Student Seminar: Security Protocols and Applications
Final Exam Part 2/2

Philippe Oechslin and Serge Vaudenay

28.6.2011

- duration: 3h00
- no document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- answers to every exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- it is unlikely we will answer any technical question during the exam
- do not forget to put your full name on your copy!

Family Name: . . . .

Given Name: . . . .

Section: . . . .

I Onion routing and TOR

In classical onion routing and Tor a circuit is first set up before data is exchanged between a client and a server. Assume we are using a classical onion routing where a sender chooses 3 symmetric keys and then creates a set-up onion by successively (re)encrypting the keys and the next hop with the public key of an exit node, an intermediate node and an entry node. Now imagine that a heap overflow (or a CBC padding attack) is discovered that allows an attacker to take control of any onion router and to recover its private key.

Q.9 Describe all the operations that an attacker has to carry out to recover all the messages that a client has sent to a server through a classical onion routing network.

Q.10 Explain why such an attack is much more difficult in Tor and under what conditions it can still succeed.

Q.11 Tor routers can be contributed and operated by anybody, thus also malicious people. What kind of information can be gained by a malicious operator of a Tor entry node?

Q.12 What kind of information can be gained by a malicious operator of a Tor exit node?

Q.13 In Tor the directory servers plays a crucial role. Explain what protections are in place to protect against an attacker who would be able to control one directory server.

Q.14 Assume that an attacker controls 10% of the entry nodes, 10% of the intermediate nodes and 10% of the exit nodes of Tor. For your activities you need to use Tor 100 times and your Tor client constructs the circuits randomly every time. What is the probability that the attacker will find out at least once the source and destination of one of your connections?

Q.15 Considering that being traced once is as bad as being traced every time, some users prefer to chose a fixed entry node and use random intermediate and exit nodes. For the same 10% of corrupt entry, intermediate and exit nodes, what would be the probability that at least 1 of the 100 connections gets traced?

Q.16 In order to offer hidden services, Tor makes use of a directory of hidden services, of introduction points and of rendez-vous points. For each of these three elements, does the control of the element by an attacker reveal the location of the server, the location of the client and/or the data they exchange?

Q.17 When establishing a connection to a hidden service, what is the mechanism that proves to the client that she is talking to the real service and not to a fake one?