HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

Martin Weber

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

Vorgeschichte

- Geplante Umstellung der Radius-Infrastruktur für das Jahr 2017
- Inbetriebnahme eines RadSec-Proxy für DFN-Roaming
- Umstellung FreeRADIUS 2 zu FreeRADIUS 3
- Änderung der Zertifikatskette auf T-Telesec
- Umstellung des Realm Aufgrund einer Umbenennung der Hochschule

- Dabei wurde auch geprüft, ob die vorhanden Konfigurationen noch dem Stand der Technik und aktuellen Sicherheitsanforderungen entsprechen
- Es gab unter anderem Handlungsbedarf bei den Anmeldeverfahren EAP-TTLS/PEAP

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

EAP-TTLS / EAP-PEAP

- Verfahren sind technisch sicher, solange die Endgeräte richtig konfiguriert sind (Zertifikatsprüfung)
- Die richtige Konfiguration der Endgeräte kann serverseitig nicht überprüft werden
- Bei einer Stichprobe hatten nur 15% eine anonyme Identität gemäß veröffentlichten Anleitungen eingetragen
- Grund: man klickt auf eduroam, gibt seine Anmeldedaten ein und ist verbunden

- Supportanfragen, wie zum Beispiel „Wieso geht das WLAN an Uni XY nicht“, konnten immer auf einen nicht vorhandenen Realm zurückgeführt werden
- Sicherheitsrisiko: Logindaten lassen sich sehr leicht von Angreifern abfangen und ggf. auch den Datenverkehr über sich umleiten

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

Lösungsvorschläge

- separates Passwort für eduroam → Angreifer kann die Nutzerdaten immer noch leicht abfangen, kann diese jedoch nur für eduroam verwenden

- Anmeldung mit Nutzerzertifikaten über EAP-TLS
  - Ausstellung von Zertifikaten über DFN-PKI für alle Mitarbeiter und Studenten zu aufwendig, keine Bereitstellung von Profildateien
  - Aufbau eigener Zertifikatsinfrastruktur einmaliger Aufwand, dafür können Profile erstellt werden
  - einige Geräte haben EAP-TLS nicht korrekt implementiert

- Womöglich Einsatz EAP-PWD, ansonsten EAP-PEAP mit „Zwang zur richtigen Konfiguration“
  - nativ unterstütz durch Linux mit wpa_supplicant / Android 4.2
  - Windows mit Aruba Software (über CAT bereitgestellt)
  - Apple-Geräte keine Nutzung möglich

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

Vorstellung EAP-PWD

- Anmeldung über Nutzername und Passwort
- Client und Server authentifizieren sich gegenseitig
- Durch verschiedene kryptografische Funktionen wird das Passwort nie im Klartext übermittelt

Vorteile

- Es wird kein Zertifikat gebraucht
- Robust gegen eine Vielzahl von Angriffen

Nachteile

- Für ältere Systeme / nicht angepasste Anmeldeserver ist ein Klartext-Passwort notwendig
- Keine äußere Identität
- Wird nicht von allen Systemen unterstützt

- Weitere Informationen siehe Vortrag 64. DFN-BT der TU Clausthal

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

EAP-PWD unter Windows

- Client für Windows ist keine freie Software

- Problem 1: merkt sich keine Logins, nach jedem Start / Standby / Verbindungsabbruch müssen die Daten wieder neu eingegeben werden

- Problem 2: häufige Verbindungsabbrüche, bei uns alle 30 Minuten
- Undefinierter Zustand über 2-3 Minuten in dem Windows angezeigt hat „Verbunden“ man jedoch schon kein Zugriff mehr hatte
- Danach wieder der Loginbildschirm teilweise sogar mehrfach

- Weder national noch international lies sich eine Einrichtung finden die EAP-PWD unter Windows nutzt

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

EAP-PWD unter Windows

- Entwicklung eines Plugins für den Passwortmanager KeePass, welches das Anmeldeformular automatisiert ausfüllt und bestätigt
- Hat die Probleme etwas abgeschwächt, hat jedoch sehr den Charakter einer „Bastellösung“ ☺

- Im Roaming hatten wir teilweise andere Zeitpannen bis zur Trennung der Verbindung, die jedoch je Einrichtung immer gleich waren

- Setzen des Session-Timeout im Antwortpaket des Radius auf 5 Minuten, Ergebnis war Verbindungsabbruch nach ca. 5 Minuten
- Timeout von 1-2 Stunden bleib die Trennung alle 30 Minuten
- Keine Eintragungen in Protokollen des Radiusservers

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

EAP-PWD unter Windows

- Traceing des EAP-Host von Windows lieferte auch nur wenige zielführende Informationen
- Dennoch konnten wir damit den Fehler auf das EAP Re-authentication Protocol (ERP) beschränken, welches bei uns einen Zeitraum von 30 Minuten vorgegeben hat
- ERP dient der regelmäßigen Schlüsselerneuerung um Angriff auf die Funkverbindung zu erschweren

- Erhöhung des ERP-Zeitraumes in den WLAN-Controllern mildert das Problem, jedoch nur im lokalen Umfeld (nicht im Roaming) und zudem auf Kosten der Sicherheit
- Fazit: aruba-Client merkt sich nicht für die Reauthentifizierung notwendige Nutzerdaten

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

EAP-PWD unter Windows

- Frage: wie aufwendig ist eine Portierung von EAP-PWD über den quelloffenen wpa_supplicant unter Linux
- Für eine Implementierung unter Windows ist eine DLL mit ein paar öffentlichen Schnittstellen, sowie ein paar Registry-Einträgen notwendig
- Dabei regelt ein Registry-Schlüssel ob vom EAP-Host ein eigenes Login-Fenster aus der DLL geladen werden soll oder der Standard von Windows genutzt wird

- Nach Ändern des Schlüssels auf „Windows-Standard“ werden die Zugangsdaten gespeichert und es gibt auch kein Problem bei ERP mehr

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

EAP-PWD unter Windows

- Anpassung des aruba-Installers ist möglich, jedoch aus rechtlicher Sicht eher schwierig
- Kapselung in einem eigenen Installer, der den Registry-Schlüssel danach austauscht - dürfte jedoch zulässig sein
- In den Lizenzbedingungen fand sich dann folgender Satz:

  „The Programs may be used solely in conjunction with Aruba's hardware products and may be copied solely for installation and back-up purposes in support of your use of such hardware products."

- Ob dies nur die allgemeinen Bedingungen sind und es Ausnahmen für CAT / education gibt, konnte weder vom DFN noch von den CAT-Entwicklern beantwortet werden
- bis heute keine zuverlässige Aussage über die Nutzung des Tools für Hochschulen

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

EAP-PEAP unter Windows und Apple-Geräte

- Einsatz von EAP-PWD unter Windows vorerst gestoppt, um rechtliche Probleme (ähnlich dem SecureW2) zu vermeiden

- EAP-PEAP für alle System außer Linux/Android
- Keine Bereitstellung einer Anleitung, alles soll über Profildateien oder CAT gelöst werden
- In den Dateien wird eine „geheime“ äußere Identität verwendet, auf die der Radius-Server entsprechend prüft
- Hier ist die Annahme: wer die Identität vorweist, hat auch die Überprüfung des Zertifikates vorgenommen

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

Probleme bei der Umstellung

Apple (PEAP)

- keine Probleme

Android (PWD)

- keine Probleme

Linux (PWD)

- manche Distributionen (Fedora, CentOS) haben den wpa_supplicant ohne EAP-PWD kompiliert
- in der GUI ließ es sich jedoch auswählen, was natürlich noch mehr Verwirrung gestiftet hat
- Keine Fehlermeldungen, nur über Konsole brachte ein direkter Verbindungsaufbau über wpa_supplicant den Hinweis „nicht unterstützter EAP-Typ“

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

Probleme bei der Umstellung

Chrome OS (PEAP)

- CAT erstellt fehlerhafte Profildateien, nach manueller Korrektur jedoch problemlos

Windows Phone

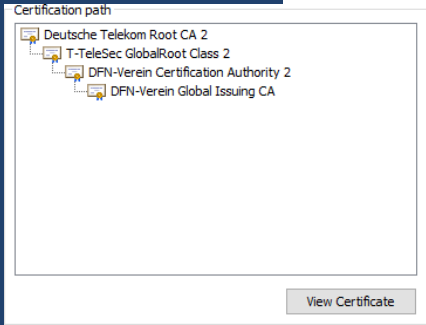
- Keine äußere Identität konfigurierbar → keine Nutzung von eduroam

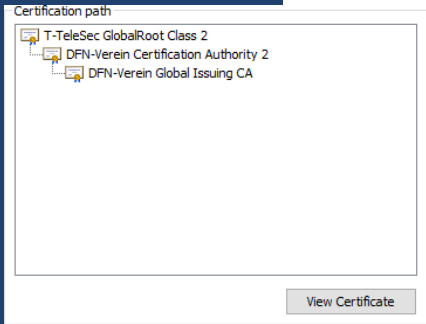
Windows RT (PEAP)

- Wird von CAT nicht unterstützt, daher haben wir eine Batch-Datei erstellt die das Profil einrichtet

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

Probleme bei der Umstellung





Windows (PEAP)

- Nutzer konnten trotz CAT keine Verbindung zum WLAN aufbauen
- Ursache lag beim Cross-Sign-Zertifikate der DFN-PKI
- Wird bei uns nicht eingesetzt, trotzdem haben manche Nutzer es sich bei anderen Einrichtungen „eingefangen“
- Der Zertifikatspfad endet bei Deutsche Telekom, Windows prüft aber gemäß CAT-Vorgaben auf T-Telesec → Verbindung wird abgelehnt
- Löschen hilft nicht, da es jeder Zeit wieder als Zwischen-CA gespeichert werden kann
- Lösung 2 CAs im CAT, kann jedoch bei anderen System wieder Probleme da diese nur 1 CA verarbeiten können

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Versuch eines EAP-PWD-Rollouts und Vergleich mit PEAP

Zusammenfassung und Fazit

- Umstellung verlief trotz kleiner Probleme recht reibungslos
- Kein Einsatz von CAT mehr
- Übergangszeit von alter CA-Gen1/FreeRADIUS2/@alt auf neue CA-Gen2/FreeRadius3/@neu wurde von wenigen genutzt
- Nach 3 Monaten hatten nur etwa 5% umgestellt, eine Stunde nach Abschaltung des alten Servers waren 75% der Systeme wieder verbunden

Folgende System können sich nicht mehr verbinden

- Android < 4.2
- Linux mit wpa_supplicant < 1.0 (ab 2.4 zugesichert)
- Linux mit „abgespecktem“ wpa_supplicant
- Windows Phone

Vielen Dank für Ihre Aufmerksamkeit

Kontaktdaten

Martin Weber

Hochschule Schmalkalden

martin.weber@hs.sm.de