Exercise 2, Standards and how to read them

T-110.6220 course staff

November 17, 2008

Introduction

You should complete the excercises in pairs and write down the answers together. When you are finished, email your answers to the course email address.

1 ISO/IEC 9798-4

The ISO/IEC 9798-4 standard defines a mechanism for entity authentication using a cryptographic check function. The protocol can be abstracted as follows:

A $\rightarrow$ B: N_A
B $\rightarrow$ A: N_B, $f_K(N_A, N_B)$

a What are N_A, N_B, K and f?

b What security goals does this protocol achieve? What are its limitations?

c If you have access to the standard, what answers does the standard give to question (b)?

d Design a similar protocol with only one message. What are its limitations?

Sources:

- ISO/IEC 9798-4:1999(E). Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function, 1999.

2 Time sync attacks

Some possible sources of time synchronization in network nodes are

a NTP

b GPS

c GSM

What kind of security mechanisms exist for these protocols and how difficult would it be for an attacker to cause an Internet host to misconfigure its clock, e.g., to be one hour or one year off?

Sources:

- `http://www.ietf.org/html.charters/ntp-charter.html` (see the referenced RFCs and IDs)
- `http://www.kowoma.de/en/gps/index.htm` (scroll down for the contents)
- Find more data by yourself

3 Seeing the big picture

Why is Kerberos used on the intranets and TLS/SSL on the Internet? Could it be the other way?

Sources:

- `http://www.ietf.org/html.charters/krb-wg-charter.html`
- `http://www.ietf.org/html.charters/tls-charter.html`

4 ASN.1 and DER

Save the DER-encoded certificate from `https://noppa.tkk.fi/noppa/kurssi/t-110.6220/` into a file and decode manually the extended key usage field. A hex editor is a good tool for instance. *Hint:* the fields are in exactly the same order as they appear in your browsers certificate viewer (at least in Firefox, your mileage may vary).

Sources:

- `http://www.itu.int/rec/T-REC-X.680/en` (unfortunately, not available free)

- http://www.ietf.org/rfc/rfc5280.txt
- http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf BER, CER and DER