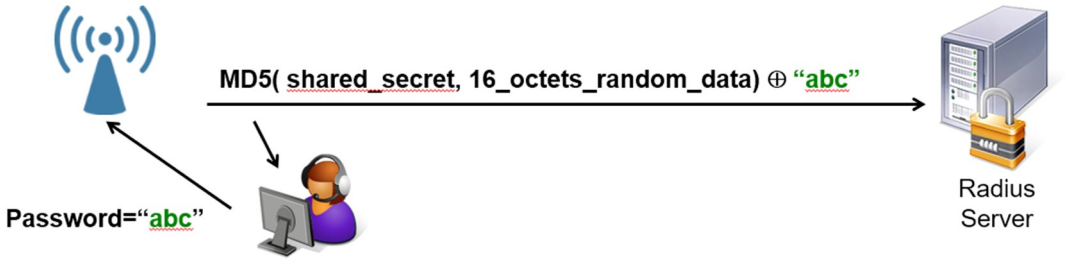
d) Some protocols are vulnerable against reflection attacks as shown in the figure:



What is meant by a reflection attack? Explain how this attack works and how it can be avoided! (2p)

It is an attack where a completely symmetric protocol can use the originator (server) to answer the question it asked the client to answer. See slides from "User authentication" lecture.

2. Authentication, encryption



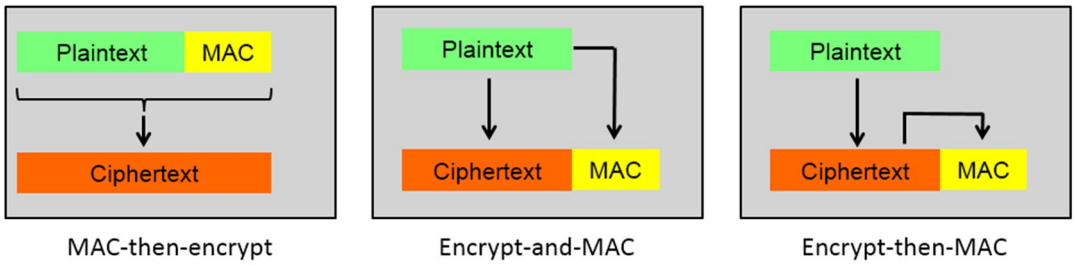
a) In the picture above, we can see an attack against a Radius server. What is the purpose of this attack? What is it the attacker tries to do? Explain how it works! (2p)

The only unknown in the request to the Radius server is the "shared secret" and it may be possible to do (an exhaustive) offline search to find the secret. The secret could be a word from a dictionary, for example.

b) Can a rainbow table be of help to the attacker in the example above? Why/why not? (2p)

It is not useful since the hash (MD5) contains random data. This data is known by the attacker but it is impossible to create pre-calculated tables since each message is unique.

c) In the course, we discussed three different ways to add MACs: MAC-then-encrypt, Encrypt-and-MAC and Encrypt-then-MAC, see the picture below.

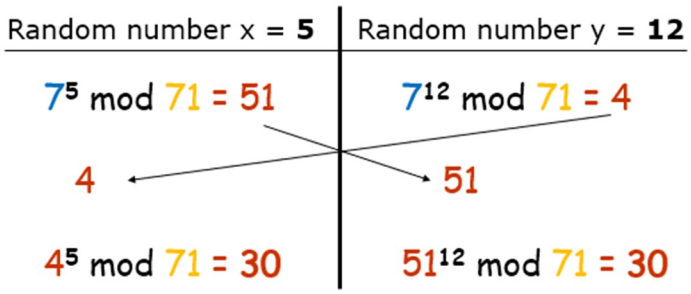


There are some pros and cons with each solution. IPsec uses the last method (Encrypt-then-MAC). Give an argument for (or against) each of these three methods when compared to the other. Motivate clearly why this is (or is not) advantageous! (3p)

See slide from lecture.

d) The Diffie-Hellman algorithm can be used to negotiate crypto-keys between two parties. What fundamental property does it rely on? Show with an example how it works with very simple numbers! (You don't have to motivate how the numbers are selected, just how they are used.) (3p)

It is based on the fact that $(g^x)^y = (g^y)^x$ and that factorization of large numbers are very hard. A simplified example (full points even if modulo was not shown):


Random number x = 5
Random number y = 12
7^5 mod 71 = 51
7^12 mod 71 = 4
4
51
4^5 mod 71 = 30
51^12 mod 71 = 30

3. Firewalls and IDS systems

a) What is a DMZ, where is it located and what purpose does it have? (2p)

It is a dedicated network outside the internal network which host external services, such as web servers, mail servers and other systems offering services to the outside world (see lecture slides). Purpose is to avoid forwarding traffic to public servers to the internal network.

b) UDP traffic is in general harder to protect by a firewall than TCP traffic. Why? (2p)

TCP is a stateful protocol and includes sequence numbers and a well-known protocol for session setup. A firewall can check that this procedure is followed and that segments that are received fit into the communication stream. UDP has no setup procedure nor any sequence numbers so the firewall has no way to know whether a datagram with a faked IP address is legitimate or not but has to pass it to the receiver unless it understands the application level protocol.

c) A stateful firewall must maintain a list of filter rules and also a state table. Give an example of what the state table should contain for TCP and UDP traffic! (2p)

TCP: IP addresses and port numbers of the parties, TCP sequence numbers, TCP state.
UDP: IP addresses and port numbers plus a timer for when to terminate the connection.

d) *Circuit level gateways* and *application-level gateways* work differently from "normal" packet filtering/inspection firewalls. Explain how they work! (4p)

Circuit-level gateways are firewalls terminating the TCP connections. It opens a new TCP connection to the other side to avoid TCP and IP headers being forwarded. The application-level protocol is not touched.

Application-level gateways also terminate the application protocol such as Telnet, FTP, SMTP, etc. It extracts the data and creates a new connection to the other side with new application headers.

4. Cryptographic protocols and WLAN

a) Encrypting traffic is not enough to guarantee freshness. Explain why not! Mention two different ways to guarantee freshness! (2p)

Freshness is to make sure packets are not replayed, which is possible even if they are encrypted. Including time stamps, sequence numbers or nonces can make it impossible to replay old packets. (Many answers possible here)

b) Many security protocols support sending messages without encryption (encryption=NULL) and can still be protected against packet modification. Describe how this is done! (2p)

The protocols can use a keyed hash (e.g. HMAC) where a key is used together with the plaintext to authenticate (sign) the data: hash(key || text).
It requires the key to be known by both parties and protects the contents of the message even if it is not encrypted.

c) Even though WEP encrypted traffic contains an encrypted checksum, it cannot prevent an attacker from modifying the packets. Explain why this is possible and explain how WEP should have been designed to avoid this problem! (2p)

WEP uses a linear CRC function to check packet integrity. With a CRC function, it is possible to calculate exactly what bits in the checksum need to be changed when a bit is changed in the input (a hash requires a complete recalculation). It does not matter whether the data or CRC is encrypted, a bit change is still possible to do.

d) WEP has at least one problem with its handling of IVs. Explain how an attacker may use this weakness! Is this problem likely to occur? (2p)

WEP allows an IV to be reused, we will have two packets encrypted with the same byte stream (since same shared key + IV being used to create the stream). This means that an XOR operation between the cipher texts will result in an XOR of the cleartexts: $c1 \oplus c2 = (p1 \oplus b) \oplus (p2 \oplus b) = p1 \oplus p2$. Since the IV is only a 24-bit value, a busy AP is very likely to reuse IVs. In fact, a busy AP will exhaust the available space in about 5 hours.

e) A feature present in WPA and WPA2 is 802.1x – port-based authentication. What is this? What does it do? How? (2p)

Port-based authentication is a link-level mechanism where a client does not get access to the network unless authenticated and authorized. It uses Radius for central authentication and authorization. When the Radius server accepts the user, full network access is given.

5. TLS and IPsec

a) TLS consists of several protocols (see the last page). Describe the functionality of the record layer, change cipher, alert and handshake protocols! (4p)

Record layer performs fragmentation -> compression -> adding MAC -> encryption.
Change cipher tells the other side to change to the last security parameters negotiated (and turn on encryption).
The alert protocol sends warnings and error messages to the other side.
The handshake protocol negotiates ciphers, keys and performs authentication.

b) SSL/TLS has a "close session" message which is used when they want to quit. Why is it needed? Why not just tear down the TCP connection instead? TCP already has a mechanism to close connections. (2p)

To prevent truncation attacks. We don't want an attacker (for example a MITM) to be able to prematurely terminate a connection between the client and the server by faking a FIN in each direction (doing a perfectly normal TCP close). This could result in both sides believing that all data has been sent and received even if some data at the end was removed by the attacker.

c) IPsec supports both tunnel and transport mode. Why? What is the difference? (2p)

Tunnel mode is used in site-to-site VPN systems and is often used between firewalls that take incoming IP messages, encrypts them and sends them to the other end (keeps original IP header inside IPsec datagram). End systems do not have to be aware of encryption.
Transport mode offers end-to-end encryption, for example between a client and a server.

d) On the last page, there is a picture of an IPsec header. Explain what the *next header and SPI fields* are used for and what purposes they have! (2p)

The SPI is an index that tells what SA (security association) should be used, i.e. a pointer to a data structure containing info about the type of connection, keys used, etc.
Next header tells what upper layer protocol should receive this data.
Padding can be used to hide the actual amount of data being transmitted (or to extend the payload to be an even multiple of the block cipher).

6. Link level security and network design

a) ARP spoofing can be a problem for hosts, but there are several possible countermeasures that, at least to some degree, can solve the problem. What is ARP spoofing? What is the goal of this attack? How can a host, at least partly, protect itself against such attacks? Mention one possible countermeasure and explain how it works! (4p)

ARP spoofing is a way to erroneously send or respond to ARP queries on the network ("who has IP address 1.2.3.4?") and make computers send IP messages to the attacker's computer instead of to the correct destination. Most systems will accept the first answer they get and treat it as valid. This way it is possible to spawn man in the middle attacks.

Possible protection mechanisms:
- Define important IP-address to MAC address translations as static (use static ARP entries),
- Try old MAC address before accepting a new address (Linux "Antidote" patch)
- Use secure ARP
- Never accept changes in IP-address and MAC address mappings (manual reconfiguration needed)

b) Is link-level authentication ever implemented? If so, give an example of how it may work and the purpose! (2p)

802.1x – port-based authentication. Before a user or a device is given network access through a switch, authentication needs to take place.

c) In the course, we have looked briefly at the Jericho Forum and their thoughts. They argue that the traditional model having a main border firewall protecting the internal network is soon outdated and that a new model for security is needed. Give some arguments supporting these thoughts! What solution do they propose (short answer only)? (4p)

The Jericho model, or zero-trust architecture is based on that:
- services nowadays are located both on internal networks and on external (e.g. cloud) servers,
- that own users are located both on the inside and on the outside of the border firewall,
- remote access by partners and other are needed to selected resources
- WLAN access on internal networks bypass the firewall if compromised
- authorization should not be based on being on the inside or not, but based on who the user is, how (s)he is authenticated, role in the organization, etc.

It is therefore impossible to control security with only a border firewall that only sees a small part of all traffic. The solution is to move protection closer to the endpoints: toward the users/client systems and to application servers.

Headers and pictures that may be useful