

eduroam mit **Android**

Timo Bernard &
Karsten Honsack



Warum wir hier sind

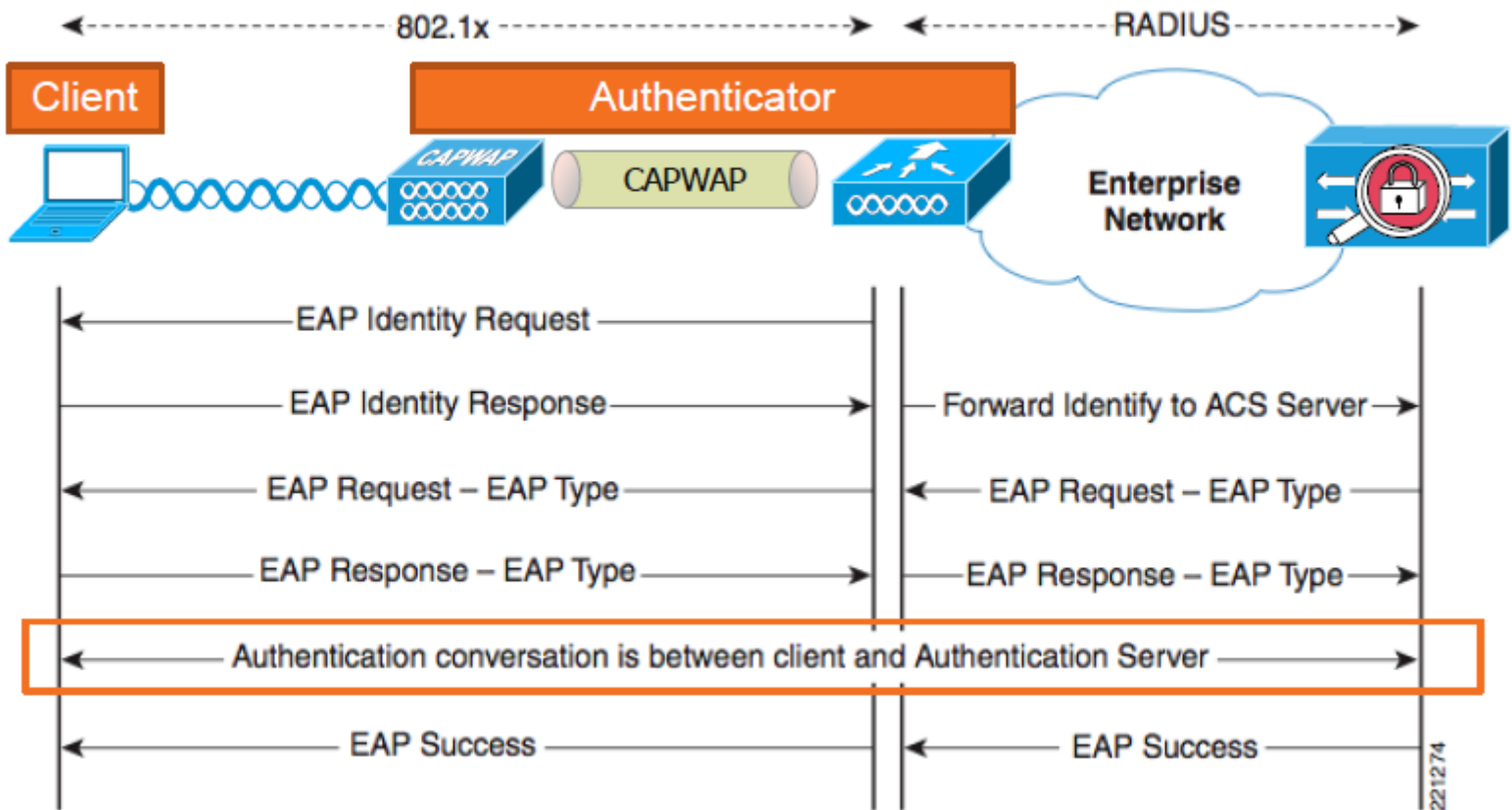
- Aktionstag der Ruhr-Universität Bochum
- Kontrolle der eduroam Konfiguration
- 2/3 von 350 Studierenden hatten unsichere Einstellungen

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

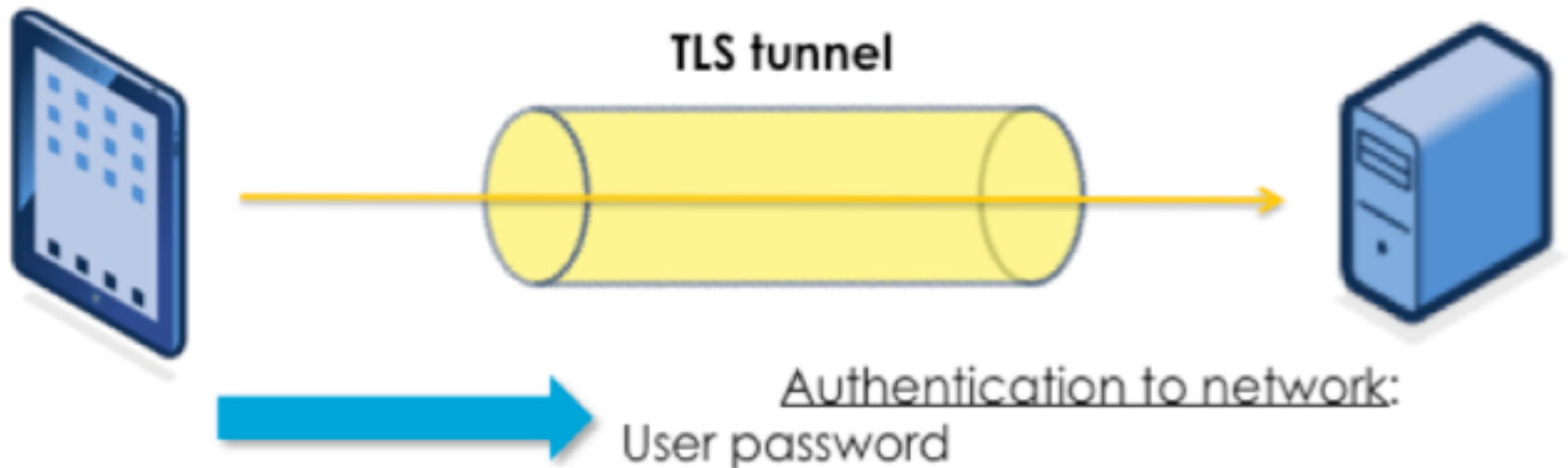
Agenda

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

Wie funktioniert EAP?



Wie funktioniert EAP?



Der Rogue AP

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

=> 14h Akkulaufzeit

Der Rogue AP



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

Angriffsszenario 1

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

Ergebnis

Gerät	Passwort im Klartext auslesbar
Samsung Galaxy S Plus	<input checked="" type="checkbox"/>
HTC Flyer	<input checked="" type="checkbox"/>
Google Nexus 4	<input checked="" type="checkbox"/>

freeradius-Log

[ttls] Got tunneled request

User-Name = "name@uni-bonn.de"

User-Password = "passwort"

FreeRADIUS-Proxied-To =

127.0.0.1

Anmerkungen

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

Angriffsszenario 2

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

Auswertung

Gerät	Passwort im Klartext
Samsung Galaxy S Plus	<input type="checkbox"/>
HTC Flyer	<input type="checkbox"/>
Google Nexus 4	<input type="checkbox"/>

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

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

Angriffsszenario 3

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

Auswertung

Gerät	Passwort im Klartext
Samsung Galaxy S Plus	<input checked="" type="checkbox"/>
HTC Flyer	<input checked="" type="checkbox"/>
Google Nexus 4	<input checked="" type="checkbox"/>

freeradius-Log

[ttls] Got tunneled request

User-Name = "name@uni-bonn.de"

User-Password = "passwort"

FreeRADIUS-Proxied-To =
127.0.0.1

Anmerkungen

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

Anmerkungen

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

Anmerkungen

- Prüfung ob Zertifikat noch gültig ist??

Angriffsszenario 4

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

Auswertung

Gerät	Passwort im Klartext
Samsung Galaxy S Plus	<input checked="" type="checkbox"/>
HTC Flyer	<input checked="" type="checkbox"/>
Google Nexus 4	<input checked="" type="checkbox"/>

freeradius-Log

[ttls] Got tunneled request

User-Name = "name@uni-bonn.de"

User-Password = "passwort"

FreeRADIUS-Proxied-To =
127.0.0.1

Anmerkungen

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

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

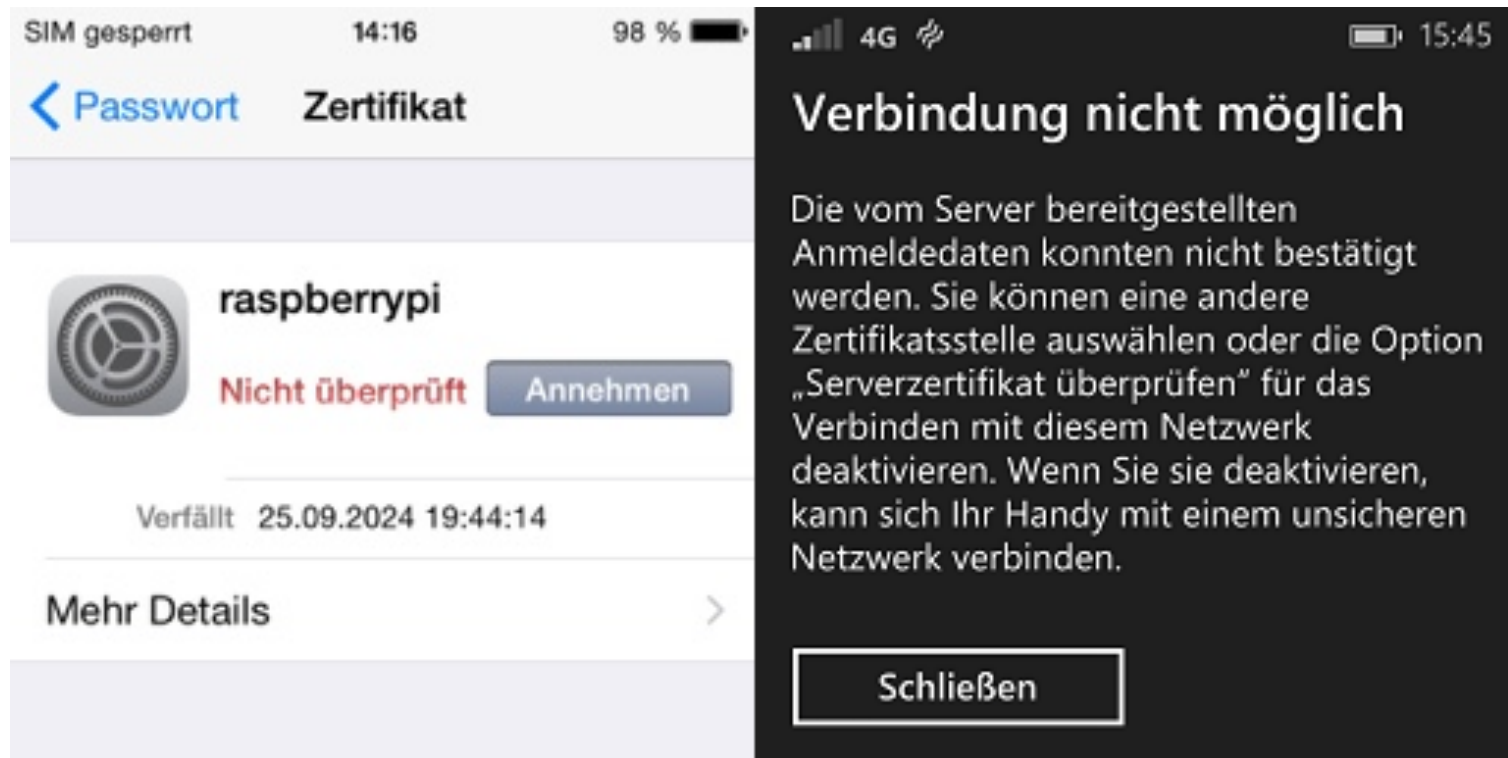
MSCHAPv2

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

Zwischenergebnis

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

Zertifikatsbestätigung



The image shows two overlapping screenshots from an Android phone. The background screenshot is the 'Zertifikat' (Certificate) screen in the Settings app. It shows a certificate for 'raspberrypi' with a status of 'Nicht überprüft' (Not checked) and an 'Annehmen' (Accept) button. The certificate expires on '25.09.2024 19:44:14'. The foreground screenshot is a black error dialog titled 'Verbindung nicht möglich' (Connection not possible). The text in the dialog reads: 'Die vom Server bereitgestellten Anmeldedaten konnten nicht bestätigt werden. Sie können eine andere Zertifikatsstelle auswählen oder die Option „Serverzertifikat überprüfen“ für das Verbinden mit diesem Netzwerk deaktivieren. Wenn Sie sie deaktivieren, kann sich Ihr Handy mit einem unsicheren Netzwerk verbinden.' (The login data provided by the server could not be confirmed. You can select another certificate authority or deactivate the option 'Check server certificate' for connecting to this network. If you deactivate it, your phone can connect to an insecure network.) There is a 'Schließen' (Close) button at the bottom of the dialog.

Der Dienstanbieter ist von Server-Seite her machtlos



Was können wir unternehmen?

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)

15.10.2014

Abbrechen

61. DFN Betriebstagung -
Speichern eduroam mit Android Abbrechen

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

36

Speichern

Vielen Dank für Ihre Aufmerksamkeit!
Fragen?