Exercise 5

Exercises Peer-to-Peer-Systems and Security (SS2010)

Monday 28.6 2010
Hand-in: Monday 12.7. 2010 in lecture or per mail
Exercise: to be announced

Dipl.-Inform. Heiko Niedermayer
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München

Rules: There will be five exercise sheets with each 10 points. You have to achieve 50 % of the points and present a solution in the exercise course to get the 0.3 bonus.

Task 1 (2 Points) Encryption

Some questions with respect to encryption.

a) Assume that Alice, Bob, and Cleta use SSL to communicate with each other. Alice sends a message via SSL to Bob and Bob forwards it via SSL to Cleta. Does the message look the same on both paths (Alice→Bob, Bob→ Cleta) for a global oberserver? Is this true for all properties of the message?

b) Assume that a static website is contacted with the encrypted HTTPS (HTTP über SSL) protocol. Even though the content is encrypted, what could an attacker use to find the content that was requested and sent?

Task 2 (4 Points) Threshold and Timed Mixes

Mixes use the randomization of the packet order to confuse observers so that they cannot trace incoming and outgoing packet. Ofcourse, such a system applies encryption in a way (e.g. onion encryption) so that the packets cannot be linked on the basis of their content.

A *threshold mix with treshold S* collects incoming messages and stores them in a buffer. Once S messages are in the mix, it fires. This means it sends out all the messages in its buffer in a random order.

a) Assume that each millisecond a message arrives with probability p=25%. How long does it take till the mix fires? Give a discrete probability distribution in the form p[i milliseconds] = x(i).

b) How large is the anonymity set?

Now to the *Timed Mix*. A timed mix waits for an interval T until it fires and sends out all messages from this intervall in random order.

c) When does a Timed Mix uncover a message accidentally?

Assume that Alice and Bob do a Voice-over-IP (VoIP) call with 128 kbps over a threshold mix. Other users of the mix download files, some chat, and others also do VoIP calls.

d) What can a passive oberserver do to confirm that Alice and Bob are the ones communicating via the mix?

e) Now you are less patient and are allowed to do active attacks (drop / delay messages) as well. You still observe the network. What can you now do to link Alice and Bob?

Task 3 (2 Points) Pool Mix

A P*ool Mix* is a mix with memory. This memory is called Pool and its size shall be P messages. Its buffer size is large enough for S+P messages. The Pool mix operates as follows. The mix waits until it stores S+P messages. At this moment it randomly sends out S of the S+P messages in a random order. The remaining P messages stay in the mix.

a) Is there an upper limit for the time a message waits in the mix?
b) How does this effect the anonymity set?
c) What could a strong attacker do to attack the Pool mix? This means that the attacker needs to identify the desired message of its victims when it enters and leaves the mix?

Task 4 (2 Points) Predecessor Attack

In a Peer-to-Peer network for anonymization messages are sent via other peers to their destination. Assume that the messages (or tunnels) from one and the same sender can be identified on the basis of the public key used to create a shared key (or establish the tunnel). In this task we are now interested in the changing paths that the sender used. For the sake of simplicity assume that each message is sent via a different path. Let the network be 8 nodes: Alice, Bob, attacker and 5 other nodes. Messages from Alice to Bob are sent via 2 intermediate relay nodes.Alice and Bob can also be relays.

a) Create 30 random paths (from random number generator in software, throw a dice, …) from Alice via random node 1 via random node 2 to Bob.
b) For all messages that go through the attacker, note the predecessor and successor the attacker has seen.
c) How often has the attacker seen each of the 8 nodes as predessor and successor? Is there anything suspicious?