

LE NUOVE ROTTE DELL'HACKING E DEI CRIMINI TECNOLOGICI

Flavio Bernardotti – Settembre 2007

flavio@bernardotti.it

Skype: Flavio58

La tecnologia corre sempre di più, grazie anche a una miniaturizzazione sempre maggiore dell'elettronica, permettendo di creare nuovi sistemi che usati da persone senza scrupoli permettono di fare truffe sempre con maggior comodità.

Proprio in questi giorni il CENTRO DI CONTROLLO DEL CRIMINE ha rilasciato la notizia che le truffe su rete hanno superato, come importo, quella del traffico di droga.

105 miliardi di dollari !

Ma come è possibile una cosa di questo tipo ?

Lo sviluppo delle reti ha sempre avuto come fenomeno collaterale l'hacking anche se spesso l'uomo una volta partito per un viaggio non si accorge che il panorama è cambiato strada facendo.

Mi spiego meglio.

Tanti anni fa Internet non esisteva e la telematica era ridotta all'uso di un modem da 300 bauds su telefoni collegati a centrali meccaniche disturbatissime.

I personal computer non erano diffusi e quindi le informazioni erano dentro ai mainframe delle università e delle ditte, in particolare di quelle americane.

Parlare di reti significava riferirsi alle grosse reti X25 quali ITAPAC la quale era connessa ai sistemi universitari ed ad altri definiti Outdial.

Questi Outdial erano sistemi ai quali si arrivava tramite rete Itapac e che permettevano di chiamare sistemi grazie a un numero di telefono.

Un collegamento telefonico con gli USA costava 1 scatto ogni secondo a 200 lire cadauno per cui stare collegato a quelle velocità delle ore era un costo terribile.

Da qui l'esigenza di entrare di frodo in Itapac e tramite questa connettersi ai vari mainframe.

Internet ha sconvolto tutto in quanto il collegamento è immediato con qualsiasi sistema e le informazioni sono presenti da tutte le parti senza dover entrare dentro ai vari sistemi VAX o quello che erano.

L'hacker per cui ha iniziato a prendere di mira i WEB su internet portando alla perdita dell'immagine che aveva una volta questo concetto.

Ma internet non è più solo una rete ma una ricostruzione virtuale della società reale per cui contiene tutto il bene e il male di questa.

Le persone orientate alle frodi hanno iniziato a sfruttare la tecnologia per prendere soldi da conti bancari, per frodare carte di credito, per creare l'ambiente sicuro per furti e altre cose di questo tipo.

Il problema è che l'hacking ha mantenuto la concentrazione delle ricerche sulla sicurezza verso i WEB e le reti collegate a internet perdendo di vista i veri pericoli.

Da questo lo stupore della gente quando sente al telegiornale notizie del tipo : "Arrestata banda che fingendo di fare furti collegava skimmer ai sistemi di pagamento con carte dei negozi e benzinai e grazie a questi duplicava carte di credito e bancomat."

O cose ancora più da fare sorridere come questa.

In pratica su una ditta americana acquistavano un sistema che permetteva via WIRELESS di creare un'estensione del posto di lavoro collegando tastiera, mouse e video.



Poi grazie a qualche trucco, che poteva essere la complicità della donna delle pulizie, entravano in banche o centri dove da terminale si facevano movimenti contabili e collegavano l'extender, nascosto, alle postazioni di lavoro.

In questo modo tranquillamente seduti in macchina potevano fare trasferimenti sui conti o altre cose sempre di carattere illegale.

Voi direte : ma le password non si vedevano a video !

Nessun problema.

Con l'installazione nascosta del KVM si installava sulla tastiera un KEYLOGGER come quello dell'immagine il quale registrava i caratteri battuti sulla tastiera per cui anche le password non erano più segrete.



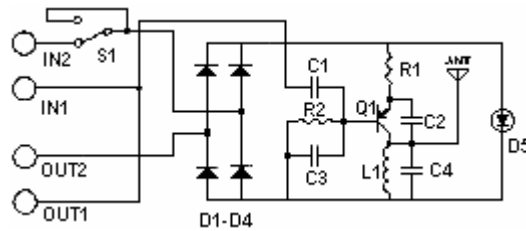
Un'altra delle meraviglie tecnologiche sono stati i bancomat 'taroccati' con sistema di duplicazione scheda magnetica e visualizzazione tramite telecamera delle password digitate.



Le immagini parlano da sole.

Per quanto riguarda i dati che passano via telefono, ad esempio i dati delle carte di credito, la cosa è ancora più semplice.

Basta collegare un circuitine da pochi euro per avere un trasmettitore FM attivo e vigile ai pagamenti.

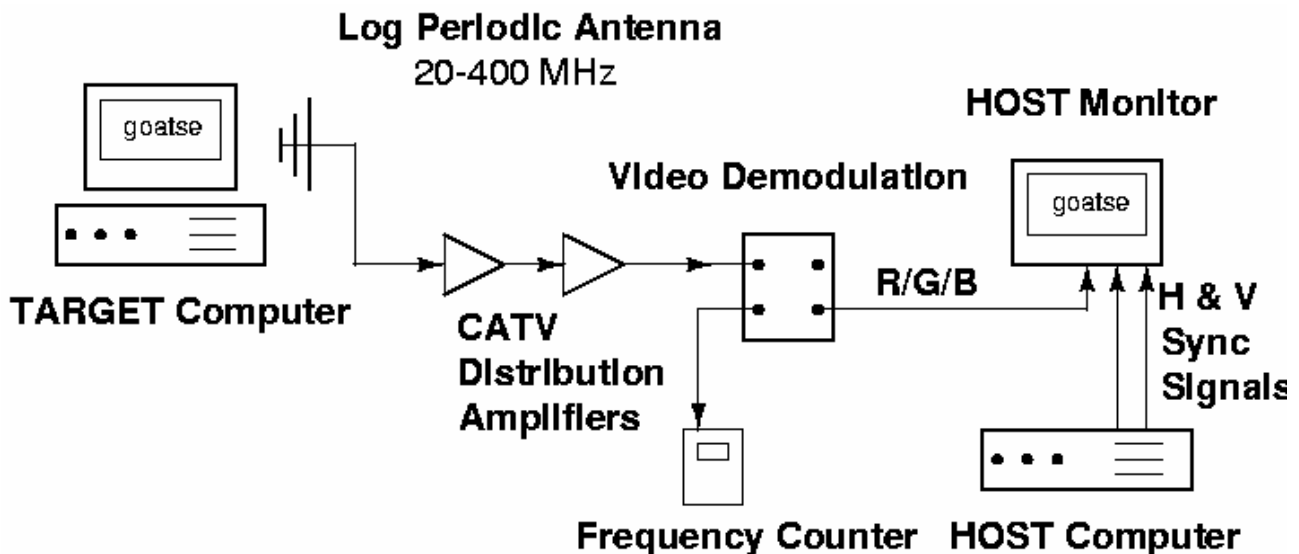


Ma la tecnologia non si ferma qui in quanto grazie alle onde elettromagnetiche gli americani stanno facendo i fucili ma grazie a queste è possibile anche visualizzare le immagini che scorrono su un computer da distanze che possono arrivare ai 100 mt senza avere nessun collegamento.

L'effetto si chiama TEMPEST e dipende dal fatto che tutti i circuiti elettronici elaborando segnali, a volte anche a frequenze altissime, emettono campi elettromagnetici che mantengono i connotati dell'informazione a cui hanno contribuito a creare.

I monitor dei computer ad esempio usano due orologi che servono a definire il ritmo con il quale un cannone elettronico disegna orizzontalmente i pixels e quello con il ritmo di creazione di ciascuna riga.

Dicendo cannone elettronico si penserebbe che solo i monitor CRT sono soggetti a questo pericolo. Questo è sbagliato in quanto anche con i monitor LCD, grazie a un antenna, a un ricevitore è possibile ricostruire da distante le immagini che uno sta guardando sul video.

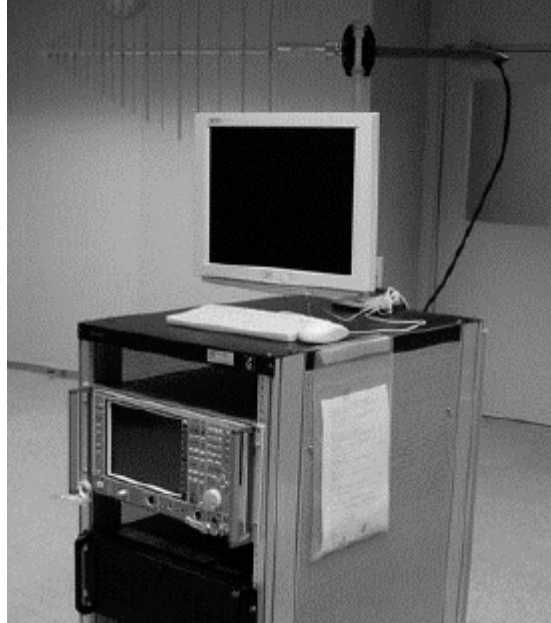


Il fenomeno venne studiato inizialmente da Erik Van Eck e descritto in un suo documento reperibile in rete intitolato : "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?".

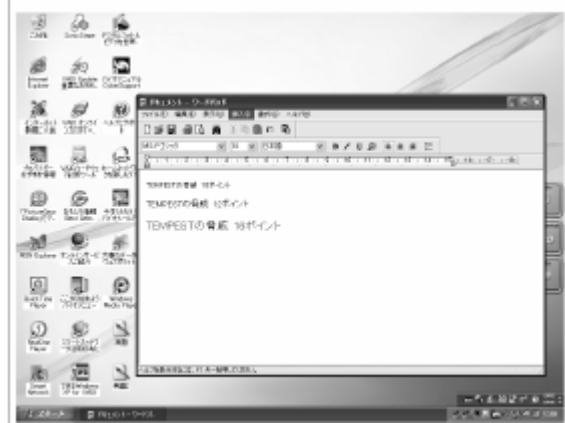
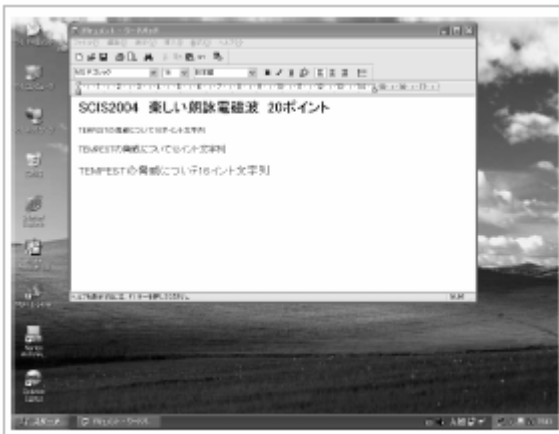
Il metodo per anni è stato tenuto sotto segreto militare e ancora adesso molte cose non rese pubbliche ma qualche anno fa un ricercatore giapponese, tale Tanaka, rese pubblico uno scritto in cui si mostrava che con meno di 2000\$ era possibile farsi in casa un ricevitore tempest.

Lo scritto si intitola : "A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave."

Il sistema usava un antenna direttiva e un analizzatore di spettro ma mostrando che anche con un ricevitore da radioamatore era possibile fare la stessa cosa.



Le immagini che seguono sono il risultato.



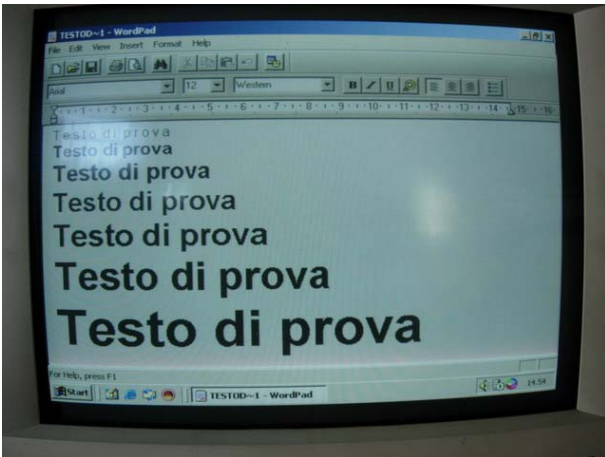
La prima è l'immagine vista con il sistema mentre la seconda l'immagine originale.

Considerate che questa immagine è stata 'vista' senza nessun collegamento, ne rete ne altro, con il computer originale.

Markus Khun del centro di ricerca sulla sicurezza dell'università di Cambridge ha redatto un volume di 300 pagine con dettagliate informazioni tecniche.

Il documento si chiama : UCAM-CL-TR-577.pdf

Questa è una prova fatta in casa dal sottoscritto, da una distanza di 10 metri attraverso un muro, grazie solo a un antenna e ad un analizzatore di spettro collegato a due oscillatori che generassero i sincronismi verticali e orizzontali .

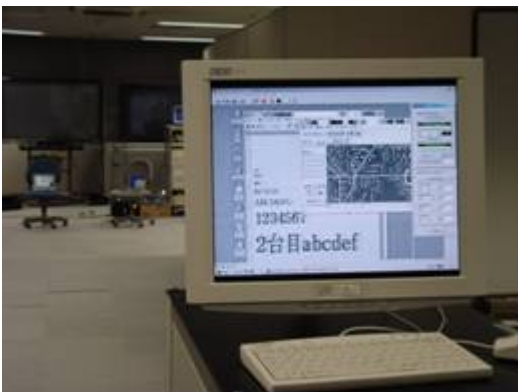


In genere gli alti costi per la creazione di un sistema d'intercettazione ha fatto sì che per anni il problema fosse ignorato.

La creazione di documenti in cui si vede come farselo in casa ha portato e cercare di identificare le soluzioni per la protezione anche se di fatto, se non previste prima, spesso sono difficilmente attuabili.

Il motivo di questa affermazione è che ad esempio l'effetto tempest coinvolge anche i cavi elettrici in quanto le emanazioni dei computer grazie a queste vengono convogliate fuori dagli edifici del sistema.

Le immagini si riferiscono a un test di intercettazione grazie ai cavi di alimentazione :



Le protezioni fondamentalmente sono legate alla creazione di locali schermati, all'uso di computer ANTITEMPEST o all'uso di mascheratori elettronici.

Un esperimento molto simpatico è TEMPEST FOR ELIZA.

In pratica all'indirizzo :

<http://www.erikyyy.de/tempest/>

è possibile prelevare un programmino LINUX al quale passandogli un file MP3 lo modula sul video.

Usando una normale radio AM/FM è possibile sentire il brano trasmesso grazie ai campi elettromagnetici del sistema.

Ogni trasmissione radio possiede una frequenza fondamentale che in questo caso è intorno ai 60 MHZ e delle oscillazioni armoniche sui multipli della frequenza della portante, con potenza sempre più bassa.

Le intercettazioni che si cercano di fare a 70 MHZ hanno il problema del grosso 'rumore radio ambientale' legato a cercapersone, radio private ecc.

Man mano che si sale in frequenza, verso il GHz, il segnale dell'armonica è molto più basso ma il rumore ambientale è inesistente per cui l'intercettazione può avvenire in modo molto migliore.

Molte volte un segnale CW pulitissimo di altissima potenza viene separato orientato verso il locale con i computer, magari molto distanti.

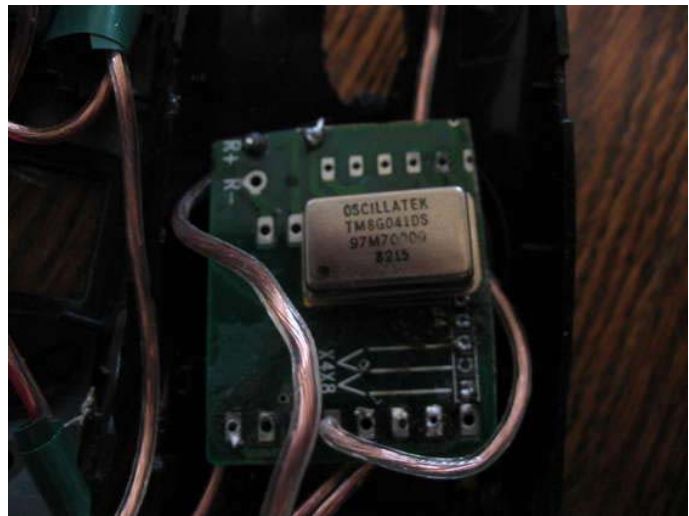
L'onda inviata incontrando il campo elettromagnetico dei computer modula la portante la quale riflessa torna indietro portandosi il segnale da visualizzare.

Ma queste sono tecniche molto più avanzate difficilmente attuabili dall'hacker casalingo.

I rischi delle nuove tecnologie comunque non si fermano a questo ma hanno colpito anche gli altri mezzi come ad esempio i cellulari.

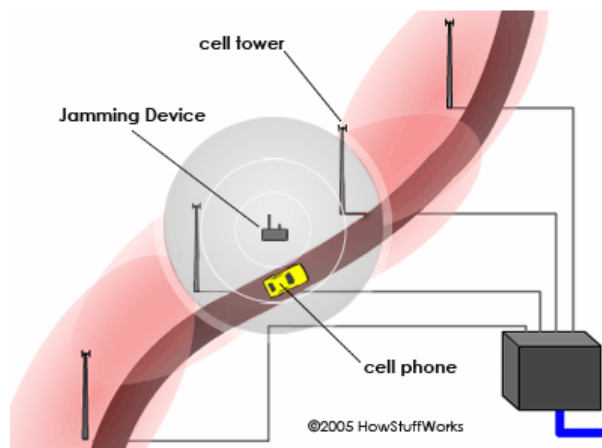
Sulla rete è possibile trovare schemi di Jammer, anche da taschino, che sono in grado di bloccare GSM e GPS.

Ad esempio molti tracciatori GPS antifurto possono essere bloccati con una spesa di poche decine di euro.



Il sistema emette disturbi che non permettono più ai cellulari e ai gps di comunicare con le cellule e con i satelliti, rendendoli quindi inutilizzabili.

Ricordiamoci che queste cose sono vendute a poco sulla rete pronte per l'uso ma grazie a schemi e



circuiti vari è possibile anche crearli in casa.

Intercettare i GSM/UMTS non è più cosa da centrale TELECOM ma con un sistema portatile è possibile farlo.



Il problema grosso è che la tecnologia corre e si è dimenticata di una cosa : per non fare sentire un informazione non si deve gridarla per la strada.

Questo è il principio di tutto quello che funziona via radio.

Ne è un esempio la rete WIRELESS.

Grazie a sistemi di codifica dei dati posso rendere difficile decodificare le informazioni trasmesse ma grazie a un sistema dotato di un oscillatore e di un amplificatore di RF posso fare in modo che tutto vada in TILT.

Prendiamo ad esempio un sistema di video sorveglianza fatto con videocamere WIRELESS a 2.4 GHZ.

Vado al supermercato e compro un trasmettitore di segnali TV e RADIO e lo collego a un amplificatore di segnale da 5 W dopo di che lo nascondo vicino alla ditta alla quale voglio disturbare il sistema di sorveglianza.

Basta ... non c'è altro da dire ... non si vedrà più nulla grazie al disturbo.

La stessa cosa può essere estesa a tutto ciò che funziona via radio come RFID, bluetooth, cellulari.

I danni del bluetooth con il quale sono stati trasmessi virus sono a conoscenza di tutti.

RFID è stato riportato come uno dei piloni della sicurezza futura senza considerare che :

- può essere coperto da un segnale radio forte
- è stato decodificato
- è stato copiato
- può essere intercettato
- può essere bruciato grazie al campo elettromagnetico emesso dal meccanismo smontato del flash di una foto camera usa e getta.

Qualche anno fa provammo a fare un esperimento.

Collegammo un oscillatore a 125 KHZ a un vecchio amplificatore audio PIONEER da 100W con risposta in frequenza da 10HZ a 100KHZ.

Poi attorno a una cassetta in plastica della frutta arrotolammo 100 metri di cavo elettrico usato come antenna.

Nel giro di 20 metri non era più possibile usare un RFID in quanto tutti erano diventati sordi grazie al forte segnale di copertura.

Ora pensate che molti sistemi antitaccheggio dei supermercati funzionano grazie a questi.

Con una macchina posteggiata fuori da questo con il sistema accesso l'antitaccheggio andrebbe in tilt non rilevando più nulla.

Ma lasciando stare circuiti per il bloccaggio di massa esistono sistemi che permettono di disabilitare ogni singolo RFID e quindi di uscire con la merce in mano senza che l'antifurto suoni.

Tutti sanno che i circuiti elettronici sono sensibili ai campi elettrostatici i quali li danneggiano.

Come creare un piccolissimo generatore di cariche statiche che avvicinate ai chip del sistema antitaccheggio lo brucia rendendolo sordo ?

Prendete una macchina fotografica usa e getta Kodak, ad esempio, con FLASH.



Usatela e poi prima di buttarla smontatela mettendo a vista il circuito che manda la scarica al FLASH.



Togliete la lampada del FLASH e al suo posto collegate una matassa di cavo elettrico in modo da fare una bobina.

Quando vorrete bruciare il CHIP basterà avvicinare la bobina a questo e premere il pulsante di scatto fotografia.

La scarica originariamente destinata al FLASH arriverà alla bobina creando un campo elettrostatico talmente forte da danneggiare RFID dell'antitaccheggio.

Per decrittare RFID un università ha scritto in VHDL, un linguaggio per creare progetti elettronici, l'algoritmo e con questo ha creato un chip su FPGA.

Poi ha messo in parallelo 50 schede e queste lavorando in collaborazione hanno decrittato l'algoritmo a 40 BITS della TEXAS.



Sempre rintracciabili in rete ci sono delle serie di prodotti, fattibili facilmente in casa, grazie ai quali la propria privacy andrebbe a farsi un giro.

Ad esempio grazie a un puntatore laser e a pochi altri componenti è possibile costruirsi un microfono laser grazie al quale è possibile sentire le micro vibrazioni dei vetri delle case dovute al nostro parlare al loro interno.



Oppure sono venduti dei KIT per trasformare un cellulare con videocamera in uno strumento di spionaggio automatico.

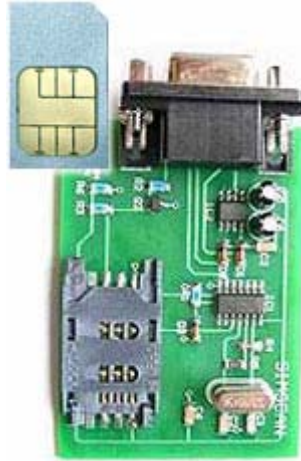
In altre parole aggiungendo un illuminatore all'infrarosso, luce non visibile dall'occhio umano, e un rilevatore di movimento si ottiene che ogni volta che una persona passa davanti al cellulare questo chiama un numero trasferendo le immagini visualizzate dall'obbiettivo.

Inoltre è anche possibile chiamare il telefono per ottenere la stessa funzione.

Ad ogni modo con le nuove tecnologie ce n'è per tutti i gusti anche grazie alle facilitazioni commerciali dovute al fatto che ormai si trova tutto e di più.

Una volta clonare una SIM era un lavoro da esperto.

Oggi si compra il KIT in scatola di montaggio.



Il problema è che i gestori della sicurezza devono iniziare ad ampliare gli orizzonti in quanto questa non è più solo in mano a firewall e router.

Il problema non è tanto le soluzioni che dovrebbero adottate grazie a contromisure elettroniche ma semplicemente il fatto di avvertire gli utenti perché facciano attenzione ai loro sistemi elettronici.

Insegnare a guardare dietro a un computer per vedere se c'è un extender KVM non è un metodo costoso come non lo è il sistema di fare guardare la linea telefonica da parte del benzinaio per vedere se tra il POS e la presa non ci sono oggetti non originali.

L'ignoranza spesso è il peggior nemico dei problemi di sicurezza in quanto una volta conosciuti i metodi il controllo è spesso veramente semplice.

D'altra parte l'elettronica va sempre più avanti.

Una volta a fare una microspia ci andavano molti componenti.

Guardate un chip che fa tutto ovvero un trasmettitore FM completo, paragonato a un a quarto di dollaro.



La reti ormai sono troppo blindate per usarle per arrivare alle truffe : però basta usare le porte laterali !