Assignment Four

Protecting the proxy network

Set: *6th of June 2011*
Due: *17th of June 2011 @ 23:55 CEST*

Synopsis:
Implement authentication and transmission encryption for the distributed anonymizing proxy network.

Introduction

This is the last of the four assignments in the *Datanet* course. The four assignments are practical assignments, where you will gradually build a distributed anonymizing proxy where your implementation and that of your fellow students are all parts of the same distributed system.

This fourth assignment is about ensuring the validity of requests, and protecting the communication from tampering and peeking.

You must extend your proxy from the previous assignment to cryptographically validate the tracker response.

You must also create an asymmetric RSA keypair and report the public key when registering with the tracker.

The tracker will now return the public keys of all registered trackers as part of the response. You must now use this information to encrypt all messages passed between proxies.

Your implementation

To allow the proxies to transfer data around you must encapsulate encrypted data in a format that is a valid HTTP request.

Rather than merely forwarding a request to a another proxy, your implementation must now do the following:

- Create a random session key (AES-256)
- Encrypt the HTTP request with the session key
- Encrypt the session key with the destination proxy public key (RSA-1024)
- Create an envelope request with an encrypted payload

The format of the envelope request is as follows:

```
DATANET * HTTP/1.1
Host: *
Session-Key: <encrypted session key>
Content-Length: <size of encrypted payload>
```

```
<CR><LF><CR><LF>
... encrypted payload ...
```

This ensures that all http capable transport mechanisms will correctly be able to forward and (not) cache data, while still introducing encryption to the transmission.

To correctly handle an encrypted request, your proxy must do the following:

- Detect the DATANET HTTP method
- Read the payload and encrypted session key
- Decrypt the session key with the proxy private key
- Decrypt the payload with the session key
- Either forward the message to another proxy (wrapped in a new envelope)
- Or forward the request to the remote destination

When the proxy receives a response it must also respond with an encrypted payload, IF the request was encrypted. This ensures that there is always a known session key, but also that the initial request (from the browser) is unencrypted.

The encrypted response must be wrapped in a header with this format:

```
HTTP/1.1 700 Encrypted
Cache-Control: no-cache
Content-Length: <size of encrypted payload>
<CR><LF><CR><LF>
... encrypted payload ...
```

Your Experiment

You must also make an experiment that uses the encrypted proxy network.

You should use your timings from the previous assignment for comparison.

While using your proxy, which is a part of the distributed network, you must try to load the same pages as you did in assignment three.

The randomization will make the timings much less reliable, so you will have to run the test a few times to get an average.

You must also download a large file (appx. 100mb) and measure the bandwidth. Again, the random nature of the network means that you will have to run the test a few times and calculate the average.

Your Report

Your report *MUST* be written in ACM format. An ACM template for LaTeXand MS-Word is available for download via Absalon.

Your reports should contain:

- An abstract describing the contents of your report

- A description of the encryption extensions
- A description of the threat (what does the system protected against?)
- A description of how the extensions improve the system security
- A description of any flaws or problems with the security system (where can you attack it?)
- A description of the types of anonymity offered by the systems (what is (not) anonymized?)
- The responsiveness and bandwidth measures that you obtained from your experiment

Deliverables for This Assignment

You are encouraged to work in informal groups for this assignment, for the purpose of discussing implementation details and limitations. We strongly encouraged you to come to the exercise, where we will use time to discuss the design, implementation etc. The implementation and report that you hand in must however be **your own individual work**. You should submit the following items:

- A single PDF file, A4 size, no more than 3 pages, in ACM format, describing each item from report section above
- A single ZIP/tbz2 file with all code relevant to the implementation

Handing In Your Assignment

You will be handing this assignment in using Absalon. Try not to hand in your files at the very last minute, in case the rest of the Datanet students stage a DDoS attack on Absalon at the exact moment you are trying to submit. **Do not email us your assignments unless we expressly ask you to do so**.

Assessment

You will get written qualitative feedback, but no grade for the assignment. Your assignments will be evaluated together with your exam and produce a final grade for the course.