

ETHICAL HACKING, UNETHICAL LAWS

Stefano Zanero, ITBH, CLUSIT

BlackHats '02

SMAU – Milano, 28/10/02

Copyright

Questo insieme di trasparenze è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali.

Il titolo ed i copyright relative alle trasparenze (ivi inclusi, ma non limitatamente a, ogni immagine, fotografia, animazione, video e testo) sono di proprietà degli autori indicati.

Le trasparenze possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione per scopi istituzionali, non a fine di lucro.

Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente a, le riproduzioni a mezzo stampa, su supporti magnetici o su reti di calcolatori) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte dell'autore.

L'informazione contenuta in queste trasparenze è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, ecc.

L'informazione contenuta in queste trasparenze è soggetta a cambiamenti senza preavviso. Gli autori non si assumono alcuna responsabilità per il contenuto di queste trasparenze (ivi incluse, ma non limitatamente a, la correttezza, completezza, applicabilità ed aggiornamento dell'informazione).

In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste trasparenze.

In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.


Incubo di una notte di mezza estate

- La SFIAT costruisce la nuovissima Duna2002
- L'auto è perfetta, tranne per un dettaglio: esplode se tamponata mentre è in terza col serbatoio pieno.
- Un gruppo per la protezione dei consumatori segnala il problema alla casa
- La casa non riesce a riprodurlo nei propri crash test e lo dichiara inesistente...

Incubo di una notte di mezza estate

- ... un pazzo maniaco inizia a tamponare tutte le Duna2002 mentre escono dai distributori
- CHI È IL RESPONSABILE ?

A) Il maniaco	B) La Sfiat
C) Il distributore	D) I ricercatori



Vi sembra fantascienza ?

- Anche a me, ma è una tragica possibilità negli Stati Uniti !
- 19 luglio 2002: "Phased" del gruppo Snosoft rilascia al pubblico i dettagli di un exploit di root contro il sistema Tru64
- La HP minaccia il gruppo di prosecuzione legale per chiedere i danni derivanti da eventuali compromissioni di sistemi realizzate con quell'exploit !

... tanto si tratta degli USA!

- Vero, però ricordiamoci che l'industria del software (e del copyright) è principalmente americana, e soggetta alle leggi USA !
- Phased non è americano, ma la minaccia legale ha comunque impedito almeno in parte i suoi diritti
- Non so voi, ma io viaggio spesso negli USA... e se siete ancora convinti della territorialità del diritto vi racconto una storia...

Mr. Researcher, you're under arrest

- Dmitry Sklyarov, programmatore russo, 27 anni, crea per la ElcomSoft il software AEBPR, che consente di convertire un e-Book di Adobe in formato PDF
- Il programma funziona solo su e-book regolarmente acquistati, ma ovviamente il PDF creato non ha più i vincoli anti-copia
- Sklyarov viene arrestato per violazione del DMCA il 17 luglio 2001 mentre presenta le proprie ricerche ad una conferenza a Las Vegas

Stato d'assedio

- Sklyvarov viene arrestato nonostante il fatto sia avvenuto fuori dal territorio USA, e non sia reato nel paese di provenienza
- Viene detenuto in carcere 3 mesi prima di tornare a casa, ed è comunque tuttora sotto processo nonostante Adobe abbia in seguito rinunciato alla causa
- Sapevate che quando entrate negli USA rinunciate ai vostri diritti se compiete atti di terrorismo, e che l'hacking è considerato terrorismo sotto il Patriot Bill ? (ne parleremo)

Capire il problema

- Per capire le dimensioni del problema dovremo fare una rapida carrellata di diritto e di politica
- Parleremo di
 - DMCA
 - UCITA
 - CBDTPA
 - Leggi sulla crittografia
 - Legislazione informatica italiana ed europea
 - Leggi antiterrorismo (Patriot Bill e annessi)
 - TCPA (“Palladium”) – anche se non si tratta di una legge

DMCA

- Il Digital Millennium Copyright act è una legge voluta fortemente da Hollywood
- La legge, oltre a una serie di giuste protezioni del lavoro protetto da copyright, garantisce uno status speciale alle misure tecnologiche di protezione da copia
- È proibito distribuire, sotto qualsiasi forma (anche un link!), tecnologie che consentano di aggirare una protezione per il copyright. La DMCA è molto chiara in proposito, e molto estensiva

DMCA (2)

- Cercare il modo in cui bypassare una tecnologia di protezione è reato. Discutere del modo in cui si può farlo è un reato: la ricerca ha le mani legate ! (esistono esenzioni, ma limitate)
- Ciò che i legislatori non comprendono è che il software (comprese le tecnologie di protezione) non è una "macchina", ma un'idea. Come tale è soggetta al dibattito: è libero pensiero
- Restringere la ricerca per proteggere i profitti di un album musicale è francamente raggelante.

CBDTPA

- Consumer Broadband and Digital Television Promotion Act. Noto anche come Hollings Bill, dal senatore Hollings (D-S.C.)
- Richiede alla FCC di emanare regolamenti sulla protezione dei contenuti, se l'industria non riesce ad accordarsi
- È sostanzialmente una spada di Damocle contro i produttori di HW e SW per convincerli ad accordarsi con le major
- Esempio: la battaglia sugli Analog2Digital

UCITA

- Uniform Computer and Information Transaction Act
- La legge sostiene il principio per cui il software non viene venduto ma concesso in licenza
- Ciò consentirebbe ai vendor una serie di benefici e agli utenti una serie di svantaggi (first sale, per esempio)
- La cosa interessante è che questa tesi è stata rigettata da tutte le corti di giustizia e la sua introduzione a Washington è fallita.

TCPA

- Trusted Computing Platform Alliance (www.trustedcomputing.org)
- È un tentativo di creare una piattaforma con misure di sicurezza built-in, che coinvolge 180 compagnie
- In sostanza si tratta di aggiungere alla CPU un Trusted Platform Module che si occupa delle verifiche di sicurezza
- L'hardware e una minima parte del software sono affidabili, le restanti componenti vengono verificate

TCPA (2)

- Accoppiato con storage e OS TCPA-compliant, il TPM può anche garantire funzioni di Digital Rights Management, ma...
- Accoppiato con la DMCA, impedisce la concorrenza (formati incompatibili) e il fair use.
- I dispositivi TCPA garantiscono funzioni di PKI e identificazione, ma...
- Hanno il piccolo difetto di eliminare la privacy e l'anonimato.
- E il software in GPL come lo certifichiamo ?

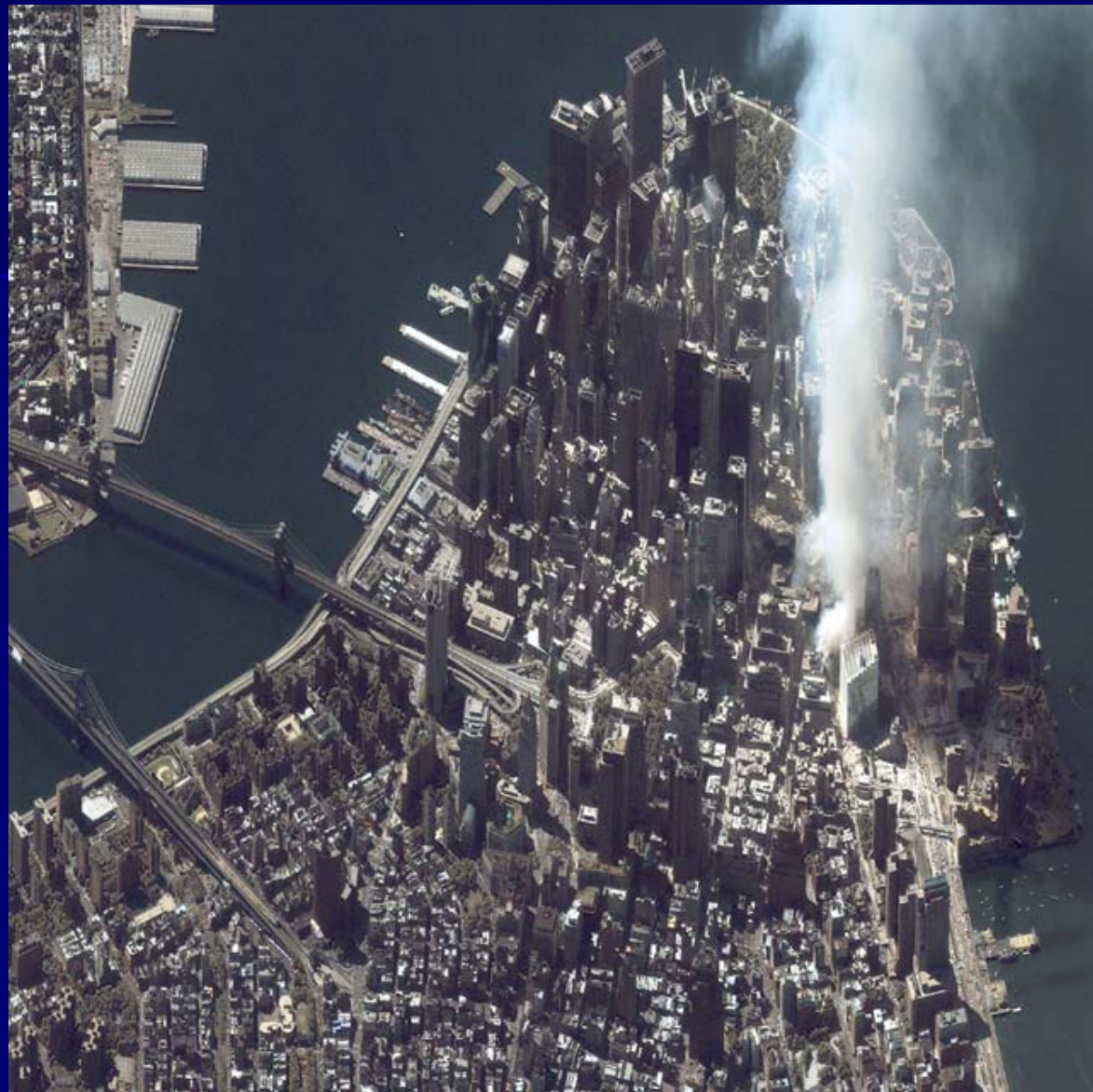
Un piccolo sommario

- Tutte queste leggi hanno come punto focale il DRM: Digital Rights Management
- Tecnicamente e accademicamente, il DRM è una "missione impossibile"
- Ciò che non possono ottenere tecnologicamente, viene imposto dalla legge: questo può anche essere giusto
- Tuttavia, non è assolutamente tollerabile che per difendere i profitti della Warner o di Vivendi venga abrogata la libertà di parola

Un pizzico di storia...

- Jack Valenti, presidente dell'MPAA, deposizione al Congresso, 02/2002: "Internet piracy threatens to disfigure and shred the future of american films"
- Jack Valenti, deposizione al Congresso, 20 anni fa: la tecnologia del VCR "poses the same threat to the movie industry as the Boston Strangler does to women"
- Esattamente un terzo dei profitti di Hollywood oggi derivano dalle videocassette.

**9/11
2001**



Patriot Bill

- Sotto il "Patriot Bill" americano viene considerato cyberterrorismo:
 - Un attacco telematico finalizzato a una azione di terrorismo reale
 - L'aggressione telematica a enti governativi e militari USA
 - Qualsiasi attacco che comporti danni per oltre 5000\$ (ovvero, secondo l'ultimo rapporto CSI/FBI, qualsiasi attacco).
- "Dal momento che non esistono clausole di estradizione per l'hacking, dobbiamo usare quelle che esistono, ad esempio quelle per terrorismo" (James Burrell, Special Agent Supervisor, FBI Computer Crime Unit)

Altre leggi antiterrorismo

- L'effetto 9-11 si è sentito ovunque.
- In Gran Bretagna è terrorismo "agire in concerto con altri per ragioni religiose o politiche" usando certi mezzi (violenza, danneggiamento, mezzi informatici) e provocando determinati effetti (morte, minaccia alla salute pubblica, danni).
- E se io volessi supportare con una petizione telematica il boicottaggio del database genetico islandese ?

Leggi sulla crittografia

- Un trattato europeo sull'"intangible export of technology" sta venendo ratificato dagli stati europei
- La Gran Bretagna ha creato un mostriciattolo: per controllare "ogni possibile scappatoia" si sono concessi ai ministri poteri mai visti, tra cui la possibilità di regolamentare i "non documentary transfers"
- Parlare è un non documentary transfer; allo stato attuale non potrei fidarmi a fare 6 mesi di stage o di Erasmus a Londra

Leggi sulla crittografia (2)

- Si tratta soltanto di un esempio (non dimentichiamoci i problemi con la legge USA sulla crittografia e l'ITAR)
- L'Italia non ha ancora implementato il protocollo, ma è più che prevedibile che seguiremo le linee guida europee alla lettera
- La matematica e la crittografia sono universali, è letteralmente impensabile che ogni paese le sviluppi indipendentemente

Un pensiero sovversivo...

- “They that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety”
- Benjamin Franklin, 1759, parlando delle conseguenze dell'11 settembre

Legislazione italiana

- Art. 615/ter: "chiunque abusivamente si introduce in un sistema informatico o telematico protetto da adeguate misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni."
- Cos'è la volontà "tacita" ? Le misure "adeguate" cosa sono ?
- Manca la giurisprudenza costante sul tema!

Legislazione italiana (2)

- L'articolo 616 punisce "chiunque prenda cognizione del contenuto di corrispondenza chiusa a lui non diretta", dove "per "corrispondenza" si intende quella "... telefonica, informatica o telematica", ovvero "ogni altra forma di comunicazione a distanza"
- Una e-mail non criptata è "chiusa" ?
- L'articolo 630 punisce le intercettazioni
- Uno sniffer va contro la legge ? Un wireless scanner (Kismet e simili) ?

Concludendo...

- Ognuno di questi atti e proposte è sintomo di un male cronico
- “Se il mondo reale non è perfetto, è da stupidi attendersi che quello digitale sia migliore” (E. Dyson)
- L'errore è cercare di restringere nel digitale libertà che nel reale diamo per scontate.
- Per governare, bisogna capire bene il nesso causa-effetto: nel caso di internet pochi politici hanno le conoscenze tecniche necessarie

... fate una promessa

- Quello che sta succedendo nasce dalla scarsa competenza tecnica dei legislatori, ma anche dalla scarsa voglia dei tecnici di occuparsi di "politica" in senso ampio
- Voi siete i tecnici: interessatevi, fate pressione, parlate e fate capire il problema
- Una modesta proposta per la UE: perché non inserire una clausola nei trattati che richieda una revisione quinquennale delle leggi e dei regolamenti tecnologici ?

QUESTIONS ?

ETHICAL HACKING, UNETHICAL LAWS

Stefano Zanero, ITBH, CLUSIT

BlackHats '02

SMAU – Milano, 28/10/02

Contacts:

raistlin@blackhats.it

<http://www.blackhats.it>