

GLI STRUMENTI HIGHTECH DEL GRANDE FRATELLO. Flavio Bernardotti – Ottobre 2007

Al giorno d'oggi termini come DNA ci risultano famigliari in quanto la stampa ne parla in continuazione sia per quanto che riguarda le tecnologie indirizzate a modificarlo che relativamente a problemi i tipo filosofico legati al fatto di considerare giuste o sbagliate queste tipologie di attività.

Il problema di fondo è che comunque le nuove tecnologie ci stanno fornendo un numero sempre maggiori di 'marcatori' che permettono di identificare e catalogare le nostre attività, i nostri usi e consumi.

Sto parlando di marcatori trasparenti che spesso non sappiamo neppure di avere ma che persone a conoscenza di questi possono usare per fini che non sempre sono utili e indirizzati a garantire la nostra sicurezza.

Da una certo punto di vista le tecnologia crea certi sistemi che in teoria dovrebbero disporre della caratteristica di aiutarci e proteggerci ma che di fatto molte volte potrebbero essere ritorcersi contro di noi.

Il fatto che grazie a carte di credito e bancomat sia possibile vedere i nostri gusti, i nostri consumi e anche i posti da noi frequentati era risaputo, solo che fino a poco tempo fa tali informazioni erano solo di proprietà delle banche e dei servizi interbancari.

Oggi internet ha ingigantito l'uso della moneta elettronica e quindi le nostre tracce molte volte cadono in mano a ditte non molto serie le quali le utilizzano per scopi non propri del mezzo di pagamento.

Non parlo di truffe in quanto quelle, grazie alle tecnologie HIGHTECH, sono possibili da tutte le parti e non solo su rete, ma di informazioni legate alle nostre abitudini commerciali.

Ma di quali altri marcatori stiamo parlando ?

Per fare un esempio possiamo riportare quel microscopico microchip che utilizza per alimentarsi l'onda radio del sistema di rilevazione e che quindi può essere inserito in schede, banconote e in altri sistemi che possiedono l'esigenza di essere identificati mediante strumenti di prossimità.

Questi chip sono conosciuti con il termine di RFID e fanno parte del nostro quotidiano più di quanto possiamo immaginare.

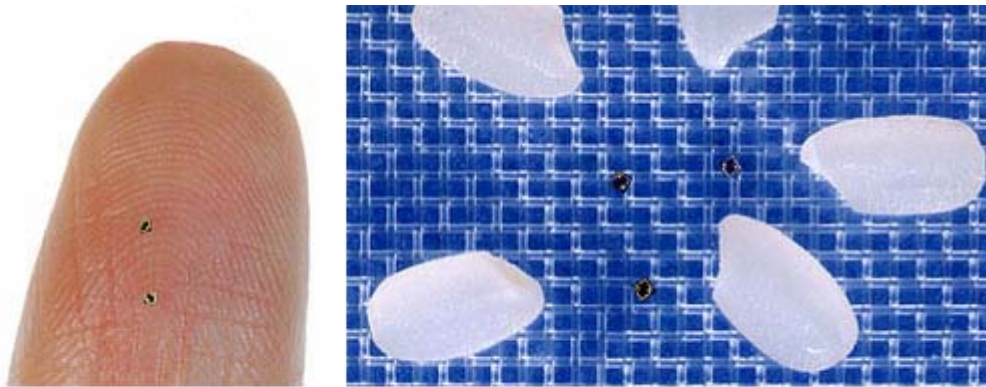
Sistemi antitaccheggio per negozi e supermercati, carte di credito, sistemi di identificazione e tantissimi altri sistemi come ad esempio il sistema antifurto presente in molte vetture chiamato CODE, presente dentro alla chiave di accensione.

Fino a qualche anno fa le dimensioni erano già ridottissime ovvero circuiti di circa 2 x 2 mm.

L'anno scorso mi è arrivato in ufficio un pacchettino con dentro una provetta piccolissima con dentro del liquido bianco spedito da Hitachi.

Guardandola la prima cosa che ho pensato è stata quella che Hitachi mi aveva spedito a scopi pubblicitari un campioncino di profumo, ma poi guardando meglio ho notato tanti piccoli puntini neri adagiati sul fondo.

Si trattava di 25 RFID microscopici.



A New RFID with Embedded Antenna μ -Chip

Eventuale link da mettere al posto immagine :

<http://radio.weblogs.com/0105910/images/hitachirfid.jpg>)

In america questi RFID sono inseriti dentro a delle banconote di grosso taglio mentre qui in europa la Banca Europea aveva intenzione di fornire i tagli superiori ai 50 € con lo stesso sistema.

Lo scopo ufficialmente sarebbe quello della semplificazione delle operazioni di tracciamento del denaro legato a certe attività ma di fatto il loro utilizzo costituirebbe un altro marcatore che teoricamente potrebbe permettere a una persona di sapere se in tasca possediamo banconote di taglio da 100 € in su.

Un altro esempio sono i telefoni cellulari i quali costituiscono il nostro tracciatore personale.

Quando ci muoviamo i nostri telefonini rimangono in collegamento con un punto d'accesso alla rete telefonica grazie a informazioni trasmesse via radio.

Questi punti sono quelli che sono definiti con il termine di 'cellule'.

Tutte le cellule colloquiano tra loro definendo quale tra loro sono quelle più adatte a mantenere il collegamento con un certo telefono cellulare.

Queste tracce sono correvate dentro ai sistemi del gestore della rete per cui se a seguito di indagini la magistratura volesse sapere gli spostamenti di una persona in un certo giorno e ad una certa ora sarebbe sufficiente che consultasse i tabulati del gestore.

In questo caso sarebbe la magistratura a possedere certe informazioni e quindi a meno che la persona non abbia qualche cosa da nascondere la cosa non dovrebbe costituire un grosso problema.

Le nuove tecnologie hanno permesso di analizzare i dialoghi tra le cellule e i telefoni cellulari permettendo di conoscere le persone presenti in una certa zona anche da parte di persone non autorizzate.

Questo sistema è alla base di apparecchiature di sicurezza indirizzate a impedire le comunicazioni cellulari a certi numeri.

Il problema è che la commercializzazione di certe tecnologie ha permesso anche a persone non autorizzate di conoscere determinate informazioni.



Anni fa gli americani nella loro corsa alle tecnologie militari creò degli enormi database basati su certi concetti legati all'identificazione di tutte quelle che erano le emissioni involontarie da parte di meccanismi e apparecchiature elettroniche come suoni e campi elettromagnetici.

Ad esempio i motori di certi sommergibili creavano rumori che captati permettevano di sapere la tipologia di questi.

Tutti gli strumenti elettronici funzionano elaborando segnali che viaggiano con temporizzazioni particolari determinate da orologi, clock, interni.

In altre parole anche i sistemi elettronici possiedono un 'aura' che captata da distanti con antenne e ricevitori permettono di sapere che tipo di apparati sono presenti in un locale.

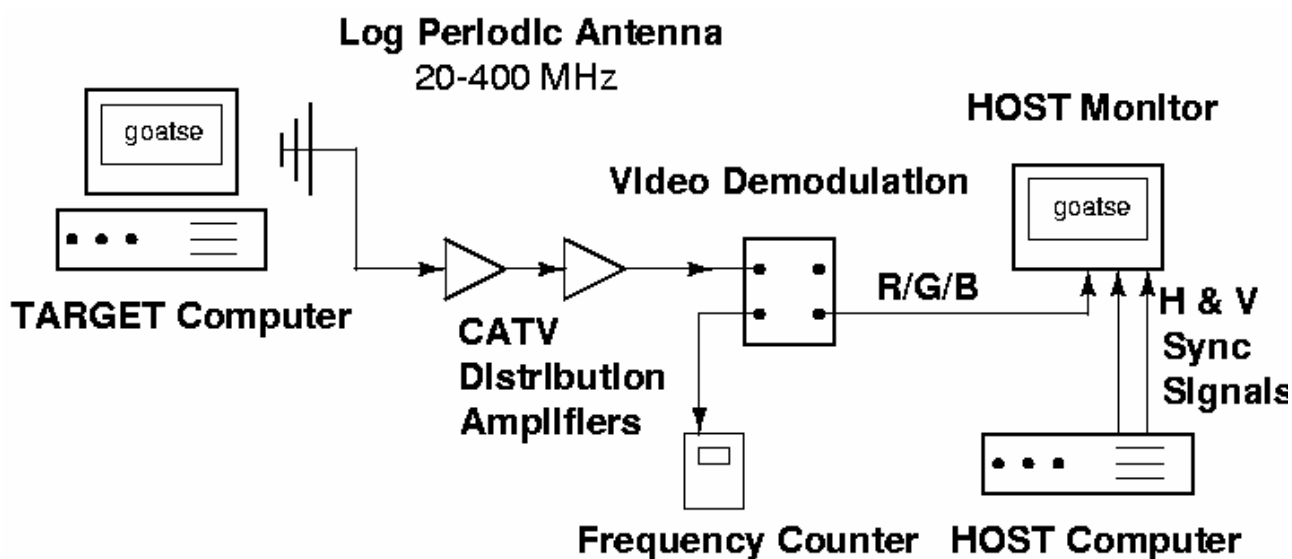
Ma la cosa più sorprendente è che grazie a queste emanazioni elettromagnetiche è possibile da distanze rilevanti vedere cosa stiamo facendo su computer, fax e strumenti di visualizzazione delle informazioni.

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.

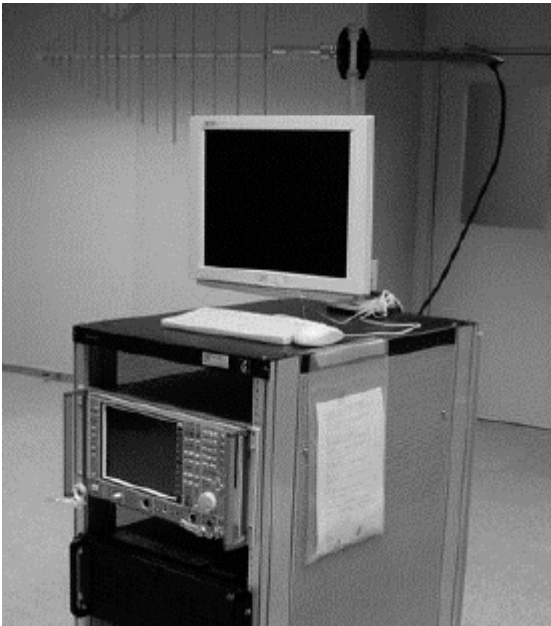


Il fenomeno venne studiato inizialmente da Erik Van Eck e descritto in un suo documento reperibile in rete intitolato : "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?".

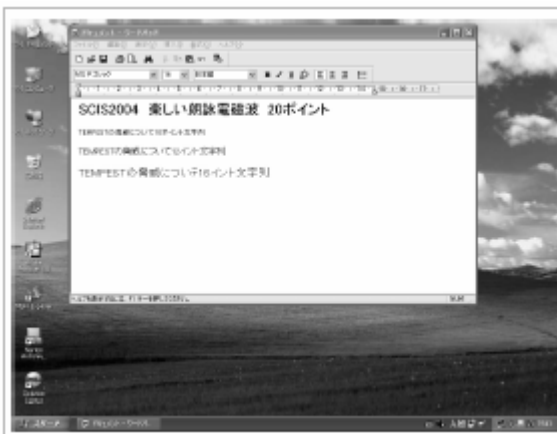
Il metodo per anni è stato tenuto sotto segreto militare e ancora adesso molte cose non rese pubbliche ma qualche anno fa un ricercatore giapponese, tale Tanaka, rese pubblico uno scritto in cui si mostrava che con meno di 2000\$ era possibile farsi in casa un ricevitore tempest.

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

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 :



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.

D'altra parte i sistemi informatici stanno contribuendo a creare questi marcatori finalizzati al tracciamento della popolazione.

Londra ad esempio dispone di circa 9000 videocamere con sistemi d'identificazione automatica ufficialmente utilizzati per l'antiterrorismo ma che di fatto seguono passo a passo qualsiasi persona. Questi erano solo alcuni esempi che volevano testimoniare il fatto che l'accettazione di molte comodità offerte dall'evoluzione dell'High Tech spesso possono avere degli effetti collaterali.

Il grosso problema è che l'uomo è sempre vissuto in un mondo a cavallo tra il bene e il male e quindi il fatto di cercare di convincere la gente che una tecnologia ha solo effetti positivi è veramente utopistico.

Qualsiasi cosa che entra a far parte del nostro mondo possiede un lato e il suo opposto.

Lo Zen ci insegna che nel mondo c'è la luce e buio, uomo e donna, suono e silenzio, buono e cattivo.

Le tecnologie non possono sottrarsi a queste regole e quindi sta a noi valutare se accertarle o meno.

Il problema è che la commercializzazione selvaggia spesso non informa pienamente sulle controindicazioni di certi prodotti e quindi le persone le usano tranquillamente.

Questo articolo non vuole assolutamente avere un carattere allarmistico in quanto spesso anche le cose che vengono descritte con aggettivi non positivi è sufficiente conoscerle per poterle sfruttare per quello che sono state create.