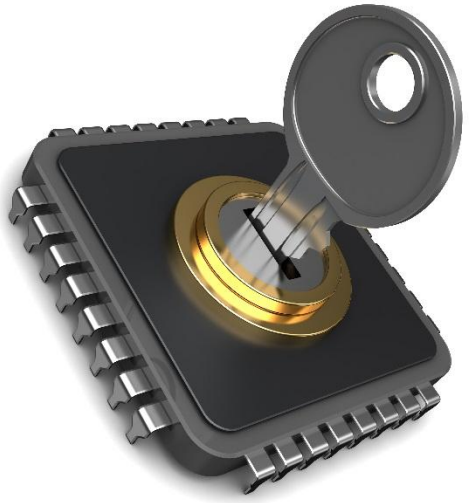
Introduction to Information Security

Tutorial Kerberos



Winter 2015/2016

Tutor David Bidner, www.iaik.tugraz.at

Kerberos - Motivation

Why?

- Sign in once, use different services
- Password is never transmitted to service
- Widely used and studied technology

How?

- Ticket proofs that the user is allowed to use a service
- This ticket is granted by a trusted third party

Kerberos - Assignment

3 Parts

- Client (the user)
- Server (trusted third party)
- Service

Different Tickets

- The Client needs a so called ticket granting ticket (TGT)
- With the TGT it can receive service granting tickets from the Server
- Keep in mind that Tickets should/could expire sometimes
- The Client shouldn’t be able to fake a ticket/timestamp

Kerberos - Assignment

Protocol

- http://web.mit.edu/kerberos/
- https://www.ietf.org/rfc/rfc4120.txt
- There’s no need to have a 100% RFC coverage, but try to keep it in mind!

Kerberos - Spec part

Send a short pdf including

- What libraries/language will you use
- Short description of the server, client, service
- Planned development steps

Kerberos - Main Assignment

In the main assignment:

- Implement your ideas
- In the end hand in a description of the source / the source itself
- Code should run on GNU/Linux or M$/Windows(!)

Kerberos - Programming

- You can choose the language (Java, Python, etc.)
- Use libraries for as many parts as possible (sockets, crypto, etc.)
- Keep security in mind! (Less code == Less bugs)

Kerberos - Grading

The Grade will depend on

- How good your POC is
- How understandable are the writeups
- How much work was done by _you_

Kerberos - Questions

If you have any questions,

- ask them now.
- ask them in the newsgroup (general questions)
- send an email (questions for possible solutions etc.)