ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Family Name: _____

First Name: _____

Section: _____

Student Seminar: Security Protocols & Applications

Final Exam - Part 2: Wireless Sensor Networks

July 16th, 2007

This document consists of 5 pages.

Instructions

Electronic devices are *NOT allowed.*

Books and lecture notes are *allowed.*

Answers must be written in the boxed spaces provided on these sheets.

Answers can be written either in French or in English.

Questions of any kind by students during the exam will certainly *not* be entertained.
Potential errors in these sheets are part of the exam.

Wireless Sensor Networks

1. **Tynisec:** In Tynisec, a counter is sent explicitly with each packet as part of the IV. The counter only has 16 bits. If an attacker was to observe 2^{16} packets sent by one node to another he might obtain two packets with identical IVs.

   (a) What kind of attack could be carried out based on the fact that two packets have the same IV?

   (b) Would sending a counter made of more bits prevent replay attacks? Why?

   (c) Give an argument that explains why it can actually be better to give up replay protection in a wireless sensor network protocol.

2. **Minisec-U:** MiniSec-U only sends the x least significant bits of its IV counter in order to save on transmission energy. If the receiver can not verify the MAC with the resulting value of the counter it will try to increment the counter y times by 2^x until it gives up and runs a resynchronization protocol. Counter resynchronizations can be avoided if two sucessfully received packets are less than $y2^x$ appart.
   For a given maximum number N of lost packets between two sucessfully received ones there are different ways of chosing x and y in order to avoid resynchronization.

   (a) From the initial motivation of this scheme, one could believe that the best solution would be to chose $x = 0$ and $y = N$ to save a maximum of energy. Why is this not true?:

   (b) Looking closer at this problem, name all the parameters on which the optimal solution for x and y depends:

(c) Describe a simple denial-of-service attack against this scheme

(d) What is the damage that your attack causes to the systems?

3. **Minisec-B:** Minisec-B uses a Bloom filter instead of counters to remember the packets it has receieved from various broadcast senders. The false positive rate of a Bloom filter that has m bits of memory and uses k hash functions is

$$\left(1 - \left(1 - \frac{1}{m}\right)^{kn}\right)^{k}$$

The authors of the Minisec protocol describe an implementation where $m = 144$ and $k = 8$. According to the above equation, the false positive rate of the Bloom filter is lower than 1% if no more than 14 messages are received during one epoch.

(a) What could a misbehaving node do to generate higher false positive rates with the same amount of packets?

(b) How many packet would the misbehaving node need to send to have all nodes reject all further packets in the same epoch?

Any attempt to look at
the content of these pages
before the signal
will be severely punished.

Please be patient.