

Motivation

Recently, researchers from Ruhr University Bochum have demonstrated the insecurity of the XML encryption standard. They were able to decrypt data by sending modified ciphertexts to the server by gathering information from the received error messages. The attack was tested against a popular open source implementation of XML Encryption, and against the implementations of companies that responded to the responsible disclosure. In all cases the result was the same: the attack worked.

In this project, this attack on the XML encryption standard should be implemented.

Goals and Tasks

- ▶ Understand XML encryption
- ▶ Investigate the necessary background of the attack
- ▶ Implement the attack



Figure 1: <http://ericcarpiosp11tca-3.blogspot.com/2011/04/16encryption.html>

Literature

- ▶ T. Jager and J. Somorovsky.
How to Break XML Encryption.
In *CCS, 2011*.
To appear.

Deliverables

- ▶ Project files (.zip, cleaned)
- ▶ Documentation (inline)
- ▶ Readme (getting started)
- ▶ Presentation (10 .ppt slides)

Project Schedule

- ▶ Start Immediately
- ▶ Month 1 Reading literature
- ▶ Month 2 Implementing
- ▶ Month 3 Final deliverables

Studies

- INF
- SW
- TEL
- TM

Prerequisites

- ▶ C programming

Advisor / Contact

martin.schlaeffer@iaik.tugraz.at