universitätbonn

eduroam mit Android

Timo Bernard &
Karsten Honsack

universitätbonn

Warum wir hier sind

- Aktionstag der Ruhr-Universität Bochum
- Kontrolle der eduroam Konfiguration
- 2/3 von 350 Studierenden hatten unsichere Einstellungen

universitätbonn

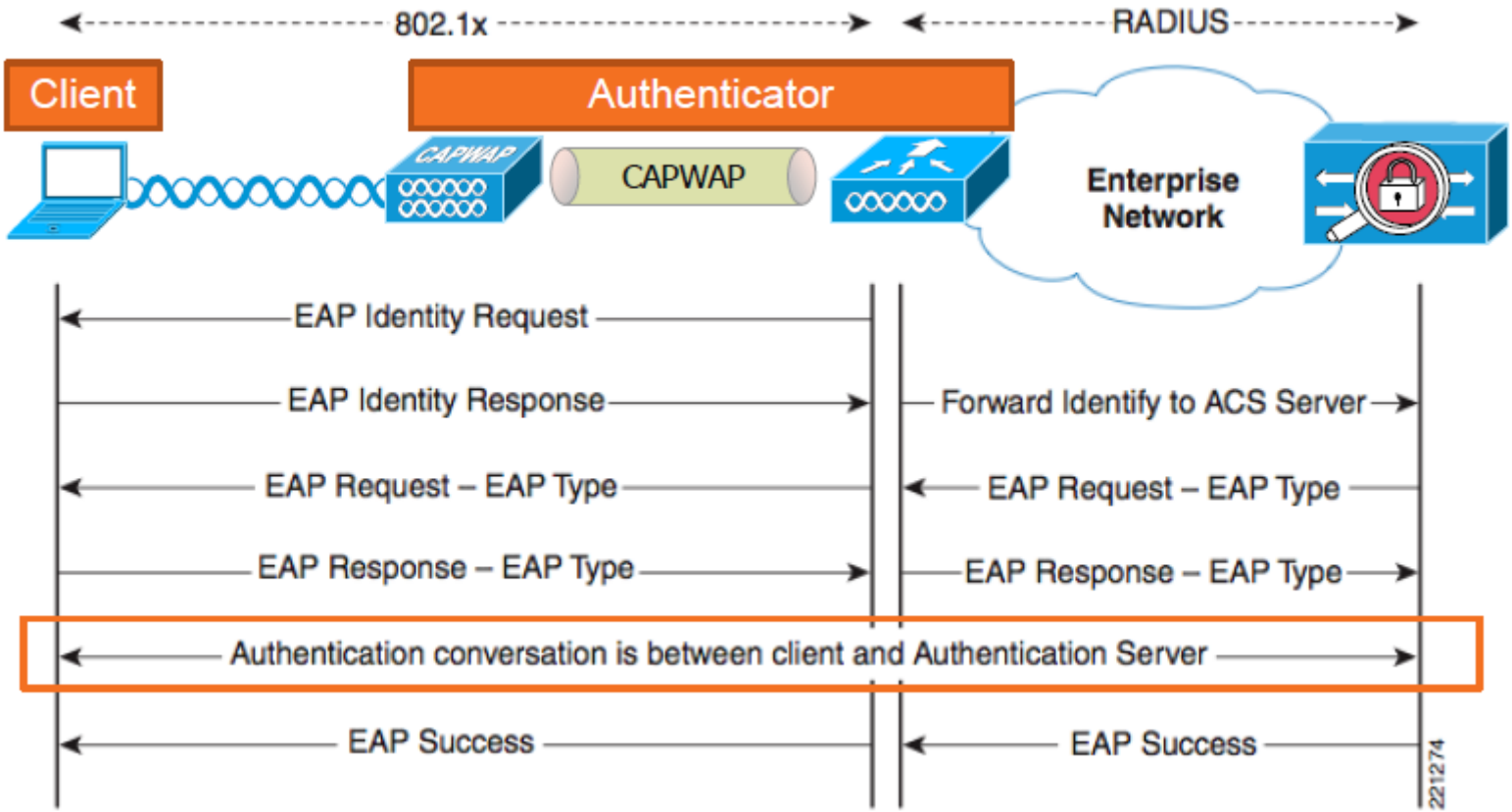
Es ist anzunehmen, dass die Zahl der unsicher konfigurierten Geräte auch in anderen Einrichtungen so hoch ist.

universitätbonn

Agenda

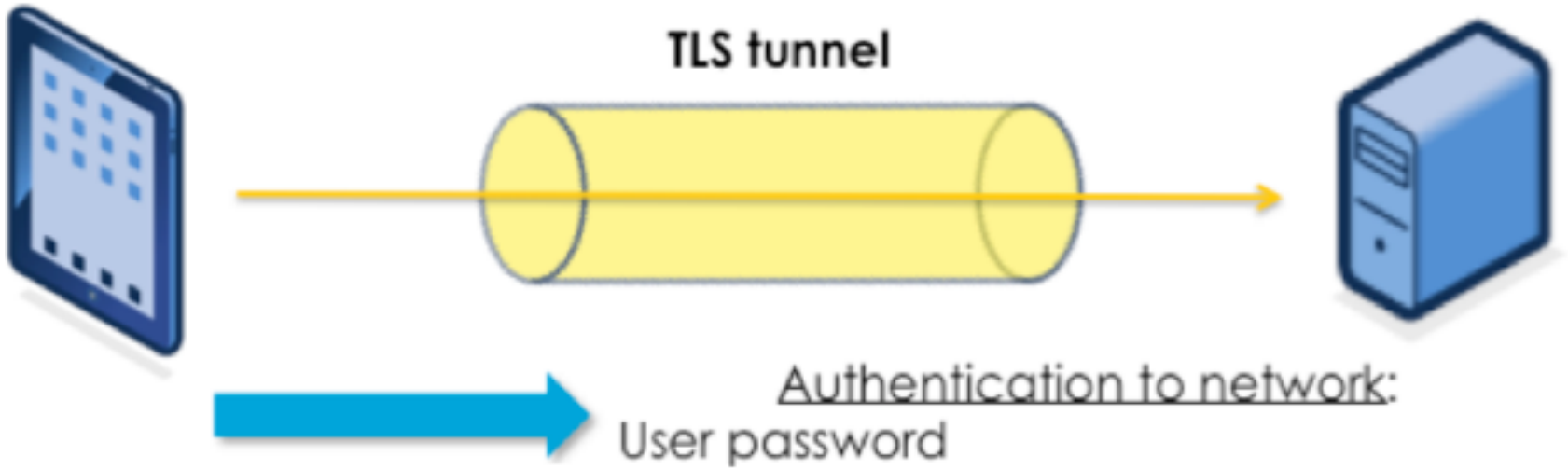
- Wie funktioniert EAP?
- Angriffsszenarien und Testergebnisse
- Zwischenfazit
- Was können wir unternehmen?

Wie funktioniert EAP?



universitätbonn

Wie funktioniert EAP?



universitätbonn

Der Rogue AP

- Raspberry Pi
- 10.000 mAh Akku
- WLAN-Stick
- hostapd
- freeradius

=> 14h Akkulaufzeit

universitätbonn

Der Rogue AP

universitätbonn

Testgeräte

Gerät	Betriebssystem	Version
Samsung Galaxy S Plus	Android	2.3.6
HTC Flyer	Android	3.2.1
Google Nexus 4	Android	4.4.4
iPhone 5	iOS	8.0.2
Nokia Lumia 925	Windows Phone	8.1

universitätbonn

Angriffsszenario 1

- Rogue AP mit freeradius Beispielzertifikat
- Client **ohne** Root CA 2 Zertifikat
- Direktverbindung
- Roaming

universitätbonn

Ergebnis

Gerät	Passwort im Klartext auslesbar
Samsung Galaxy S Plus	☑
HTC Flyer	☑
Google Nexus 4	☑

universitätbonn

freeradius-Log

[ttls] Got tunneled request

User-Name = “name@uni-bonn.de"

User-Password = “passwort"

FreeRADIUS-Proxied-To = 127.0.0.1

universitätbonn

Anmerkungen

- Galaxy S Plus & HTC Flyer versuchen kontinuierlich zu roamen
- Nexus 4 quittiert das WLAN Profil mit „Authentifizierungsproblem“
- **Keine** Zertifikatsbestätigung

universitätbonn

Angriffsszenario 2

- Rogue AP mit freeradius Beispielzertifikat
- Client **mit** Root CA 2 Zertifikat
- Direktverbindung
- Roaming

universitätbonn

Auswertung

Gerät	Passwort im Klartext
Samsung Galaxy S Plus	☐
HTC Flyer	☐
Google Nexus 4	☐

universitätbonn

freeradius-Log

[ttls] <<< TLS 1.0 Alert [length 0002], fatal unknown_ca

TLS Alert read:fatal:unknown CA

TLS_accept: failed in SSLv3 read client certificate A

rlm_eap: SSL error error: 14094418:SSL routines:SSL3_READ_BYTES:tlsv1 alert unknown ca

universitätbonn

Anmerkungen

- Galaxy S Plus markiert das WLAN-Profil als „Deaktiviert“
- Nexus 4 quittiert das WLAN Profil mit „Authentifizierungsproblem“
- HTC Flyer „blacklisted“ den Rogue AP
- **Keine** Zertifikatsbestätigung

universitätbonn

Angriffszenario 3

- Rogue AP mit gestohlenem Serverzertifikat
- Client **mit** Root CA 2 Zertifikat
- Direktverbindung
- Roaming

universitätbonn

Auswertung

Gerät	Passwort im Klartext
Samsung Galaxy S Plus	☑
HTC Flyer	☑
Google Nexus 4	☑

universitätbonn

freeradius-Log

[ttls] Got tunneled request

User-Name = “name@uni-bonn.de"

User-Password = “passwort"

FreeRADIUS-Proxied-To = 127.0.0.1

universitätbonn

Anmerkungen

- Galaxy S Plus & HTC Flyer versuchen kontinuierlich zu roamen
- Nexus 4 quittiert das WLAN Profil mit „Authentifizierungsproblem“
- iPhone hier ebenfalls angreifbar!

universitätbonn

Anmerkungen

- **Keine** Zertifikatsbestätigung
- Endgerät prüft **nicht** ob Serverzertifikat gesperrt wurde
- Endgerät prüft **nicht** ob Serverzertifikat abgelaufen ist

universitätbonn

Anmerkungen

- Prüfung ob Zertifikat noch gültig ist??

universitätbonn

Angriffsszenario 4

- Manueller Wechsel von einem 802.1X WLAN zu eduroam (Rogue AP)
- Erstes WLAN-Profil ohne Zertifikat
- eduroam Profil **mit** Root CA 2

universitätbonn

Auswertung

Gerät	Passwort im Klartext
Samsung Galaxy S Plus	☑
HTC Flyer	☑
Google Nexus 4	☑

freeradius-Log

[ttls] Got tunneled request

User-Name = “name@uni-bonn.de"

User-Password = “passwort"

FreeRADIUS-Proxied-To = 127.0.0.1

universitätbonn

Anmerkungen

- Keine Zertifikatsprüfung trotz Root CA 2 in Konfiguration
- DFN-CERT-2014-0833

universitätbonn

MSCHAPv2

mschapv2: Fri Oct 10 12:01:48 2014

username: name@uni-bonn.de

challenge: 56:fb:0c:56:ef:59:49:46

response: 59:2a:61:8f:ae:..:11:71:bc

jtr NETNTLM: name@uni-bonn.de:$

MSCHAPv2

asleap -C challenge -R response -W wordlist

asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>

Using wordlist mode with "/usr/share/dict/propernames".

hash bytes: b655

NT hash: 089659f3429d310d0ef72800ea19b655

password: passwort

universitätbonn

MSCHAPv2

- Dictionary Attack
- 500.000 PW/s mit Raspberry Pi
- 28s für 14 Mio. Passwörter
- GPU oder sogar Clouddienste nutzbar

universitätbonn

Zwischenergebnis

- Bugs im Betriebssystem
- Fragmentierung
- Unwissender/Bequemer Anwender
- Keine Zertifikatsbestätigung

Zertifikatsbestätigung

universitätbonn

Der Dienstanbieter ist von Server-Seite her machtlos

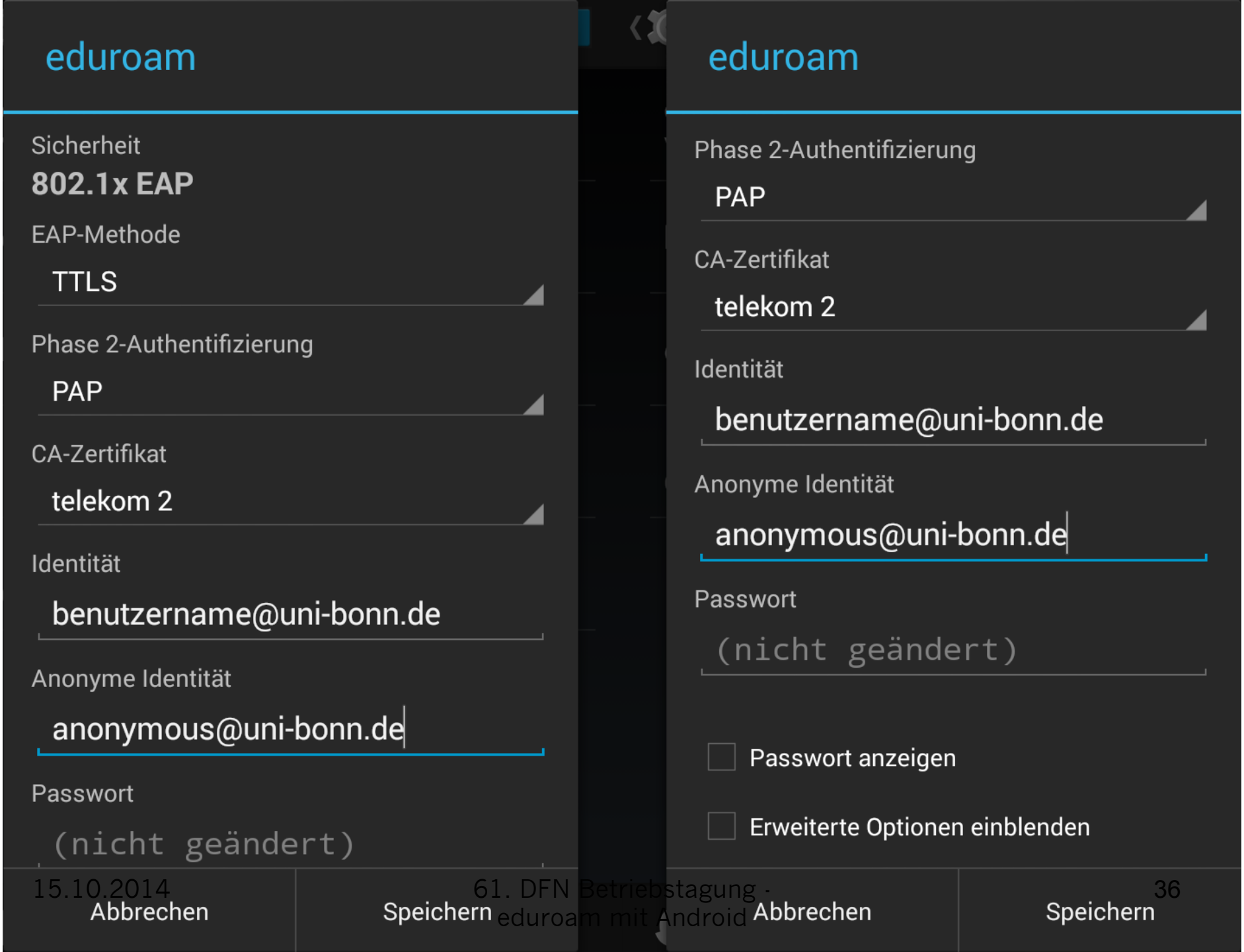
universitätbonn

Was können wir unternehmen?

universitätbonn

Handlungsmöglichkeiten

- Root CA 2 in WLAN-Profil einbinden
- Anleitungen kontrollieren/ anpassen!
- Zertifikat „bequem“ bereitstellen
- Support-Personal schulen
- Aktionstage veranstalten
- Apps für Eduroam


eduroam
Sicherheit
802.1x EAP
EAP-Methode
TTLS
Phase 2-Authentifizierung
PAP
CA-Zertifikat
telekom 2
Identität
benutzername@uni-bonn.de
Anonyme Identität
anonymous@uni-bonn.de
Passwort
(nicht geändert)
Abbrechen
Speichern
eduroam
Phase 2-Authentifizierung
PAP
CA-Zertifikat
telekom 2
Identität
benutzername@uni-bonn.de
Anonyme Identität
anonymous@uni-bonn.de
Passwort
(nicht geändert)
Passwort anzeigen
Erweiterte Optionen einblenden
Abbrechen
Speichern

universitätbonn

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?