Reti 4G/5G: profili di vulnerabilità e possibili contromisure

Le reti mobili stanno evolvendo velocemente nell'ultimo periodo.

Dall'entrata in funzione del 4G, si sono potuti toccare con mano i benefici della banda larga anche nelle connessioni in mobilità. A distanza di qualche anno, il 4G Plus ha permesso un incremento di prestazioni sostanziale rispetto alla tecnologia di base. Con l'arrivo del 5G, previsto nel 2020, saremo di fronte ad una vera e propria rivoluzione, che prevede la proliferazione dei dispositivi IoT e un incremento di velocità di banda nell'ordine dei Gbit/s.

Come appreso dal recente passato, ogni miglioria tecnologica porta con sé l'introduzione di nuove vulnerabilità di progettazione, potenzialmente sfruttabili da utenti malevoli. È quindi facilmente ipotizzabile che, come per le connessioni Bluetooth e WiFi, anche le connessioni mobili soffrano di potenziali errori di progettazione.

Difatti, nell'ultimo periodo sono emersi numerosi studi nei quali alcuni ricercatori evidenziano le vulnerabilità dello standard 4G. La cosa ben più grave è che alcune di esse impattano anche sul nuovo standard 5G di imminente introduzione.

Analizziamo, quindi, di seguito le falle più gravi e verifichiamo se vi sono contromisure applicabili.

AUTHENTICATION RELAY ATTACK (4G)

Questo tipo di attacco potrebbe non solo consentire a un attaccante di compromettere la rete cellulare per leggere i

messaggi – in entrata e in uscita – delle vittime, ma anche di impersonificare qualcun altro per l'esecuzione di un qualsiasi atto delinquenziale.

Come è banalmente intuibile analizzando la figura precedente, disponendo di una cella e di un dispositivo effimeri, è possibile:

1. forzare la disconnessione del dispositivo vittima da una cella valida[1];
2. forzare la connessione di quest'ultimo alla cella effimera;
3. reindirizzare la richiesta di autenticazione fornita dal dispositivo vittima al fornitore del servizio;
4. tramite la cella effimera, far decodificare i messaggi di autenticazione al dispositivo vittima;
5. completare l'autenticazione, al posto del dispositivo vittima, con dispositivo effimero.

A seguito dell'autenticazione, l'attaccante possiede una copia speculare (agli occhi della rete) del dispositivo della vittima.

aLTEr (4G/5G?)

Gli standard 4G/5G prevedono diversi meccanismi di sicurezza. Quando un dispositivo si collega alla rete, stabilisce un'autenticazione reciproca[2] con il fornitore del servizio, ottenendo una chiave di crittografia condivisa per la trasmissione sicura dei dati.

Tale chiave è utilizzata per crittografare anche il traffico di "controllo". Quest'ultimo è protetto da meccanismi di controllo dell'integrità, il che significa che l'utente malintenzionato non è in grado di manipolare il traffico durante la trasmissione.

Scendendo nel dettaglio, aLTEr interviene sfruttando un errore

di progettazione relativo alla gestione del “livello 2” dello stack di rete. Nello stack del protocollo TCP/IP, il layer 2 è quello che corrisponde al *Data Link*, posto gerarchicamente al di sotto dei livelli TCP ed IP, nei quali è implementato il meccanismo di sicurezza precedentemente illustrato.

Brevemente: i dati utente, a livello 2 – *Data Link*, vengono crittografati in modalità contatore (AES-CTR), in cui l’algoritmo genera un keystream (caratteri pseudorandomici). Il testo cifrato viene quindi calcolato dallo XORing del keystream con il testo in chiaro.

Non essendo stati previsti negli standard dei controlli di integrità a questo livello, e conoscendo il testo in chiaro originale della richiesta[3], è facile modificare il contenuto di un pacchetto DNS anche se crittografato, reindirizzando la richiesta a un server DNS sotto il controllo dell’avversario.

Riassumendo: un utente malintenzionato può creare una cella LTE effimera, alla quale il dispositivo della vittima si collegherà in automatico, poiché il segnale di quest’ultima sarà più potente per prossimità rispetto a una qualsiasi cella reale limitrofa. A questo punto il traffico e le relative richieste effettuate dal dispositivo mobile della vittima verranno tutte filtrate dalla cella effimera, per essere poi inoltrate alla cella reale, ignara di eventuali manipolazioni avvenute precedentemente.

La dimostrazione dell’attacco è visionabile tramite il video https://www.youtube.com/watch?v=3d6lzSRBHU8.

ToRPEDO (4G/5G)

Acronimo di *TRacking via Paging mEssage DistributiOn*, sfrutta una debolezza nel protocollo di *paging* utilizzato dagli ISP per segnalare ad un dispositivo in stato di inattività una notifica, prima dell’effettivo arrivo di una comunicazione in entrata.

Se un dispositivo non stabilisce, per un certo periodo, una comunicazione attiva con la rete cellulare, entra in una sorta di modalità di risparmio della batteria. In questo contesto la rete cellulare, prima che una chiamata o un messaggio di testo raggiungano il dispositivo, invia a quest'ultimo un messaggio di paging per anticipare, tramite una notifica, una chiamata o un messaggio in arrivo. Il messaggio di paging incorpora in sé l'identificativo temporaneo del dispositivo – TMSI (*Temporary Mobile Subscriber Identity*)[4] – che viene aggiornato, a seguito dell'aggancio ad una cella, solo in rari casi.

I ricercatori hanno scoperto che, effettuando e annullando un gran numero di chiamate in un breve lasso di tempo, avviene, da parte del fornitore del servizio, l'aggiornamento del valore TMSI nel proprio database più frequentemente del solito. Quanto detto si compie unicamente sulla stazione mobile, senza generare un tipo di avviso nel dispositivo vittima. A seguito di quanto descritto, utilizzando un IMSI Catcher[5], un malintenzionato può verificare se la vittima si trova in un raggio di distanza entro il quale è possibile intercettare eventuali comunicazioni.

Quindi, conoscendo il *Paging Occasion* (PO)[6], l'attaccante potrebbe:

- tracciare il dispositivo vittima;
- dirottare il canale di paging iniettando o negando i messaggi di paging di controllo;
- effettuare lo spoofing delle comunicazioni;
- lanciare attacchi DoS, saturando le risorse del dispositivo vittima, fino al punto da mandarlo in blocco.

PIERCER IMSI-Cracking attack (4G/5G)

I ricercatori hanno ulteriormente precisato che Torpedo può fungere da apripista per altri due tipi di attacco.

Il primo, denominato Piercer (*Persistent Information ExposuRe by the CorE netwoRk*), consente all'attaccante di determinare l'IMSI (*International Mobile Subscriber Identity*) della vittima sulla rete 4G/5G, ed associarlo al proprio dispositivo.

I numeri IMSI sono crittografati nelle reti 4G e 5G, in modo da poterli proteggere da eventuali attacchi; tuttavia i ricercatori hanno nuovamente riscontrato che tali protezioni sono inadeguate.

Il problema sta nell'implementazione del vettore, denominato per l'appunto Piercer, che espone i numeri IMSI sull'attuale rete 4G e sulla futura rete 5G. Alcuni fornitori di servizi utilizzano l'identificativo IMSI al posto del TMSI nei messaggi di paging per identificare i dispositivi con servizi "eccezionali", o per verificare servizi rimasti in stato "pending". I test effettuati hanno rivelato che è possibile dare l'impressione, al fornitore di servizi, che si stia verificando uno di questi casi eccezionali, in modo da costringere il dispositivo a rivelare il proprio IMSI.

Il secondo attacco, detto IMSI-Cracking attack, utilizza un attacco a forza bruta per individuare il codice IMSI su rete 4G o 5G.

Con il numero IMSI a disposizione, gli aggressori possono inscenare attacchi di vario genere: potrebbero spiare la lista delle chiamate della vittima, registrare le conversazioni audio, leggere gli SMS in arrivo, individuare l'esatta posizione del dispositivo, quindi gli spostamenti della vittima durante l'arco della giornata. E molto altro ancora…

Considerazioni

I requisiti hardware per effettuare questo tipo di attacchi bisogna trovarsi abbastanza vicini al terminale che si vuole hackerare. Va premesso inoltre che per attuare questo tipo di

attacco serve dell’attrezzatura abbastanza costosa, per le tasche dell’utente comune: circa 4.000$[7].

Tuttavia, se prendiamo ad esempio contesti come lo spionaggio industriale o, peggio ancora, quello politico, ci rendiamo conto l’eventuale costo dell’attrezzatura è assolutamente trascurabile.

Possibili contromisure

Per l’**Autentication Relay Attack** non vi sono contromisure. Fonti attendibili confermano che tale metodologia è spesso sfruttata dagli organismi investigativi statunitensi, per perseguire eventuali azioni delinquenziali.

Per quanto riguarda **aLTEr**, l’utente non ha modo di difendersi, se non quello di consultare esclusivamente siti web che utilizzano HSTS (*HTTP Strict Transport Security*), cosa ben diversa dal protocollo HTTPS (*HTTP secure*).

Sta agli *Internet Service Provider*, quindi ai gestori telefonici, utilizzare protocolli di autenticazione del tipo AES-GCM o ChaChat20-Poly1305. Come evidenziato anche dai ricercatori, però, una modifica dell’attuale infrastruttura comporterebbe un elevato sforzo finanziario e organizzativo. Perciò, la maggior parte dei gestori potrebbe decidere di non fixare la vulnerabilità, dal momento che non è obbligatorio farlo.

Altra contromisura potrebbe consistere nell’adozione del protocollo *DNS over TLS or DTLS*, che permetterebbe di proteggere i dispositivi provvedendo alla cifratura del traffico DNS, garantendo la di fatto l’integrità dello stesso.

Ad ogni modo, allo stato dell’arte, ne deriva che anche il 5G potrebbe essere potenzialmente insicuro a questo tipo di attacco. Essendo la crittografia autenticata una funzione ad implementazione facoltativa, molti ISP potrebbero decidere di non adottarla nelle nuove reti 5G che stanno implementando.

Per quanto riguarda **ToRPEDO, PIERCER ed IMSI-Cracking, vengono sfruttate debolezze intrinseche nei protocolli LTE 4G e 5G, che riguardano le prime fasi dell'interazione con i terminali mobili ed al mutuo riconoscimento con la rete in previsione di trasferimento di messaggi e chiamate.**

Conclusioni

Le dinamiche di autenticazione ed identificazione reciproca dovrebbero essere rese più sicure sin dalla fase di progettazione. Sarebbe opportuno evitare l'applicazione di metodi di **autenticazione antiquati volti a garantire** vecchie esigenze, dipendenti da reti e terminali meno performanti, o a metodi di comunicazione di base (ad esempio la retro-compatibilità) in cui non si è tenuto conto del concetto di "security by design".

Come si comporteranno i vari fornitori? Probabilmente non prenderanno alcun provvedimento. Secondo gli stessi ricercatori è difatti molto probabile che queste vulnerabilità siano troppo onerose da correggere (sia tecnicamente che economicamente), e che sia necessario aspettare una radicale modifica del protocollo per una reale risoluzione del problema.

Nel contempo sarà meglio tener presente che gli input digitali che ci giungono, potrebbero non provenire dal reale mittente della comunicazione e/o potrebbero essere intercettati da chiunque sia a portata di tiro.

Benvenuti nell'Era della paranoia…

Note

[1] Stealthy kicking-off Attack.

[2] Autenticazione reciproca significa che la rete e il telefono possono verificare rispettivamente le loro identità.

[3] Ipotizzando i siti più visitati dalla vittima, tramite Website Fingerprinting.

[4] Un numero univoco che lo smartphone utilizza per interfacciarsi con la rete GSM. Serve a garantire la riservatezza degli utenti, evitando di mandare il codice IMSI: https://it.wikipedia.org/wiki/IMSI.

[5] Ad esempio Stingrays and DRTBox.

[6] http://www.techtrained.com/paging-procedure-lte/.

[7] Secondo gli stessi ricercatori che hanno messo in atto i vari scenari di attacco.

Articolo a cura di **Daniele Rigitano**

https://www.ictsecuritymagazine.com/articoli/reti-4g-5g-profili-di-vulnerabilita-e-possibili-contromisure/