

The problem with EduRoam

GNOMIS 2005 Oslo

Leif Johansson
Stockholm university

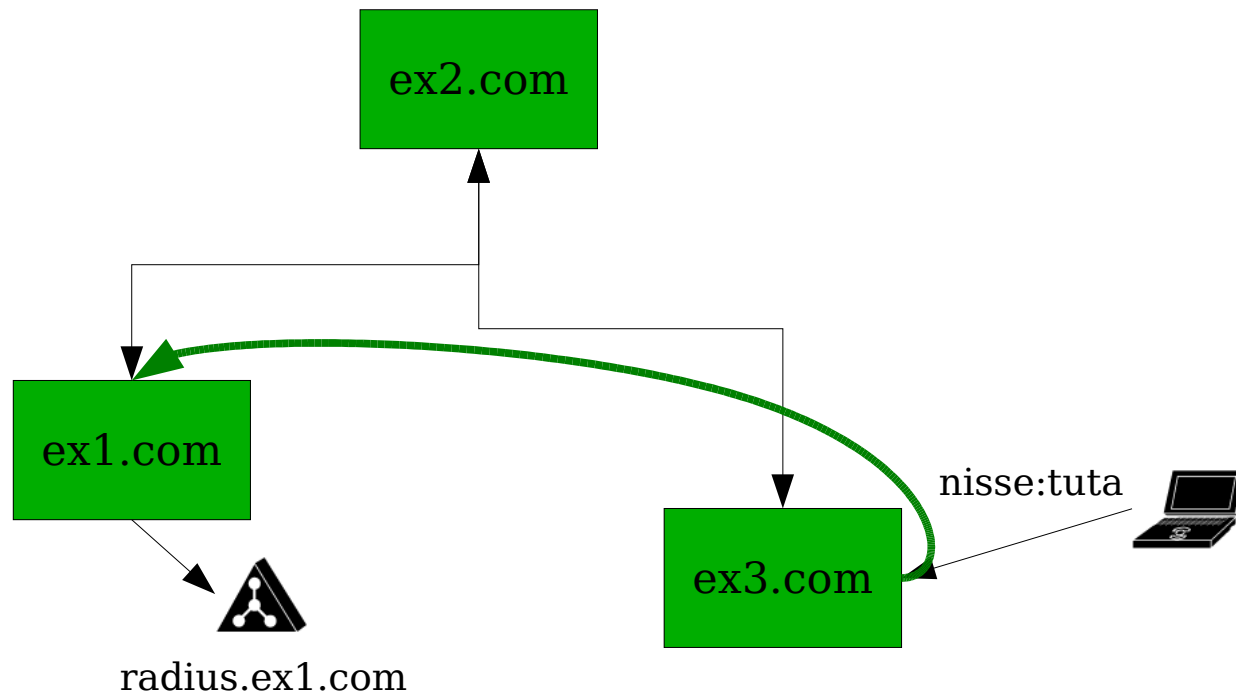
Almost e2e security...

- EAP-TLS end-to-end over a hierarchy of RADIUS servers
- Password sent over an e2e tls channel
- Client X.509 certificates for extra security
 - It all sounds good!
 - but...

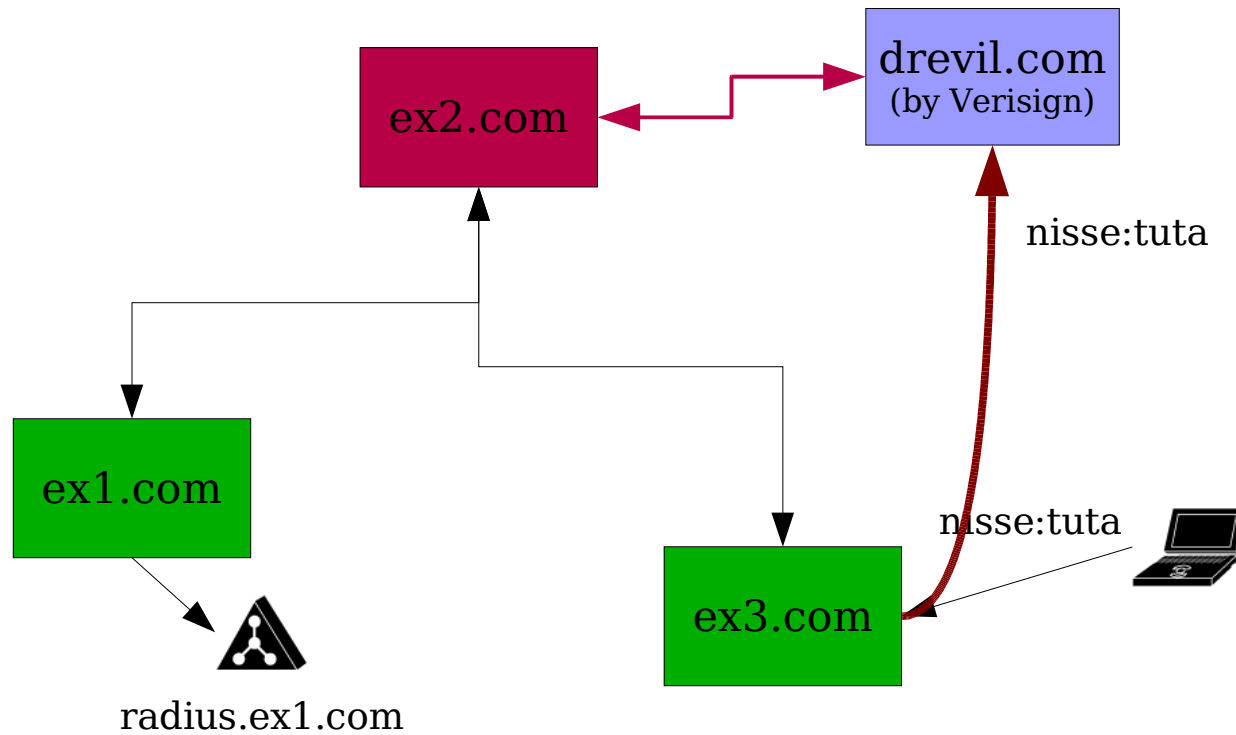
The problem

Current IEEE 802.1x clients do not place restrictions on peer certificates.

Now you see it...



Now you dont!



Summary

By attacking a node in the hierarchy and by using a valid certificate from a well know CA an attacker can emlulate a valid subtree of the hierarchy by always returning "OK". At the same time all passwords are collected.

The solution

Modify all 802.1x clients to allow policy to be placed on which X.509 certificates are allowed to authenticate and protect channels over which authentication information is sent.

Local policy (on the roaming laptop) must govern where passwords are sent.