T-110.5240 Network security
Lecturer: Tuomas Aura
Examination 2010-05-18

Answer at most 5 of the 6 parts. (If you answer too many, Part 6 will not be marked.)

Part 1: Key-exchange protocols

Consider the following key-exchange protocol:

1. $A \rightarrow B$: g, p, g^x
2. $B \rightarrow A$: $g^y, E_{SK}(g^y, g, p, g^x, S_B(g^y, g, p, g^x), Cert_B)$
3. $A \rightarrow B$: $E_{SK}(g, p, g^x, g^y, S_A(g, p, g^x, g^y), Cert_A)$

$SK = h(g^{xy})$

(a) Does this protocol provide mutual authentication?
(b) What is SK and where is it needed?
(c) What is $Cert_A$ and where does A get it from?
(d) If an attacker compromises the server A, is it possible for the attacker to recover old session keys?
(e) Does this protocol provide identity protection for A and B? Why?
(f) Does this protocol provide key confirmation for A and B? Why?

Part 2: Email security

A university webmail server, such as *webmail.tkk.fi*, allows users to read their email with a web browser.
(a) What security threats should be considered by the designers and implementers of the webmail service? (b) Which of these security threats can and which cannot be mitigated by using TLS? Why?

Part 3: TLS

The following diagram is from the TLS specification. Explain the approximate contents and purpose of the messages in a *typical* TLS handshake that uses the RSA key exchange algorithm. (You can choose another key exchange algorithm, such as DHE_DSS, instead of RSA, but RSA is the simplest method to explain.)

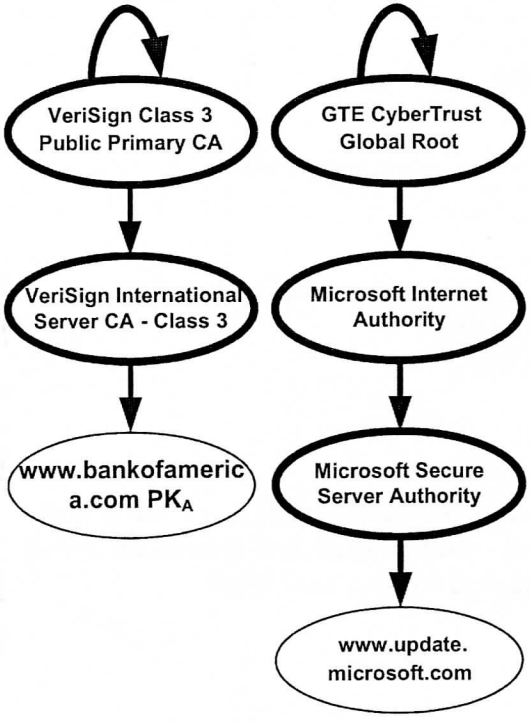
```
Client                                               Server

ClientHello                  -------->
                                                ServerHello
                                               Certificate*
                                         ServerKeyExchange*
                                        CertificateRequest*
                             <--------      ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                     -------->
                                          [ChangeCipherSpec]
                             <--------             Finished
Application Data             <------->     Application Data
```

Part 4: Wireless security

Alice has configured her wireless access point and laptop computer to use *WPA2-Personal*. Explain the protocol that takes place when the laptop connects to the access point.

Part 5: PKI



The picture on the left shows two certificates chains from actual web sites.

(a) Explain *in detail* how the web browser checks a certificate chain of arbitrary length and how it is used in an authenticated key exchange to authenticate the web site. 5p

(b) What security reasons are there for VeriSign and Microsoft to have two CAs in the chain and not just one? 1p

Part 6: Firewalls

Consider the following stateless firewall rules:

Protocol	Src IP	Src port	Dst IP	Dst port	Action
TCP	223.20.13.0/24	*	*	80,443	Allow
TCP	*	80,443	223.20.13.0/24	*	Allow
*	*	*	*	*	Block

(a) What kind of security policy does the firewall try to implement?

(b) What security problem is there with the rules?

(c) Fix the firewall rules so that they implement the intended policy. (Explain also, what kind of additional features your solution requires from the firewall.)