UNIVERSITÀ
DEGLI STUDI
DELL'AQUILA

Dipartimento di Ingegneria e Scienze
dell'Informazione e Matematica

Università degli Studi dell'Aquila

Attacchi Wifi: Bypassare la cifratura Wi-Fi manipolando le Transmit Queues

Matteo Capricci, 288602

Indice

Indice **i**

1 Code di trasmissione degli access point Wi-Fi **1**
1.1 Security Context nelle reti Wi-Fi 1
1.2 Meccanismi di risparmio energetico Wi-Fi 2
1.2.1 Frame Queuing sullo Stack Wi-Fi 2
1.3 Wi-Fi Management Frame Protection (MFP) 2
1.3.1 Utilizzo della MFP 3

2 Vulnerabilità delle code di trasmissione e loro sfruttamento **4**
2.1 Leaking di Frame dalla Coda Wi-Fi 4
2.1.1 Threat Model 5
2.1.2 Strategia Generale di Attacco e Metodologia 5
2.1.2.1 Strategia di Attacco 5
2.1.2.2 Implementazione dell'Attacco 6
2.1.3 Exploining dell'attacco 6
2.1.3.1 Leak di Frame in FreeBSD 7
2.1.3.2 Attuazione dell'Attacco 7
2.1.3.3 Leak di Frame in Linux 7
2.1.3.4 Attuazione dell'Attacco 8
2.1.4 Difese 8
2.2 Sfruttamento della Coda per Interruzioni di Rete 9
2.2.1 Coda delle Richieste SA Query 9
2.2.2 Coda dei Messaggi di 4-Way Handshake 9
2.2.3 Outline dell'Attacco 9
2.3 Sovrascrittura del Contesto di Sicurezza 10
2.3.1 Descrizione dell'Attacco 11
2.3.2 Difese 12

3 Conclusioni **13**

CAPITOLO 1

Code di trasmissione degli access point Wi-Fi

Una coda di trasmissione, nel contesto degli access point Wi-Fi, è un meccanismo che gestisce l'invio dei pacchetti dalla rete locale (LAN) ai dispositivi wireless connessi. L'access point dispone di una coda di trasmissione per ogni dispositivo connesso.

Per decidere l'ordine di invio ai dispositivi connessi, tenendo conto di fattori come la larghezza di banda disponibile, il carico di rete, la qualità del segnale e le priorità dei pacchetti, la coda di trasmissione aiuta a regolare il flusso dei dati tra l'access point e i dispositivi wireless, per garantire una trasmissione efficiente e senza congestionamenti.

Il suo utilizzo è un elemento essenziale per gestire in modo ottimale il traffico di rete e garantire una connessione wireless stabile e affidabile per tutti i dispositivi connessi.

In alcuni casi, questo meccanismo può essere manipolato con scopi malevoli per bypassare la crittografia utilizzata o causare disservizi della rete.

Prima di presentare tali problematiche si devono introdurre alcuni concetti fondamentali per la comprensione delle vulnerabilità e delle minacce che queste comportano.

1.1 Security Context nelle reti Wi-Fi

Il "Security Context" (contesto di sicurezza) è quell'insieme di informazioni e impostazioni di sicurezza associate a una connessione tra un access point (AP) e un dispositivo client; questo comprende diversi elementi che definiscono come la connessione viene autenticata, crittografata e protetta da attacchi.

Nel contesto delle reti Wi-Fi, i dispositivi possono avere l'esigenza di bufferizzare, cioè mettere nelle trasmitting queue, i pacchetti prima della loro trasmissione. Tuttavia, la gestione del *security context* dei frame messi in coda è un aspetto critico di questa tecnologia.

Gli standard Wi-Fi, come l'802.11, non forniscono linee guida esplicite sulla gestione dei contesti di sicurezza dei frame bufferizzati. La gestione inadeguata dei security context può influire sulla protezione dei dati trasmessi.

1.2 Meccanismi di risparmio energetico Wi-Fi

I meccanismi di risparmio energetico fanno parte dello standard IEEE 802.11 sin dal suo primo rilascio nel 1997. Con l'introduzione dell'emendamento IEEE 802.11e, che definisce miglioramenti della qualità del servizio per le reti LAN wireless, lo standard ha adottato meccanismi di risparmio energetico più avanzati.

1.2.1 Frame Queuing sullo Stack Wi-Fi

Analizzando nello specifico quando e dove i frame vengono messi in coda, vediamo che, come illustrato in Figura 1.1, avviene uno scambio tipico di messaggi di risparmio energetico tra un client e un access point. In qualsiasi momento durante la connessione, il client può indicare che entrerà in modalità di risparmio energetico tramite uno specifico bit nel formato del frame dell'intestazione IEEE 802.11. A questo punto, quando l'access point riceve i frame da trasmettere al client, viene eseguita un'operazione di equeuing nella coda di trasmissione del kernel fino a quando il client si "sveglia", eseguendo un'operazione di Wake-Up, o la durata del frame scade, ovvero finisce il tempo massimo in cui un frame può restare in coda.

1.3 Wi-Fi Management Frame Protection (MFP)

La Protezione dei Frame di Gestione Wi-Fi (MFP) standardizza meccanismi di protezione per i frame di gestione, garantendo confidenzialità, integrità, autenticità dell'origine e protezione dalla riproduzione dei dati. La MFP Wi-Fi è definita nell'emendamento 802.11w e incorporata nella versione 2012 dello standard di base 802.11.

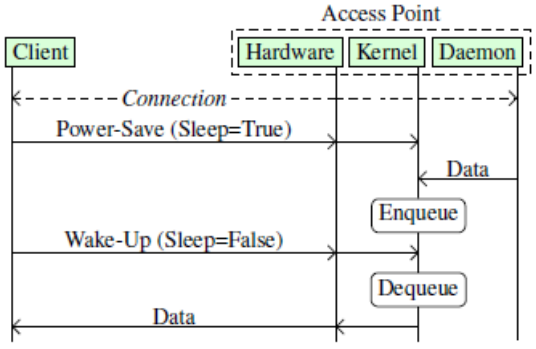

Figura 1.1: Power-saving mechanisms.

1.3.1 Utilizzo della MFP

Quando la MFP Wi-Fi viene utilizzata tra due stazioni compatibili, gli association e disassociation frame sono protetti tramite la Security Association (SA) corrente. L'Associazione di Sicurezza viene memorizzata da ciascuna delle parti coinvolte nell'associazione. Quando una stazione ha un'associazione di sicurezza esistente, ogni frame di associazione viene temporaneamente respinto dall'AP per prevenire attacchi di *denial-of-service*. Successivamente, l'access point avvierà la procedura di SA Query per determinare se il client ha ancora un'associazione di sicurezza attiva con se stesso. In una procedura di SA Query, le stazioni scambiano una richiesta e una risposta, entrambe protette. Se la procedura ha successo, si determina che l'associazione di sicurezza sia ancora valida e le stazioni possono continuare a utilizzare l'associazione in modo sicuro. Di conseguenza, i frame di associazione non protetti possono essere scartati in modo sicuro. Se la procedura fallisce o scade il timeout, potrebbe esserci una discrepanza nell'associazione (ad esempio, a causa di un riavvio imprevisto della stazione client) e quindi l'associazione di sicurezza viene interrotta.

CAPITOLO 2

Vulnerabilità delle code di trasmissione e loro sfruttamento

In questo capitolo si tratteranno le vulnerabilità delle **Transmit Queues** ed i possibili exploiting per lanciare ed eseguire attacchi. In particolare si analizzeranno i seguenti tre attacchi:

- Leaking di Frame dalla Coda Wi-Fi
- Abuso della Coda per Interruzioni di Rete
- Sovrascrittura del Contesto di Sicurezza

2.1 Leaking di Frame dalla Coda Wi-Fi

In presenza di dispositivi Wi-Fi, non è sempre possibile trasmettere istantaneamente i pacchetti provenienti dal livello superiore e, spesso, i frame vengono messi in coda prima della trasmissione. Ciò può avvenire quando il ricevitore è in modalità di risparmio energetico o quando i frame non sono ancora in attesa di ackonwladgement e potrebbero quindi richiedere una ritrasmissione.

Analizzando gli standard 802.11, si è constatato che questi forniscono solo indicazioni **indirette** riguardo la gestione dei frame in coda da parte di un trasmettitore, non indicata nessuna specifica per il mittente nel caso nel caso in cui il *security context* cambi tra il momento in cui un frame viene messo in coda e il momento in cui viene effettivamente ritrasmesso.

Benché sia menzionata una funzione di **aging** per eliminare i frame che attendono in coda per un tempo eccessivo, non viene definito con precisione il comportamento di tale funzione; si legge che *"La specifica esatta della funzione di aging è oltre lo scopo di questo standard"*.

Nonostante siano presenti specifiche di servizio che garantiscono che una stazione **non debba inviare frame in chiaro dopo l'attivazione della crittografia**, non sono state trovate istruzioni esplicite su come gestire i cambiamenti nei security context né su come i frame in coda debbano essere rimossi o temporaneamente conservati quando un

dispositivo si disconnette o si riconnette alla rete. Al fine di analizzare l'implementazione pratica di questi casi limite, sono stati esaminati sistemi operativi e firmware open-source.

2.1.1 Threat Model

Si consideri un attaccante il cui obiettivo è rivelare i frame provenienti dall'access point e destinati a un client vittima; questo è in grado di iniettare/intercettare i frame e manipolare il security context del client, ad esempio tramite l'iniezione di frame di gestione non protetti come i frame di autenticazione e associazione. Inoltre, l'attaccante può alterare lo stato di risparmio energetico del client vittima mediante l'iniezione di frame che utilizzano il bit di risparmio energetico. Tipicamente, l'attaccante non ha bisogno di conoscere le credenziali di rete e quindi costituisce una minaccia esterna. Tuttavia, in determinate condizioni, i frame rivelati possono essere protetti dalla group key di rete.

2.1.2 Strategia Generale di Attacco e Metodologia

La strategia di attacco di base dietro il leak di frame dalla coda di trasmissione si basa sull'osservazione che la maggior parte degli stack Wi-Fi non rimuove o svuota adeguatamente le proprie code di trasmissione quando il contesto di sicurezza cambia. Come attaccante, si può sfruttare questo comportamento eseguendo uno spoofing di determinati frame di gestione utilizzando l'indirizzo MAC di un client vittima, interferendo in modo intelligente nel security context e nel meccanismo di risparmio energetico.

2.1.2.1 Strategia di Attacco

Si consideri un client che è connesso ad un access point con supporto alla modalità *power saving*. Nella Figura 2.1, viene illustrato come un attaccante può ingannare un access point vulnerabile per rivelare i frame destinati al client vittima dalle sue code di trasmissione.

L'attaccante spoofa un frame di risparmio energetico non protetto per ingannare l'access point portandolo a credere che il client vittima stia entrando in modalità di risparmio energetico. Di conseguenza, l'access point mette in coda tutti i frame per il client fino a quando questo indica di essere uscito dalla modalità di risparmio energetico. È importante notare che, in questa fase, tutti i frame sono messi in coda **in chiaro**. L'attaccante cerca ora di ingannare l'access point per rimuovere la pairwise key. In generale i frame di gestione, come le richieste di autenticazione e riassociazione, inducono l'access point a aggiornare il security context. Se l'attacco ha successo, l'access point non avrà più accesso a una pairwise key per il client vittima. A questo punto l'attaccante spoofa un frame di wake-up non protetto per indurre l'access point a trasmettere tutti i frame messi in coda per il client. Poiché l'access point vulnerabile non dispone più di una pairwise key per il client, potrebbe decidere di utilizzare la trasmissione in chiaro o

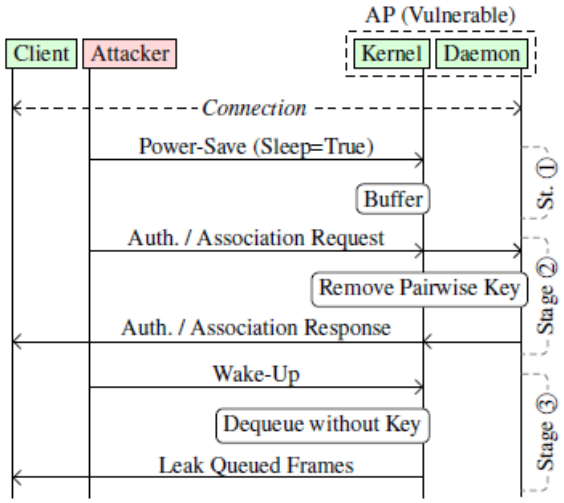

Figura 2.1: Leak nei confronti di un AP vulnerabile.

di utilizzare la group-addressed encryption key. A seguito dell'attacco, chiunque si trovi nel raggio di comunicazione dell'access point vulnerabile può intercettare i frame rivelati in chiaro o cifrati utilizzando la chiave di crittografia indirizzata al gruppo, a seconda dell'implementazione specifica dello stack.

2.1.2.2 Implementazione dell'Attacco

Al fine di verificare se un simile attacco sia fattibile in pratica, sono state analizzate implementazioni di code di trasmissione open-source. Ciò ha rivelato vari comportamenti, specifici dell'implementazione, che devono essere presi in considerazione per eseguire con successo l'attacco. Ad esempio, il tipo di frame utilizzato nella fase 2 per rimuovere la pairwise key dipende dall'implementazione presa di mira. Inoltre, il frame può essere rivelato in chiaro, può essere cifrato utilizzando una chiave composta da zeri (all-zero key), può presentare un'intestazione di crittografia apparentemente valida pur avendo un contenuto in chiaro, può essere erroneamente cifrato utilizzando WEP, e così via. Ciò comporta diverse applicazioni della strategia di attacco.

2.1.3 Exploining dell'attacco

Sono stati valutati e discussi attacchi verso sistemi operativi open-source in access point con supporto alla power saving mode. In particolare, verranno valutati FreeBSD 13.0 e 13.1, Linux 5.5.0 fino a 5.17.6.

2.1.3.1 Leak di Frame in FreeBSD

Per iniziare, si va ad esaminare se l' attacco è fattibile contro gli access point che operano su FreeBSD 13.0 e 13.1. Per comprendere appieno lo stack di rete e il suo comportamento, si vanno ad analizzare il codice del kernel e i driver specifici del produttore e si rivelano due problemi principali che devono essere presi in considerazione:

1. I driver sono spesso programmati per richiamare le funzioni predefinite nel kernel di FreeBSD. Ad esempio, la funzione "ieee80211_crypto_get_txkey()" viene utilizzata per selezionare la chiave crittografica. È interessante notare che questa funzione ricorrerà alla chiave di group-addressed encryption key se non è disponibile alcuna pairwise key. Un attaccante può sfruttare questo comportamento per costringere l'access point vulnerabile a crittografare i frame messi in coda utilizzando la chiave di crittografia del gruppo.

2. I dispositivi moderni sono spesso in grado di eseguire operazioni di crittografia in hardware, inclusa la selezione delle chiavi. Sebbene le implementazioni specifiche non siano disponibili, si riscontra che i dispositivi con crittografia hardware possono ricadere sulla trasmissione in chiaro o su una chiave di crittografia composta da zeri.

2.1.3.2 Attuazione dell'Attacco

L'attacco risultante contro gli access point di FreeBSD segue da vicino la strategia di attacco descritta nella sezione precedente e illustrata nella Figura 2.1. In particolare, l'attaccante deve utilizzare una richiesta di riassegnazione per ingannare l'access point vulnerabile affinché rimuova la chiave pairwise del client vittima, ma l'avversario deve essere consapevole che i frame possono anche essere rivelati utilizzando la chiave di crittografia del gruppo. È importante notare che se la coda viene rivelata utilizzando la chiave di crittografia del gruppo, l'attaccante deve disporre di credenziali di rete valide per ottenere la rispettiva chiave di crittografia.

2.1.3.3 Leak di Frame in Linux

Un'altra categoria di AP vulnerabili a diverse varianti di attacco sono gli access point su Linux (da 5.5.0 fino a 5.17.6).

Leak su Collegamenti Crittografati senza Chiave di Crittografia

Le implementazioni precedenti del kernel Linux non eliminavano i frame di dati quando la chiave di crittografia non era più disponibile su collegamenti crittografati, ma i suoi frame venivano trasmessi in chiaro. Affinché questa variante di attacco abbia successo, l'access point non deve essere in grado di mantenere lo stato completo del client. Ciò si applica ai kernel Linux più vecchi (ossia il modulo del kernel mac80211 abilita lo stato completo del client dell'access point di default dal kernel Linux 4.5.0) e può applicarsi alle implementazioni del driver FullMAC (ossia i driver FullMAC utilizzano la

propria implementazione del modulo mac80211). A causa della mancata gestione dello stato completo del client, il *demon* dello spazio utente non eliminerà l'intero stato di una stazione client (compresa la sua coda di trasmissione) quando riceve, ad esempio, una richiesta di autenticazione. Un attaccante può sfruttare questo comportamento per eliminare la pairwise key e rivelare tutti i frame dalla coda di trasmissione in chiaro.

2.1.3.4 Attuazione dell'Attacco

Consideriamo un client connesso ad un access point che non mantiene lo stato completo del client. Simile all'attacco descritto in Figura 2.1, un attaccante può sfruttare questo comportamento per rivelare i frame dalla coda di trasmissione in chiaro. Dopo aver costretto l'access point a mettere in coda i frame per il client vittima, l'attaccante invia una richiesta di autenticazione. Poiché l'access point non mantiene lo stato completo del client, la pairwise key viene eliminata senza aggiornare la coda di trasmissione. Infine, l'attaccante può inviare un frame di *Wake-Up* per avviare il processo di dequeuing e un access point vulnerabile rivelerebbe tutti i suoi frame in chiaro.

2.1.4 Difese

Per garantire la sicurezza delle code di trasmissione negli access point Wi-Fi, è necessario stabilire procedure chiare e definite per la gestione delle code in caso di cambiamento del contesto di sicurezza. Attualmente, lo standard non affronta esplicitamente questa problematica, lasciando spazio a potenziali vulnerabilità.

Al fine di mitigare il rischio di perdite di frame o di divulgazione non autorizzata, sono raccomandate due possibili difese:

1. Svuotamento della Coda: Prima di eliminare la pairwise key, l'access point dovrebbe svuotare completamente la coda di trasmissione da i frame, inviandolo al client indipendentemente dallo stato di risparmio energetico. Questo garantirebbe che tutti i frame memorizzati nella coda vengano consegnati prima che la chiave venga eliminata, evitando possibili falle di sicurezza.

2. Pulizia della Coda: Prima di eliminare la chiave di crittografia pairwise, l'access point deve eliminare completamente la coda di trasmissione. In questo modo, tutti i frame memorizzati nella coda vengono scartati, evitando che informazioni sensibili vengano divulgati accidentalmente o possano essere sfruttati da potenziali attaccanti.

2.2 Sfruttamento della Coda per Interruzioni di Rete

Un'ulteriore problematica riscontrata è che un access point può essere eluso e convinto ad attivare i meccanismi di risparmio energetico per un client vittima. In altre parole, poiché il bit di risparmio energetico nell'intestazione di un frame non è protetto, un attaccante può facilmente abilitare tali meccanismi e quindi mettere in coda selettivamente i frame presso l'access point. Di conseguenza, i client sono vulnerabili ad attacchi di disconnessione e *denial-of-service*.

2.2.1 Coda delle Richieste SA Query

La procedura di SA Query possa essere sfruttata per disconnettere un client dalla rete. Ricordiamo che lo standard definisce quali frame di gestione possono essere messi in coda e quali memorizzati nella coda utilizzando un meccanismo di risparmio energetico. I frame di richiesta e risposta SA Query vengono trasmessi come **action frames** protetti. Tuttavia, lo standard non li esclude esplicitamente dalla possibilità di essere messi in coda, cioè possono essere messi in coda con alcune eccezioni. Quando una stazione mette in coda una richiesta o una risposta, si può causare un timeout dal lato ricevente poiché si tratta di una procedura di sicurezza sensibile al tempo. Di conseguenza, l'associazione di sicurezza deve essere interrotta, disconnettendo efficacemente il client vittima dalla rete. A causa di questo comportamento, gli access point sono esposti ad un possibile attacco di disconnessione basato sulla coda verso i propri client, anche se la configurazione di rete impone la protezione Wi-Fi MFP, come ad esempio, WPA3.

2.2.2 Coda dei Messaggi di 4-Way Handshake

Oltre agli action frames precedenti, un attaccante può forzare la messa in coda di data frames. Nel caso dei messaggidi 4-Way Handshake, durante la procedura di connessione, questo può facilmente condurre a un attacco di denial-of-service basato sulla coda. Poiché questo attacco mira al 4-Way Handshake, è efficace contro qualsiasi tipo di configurazione di rete.

2.2.3 Outline dell'Attacco

Consideriamo un client vittima che si sta connettendo a un access point vulnerabile. Nella Figura **??**, mostriamo come un attaccante possa mirare a un access point vulnerabile per impedire al client vittima di connettersi, in tre fasi:

- Dopo la procedura di associazione, l'attaccante esegue uno spoofing di un frame nullo e imposta il bit di risparmio energetico nell'intestazione del frame. Ciò fa sì che il kernel faccia marcare il client vittima in modalità power saving.

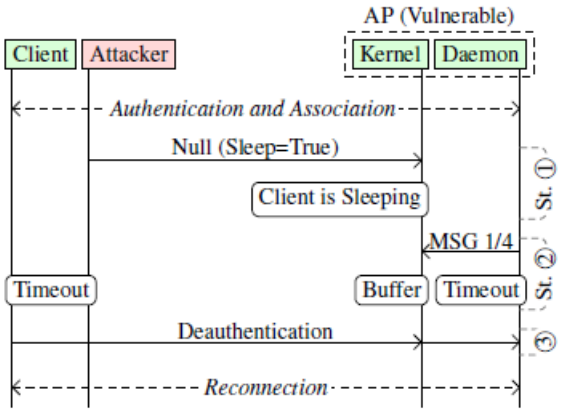

Figura 2.2: Attacco 4-Way Handshake.

- L'access point vulnerabile metterà ora in coda tutti i frame che possono entrare nel buffer, compreso il primo messaggio del 4-Way Handshake (che viene inviato come un data frame). Questo comportamento porta a un timeout del 4-Way Handshake sia per l'access point che per il client vittima, poiché i messaggi di handshake non vengono mai inviati.
- Il client vittima si aspetta il primo messaggio del 4-Way Handshake, ma non ne riceve alcuno. Di conseguenza, scatta un timeout che interrompe la procedura di handshake, costringendo il client vittima a inviare un messaggio di deautenticazione.
- Poiché l'access point sta ancora memorizzando i frame nella coda, il suo messaggio di deautenticazione non viene trasmesso nemmeno al client vittima. Di conseguenza, il client si disconnetterà dalla rete.

2.3 Sovrascrittura del Contesto di Sicurezza

Un altro possibile attacco ha l'obiettivo di controllare completamente il contesto di sicurezza utilizzato da un access point. L'attaccante si connette all'AP e negozia un nuovo contesto di sicurezza controllato dall'attaccante stesso. Successivamente, si inganna l'AP affinché associ il contesto di sicurezza controllato dall'attaccante ai frame appartenenti alla vittima. Di conseguenza, l'attaccante può decriptare i frame destinati alla vittima. Questo attacco sfrutta difetti di progettazione relativi all'associazione del contesto di sicurezza con i frame in uscita ed è sfruttabile nelle reti hotspot-like.

2.3.1 Descrizione dell'Attacco

L'attaccante può sovrascrivere il contesto di sicurezza associato dall'AP a un client facendo spoofing dell'indirizzo MAC del client e quindi connettendosi all'AP. Ciò fa sì che l'AP cifri il traffico destinato a questo client utilizzando le chiavi di sessione possedute dall'attaccante. Nella Figura **??**, illustreremo le fasi individuali di questo attacco:

Supponiamo che la vittima sia attualmente connessa all'AP e si appresti a ricevere un frame che l'attaccante desidera intercettare. Ad esempio, la vittima potrebbe inviare una richiesta HTTP senza utilizzare TLS, e l'attaccante desidera intercettare la risposta HTTP.

Prima che il client riceva la risposta, l'attaccante falsifica l'indirizzo MAC della vittima e si connette all'AP utilizzando le proprie credenziali (ad esempio, le proprie credenziali personali nelle reti aziendali WPA2 o WPA3). Di conseguenza, l'attaccante sovrascrive il contesto di sicurezza associato dall'AP all'indirizzo MAC della vittima con il contesto di sicurezza controllato dall'attaccante.

L'AP invia ora i frame all'indirizzo MAC della vittima utilizzando il contesto di sicurezza dell'attaccante. In altre parole, i pacchetti destinati alla vittima, come le risposte HTTP, sono ora criptati con le chiavi di cui l'attaccante è in possesso.

Poiché i pacchetti destinati alla vittima sono ora criptati utilizzando le chiavi possedute dall'attaccante, l'attaccante può decifrarli facilmente. In altre parole, è possibile bypassare la crittografia a livello Wi-Fi. È importante notare che anche se la risposta è crittografata a un livello superiore utilizzando un protocollo come TLS, l'attacco comunque rivela gli indirizzi IP ai quali la vittima si sta connettendo.

Una limitazione pratica dell'attacco è che potrebbe richiedere un tempo considerevole all'attaccante per connettersi all'AP, causando il mancato ricevimento della risposta. Ad esempio, quando si utilizzano protocolli basati su EAP (Extensible Authentication Protocol) per l'autenticazione, di solito viene utilizzato un server RADIUS remoto per autenticare il client, e la comunicazione con questo server può comportare notevoli ritardi. Se la risposta che desideriamo intercettare viene inviata tramite TCP, ciò non è un problema: il mittente la ritrasmetterà automaticamente se non viene ricevuta l'acknow-

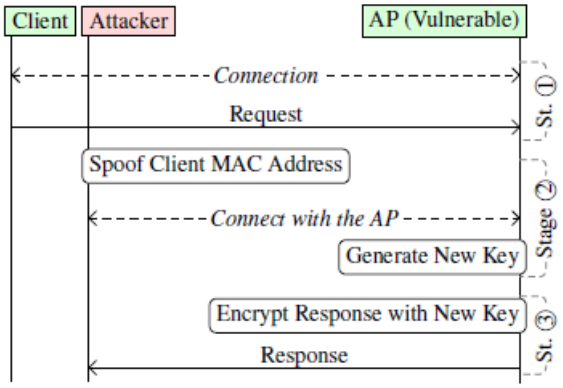

Figura 2.3: Attacco di Security Context Overriding.

ledgement. Tuttavia, per protocolli come UDP, ciò potrebbe essere problematico, poiché la risposta potrebbe essere persa.

2.3.2 Difese

Per mitigare gli attacchi contro le reti hotspot-like, un AP può impedire temporaneamente ai client di connettersi se stanno utilizzando un indirizzo MAC che è stato recentemente connesso all'AP. Ciò impedisce all'attaccante di falsificare un indirizzo MAC e intercettare i frame in sospeso verso una vittima. Quando può essere garantito che l'utente dietro un indirizzo MAC non è cambiato, al client può essere consentito di riconnettersi immediatamente.

Per riconoscere in modo sicuro gli utenti che si sono connessi di recente, un AP può memorizzare una mappatura tra l'indirizzo MAC di un client e le sue associazioni di sicurezza memorizzate (ad esempio, il PMK, Pairwise Master Key). Un client può connettersi immediatamente o riconnettersi dimostrando di possedere le proprie associazioni di sicurezza memorizzate, ad esempio connettendosi utilizzando il corretto PMK memorizzato.

CAPITOLO 3

Conclusioni

In conclusione, questo report ha avuto l'obiettivo di analizzare il meccanismo di accodamento dei frame negli access point, in particolare nel loro comportamento in caso della *Power Saving Mode*, modalità risparmio energetico.

Le vulnerabilità discusse mettono in luce le debolezze presenti nell'implementazione delle code di trasmissione degli access point WiFi; queste consentono agli attaccanti di alterare il contesto di sicurezza dell'access point e di intercettare o manipolare il traffico dati tra gli access point e i dispositivi client.

Il lavoro di questo elaborato è basato sulle informazioni dell'articolo [**schepers2023towards**].