Conosciamo il Nemico - Profilazione di un Attaccante

Michele Corrias

Lombardia Plus 2019 Cyber Security - GALDUS

10/01/2020

Index

Introduzione

Sinossi

Nascita della Sicurezza Informatica

- la sicurezza informatica risale ai primi anni ’70, con la diffusione a livello informatico dei primi sistemi multiutente
- fino all’avvento della multiutenza nessuno si era posto il problema della sicurezza informatica

Introduzione

Sistema Informatico

Definizione

Sistema costituito da:

- uno o più computer
- apparati
- sottosistemi elettronici
- server, database, mainframe, supercomputer, switch, router, modem, terminali ...
- interconnessi in rete
- in un'architettura di base di tipo client-server
- dedicati a una o più funzioni o a servizi di elaborazione
- più in generale è detta infrastruttura IT di un'azienda
- anche un semplice computer è un sistema informatico

Introduzione

Sistema Sicuro

Definizione

Un sistema informatico è *sicuro* se vengono garantiti i seguenti requisiti:

- *integrità* → l'informazione memorizzata nel sistema (dati e programmi) è protetta contro modifiche accidentali o dolose
- *confidenzialità* o *riservatezza* o *privacy* → il sistema è in grado di proteggere le informazioni segrete memorizzate da letture non autorizzate
- *disponibilità* → le risorse del sistema (servizi e informazioni) sono sempre disponibili quando richieste

Introduzione

Sistema Sicuro

Problemi

Difficile certificare la totale sicurezza di un sistema informatico

- la maggior parte delle attività svolte da un sistema informatico è predeterminata dal software eseguito
- *errare humanum est*: software e hardware realizzati da persone che possono introdurre vulnerabilità (*bug*)
  - *vulnerabilità* =
    - istruzione, o sequenza di istruzioni, scorretta
    - dichiarazione di dati scorretta
- vulnerabilità non rilevate in *debugging* possono rimanere nascoste nel sistema sino all'esecuzione: non esiste *testing* che garantisca che un programma svolga SOLO qualcosa
- lo sfruttamento (*exploit*) di una vulnerabilità da parte di una minaccia (*threat*) causa una *security failure*

Introduzione

Sistema Sicuro

Problemi

- i sistemi informatici sono molto complessi, costituiti da sottosistemi a loro volta complessi
  - la realizzazione di questi sistemi è a carico di esseri umani, che possono sbagliare ed a volte non possiedono preparazione adeguata
  - l'installazione, la configurazione e l'utilizzo di questi sistemi è demandato spesso a personale inesperto o non qualificato
- vulnerabilità dovute ad errori di progettazione ed errori di programmazione
- errate configurazioni, cattive gestioni, accessi non autorizzati e indicazioni assenti per gli utenti finali su un uso corretto

Introduzione

Security Failure & Exploit

Politica di sicurezza

Un insieme di asserzioni che specificano i requisiti di sicurezza di un sistema

Security Failure

La compromissione delle politica di sicurezza di un sistema

- accesso ad informazioni riservate
- modifica di informazioni riservate
- compromissione del corretto funzionamento di un sistema

Exploiting

L'individuazione di una vulnerabilità in un programma e il suo utilizzo per scopi maligni (*exploit*)

Introduzione

Vulnerabilità in Numeri

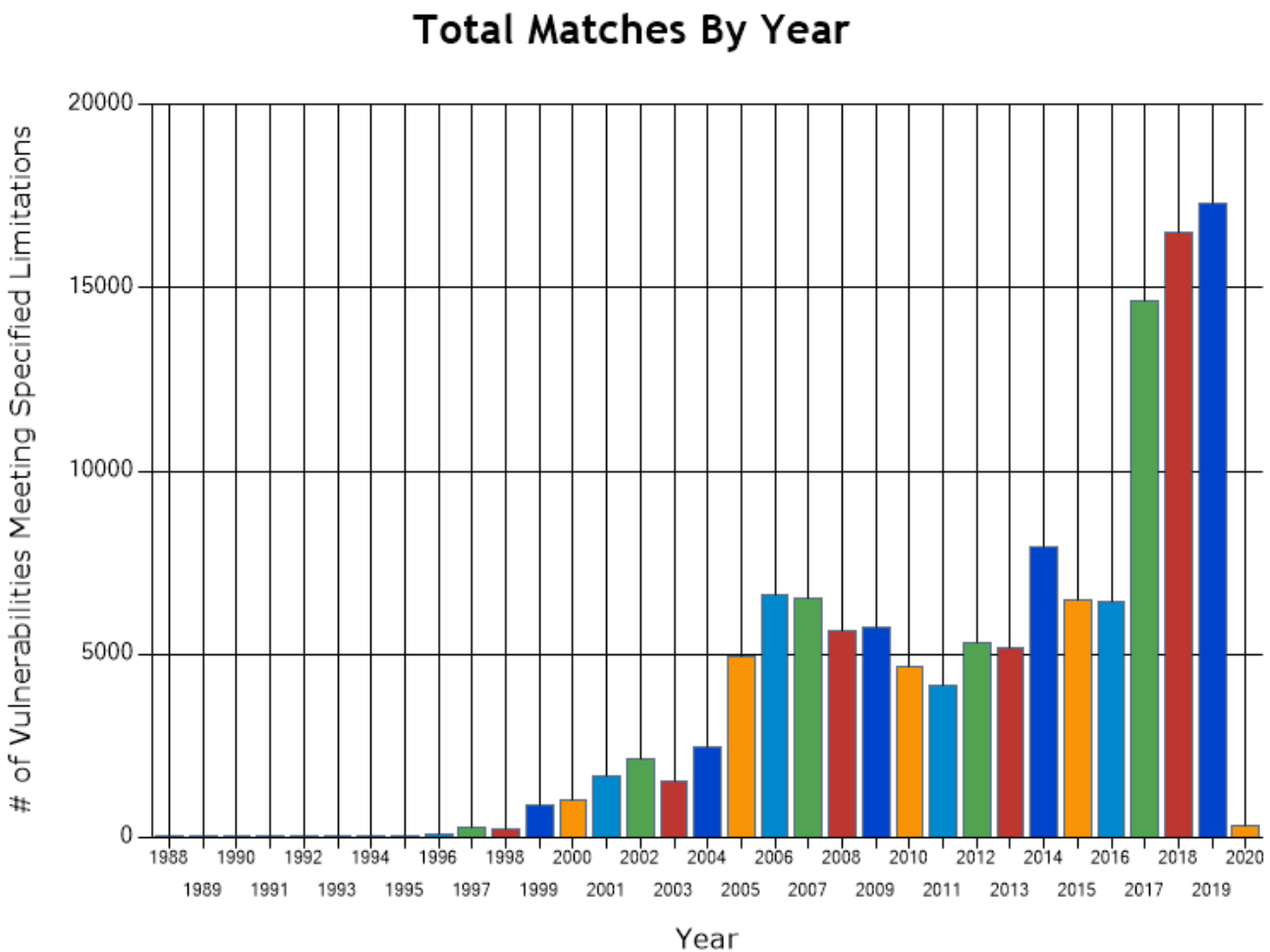
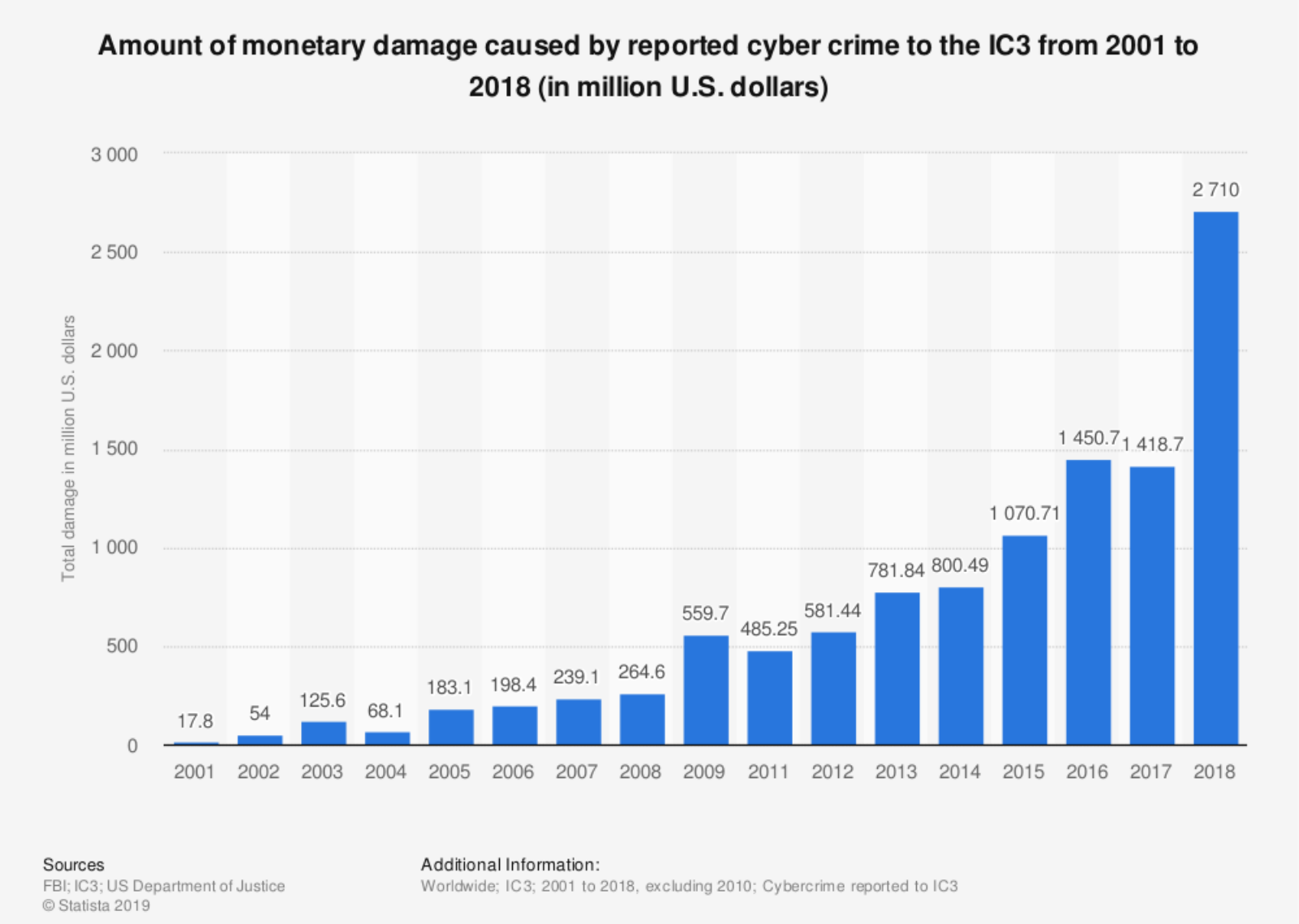


Figura 1: https://www.nist.gov

Introduzione

Costi delle Vulnerabilità



Introduzione

Repository di Vulnerabilità

Bugtraq

Repository accessibile via web:

- Bugtraq Database → `http://www.securityfocus.com/bid`
- identificativo della vulnerabilità
- classe → *Input Validation Error* ...
- identificativo `CVE`
- tipologia → remota/locale
- data di pubblicazione e aggiornamenti
- piattaforme coinvolte
- eventuali discussioni
- exploit (possibilità di errori per motivi etici)
- soluzioni

Introduzione

Repository di Vulnerabilità

Common Vulnerabilities and Exposures

Dizionario di vulnerabilità e falle note pubblicamente:

- `CVE Database` → `http://cve.mitre.org`
- identificazione univoca delle `CVE` permette una maggiore comunicazione nel mondo della sicurezza
- standard di riferimento per i nomi delle vulnerabilità e la loro descrizione
- `CVE identifiers` (ID `CVE`)
- status *entry* (accettato) vs. *candidates* (in revisione)
- *MITRE corporation*
- *CNA* (`Apple`, `Oracle`, `Microsoft` ...) sui propri prodotti
- terze parti come *CERT Coordination Center*

Introduzione

PoC

Proof Of Concept

- exploit non dannoso
- solitamente consiste in uno *snippet* di codice
- non ha lo scopo di causare danni, ma di mostrare vulnerabilità di sicurezza
- la dimostrazione del problema consente al *vendor* di correggere la vulnerabilità

Introduzione

Vulnerability Analysis

Analisi di Sicurezza di un Software

Trovare bug e vulnerabilità di sicurezza all'interno di programmi software

- testing non serve per *certificare* la sicurezza di un prodotto, ma semplicemente per dare indicazioni sul livello di robustezza
- necessarie conoscenze sui dettagli:
  - dell'architettura su cui si opera
  - del sistema operativo sottostante
  - del software utilizzato

Storia

Attacchi Importanti

Intrusioni storiche

1. 1986: un gruppo di cracker tedeschi attacca il *Lawrence Berkeley National Laboratory* (*LBNL*) per accedere a segreti militari
2. 1988: un cracker statunitense mette fuori uso la rete Internet
3. 1994: un cracker statunitense attacca il *San Diego Supercomputer Center* (*SDSC*)
4. 1995: un gruppo di cracker russi attacca la *CITIBANK* (`https://online.citibank.com`)

Storia

Attacchi Importanti

LBNL [1]

- Hannover: viene arrestato il tedesco Markus Hess, uno dei più famosi hacker della storia
- nell'anno precedente era riuscito ad intromettersi nei computer del *LBNL* e connettersi abusivamente ai seguenti sistemi:
  - *Stanford Research Institute* (*SRI*) *International*, Menlo Park (California)
  - *U.S. Army Materiel Command* (*AMC*), Seckenheim (West Germany)
  - *Fort Bruckner Army Base*, Okinawa (Japan)
  - *U.S. Army 24th Infantry*, Fort Stewart (Georgia)
  - *U.S. Navy's Naval Coastal Systems Command*, Panama City (Florida)

Storia

Attacchi Importanti

LBNL [1]

- - *U.S. Air Force*, Ramstein (West Germany)
  - *Massachusetts Institute of Technology* (*MIT*) *MX Computer*, Cambridge (Massachusetts)
  - *OPTIMUS Database*, Pentagon, USA
  - *Air Force Systems Command*, El Segundo (California)
  - *Anniston Army Depot* (*ANAD*), Anniston (Alabama)
- catturato durante il download di alcuni file, opportunamente predisposti dall'FBI, che apparentemente contengono informazioni in merito al progetto `Star Wars`
- riceve una condanna di 20 mesi di prigione e $10k$ DEM ($\approx 5k$ €)

Storia

Attacchi Importanti


The New York Times

U.S. to Ease Methadone Rules For Addicts to Combat AIDS

SOLIDARITY PLANS TO JOIN THE REGIME IN ASKING DEBT AID

The Assault on the Ozone

12 EUROPE NATIONS TO BAN CHEMICALS THAT HARM OZONE

F.B.I. Report on Tower Provokes Bitterness as Senate Opens Debate

Britain, in Talk Aimed at Iran, Calls Rushdie Book Offensive

West Germans Raid Spy Ring That Violated U.S. Computers

New Proposal Made By Eastern Airlines In Mechanic Talks

Figura 3: Markus Hess

Storia

Attacchi Importanti

Internet Worm [2]

- 2 Nov. 1988: Robert Morris, studente di Ph.D della *Cornell University*, mette fuori uso 6000 computer connessi a Internet in poche ore (10% della rete di allora)
- implementa un *worm* in 150 righe di codice C, sfruttando bug di `sendmail` e `finger`
  - *worm* = malware in grado di autoreplicarsi e diffondersi attraverso una rete di computer, infettando gli host collegati
- realizza il primo *buffer overflow* e il primo *dictionary attack* (`password cracking` con dizionario di 432 word)
- errore nel `worm` causa `denial-of-service (DoS)`
- riceve una condanna di 3 anni di prigione, 10k \$ di multa e 400 ore di servizi alla comunità

Storia

Attacchi Importanti

Figura 4: Robert Morris

Storia

Attacchi Importanti

SDSC [3]

- primo attacco di tipo *TCP spoofing* della storia
- l'attacco sfrutta la relazione di `trust` tra host:
  - `x-terminal`: `SPARC` diskless station con `Solaris 1`
  - `server`: host che fornisce boot image a `x-terminal`
- `x-terminal` consente login provenienti dal `server` senza autenticazione
- *DoS* verso il `server`
- impersonificazione del `server` (offline) verso `x-terminal`

Storia

Attacchi Importanti

Kevin Mitnick

- *Condor*
- il 15 Febbraio 1995 il programmatore Kevin Mitnick viene arrestato dall'FBI in North Carolina
- riceve una condanna di 46 mesi di carcere
- a Gennaio 2000 Mitnick viene scarcerato con il divieto di usare Internet per i successivi 3 anni
- a Gennaio 2003 Mitnick è di nuovo sulla rete, dopo 8 anni di assenza

Storia

Attacchi Importanti

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ M218460021).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN

Figura 5: Kevin Mitnick

Storia

Attacchi Importanti

CITIBANK [4]

- intrusori russi acquisiscono password di utenti dei sistemi della *CITIBANK* e tentano il trasferimento di $10M$\$ su conti personali
- la banca perde $400k$\$
- il principale protagonista, Vladimir Levin, viene condannato a 36 mesi di carcere

Storia

Attacchi Importanti

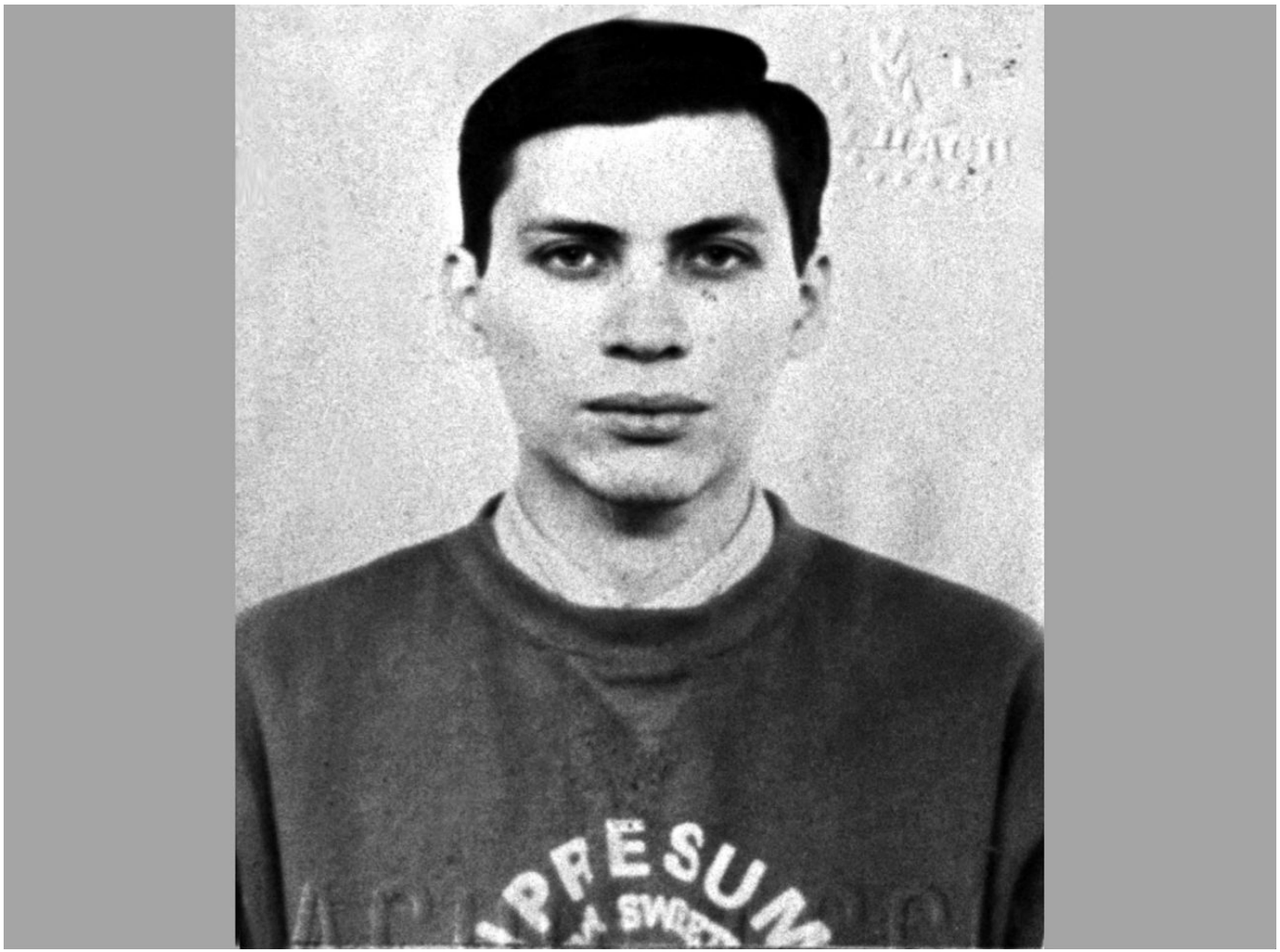


Figura 6: Vladimir Levin

Storia

Hacker

Definizione (*The new Hacker's Dictionary*)

[originally, someone who makes furniture with an axe]

1. a person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary
2. one who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming
3. a person capable of appreciating hack value *hack value*
4. a person who is good at programming quickly

Storia

Hacker

Definizione (*The new Hacker's Dictionary*)

Termine coniato al *MIT* negli anni '60

[originariamente chi faceva mobili con un'ascia]

1. persona che si diverte ad esplorare dettagli di sistemi programmabili e capire come ampliare le loro caratteristiche, contrariamente a molti utenti che preferiscono imparare solo lo stretto necessario
2. colui che programma con entusiasmo, anche ossessivo, o comunque che si diverte a programmare piuttosto che teorizzare solamente concetti di programmazione
3. persona capace di apprezzare l'*hack value*
4. persona abile nel programmare velocemente

Storia

Hacker

Definizione (*The new Hacker's Dictionary*)

5. an expert at a particular program, or one who frequently does work using it or on it; as in *a Unix hacker* (definitions 1 through 5 are correlated, and people who fit them congregate)
6. an expert or enthusiast of any kind. One might be an astronomy hacker, for example
7. one who enjoys the intellectual challenge of creatively overcoming or circumventing limitations
8. (deprecated) a malicious meddler who tries to discover sensitive information by poking around. Hence password hacker, network hacker. The correct term for this sense is *cracker*

Storia

Hacker

Definizione (*The new Hacker's Dictionary*)

5. esperto di un particolare programma o che spesso lavora con tale programma, es.: *hacker Unix* (le definizioni da 1 a 5 sono correlate)
6. esperto o entusiasta di qualsiasi materia: per esempio, una persona può essere un hacker di astronomia
7. persona che si diverte nella sfida intellettuale di superare o aggirare limitazioni in modo creativo
8. (deprecato) ficcanaso malizioso che cerca di scoprire informazioni sensibili introducendosi in sistemi altrui: da ciò hacker di password, hacker di rete; il termine esatto in questo senso è *cracker*

Storia

Hacker

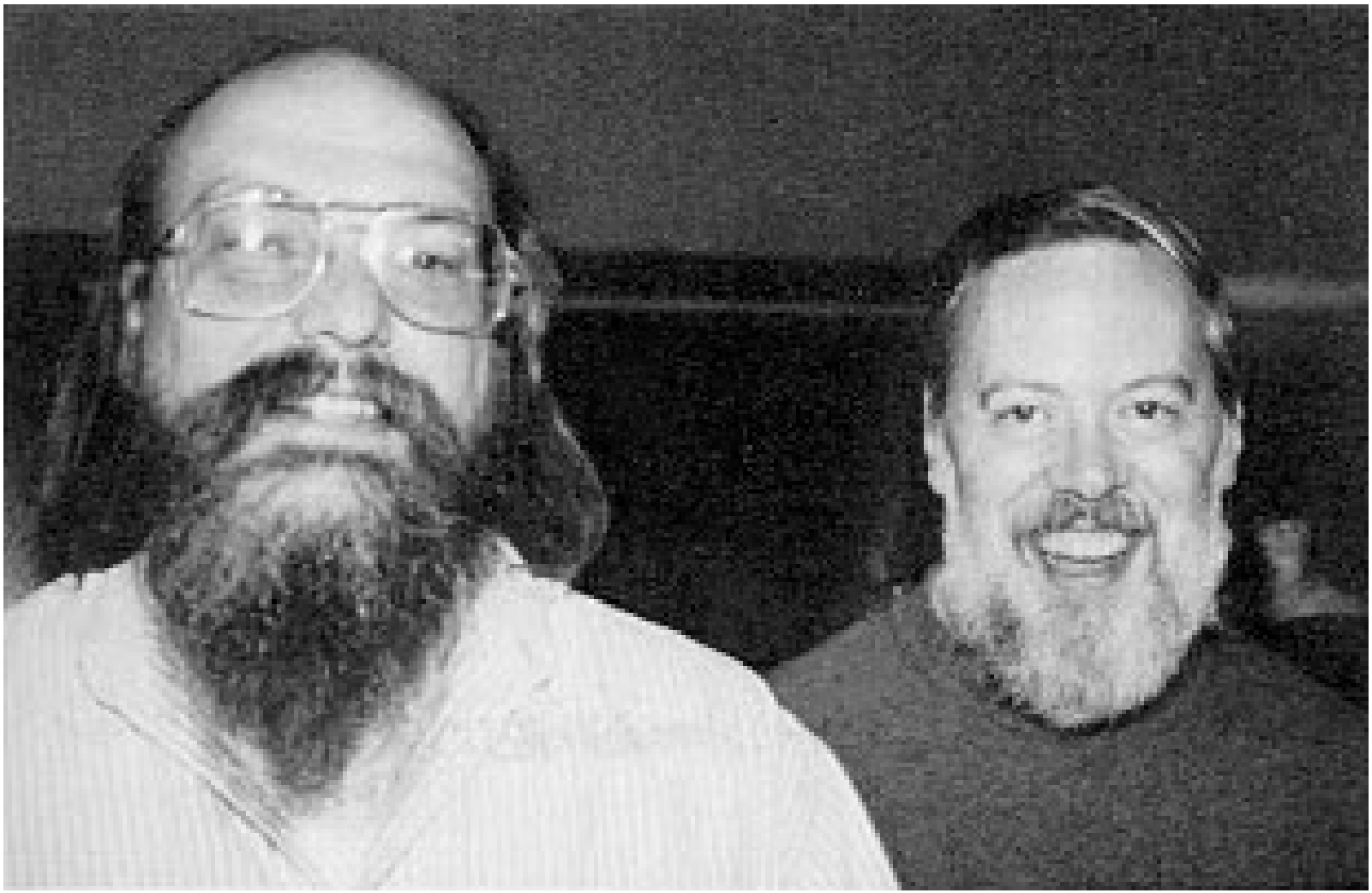


Figura 7: Dennis Ritchie e Ken Thompson

Storia

Hacker

Figura 8: Richard Stallman

Storia

Hacker

Figura 9: Steve Wozniak

Storia

Hacker

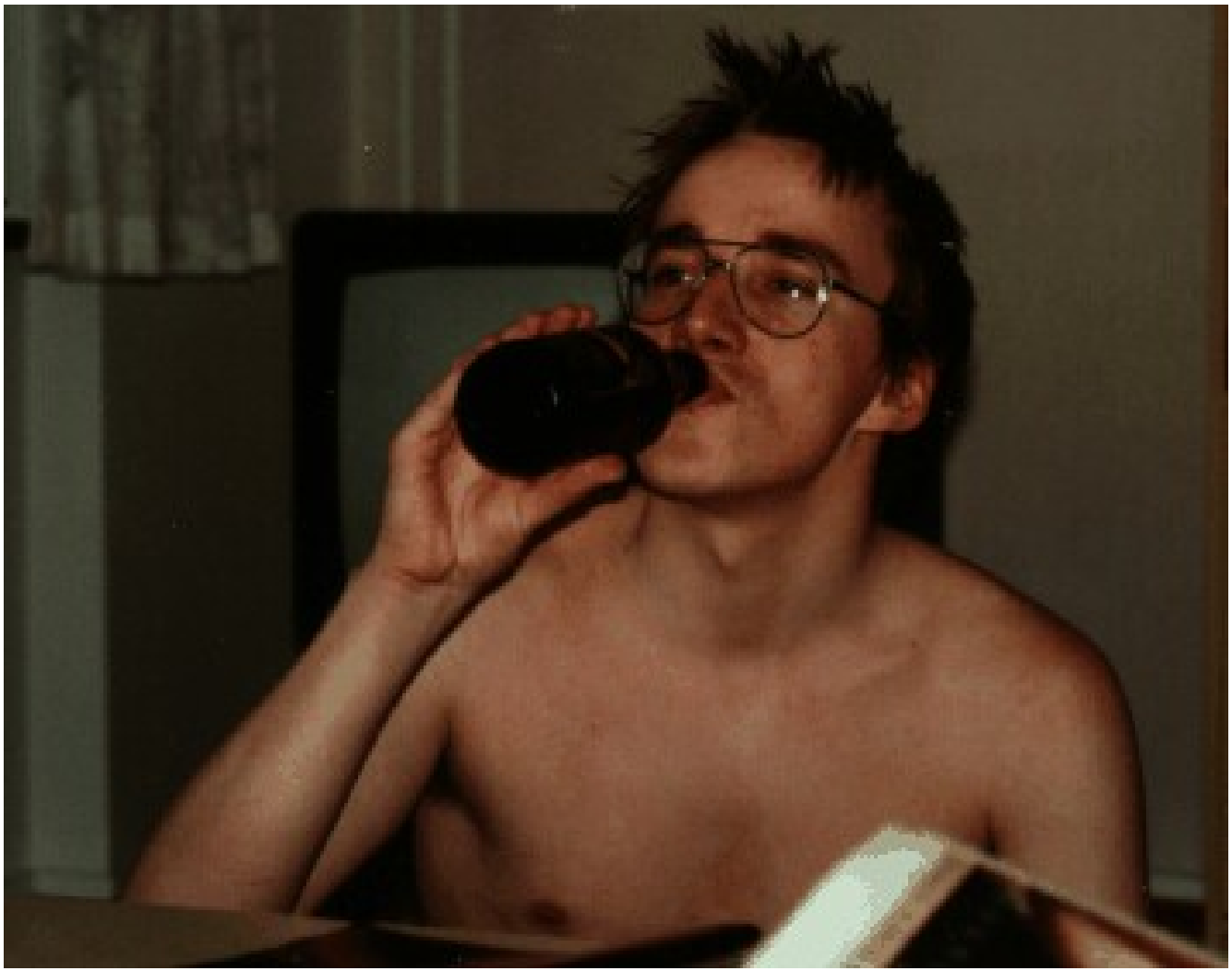


Figura 10: Linus Torvalds

Storia

Cracker

Definizione (*The new Hacker's Dictionary*)

1. one who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of hacker (q.v., sense 8). An earlier attempt to establish *worm* in this sense around 1981-82 on *Usenet was largely a failure*
2. use of both these neologisms reflects a strong revulsion against the theft and vandalism perpetrated by cracking rings. While it is expected that any real hacker will have done some playful cracking and knows many of the basic techniques, anyone past larval stage is expected to have outgrown the desire to do so except for immediate, benign, practical reasons (for example, if it's necessary to get around some security in order to get some work done)

Storia

Cracker

Definizione (*The new Hacker's Dictionary*)

1. chi infrange la sicurezza di un sistema: termine nato nel 1985 dagli hacker a propria difesa contro l'uso mediatico errato del termine hacker; recentemente chi tentava di inviare *worm* attorno al 1981-82; su *Usenet* molto diffuso
2. l'uso di entrambi questi neologismi riflette una forte repulsione contro i furti e i vandalismi perpetrati dalla cerchia dei cracker: mentre ci si aspetta che qualsiasi vero hacker abbia fatto qualche *crack* per gioco e conosca molte delle tecniche base, chiunque, passato lo stadio larvale, attende di liberarsi dal desiderio di crackare ad eccezion fatta per immediate, buone e pratiche ragioni (per esempio, se è necessario aggirare la sicurezza per completare un lavoro)

Storia

Cracker

Definizione (*The new Hacker's Dictionary*)

3. thus, there is far less overlap between hackerdom and crackerdom than the mundane reader misled by sensationalistic journalism might expect. Crackers tend to gather in small, tight-knit, very secretive groups that have little overlap with the huge, open poly-culture this lexicon describes; though crackers often like to describe themselves as hackers, most true hackers consider them a separate and lower form of life

Storia

Cracker

Definizione (*The new Hacker's Dictionary*)

3. ci sono molte meno sovrapposizioni tra cultura hacker e cracker rispetto a ciò che il lettore mondano, fuorviato dal giornalismo sensazionalistico, si dovrebbe aspettare: i cracker tendono a riunirsi in piccoli gruppi affiatati e molto riservati, che si sovrappongono poco all'enorme poli-cultura aperta descritta in questo lessico; sebbene i cracker spesso adorino descrivere loro stessi come hacker, la maggior parte dei veri hacker li considera una forma di vita separata e inferiore

Storia

Hat

Definizione (*The new Hacker's Dictionary*)

- a *black hat* is a cracker, someone bent on breaking into the system you are protecting. Oppose the less comon *white hat* for an ally or friendly security specialist; the term *gray hat* is in occasional use for people with cracker skills operating within the law, e.g. in doing security evaluations. All three terms derive from the dress code of formulaic Westerns, in which bad guys wore black hats and good guys white ones

Storia

Hat

Definizione (*The new Hacker's Dictionary*)

- un *black hat* è un cracker, qualcuno che cerca di intrufolarsi nel sistema che state proteggendo; opposto al meno comune *white hat*, uno specialista di sicurezza alleato o amico; il termine *gray hat* è occasionalmente usato per la gente con esperienza di cracker che opera nei limiti legali (facendo perizie di sicurezza): tutti e tre i termini derivano dal *dress code* degli Western canonici, dove i cattivi portano i cappelli neri e i buoni i cappelli bianchi

Storia

Script Kiddie

Definizione (*The new Hacker's Dictionary*)

- the lowest form of *cracker*; script kiddies do mischief with *script* and *rootkit* written by others, often without understanding the exploit they are using. Used of people with limited technical expertise using easy-to-operate, pre-configured, and/or automated tools to conduct disruptive activities against networked systems. Since most of these tools are fairly well-known by the community, the adverse impact of such actions is usually minimal
- people who cannot program; a script kiddie writes (more likely cuts and pastes) code without either having or desiring to have a mental model of what the code does; someone who thinks of code as magical incantations and asks only «what do I need to type to make this happen?»

Storia

Script Kiddie

Definizione (*The new Hacker's Dictionary*)

- forma meno evoluta di *cracker*: gli script kiddies fanno danni con *script* e *rootkit* scritti da altri, spesso senza nemmeno capire l'exploit usato; persone con esperienza tecnica limitata, che usano tool facili da far funzionare, preconfigurati, e/o automatizzati, per condurre attività distruttive contro sistemi connessi a Internet; dato che la maggior parte di questi tool sono ben conosciuti dalla comunità, l'impatto negativo di tali atti è di solito minimo
- persona che non sa programmare, ma scrive (più precisamente copia e incolla) codice, senza interessarsi davvero di quello che il codice fa; qualcuno che pensa alla programmazione come magia e si chiede solo «cosa devo scrivere per far succedere questo?»

Storia

Lamer & Wannabee

Lamer (*The new Hacker's Dictionary*)

- synonym for *luser*, a lamer is one who scams codes off others rather than doing cracks or really understanding the fundamental concepts

Wannabee (*The new Hacker's Dictionary*)

- the connotations of this term differ sharply depending on the age and exposure of the subject; used of a person who is in or might be entering *larval stage*, it is semi-approving; the said person is trying to cuddle up to the hacker mystique
- *newbe*

Storia

Lamer & Wannabee

Lamer (*The new Hacker's Dictionary*)

- colui che utilizza il codice e gli strumenti realizzati da altri, invece di inventare qualcosa di proprio o almeno tentare di capire i concetti fondamentali, con il solo scopo di voler danneggiare sistemi informatici

Wannabee (*The new Hacker's Dictionary*)

- i significati di questo termine differiscono profondamente secondo l'età e la collocazione del soggetto: detto di una persona che è, o sta per entrare, nello *stadio larvale* dell'*hacking* è quasi giusto; implica che la persona sta provando ad avvicinarsi all'hacking appunto
- *newbe*

Storia

Honey Pot & w00t

Honey Pot (*The new Hacker's Dictionary*)

- a box designed to attract crackers so that they can be observed in action. It is usually well isolated from the rest of the network, but has extensive *logging*
- sometimes it is also a defensive network security tactic — you set up an easy-to-crack box so that your real servers don't get messed with

w00t (*The new Hacker's Dictionary*)

- an interjection similar to *Yay!*, often used for small victories
- some claim this is a bastardization of *root*, the highest level of access to a UNIX-system, originated in `133t`, and said as an exclamation upon gaining root access

Storia

Honey Pot & w00t

Honey Pot (*The new Hacker's Dictionary*)

- una macchina progettata per attrarre i *cracker*, in modo che possano essere osservati durante le loro azioni: in genere si trova ben isolata dal resto della rete, ma con un *log* molto prolisso
- a volte è anche una tattica difensiva per la sicurezza della rete: imposto una macchina facile da crackare, in modo che i server veri non siano esposti

w00t (*The new Hacker's Dictionary*)

- interiezione simile a *Yay!*, usata spesso per piccole vittorie
- corruzione di `root`, il più alto livello di accesso ai sistemi UNIX, che trae origine dal `133t`; usato come esclamazione nell'acquisire l'accesso di root-user

Aspetti Legali

Legge n° 547

Modifica del codice penale

Legge n° 547 del 23 Dicembre 1993 (*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*) ha integrato il codice penale, prevedendo ipotesi di reato specifiche a tutela del bene giuridico informatico

Accesso abusivo ad un sistema informatico o telematico

- Art. 615-ter del codice penale dice che *chiunque abusivamente s'introduce in un sistema informatico o telematico protetto da 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 sino a tre anni*

Aspetti Legali

Legge n° 547

Accesso abusivo ad un sistema informatico o telematico

- se i fatti riguardano sistemi di interesse militare, ordine pubblico, sanità, protezione civile o comunque di interesse pubblico, la pena è aggravata sino a otto anni

Detenzione e Diffusione Abusiva di Codici di Accesso

Art. 615-quater del codice penale punisce con la reclusione sino ad un anno e la multa fino a 5164 € la condotta di *chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo*

Aspetti Legali

Legge n° 547

Diffusione di programmi

Art. 615-quinques del codice penale punisce con la reclusione sino a due anni e con la multa sino a 10329 €, la condotta di *chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici*

Aspetti Legali

Legge n° 547

Tutela della Corrispondenza Informatica

- Art. 617-quater del codice penale punisce con la reclusione da sei mesi a quattro anni *chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe*
- la medesima pena è prevista nei confronti di chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte il contenuto delle predette comunicazioni

Aspetti Legali

Legge n° 547

La Frode Informatica

- Art. 640-ter del codice penale punisce con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1032 € *chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno*
- esistono ulteriori aggravanti

Bibliografia

Riferimenti

Libri & Articoli

- `Internet Worm`: E. Spafford, *The Internet Worm: Crisis and Aftermath*, Communications of the ACM, Vol. 32, No. 6, 1989
- `LBNL`:
  - Clifford Stoll, *The Cuckoo's Egg: Tracking A Spy Through The Maze Of Computer Espionage*
  - Clifford Stoll, *Stalking the Wily Hacker*, Communication of the ACM, Vol. 31, No. 5, 1988
- `Mitnick`: Jonathan Littman, *The Fugitive Game: Online With Kevin Mitnick*, Little Brown & Co