Seminar Smart Environments

Benutzerorientierte Sicherheitsaspekte

René Gallati
8. Juni 2004
Betreuer: Harald Vogt

[CT903]

Inhalt

- Einführung
- Anforderungen und Probleme
- Angriffsvarianten
- Ortsbasierte Authentifizierung
- Drag and Drop Interaktion
- Fazit
- Fragen

Einführung

- Viele Mobile Geräte
- Spontane Netzwerke
- Evtl. keine Basisinfrastruktur
- “Feindliche” Infrastruktur
- Unvollständige/Verteilte Trust-Ketten

[Chivers03]

Einführung

- Viele Mobile Geräte
- Spontane Netzwerke
- Evtl. keine Basisinfrastruktur
- “Feindliche” Infrastruktur
- Unvollständige/Verteilte Trust-Ketten

Wollen aber:

- Jederzeit Datenzugriff
- Dienste nutzen
- Sicherheit von Daten wahren

[Chivers03]

Einführung

MITM Angriff (heute)

Einführung

MITM Angriff (heute)

- Client baut Verbindung auf, MitM fängt Daten auf

Einführung

MITM Angriff (heute)

- Client baut Verbindung auf, MitM fängt Daten auf
- MitM sendet seine Anfrage an den Server

Einführung

MITM Angriff (heute)

- Client baut Verbindung auf, MitM fängt Daten auf
- MitM sendet seine Anfrage an den Server
- Server fragt Challenge

Einführung

MITM Angriff (heute)

- Client baut Verbindung auf, MitM fängt Daten auf
- MitM sendet seine Anfrage an den Server
- Server fragt Challenge
- MitM leitet Challenge an Client weiter

Einführung

MITM Angriff (heute)

- Client baut Verbindung auf, MitM fängt Daten auf
- MitM sendet seine Anfrage an den Server
- Server fragt Challenge
- MitM leitet Challenge an Client weiter
- Client gibt Lösung preis

Einführung

MITM Angriff (heute)

- Client baut Verbindung auf, MitM fängt Daten auf
- MitM sendet seine Anfrage an den Server
- Server fragt Challenge
- MitM leitet Challenge an Client weiter
- Client gibt Lösung preis
- MitM leitet Lösung weiter

Einführung

MITM Angriff (heute)

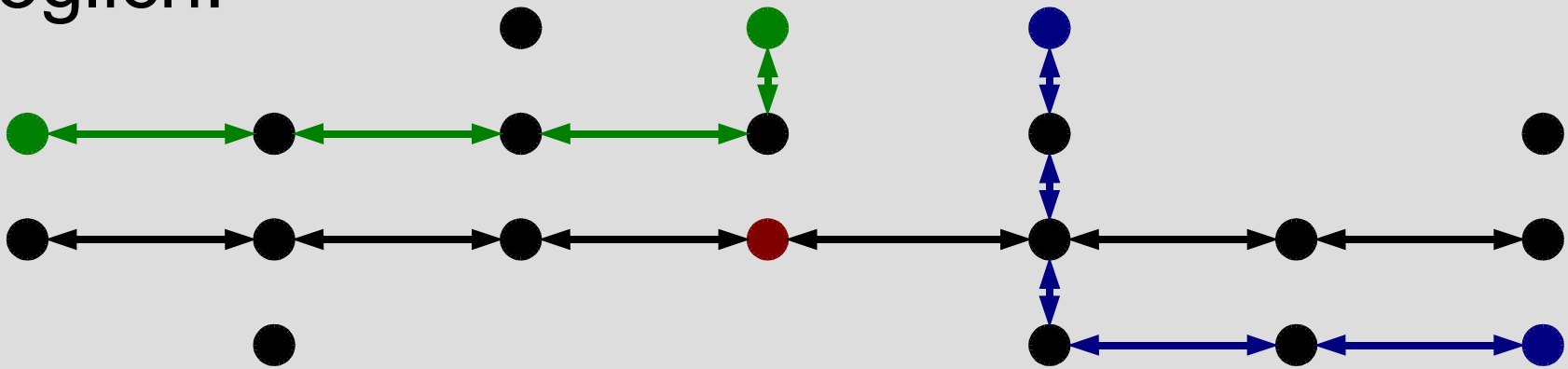
- Client baut Verbindung auf, MitM fängt Daten auf
- MitM sendet seine Anfrage an den Server
- Server fragt Challenge
- MitM leitet Challenge an Client weiter
- Client gibt Lösung preis
- MitM leitet Lösung weiter → vollständiger Zugriff

Einführung

Man in the Middle Attacks

- Gefährlich
- evtl. Schwer zu detektieren
- Erfolgreich auch bei SSL und SSH!

Aber nur entlang des Kommunikationspfades möglich!

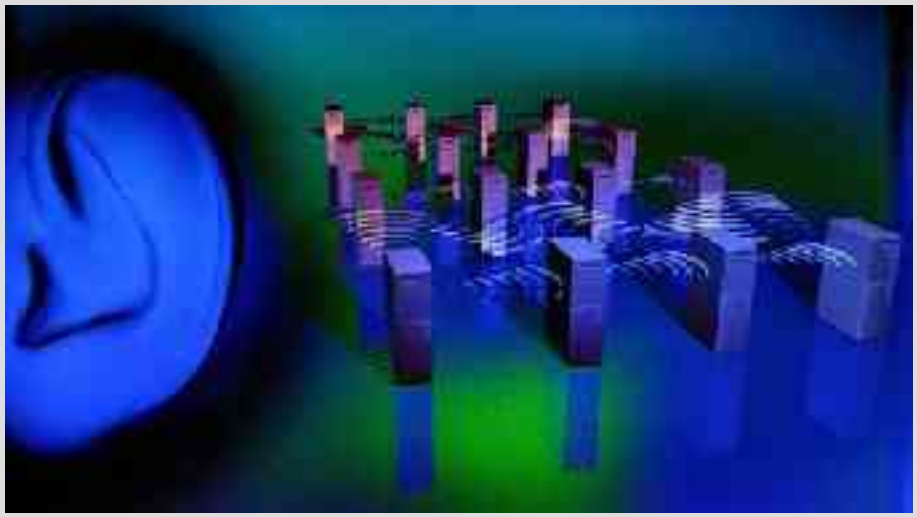


Einführung

Man in the Middle Attacks

In mobilen WLAN-basierten Netzen jedoch...

- Einfach
- Sicher (für Angreifer)
- Aus Distanz (mehrere km mit entsprechendem Equipment !)



[CT201]

Verhindern durch Secure Location Verification

Anforderungen und Probleme

- Einfach zu verwenden
- Sicher
- Intuitiv
- Nützlich
- Fälschungssicher
- Diebstahlsicher
- Replay-Attack sicher
- Sicher vor MitM

Geht das alles??

[Chivers03]

Anforderungen und Probleme

Heute im Einsatz

- PIN
- Benutzername / Passwort
- Badge
- SmartCard
- Pass/ID
- Schlüssel

Besitz oder Kentniss reicht

- Biometrie
  - Fingerabdruck
  - Retinalscan
  - DNA
- Wachmann

eigene Probleme...

Anforderungen und Probleme

Biometrie ausgetrickst...

[CT1102]

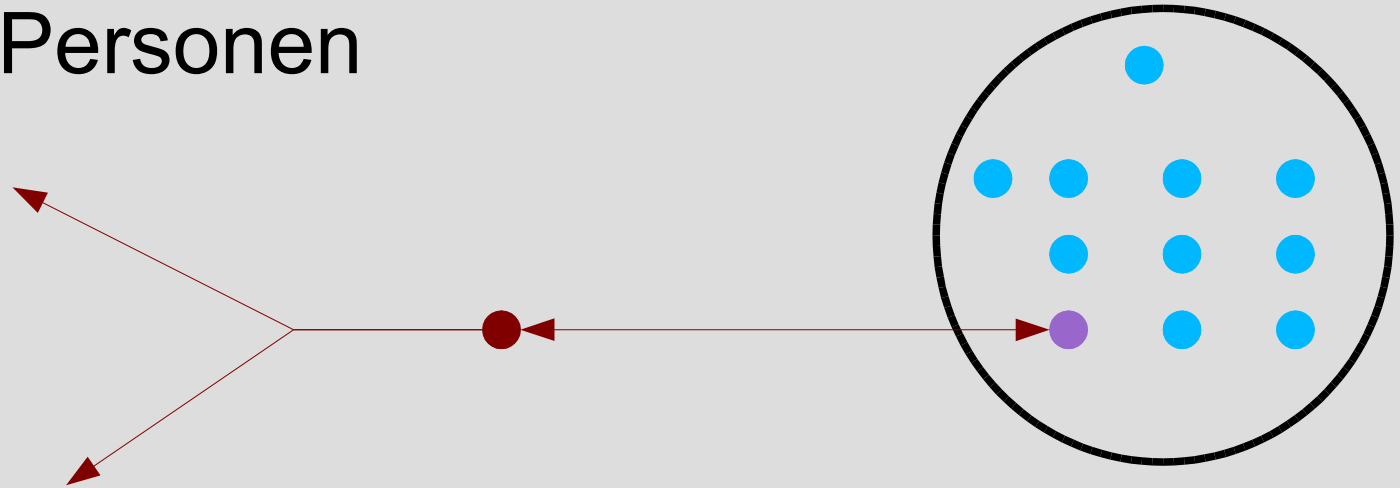
Angriffsvarianten

- Nicht technischer Art
  - Diebstahl
  - Bestechung / Erpressung
  - Klassischer Überfall
  - Social Engineering
- Technisch/ungezielt
  - Brute Force
  - Replay-Attack
  - Wurm / Virus
- Gezielt
  - Proxy/MitM
  - Trojaner
  - Hijacking
  - Exploits

Angriffsvarianten

Proxy-Attack

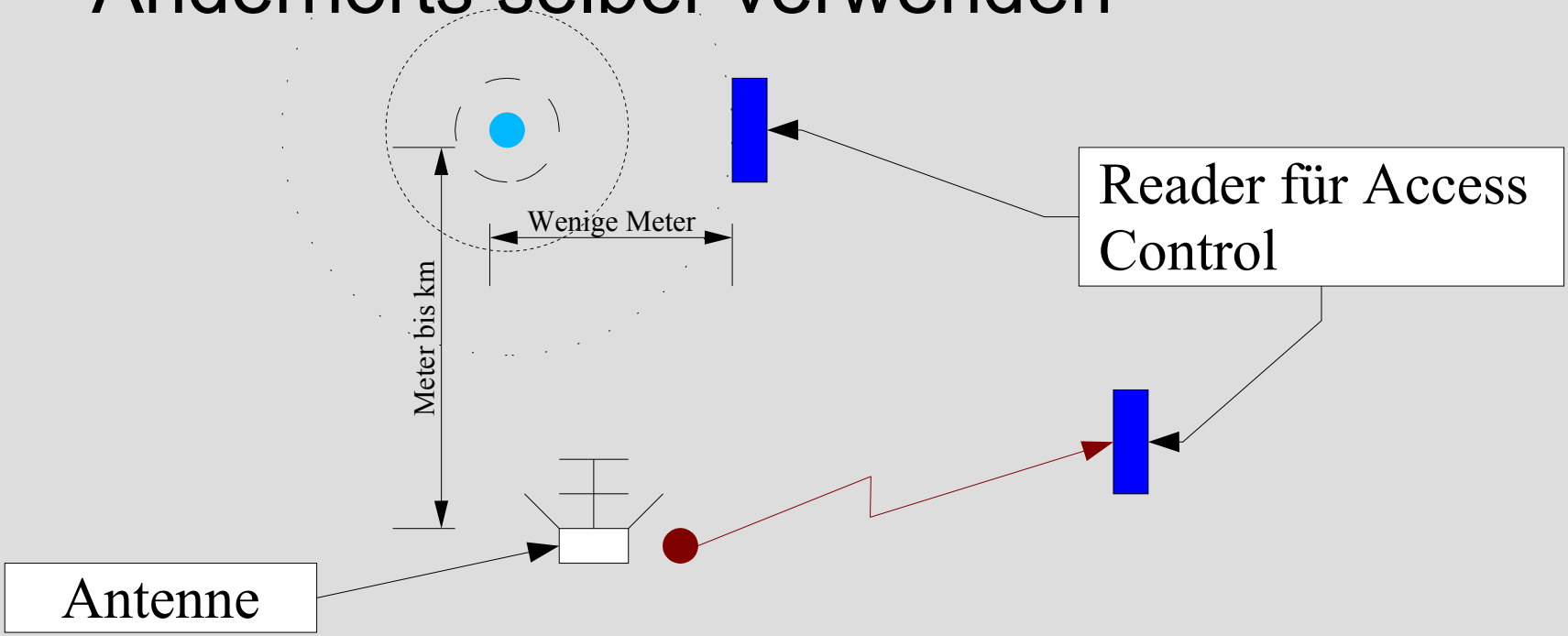
- Proxy mit Erlaubnis leitet Daten weiter
- “Insider”-Angriff
- Sehr schwer zu detektieren!
- Keine wirklich technische Lösung ohne massive Einschränkung beteiligter Devices/Personen



Angriffsvarianten

Replay-Attack

- Benutzer authentifiziert an Reader
- Signal abfangen
- Andernorts selber verwenden



Inhalt

- Einführung
- Anforderungen und Probleme
- Angriffsvarianten
- Ortsbasierte Authentifizierung
- Drag and Drop Interaktion
- Fazit
- Fragen

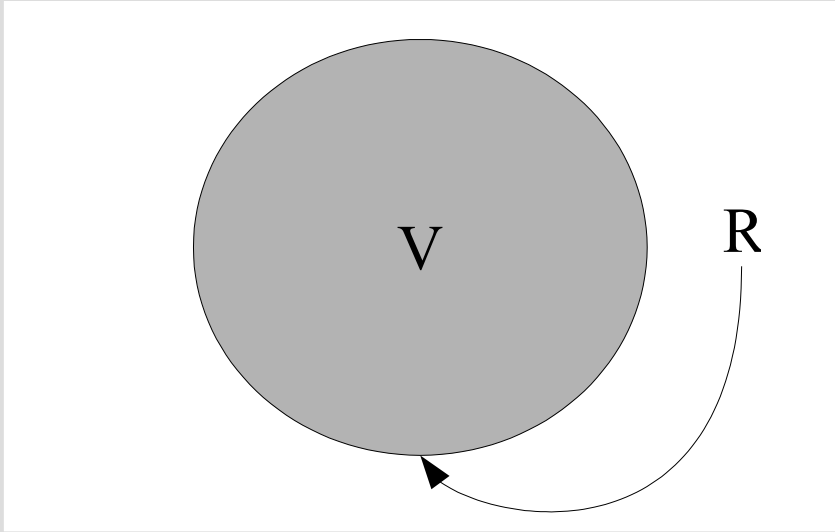
Ortsbasierte Authentifizierung

- Ortsinformation bei Authentifizierung miteinbeziehen
- Besitz von Token reicht, aber nur **“hier”**
- Aktionen nur an bestimmten Orten möglich
- Ermöglicht neue Dienste
- Einfache Administration da Binärwert (im Bereich / ausserhalb Bereich)
- Beispiele Echo-Protokoll, Distance-Bounding Protocol

Ortsbasierte Authentifizierung

Echo Protokoll

- Radio und Ultra-Schall
- Prüfling p, Verifier v der Region R überwacht



1. Prüfling teilt seine Position (Abstand l) mit
2. Verifier sendet *nonce* via Radio
3. Prüfling sendet *nonce* via Ultraschall retour
4. Verifier entscheidet über Annahme oder Abweisung

1. $p \xrightarrow{\text{radio}} v : \ell$
2. $v \xrightarrow{\text{radio}} p : N$
3. $p \xrightarrow{\text{sound}} v : N$

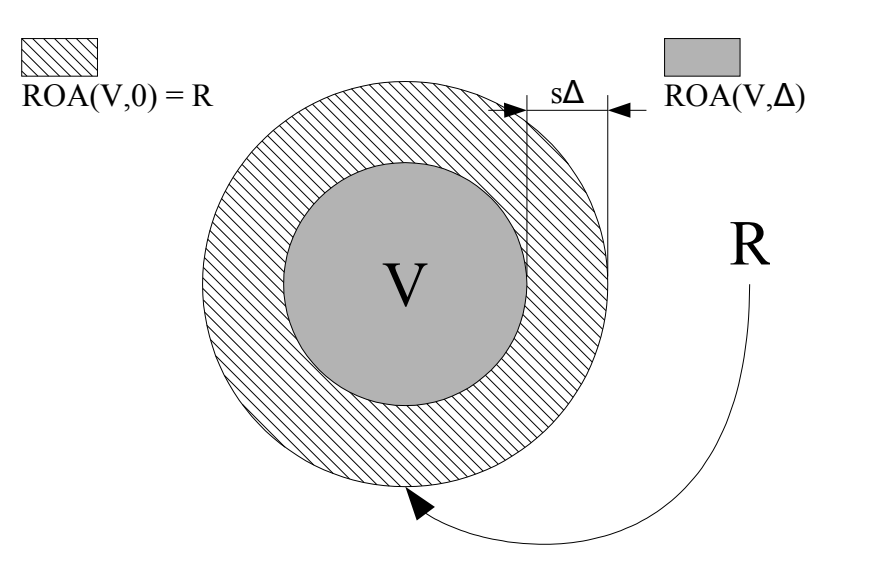
v accepts iff $\ell \in R$ and elapsed time $\leq d(v, \ell) \cdot (c^{-1} + s^{-1})$.

[Sastry03]

Ortsbasierte Authentifizierung

Echo Protokoll

- Entscheidung durch Zeitdifferenz zwischen senden der nonce und Empfang derselben
- Problem: Unbekannte Verzögerung im Prüfling
- Verifier lehnt ab falls Δ zu gross oder Prüfling ausserhalb Reichweite

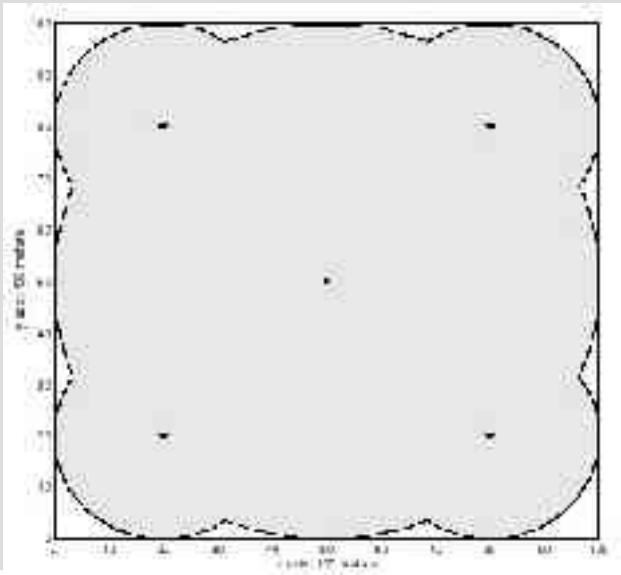


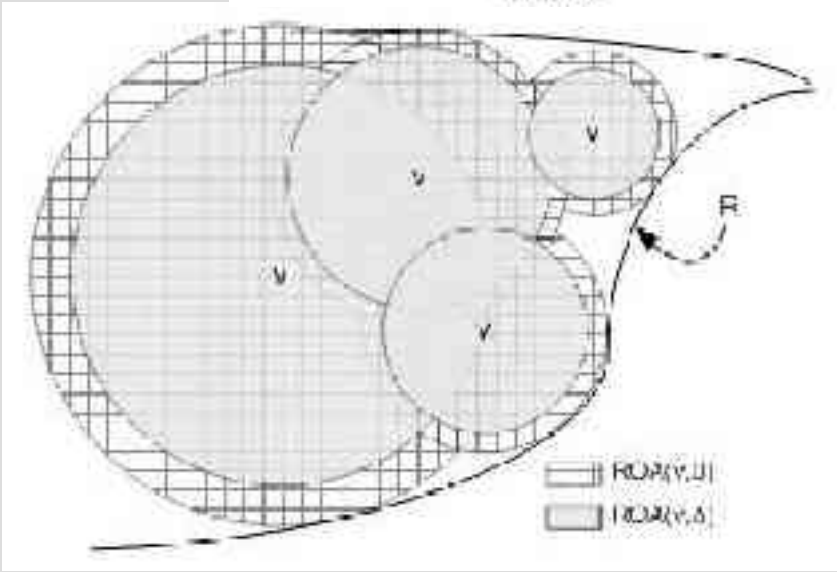
[Sastry03]

Ortsbasierte Authentifizierung

Echo Protokoll

- Mehrere Verifier für Raumabdeckung
- Erweiterbar
  - Authentifizierung
- Warum Radio/Ultraschall und nicht Radio/Radio oder Ultraschall/Radio?
  → Sicherheitsproblem

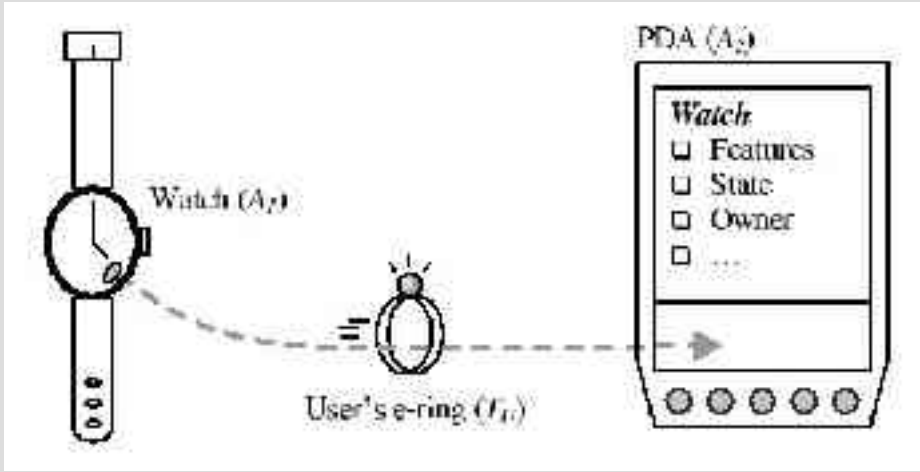




[Sastry03]

Drag and Drop Interaktion

- Tragbares Token
- Berührung löst Aktion aus
- Simple aber limitierte Anzeige
- Intuitive Interaktion
- Aktivierung als Diebstahlschutz
- Bekanntes Drag and Drop Paradigma



[Bussard03]

Drag and Drop Interaktion

Distance-Bounding Protokoll

Distance Bounding A » B:

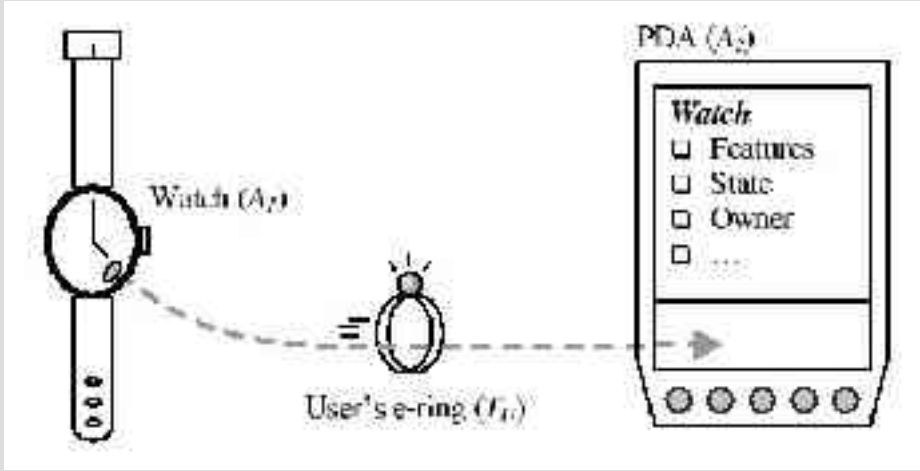
1) Initialization
   1.1) A Choose a N bit random number R_A
   1.2) B Choose a N bit random number R_B
2) Rounds (for i in {1...N})
   2.1) A Start measuring round trip time
   2.2) A → B $R_A[i]$
   2.3) B → A $R_B[i]$
   2.4) A Verify round trip time
3) Verification
   3.1) A ← B $SIGN_B(R_A,R_B)$

[Bussard03]

Drag and Drop Interaktion

Distance-Bounding Protokoll

1) **Drag**
   1.1) $T_U \rightarrow A_1$ <Get Description>
   1.2) $T_U \leftarrow A_1$ $CERT_{A1} = CERT_{CA}(K_{PA1}, \text{attributes})$
   1.3) T_U » A_1 Distance-Bounding Protokoll
2) **Drop** (before timeout)
   2.1) $T_U \rightarrow A_2$ <Put Description>:
   $CERT_{TU}(T_U \text{ touched } A_1, CERT_{A1})$
   2.2) A_2 Display description of A_1

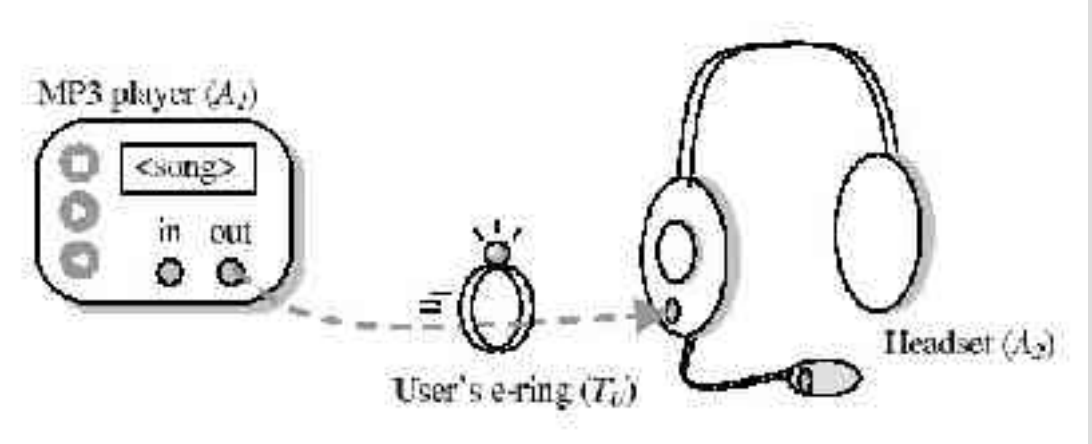


[Bussard03]

Drag and Drop Interaktion

+ Einfache und Intuitive Benutzung
+ Alltagstauglich
+ Zertifikatsspeicher (digitale Unterschriften)
+ Zusätzlich “Pointer” Möglichkeit

- Keine Komplexen Interaktionen
- Braucht Infrastruktur



[Bussard03]

Fazit

- Räumliche Nähe wichtig in UbiComp
- Umsetzung durch Zeitmessung
- Billige Geräte
- Relativ Simple Protokolle
- Einfach/Intuitiv in der Anwendung

Aber...

Fazit

- Räumliche Nähe wichtig in UbiComp
- Umsetzung durch Zeitmessung
- Billige Geräte
- Relativ Simple Protokolle
- Einfach/Intuitiv in der Anwendung

Aber...

- Benötigt entsprechende Infrastruktur
- Löst alleine nicht alle Probleme

Fazit

Sicherheit ist ein Prozess, kein Produkt!

Fragen

Referenzen

[CT903] c't Magazin für Computer Technik 09/2003 S. 114ff. "Rundumschutz für Windows"

[Chivers03] Howard Chivers, John A. Clark, and Susan Stepney. Smart Devices and Software Agents: The Basics of Good Behaviour. Security in Pervasive Computing 2003, LNCS 2802, pp. 39-52, 2004

[CT201] c't Magazin für Computer Technik 02/2001 S.28 "WEP Löcher geflickt"

[CT1102] c't Magazin für Computer Technik 11/2002 S.114ff. "Einbruch per Fingerabdruck"

[Sastry03] Naveen Sastry, Umesh Shankar, David Wagner. Secure Verification of Location Claims. ACM 1-58113-769-9/03/0009

[Bussard03] Laurent Bussard and Yves Roudier. Embedding Distance-Bounding Protocols within Intuitive Interactions. Security in Pervasive Computing 2003, LNCS 2802, pp. 143-156, 2004