Navi nella Rete, navi alla deriva

(326) — Da questo pulpito Cassandra ha già tuonato denunciando la leggerezza con cui i prodotti dell'elettronica di consumo, ultime le…

Navi nella Rete, navi alla deriva

(326)—Da questo pulpito Cassandra ha già tuonato denunciando la leggerezza con cui i prodotti dell'elettronica di consumo, ultime le SmartTV, vengono progettate dalle industrie seguendo convenienze che nulla hanno a che vedere con la sicurezza e la protezione dei dati dei loro utenti.La situazione non è tuttavia migliore quando esistono standard elaborati da consorzi "indipendenti", ma spesso guidati solo da aziende produttrici di informatica, che producono standard altrettanto disinteressati alle necessità ed ai desideri degli utenti finali.

18 luglio 2014—Ma cosa avviene uscendo dall'ambito dell'elettronica di consumo, ed entrando in quello dei sistemi telematici "importanti" come i sistemi SCADA, i sistemi di controllo aereo ed altri sistemi telematici da cui dipendono i servizi essenziali e spesso la sicurezza fisica delle persone?

Di SCADA e dell'insicurezza di questi sistemi si è già molto parlato: le radici della loro insicurezza affondano nel passato, e vanno ricercate spesso nell'hardware, cioè nei componenti fisici utilizzati, risalenti talvolta a 30/40 anni fa. Spesso nuovi componenti addizionali "intelligenti" vengono usati per modernizzare sistemi antiquati: si tratta di una "iniezione" di componenti telematici potenti, economici e flessibili, che aggiungono possibilità interessantissime, ma che nulla proteggono e da nulla si proteggono.

Un esempio: la trasmissione dati di impianto dai tralicci elettrici, via 3G e TCP/IP, in chiaro.

Nascono per fortuna nuovi sistemi e nuovi protocolli, progettati da zero ed in questo millennio, che sostituiscono quelli più "antichi". Il controllo del traffico aereo ne è un esempio, come pure il più semplice controllo del traffico navale AIS (le navi vanno molto più piano…).

Oggi parleremo di quest'ultimo: si tratta di un sistema progettato nei primi anni del millennio (2002), e che fin dall'inizio si propone di integrare la Rete nel sistema di elaborazione e trasmissione delle informazioni. Un inciso: ormai dal 1990 i protocolli che costituiscono l'ossatura della Rete sono perfettamente in grado di gestire comunicazioni sicure ed affidabili, come quelle del vostro conto corrente.

Lo spunto per questo articolo arriva da Hackmeeting 0x11, i cui contenuti, a parere di Cassandra, sono stati quest'anno di ottimo livello, all'altezza di altre manifestazioni europee, e per l'esattezza da un interessantissimo intervento intitolato un po' cripticamente AIS Exposed

Ma torniamo ai sette mari.

Il traffico navale viene regolato a livello planetario grazie a delle trasmittenti radio dedicate appartenenti ad un sistema chiamato AIS—Automatic Identification System che le navi, anche se di piccolo tonnellaggio, sono ormai da anni obbligate ad avere a bordo, e che trasmettono automaticamente e continuamente la posizione, rilevata utilizzando la costellazione GPS. Questi segnali radio vengono captati da stazioni di ascolto situate su boe, fari o nelle capitanerie di porto, e diffuse a livello globale, in modo da poter essere utilizzate dovunque. La struttura delle comunicazioni di AIS prevede che i dati vengano scambiati via Internet.

Possono quindi essere visualizzati dati relativi ad interi porti, a puro titolo di esempio quello di Genova, e chiunque può conoscere in tempo reale posizioni e caratteristiche delle navi in rada, in arrivo o in partenza, o di particolari navi, come ad esempio la USS Nimitz.

I dati stessi, oltre che disponibili in tempo reale, sono anche memorizzati da un paio di aziende, che poi li rivendono come dati storici (vi vengono in mente i dati di cella GSM? Anche a Cassandra).

Ma descriviamo con qualche dettaglio in più questo potente ed utile sistema informatico.I dati di posizione trasmessi sono scritti in un particolare formato, utilizzando solo caratteri ASCII, e vengono trasmessi via radio in chiaro; sempre in chiaro vengono ritrasmessi a terra e finalmente diffusi via internet. Chiunque può intercettarli, ma in questo caso non è un male, visto che sono destinati alla massima diffusione possibile.

Su AIS viaggiano anche gli allarmi "uomo in mare". Se qualcuno si getta in mare con un giubbotto moderno, il contatto con l'acqua salata attiva una trasmittente che invia il messaggio di allarme fino a 30–60 chilometri di distanza: tutte le navi che lo ricevono, appunto via AIS, devono per legge convergere sulla posizione. Le stesse trasmittenti AIS scatenano un allarme di possibile collisione quanto ricevono direttamente via radio il segnale di un'altra nave che si sta avvicinando.

Davvero un sistema utile.

Ma… Chi garantisce l'autenticazione della nave? Chi garantisce che una certa posizione sia stata trasmessa proprio dalla nave giusta? AIS è figlio dei tempi in cui l'hardware dettava legge, anche se nel 2002 ormai quasi tutti si erano accorti che non era più così. L'"autenticazione" quindi deriva unicamente dal fatto che una trasmittente AIS può essere acquistata solo da fornitori referenziati, ed il codice della nave è scritto in maniera univoca ed inalterabile nella trasmittente stessa.

…e la Luna è fatta di formaggio verde…

Da 10 anni a questa parte le radio sono ormai "software defined radio": non si commutano più i quarzi per cambiare la frequenza e, a parte lo stadio finale di

potenza e l'antenna, tutto il resto di una trasmittente è basato su componenti controllati via software, o semplicemente simulati su un pc.

Cassandra ha già scritto su questi temi riguardo a possibili attacchi alle SmartTV e qui la debolezza del protocollo di comunicazione AIS è molto più grave di quella di HbbTV.

Come fare quindi per costruirsi un AIS per la propria nave? Basta scrivere un programma per generare i codici AIS, prendere la posizione da una antenna GSM (il vostro cellulare?) e collegare tutto ad un modulatore controllabile via software con programmi FOSS come Gnu Radio.

Per terminare, attaccare a quanto sopra il finale di potenza e l'antenna di una trasmittente commerciale, scrivere il nome giusto e le caratteristiche della vostra vera nave nei parametri *et voilà*, è possibile fare a meno di comprare il costoso ed ufficiale trasmettitore AIS.

Ma… E se i dati fossero "sbagliati"? In effetti, in maniera altrettanto semplice sarebbe possibile (in maniera completamente illegale) trasmettere l'identità di qualunque nave civile o militare, grande o piccola, reale o immaginaria…

E fare entrare il vascello prescelto (magari una bella portaerei a propulsione nucleare classe "Nimitz") in un porticciolo turistico, nel lago di Garda o in mezzo ad un deserto.

E per far "scomparire" la nave esistente, magari per evitare che "smentisca" le coordinate false che il nostro buontempone volesse diffondere? Ahimè, il protocollo AIS prevede anche un necessario meccanismo tramite il quale le autorità portuali possono istruire una trasmittente AIS ad utilizzare una data frequenza di trasmissione dipendente dalla zona in cui naviga. Basta trasmettere il comando giusto e la trasmittente AIS della vera nave comincerà ad usare una frequenza su cui, in quella zona, nessuno ascolta: a tutti gli effetti "scomparirà dai radar".

Il buontempone di turno sarà così libero di trasmettere posizioni false sulla frequenza giusta.Per finire: nessuno vuole processare chi ha concepito, realizzato e reso capillarmente obbligatori sistemi così importanti ed utili.Lode a loro e guai a chi li volesse sovvertire.

Ma si poteva fare a meno di progettarli come un colabrodo? Purtroppo, esaminando quanto accade con oggetti più sofisticati come i nuovi sistemi di controllo del traffico aereo, o tanta altra "intelligenza" scritta nel silicio seminato in giro per il mondo, sembra che ci siano motivi imperscrutabili che rendono questo problema inevitabile.

Originally published at punto-informatico.it.

By Marco A. L. Calamari on September 8, 2017.

Canonical link