Rischi per l'utente finale durante le connessioni a Wi-Fi pubbliche non cifrate

Andrea Lora

CNR-Istituto di Cristallografia - Area della Ricerca Roma 1

Abstract. Connettersi ad una rete wireless 802.11 non protetta espone il client finale ad alcuni attacchi. Alcuni di questi sono di tipo Denial of Service, altri, più complessi, sono finalizzati alla sottrazione di credenziali di accesso, all'acquisizione di dati personali o all'elusione delle tecnologie di sicurezza che la rete offre. Verranno analizzati alcuni di questi attacchi al fine di aumentare la consapevolezza sull'utilizzo delle Wi-Fi pubbliche concentrandosi in particolare sull'interazione Wi-Fi pubblica e captive portal di autenticazione.

1. Introduzione

L'implementazione attuale delle reti metropolitane e regionali Wi-Fi di tipo pubblico si basa su tecnologia di tipo 802.11 b/g/n ad accesso non protetto (assenza di crittografia WEP o WPA) con l'ausilio di Captive Portal per l'autenticazione. Il client si connette ad un SSID annunciato (ad es. provinciawifi), riceve un indirizzo IP dal DHCP locale, e viene messo in "client isolation". Successivamente qualsiasi richiesta di tipo HTTP prevede il reindirizzamento ad un Captive Portal che richiede le credenziali di accesso al sistema o la registrazione ad esso. Qualunque altra richiesta verso porta non standard viene silenziosamente scartata. A seguito di immissione di credenziali corrette l'IP del client viene sbloccato e viene consentito l'accesso verso internet. Questo tipo di approccio si presta ad una serie di attacchi, verranno dunque illustrati quelli che coinvolgono il client finale.

2.Attacchi DOS

Gli attacchi di tipo Denial of Service su questo tipo di rete sono quelli comuni a 802.11.

Il Wi-Fi Jamming prevede l'occupazione del canale radio dove opera l'AP che viene riempito (flooding) con traffico dati, limitando la capacità di fornire il servizio. A causa dell'utilizzo del protocollo CSMA/CA da parte di 802.11, i client o l'access point si vedrebbero deteriorare o completamente annullare le capacità di trasmissione. L'attacco può avvenire sia sul layer PHY che sul MAC.

Il DeAuth Attack invia pacchetti contraffatti (spoofed) che forzano il client a scollegarsi dall'access point. Le tecniche che comportano la perdita di connessione sono molteplici, ma tutte si basano sulla possibilità di un dispositivo terzo di inviare un pacchetto spoofed, spacciandosi per un altro dispositivo. Alcuni pacchetti di servizio, tipici di 802.11, sono in grado di disassociare o deautenticare il client dall'access point. Contraffacendo un pacchetto appositamente forgiato si è quindi in grado di ottenere la disconnessione. Sono stati proposti dei workaround a questo problema che non colpisce solo le reti non crittografate, ma anche quelle protette da WPA e WEP. I pacchetti di servizio nello standard 802.11, infatti, non si avvalgono mai di crittografia se non nel futuro standard 802.11w, che aggiungerà un valore di hash a tutti i frame di management.

L'Authentication Flood invia un elevato numero di richieste contraffatte di autenticazione verso l'access point, mirando all'esaurimento delle sue risorse. Potendo contare sullo spoofing dei pacchetti, un attaccante è in grado di generare centinaia di richieste di associazione all'access point che potrebbero andare a saturare la memoria del dispositivo, inibendo la possibilità di accettare nuove associazioni (nel migliore dei casi) o un suo malfunzionamento che impedisce di comunicare anche con i client già associati.
Il DHCP Starvation opera a layer più elevato, invia numerose richieste DHCP e tenta di esauri-

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

re il pool di IP assegnabili. La tecnologia di autenticazione con Captive Portal necessita che il client abbia uno stack IP completamente funzionante per potersi autenticare. Da qui la necessità che sulla rete ci sia un DHCP che assegna gli IP non appena la connessione è stabilita. Anche in questo caso l'attaccante può contare sullo spoofing e saturare una subnet /24 in pochissimo tempo. A seconda della topologia della rete questo attacco può ripercuotersi su Access Point fisicamente distanti da quello attaccato ma che ne condividono la rete.

2. Client Isolation

Una parte della sicurezza delle reti aperte è affidata alla capacità di alcuni Access Point che consentono di attivare il cosiddetto Client Isolation (il nome varia a seconda del vendor), una feature atta ad impedire lo scambio di dati tra client collegati allo stesso AP, di fatto inibendo la possibilità di stabilire le comunicazioni tra client. Ciò è possibile poiché le specifiche 802.11 prevedono che a seguito di una connessione ad una rete managed (non ad hoc) i client possano trasmettere e ricevere dati solamente con l'Access Point.

L'implementazione per raggiungere questo scopo consiste nell'inibire il trasporto di pacchetti che devono raggiungere il dominio di broadcast locale non aventi target mac address autorizzati. In una rete composta da un access point e due client l'ARP request inviata dal Client 1 per richiedere l'indirizzo Ethernet dell'IP a cui è associato il Client 2 viene silenziosamente scartata. Il Client 2 non riceverà mai la richiesta ARP e non potrà inviare dunque risposta. Anche in presenza di ARP table con entry statiche la client isolation continua a impedire la comunicazione tra i client. I client non sono mai consapevoli di essere in client isolation poiché è una feature dell'AP e gestita interamente da lui.

Considerato che il traffico tra il Client 1 e l'AP viaggia su etere è possibile per un attaccante intercettarlo e fingendosi l'AP, trasmettere l'informazione al Client 2, che a sua volta risponderà alla richiesta. L'informazione giungerà sia all'AP legale, che la scarterà a causa della client isolation, sia all'attaccante, che di nuovo si fingerà l'AP e trasmetterà l'informazione al Client 1. In questo modo la client isolation viene sconfitta.

L'implementazione di un anti client isolation è possibile tramite Airtun-ng della suite aircrack-ng. Esso permette di creare un'interfaccia virtuale nel sistema linux adatta sia al ricevimento di tutti i dati trasmessi da un certo BSSID, sia all'invio di pacchetti, siano essi inviati dallo stack normale TCP/IP, sia contraffatti (crafted) attraverso librerie netfilter. È stata concepita una proof of concept basata su scapy che agisce da relay di pacchetti appartenenti allo stesso dominio di broadcast. Il risultato è che la client isolation viene elusa fintanto che i client siano in range, oltre che dell'AP legale, del dispositivo che si occupa del relaying. A causa della bassa qualità dei componenti utilizzati per la PoC la velocità di trasferimento è molto ridotta, ma è possibile per esempio inviare pacchetti ICMP ping e ricevere la risposta tra Client 1 e Client 2 in presenza di Client Isolation. Poter eludere la client isolation ha come conseguenza la possibilità di eseguire ARP poisoning sulla rete, e quindi attacchi man in the middle (MITM).

3. Rogue Access Point

I Rogue Access Points sono l'altra minaccia per l'utente finale. Un RAP è un access point che annuncia un SSID noto (come ad esempio provinciawifi) ma è sotto il controllo di un attaccante. Si tenga presente che la gestione del Wi-Fi del sistema operativo del client esegue numerose operazioni in maniera trasparente per l'utente. Per esempio in mancanza di connessione si collega automaticamente ad un ESSID conosciuto, o si scollega da un AP e si collega ad un RAP se quest'ultimo offre un segnale molto migliore o se viene forzata una disconnessione dall'AP iniziale tramite un DeAuth attack. Una volta collegato ad un RAP l'utente finale è alla mercé dell'attaccante, poiché esso agisce da router ed è quindi in grado di intercettare le richieste e di mettere in atto attacchi di tipo MITM.

4. Attacchi MITM

Gli attacchi di tipo Man in the middle comporta-

no un certo grado di information disclosure. Gli attacchi prendono questo nome dal fatto che le comunicazioni tra client e server vengono intercettate da un attaccante che si pone in mezzo ed esegue operazioni di intercettazione (sniffing) o manipolazione di pacchetti. Affinché un attacco MITM possa essere effettuato l'attaccante deve in qualche modo poter frapporsi tra il client e il server in modo da poter controllare le connessioni. Questo vuol dire che precedentemente deve essere stato eseguito un ARP poisoning o il client bersaglio deve essere collegato ad un RAP sotto controllo dell'attaccante.

Un attacco di tipo MITM su una connessione in chiaro (http/smtp/pop/telnet) è completamente trasparente all'utente finale, mentre è rilevabile nel caso di connessioni SSL. Nelle connessioni SSL, infatti, è presente un certificato legato al nome a dominio che garantisce la sicurezza della connessione end-to-end. In caso di certificato contraffatto viene presentato un messaggio non facilmente ignorabile da parte dell'utente, se non altro nelle sessioni HTTPS.

5. SSLSTRIP

Più pericolosi per l'utente finale sono gli attacchi basati su sslstrip, un tool che in condizioni specifiche consente di evitare l'instaurarsi di connessioni HTTPS e di trasformarle in semplici HTTP, permettendo quindi di intercettare il traffico che passa in plain text. Per comprendere il funzionamento di sslstrip bisogna tenere presente come viene stabilita una connessione HTTPS.

In generale la connessione ad un server in HTTPS non avviene attraverso la scrittura diretta nella barra di indirizzi del browser, non si chiede quindi https://example.com

Quello che accade invece è che si giunga a https://example.com tramite:

a) Un link presente in una pagina di tipo http: <a href="https://example.com">

b) Un codice di reindirizzamento HTTP 302 che fa transitare da http://example.com a https://example.com

Se un attaccante ha predisposto un MITM attack può modificare i dati trasmessi, e trasformare l'href del caso a in un semplice <a href="http://example.com">. Lo stesso meccanismo permette di trasformare il codice di reindirizzamento e impedire che ci si sposti in HTTPS.

Un client che richiede una pagina web ad un server remoto mentre SSLSTRIP agisce da transparent proxy non troverà mai link HTTPS all'interno delle pagine, né accadrà mai che possa transitare in HTTPS tramite un codice 302. Al suo interno SSLSTRIP tiene una mappa delle richieste fatte dal client in maniera da poter eseguire le richieste HTTPS invece del client legittimo e di fornire le risposte corrette al client.

CLIENT <-----> http <-----> SSLSNIFF <-----> https <-----> LegitServer

Sslstrip, usato a seguito di altri attacchi rappresenta uno dei tool più insidiosi per catturare credenziali. Questo perché l'utente finale non è informato del fatto che la connessione su cui transitano le informazioni usa un certificato non valido, semplicemente transita tramite http.

6. HSTS

L'HTTP Strict Transport Security (HSTS) doveva essere la risposta ad attacchi di tipo sslstrip. HSTS permetteva di registrare nei browser informazioni riguardanti nomi a dominio che dovevano essere interrogati via HTTPS, e solo tramite esso, impedendo quindi che sslstrip potesse portare a termine l'attacco. Se l'utente richiede un sito per cui è presente un record HSTS il browser procede automaticamente ad un reindirizzamento interno (http code 307) e contatta il server remoto direttamente in HTTPS. I browser hanno una lista precompilata con i siti protetti da HSTS, ma è possibile per un server informare il client di aggiornare la lista HSTS con il proprio sito tramite un header particolare:

Strict-Transport-Security: max-age=expireTime [; includeSubdomains]

7. SSLSTRIP+

Al BlackHat Asia 2014 Leonardo Nve Egea ha presentato un fork di sslstrip che consente di inibire il funzionamento di HSTS in determinate condizioni. È impossibile impedire ad un browser di eseguire il reindirizzamento interno nel caso si scriva nella barra di indirizzi una url di cui è pre-

sente il record HSTS, ma è possibile modificare le pagine web http che contengono link protetti non solo strippando la parte sicura di HTTPS, ma anche modificandone il nome a dominio in qualcosa di simile (in maniera da non allarmare l'utente) ma comunque diverso dall'originale (impedendo quindi che venga riconosciuto dal browser come qualcosa per cui è presente un record HSTS). Per esempio nel tool di Nve il dominio google.com diventa gooogle.com.

8. Certificati Root Installati

Un'altra problematica per i client è quella che deriva dall'installazione nel proprio sistema operativo di un certificato root di proprietà dell'attaccante. Difficilmente gli utilizzatori finali sono a conoscenza di cosa sia questo tipo di certificato o di quali pericoli si corrano ad installarlo.

Se l'attaccante è in grado di eseguire un attacco MITM e riesce a convincere il client ad installare un proprio certificato root, sarà in grado di agire da transparent proxy direttamente via HTTPS, mostrando la famosa "chiave verde" all'interno dell'indirizzo, impedendo all'utilizzatore finale di capire di aver subito un attacco. SSLsniff esegue questo tipo di attacco.

9. Captive Portal

I Captive Portal sono un caso molto svantaggiato in questo contesto. Non possono essere protetti da HSTS in maniera preventiva, perché un attaccante può modificare il nome a dominio e sono, quindi, soggetti ad attacchi di tipo MITM, mettendo a repentaglio le credenziali di accesso. Combinando più attacchi si creano scenari complessi e in grado di ottenere le credenziali di accesso a reti anche ritenute più sicure, come ad esempio IDEM-Wifi, senza insospettire l'utente finale.

Sebbene l'utilizzo stock di sslstrip di primo acchito mostri l'inefficacia dell'attacco nei confronti dei sistemi di Single Sign On offerti da Shibboleth l'analisi delle risposte e le opportune modifiche ad sslstrip rendono possibile l'autenticazione dei client agli IdP basati su shibboleth e la cattura dei dati di autenticazione.

10. Conclusioni

Gli attacchi sopra descritti sono stati possibili perché prendevano di mira le due debolezze delle reti Wi-Fi aperte. Da una parte veniva sfruttato il fatto che la trasmissione dei dati avvenisse in chiaro: questo permetteva di utilizzare tecniche di anti isolation. Dall'altra si abusava del fatto che uno SSID da solo non garantisse l'identità dell'AP. 802.1x può essere la soluzione ai problemi di tipo client attack. Lo standard, già utilizzato ampiamente in ambito enterprise e colonna portante della rete eduroam, prevede l'utilizzo di chiavi private tra Access Point e Client che impedisce l'elusione della client isolation, e una forte crittografia in fase di autenticazione. Il baco classificato come Hole 196, per cui il traffico broadcast viene codificato con una chiave condivisa (GTK) tra i client potrebbe essere di qualche entità nel caso non fosse abilitata la client isolation. Ma in presenza di questa feature 802.1x si rivela our best bet per proteggere i client dagli attacchi di tipo MITM.

Riferimenti bibliografici

[1] http://www.thoughtcrime.org/software/sslstrip
[2] http://www.slideshare.net/Fatuo__/offensive-exploiting-dns-servers-changes-blackhat-asia-2014
[3] http://youtu.be/pAtup7n1BlI

Andrea Lora
andrea.lora@cnr.it

Lavora come system engineer presso il CNR all'Istituto di Cristallografia presso l'Area della ricerca di Montelibretti (RM1) in forza al Servizio Reti. Si occupa di virtualizzazione e storage, implementazione, amministrazione e monitoring di servizi e di network security. Attualmente è impegnato nell'implementazione di IPv6 nella rete dell'Area e nel miglioramento delle operazioni interne