T-110.6220 Special Course in Network Security
Lecturer: Tuomas Aura
Examination 2008-12-15 marking criteria

Part 1:

(a) B uses a random number generator to select the values of the nonce N_B and the session key SK.

(b) The certificate must be issued to B by a certification authority (CA) that is trusted by A.

(c) No, B selects the session key SK alone.

(d) Yes, for both A and B. B is authenticated by B's signature on A's nonce in message 2. A is authenticated by message 3 because only A can know the session key and send this message. (B knows that message 3 is fresh because the session key is fresh.)

(e) No, if A's private key, which is a long-term secret, is compromised later, the attacker can recover the session key from recorded message 2.

(f) Entity authentication of A is lost and, of course, also the key confirmation for A.

(1p each)

Part 2:

(a) The oldest and most important threat is unauthorized access to the mailbox, i.e., that someone else can read your email. Another major threat is that the service could be used to send spam. There are many other threats such as sniffing the email contents from the network, forged emails, spreading of malware, phishing, DoS attacks by filling mailboxes etc. (2p for mentioning at least two completely different threats. One of them has to be the unauthorized access, although that could be implied e.g. by referring to access control or user authentication in answers (a) or (b).)

(b) TLS between the user workstation and the email service prevents sniffing of the login password and, thus, helps to secure access control for the mailbox. It also prevents sniffing of email between the user and the server. TLS does not help with the other threats, especially not with anything that has to do with the content of the emails. (2p)

(c) TLS is between TCP (i.e., transport layer) and applications. (2p)

Part 3:

(a) Your conclusion can be *yes* or *no* depending on which threats and use cases you are considering. If IPsec is used as a VPN tunnel and all application data is sent thought the tunnel, then the security of the access network has no effect on the security of those applications. On the other hand, if the IPsec tunnel is used only to access intranet services and the client also accesses the Internet directly or accesses services local to the access link, then WLAN security mechanisms can prevent sniffing and man-in-the-middle attacks on the wireless link. Even with a VPN, there may be an initial period when the client uses services on the local network, such as DNS. Moreover, from the WLAN network operator's point of view, it may be necessary to control access to the WLAN and services on it, even if you as a user don't care. (2p for making a good argument for each side)

(b) Certificates are revoked when (i) they were issued mistakenly, (ii) the conditions for issuing the certificate no longer hold, or (iii) the subject private key may have been compromised. For WLAN access, case (ii) is the most common when the user's employment or service subscription is terminated. Case (iii) occurs when the user computer has been lost or stolen. Certificates are *not* revoked when they expire! (2p for two different situations)

(c) Passive observers only sniff the IMSI when the user connects to a new network for the first time, e.g., after arriving in a new country. After that, a temporary identifier TIMSI is assigned to the mobile. An active attacker can still use an IMSI catcher, which pretends to be a base station and asks the mobile for the IMSI. (2p for making two of these points)

Part 4:

(a) Kerberos is used for user authentication for intranet services.

(b) A denotes the user and the client workstation, AS is the authentication server, TGS is the ticket granting server, and B is the service that the user wants to access.

(c) TGT is the ticket granting ticket. The client workstation receives it from the authentication server after user authentication, and it is used to obtain Tickets from the TGS. Ticket is used for authenticating the user to a specific service.

(d) Preauthentication proves to AS that the sender of message 1 knows the user's password and the key K_A, which is derived from the password. This prevents remote attackers from obtaining the TGT by spoofing message 1. This is important because an attacker could use the TGT for brute-force cracking of the user password.

(e) There are many good answers. The keys used for protecting TGT and Ticket are different (unless the TGS is also the server B, which it is not in any realistic setting), which means that the replayed tickets cannot be decrypted. Moreover, Kerberos tickets are encoded with ASN.1 DER encoding roles, which include a type tag in every message and message part. This is a general mechanism that prevents replay attacks where messages or their parts are used out of context. Data fields in the data structures may also act as implicit type tags that would cause the wrong ticket to be rejected.

(f) Identity delegation in Kerberos means that the client gives its TGT and secret key ($K_{A\text{-}TGT}$) to a service so that the service can impersonate the client to other services. For example, the client could delegate the user's identity to a database frontend server so that the frontend server can access the backend database server with the user's access rights.

(1p each)

Part 5:

(a) The intention is to allow outbound HTTP and HTTPS connections from the local network to the Internet, and nothing else. No inbound connections should be allowed. (2p)

(b) An attacker on the Internet can open a TCP connection to any host and port on the local link if it uses the client port 80 or 443. (To use these privileged ports as the client port, the attacker needs to modify the client software and also needs root access on his own computer.) (2p)

(c) Two different solutions depending on the functionality of the firewall: In a stateful firewall, the first rule (for outbound packets) can be configured to create a temporary state in the firewall and the second rule (for inbound packets) can be made to check for the state. That is, inbound packets are allowed only if the same host on the intranet has first sends an outbound packet such as TCP SYN for the same TCP connection. In a stateless firewall, the second rule can be configured to allow only packets where the ACK flag is set. This prevents the Internet hosts from sending inbound SYN packets (which do not have the ACK flag set) and, thus, from opening inbound TCP connections. (2 p for one solution)

Part 6:

The attacker can add the target company's employees onto thousands of email mailing lists and post their email addresses on the web so that they get added onto spam lists. Many email lists prevent this by verifying the new addresses with a confirmation email that contains a key that must be emailed back or sent to a web server to confirm the subscription. The attacker can mount the same kind of attack by adding the company's employees on physical mailing lists, such as by subscribing to hundreds of mail-order catalogs. This could be prevented with a similar protocol where the customer is asked to confirm the subscription, although that is no done in practice. The attacker can cause a flash crowd of thousands or millions of web surfers to access the company's web server by posting a link to the server onto popular web sites or blogs, such as Slashdot. A small company's web server is often not planned to handle more than a few queries at a time and will fail. This attack is more difficult to prevent because it depends on a larger crowd who each may send only few TCP SYN packets or download a part of a web page before giving up. (This is an open-ended problem and there are many ways of answering. 6p for a relatively complete answer.)