PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3874 di venerdì 14 ottobre 2016

GPS: dallo jamming allo spoofing

Le tecnologie dei malviventi si stanno evolvendo e oggi sembrano essere disponibili anche dispositivi in grado non solo di bloccare la ricezione del segnale, ma addirittura di alterarlo, modificando le coordinate ricevute dall'apparato. Di A.Biasiotti.

In un celebre film di 007 (il domani non muore mai), una banda di malviventi riesce ad alterare i segnali ricevuti da una nave da battaglia inglese, operante nel Mar della Cina, portandola ad invadere le acque territoriali cinesi.

Ciò che era finzione nel 1997, quando il film venne lanciato in tutto il mondo, sta diventando oggi una realtà.

I lettori sono certamente al corrente del fatto che è facilmente acquistabile sul mercato un dispositivo, chiamato jammer, con una portata di qualche diecina di metri, che blocca la ricezione del segnale GPS da parte degli apparati riceventi, installati ad esempio a bordo di autovetture oppure di furgoni blindati. Con questo accorgimento, il mezzo non è più in grado di trasmettere alla centrale di monitoraggio le proprie effettive coordinate di posizione e quindi si offre il destro ai malviventi di nascondere il luogo dove l'automobile è stata celata o di assaltare il furgone blindato.

Completamente diverso è l'argomento che desidero affrontare oggi, che riguarda invece il fenomeno dello spoofing.

Questa tipologia di attacco permette di inviare segnali preconfezionati al ricevitore, che visualizza quindi una posizione, che non è quella effettiva.

Sembra che uno dei primi attacchi, svolti utilizzando questa tecnologia, sia avvenuto quando, all'inizio del 2016, due imbarcazioni della marina americana, che si trovavano nel Golfo Persico, entrarono nelle acque territoriali iraniane. Gli iraniani intercettarono le navi e catturarono 10 marinari, creando una situazione di imbarazzo, per non dire di pericolo. I marinai furono prontamente rilasciati e nessuno riuscì a spiegare il motivo per cui le imbarcazioni avevano invaso le acque territoriali iraniane.

La difficoltà nel creare segnali simulati sta nel fatto che i segnali dei satelliti GPS sono protetti da un robusto algoritmo criptografico e, per simulare un segnale, l'attaccante avrebbe dovuto essere in grado di violare questo robusto algoritmo.

Un altro evento si è verificato quando un drone americano è stato catturato, inducendolo ad atterrare in una zona controllata dai nemici.

Il dipartimento della sicurezza nazionale degli Stati Uniti ha pertanto creato una squadra specializzata per analizzare la possibilità di realizzare questo trasmettitore di segnali GPS, che sono indistinguibili da quelli reali. Durante un esperimento

condotto nel poligono militare di White Sands, nel Nuovo Messico, questa squadra riuscì ad ingannare un drone, facendo credere agli apparati di bordo che esso stava salendo in quota, mentre invece stava scendendo; il drone fu salvato l'ultimo istante, prima di precipitare nella sabbia del deserto. Il salvataggio fu portato a termine da un pilota che neutralizzò i controlli automatici e assunse il comando manuale del drone.

Gli studiosi, che hanno affrontato la possibilità di alterazione dei segnali GPS, hanno messo in guardia il mondo delle comunicazioni, della finanza e delle reti elettriche circa le possibili conseguenze negative critiche, che l'alterazione di questi segnali potrebbe causare.

Per dare un contributo da queste ricerche, il proprietario di una imbarcazione di 65 metri, che utilizza il sistema GPS per la navigazione in alto mare, ha messo a disposizione questa imbarcazione per effettuare dei test. Il risultato del test è stato sconcertante, perché il sistema di bordo è stato totalmente ingannato.

Anche se le apparecchiature utilizzate erano troppo sofisticate per essere messe a punto da un hacker di medio livello, la tecnologia è certamente alla portata di nazioni aggressive, come ad esempio la Corea del Nord.

Ad oggi, sono state messe a punto tre tecnologie che potrebbero consentire un certo livello di protezione da questo tipo di attacco.

La prima protezione è quella di utilizzare applicativi criptografici più elevati, di tipo dinamico, in modo da rendere oltremodo difficoltosa la creazione di segnali accettabili. È questa la tecnologia che viene utilizzata dai militari, e che si basa su chiavi criptografiche evolutive, ma non disponibili per applicazioni civili.

È bene sottolineare che il sistema di navigazione satellitare europeo, chiamato Galileo, dispone di protezioni ben più avanzate.

Un'altra tecnica di difesa è basata sulla individuazione di un segnale distorto. Quando il segnale generato dall'hacker è diverso da quello ricevuto dalla costellazione satellitare, è possibile rivelare delle brevi anomalie nel segnale ricevuto, che potrebbero indicare un tentativo di attacco. Per individuare questa distorsione temporanea bisogna utilizzare sofisticate apparecchiature elettroniche, che esaminano i segnali provenienti dai vari canali satellitari e individuano queste brevi distorsioni. Tuttavia questi apparati funzionano solo se sono già in funzione all'inizio dell'attacco e alla fine dell'attacco stesso; ci troviamo davanti a un processo che può durare solo pochi minuti.

Infine, una terza tecnica di protezione è basata sulla individuazione della direzione da cui arrivano i segnali dei satelliti. Se la antenna che riceve i satelliti è di tipo direzionale, è possibile rendersi conto che il segnale in arrivo non proviene dalla posizione calcolata dei satelliti, ma questo tipo di elaborazione informatica richiede ore di calcolo e potenti disponibilità informatiche.

Alla luce dei risultati preoccupanti di queste simulazioni, il fabbricante di un apparato GPS, all'inizio del 2016, ha messo in commercio il primo ricevitore dotato di difese anti spoofing. L'azienda non ha offerto dettagli sul metodo di rivelazione adottato, ma è probabile che l'approccio utilizzato si basi sulla rivelazione di un segnale distorto.

Potrebbe sembrare più efficiente la tecnica che rileva la direzione di arrivo dei segnali satellitari, ma ciò significa installare numerose antenne e avere a disposizione un programma che calcoli, istante per istante, la posizione dei satelliti nel cielo. Ciò mette fuori gioco la stragrande maggioranza dei ricevitori satellitari, di tipo portatile. La soluzione più economica oggi disponibile si basa sulla installazione di almeno due antenne e di un algoritmo, in grado di calcolare la direzione di arrivo del segnale. Questo prodotto potrebbe essere inserito tra breve nel catalogo del fabbricante, a un prezzo dell'ordine dei 10.000 dollari per unità.

Potrebbe darsi che operatori commerciali ad alto rischio non esitino più di tanto ad installare questa tecnologia avanzata.

D'altro canto l'incremento dell'utilizzo di apparati satellitari e Wi-Fi ha comportato, quasi automaticamente, un aumento del numero di hacker che si sono dedicati ad attaccare questi sistemi. Gli attacchi condotti contro le moderne autovetture, dotate di reti senza fili a bordo, ne sono una prova.

Ancora una volta, il primo passo per difendersi è conoscere le tecniche usate dall'attaccante (know your enemy!).

Adalberto Biasiotti

---

www.puntosicuro.it