PREMESSA: Diciamo subito che è un racconto di fantasia così stiamo tutti tranquilli...

Spionaggio di stato da parte degli stati Uniti d'America: metodi ed evoluzione degli stessi dagli anni '70 ad oggi. E come il mondo si difende (o almeno ci prova).

ESEMPIO

USA (CATTIVI)

- Metodo “by Law”

La crittografia era equiparata ad arma da guerra: non si potevano esportare algoritmi crittografici “forti” e la lunghezza delle chiave era imposta a 40 bit: (**leggi: gli USA già disponevano di computer abbastanza potenti per scardinare chiavi a 40 bit in poco tempo**).

- Metodo “by math”

Tramite “spinte” governative, l'algoritmo DES, originariamente con chave a 64 bit, fu portato a 56 bit. Si scoprì in seguito che benchè l'algoritmo fosse apparente robusto, ricorrendo a matematica specialistica, lo si poteva “forzare”. **(leggi: i matematici al soldo dell'NSA, NEL CAMPO DELLA CRITTOGRAFIA, erano più avanti di tutti i dipartimeti Universitari di matematica del mondo.)**

MONDO (BUONI)

- Metodo “by math”

Negli USA, viene sviluppato l'algoritmo PGP, che impedisce un attacco a “forza bruta” in tempi umani, ma e' una “arma da guera”.... come salvarsi dalla galera, da parte dello sviluppatore?

- Metodo “by law”

Lo sviluppatore del software STAMPA l'algoritmo e lo deposita presso la Biblioteca Nazionale Statunitense: gli scritti sono protetti da uno degli emendamenti e i caporioni NSA sono costretti a denti stretti a fare retromarcia ma non la prendono bene... (lo sviluppatore, pur evitando la galera, avrà comunque dei grattacapi da parte dei galantuomini del Governo)

SPIONAGGIO INTERNAZIONALE

https://it.wikipedia.org/wiki/Echelon

Rete di spionaggio composta da Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti, noto come AUSCANNZUKUS o cinque occhi). Echelon è stato anche descritto come l'unico sistema software che controlla il download e la diffusione della intercettazione di comunicazioni via satellite.

PERCHE' LO SPIONAGGIO??
I MOTIVI DI FACCIATA

Terrorismo

Predatori sessuali

SEI UN COMPLOTTISTA PARANOICO!!!

MA ANCHE NO!
Vediamo cosa dicono le direttive del PARLAMENTO EUROPEO
al capitolo 10 di
http://www.privacy.it/ueechelon.html

10.9. Gli USA e lo spionaggio dopo la guerra fredda

Dopo il 1990 il governo americano tende sempre più a mettere sullo stesso piano la sicurezza economica e la sicurezza nazionale. La relazione annuale della Casa bianca "National Security Strategy" 214 sottolinea ripetutamente che "**la sicurezza economica costituisce una parte integrante non soltanto degli interessi nazionali ma anche della sicurezza nazionale**".

PERCHE' LO SPIONAGGIO??
I MOTIVI VERI: CONTROLLO = SOLDI

Caso	Chi	Quando	Cosa	Come	Obiettivo	Conseguenze
Air France	DGSE	fino al 1994	Conver- sazioni di uomini d'affari in viaggio	Nelle cabine di prima classe di Air France sono nascoste alcune comici — La compagnia aerea ha presentato pubblicamente le proprie scuse	Raccogliere informa- zioni	Non comunicate
Airbus	NSA	1994	Informazioni sugli affari tra Airbus e la linea aerea arabo-saudita	Intercetta- zione di fax e telefonate tra i partner	Passare informa- zioni ai concorrenti statuni- tensi Boeing e Mc- Donnell- Douglas	Gli americani concludono l'affare da 6 miliardi di dollari
Airbus	NSA	1994	Contratto di oltre 6 miliardi di dollari con l'Arabia Saudita Corruzione del gruppo europeo Airbus.	Intercetta- zione di fax e telefonate tra il gruppo europeo Airbus e la compagnia aerea/il governo sauditi tramite satelliti per le comunica- zioni	Scoprire casi di corruzione	McDonnel- Douglas, il concorrente statunitense di Airbus, conclude l'affare
BASF	Vertrie bsmann	Non comunicato	Descrizione di processi per la produzione di materie prime per creme per la pelle della società BASF (settore della cosmesi)	Non comunicato	Non comunicato	Nessuna, perché tentativo sventato
Ministero federale dell' Economia (Germania)	CIA	1997	Informa- zioni su prodotti di alta tecnologia nel ministero federale dell' Economia	Impiego di un agente	Raccogliere informa- zioni	L'agente viene scoperto nel tentativo di agire ed espulso

PERCHE' LO SPIONAGGIO??
I MOTIVI VERI: CONTROLLO = SOLDI

MERCOLEDÌ 1° LUGLIO 2015

NSA ha monitorato l'economia francese

Ulteriori rivelazioni raccolte da Wikileaks svelano come nel mirino delle spie statunitensi ci fossero anche le aziende francesi, le loro strategie, e le politiche economiche secondo cui sono state amministrate tra il 2004 e il 2012

Roma - Si allarga l'elenco dei bersagli dell'intelligence a stelle e strisce in Francia: oltre ai politici sarebbero finiti nelle intercettazioni anche le principali aziende del paese.

A riferirlo sono le nuove indiscrezioni divulgate da Wikileaks, ospitate da Libération e Mediapart, che ancora una volta fanno luce sulle operazioni condotte dagli agenti statunitensi della National Security Agency (NSA): questi non si sarebbero, dunque, limitati a spiare rappresentanti del potere politico come divulgato la scorsa settimana, ma avrebbero anche attivato un servizio di sorveglianza ai danni di imprenditori locali.

Secondo i documenti riservati divulgati, cinque in tutto, tra il 2004 ed il 2012 la NSA avrebbe messo in pratica un piano ben preciso per carpire la strategia adottata dalla Francia per lo sviluppo economico. Nel faldone dei dati raccolti da NSA, dunque, sarebbero finite le conversazioni tra Parigi e gli istituti finanziari internazionali, le bozze preparatorie per G8 e G20 ed i grandi contratti commerciali adottati dal paese con le sue principali aziende, tutte quelle cioè con un fatturato superiore ai 200 milioni di dollari.

Mentre nel caso dei politici le informazioni sembravano essere utilizzate ai fini dell'intelligence diplomatica, le intercettazioni delle aziende non possono che configurarsi come vero e proprio spionaggio industriale: gli Stati Uniti, insomma, sembrano essersi comportati proprio come se fossero in guerra con la Francia.

http://punto-informatico.it/4255394/PI/News/nsa-ha-monitorato-economia-francese.aspx?o=0&ct=0&c=1#p4255978

NAZIONI UNITE PARANOICHE? NO.

Tecnocontrollo, Nazioni Unite per la cifratura

L'ONU redige un rapporto in difesa delle tecnologie per la cifratura dei dati e dell'anonimato, con un'apertura in corner sull'intervento circostanziato delle autorità governative. USA e UK vogliono le backdoor

email

Roma - Il Consiglio per i diritti umani delle Nazioni Unite ha pubblicato un rapporto sulla promozione e la protezione del diritto alla libertà di opinione e di espressione, uno studio che affronta in maniera frontale la spinosa questione delle tecnologie crittografiche e il tentativo dei governi nazionali di "indebolire" i suddetti sistemi per sorvegliare gli utenti.

La prima conclusione del rapporto dell'ONU è chiara: crittografia e anonimato garantiscono la privacy e la sicurezza "necessarie" per la libertà di espressione nell'era digitale. Si tratta di sistemi potenzialmente essenziali, e vista la loro importanza le restrizioni all'uso della cifratura devono essere "strettamente limitate" in accordo con i principi di legalità, necessità, proporzionalità e legittimità degli obiettivi.

http://punto-informatico.it/4249396/PI/News/tecnocontrollo-nazioni-unite-cifratura.aspx

FIFI: TEORIA E PRATICA

“FIFI”
non è il nome di un gattino famoso su Youtube ma sta per:

- Fretta
  - Ignoranza
    - Faciloneria
      - Incompetenza

La scarsa importanza annessa alla sicurezza delle imprese nella gerarchia aziendale porta, unita alle insufficienti conoscenze dei decisori in materia di sicurezza, a decisioni inopportune.

SMARTPHONE? ALLA LARGA!

martedì 5 dicembre 2006

A+ A-

Commenti (105)

FBI spia attraverso cellulari spenti

Quando il romanzo di genere incontra la realtà: i federali avrebbero trovato il modo di servirsi dei cellulari di due membri di un clan mafioso per ascoltare le loro conversazioni. Lo hanno detto in tribunale

email

Washington - La lotta alla mafia italo-americana, nella visione del Federal Bureau of Investigation, passa per **l'utilizzo di tecnologie all'avanguardia** in grado di dribblare la proverbiale ritrosia dei *mobs* e fornire il materiale adeguato per le investigazioni e le incriminazioni. È quello che emerge dalle recenti cronache giudiziarie statunitensi: un giudice distrettuale ha approvato un sistema di intercettazione definito *cimice vagante*, grazie al quale i federali sarebbero riusciti ad ascoltare le conversazioni di due noti mafiosi usando i loro cellulari come microfoni ambientali.

http://punto-informatico.it/1797437/Telefonia/News/fbi-spia-attraverso-cellulari-spenti.aspx?c=3&o=0&ct=0#p1797931

IO NON HO NULLA DA NASCONDERE!

"Chi non ha nulla da nascondere non ha nulla da temere".

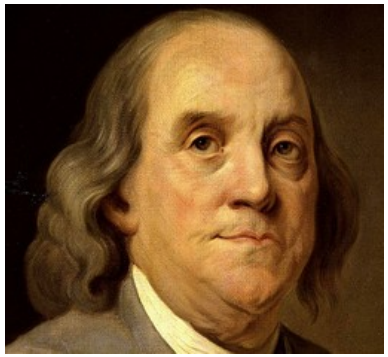
Joseph Goebbles

Ministro della Propaganda del Terzo Reich 1926-1945

"Datemi tre righe scritte dal più onesto degli uomini e vi troverò un motivo per farlo impiccare".

Cardinale Richelieu

Primo Ministro di luigi XIII di Francia

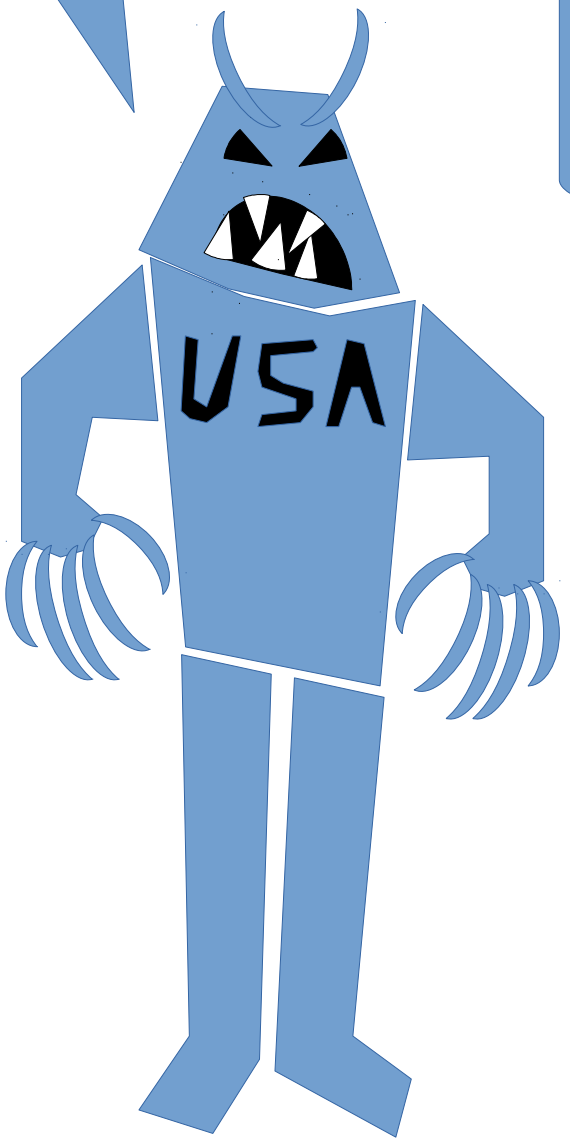


"Chi è disposto a rinunciare alle proprie libertà fondamentali per briciole di temporanea sicurezza non merita né le une né le altre.

Benjamin Franklin

Scienziato, Padre Fondatore Degli stati uniti D'america

SPIARE E' COMPLESSO...



LE PIU' GRANDI IMPRESE INFORMATICHE SONO STATUNITENSI: CONTROLLANDO LORO, CONTROLLEREMO CHI USA I LORO PRODOTTI

Coproration U.S.A.

- MICROSOFT
- APPLE
- CISCO
- GOOGLE
- ORACLE
- ...
- ...

Droga - fidelizzazione cliente: prima dose, gratis!

Windows 10 - fidelizzazione cliente: primo anno, gratis!

IL FUTURO DI WINDOWS? CLOUD!!

Roma - Windows 10 arriverà entro l'estate, ma solo su PC: lo conferma Joe Belfiore, vicepresidente Microsoft e responsabile del design della versione mobile del sistema operativo al centro della nuova strategia tutta cloud, advertising e servizi ad abbonamento della corporation di Redmond.

Sui dispositivi diversi dai PC, ha spiegato Belfiore, Windows 10 farà la sua comparsa nei mesi successivi al lancio della versione dell'OS per computer; HoloLens, Xbox, Surface e gadget mobile saranno interessati da una successiva ondata di lanci "scaglionati" del sistema Windows di nuova generazione, ha riferito il dirigente.

Utenti e mercato devono poi abituarsi alla nozione di "Windows come servizio", sostiene il manager, perché l'OS verrà aggiornato con nuove e importanti funzionalità anche dopo il lancio. In concreto, l'affermazione di Belfiore descrive un Windows 10 monco di alcune delle caratteristiche sin qui presentate al pubblico (come il supporto alle estensioni HTML5/JS del browser Edge, per esempio) e la loro implementazione come update incrementali in un momento successivo.Certo è che un Windows 10 "come servizio" presta il fianco a più di un dubbio sulle intenzioni di Microsoft per il prossimo futuro, con nuovi episodi inquietati come l'aggiornamento "consigliato" di Windows 7 pensato esclusivamente per pubblicizzare l'uscita della versione RTM di Windows 10 a tempo debito.

Un Windows 10 "come servizio", anche considerando l'offerta di aggiornamento gratuito valida per un anno, potrebbe secondo alcuni osservatori, veicolare advertising, adware o pretendere dall'utente il pagamento di una somma mensile a mo' di abbonamento.

http://punto-informatico.it/4244232/PI/News/windows-10-cosa-come-quando-quanto.aspx

Il grande fratello: versione “a colori”

Samsung

Perché un televisore (che dovrebbe solo ***dare*** informazioni) ha una connessione ad internet 24/24 e ha una telecamera e microfono (che ***prendono*** informazioni?)

SAMSUMG A BRAGHE CALATE (e due!)

TROVATA BACKDOOR NEL SAMSUNG GALAXY

Unveiling the Samsung Galaxy back-door

Posted on March 13, 2014 by Paul Kocialkowski

Yesterday, we disclosed our findings about the Samsung Galaxy back-door, **an anti-feature found in Samsung Galaxy devices that lets the modem access the files stored on the device**. For a complete statement about the issue, you can refer to the article we published at the Free Software Foundation's website. A technical description of the issue is available on a dedicated page of the Replicant wiki, along with more information regarding the back-door.

The information spread out very quickly and we're glad the
matters as privacy and unjust control over one's computin
time why free software is essential and how a single piece
compromise a whole device.

We have yet to hear from Samsung about this issue, as w
presence of this back-door will be clarified. In that regard,
Samsung in order to make things right, for instance throug
documentation that would make it easy for community And
incriminated blob.

una caratteristica "malvagia" trovata nei Samsung Galaxy permette al modem di accedere ai file dell'utente

RISPOSTA DI SAMSUNG (IN SINTESI): NON E' UN PROBLEMA NON PREOCCUPATEVI. PERO' IL CODICE SORGENTE NON VE LO FACCIAMO VEDERE; FIDATEVI DI NOI.

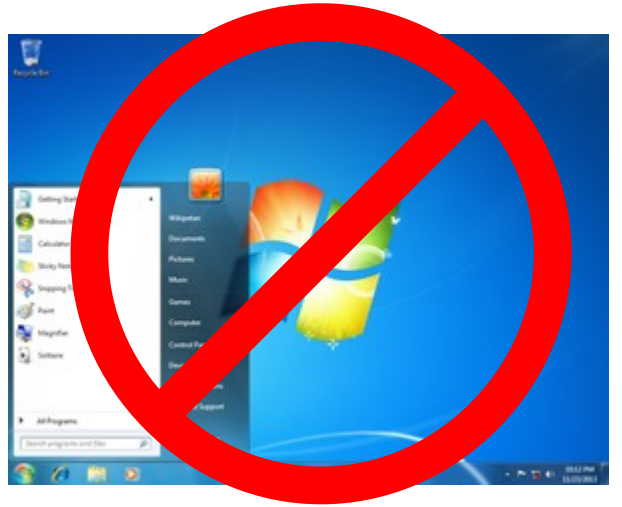
FONTE: http://blog.replicant.us/2014/03/unveiling-the-samsung-galaxy-back-door/

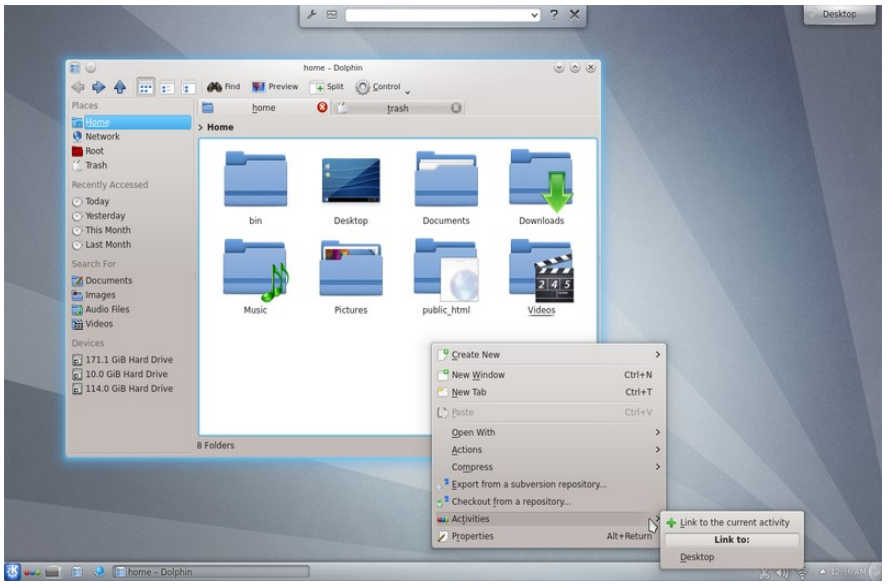
REAZIONE: GPL

Usare sistemi liberi (es: GNU/Linux) al posto di windows e OSX

<== OSX

Windows ==>





<== GNU/Linux

GNU/Linux è un sistema maturo in grado di soddisfare le esigenze dell'utente medio con migliaia di programmi per tutte le necessità, disponibili LIBERAMENTE senza vincolo d'uso.

DOMINARNE UNO PER CONTROLLARE TUTTO

TELEFONATE

MAIL

RETI SOCIALI

RUBRICA CONTATTI

SMS

SKYPE

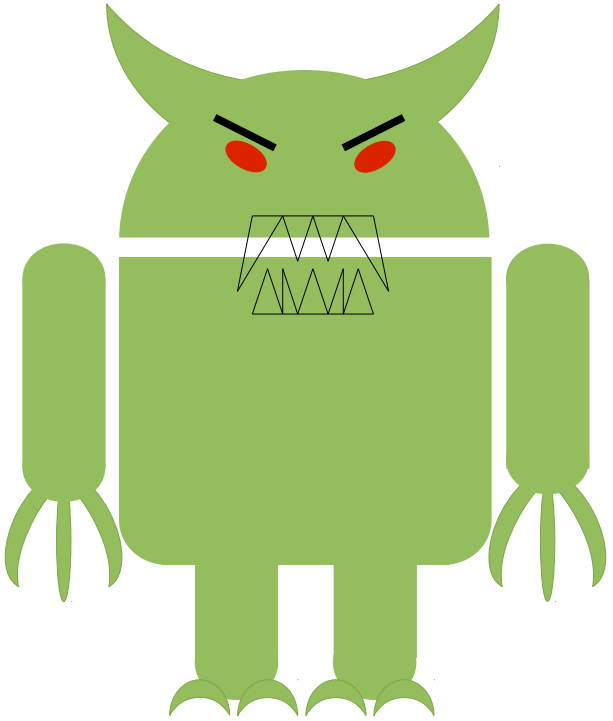
NAVIGAZIONE WEB

Fonia: alternativa

Replicant (**WWW.REPLICANT.US**) è una versione di Android completamente “ripulita” che mette al primo posto la Libertà dell'utente e il rispetto della sua Privacy e la Sicurezza Informatica.

traduzione:

REPLICANT = ANDROID – SCHIFEZZE DI GOOGLE/SAMSUNG/ECC



Android: MALVAGIO

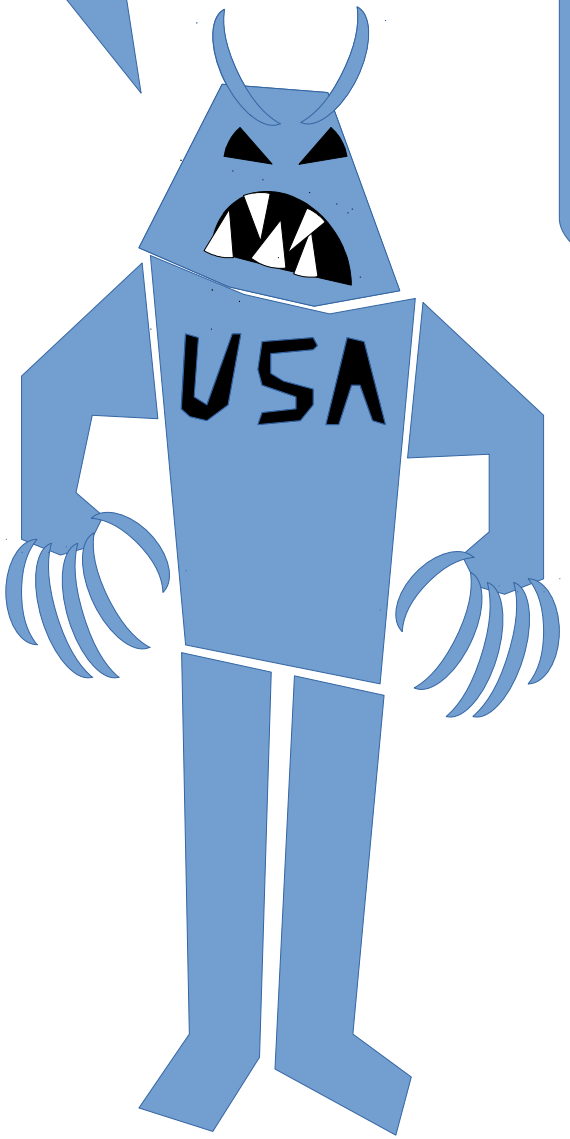
Replicant: BUONO

(ma insufficiente!!!)

Oppressione 1.0 (coatta)

Difetti: costosa e di gestione complessa

DOMINARE
E' COSTOSO...



NON SERVE OPPRIMERE I CORPI QUANDO PUOI CONTROLLARNE LE MENTI: FAREMO IN MODO CHE LA GENTE DESIDERI ESSERE SPIATA, SARANNO LORO STESSI A DIRE COSA FANNO!

“ESPLOSIONE” DEI SOCIAL

- Facebook
- Instagram
- Linkedin
- Ecc

Se non sei in “Rete”, non sei nessuno!

Oppressione 2.0 (indotta)

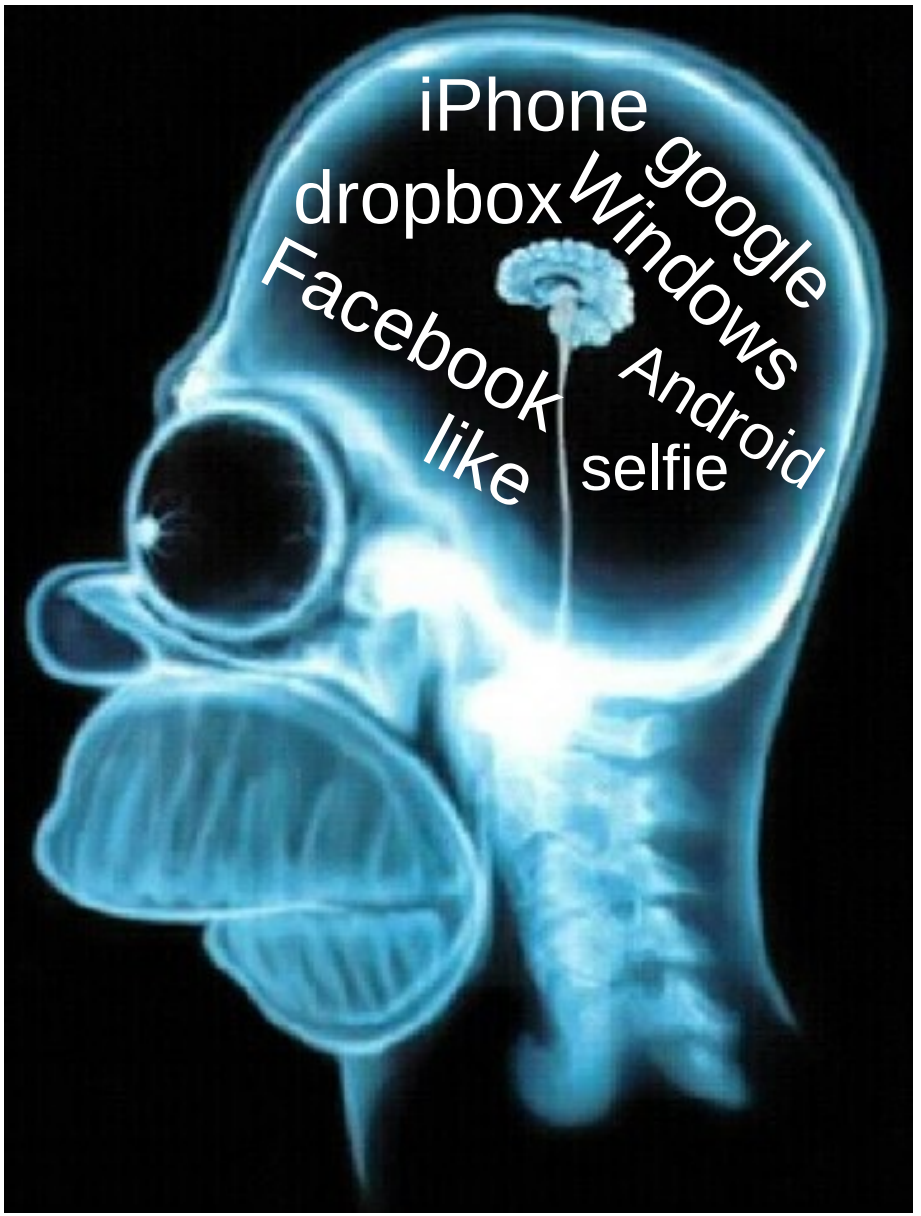
VANTAGGI: sono le stesse vittime a chiedere di entrare nel recinto e, per farlo, fanno la fila e PAGANO pure!

Capo di bestiame “umano” FELICE di aver comprato la sua nuova catena!

PRIVACY ZERO
ovvero:
L'EQUAZIONE DEL DISASTRO

SMARTPHONE + DUMB USER = KABOOOM!!

TIPICO UTENTE “SOCIAL”



GIA' DOMINO SU WINDOWS 10, IPHONE, GMAIL, RETI SOCIALI.. MA IL CONTROLLO DEL SOLO “LATO SOFTWARE” ANCORA NON MI BASTA, DEVO AVERE IL DOMINIO TOTALE DI OGNI SISTEMA CONNESSO ALLA RETE INDIPENDENTEMENTE DAL SISTEMA OPERATIVO CHE CI GIRA SOPRA!

PADRONE, COMANDA E SARA' FATTO: OGNI TUO DESIDERIO E' UN ORDINE PER IL TUO UMILE SERVO

IL NEMICO IN CASA

Il Sistema ME (presente in *OGNI* cpu INTEL dal dual core in poi) e' una cpu a 32 bit INDIPENDENTE dalla cpu principale ed e' dotato di un proprio sistema operativo che puo controllare TUTTO quello che l'utente fa.

In altre parole, il sistema ME agisce ad un livello hardware talmente basso da essere irraggiungibile dal sistema operativo della cpu principale ed e' in grado di by-passare QUALUNQUE controllo del sistema operativo “utente”, qualunque esso sia.

IDC: grattacapi per la NSA

NSA pensa al tecnocontrollo delle Cose

IoT? Biotech interconnesso? Per l'intelligence USA rappresentano la nuova frontiera dello spionaggio tecnologico, anche se al momento si parlerebbe ancora di studi di fattibilità più che di infrastrutture di controllo concrete

Roma - Dalla National Security Agency (NSA) continuano ad arrivare segnali sulle prospettive del tecnocontrollo di nuova generazione, una generazione che a quanto pare andrà a braccetto con la Internet delle Cose (IoT) e, peggio ancora, con gli apparati biomedicali ad alto contenuto di hi-tech.

L'intelligence statunitense è a dir poco interessata alle potenzialità della IoT in fatto di raccolta di informazioni e spionaggio a danno degli utenti, il fatto è ben noto ed è già stato candidamente ammesso dal direttore di NSA James Clapper davanti al Comitato sui servizi del Senato USA.

A rimarcare le potenzialità della IoT per lo spionaggio arriva ora Richard Ledgett, vice-direttore dell'agenzia a tre lettere che definisce i sensori interconnessi della Internet delle Cose come un "incubo per la sicurezza" da cui potrebbe scaturire un fiume senza fine di **nuovi segnali da dare in pasto agli analisti dell'intelligence**.

SOLUZIONI: ESISTONO???

SI!

Ma non potrete avere botte piena...

..e moglie ubriaca

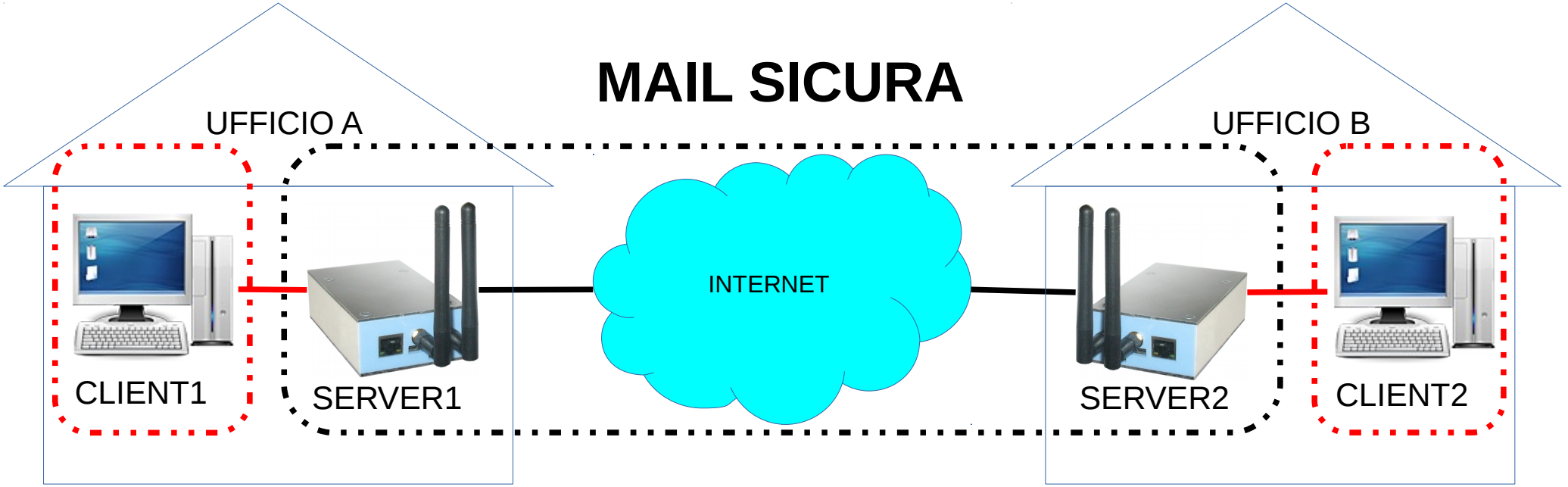
IN ALTRE PAROLE, LA PRIVACY NELLE COMUNICAZIONI ELETTRONICHE E' ANCORA POSSIBILE,

MA:

- Non puoi fidarti del tuo hardware (PC, cellulare, desktop, ecc)
- Non puoi fidarti del tuo software (windows, linux, ios, android, ecc)

COME?

Separando l'apparato che legge/scrive i messaggi di posta elettronica dall'apparato che li veicola.



Un meccanismo di “comunicazione sicura” end-to-end è stato implementato e i primi prototipi hanno dimostrato di funzionare correttamente.

ALTRO?

- Il sistema e' indipendente da fornitore, che in tal modo non può essere tentato – o obbligato – a spiare i propri clienti. (protezione dei dati)

- Le comunicazioni avvengono attraverso un proprio circuito di connessione indipendete dal protocollo smtp (protezione dei metadati)

- I messaggi sono criptati end-to-end, quindi indecifrabili tramite bruteforce (protezione dei dati)

Info@armoredmail.eu