



A Context Authentication Proxy for IPSec using Spatial Reference

6. December 2006 13:00, Yogyakarta
TwUC 2006, Session B

Rene Mayrhofer
Computing Department
Lancaster University, UK
rene@comp.lancs.ac.uk

Motivation: Why authenticate?

Introduction

- Security is currently one of the largest problems in computer science (not the only one though...)
- **Securing** a network connection only makes sense **after authentication**

Approach

Identification vs. Authentication

- Typical systems: first identify subject (username), then authenticate identity (password)
- But: Authentication does not require unique identification
⇒ **anonymous or pseudonymous communication**
- For ubiquitous computing most of the time unimportant how the service is called, only want to use it!

Spatial Authentication

Authentication Proxy

Demonstration Application

User vs. device authentication

- Can authenticate different subject, e.g. users or devices
- For ubiquitous computing devices often handle our interactions
⇒ **device authentication**

Summary

User vs. device authentication

Introduction

- User authentication works well for the “1:1” (one user, one device) and “n:1” (many users, one device) cases, i.e. for typical server- and desktop-computing

Approach

- But: scales poorly for the “1:n” (one user, many devices) approach that ubiquitous computing is proclaiming

Spatial Authentication

- Intuitive alternative to direct user authentication: a **trusted personal device** that authenticates its user once (e.g. when being switched on) and is assumed to be owned and used by a **single user**:

Authentication Proxy

- cf. conventional key chain
- PDA
- mobile phone



Demonstration Application

Advantage: **unobtrusive**, **scales** well to many devices

Challenges: this device must be **secure**

Summary

- Authentication is thus shifted from user-to-device to **device-to-device**

How not to touch the data devices?

Introduction

Frank Stajano: simple solution of direct electrical contact

Approach



Spatial Authentication

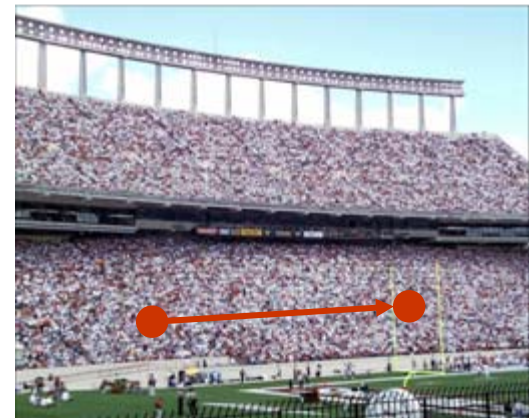
Authentication Proxy

but: ...

- direct electrical contact is fragile and wears out
- is often infeasible because of distances

Demonstration Application

Summary



Context Authentication

Introduction

- Authentication is harder in ubiquitous computing because there is no conventional UI

Approach

- But: ubiquitous computing builds upon the notion of **context**
- ⇒ exploiting this context for authentication allows to build more intuitive methods of authenticating

Spatial Authentication

Users and devices

Authentication Proxy

- **what I know** (password)
- **what I have** (token, smart card)
- **what I am** (finger print, iris)
- **where I am**
- **what I am doing**
- **who is with me**
- **what I ate** (hopefully not...)
- **how I feel** (hopefully not...)
- ...

Demonstration Application

Summary

Approach to authenticating with remote devices

Introduction

Still a problem: **distant devices** that do not share any aspect of the user's context

Approach

- what if a device can not sensibly be equipped with sensors?
- what if it would be simply inconvenient to share context with the device?

Spatial Authentication



Authentication Proxy

- example: WLAN access points built into the infrastructure

Demonstration Application

⇒ Proposed solution **authentication proxy**:

Summary

- associated with the real target by some pre-shared knowledge
- authenticate with this one instead
- Difference to e.g. laptop: is often shared temporarily, an authentication proxy should never be shared

Measuring Spatial References

Introduction

Spatial references: verifiable by the user **and** the device: both can come to the same conclusions as to which device they are interacting with

Approach

Relate is a system for relative positioning

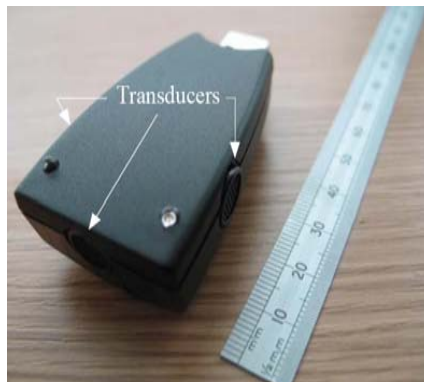
**Spatial
Authentication**

- based on ultra sound
- currently 2D, 3D is being worked on
- accuracy: <10cm, <30°
- no infrastructure support required, but peer-to-peer
- currently implemented in the form of USB dongles (based on Smart-Its) and Java host software

Authentication
Proxy

Demonstration
Application

Summary



Interaction by Spatial References

Introduction

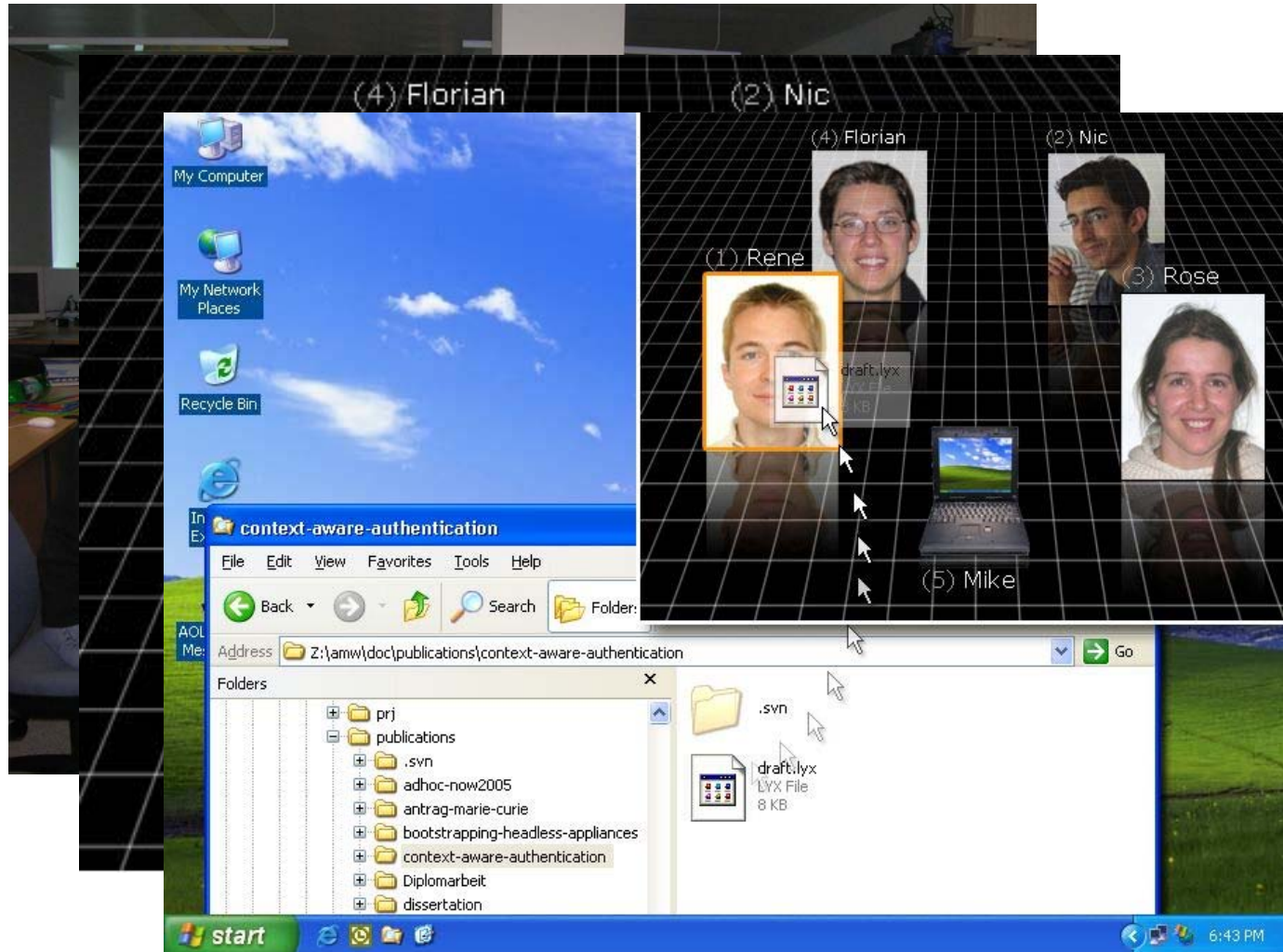
Approach

Spatial Authentication

Authentication Proxy

Demonstration Application

Summary



Authentication by Spatial Reference: Overview

Introduction

- non-Related RF channel (e.g. WLAN, BT) used for unauthenticated key-agreement protocol (e.g. DH)

Approach

- each host finds a random number used only for this authentication (**nonce**)
- nonces are transmitted both over the RF and the ultra sound channels over multiple rounds:

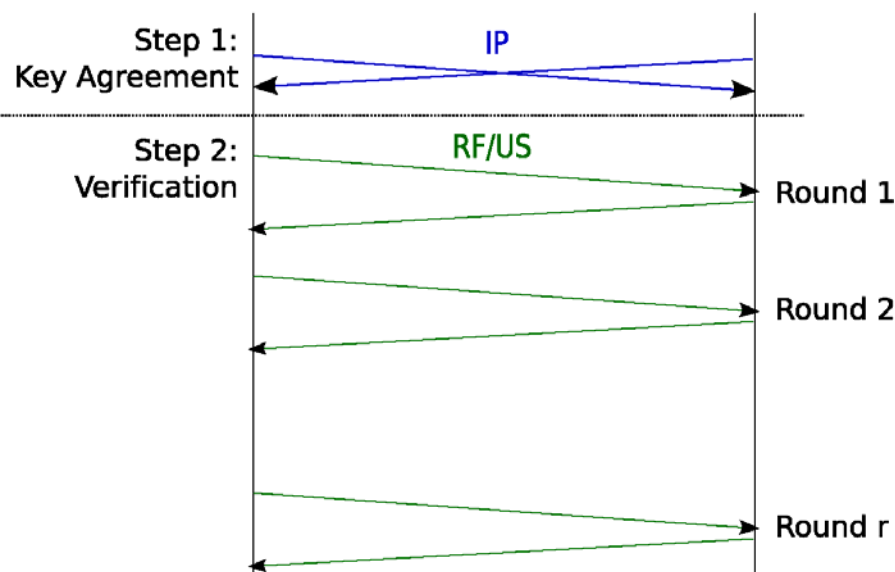
Spatial
Authentication

- encrypted with the session key of step 1 over RF
- as plaintext over ultra sound

Authentication
Proxy

- both hosts compare the received RF packets with the data received within the ultra sound channel. authentication successful when equal

Alice Bob



Demonstration
Application

Summary

Authentication by Spatial Reference: MITM

Introduction

How can an attacker be prevented from:

Approach

- Performing an active MITM attack on the RF level (possible by assumption)
⇒ shared key with Alice and shared key with Bob
- Decrypting the packets sent by Alice on th RF level
- Re-encrypting them for and forwarding them to Bob (and vice versa)
- Note: this attack could be performed purely on the RF level (no eavesdropping or active attacks necessary on ultra sound channels)

Spatial
Authentication

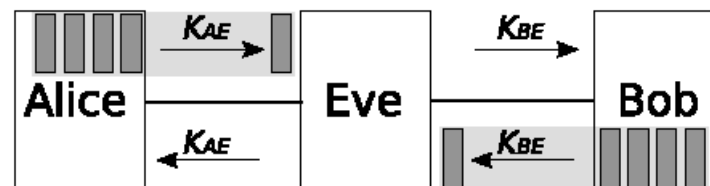
Authentication
Proxy

Solution: interlock protocol

Demonstration
Application

- RF packets are block-encrypted and split over multiple rounds
- Packet $i+1$ is only sent after the receipt of packet i from the other host
- MITM can not decrypt packets before all rounds have been completed
- MITM can not store packets and wait until all have been sent before forwarding *something* to the other host
- Hosts effectively commit themselves to what they will be sending later

Summary



Authentication by Spatial Reference: Protocol

Introduction

- Ultra sound transducers send only single, un-encoded pulses
- Method to transmit information: **delay pulses** at sender and compute transmitted value at receiver by subtracting a reference measurement

Approach

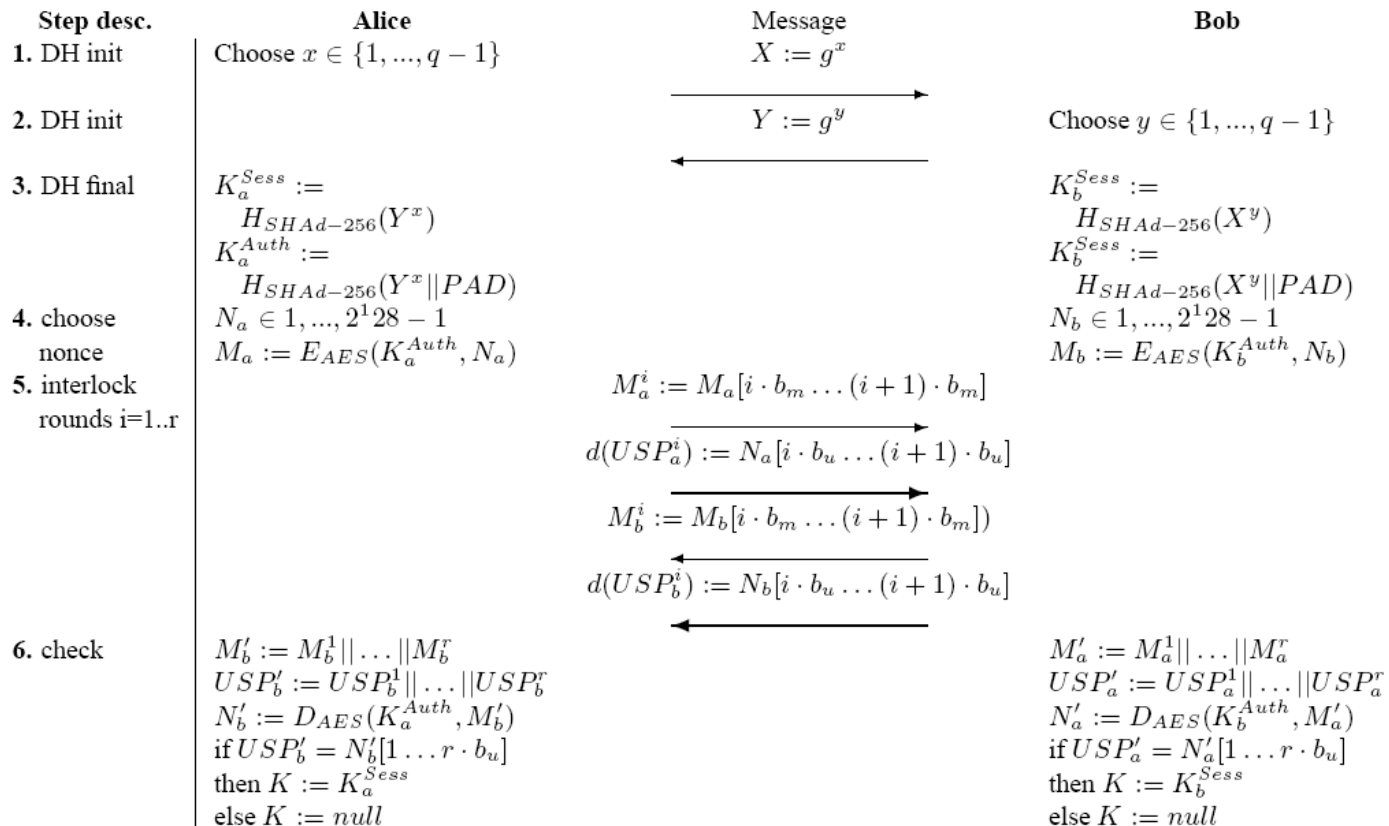
- Transmitted value **depends implicitly on reference measurement** (which has been used to select the device in the first place, i.e. for identification)

Spatial
Authentication

Authentication
Proxy

Demonstration
Application

Summary



Threat scenarios and protocol security

Introduction

Threat scenarios

- **Passive Eavesdropping on RF and ultra sound:** if a key-agreement protocol is used, should not reveal anything (no plaintext is transmitted other than nonce)
- **Active MITM on RF level:** could agree to a key K_a with A and a (different) key K_b to B and relay messages (but could not decrypt and re-encrypt parts of messages)
- **Active MITM on ultra sound level:** if combined with RF MITM, then attack will be successful – it would probably need two devices near hosts A and B that collaborated with each other
- **DoS on RF or ultra sound:** can currently not be dealt with, next hardware generation will allow better resistance against DoS
- **Attacks on the two devices themselves:** out of the scope of this research

Approach

Spatial
Authentication

Authentication
Proxy

Protocol security

Demonstration
Application

- **Based on the following assumptions:**
 - it is very difficult for an attacker to fake the direction of ultrasonic pulses
⇒ all hosts should check that the receiving characteristic does not change during the authentication phase, the user should check that there is nothing between the devices and nothing close to them
 - the device we authenticate with is itself secure....
 - DH is secure, chosen symmetric block cipher is secure
 - random number generation on A and B is secure, i.e. it is **very** unlikely that $K_a = K_b$
- **Security comes from:**
 - the encrypted N_a/N_b can only be decrypted after **all** parts have been received, and then the peer has already committed itself to all the delays

Summary

Variants of Authentication Proxies

Introduction

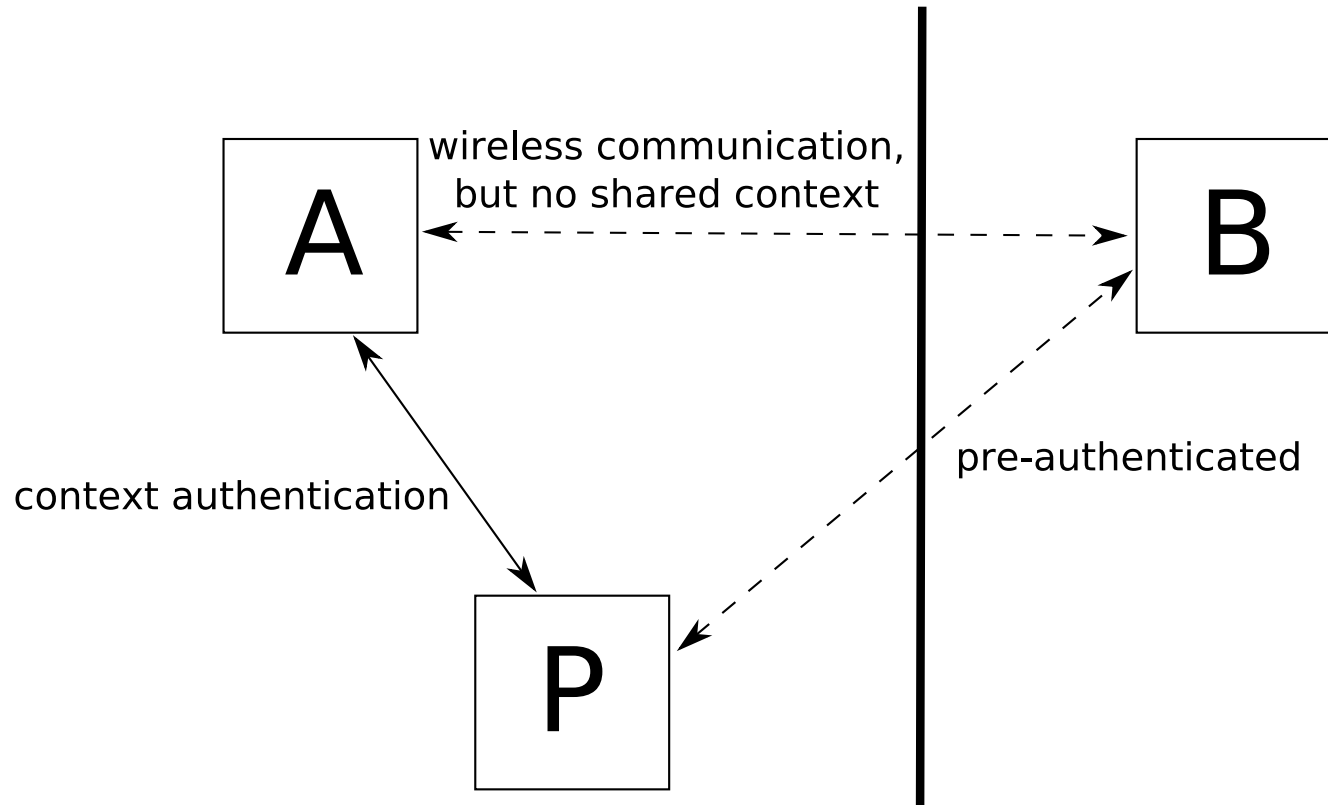
Approach

Spatial
Authentication

Authentication
Proxy

Demonstration
Application

Summary



Possibilities for authentication proxies:

- **Trust relationships:** e.g. passwords/shared secrets, OpenPGP, **X.509 cert.**
- **Interaction in context:** passive vs. **active**
- **Contact with service:** online vs. offline

Online vs. Offline Relationship

Introduction

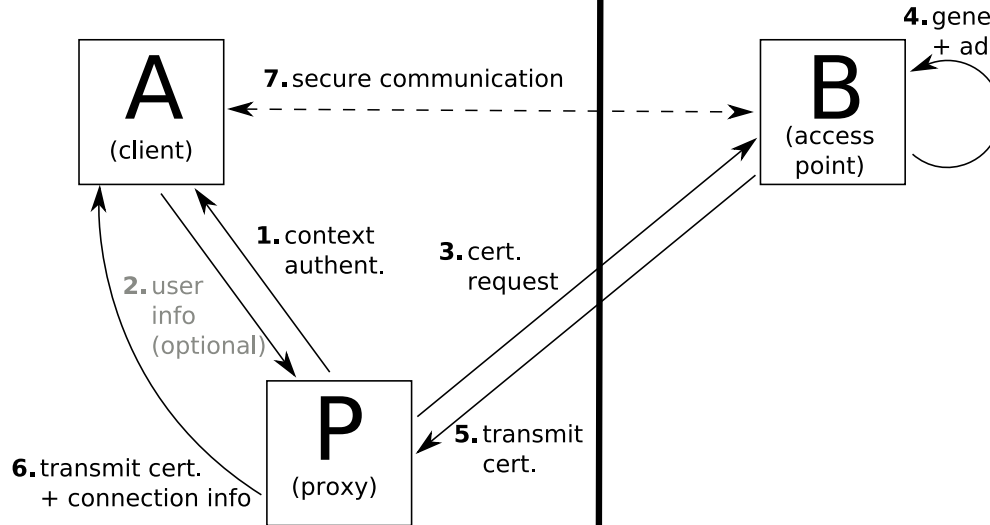
Approach

Spatial Authentication

Authentication Proxy

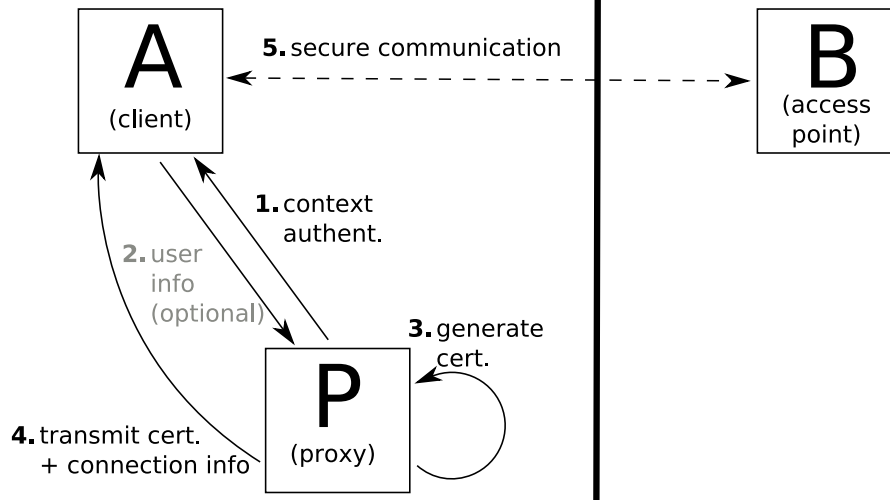
Demonstration Application

Summary



Online

⇒ less trust in proxy required (authenticate, but not authorize)



Offline

⇒ can be used even when no contact to service is available

Demonstration Application: IPsecME

Introduction

Approach

Spatial
Authentication

Authentication
Proxy

Demonstration
Application

Summary



5. secure communication

1. context
authent.

2. user
info
(optional)

4. transmit cert.
+ connection info



IPSecME: Implementation details

Introduction

Trust relationship between proxy and service: via X.509 certificates

Approach

- Accepted standard, flexible
- Allows to implement both online and offline proxy/service interactions
- Current implementation: Proxy acts as certification authority (CA), and service trusts certificates signed by it ⇒ **Active proxy** can be used anywhere, anytime

Spatial Authentication

Secure channel between client and service: IPSec

Authentication Proxy

- Secure
- Accepted standard, flexible
- Available in most current client operating systems

Demonstration Application

Platform:

- **Java Webstart** package for clients and in **J2ME** for proxies
- Any off-the-shelf access point and IPSec gateway will do (only need to support X.509)
- Demonstrator:
 - Asus WL-500G access point with OpenWRT
 - PocketPC PDA as proxy
 - Windows, Linux, or MacOS/X as client

Summary

IPSecME: User and Administrator View

Introduction

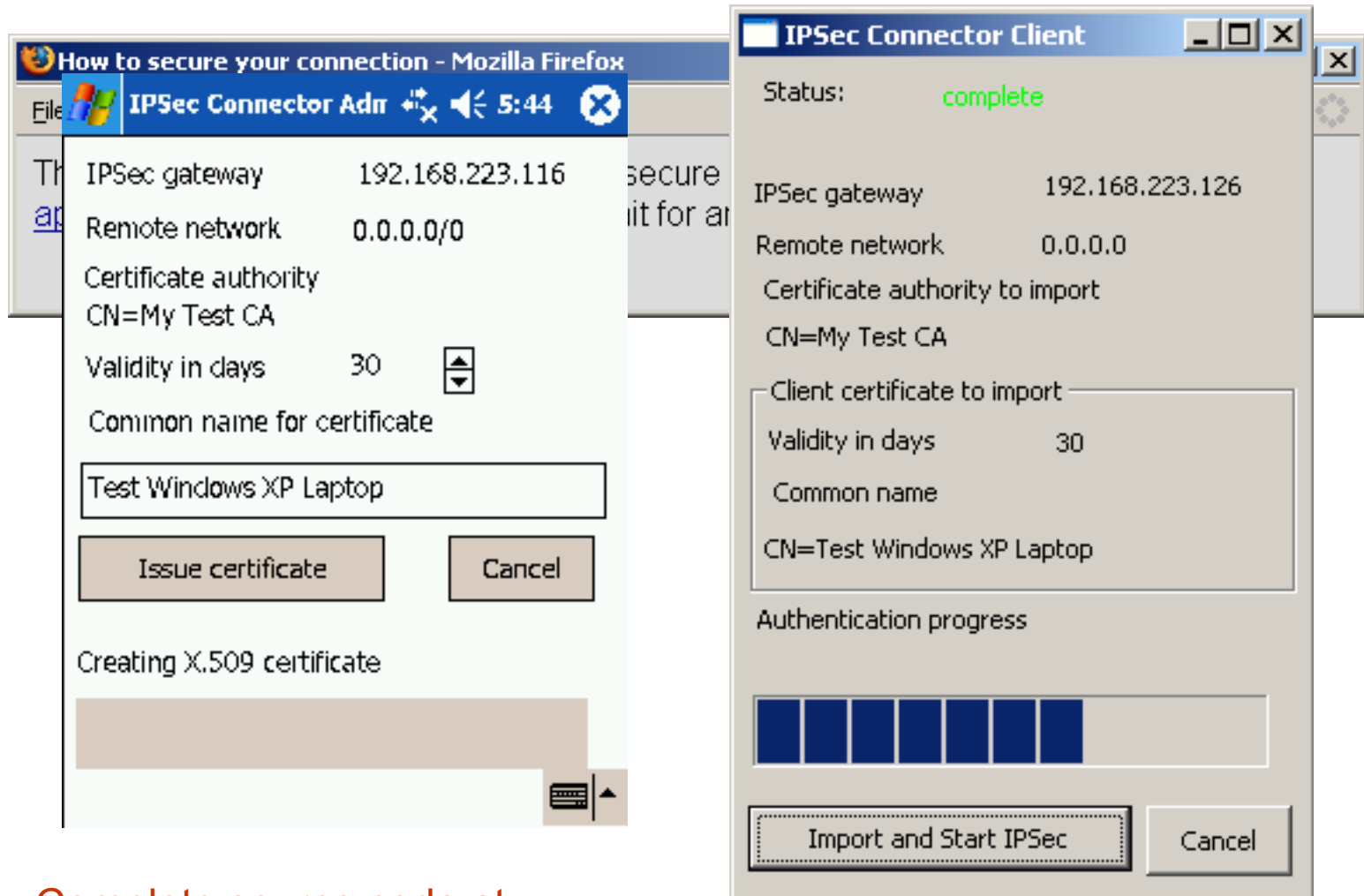
Approach

Spatial
Authentication

Authentication
Proxy

Demonstration
Application

Summary



Complete source code at

<http://www.openuat.org/spatial-ipsec-proxy>

Summary

Introduction

- Security in ubiquitous computing is still largely unexplored.

Approach

- Authentication is necessary to create secure connections.

Spatial Authentication

- We proposed an intuitive and unobtrusive method to authenticate devices: by **spatial reference**.

Authentication Proxy

- Verifying shared context with sensors may not be possible with distant devices.

Demonstration Application

- Proposed solution: **Context authentication proxies** can act as intermediaries.

Summary

- There are different possibilities with regards to trust relationships, active/passive, and online/offline scenarios.
- Our demonstration application uses this method to make the **setup of IPSec** channels easier and suitable for spontaneous interaction.



The problem with passwords is that they're too easy to lose control of.”

Bruce Schneier, March 2005

“We must plan for freedom, and not only for security, if for no other reason than only freedom can make security more secure.”

Karl Popper



Thank you for your attention!

Slides: <http://www.mayrhofer.eu.org/presentations>

Later questions: rene@mayrhofer.eu.org

OpenPGP key: 0xC3C24BDE

7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE