Evil-Twin-Accesspoint

Andreas Huber
Betreuer: Marcel von Maltitz
Seminar Innovative Internettechnologien und Mobilkommunikation SS2014
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: hubera@in.tum.de

KURZFASSUNG

Diese Arbeit beschreibt den Angriff durch einen Evil-Twin-Accesspoint. Dazu wird im ersten Teil die exemplarische Vorgehensweise beim Durchführen dieses Angriffs erläutert. Aus der Perspektive des Angreifers sind die Rahmenbedingungen für einen erfolgreichen Angriff und die Möglichkeit des Angreifers gut zu erkennen. Im zweiten Teil der Arbeit werden Maßnahmen, die zum Erkennen und Verhindern dieses Angriffs vorgeschlagen wurden, auf Wirksamkeit und Durchführbarkeit verglichen. Hierbei wird auf die Möglichkeiten von Administratoren und Clients eingegangen. Zusätzlich werden Protokolle aufgezeigt, die Evil-Twin-Accesspoints verhindern sollen.

Schlüsselworte

Evil Twin, Evil-Twin Rogue Access Point, Angriff, Sicherheit WLAN

1. EINLEITUNG

Öffentlich zugängliche WLAN Netzwerke sind heute fast überall anzutreffen. Egal ob im Café, am Flughafen, in der Bibliothek oder im Restaurant, der Internetzugang über Funk ist selbstverständlich. Da es sich dabei oft um sehr kleine Netzwerke handelt, wird die Administration dieser Netze oft vernachlässigt. Auch aus Gründen des Komforts sind viele dieser Netzwerke nicht verschlüsselt. Da die einzige Information, die Netze für den Endanwender sichtbar voneinander unterscheidet, der Netzwerkname (ESSID) ist, ist es sehr einfach das öffentliche Netzwerk mit einem Laptop oder Smartphone nachzuahmen, indem mit dem mobilen Gerät ein Hotspot mit dem gleichen Namen, wie dem des öffentlichen Netzwerks, geöffnet wird. Es wird ein sogenannter „Evil-Twin-Accesspoint" gestartet. Ist dieser in der Nähe des Opfers, ist der Empfang des Evil-Twin-Netzes besser und das Opfer verbindet sich mit ihm. Das Opfer erkennt keinen Unterschied zwischen dem Hotspot des Angreifers und dem öffentlichen Netzwerk, da Anfragen an das Internet vom Angreifer über seine Internetverbindung weitergeleitet werden. Der Angreifer ist nun in der Lage, einen Man in the middle Angriff durchführen, er kann den Internetverkehr seines Opfers abhören, um beispielsweise Passwörter oder E-Mails mitzulesen und er kann den Internetverkehr gezielt beeinflussen, um das Opfer auf gefälschte Seiten umzuleiten, in denen Daten eingetragen werden im Glauben auf der offizielle Seite zu sein. In Wirklichkeit werden aber dem Angreifer die Daten ausgehändigt.

Der Aufbau eines Evil-Twin-Accesspoints im ersten Teil der Arbeit zeigt die einfache Durchführbarkeit dieses Angriffs und die Bedingungen, unter denen dieser Angriff möglich ist. Um diesen Angriff zu verhindern gibt es einige Ansätze, wie dieser erkannt und gestoppt werden kann. Es werden benutzer- und administratorseitige Möglichkeiten genannt. Mithilfe der Sicht aus Angreifer- und Verteidigerperspektive aus den ersten beiden Abschnitten werden daraufhin die Abwehrmöglichkeiten anhand wichtiger Kriterien für die Maßnahmen verglichen.

2. DURCHFÜHRUNG EINES EVIL-TWIN-AP-ANGRIFFS

Um die Funktionsweise und Wirksamkeit von Abwehrmaßnahmen gegen Evil-Twins beurteilen zu können, ist es hilfreich die Sicht eines Angreifers einzunehmen. Dazu wird im folgenden die Vorgehensweise zum Aufbau eines Evil-Twins erläutert.

2.1 Ausgangssituation

Der Evil-Twin-Accesspoint kann in Situationen eingesetzt werden, in der mindestens ein Rechner mit einem WLAN-Netzwerk verbunden ist, das keine Verschlüsselung benutzt, oder mit WEP, WPA oder WPA2 Personal gesichert ist, wobei der Schlüssel dem Angreifer bekannt ist. Der Beispielangriff arbeitet mit dem unverschlüsselten Netzwerk „Netzwerk1", mit dem der Benutzer verbunden ist. Abbildung 1 zeigt das Schema eines Evil-Twin-Angriffs, bei dem das Opfer eine Verbindung mit dem öffentlichen Netzwerk annimmt, in Wirklichkeit aber mit dem Evil-Twin verbunden ist, der die Anfragen in das öffentliche Netzwerk weiterleitet.

2.2 Ziel des Angriffs

Der Aufbau eines Evil-Twin-Accesspoints dient dem Angreifer dazu, einen Man in the middle Angriff auf das Opfer durchzuführen, bei dem private Daten des Opfers ausgelesen und der Internetverkehr umgeleitet werden kann.

2.3 Benötigte Tools

Um den Angriff durchführen zu können, benötigt man ein mobiles Gerät mit WLAN-Zugriff und einer weiteren Möglichkeit eine Verbindung mit dem Internet herzustellen. Dazu muss die WLAN-Karte des Gerätes einen Betrieb als gleichzeitiger Hotspot und Client erlauben, um den Internetverkehr des Opfers über eine Verbindung ins öffentliche Netz leiten zu können. Eine Alternative dazu ist die Einwahl des Angreifers in das Handynetz, oder dem Angreifer steht ein LAN zur Verfügung mit dem er die Nachrichten

doi: 10.2313/NET-2014-08-1_19

Abbildung 1: Aufbau des Angriffs

des Opfers ins Internet leitet. Von letzterem wird im folgenden Beispiel ausgegangen. Für diesen beispielhaften Angriff wurde ein Laptop mit Linux als Betriebssystem verwendet.

Das Programm `Aircrack-ng` wurde hauptsächlich entwickelt, um zu zeigen, wie einfach WEP-Netzwerke geknackt werden können. Es eignet sich auch als Universalwerkzeug, um Sicherheitslücken in WLAN-Netzen zu finden.[1] Im folgenden Angriff wird es zum Auslesen des Netzwerks und zum Erstellen des Hotspots benötigt. Zur Vergabe von gültigen IP-Adressen verwendet der Angriff den `ISC-DHCP-Server`[2]. Der Open Source DHCP Server kann mit einer Konfigurationsdatei angepasst werden. Das Routing der Internetverbindung in das WLAN-Netz erfolgt durch die Linux Kernel Programme `ifconfig` und `iptables`, die das Netzwerkinterface und die Firewall des Rechners konfigurieren. Weiterhin wird ein Programm zum Auslesen des Internetverkehrs benötigt. Der Beispielangriff nutzt hierzu `ngrep`[3], das anhand von regulären Ausdrücken Nachrichten aus dem Nachrichtenstrom filtert. Unter Ubuntu 13.10 können die vorgestellten Programme mit dem Befehl `apt-get install Aircrack-ng isc-dhcp-server ngrep` installiert werden.

2.4 Vorgehensweise

Die Vorgehensweise orientiert sich an [9]. Ein vorhandenes WLAN-Netz wird kopiert, indem ein WLAN-Netz mit gleichem Namen gestartet wird und die ursprüngliche Verbindung des Clients zum Accesspoint gestört wird.

2.4.1 Auslesen der WLAN-Infrastruktur

Zum Auslesen der WLAN-Infrastruktur wird die Programmsammlung `Aircrack-ng` benutzt. Ein Aufruf von `airmon-ng start wlan0 1` erzeugt ein Monitoring Device `mon0` auf Wifikanal 1. Mit dem Aufruf `airodump-ng mon0` werden die vorhandenen WLAN-Netze angezeigt. Der Aufruf liefert den Output aus Abbildung 2. Im oberen Teil des Outputs werden die gefundenen Netzwerke angezeigt, der untere Teil zeigt mit den Netzwerken verbundene Geräte. Von den gefundenen Netzwerken wird die MAC-Adresse des Routers (BSSID), die Empfangsstärke (PWR), die Anzahl der empfangenen Initialisierungspakete (Beacons), die gesendeten Daten (#Data, #/s), der Kanal (CH), die Bandbreite des Netzwerks (MB), die Verschlüsselung (ENC, CIPHER, AUTH) und der Netzwerkname (ESSID) angezeigt. Zum Durchführen eines Angriffs wählt man das Opfer-Netz aus der Liste der vorhandenen Netze aus. Für die weiteren Schritte werden Netzwerkname, Router-MAC-Adresse und Kanal, also ESSID, BSSID und CH des Zielnetzwerkes benötigt. Hier wird das Netzwerk mit der ESSID „Netzwerk1", das auf Kanal 8 sendet und BSSID 62:1B:5E:D9:7D:2E besitzt, ausgewählt, da #Data zeigt, dass in dem Netzwerk Daten versendet werden, also mindestens ein Benutzer aktiv ist, und keine Verschlüsselung angewandt wird. Anschließend wird das Programm `airodump-ng` beendet und das Interface `mon0` mit den Befehlen `airmon-ng stop mon0` und `airmon-ng stop wlan0` geschlossen.

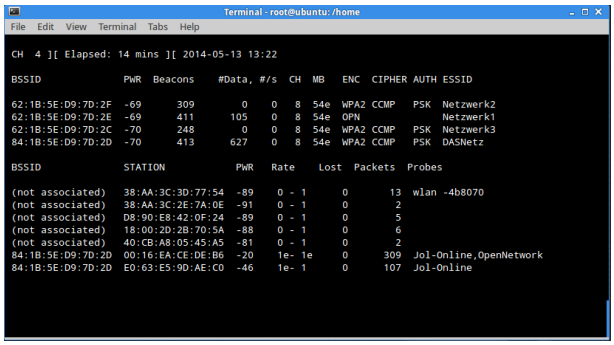

Abbildung 2: Ausgabe von Airodump-ng

2.4.2 Konfiguration des DHCP-Servers

Zur Konfiguration des DHCP-Servers wird im Dateisystem die Datei `/etc/dhcp/dhcpd.conf` erstellt. Diese Konfigurationsdatei wird mit folgenden Werten beschrieben:

doi: 10.2313/NET-2014-08-1_19

Listing 1: Konfigurationsdatei des DHCP Servers

```
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.2.128 netmask 255.255.255.128
{
    option subnet-mask 255.255.255.128;
    option broadcast-address 192.168.2.255;
    option domain-name-servers 8.8.8.8;
    option routers 192.168.2.129;
    range 192.168.2.130 192.168.2.140;
}
```

In der Konfigurationsdatei aus Listing 1 werden `default-lease-time` auf 600 Sekunden und `max-lease-time` auf 7200 Sekunden festgelegt. Diese Werte geben die Gültigkeitsdauer der DHCP-Konfiguration an. Nach Verstreichen der Default-lease-time bittet der Client um eine Verlängerung der Gültigkeit der IP-Konfiguration. War ein Client für die Dauer von Max-Lease-Time nicht verbunden, verfällt die IP-Adresse des Clients. Danach wird dem Client bei erneutem Verbinden eine andere IP-Adresse zugewiesen. Mit dem Befehl `subnet 192.168.2.128 netmask 255.255.255.128` wird das Subnet der Clients definiert, für das weitere Einstellungen vorgenommen werden. Die mit `option` angegebenen Werte überträgt der DHCP-Server an seine Clients. So erhalten die Clients Subnetzmaske, Broadcast-Adresse, die Adresse des Domain-Name-Servers und die Router-IP-Adresse. Diese wird später dem Angreifer-Laptop zugewiesen. Der angegebene DNS-Server an der IP-Adresse `8.8.8.8` ist ein öffentlicher DNS-Server von Google, an den die Clients ihre DNS-Anfragen richten werden. In dieser Konfiguration ist auch DNS Spoofing möglich. Dazu betreibt das Angreiferlaptop einen eigenen DNS-Server, um das Opfer auf Phishingseiten umzuleiten. In diesem Fall würde die IP-Adresse des Angreifer-Laptops als DNS Server angegeben. Die Zeile `range 192.168.2.130 192.168.2.140` legt den Bereich der verfügbaren IP-Adressen fest, die der Server vergeben kann.

2.4.3 Starten des Evil-Twin-AP

Jetzt kann der WLAN-Hotspot auf dem Laptop gestartet werden. Dazu wird erst mit `airmon-ng start wlan0 8` ein Aircrack-ng Monitoring Interface auf dem Kanal des Opfer-Netzwerks gestartet. Danach öffnet der Befehl `airbase-ng -e Netzwerk1 -c 8 -a 00:12:23:34:45:56 mon0` ein unverschlüsseltes WLAN-Netz mit der SSID „Netzwerk1" auf dem Kanal 8. Mit der Option -a wird dem Hotspot die willkürliche Mac-Adresse 00:12:23:34:45:56 zugewiesen. Das Programm läuft während des gesamten Angriffs. Abbildung 3 zeigt die Ausgabe des Programms `airbase-ng` nachdem sich ein Client mit dem Hotspot verbunden hat. Das Programm erstellt das Interface `at0`, auf dem die Nachrichten der Opfer ankommen. Verbindet sich ein Client mit dem Hotspot, wie beispielsweise in Abbildung 3 um 14:02:31 gezeigt, wird seine MAC-Adresse und das Netzwerk, mit dem er sich verbindet, angezeigt. Hier hat das Gerät die MAC-Adresse 64:20:0C:DF:2F:AC und verbindet sich mit dem „Netzwerk1", das vorher erstellt wurde. Der Ausdruck „reassociated" zeigt, das das Opfer-Gerät davon ausgeht im gleichen Netzwerk auf einen anderen Accesspoint zu wechseln. Das Opfer erkannte den Evil-Twin also nicht als solchen.

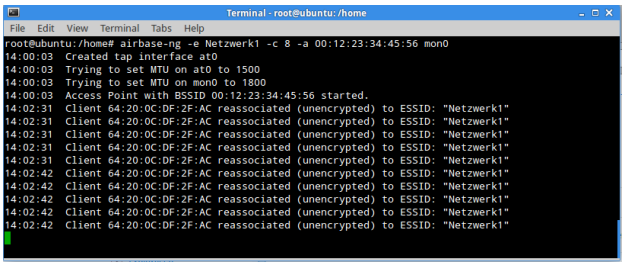

Abbildung 3: Ausgabe von airbase-ng nachdem sich ein Opfer verbunden hat.

2.4.4 Einrichten von Routing und DHCP-Server

In einem neuen Konsolenfenster wird nun das Routing so eingerichtet, dass die verbundenen Clients Internetzugang haben. Zuerst muss das Interface des Hotspots `at0` gestartet werden. Dies geschieht durch `ifconfig at0 up`. Daraufhin werden dem Interface mit `ifconfig at0 192.168.2.129 netmask 255.255.255.128` Router-IP-Adresse und Netzmaske des durch den DHCP-Server verwalteten Netzes zugewiesen. Der DHCP-Server wird durch den Befehl `dhcpd -cf /etc/dhcpd/dhcpd.conf` mit der vorher konfigurierten Datei `/etc/dhcpd/dhcpd.conf` gestartet. Um ein korrektes Laden der Konfigurationsdatei sicherzustellen, wird mit `service isc-dhcpd-server restart` der Server neu gestartet.

Die Linux Firewall besteht aus verschiedenen Tabellen, in denen jeweils bestimmte Nachrichten verändert, weitergeleitet oder gelöscht werden. Die Bearbeitung der Nachrichten in der Firewall erfolgt in Chains, in denen die Nachrichten vom einen Befehl zum nächsten gereicht werden. Die Konfiguration der Linux Firewall wird durch das Programm `iptables` durchgeführt.[5]

Die folgenden Befehle aus [9] konfigurieren die Firewall des Evil-Twins:

```
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
iptables --table nat --append POSTROUTING
         --out-interface eth0 -j MASQUERADE
iptables --append FORWARD -j ACCEPT
         --in-interface at0
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Mit den flush-Befehlen werden die Firewall-Regeln aus den Chains gelöscht, bevor mit delete-chain auch die vorhandenen Chains gelöscht werden. Beide Befehle werden sowohl für die Standardtabelle filter (ohne `--table`-Option), als auch für die Network Address Translation(NAT)-Tabelle durchgeführt. Der Befehl `iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE` fügt der Chain `POSTROUTING` in der Chain der NAT-Tabelle eine Regel hinzu, die Nachrichten an das Interface `eth0` verändert, hinzu. Die hinzugefügte Regel `-j MASQUERADE` startet eine Network Address Translation für die dynamisch vergebenen IP-Adressen des Hotspots. So sieht das Netz, an dem der Angreifer mit dem Internet verbunden ist, nicht, dass mehrere Geräte auf das Netzwerk zugreifen und das Netzwerk kann den Angreifer nicht als solchen erkennen. Mit `iptables --`

doi: 10.2313/NET-2014-08-1_19

`append FORWARD -j ACCEPT --in-interface at0` wird der Chain der Standardtabelle (`filter`) der Firewall eine Regel hinzugefügt. Sie erlaubt allen Nachrichten aus dem Hotspot-Netz `at0` das Passieren der Firewall. Der Befehl `echo 1 > /proc/sys/net/ipv4/ip_forward` leitet eine Eins in die Datei `/proc/sys/net/ipv4/ip_forward`. Diese Konfiguration des Linux-Kernels erlaubt das Weiterleiten von IPv4-Nachrichten und das Angreifer-Laptop kann als Router arbeiten.

2.4.5 *Auffinden und Stören von Client-Verbindungen*

Der Befehl `airodump-ng --bssid 62:1B:5E:D9:7D:2E -c 8 mon0` mit MAC-Adresse und Kanal des Opfernetzwerks startet das Programm `airodump-ng`, das das Zielnetzwerk und seine Clients auflistet. Abbildung 4 zeigt die Ausgabe des Programms. In der Tabelle findet man die BSSID des potentiellen Opfers. Mit dieser kann im Folgenden eine Nachricht zur Unterbrechung der Verbindung vom Accesspoint an den Client gefälscht werden. Dazu benötigt man die MAC-Addresse des Opfers, die im unteren Teil der Ausgabe unter `STATION` abgelesen werden kann, hier 00:16:EA:CE:DE:B6 (Abbildung 4, mitte). Mit dem Befehl `aireplay-ng -0 0 -a 62:1B:5E:D9:7D:2E -c 00:16:EA:CE:DE:B6 -e Netzwerk1 --ignore-negative-one mon0` sendet der angreifende Rechner ständig Deauthentifizierungsnachrichten an den Client. Mit den Optionen `-a -c` und `-e` werden die MAC-Adressen von Accesspoint und Client und die ESSID des Netzwerks angegeben. Diese Informationen sind in den Deauthentifizierungsnachrichten enthalten und werden deshalb vom Programm als Eingabe benötigt. Abbildung 4 zeigt die Ausgabe des Programms, das in regelmäßigen Abständen Unterbrechungen sendet und die empfangenen Bestätigungen des Clients anzeigt. Die Verbindung des Opfers mit dem Originalnetzwerk bricht ab.

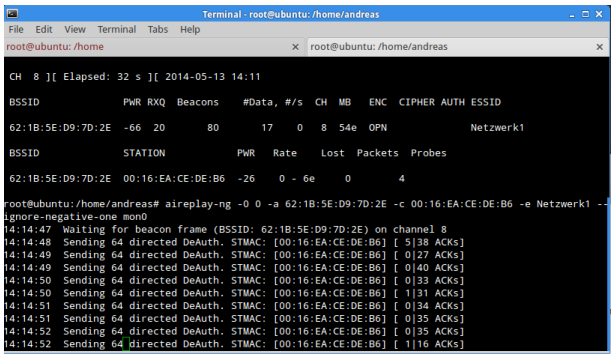

Abbildung 4: Ausgabe von airodump-ng und aireplay-ng

2.4.6 *Opfer verbindet sich mit Angreifer*

Da die Verbindung zum ursprünglichen Netzwerk abgebrochen ist, versucht der Client sich mit dem Netzwerk erneut zu verbinden. Dies geschieht je nach Gerät und Betriebssystem manuell oder automatisch. Da der Name des Originalnetzwerks mit dem des Angreiferhotspots identisch ist und eine Verbindung zum Originalnetzwerk durch das Programm `aireplay-ng` verhindert wird, verbindet sich das Opfer mit dem Netzwerk des Angreifers. Oft ist das Stören der Verbindung des Clients nicht notwendig. Eine entscheidende Rolle bei der (automatischen) Wahl des Accesspoints spielt die Empfangsstärke des Netzwerks. Ist das Angreiferlaptop dem Opfer näher als der Accesspoint, verbindet sich das Opfer-Gerät oft automatisch mit dem Angreifer, da das mobile Gerät aus Energiespargründen Accesspoints mit besserem Empfang bevorzugt.

2.4.7 *Abgreifen und verändern von Daten*

Nach einer erfolgreichen Verbindung läuft der gesamte Internetverkehr des Opfers über das Angreiferlaptop. Jetzt können beispielsweise die HTTP-Nachrichten des Opfers mit `ngrep -d at0 -t '^(GET|POST)' 'tcp and dst port 80 and src host 192.168.2.130'` abgegriffen werden. Die Option `-d` legt das Interface auf `at0` fest. Mit `-t` wird die Zeit der Nachricht mit angezeigt. Durch den regulären Ausdruck `'^(GET|POST)'` werden alle GET- und POST-Befehle des Opfers aufgezeichnet, die durch den Filter `tcp and dst port 80 and src host 192.168.2.130` gekommen sind, also vom Opfer mit der IP-Adresse 192.168.2.130 an den TCP-Port 80 gesendet wurden. Werden vertrauliche Nachrichten unverschlüsselt mit HTTP-GET oder HTTP-POST an den Server übertragen, so kann der Angreifer diese aufzeichnen und gelangt beispielsweise an Passwörter des Opfers. Durch Veränderung des regulären Ausdrucks und des Filters ist es auch möglich über HTTP, IMAP oder POP3 unverschlüsselt übertragene E-Mails des Opfers aufzuzeichnen.

Eine weitere Möglichkeit, die dieser Angriff bietet ist das Phishing von Online-Accounts. Dazu wird auf dem Angreifergerät ein DNS-Server, beispielsweise `bind` [4] gestartet. Der Domain Name Server-Eintrag in der DHCP-Serverkonfiguration aus Listing 1 wird auf die IP-Adresse des Angreiferlaptops `192.168.2.129` umgeändert. Der DNS-Server wird so konfiguriert, dass Anfragen zu der anzugreifenden Seite auf `192.168.2.129`, also auf das Angreiferlaptop geleitet werden, auf dem zusätzlich ein Webserver läuft, der eine zum Original möglichst identische Loginseite präsentiert, auf der das Opfer seine geheimen Daten eintippt und sie so dem Angreifer preisgibt.

Der vorgestellte Angriff ist ähnlich auch in Netzwerken möglich, die mit WEP verschlüsselt sind, vorausgesetzt der Angreifer kennt das Kennwort des Netzwerks. Das Auslesen der Netzinfrastruktur und die Konfiguration der Firewall bleiben gleich. Der einziger Unterschied ist der Aufruf von `airbase-ng` mit der Option `-w Schlüssel`, bei der der Netzwerkschlüssel angegeben wird. WPA-, WPA2-Personal- und WPA2-Enterprise-verschlüsselte Netzwerke können mit diesem Tool nicht gefälscht werden, allerdings ist es möglich ein unverschlüsseltes Netzwerk mit gleichem Namen zu erstellen. Wenn gleichzeitig das Originalnetzwerk mit `aireplay-ng` gestört wird, ist es möglich, dass sich Benutzer ohne weiteres Nachdenken mit dem Netzwerk mit gleichem Namen verbinden, falls dieses eine funktionstüchtige Internetverbindung bietet. Mit diesem Trick ist auch das Phishing des Netzwerkschlüssels möglich, wenn nämlich jeder Aufruf einer Internetseite auf eine Landing Page führt, die unabhängig von der aufgerufenen Seite auf jede Anfrage an das Web zurückgegeben wird, wo die Anmeldedaten des Nutzers abgefragt werden. Unvorsichtige Benutzer geben hier ihre Anmeldedaten ein und händigen sie so dem Angreifer aus.[9]

2.5 Funktionsfähigkeit des Angriffs

Der Angriff, wie hier beschrieben wurde mit verschiedenen Geräten als Client getestet. Während ein PC mit Microsoft Windows 8.1 und ein Apple iPad mit iOS7 eine Verbindung zum Evil-Twin herstellten und je nach Empfangsqualität der Netze zwischen Originalnetzwerk und Evil-Twin wechselten, war es mit einem Android 4.4-Smartphone nicht möglich sich mit dem Evil-Twin zu verbinden. Dies zeigt, dass Evil-Twin-Angriffe schwer zu erkennen sind und auf verschiedenster Hard- und Software durchführbar sind.

3. MÖGLICHE ANGRIFFSABWEHR

Um das Abgreifen von Benutzer- und Firmendaten durch einen Evil-Twin-AP zu verhindern, gibt es sowohl auf der Seite des Netzes als auch auf der Seite des Benutzers Ansätze, wie Evil-Twins erkannt und entfernt werden können. Im folgenden werden jeweils zwei Möglichkeiten auf Administratorseite und auf Clientseite vorgestellt. Auch durch Änderung des WLAN-Protokolls und durch die Verwendung von verschlüsselten Protokollen in der Anwendungsebene kann ein Angriff eines Evil-Twins verhindert werden.

3.1 Administratorseitige Möglichkeiten

Es liegt im Interesse von Netzwerkadminstratoren das Netz gegen Angriffe von Evil-Twin-Accesspoints zu schützen, da Angreifer mit Evil-Twin-APs an vertrauliche Daten im Netzwerk gelangen können. Dazu überwacht der Administrator das Netzwerk, findet falsche APs und initiiert deren Abschaltung.

3.1.1 Funküberwachung

Bei der Funküberwachung werden die Funkfrequenzen von WLAN nach unberechtigten WLAN-Netzen abgesucht. Dazu werden die Daten der autorisierten Accesspoints im Netzwerk in einer Datenbank verwaltet. Es werden Daten, wie Netzwerkname, Funkkanal und MAC-Adresse des Accesspoints gesammelt und mit den Werten in der Datenbank verglichen. Startet ein Angreifer einen Evil-Twin des Originalnetzwerks, sieht das Messgerät das neue Netz und bemerkt, dass die MAC-Adresse des Accesspoints nicht bekannt ist und es sich um einen Angreifer handeln kann. Diese Maßnahme kann entweder in regelmäßigen Abständen manuell durch den Administrator durchgeführt werden, indem dieser mit einem mobilen Gerät den Sendebereich des WLAN-Netzwerks absucht, oder durch fest installierte Geräte, die eine ständige Überwachung durchführen. Durch Einschleusen von Broadcast-Paketen in das Netzwerk können zusätzlich Geräte gefunden werden, die nur sehr selten senden, wenn sie auf diese eingeschleusten Pakete reagieren und somit mit dem eigenen Netzwerk verbunden sind. Das Verhindern des Angriffs kann durch Finden und Entfernen des Angreifergeräts erfolgen, oder die Verbindungen des Angreifernetzwerks werden ähnlich wie in 2.4.5 durch Senden von Deauthentifizierungsnachrichten unterbrochen.[6]

3.1.2 Netzwerküberwachung

Bei der Netzwerküberwachung wird durch die Überwachung des Netzwerkverkehrs an einem zentralen Punkt, wie dem Router, versucht die Netzwerkinfrastruktur zu erkennen. Dazu werden die Daten der autorisierten Benutzer benötigt, ihre MAC- und IP-Adresse und weitere Charakteristiken, wie geöffnete Ports, müssen bekannt sein. Durch Einstellungen der Firewall am Router werden nur Pakete bekannter Adressen ins Internet geleitet. Eine andere Möglichkeit ist das aktive Absuchen. Mit dem Senden von Nachrichten an bestimmte Adressräume, die Evil-Twins nutzen könnten, versucht der Administrator Charakteristiken angeschlossener Geräte zu bekommen und vergleicht sie mit den Charakteristiken der erlaubten Geräte. Bei unbekannten Geräten wird von Angreifern ausgegangen. Sie werden vom Netzwerk ausgeschlossen.[6]

3.2 Clientseitige Möglichkeiten

Da der Client keinen Überblick über die Sicherheitsmaßnamen des Administrators im Netz hat und vor allem kleinere, öffentlich zugängliche Netzwerke oft schlecht geschützt sind, ist es für den Client wichtig, Möglichkeiten zu haben, festzustellen, ob man sich mit dem echten Netzwerk verbindet, oder ob die Verbindung über einen Evil-Twin-Accesspoint führt.

3.2.1 Zeitmessung

Wird davon ausgegangen, dass Evil-Twin-Accesspoints die Internetverbindung des öffentlichen WLAN Netzes nutzen, um selbst mit dem Internet verbunden zu sein und dieses WLAN-Netz ein älteres Netz nach dem Standard 802.11b/g ist, gibt es eine erfolgreiche Möglichkeit um auf der Clientseite Evil-Twin-APs erkennen zu können. Dazu wird die Zeit gemessen, die eine Nachricht im Netzwerk zu einem bestimmten Server braucht. Da eine Nachricht, die über einen Evil-Twin-AP gesendet wurde, nicht nur die Funkstrecke zwischen Benutzer und Accesspoint überwinden muss, sondern vom Benutzer zum Evil-Twin und von dort zum Accesspoint geleitet wird, ist die Zeit der Nachricht im Netzwerk entsprechend länger. Sind Charakteristiken des Netzwerks bekannt, kann die aktuelle Zeit zwischen zwei ankommenden Nachrichten genutzt werden, um sie mit den Durchschnittswerten im Netzwerk zu vergleichen. Da diese Charakteristik relativ stabil bei unterschiedlichen Nutzungsraten im Netzwerk verhält, ist der Einfluss der Anzahl der Benutzer im Netz gering. Lange Nachrichtenübertragungszeiten im Vergleich zum Durchschnitt des Netzwerks deuten auf eine Verbindung über einen Evil-Twin-AP hin. Ist die Charakteristik eines Netzwerks unbekannt, kann ein alternativer Algorithmus das Risiko eines Evil-Twin-Angriffs ohne Vorkenntnisse zum spezifischen Netz bewerten. Als Charakteristik hierzu dient der Quotient aus der Zeit zwischen zwei eingehenden Nachrichten vom Server und der Antwortzeit des nächsten Accesspoints, der entweder der Accesspoint im Originalnetzwerk ist, oder der Evil-Twin-AP. Je größer dieser Quotient ist, um so wahrscheinlicher ist ein Evil-Twin-AP, da dann die Nachricht zum Server im Vergleich zu einer Nachricht zum Accesspoint sehr lange dauert und somit die Strecke nach dem Accesspoint lang ist.[7]

Ein Problem dieses Ansatzes ist, dass er auf viele Annahmen aufbaut, die nicht immer bei Evil-Twin-APs zutreffen. Der Evil-Twin muss nicht unbedingt über WLAN und mit dem gleichen Netzwerk verbunden sein, er kann beispielsweise Zugriff auf Ethernet haben, oder mit dem Handynetz verbunden sein. Damit verändert sich die Nachrichtenübertragungszeit zwischen Evil-Twin und Server und der Evil-Twin ist nicht mehr als solcher identifizierbar. Es wird auch von einem Internetzugang mit sehr kurzen Reaktionszeiten aus-

doi: 10.2313/NET-2014-08-1_19

gegangen, die Reaktionszeiten zwischen AP und Server im Internet müssen kurz sein. Ist das nicht der Fall, wird die gemessene Antwortzeit des Servers zu lange und es wird fälschlicherweise ein Evil-Twin-Angriff angenommen. Der Ansatz in [7] setzt sich auch nur mit den älteren WLAN-Varianten 802.11b/g auseinander. Die kürzere Übertragungszeit von Nachrichten durch die höhere Bandbreite bei neueren WLAN-Varianten kann zu einem kleineren Unterschied der Nachrichtenübertragungszeiten führen und damit zum erschwerten Erkennen von Evil-Twins. Ist das Verhalten des Clients bekannt, kann der Evil-Twin den aufgerufenen Server simulieren und die Erkennung wird unmöglich.

3.2.2 Context Leashing [8]

Evil-Twin-Angriffe sind nicht nur an der Stelle möglich, an der das originale WLAN-Netz vorhanden ist, wenn ein Evil-Twin ein dem Opfer bekanntes Netzwerk an einem beliebigen anderen Ort öffnet, geht das Opfer vom Originalnetzwerk aus und verbindet sich mit dem Angreifer. Da der Angriff nicht im Originalnetz oder in dessen Nähe stattfindet, hat der Administrator des Netzes keine Möglichkeit diesen Angriff zu verhindern. Deshalb ist diese Maßnahme für die Clientseite wichtig. Durch das Vergleichen der vorhandenen Netze an der Stelle an der verbunden wird, kann dies verhindert werden. Dazu speichert das Gerät SSID und Empfangsstärke der umgebenden WLAN-Netzwerke beim ersten Verbinden mit dem WLAN-Netz. Beim erneuten Verbinden mit dem Netz wird die vorhandene WLAN-Infrastruktur mit den gespeicherten Werten verglichen. Wird dabei ein Unterschied der gespeicherten Netze zu den vorhandenen erkannt, wird von einem Evil-Twin ausgegangen. Um zu verhindern, dass ein Angreifer nicht nur das Opfer-Netzwerk nachahmt, sondern durch senden entsprechender Beacons alle Netze simuliert, kann zusätzlich zu den Namen der Netze deren Empfangsstärke ausgewertet werden. Dazu wird die Summe der Empfangsunterschiede von gespeichertem und aktuell gemessenem Netzwerk berechnet. Überschreitet die Summe einen Grenzwert, wird von einem Evil-Twin-AP ausgegangen.[8]

Dieses System macht den Aufwand eines erfolgreichen Evil-Twin-Angriffs an einer Stelle, an der das Netz nicht verfügbar ist, größer, allerdings kann der Angriff damit nicht ausgeschlossen werden. Wenn der Angreifer nicht nur die umgebenden Netze simuliert, sondern auch deren Sendestärke variiert und sie den gemessenen Werten anpasst, erkennt der Ansatz keinen Unterschied zur Originalinfrastruktur und eine Verbindung mit dem Evil-Twin wird hergestellt. Durch die Funktion moderner Smartphones und Rechner, die das einfache Öffnen eines Hotspots an beliebiger Stelle erlauben, um beispielsweise Daten auszutauschen, besteht bei diesem Ansatz außerdem die Gefahr, das echte Netze unrichtigerweise als Evil-Twins erkannt werden. Da diese mobilen Hotspots oft ein- und ausgeschaltet werden und zusätzlich häufig ihre Position ändern, ist es nicht sicher, ob sich die WLAN-Infrastruktur an einer Stelle bis zum nächsten Verbinden nicht ändert. Damit können originale Netze als Evil-Twin erkannt werden.

3.3 Angriffsverhinderung durch das Protokoll

Die Ansätze auf Client- und Administratorseite können Evil-Twin-Angriffe verhindern, ein vollkommener Schutz vor Evil-Twins ist durch diese Ansätze aber nicht sicher möglich, da alle Schutzmaßnahmen umgangen werden können. Diese Gefahr besteht auch unabhängig von der Verschlüsselung der WLAN-Verbindung. Auch wenn der Angriff für unverschlüsselte Netzwerke einfacher ist, als für verschlüsselte, kann ein Angreifer, der an den Schlüssel des Netzwerks gelangt ist, auch Evil-Twins von verschlüsselten Netzwerken zu erstellen, die nicht von den Original-Netzen zu unterscheiden sind. Selbst Netzwerke, die über WPA2 Enterprise geschützt sind, können mit entsprechendem Aufwand von einem Evil-Twin kopiert werden, wie in [10] gezeigt wird. Der Standard von WPA2 Enterprise 802.1X verwendet zur Authentifizierung der Clients das Extensible Authentication Protocol (EAP), das verschiedene Möglichkeiten der Authentifizierung bietet. Wird eines der weit verbreiteten Protokolle PEAP oder TTLS zur Authentifizierung verwendet, besteht die Gefahr eines Angriffs. Die Authentizität des Accesspoint-Betreibers wird durch X509-Zertifikate gewährleistet. Ist es dem Angreifer möglich sich ein Zertifikat der gleichen Zertifizierungsstelle, von der auch das Zertifikat des Originalnetzes stammt, ausstellen zu lassen, so vertraut der Client dem Angreifer-AP. Das häufig verwendete innere Authentifizierungsverfahren auf das der Angreifer jetzt Zugang hat ist MSCHAPv2, das mit etwas Aufwand geknackt werden kann. Gelingt dies, erkennt der Benutzer in dem Angreifer-AP einen gültigen Accesspoint.[11]

3.3.1 Protokoll mit Trust-On-First-Use

Der Schwachpunkt, der bei dem Angriff auf WPA2 Enterprise-Netze ausgenutzt wird, ist die Angreifbarkeit des EAP. Eine Möglichkeit diesen Schwachpunkt zu beheben, ist die Erweiterung des Protokolls um Trust-On-First-Use, das heißt, dass der Benutzer dem AP beim ersten Verbinden explizit vertraut, damit wird das Zertifikat des APs auf dem Client-Gerät gespeichert. Bei erneutem Verbinden wird das Zertifikat des APs mit dem bekannten Zertifikat verglichen. So wird sichergestellt, mit diesem AP bereits verbunden gewesen zu sein. Diese Funktionalität ist beispielsweise auch bei ssh umgesetzt. Durch diese Erweiterung des EAP-Protokolls, die auf dem häufig verwendeten Authentifizierungsverfahren TTLS basiert, und den Benutzer entscheiden lässt, ob der AP vertrauenswürdig ist, wird jeder Angriff, bei dem der Evil-Twin nicht beim ersten Verbinden mit dem Netzwerk aktiv ist, verhindert. Vor allem Netzwerke, mit denen häufiger eine Verbindung aufgebaut wird, werden so geschützt. Aber auch die Angreifbarkeit eines Benutzers der sich nur einmal mit dem Netzwerk verbindet, wird verringert, da ein Angriff, wie in Abschnitt 2 beschrieben, bei dem eine bestehende Verbindung unterbrochen wird, nicht mehr möglich ist. [8]

3.3.2 TLS/SSL in höheren Schichten

Vor dem Hintergrund, dass Nachrichten, die in das Internet gesendet werden, einen unbekannten Weg über zahlreiche Punkte, die den Netzwerkverkehr mitlesen und verändern können, nehmen, ist offensichtlich, dass kritische Daten immer verschlüsselt über das Internet übertragen werden sollten. Werden diese Daten aber bereits mit einem Verfahren, wie TLS übertragen, bei dem die Daten verschlüsselt werden und sich der Sender authentifiziert, ist ein Evil-Twin-AP keine Gefahr, da dieser weder Informationen mitlesen, noch Nachrichten verändern kann. Werden beispielsweise in einem öffentlichen Netzwerk nur Seiten aufgerufen, die über TLS/SSL gesichert sind, ist es für den Angreifer unmöglich

doi: 10.2313/NET-2014-08-1_19

die Nachrichten mitzulesen. Die Daten fließen zwar über den Evil-Twin-AP, aber der kann die verschlüsselten Daten nicht nutzen. Vor allem in öffentlichen WLAN-Netzen ist dies eine Methode, Mitleser auszuschließen. Um eine Verbindung über TLS zu ermöglichen, muss der Server, mit dem man sich verbinden möchte TLS unterstützen. Soll eine Verbindung zu einem Server aufgebaut werden, der kein TLS unterstützt, kann eine verschlüsselte VPN-Verbindung zu einem vertrauenswürdigen Proxy-Server aufgebaut werden. Von diesem Server werden die Nachrichten unverschlüsselt ins Internet gesendet, ohne dass ein Evil-Twin mitlesen kann.

3.4 Vergleich der Abwehrmöglichkeiten

Die Vorgestellten Abwehrmöglichkeiten von Evil-Twin-APs haben sehr verschiedene Eigenschaften. Entscheidende Dimensionen, die über den Erfolg der Abwehrmaßnahmen entscheiden, sind zum einen die Zuverlässigkeit der Maßnahme, außerdem ist die Einfachheit der Einführung einer Maßnahme entscheidend und zum dritten ist ein entscheidender Punkt, wie gut sich die Maßnahme auf große Netzwerke anwenden lässt.

3.4.1 Erkennungssicherheit/Zuverlässigkeit

Damit eine Angriffsabwehr sinnvoll ist, sollten möglichst alle Angriffe eines Evil-Twins erkannt werden. Die Abwehrstrategie sollte möglichst zuverlässig Evil-Twins erkennen und eine Verbindung mit ihnen verhindern.

Die Überwachung des Netzes auf Administratorseite ist nur möglich, wenn der Evil-Twin-AP in der Reichweite der Administrators aufgebaut wird. Ist der Angreifer nicht mit dem Netzwerk des Administrators verbunden, so hat dieser keine Chance den Angreifer anhand von Paketen im Netzwerk, wie in Abschnitt 3.1.2 beschrieben zu erkennen, da der Evil-Twin keine Pakete im Netzwerk sendet. Die Funküberwachung aus Abschnitt 3.1.1 erkennt Netzwerke, die im Bereich des Originalnetzes geöffnet werden, auch wenn keine Verbindung mit dem Originalnetz besteht. Allerdings hat sie keine Möglichkeit Angriffe zu verhindern, bei denen der AP an einem anderen Ort nachgebildet wird. Die administratorseitigen Ansätze können also vor allem das Netz und Daten im Netzwerk schützen. Da eine Verbindung vom Benutzer in ein anderes Netz nicht erkannt wird, können Benutzer nicht sicher geschützt werden. Ein weiterer Nachteil administratorseitiger Möglichkeiten ist, dass der Benutzer keinen Einblick auf die Arbeit des Administrators hat und nicht überprüfen kann welche Sicherheitsmaßnahmen dieser trifft und so nicht feststellen können, ob sich Netzwerk Evil-Twins befinden, die der Administrator nicht erkannte.

Die möglichen Maßnahmen der Clients erkennen auch nicht alle Angriffe sicher. Die Zeitmessung aus Abschnitt 3.2.1 baut auf die Annahme auf, dass der Evil-Twin über WLAN mit dem Original Netzwerk verbunden ist. Ist diese Voraussetzung nicht erfüllt, wird das Ergebnis des Algorithmus zum Erkennen des Evil-Twins sehr unzuverlässig, da beispielsweise eine schnellere Kabelverbindung die Dauer der Nachrichtenübertragung verkürzt. Die in Abschnitt 3.2.2 beschriebene Möglichkeit des Context Leashings bietet eine einfache Möglichkeit Evil-Twin Angriffe zu erschweren. Sie bieten zwar keinen absolut sicheren Schutz vor Angriffen, erschweren aber den Angriff vor allem an Orten, an denen andere oder keine WLAN-Netze vorhanden sind. Der Angreifer muss dann die Netz-Infrastruktur an dem Ort kennen, an dem das Gerät mit dem Netz verbunden war und diese Infrastruktur replizieren können. Wird eine Verbindung von Context Leashing auf Client-Seite und Funküberwachung auf Administratorseite angewendet, lässt sich ein relativ zuverlässiger Schutz vor Evil-Twin-Angriffen erreichen. Es gibt jedoch dann immer noch Möglichkeiten, wie erfolgreiche Evil-Twin Angriffe unternommen werden können, wenn beispielsweise der Evil-Twin die gesamte WLAN-Infrastruktur an anderer Stelle repliziert.

Durch ein Protokoll, das Trust-On-First-Use umsetzt (Abschnitt 3.3.1) lässt sich ein Angreifer am sichersten erkennen, vorausgesetzt es wurde bereits eine Verbindung aufgebaut und der Client kennt das Zertifikat des Netzes. Die einzige Möglichkeit, wie ein Evil-Twin nicht erkannt wird, ist dass er bereits bei der ersten Verbindung eine Kopie des APs präsentiert, mit der sich das Opfer verbindet. Bei der Verwendung von verschlüsselten Verbindungen in höheren Schichten als einzige Sicherheitsmaßnahme wird der Evil-Twin nicht erkannt. Der Angreifer, kann aber wegen der Verschlüsselung die gesendeten Nachrichten nicht lesen oder ändern. Wird jedoch nicht der gesamte Verkehr verschlüsselt, weil die Gegenstelle eine Verschlüsselung in höheren Schichten nicht unterstützt, kann der Evil-Twin die unverschlüsselte Nachricht mitlesen und so vertrauliche Daten erhalten.

3.4.2 Einfachheit der Umsetzung

Damit eine Abwehrmöglichkeit erfolgreich eingesetzt werden kann, ist es von Vorteil, wenn der Erfolg der Abwehrmaßnahme von möglichst wenigen abhängt. Der Vorteil der einseitigen Möglichkeiten zur Abwehr ist, dass die jeweils andere Seite keine Anpassungen durchführen muss, damit die Abwehr funktioniert. Eine Überwachung der Nachrichten im Netzwerk, wie in Abschnitt 3.1.2 ist relativ einfach, wenn sich die verbundenen Geräte nicht häufig ändern, es müssen nur die Adressen der berechtigten Geräte gespeichert und mit den Daten im Netzverkehr abgeglichen werden. Ändern sich allerdings die Clients häufig, wird der Aufwand die Liste der berechtigten Clients zu aktualisieren größer, so dass diese Abwehrmaßnahme unpraktikabel wird.

Das Überwachen des Funkverkehrs (Abschnitt 3.1.1) ist aufwändiger. Hier muss das Netzwerk entweder manuell überwacht werden, was wegen der häufigen Wiederholung im gesamten Netz sehr aufwendig ist, oder es müssen spezielle Geräte installiert und gewartet werden, die dies automatisch durchführen. Der größte Aufwand ist in diesem Fall die Installation und Einrichtung.

Die Möglichkeiten auf der Clientseite sind einfach in der Umsetzung. Die Zeitmessung in einem Netzwerk aus Abschnitt 3.2.1 kann unabhängig von der Verbindung als eigenständiges Programm umgesetzt werden, das Nachrichten ins Netzwerk sendet und die Zeit bis zur Antwort misst, und ist somit einfach in eine Netzwerkinfrastruktur zu integrieren. Ein Programm, das Context Leashing betreibt, benötigt, wie in Abschnitt 3.2.2 beschrieben, Informationen über vorhandene Netze und Empfangsstärke,das es einfach bekommen kann. Da aber keine zweite Seite involviert ist, ist die Umsetzung auch hier auch einfach möglich.

Möglichkeiten, die auf eine Änderung des Protokolls aufbau-

en sind schwieriger umzusetzen, da beide Seiten die Neuerungen unterstützen müssen. Eine Erweiterung des EAP-Protokolls aus Abschnitt 3.3.1 muss von den Servern auf der Netzseite und von dem mobilen Gerät umgesetzt sein, um zu funktionieren. Da aber viele Hersteller von Hardware und Software beteiligt sind, gestaltet sich eine Einführung schwierig.

Auch für die Verwendung von Verschlüsselung in höheren Schichten muss diese von beiden Seiten unterstützt werden. Da aber heute TLS weit verbreitet ist alle mobilen Geräte über eine Implementierung von TLS verfügen, und auch Open-Source-Software für Server vorhanden und weit verbreitet ist, ist die in Abschnitt 3.3.2 beschriebene Verschlüsselung einfach umzusetzen.

3.4.3 Automatisierbarkeit und Skalierbarkeit

Damit die Abwehr von Evil-Twins erfolgreich ist, muss sie ständig und mit wenig manuellem Eingreifen durchführbar sein. Nur so können Fehler der Benutzer, die zu erfolgreichen Angriffen führen, verhindert werden.

Das Mitlesen und Auswerten von Nachrichten auf Administratrorseite aus Abschnitt 3.1.2 ist automatisch möglich. Da jedoch manuelle Einträge für jedes Gerät im Netz notwendig sind, ist diese Methode schlecht skalierbar.

Der manuelle Aufwand für eine Funküberwachung aus Abschnitt 3.1.1 ist groß, falls das Netz manuell mit einem mobilen Gerät abgesucht wird. Er beschränkt sich auf das aktualisieren der erlaubten Netze, falls für den ganzen Bereich des Netzes fest installierte Messgeräte aktiv sind, die die Funkfrequenzen überwachen, und so fremde Netze finden. In diesem Fall werden für größere Netze mehr Messgeräte benötigt, wodurch die Kosten für größere Netze steigen.

Durch das automatische Starten der Programme zum Erkennen von Evil-Twins lassen sich clientseitige Maßnahmen gut automatisieren. Da für die Messung der Antwortzeit die Netzgröße unerheblich ist, ist die Skalierbarkeit für die Methode aus Abschnitt 3.2.1 gut.

Auch das Context Leashing aus Abschnitt 3.2.2 kann unabhängig von der Größe des Netzes durchgeführt werden. Ein Problem könnte dabei sein, dass große Netze viele Nachbarnetze haben und somit das richtige Netz oft für einen Evil-Twin gehalten wird. Da hier manuelles Abschätzen des Risikos notwendig ist, hat in diesem Fall die Automatisierung Grenzen.

Wird das Protokoll zum Schutz vor Evil-Twins angepasst, wie in Abschnitt 3.3.1, spielt die Größe des Netzes keine Rolle, die manuellen Eingriffe beschränken sich auf das Bestätigen des Vertrauens zum Netz.

Bei der Verwendung von TLS, wie in Abschnitt 3.3.2 beschrieben, sind keine Eingriffe in das Netzwerk nötig. Die Größe des Netzwerks spielt deshalb keine Rolle.

4. ZUSAMMENFASSUNG

In dieser Arbeit wurde das Aufbauen eines Evil-Twin-AP gezeigt. Es wird deutlich, dass der Angriff mit wenigen frei verfügbaren Tools in kurzer Zeit durchgeführt werden kann. Die Ziele des Angriffs können vielfältig sein. Der Angriff kann genutzt werden, um Nachrichten des Opfers mitzulesen und zu verändern. Durch das Betreiben eines DNS-Servers kann das Opfer auf Phishingseiten umgeleitet werden, auf denen es ungewollt Passwörter preisgibt. Vor diesem Angriff schützt keine Verschlüsselungsart völlig zuverlässig. Nicht nur unverschlüsselte und WEP oder WPA/WPA2 verschlüsselte Netzwerke mit gemeinsamen Schlüssel können kopiert werden, auch Netzwerke die WPA2 Enterprise nutzen, können mit entsprechendem Aufwand kopiert werden. Zum Verhindern der Evil-Twins gibt es Ansätze auf Administratorseite, Benutzerseite und Ansätze, die das Protokoll der Authentifizierung so verändern, dass Evil-Twins erkannt werden. Der Administrator kann durch Überwachen der Nachrichten im Netz unbekannte Geräte erkennen, und sie stoppen, oder durch Überwachung des Funkverkehrs unberechtigte Accesspoints erkennen. Der Client kann aus der Dauer der Nachrichtenübertragung Rückschlüsse auf die Echtheit des APs ziehen. Durch Beobachten der umgebenden Netzinfrastruktur kann der Client seinen Standort abschätzen und so eine Verbindung zum Accesspoint nur am richtigen Ort aufbauen, wodurch der Angriff an anderer Stelle vermieden wird. Die Ansätze haben unterschiedliche Einsatzbereiche. Maßnahmen, die nur von Benutzer oder Administratoren durchgeführt werden, können die Angriffe nicht verhindern, sie erschweren diese allerdings. Vor allem das Context Leashing auf der Clientseite und die Funküberwachung durch den Administrator sind wirkungsvolle Maßnahmen, die gemeinsam angewendet Angriffe deutlich erschweren. Durch Erweiterung des EAP-Protokolls um Trust-On-First-Use wird die Möglichkeit eines Evil-Twin-Angriffs in WPA2-Netzwerken weiter verringert. Weil aber eine Verschlüsselung der Daten in höheren Schichten heute bereits sehr weit verbreitet ist und weiter zunimmt, verliert der Evil-Twin-Angriff an Relevanz, da durch die Verwendung von TLS das Mithören und Verändern der Nachrichten verhindert wird und das nicht nur im lokalen Netzwerk, sondern sondern auch durch das gesamte Internet bis zum Empfänger der Nachricht. Dann kann man auch im Cafe das öffentliche WLAN nutzen, ohne Angst haben zu müssen, abgehört zu werden.

5. LITERATUR

[1] *Aircrack-ng Home Page*, `http://www.aircrack-ng.org/`

[2] *ISC DHCP SERVER*, `http://www.isc.org/downloads/dhcp/`

[3] *ngrep - network grep*, `http://ngrep.sourceforge.net/`

[4] *ISC BIND DNS SERVER*, `http://www.isc.org/downloads/bind/`

[5] *man pages of iptables*, `http://ipset.netfilter.org/iptables.man.html`

[6] Airdefence, *TIRED OF ROGUES? Solutions for Detecting and Eliminating Rogue Wireless Networks*, White paper, `http://goo.gl/uuZBEH`

[7] Y. Song and C. Yang and G. Gu: *Who Is Peeping at Your Passwords at Starbucks? – To Catch an Evil Twin Access Point*, In Proceedings of the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'10), Juni 2010

[8] H. Gonzales, K. Bauer, J. Lindqvist, D. McCoy, D. Sicker: *Practical Defenses for Evil Twin Attacks in*

802.11, In IEEE Globecom Communications and Information Security Symposium, Miami, FL, Dezember 2010

[9] *Video Tutorial zum Aufbau eines Evil-Twin-Angriffs* `http://vimeo.com/34309678`

[10] Wright, J. Antoniewicz, B.*PEAP Shmoocon 2008* `http://goo.gl/VZoyks`

[11] Antoniewicz, B. *802.11 Attacks*, 2010

doi: 10.2313/NET-2014-08-1_19