Eingrenzung von Risiken durch Diebstahl von Eduroam-Credentials

Guido Bunsen[1]

Abstract: Die Credentials für WLAN-Zugänge sind in vielen unterschiedlichen Endgeräten abgelegt. Je nach Qualität der Implementierungen der Netzwerktreiber und dem Kenntnisstand der Endnutzer ist es möglich, diese von den Endgeräten oder mit Hilfe von nicht legitimierten Accesspoints zu stehlen. Dieser Beitrag beschäftigt sich mit den daraus entstehenden Risiken und Gegenmaßnahmen, die nicht den verbesserten Schutz wertvoller Passworte zum Ziel haben, sondern die Verwendung von weniger vertraulichen Passworten zu erzwingen, für die der vorhandene Schutz ausreicht. Im Anschluss wird auf die Herausforderungen im Umsetzungsprojekt eingegangen und auf das Potenzial, das entstandene System als Service für andere Hochschulen anzubieten.

Keywords: Eduroam, Passwort, Informationssicherheit,

1 Einleitung

Seit dem Start im Jahr 2002 hat sich Eduroam an den meisten europäischen Hochschulen als ein Standard für den WLAN-Zugang etabliert. Die Roamingfähigkeit von Eduroam hat dabei maßgeblich zum Erfolg beigetragen. Die weite Verbreitung von WLAN in mobilen Endgeräten mit dem Aufkommen der Smartphones hat dazu geführt, dass der durchschnittliche Hochschulangehörige bereits 2 und mehr Endgeräte besitzt, die Eduroam nutzen können.

Damit steigt auch das Risiko, dass Eduroam für Angriffe auf die Hochschulinfrastruktur missbraucht werden kann. Die Ursache liegt weniger im Design der Eduroam-Protokolle, als vielmehr in teilweise unvollständig implementierten Schnittstellen in den Endgeräten sowie mangelnder Sensibilisierung und unzureichenden Kenntnissen bei den Endnutzern.

In diesem Artikel werden diese Risiken dargestellt und im Anschluss daran werden mögliche Maßnahmen diskutiert, um die Risiken zu reduzieren oder die Auswirkungen abzumildern. Anschließend wird ein mittlerweile umgesetztes Projekt zur Realisierung der ausgewählten Maßnahmen vorgestellt und welche Erfahrungen dabei gemacht wurden.

[1]RWTH Aachen, IT Center, Seffenter Weg 23, 52056 Aachen, bunsen@itc.rwth-aachen.de

2 Funktionsweise von Eduroam und Gefährdungen

Eduroam geht auf einen Vorschlag von Klaas Wierenga vom niederländischen SurfNET aus dem Jahr 2002 zurück [Edu16]. Kern dieses Vorschlags ist, den Angehörigen der teilnehmenden Einrichtungen das Roaming zwischen den jeweiligen WLAN Infrastrukturen zu ermöglichen. Vereinfacht kommt dafür auf den Endgeräten des Nutzers ein sogenannter IEEE 802.1X Supplikant zum Einsatz um die Autorisierung am Accesspoint und an den Radiusservern der lokalen Einrichtung und gegebenenfalls der Heimateinrichtung vorzunehmen. Die Radiusserver müssen dazu über eine Softwarekomponente verfügen, um die Autorisierungsanfragen von nicht lokalen Benutzern an deren Heimateinrichtung weiterzuleiten (Proxy-Funktionalität). Da die Autorisierungen gegebenenfalls über mehrere Radiusserver geleitet werden, ist es erforderlich, dass die Anfragen „Ende zu Ende“ verschlüsselt werden um Man-in-the-Middle-Angriffe (MITM Angriffe) auf die Passworte des Benutzers zu verhindern. Eduroam nutzt dazu das TLS-Protokoll, um zwischen dem Supplikanten auf dem Endgerät und dem Radius-Server der Heimateinrichtung einen gesicherten Tunnel zu etablieren. Es ist von entscheidender Bedeutung, dass das Endgerät den Radiusserver korrekt verifiziert, indem das vom Radiusserver präsentierte Zertifikat geprüft wird.

Sofern das Zertifikat des Radius-Servers korrekt verifiziert wird, kann man derzeit von einem ausreichenden Schutz der Benutzerkennung und des Passwortes ausgehen. Eduroam verwendet sichere Protokolle, wenn die Supplikanten diese vollständig und korrekt implementieren, UND wenn die Nutzer die Endgeräte korrekt konfigurieren.

Während man in der Anfangszeit von Eduroam noch davon ausging, dass die meist technikaffinen Nutzer in der Lage waren, die wenigen auf Windows und Linux basierenden Endgeräte korrekt zu konfigurieren, hat sich die Situation bis heute grundlegend geändert. Mittlerweile nutzen die Angehörigen einer Hochschule im Schnitt bereits deutlich mehr als ein Endgerät und die Varianten von Endgeräten (Smartphone, Notebooks, Chromebooks, FireSticks, Chromecast, …) und zugrunde liegenden Betriebssystemen (Windows, Linux, IOS, Androids, …) und deren Versionen sind kaum noch zu überschauen. Für die Hersteller von Geräten ist es wichtiger, dass der Nutzer schnell seine Internetverbindung bekommt, als das diese ausreichend geschützt ist. Im Zweifelsfall unterbleibt die Verifizierung des Zertifikates, wenn sonst die Verbindung nicht zustande kommt. Usability geht vor. Selbst wenn sich ein Endgerät sicher konfigurieren lässt, ist fraglich, ob der Endnutzer die Risiken und die technischen Grundlagen versteht und die Einstellungen korrekt vornimmt. Selbst durch umfangreiche Sensiblisierungsmaßnahmen und Schulungsmaterialien lässt sich keine ausreichende Umsetzung erreichen.

Die beschriebenen Mängel führen dazu, dass Passworte der Benutzer durch sogenannte „Rogue Access Points“ oder „Evil Twins“ mit der SSID „Eduroam“ gestohlen werden können.

Der Vollständigkeit halber sei erwähnt, dass die Passworte auf dem Endgerät im Klartext

verfügbar sein müssen und somit zumindest für Personen mit Administrationsrechten und technischem Know-How zugänglich sind. Ebenso ergibt sich ein Risiko dadurch, dass moderne Smartphones den Inhalt der Geräte in der Cloud „sichern“ oder gar in sozialen Netzwerken mit Freunden teilen [Pcw15].

3 Welche Risiken entstehen für die Hochschule

Seit der Einführung von Eduroam vor mehr als 10 Jahren hat sich die Hochschul-IT-Landschaft dramatisch verändert. Mobile Endgeräte waren noch die Ausnahme und die Prozesse im Student-Life-Cycle wurden erst nach und nach auf Selfservice-Portale im Internet umgestellt. Heute sind die Prozesse im Campusmanagement auf eine zuverlässige Authentifizierung der Nutzer angewiesen. Auch der Betrieb einer E-Mail-Infrastruktur erfordert sichere Authentifizierung der Nutzer. Anderenfalls muss man damit rechnen, das gestohlene Accounts für den Spamversand missbraucht werden und die Reputation der Infrastruktur unter ein akzeptables Maß fällt.

Der im vorherigen Abschnitt skizzierte Diebstahl von Passworten für den WLAN-Zugang alleine ist bereits unerwünscht. Zwar ist die missbräuchliche Nutzung von Bandbreite nicht so problematisch. Aber oft reicht der Zugang zum WLAN einer Hochschule, um kostenpflichtig lizenzierte Dienste zu nutzen.

Das größere Problem aber resultiert aus der Tatsache, dass häufig die Passworte für den WLAN-Zugang auch für den Zugang zu anderen Informationen und Diensten genutzt werden können. Zum Teil war es die Politik zahlreicher Hochschulen unter dem Stichwort Single-Sign-On (SSO) die Usability der Infrastruktur zu verbessern und anderes überhaupt nicht zuzulassen. Zum anderen kamen die Nutzer mangels Sensibilisierung nicht auf die Idee, für unterschiedliche Dienste im Internet verschiedene Passworte zu wählen. So können gestohlene WLAN Credentials auch an anderen Stellen missbraucht werden mit der Konsequenz, dass nicht nur der Eigentümer des Accounts mit unangenehmen Konsequenzen rechnen muss. Auch für die Betreiber des WLANs und anderer Dienste ist mit negativen Konsequenzen zu rechnen wie Reputationsverlust und Aufwänden für forensische Untersuchungen und Aufräumarbeiten.

Aus den obigen Überlegungen lassen sich die folgenden Schlüsse ziehen: Die Angreifbarkeit der WLAN-Zugänge ist von den unmittelbaren Folgen her beherrschbar, weil die Bandbreitennutzung von den Kosten her vernachlässigt werden kann und eine gesetzwidrige Nutzung außerhalb der Verantwortung des Betreibers liegt. Die Verwendung von gestohlenen Credentials für höherwertige Dienste ist deutlich weniger zu akzeptieren.

4 Was können wir tun

Die Frage, die sich natürlicherweise nun stellt, ist die nach geeigneten Maßnahmen um die Risiken für den Diebstahl von WLAN-Passworten zu reduzieren oder zumindest die Folgen eines solchen Diebstahls abzuschwächen.

1. Zunächst zur Betrachtung der Maßnahmen, deren Umsetzung überwiegend in der Verantwortung der Nutzer zu sehen ist. Eine solche Maßnahme wäre die Nutzer so zu schulen, dass sie in der Lage und willens sind, das Endgerät „sicher“ zu konfigurieren. Derartige Sensibilisierungen und Schulungen in Form von Dokumentation sind sinnvoll und sollen auch bereitgestellt werden. Wir sind jedoch davon überzeugt, dass mit dieser Maßnahme allein keine eine ausreichende Wirkung nicht zu erzielen ist.
2. Eine Beschränkung auf Geräte mit einer „guten“ Implementierung würde die Risiken reduzieren. Jedoch ließe sich diese Maßnahme weder erzwingen, noch wäre es möglich, sie zu überwachen. Zusätzlich müsste eine Liste von „guten“ Geräten geführt und hinreichend begründet werden. Auch diese Maßnahme wurde verworfen.
3. Die zwangsweise Verwendung von solchen Passworten für den WLAN-Zugang, die nicht gleichzeitig auch für den Zugang beim Campusmanagement oder für E-Mail-Konten nutzbar sind, lässt sich über geeignete Passwort-Policies realisieren. Dafür hätten jedoch die Passwortregeln für Campusmanagement, den Mailserver und weitere Services angepasst werden müssen.
4. Die zwangsweise Verwendung von solchen Passworten für den WLAN-Zugang, die nicht gleichzeitig auch für den Zugang beim Campusmanagement oder für E-Mail-Konten nutzbar sind, lässt sich auch erreichen, indem die Passworte nicht durch den Benutzer frei wählbar sind, sondern zugewiesen werden. Diese Variante stieß zunächst auf Ablehnung. Weiter unten wird begründet, warum aus unserer Sicht die Nachteile vernachlässigt werden können.
5. Da der Diebstahl von Passworten nur schwer völlig zu verhindern ist, ist es gut, wenn ein solcher Diebstahl möglichst früh entdeckt wird. Das hilft nicht nur bei Diebstahl durch einen bösartigen Accesspoint wie oben beschrieben, sondern auch gegen Diebstahl durch Keylogger oder Phishing. Um einen Diebstahl zu entdecken, soll dem Benutzer die Möglichkeit gegeben werden ein Protokoll seiner Logins einzusehen. Dieses Protokoll könnte neben Datum und Uhrzeit auch eine Geolokation enthalten. Besonders auffällige Muster können benutzt werden, um den Nutzer anzuschreiben oder Accounts zu deaktivieren. Diese Maßnahme muss selbstverständlich datenschutzkonform gestaltet werden.

Wir haben uns entschieden, eine Kombination der beschriebenen Maßnahmen umzusetzen. Die Maßnahmen zur Sensibilisierung und Schulung lassen sich unabhängig von den anderen Maßnahmen durchführen und wurden auch in der Vergangenheit genutzt. Eine Intensivierung ist jedoch sinnvoll und möglich. Auch die Maßnahme zur

schnelleren Entdeckung von gestohlenen Accounts durch mehr Transparenz soll umgesetzt werden, allerdings erst zu einem späteren Zeitpunkt.

Die Maßnahme mit der größten Auswirkung auf den Nutzer und mit größeren Umbauarbeiten in der (Software-) Infrastruktur, nämlich der Zuweisung von Userid und Passwort für WLAN-Zugänge ist bereits im Rahmen eines weiter unten beschriebenen Projektes umgesetzt worden. Dazu vorab noch einige Bemerkungen.

Der Benutzer ist es gewohnt, sein Passwort frei zu wählen. Das ist unter Aspekten der Usability vorteilhaft, weil es so möglich ist, ein Passwort zu verwenden, das man sich leicht merken kann, z. B. weil es bestimmten Bildungsgesetzen folgt oder weil man es an vielen anderen Stellen ebenfalls nutzt. Allerdings geht es hier um WLAN-Passworte, die man typischerweise nur bei der Einrichtung eines Gerätes einmal einträgt und sich dann nicht mehr merken muss. Aus diesem Grund glauben wir, dass dieser Usability-Aspekt eine untergeordnete Rolle spielt. Um diesen gefühlten Nachteil weiter zu kompensieren, kann der Nutzer jederzeit weitere WLAN-Credentials anfordern, wenn er z. B. ein weiteres Gerät anbinden möchte. Er wird sogar dazu ermutigt, für jedes Gerät eigene Credentials zu verwenden. Das hat weitere Konsequenzen. So ist bei korrumpierten Accounts sogar feststellbar, welche Credentials missbraucht werden und damit, von welchem Endgerät sie gestohlen wurden. Alte unbenutzte Accounts werden automatisch nach mehrmonatiger Inaktivität gelöscht. Im Zusammenhang mit einer App wie z.B. der RWTH-App ist es möglich, für Smartphones das Passwort regelmäßig ohne Benutzerinteraktion im Hintergrund zu ändern. Da jedes Gerät eigene Credentials verwendet, sind durch die automatischen Passwortänderungen im Hintergrund keine Auswirkungen auf andere Geräte zu erwarten.

5 Umsetzungsprojekt

Die in den vorherigen Abschnitten beschriebenen Ziele und Ideen wurden etwa von März bis Juni 2014 entwickelt. Im September 2014 fiel die Entscheidung, ein Projekt „Eduroam-Gerätemanagement“ zur Realisierung dieser Ideen aufzusetzen. Zeitgleich wurde ein entsprechender Projektplan mit dem Projektende Dezember 2014 erstellt. Das Projekt hatte die folgenden für den Projektablauf entscheidenden Eigenschaften:

- Die Mehrzahl der Abteilungen im IT Center ist beteiligt (Netze, Services und Betrieb, Servicedesk, IT Prozessunterstützung, Administration und Organisation)
- Zahlreiche IT-Systeme oder Softwareprodukte müssen modifiziert werden (Radius, LDAP, Webanwendung für den Selfservice, Shibboleth)
- Unterstützung der stufenweisen Einführung durch geeignete Öffentlichkeitsarbeit in Zusammenarbeit mit dem Servicedesk für die Erstellung der zielgruppengerechten Dokumentation.

Es zeigte sich im Laufe des Projektes, dass aufgrund dieser Eigenschaften die folgenden

Aspekte in den Planungen berücksichtigt werden müssen:

- Konflikte zwischen Tagesgeschäft und Projektgeschäft
- Die Erfordernis, dass für bestimmte Arbeitspakete Kolleginnen und Kollegen aus verschiedenen Abteilungen gleichzeitig verfügbar sein müssen.
- Konflikte mit anderen Projekten
- Ausfälle durch Urlaub oder Krankheit
- Unklare Priorisierungen

Tatsächlich waren die Kernarbeiten erst Ende 2015 beendet. In der Zukunft werden Projekte, die abteilungsübergreifend durchgeführt werden, eher zunehmen und zur Normalität werden. Daraus resultieren neue Herausforderungen für das Projektmanagement und die abteilungsübergreifende Ressourcenplanung.

6 Erreichte Ziele

Auslöser für das Projekt Eduroam-Gerätemanagement war die Erkenntnis, dass unzureichende Vertraulichkeit der WLAN-Passworte negative Auswirkungen auf die Vertraulichkeit und Integrität anderer Services und Prozesse haben kann. Den damit verbundenen Risiken wurde begegnet, indem die Lösung nicht darin gesucht wurde, durch zahlreiche Maßnahmen einen ausreichenden Schutz der WLAN-Passworte zu erreichen. Ein solcher Schutz wäre nicht in ausreichendem Maße und mit vertretbarem Aufwand zu erreichen gewesen. Viel mehr besteht die Lösung darin, die Abhängigkeiten durch das Ausrollen von unabhängigen Passworten für den WLAN-Zugang aufzulösen.

7 Weitere Entwicklung

Schon in frühen Projektphasen gab es Ideen, das Eduroam Gerätemanagement als Service anzubieten. Der WLAN-Nutzer an der RWTH verwaltet seine WLAN-Accounts nach dem Wechsel auf das neue Verfahren über eine Webanwendung. Dort kann er für jedes seiner Geräte einen neuen Account anlegen. Den Zugang zu dieser Webanwendung erhält er nach Authentifizierung über das Verfahren Shibboleth zur verteilten Authentifizierung und Autorisierung [Sh16]. Zeitgleich mit dem Ergebnis der Authentifizierung erhält die Anwendung die Information, ob der Nutzer berechtigt ist, WLAN-Accounts anzulegen (Autorisierung).

Einer der durch den DFN für seine Mitglieder angebotenen Dienste ist die Authentifizierung- und Autorisierungsinfrastruktur, kurz DFN-AAI. Diese Infrastruktur ermöglicht Nutzern von Einrichtungen aus Wissenschaft und Forschung (Teilnehmer) über das Wissenschaftsnetz einen Zugang zu geschützten Ressourcen von Anbietern.

Nutzer, die auf geschützte Ressourcen zugreifen wollen, können sich an ihrer Heimateinrichtung authentifizieren und nach Übertragung der zur Autorisierung notwendigen Daten (Attribute) Zugang zu den Ressourcen erlangen.

Da die DFN-AAI auch auf Shibboleth basiert, kann die Webanwendung zur Verwaltung von WLAN-Accounts problemlos im Kontext des DFN-AAI als Anbieter eingesetzt werden [Dfna16]. Interessierte Mitglieder im DFN-Verein könnten so mit minimalem Aufwand ihren Angehörigen diesen Service bieten und so die Vertraulichkeit von Passworten für höherwertige Dienste verbessern. Im Rahmen eines Nachfolgeprojektes werden derzeit die Details für Migrations- und Supportkonzepte sowie für entsprechende Serviceangebote erarbeitet.

Eine andere geplante Weiterentwicklung betrifft die Verbindung von Eduroam-Gerätemanagement mit der RWTH-App für IOS oder Android. Durch Erweiterung des Eduroam-Gerätemanagements um einen entsprechenden Webservice kann die bereits authentifizierte App das Eduroam-WLAN automatisch einrichten und später auch periodisch das Eduroam-Passwort für das Endgerät wechseln. Die Vorteile für den Nutzer sind offensichtlich, mit den Details der Konfiguration muss er sich nicht mehr auseinandersetzen und durch die periodische Änderung des Passwortes bestehen eventuelle Risiken durch gestohlene Passworte nur für einen limitierten Zeitraum.

Literaturverzeichnis

[Edu16] eduroam, https://en.wikipedia.org/wiki/Eduroam, Abrufdatum: 5. Januar 2016

[Dfnc15] Google Android / eduroam-Zugangsdaten, https://www.dfn-cert.de/aktuell/Google-Android-Eduroam-Zugangsdaten.html, Abrufdatum 5. Januar 2016

[Pcw15] Windows 10's Wi-Fi Sense password sharing sparks security concerns, http://www.pcworld.com/article/2943752/wifi-passwordsharing-feature-in-windows-10-raises-security-concerns.html, Abrufdatum 5. Januar 2016

[Sh16] Shibboleth (Internet), https://de.wikipedia.org/wiki/Shibboleth_%28Internet%29, Abrufdatum 5. April 2016

[Dfna16] DFN-Verein: DFN-AAI, https://www.dfn.de/dienstleistungen/dfnaai/, Abrufdatum: 5. April 2016