

Sicurezza dei Dati

a.a. 2020/21

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

<http://www.di-srv.unisa.it/~ads>



Settembre 2020

Informazioni sul Corso

➤ Durata: 12 settimane (dal 22 settembre al 13 dicembre)

- 72 ore di lezioni frontali
- 36 lezioni

➤ Orario lezioni:

- Lunedì 16:00 - 18:00, Aula F/5 - Teams
- Giovedì 11:00 - 13:00, Aula F/5 - Teams
- Venerdì 11:00 - 13:00, Aula F/5 - Teams

➤ Home-page del corso:

- <http://www.di-srv.unisa.it/~ads/pages/index.php/sicurezza/>



Variazioni da anni precedenti

- Fino all'anno 2010/11:
"Sicurezza su Reti II", 6 crediti e non 9
- Anni 2011/12, 2012/13, 2013/14 "Sicurezza"
- Dall'anno 2014/15 "Sicurezza dei Dati"
- Anno 2020/21 docenti
 - Alfredo De Santis
 - Esposito Christiancarmine

Nessuna conoscenza pregressa di sicurezza

- Solo pochi studenti hanno sostenuto "Sicurezza"/"Sicurezza su Reti" alla triennale
- Rivedremo i punti principali del corso della triennale

Organizzazione

- Bibliografia
 - Libri
 - Materiale/Appunti dalle lezioni
 - <http://www.di-srv.unisa.it/~ads/pages/index.php/sicurezza/>
- Laboratorio
- Progetti e presentazioni di argomenti specifici



Sicurezza su Reti

Docente prof. Alfredo De Santis, ads@dia.unisa.it

Anno Accademico 1999/2000

Benvenuti alla pagina principale del corso di Sicurezza su Reti.

Tesine (molte sono ancora bozze!)

- [Crittografia Classica](#) (versione 7/3/2001)
- [Crittanalisi \(Vigencere\)](#) (versione finale 27/7/2000)
- [Data Encryption Standard \(DES\)](#) (versione finale 27/7/2000)
- [Advanced Encryption Standard \(AES\)](#) (versione finale 21/7/2000)
- [Crittografia a chiave pubblica](#) (versione finale 31/7/2000)
- [Firme Digitali](#) (versione 31/7/2000)
- [Funzioni Hash](#) (versione finale 13/10/2000)
- [Autenticazione e Password](#) (versione 27/10/2000)
- [Sistemi Biometrici](#) (versione finale 21/3/2001)
- [Schemi di Identificazione](#) (versione finale 1/8/2000)
- [Randomness](#) (versione finale 17/10/2000)
- [Key Escrow](#) (versione finale 30/10/2000)
- [Schemi a Condivisione di Segreto](#) (versione 31/7/2000)
- [Crittografia Visuale](#) (versione finale 2/8/2000)
- [PKI](#) (versione 7/9/2000)
- [Sistema di telefonia GSM](#) (versione finale 21/7/2000)
- [UMTS](#) (versione finale 3/9/2001)
- [Windows NT](#) (versione finale 27/7/2000)
- [Hacking Windows NT](#) (versione finale 25/10/2000)
- [Sicurezza Unix](#) (versione finale 27/10/2000)
- [TCP/IP](#) (versione finale 4/8/2000)
- [HTTP](#) (versione 5/9/2000)
- [SSL](#) (versione finale 12/9/2000)
- [Firewall](#) (versione 11/12/2000)
- [WAP](#) (versione finale 10/10/2000)
- [PGP](#) (versione finale 24/7/2000)
- [SET](#) (versione finale 4/8/2000)
- [Commercio Elettronico](#) (versione finale 3/8/2000)
- [IPv6](#) (versione finale 14/9/2000)
- [Anonimia](#) (versione 4/8/2000)
- [Network Sniffer](#) (versione 2/8/2000)
- [Network Scanner](#) (versione 31/7/2000)
- [Common Gateway Interface and Web Security](#) (versione 26/7/2000)
- [Script Ostili](#) (versione finale 25/7/2000)
- [Sicurezza in Java](#) (versione finale 12/10/2000)
- [Sicurezza e ASP \(Active Server Pages\)](#) (versione 5/3/2001)
- [Sicurezza nei Data Base \(Oracle\)](#) (versione finale 18/10/2000)

- [Computer Virus](#) (versione finale 5/10/2000)
- [Watermark](#) (versione finale 28/9/2000)
- [Monitoraggio attivo utenti](#) (versione finale 3/8/2000)
- [Distributed Denial of service](#) (versione 3/8/2000)
- [CryptoAPI](#) (versione 1/8/2001)
- [Smart Card](#) (versione 5/12/2001)
- [PGP con Windows](#) (versione 28/10/2003)
- Modello tesine ([exe](#), [zip](#))

Presentazioni

- Introduzione ([html](#), [ps](#), [pdf](#))
- Crittografia Classica ([html](#), [ps](#), [pdf](#))
- Crittoanalisi ([html](#), [ps](#), [pdf](#))
- DES ([html](#), [ps](#), [pdf](#))
- AES ([html](#), [ps](#), [pdf](#))
- Stream Cipher ([html](#), [ps](#), [pdf](#))
- Crittografia a Chiave Pubblica ([html](#), [ps](#), [pdf](#))
- Firme Digitali ([html](#), [pdf](#), [ps](#))
- Diffie Hellman ([html](#), [ps](#), [pdf](#))
- Funzioni Hash ([html](#), [pdf](#), [ps](#))
- Randomness ([html](#), [ps](#), [pdf](#))
- Digital Timestamping ([html](#), [ps](#), [pdf](#))
- Digital Watermark ([html](#), [ps](#), [pdf](#))
- Tecniche biometriche di identificazione ([html](#), [ps](#), [pdf](#))
- Protocolli ([html](#), [ps](#), [pdf](#))
- Mental Poker ([html](#), [ps](#), [pdf](#))
- Crittografia Visuale ([html](#), [ps](#), [pdf](#))
- PGP ([html](#), [pdf](#), [ps](#))
- Windows NT: architettura del sistema ([html](#), [pdf](#), [ps](#))
- Windows NT: sicurezza in locale ([html](#), [pdf](#), [ps](#))
- Windows NT: organizzazione di rete ([html](#), [pdf](#), [ps](#))
- Windows NT: password ([html](#), [pdf](#), [ps](#))
- Hacking Windows NT ([html](#), [pdf](#), [ps](#))
- File System cifrati ([html](#), [pdf](#), [ps](#))
- Java security ([html](#), [pdf](#), [ps](#))
- Web & CGI Security ([html](#), [pdf](#), [ps](#))
- Network Sniffer ([html](#), [ps](#), [pdf](#))
- Distributed Denial of Service ([html](#), [ps](#), [pdf](#))
- Monitoraggio attivo utenti ([html](#), [ps](#), [pdf](#))
- Network scanner ([html](#), [pdf](#), [ps](#))
- [Progetti del corso](#), [Progetti assegnati e gruppi](#)

[Anno Accademico 1998/1999](#)

Sicurezza su Reti

Docente prof. Alfredo De Santis, ads@dia.unisa.it

Anno Accademico 2000/2001

Benvenuti alla pagina principale del corso di Sicurezza su Reti.

Presentazioni

- Introduzione ([html](#), [pdf](#))
- Crittografia Classica ([html](#), [pdf](#))
- Crittoanalisi ([html](#), [pdf](#))
- DES ([html](#), [pdf](#))
- RC2, RC5 ([html](#), [pdf](#))
- AES ([html](#), [pdf](#))
- Crittografia a Chiave Pubblica ([html](#), [pdf](#))
- Accordo su chiavi ([html](#), [pdf](#))
- Firma digitale ([html](#), [pdf](#))
- Funzioni Hash ([html](#), [pdf](#))
- Message Authentication Codes (MAC) ([html](#), [pdf](#))
- Autenticazione ([html](#), [pdf](#))
- Crack ([html](#), [pdf](#))
- PKI ([html](#), [pdf](#))
- Pluggable Authentication Modules (PAM) ([html](#), [pdf](#))
- Protocolli Crittografici ([html](#), [pdf](#))
- Pretty Good Privacy (PGP) ([html](#), [pdf](#))
- SSH ([html](#), [pdf](#))
- SSL ed OpenSSL ([html](#), [pdf](#))
- Protezione posta sotto Linux ([html](#), [pdf](#))
- Randomness ([html](#), [pdf](#))
- Kerberos ([html](#), [pdf](#))
- Firewall 1 ([html](#), [pdf](#))
- Intrusion Detection ([html](#), [pdf](#))
- Snort ([html](#), [pdf](#))
- StackGuard ([html](#), [pdf](#))
- Tools Steganografici ([html](#), [pdf](#))
- Packet Sniffing ([html](#), [pdf](#))
- Packet Sniffer con libreria PCAP ([html](#), [pdf](#))
- Packet Sniffing: la libreria Winpcap ([html](#), [pdf](#))
- Port Scanning ([html](#), [pdf](#))
- Retina ([html](#), [pdf](#))
- StegFS ([html](#), [pdf](#))
- How Assess, Evaluate, Optimize a .COM Security Infrastructure ([pdf](#))

Tesine

- Message Authentication Codes (MAC) (versione finale 14/12/01)
- Cifrari a blocchi: AES, RC2, RC5 (versione finale 20/12/01)
- Crittosistemi basati su Curve Ellittiche (versione finale 20/12/01)
- Steganografia (versione finale 9/7/01)
- PGP con Windows (versione 5/12/01)
- SSH (versione finale 2/8/01)
- OpenSSL (versione finale 20/7/01)
- Protezione posta sotto Linux (versione finale 14/11/01)
- Packet Sniffer (versione 31/7/01)
- Packet Sniffer con libreria PCAP (versione finale 10/7/01)
- Packet Sniffing: la libreria Winpcap (versione 26/7/01)
- SNORT (versione finale 26/7/01)
- Port Scanning (versione 26/7/01)
- Retina (versione finale 4/12/01)
- Rilevazione dello Scanning (versione finale 18/10/01)
- StackGuard (versione finale 24/7/01)
- Crack (versione 5/7/01)
- Kerberos V5 (versione finale 11/9/01)
- Sicurezza in Windows 2000 (versione finale 19/10/01)
- StegFS (versione finale 22/3/02)
- Firewall 1 (versione finale 4/12/01)
- PAM (versione finale 8/4/02)

[Anno Accademico 1999/2000](#)

[Anno Accademico 1998/1999](#)

Progetti di Digital Forensics

- Windows Forensics (Valerio Cinque, Francesco Testorio, Andrea Di Maio)
- Falso alibi digitale su Windows 7 (Alessandro Bove, Alfonso Martorelli, Giuseppe Valentino, Luigi Di Biasi)
- Distribuzioni Linux per analisi forense (Helix 3, DEFT Linux 6, CAINE, Backtrack)
 - Live forensic (Mario Fiore Vitale, Fabio Fulgido, Gaetano Rocco)
 - Post-mortem forensic (Umberto Annunziata, Claudio Gargiulo)
- Linux Forensics (Domenico Viscito, Fabio Favale)
- Falso alibi digitale su Linux (Antonio Sanfelice, Sara Cantalupo, Demia Massaro, Giovanni Costa)
- iPod ed iPhone Forensics (Giovanni Mastroianni, Luisa Siniscalchi, Domenico Voto)
- Android Forensics (Davide Barbuto, Francesco Capano, Gaetano Contaldi, Andrea Vallati)
- Image Forensics (Giuseppe Lanzilli, Hamza Hamim, Gianluca Roscigno)
- GPS Navigation Devices Forensics (Ermanno Travaglino, Armando Faggiano)
- Investigazione di un Computer (Alessio Marzaioli, Francesco Pisano)
- Network Investigations (Dario Casciello, Domenico Memoli, Antonio Della Sala)

<http://www.dia.unisa.it/professori/ads/ads/Sicurezza.html>

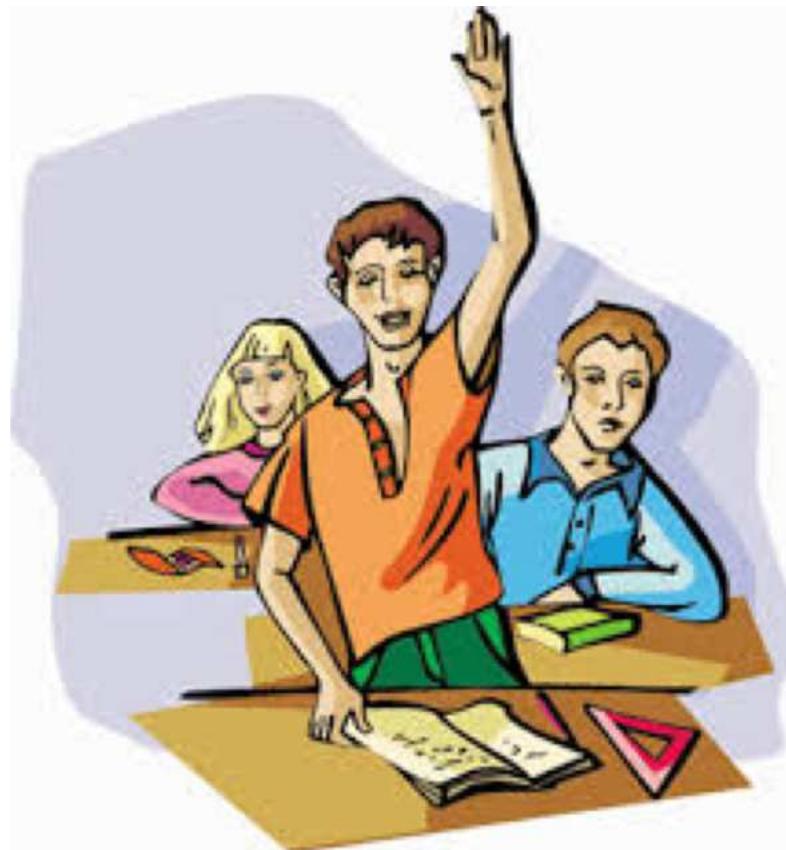
Esempi progetti precedenti

- Network Anomaly Detection
- Honeypot
- Internet of Cars
- The Heartbleed Bug
- Identification and Analysis of HomePlug AVLN
- Cloud Security
- Malware
- Android Battery
- Dropbox
- GPS
- VoIP Security

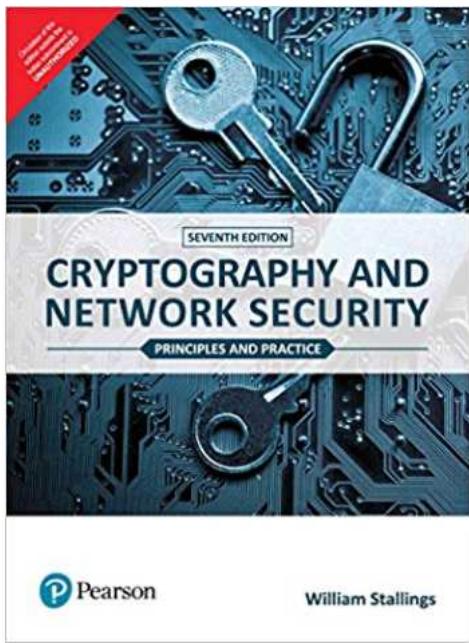
Interazione

Domande

Interesse



Testi di riferimento

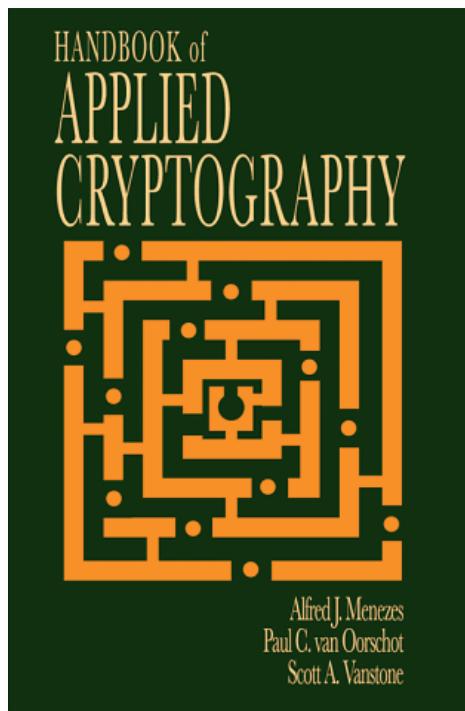


Cryptography and Network Security:
Principles and Practices
Prentice-Hall (7/Ed)
by William Stallings, 2016

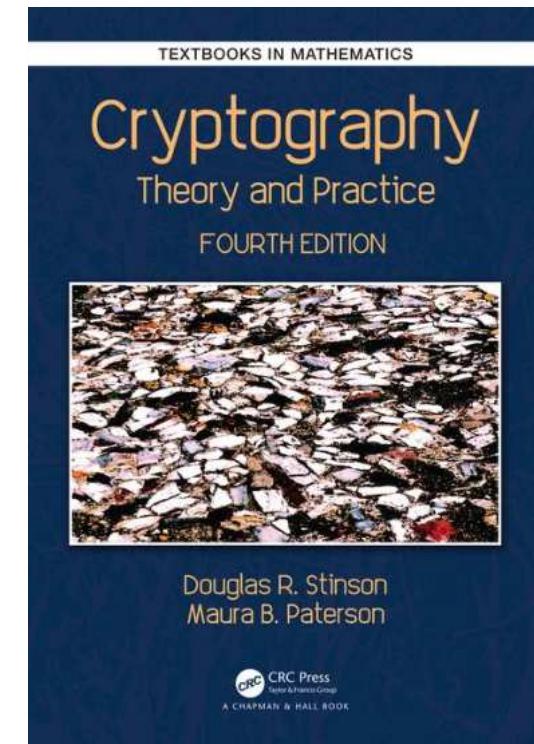
Crittografia e Sicurezza delle Reti
McGraw-Hill (2/Ed)
by William Stallings, 2007



Altri testi utili



Handbook of Applied Cryptography
Alfred J. Menezes, Scott A. Vanstone, 1996
<http://cacr.uwaterloo.ca/hac/>



Cryptography: Theory and Practice (4th Ed.)
by Douglas Stinson and Maura Paterson, 2018

Laboratorio

Una simulazione della rete Internet
Collaborazione dott. Luigi Catuogno

- a.a. 2004/05
- a.a. 2005/06
- a.a. 2006/07
- a.a. 2007/08



<http://sicurezza2.dia.unisa.it/>

Esami

- Esame classico
- Progetti e presentazioni

Esami

- L'esame prevede una prova scritta e una prova orale
- Sono previsti **sette appelli** suddivisi come segue:
 - Tre appelli nel periodo Gennaio 2021 - Febbraio 2021
 - Un appello straordinario Aprile 2021;
 - Due appelli nel periodo Giugno 2021 - Luglio 2021.
 - Un appello Settembre 2021.

Niente prove intercorso

Corsi ambito Sicurezza

Magistrale Informatica

- Cybersecurity
- Penetration Testing and Ethical Hacking
- Digital Forensics
- Programmazione Sicura
- Elementi di Crittografia
- IoT Security



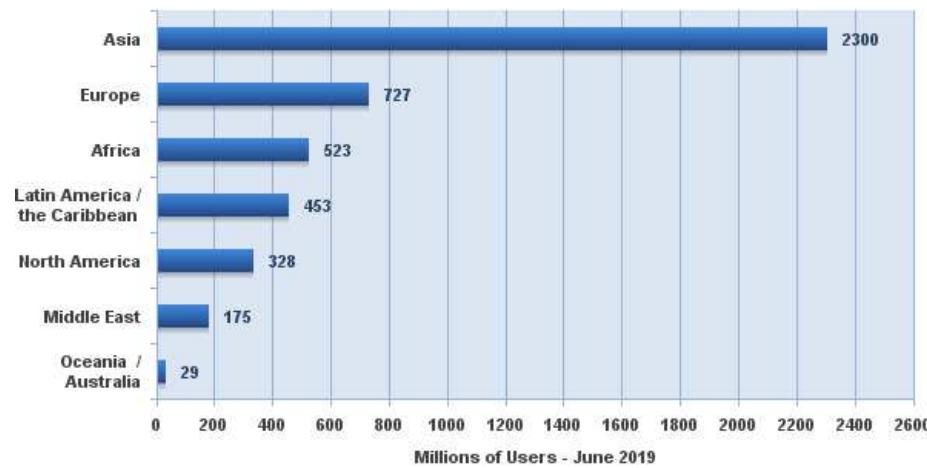
**Ed ora ...
qualcosa sui
contenuti**

Course Outline

- STRUMENTI CRITTOGRAFICI
- INFRASTRUTTURE DI SICUREZZA
- SICUREZZA DEI SISTEMI E DELLE RETI
- LEGISLAZIONE, STANDARD E SICUREZZA
- TECNOLOGIA BLOCKCHAIN, CONSENSO DISTRIBUITO E SMART CONTRACT
- TRUSTED EXECUTION ENVIRONMENT
- SICUREZZA NELLE ARCHITETTURE A MICROSERVIZI
- SICUREZZA NELLE BASI DI DATI

Utenti Internet nel mondo

Internet Users in the World
by Geographic Regions - Mid-Year 2019

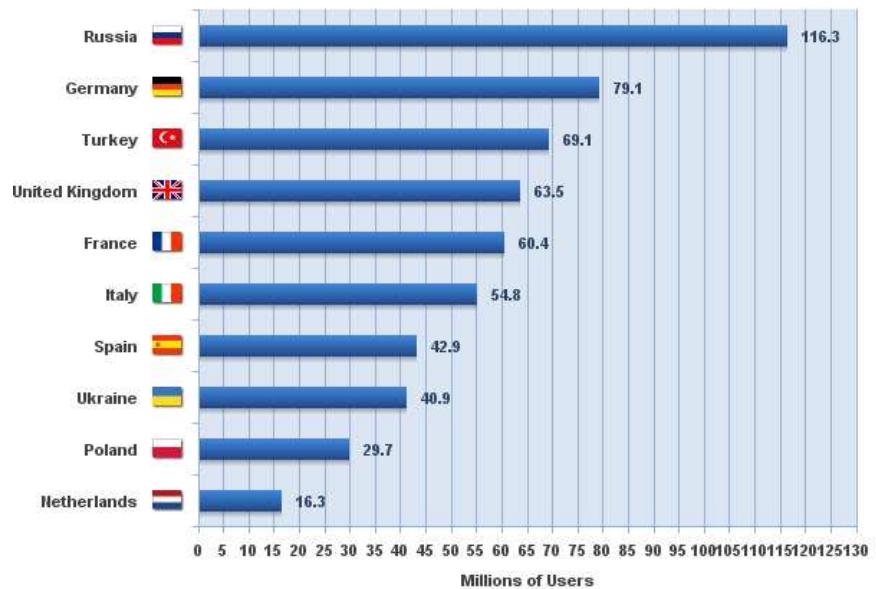


Source: Internet World Stats - www.internetworldstats.com/stats.htm

Basis: 4,536,248,808 Internet users estimated in June 30, 2019

Copyright © 2019, Miniwatts Marketing Group

Internet Top 10 Countries in Europe
June 30, 2019



Source: Internet World Stats - www.internetworldstats.com/stats4.htm

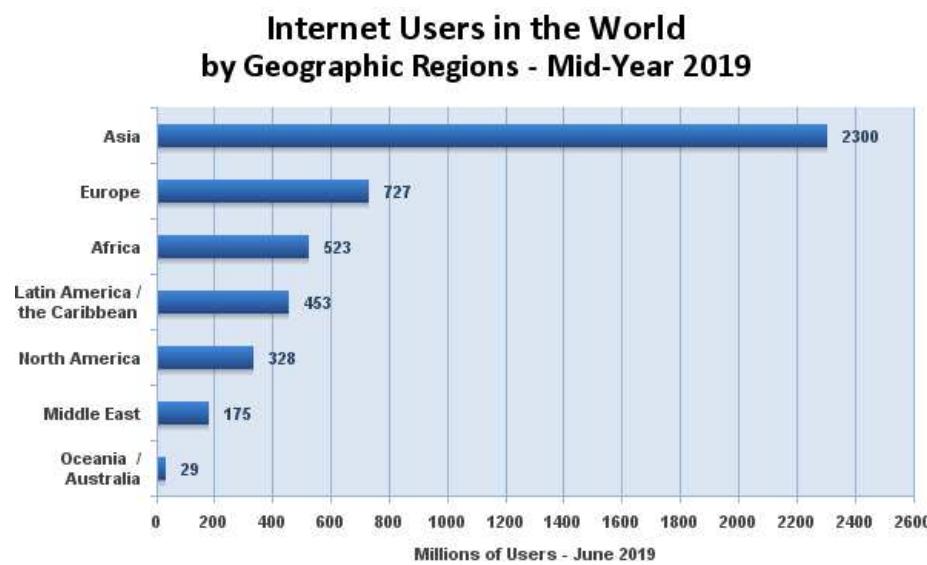
Basis: 727,559,682 estimated Internet Users in Europe on June 2019

Copyright © 2019, Miniwatts Marketing Group

Internet Usage and World Population Statistics are
for Jun 30, 2019:
Population 7,716,223,209
58.8% of population 4,536,248,808

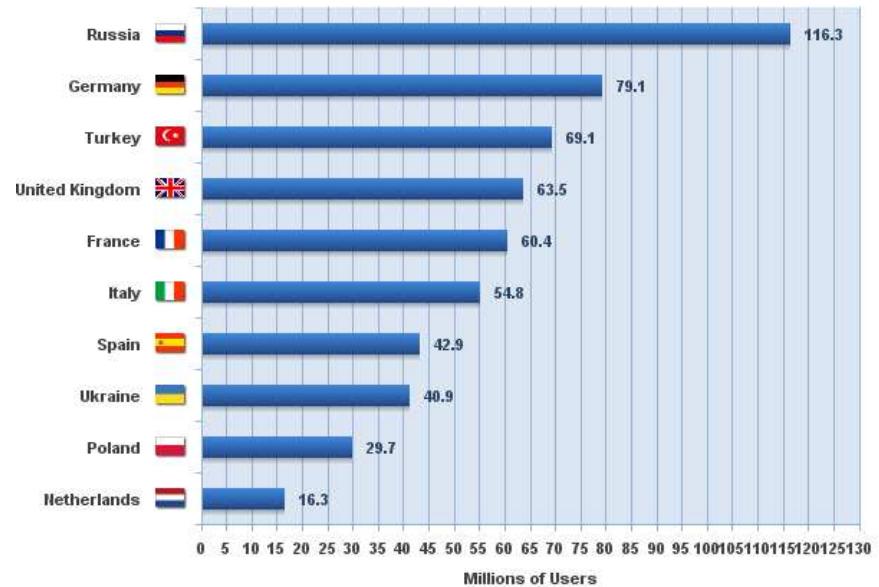
Utenti Internet nel mondo

Before we can measure or forecast Internet Usage, we must first answer a basic question: **Who is an Internet user?** Research firms, analysts, consultancies and other sources all disagree on how to answer this seemingly simple question.



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,536,248,808 Internet users estimated in June 30, 2019
Copyright © 2019, Miniwatts Marketing Group

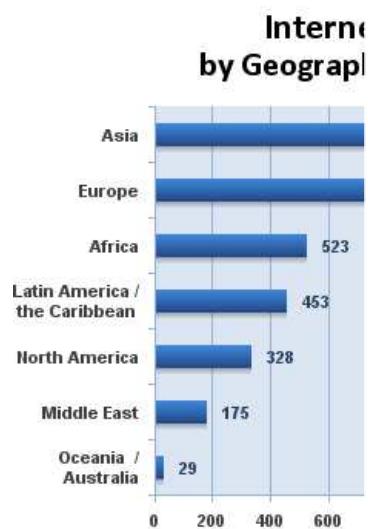
**Internet Top 10 Countries in Europe
June 30, 2019**



Source: Internet World Stats - www.internetworldstats.com/stats4.htm
Basis: 727,559,682 estimated Internet Users in Europe on June 2019
Copyright © 2019, Miniwatts Marketing Group

**Internet Usage and World Population Statistics are
for Jun 30, 2019:**
Population 7,716,223,209
58.8% of population 4,536,248,808

Utenti Internet nel mondo



Source: Internet World Stats - www.internetworldstats.com
Basis: 4,536,248,808 Internet users estimated
Copyright © 2019, Miniwatts Marketing Group

1.1 INTERNET USAGE

Before we can measure or forecast Internet Usage, we must first answer a basic question: **Who is an Internet user?** Research firms, analysts, consultancies and other sources all disagree on how to answer this seemingly simple question.

The ITU subscribes to the definition of an Internet user as someone aged 2 years old and above, who went online in the past 30 days. The US Department of Commerce, in contrast, defines Internet users as those 3 years or older who 'currently use' the Internet. The CNNIC defines the Internet user as a Chinese citizen, aged 6 or above, who uses the Internet at least one hour per week.

Other market researchers and market research organizations have their own definitions. For example, **Nielsen Online** in its reports presents two figures for the Internet users: the first is "Active Internet User", which is defined as the number of users that viewed the Internet at least once during the last month, and the other figure is, of course, the total universe estimate of Internet users in a country, region, or city.

We believe that a definition must be as general and as simple as possible. Therefore, for analyzing and comparing Internet users on a global scale, **IWS** adopts as its benchmark a broad definition and defines an Internet User as **anyone currently in capacity to use the Internet**. In our opinion, there are only two (2) requirements for a person to be considered an Internet User:

- (1) The person must have **available access** to an Internet connection point, and
- (2) The person must have the **basic knowledge** required to use web technology.

Internet Usage and World Population Statistics are
for Jun 30, 2019:
Population 7,716,223,209
58.8% of population 4,536,248,808

<https://www.internetworldstats.com/surfing.htm#1>

Problemi

Internet consente alle aziende di

- Effettuare commercio elettronico
- Fornire un migliore servizio ai clienti
- Ridurre i costi di comunicazione
- Accedere facilmente alle informazioni



...tuttavia...

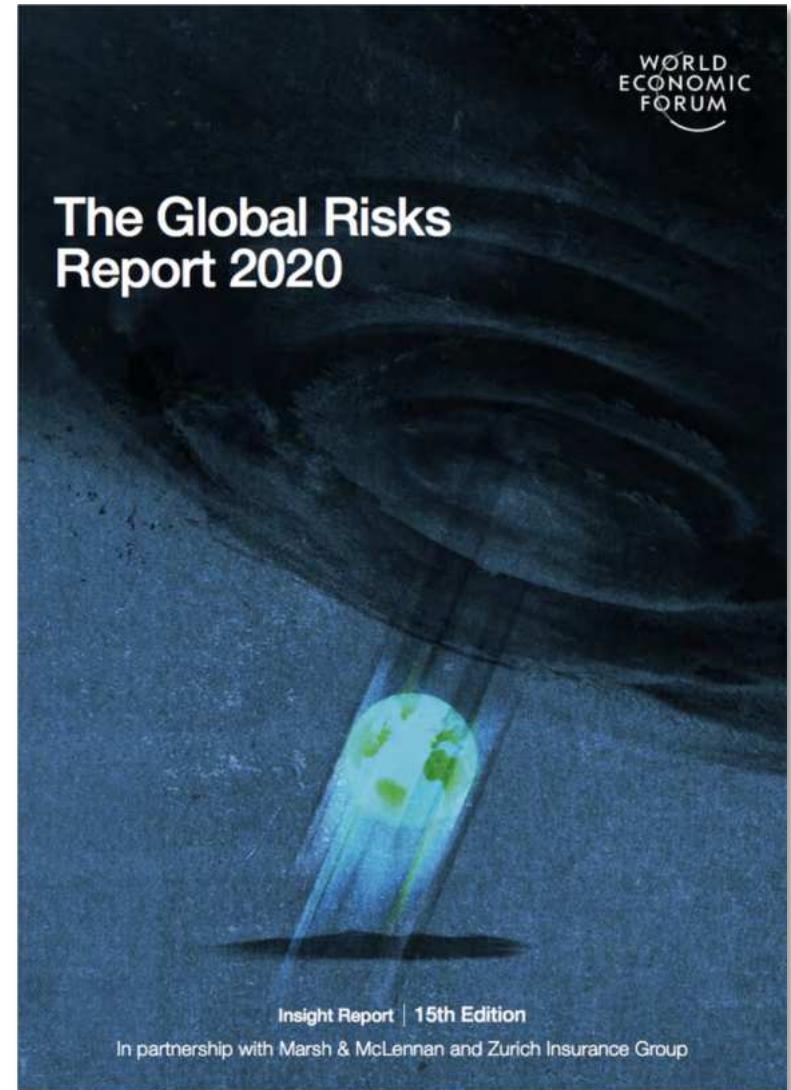
... espone i computer all' azione di attacchi da parte di malintenzionati

- Il numero di incidenti aumenta di anno in anno
- Le perdite finanziarie hanno raggiunto livelli misurabili in miliardi di dollari



The Global Risks Report 2020

the biggest risks facing
our world in 2020



http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

The Global Risks Report 2020

Top 5 Global Risks in Terms of Likelihood



The Global Risks Report 2020

Top 5 Global Risks in Terms of Impact



Economic Environmental Geopolitical Societal Technological

Source: World Economic Forum 2007-2020, Global Risks Reports.

The Global Risks Landscape 2020

Top 10 risks in terms of

Likelihood

- 1 Extreme weather
- 2 Climate action failure
- 3 Natural disasters
- 4 Biodiversity loss
- 5 Human-made environmental disasters
- 6 Data fraud or theft
- 7 Cyberattacks
- 8 Water crises
- 9 Global governance failure
- 10 Asset bubbles

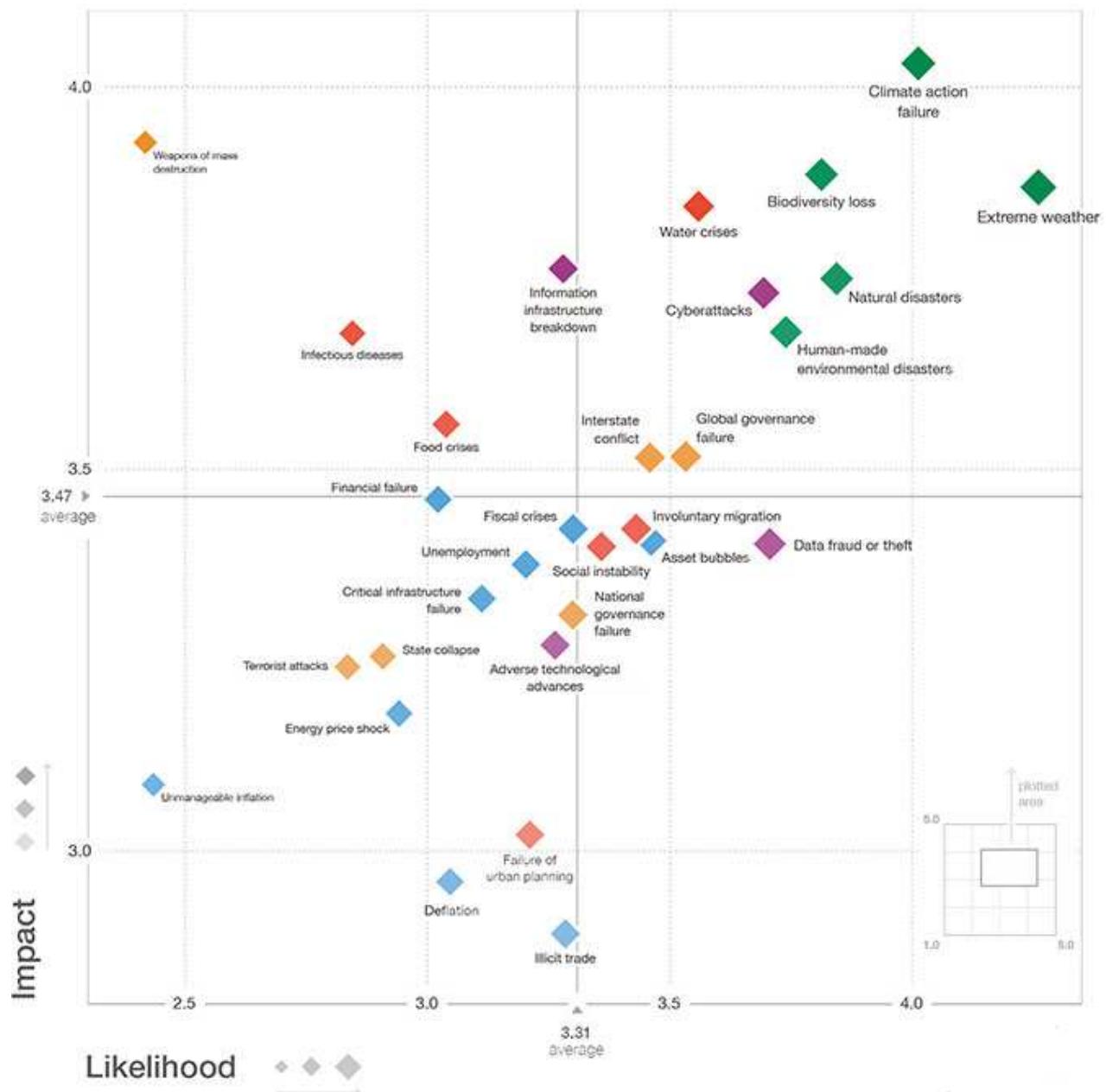
Top 10 risks in terms of

Impact

- 1 Climate action failure
- 2 Weapons of mass destruction
- 3 Biodiversity loss
- 4 Extreme weather
- 5 Water crises
- 6 Information infrastructure breakdown
- 7 Natural disasters
- 8 Cyberattacks
- 9 Human-made environmental disasters
- 10 Infectious diseases

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological



The Risk-Trends Interconnections Map 2020



Economic
Risks

Environmental
Risks

Societal
Risks

Geopolitical
Risks

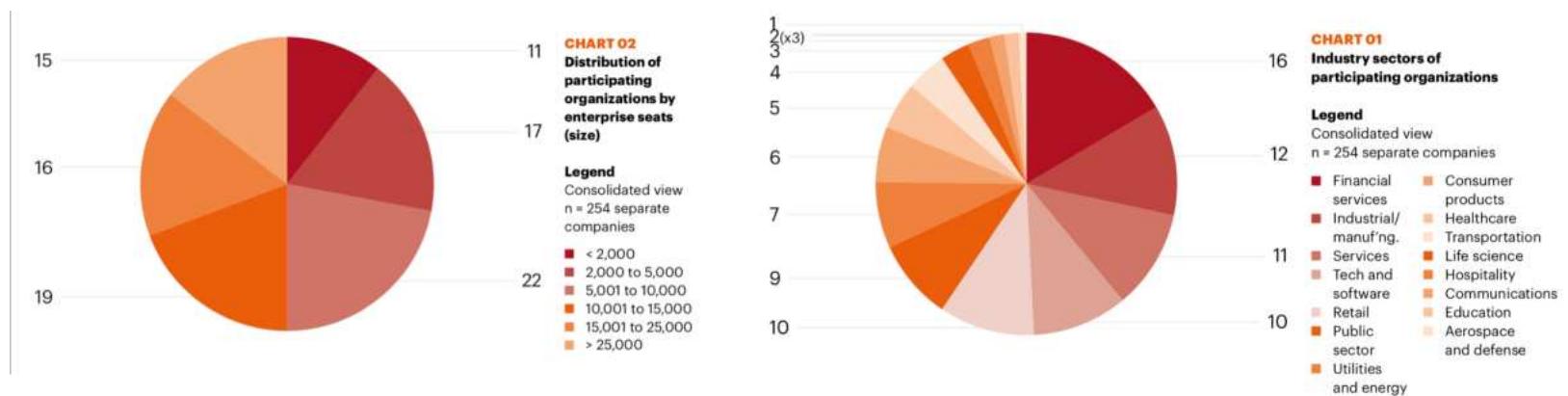
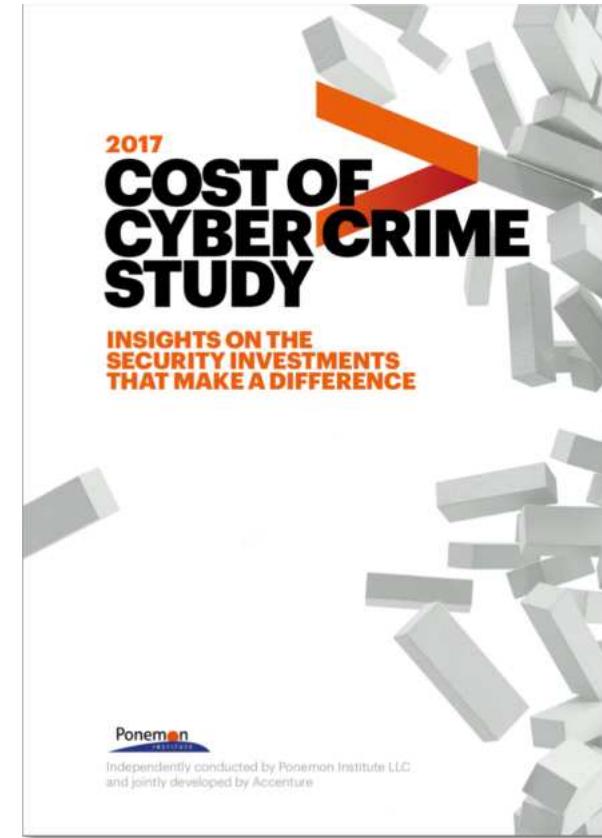
Technological
Risks



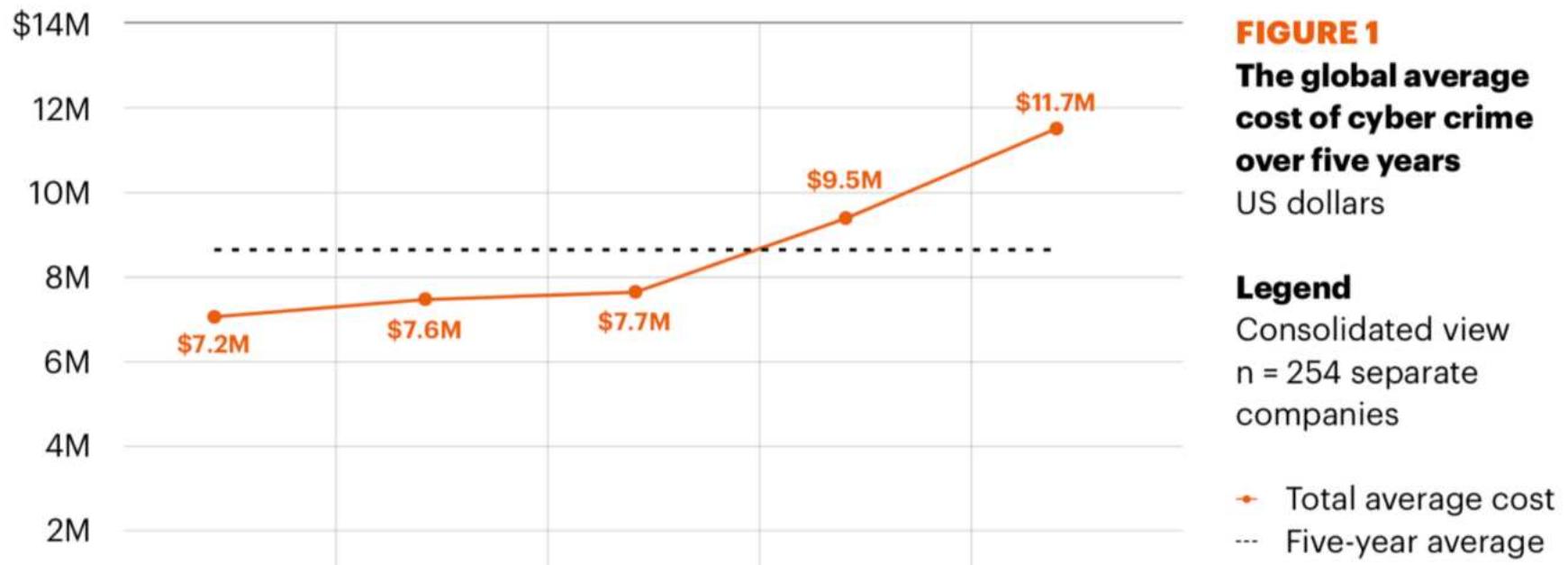
Number and strength
of connections
("weighted degree")

Statistiche

Risposte a 2182 interviste da
254 aziende in sette nazioni
(Australia, Francia, Germania,
Italia, Giappone, UK e USA)



Costo Cybercrime



Percentage change in average cost over five years is 62 percent

Costo Cybercrime in 7 nazioni

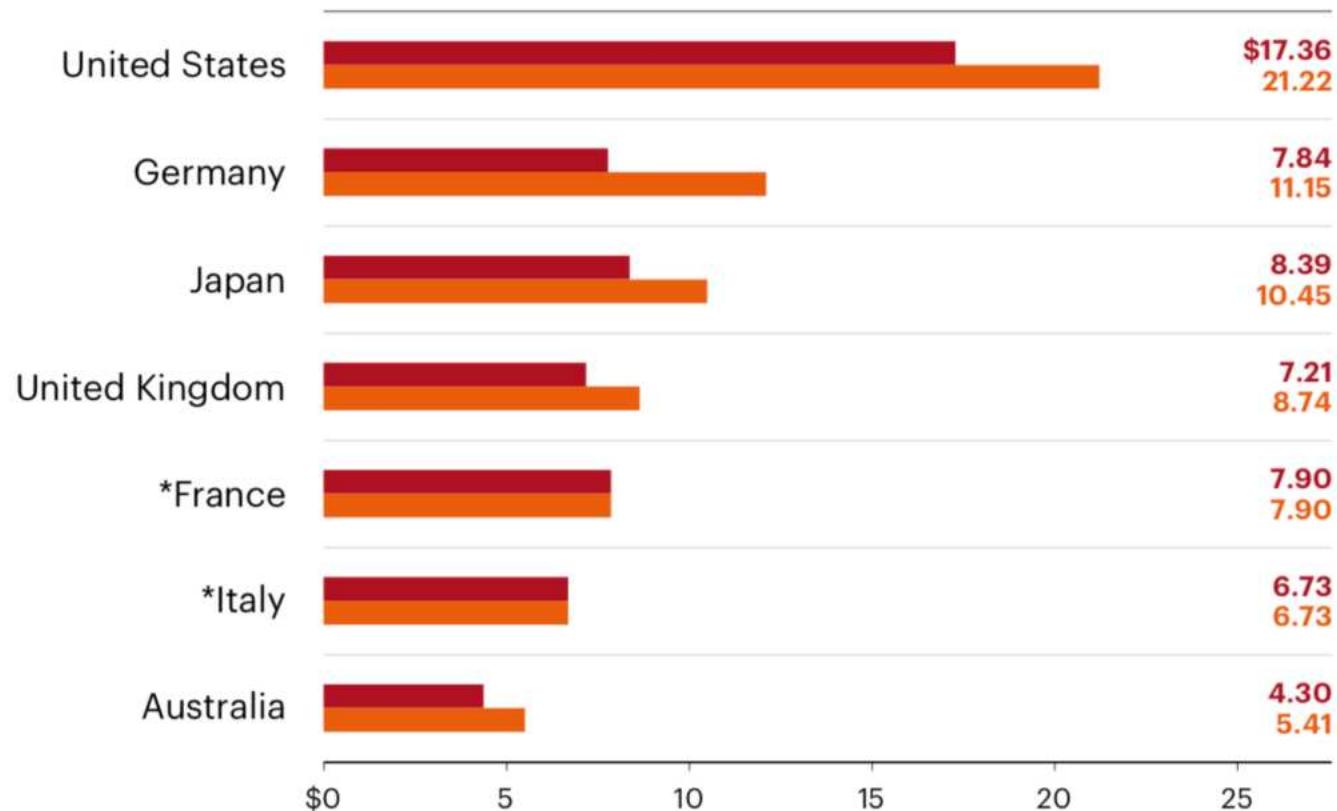


FIGURE 2

**Total cost of cyber crime
in seven countries**

*Historical data does
not exist for newly added
country samples

Legend

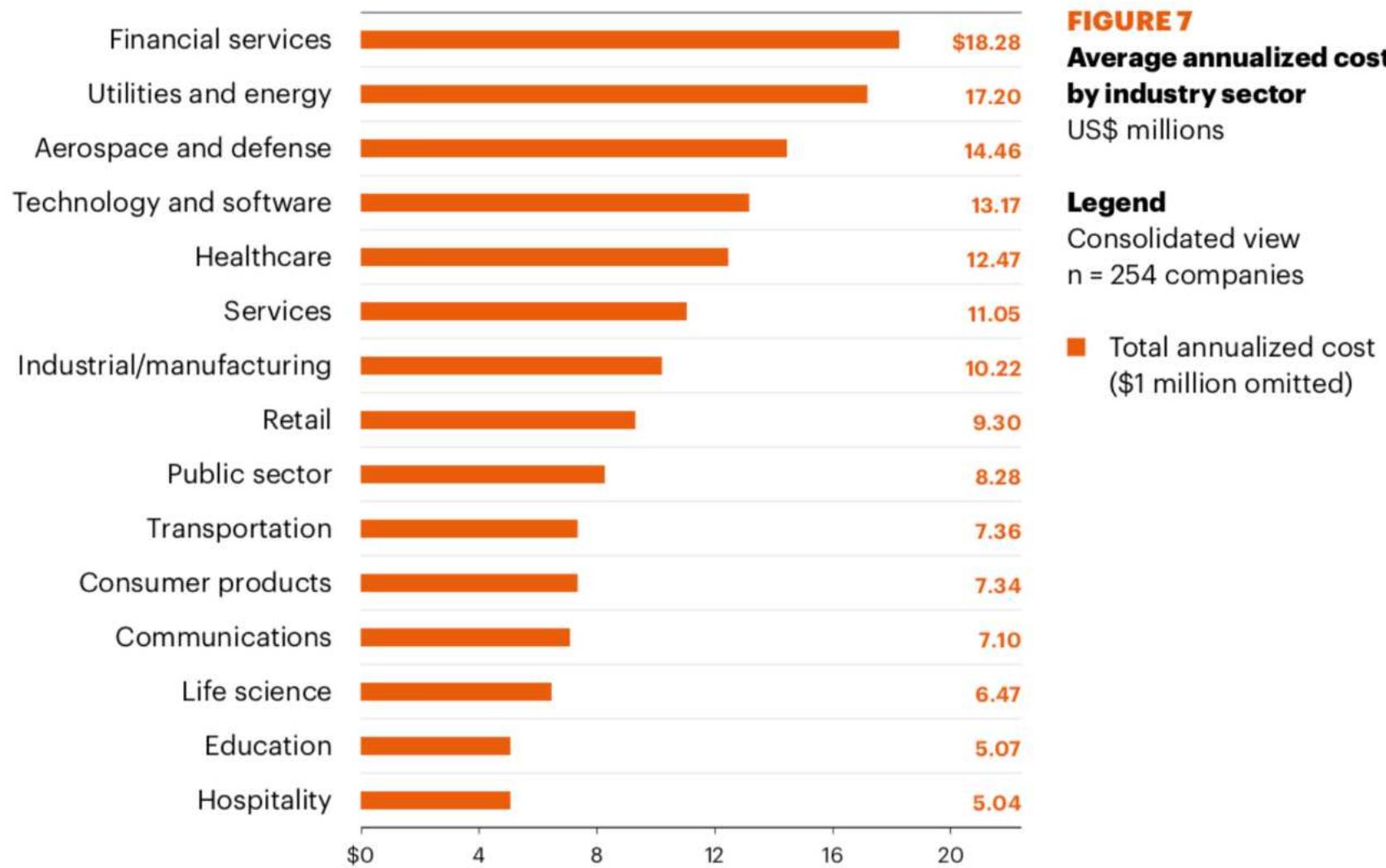
US\$ millions

n = 254

■ FY2016 (US\$ millions)

■ FY 2017 (US\$ millions)

Costo Cybercrime per settore industriale



Costo Cybercrime per tipo di attacco

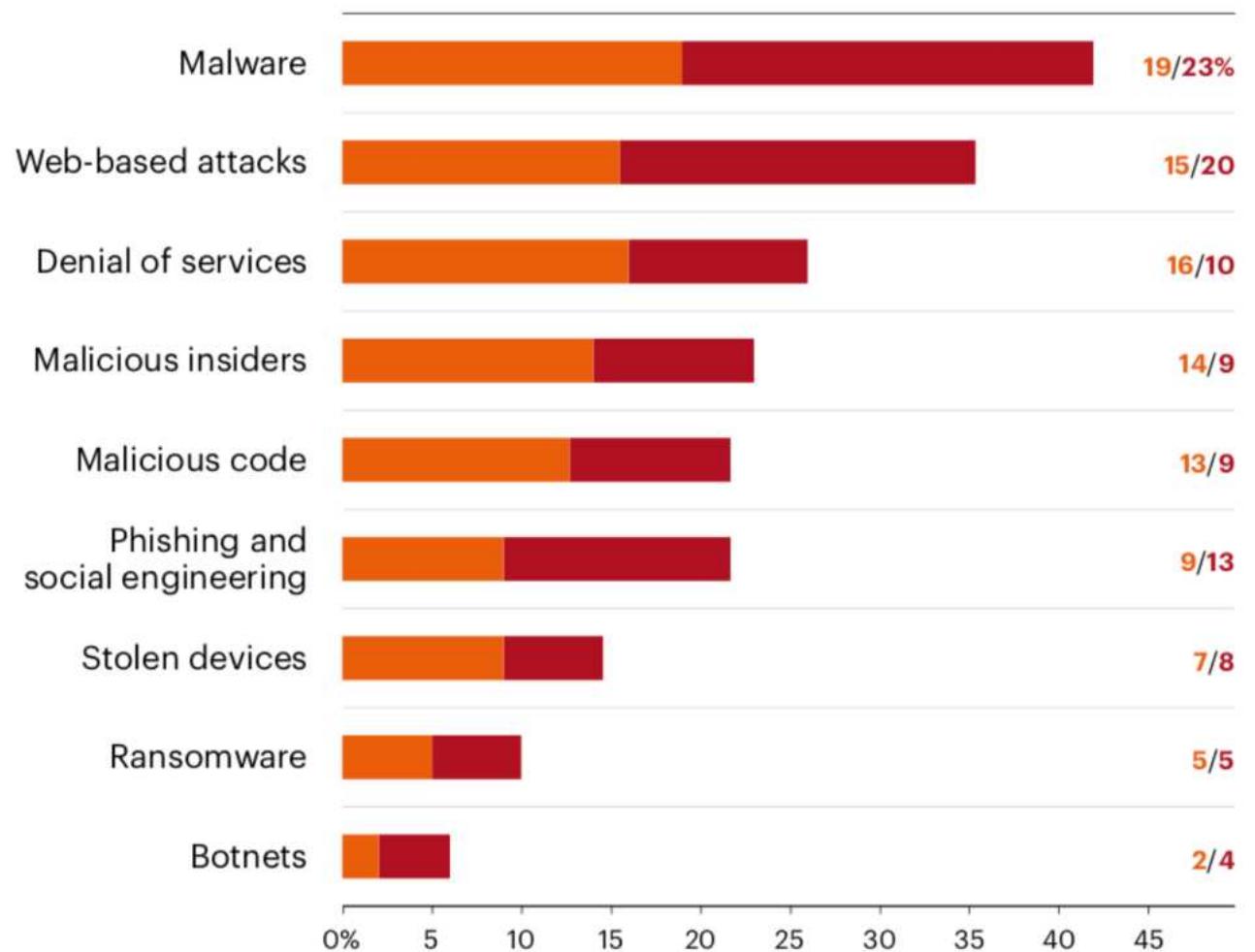


FIGURE 8
**Organizational size
affects the cost of nine
attack types**
Size measured according
to the number of
enterprise seats within
the participating
organizations

Legend
Consolidated view
n = 254 companies

- Above median
number of enterprise
seats
- Below median
number of enterprise
seats

Costo Cybercrime per tipo di attacco e paese

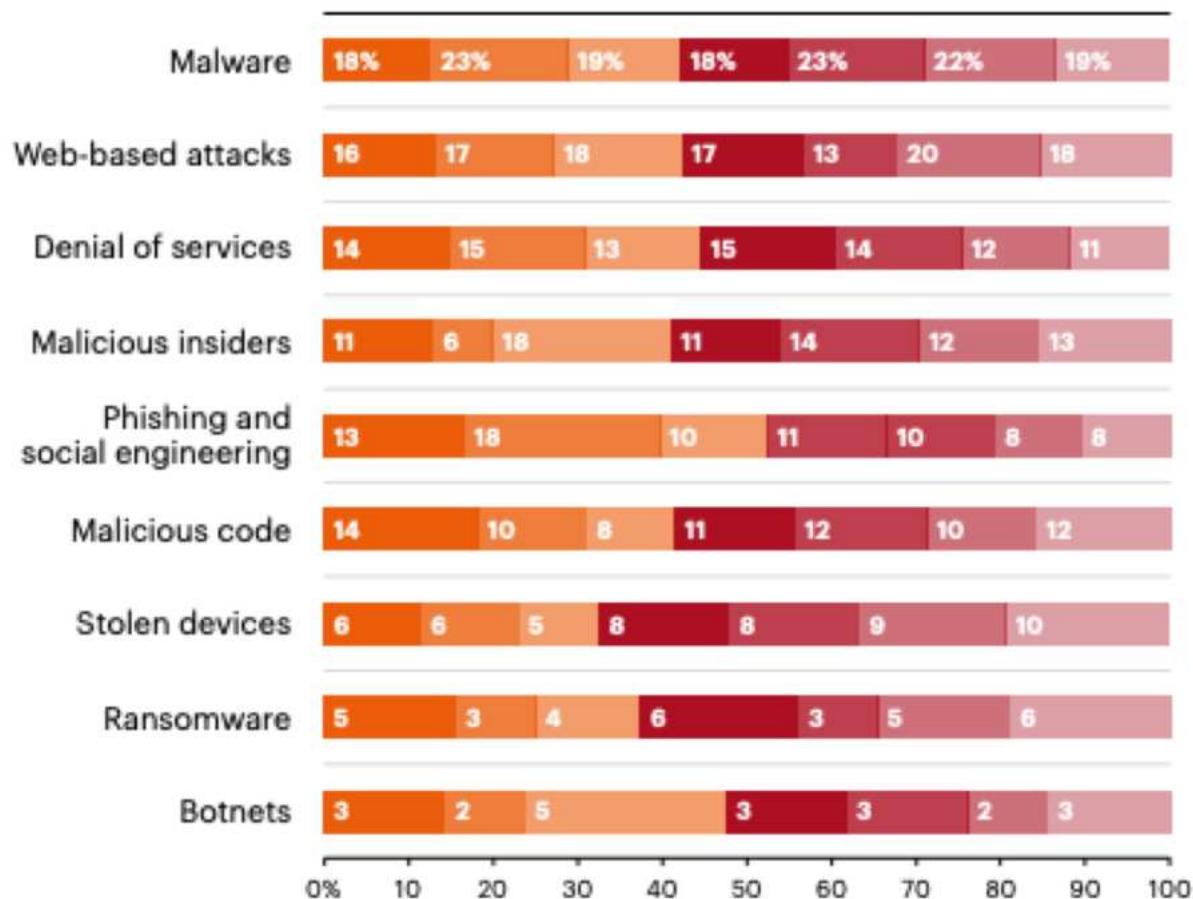


FIGURE 10
Percentage annualized
cyber crime cost by
attack type and country

Legend

Consolidated view
n = 254 companies

- United States
- Germany
- Japan
- United Kingdom
- Australia
- France
- Italy

Costo Cybercrime per attività interna

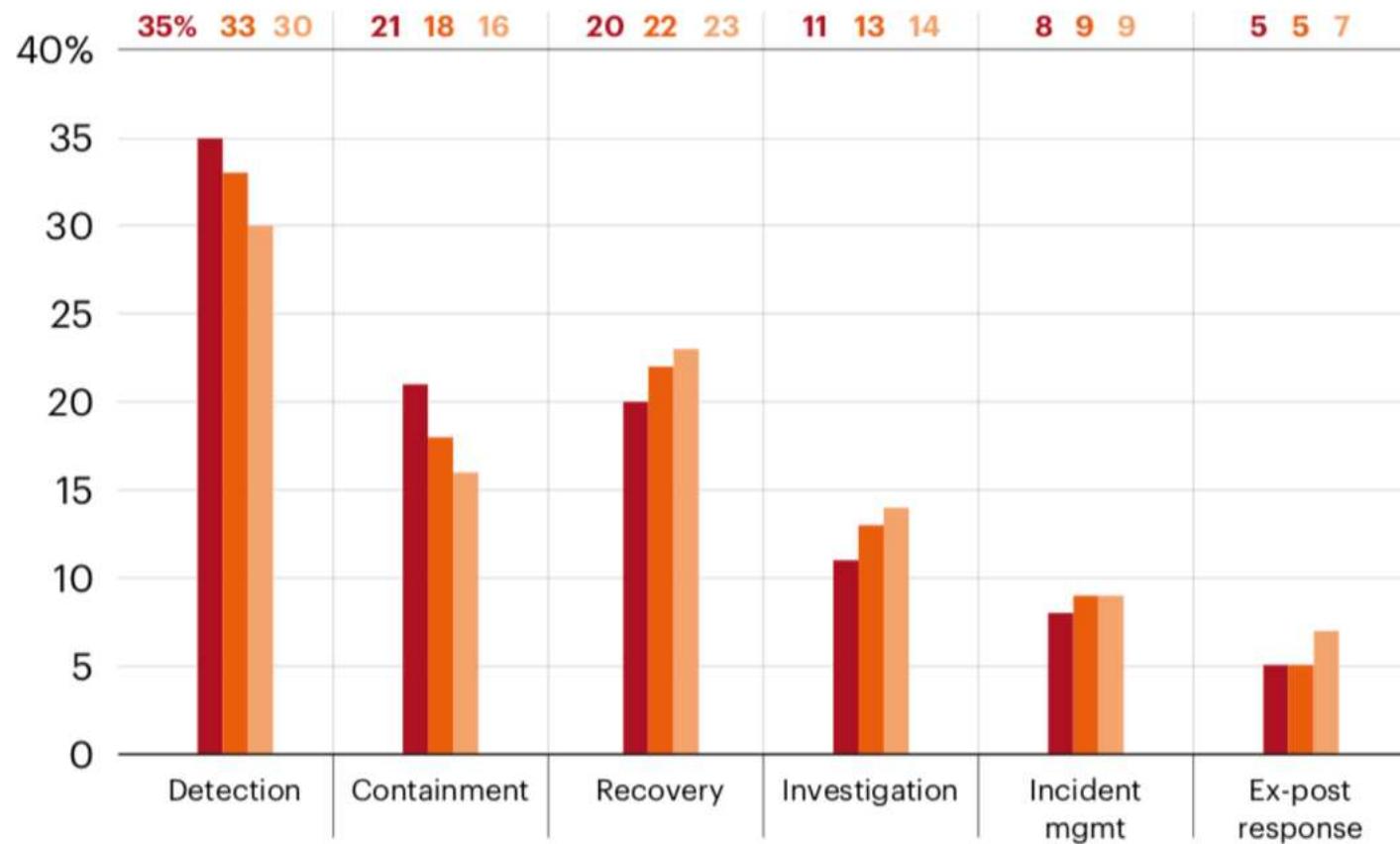


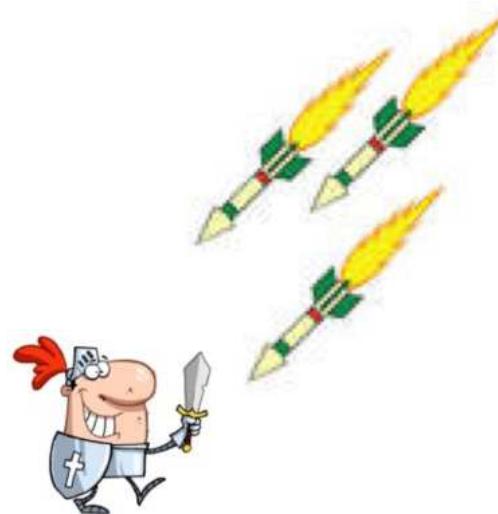
FIGURE 16
Percentage cost by internal activities

Legend
Consolidated view
n = 254 companies

- FY 2017
- FY 2016
- FY 2015

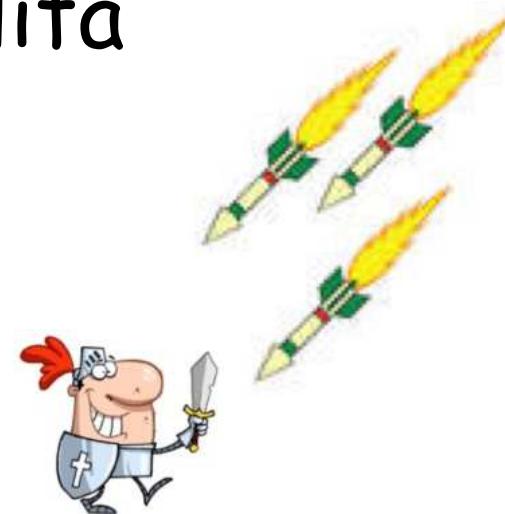
Difese statiche e dinamiche

- Difesa statica prima o poi cede
dopo nuovi attacchi



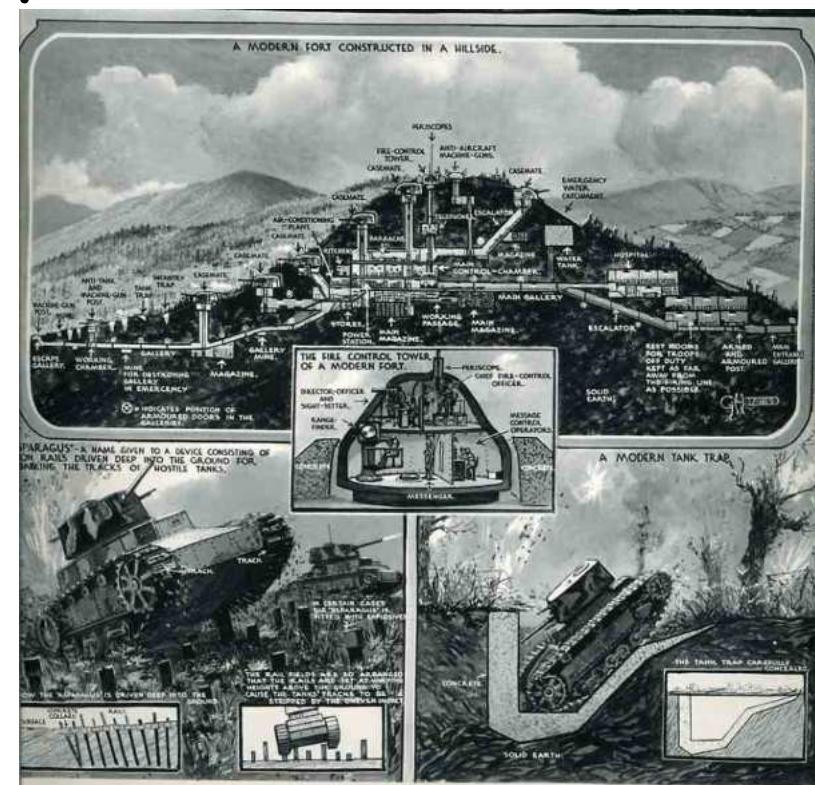
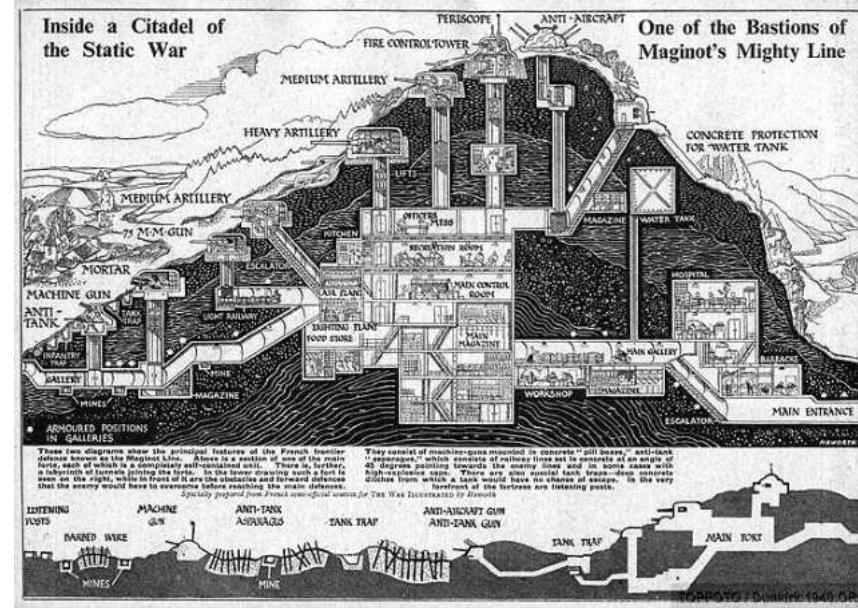
Difese statiche e dinamiche

- Difesa statica prima o poi cede dopo nuovi attacchi
- Difesa deve adattarsi dinamicamente ai nuovi attacchi per avere maggiori possibilità



Linea Maginot

- Costruita 1930-37
- Ministro della guerra André Maginot
- 400 km, frontiera franco-tedesca



Linea Maginot

- Costruita 1930-37
- Ministro della guerra André Maginot
- 400 km, frontiera franco-tedesca
- Francia invasa nel 1940
 - Tedeschi passarono attraverso il Belgio
- Idea difensiva vecchia (guerra 1914-18)
 - Non considerata l'estrema mobilità dei reparti meccanizzati



Weakest link principle



George Smith Patton, Jr.

- Generale americano
(1885 - 1945)
- "Fixed fortifications
are a monument to
the stupidity of man.
If mountain ranges and
oceans can be
overcome, anything
made by man can be
overcome."



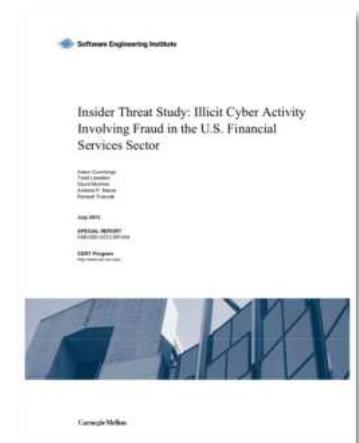
Muraglia cinese

- III secolo A.C.
- 8.851 km, spessore 9,5 m,
altezza 4,5 - 12 m
- Difesa da Mongoli
- *Insider attack nel 1644*: dopo che la sua concubina Chen Yuanyuan era stata presa dall'imperatore Li Zicheng, il generale Wu Sangui aprì le porte a Shенхаигуан e fece entrare i ribelli della Manciuria



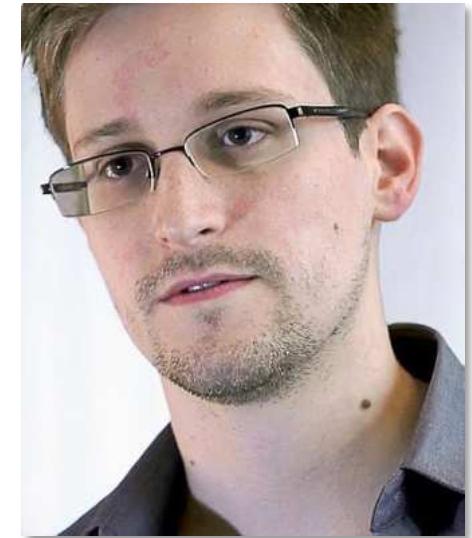
Insider Threat

- In 87% of the cases, the insider used legitimate system commands in committing the malicious activity. The insiders needed little technical sophistication because they tended to exploit known or newly discovered design flaws in systems used to enforce business rules or policies.
- Of the perpetrators, 81% planned their actions in advance.
- In 85% of the cases, someone else knew about the insider's actions before or during the malicious acts.
- In 81% of the cases, financial gain motivated the perpetrators. Revenge was the motivator in 23% of the cases, and 27% of the perpetrators were experiencing financial difficulties at the time they committed the acts.
- Perpetrators came from a variety of positions and backgrounds within the victim organization, but management had identified 33% of them as "difficult" and 17% as "disgruntled."
- Audit logs helped to identify the insiders in 74% of the cases.
- Of the victim organizations, 91% suffered financial loss, with amounts ranging from hundreds to hundreds of millions of dollars.
- Of the perpetrators, 80% committed the malicious acts while at work, during working hours.



Edward Snowden

- System administrator all'NSA (National Security Agency)
- Ottiene login e password di 20/25 colleghi ad NSA usando *social engineering*
- Nel maggio 2013 rivela migliaia di documenti classificati a giornalisti
- ha rivelato diverse informazioni su programmi di intelligence classificati, tra cui
 - PRISM: accesso diretto ad account americani di Google e Yahoo
 - Tempora: programma di sorveglianza britannico di GCHQ, partner di NSA
 - Xkeyscore: ricerca ed analisi dei dati Internet, collezionati ogni giorno, "almost anything done on the internet"
 - programma di intercettazione telefonica tra Stati Uniti e Unione europea riguardante i metadati delle comunicazioni
- 14 giugno 2013, accusato di spionaggio
- Ora ha asilo in Russia (fino al 2020)



Missili Scud

- Usati da Iraq, Gulf war (1990-91)
- Veicolo TEL (trasportatore-elevatore-lanciatore),
 - Autonomia carburante per distanza di 250 km (500 km andata e ritorno)
 - Velocità max 60 km/h
- Precisione scarsa: CEP 1100m a 440 km
- Molto mobile e difficile da individuare



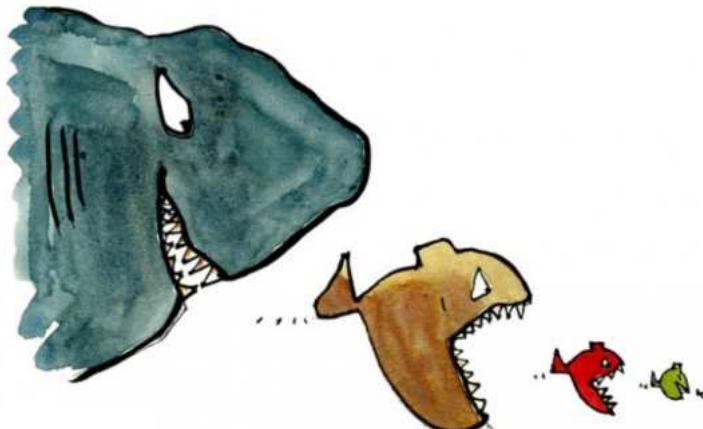
Prede e predatori

- Teoria dell'evoluzione
- Evoluzione dei predatori

Canini ed artigli più grandi ed affilati,

... ed evoluzione prede

corazze più resistenti e zampe più veloci



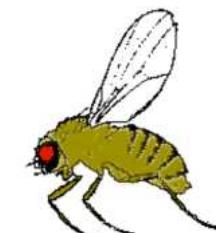
Antilocapra americana



- Habitat: prateria
- Predatori: lupo, coyote, lince rossa
- Animale terrestre più veloce dopo il ghepardo
 - Raggiunge i 100 km/h (superato solo su brevi distanze)
- Rileva movimenti ad una distanza di 4-5 km

Drosofilia (moscerino della frutta)

- Le ali di una mosca possono battere fino a 250 volte al secondo.
- Volo con tratti lineari, con rapidi cambi di direzione
 - Può ruotare di 90 gradi in meno di 50 millisecondi
- Presenta nervi ottici collegati direttamente ai muscoli delle ali (mentre in altri insetti c'è in ogni caso un passaggio attraverso il cervello), rendendo bassissimo il tempo di reazione





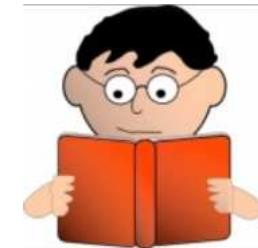
ABSTRACT

The diurnal thermophilic Saharan silver ant, *Cataglyphis bombycinus*, is the fastest of the North African *Cataglyphis* desert ant species. These highly mobile ants endure the extreme temperatures of their sand dune environment with outstanding behavioural, physiological and morphological adaptations. Surprisingly, *C. bombycinus* has comparatively shorter legs than its well-studied sister species *Cataglyphis fortis* from salt pan habitats. This holds despite the somewhat hotter surface temperatures and the more yielding sand substrate. Here, we report that *C. bombycinus* employs a different strategy in reaching high running speeds, outperforming the fastest known runs of the longer-legged *C. fortis* ants. Video analysis across a broad range of locomotor speeds revealed several differences to *C. fortis*. Shorter leg lengths are compensated for by high stride frequencies, ranging beyond 40 Hz. This is mainly achieved by a combination of short stance phases (down to 7 ms) and fast leg swing movements (up to 1400 mm s^{-1}). The legs of one tripod group exhibit almost perfect synchrony in the timings of their lift-offs and touch-downs, and good tripod coordination is present over the entire walking speed range (tripod coordination strength values around 0.8). This near synchrony in leg movement may facilitate locomotion across the yielding sand dune substrate.

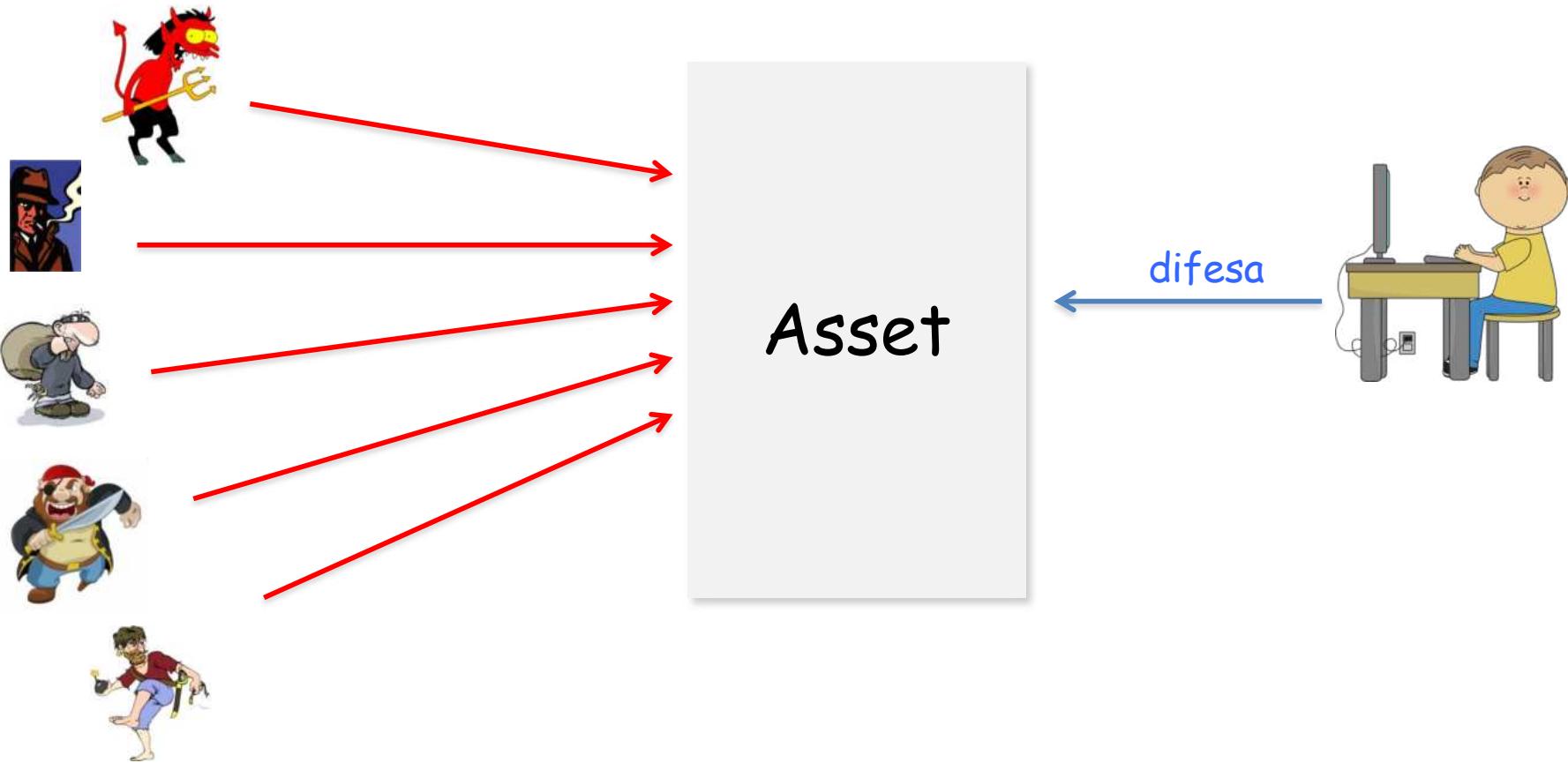
Mondo digitale esempio



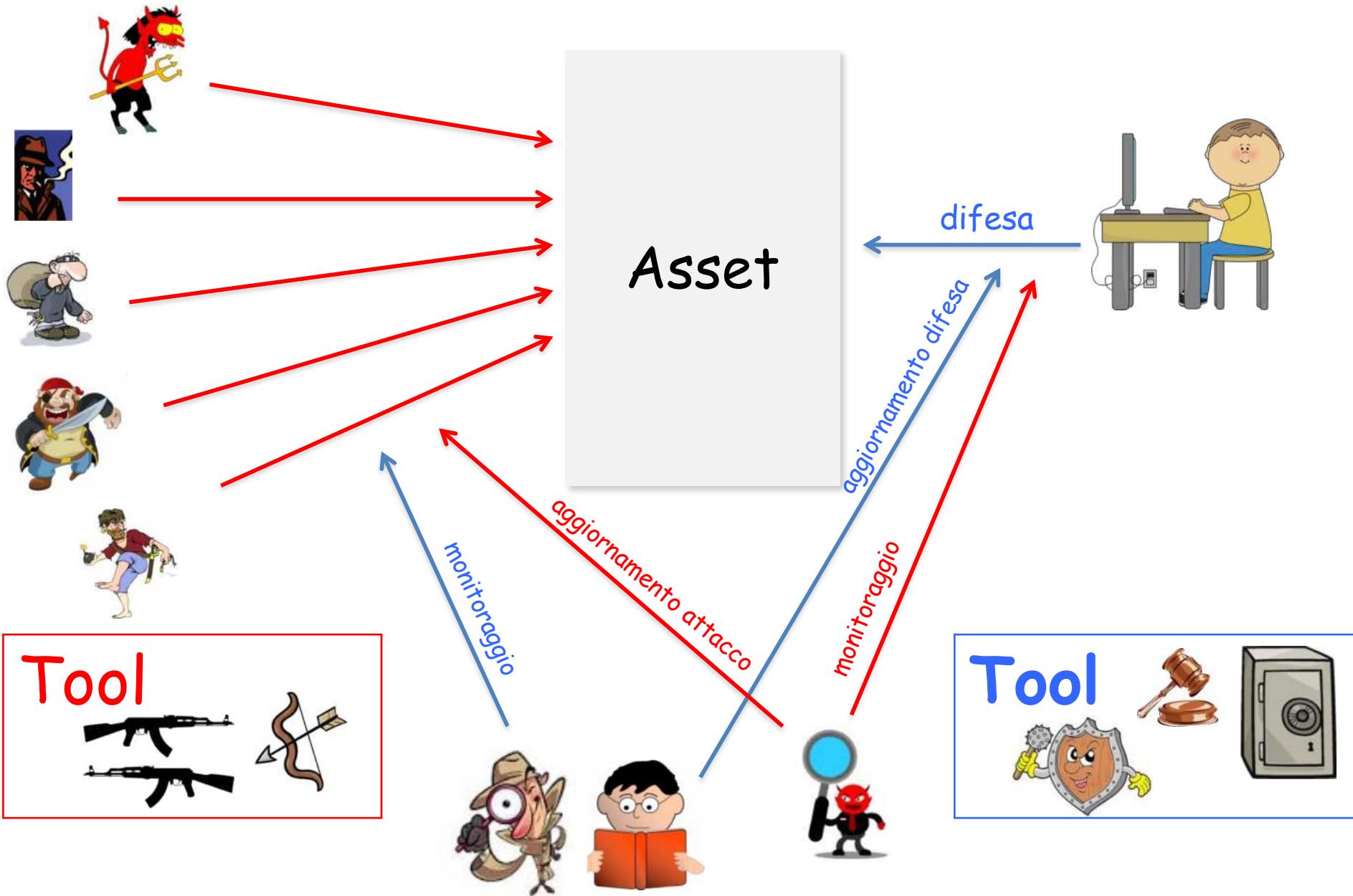
- Virus Polymorphic si modificano continuamente per evitare di essere rilevati.
- Autori dei virus modificano algoritmi di mutazione dopo aver appreso le nuove tecniche di rilevazione.
- Bisogna essere costantemente aggiornati e rispondere subito alle novità!



Scenario attacco e difesa



Scenario attacco e difesa



Vulnerabilità e Attacchi

Vulnerabilità

- Debolezza di un sistema di sicurezza che può essere utilizzata per causare danni

Attacco

- Sfruttamento di una vulnerabilità di un sistema

Classificazione vulnerabilità

hardware	susceptibility to humidity
	susceptibility to soiling
	susceptibility to dust
	susceptibility to unprotected storage
software	insufficient testing
	lack of audit trail
	design flaw
network	unprotected communication lines
	insecure network architecture
personnel	inadequate recruiting process
	inadequate security awareness
physical site	area subject to flood
	unreliable power source
organizational	lack of regular audits
	lack of continuity plans
	lack of security

Tipi di attacchi

Attacchi passivi: non alterano i dati in transito

- Intercettazione del traffico
- Analisi del traffico

Attacchi attivi: modificano il flusso di dati o creano un falso flusso:

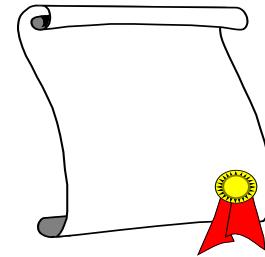
- Riproduzione
- Modifica dei messaggi
- Denial of service



Documenti fisici e digitali

Documenti fisici:

- La copia è distinguibile dall'originale
- L'alterazione lascia tracce
- La "prova" di autenticità si basa su caratteristiche fisiche (firma, ceralacca, ...)



Documenti digitali

- La copia è indistinguibile dall'originale
- L'alterazione non lascia tracce
- La "prova" di autenticità non si basa su caratteristiche fisiche

Sicurezza Dati: obiettivi

- Confidenzialità
- Autenticazione
- Non-ripudio
- Controllo Accessi
- Integrità
- Anonimia
- Disponibilità Risorse
- Protezione Proprietà Intellettuale

Confidenzialità

Privacy, Segretezza

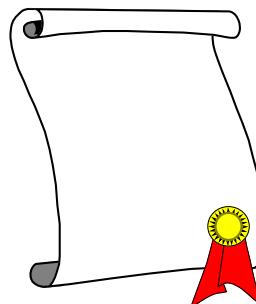


Informazioni { trasmesse
memorizzate

sono accessibili in lettura
solo da chi è autorizzato

Autenticazione

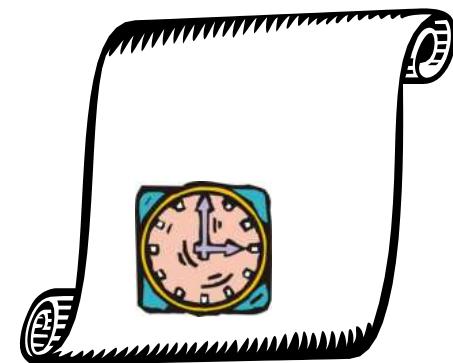
messaggi



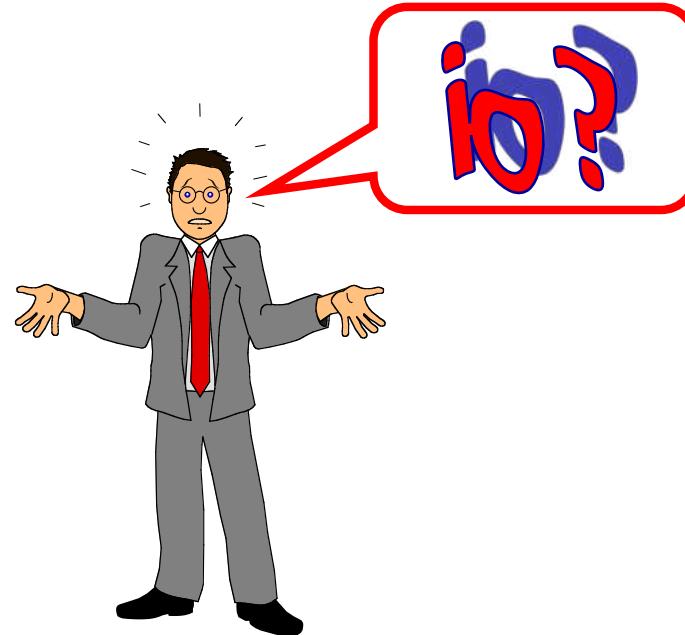
entità
(Identificazione)



tempo
(Timestamp)



Non-ripudio



{ Chi invia
Chi riceve

non può negare la
trasmissione del
messaggio

Controllo Accessi

Accesso alle informazioni

controllato da o per

il sistema



Integrità

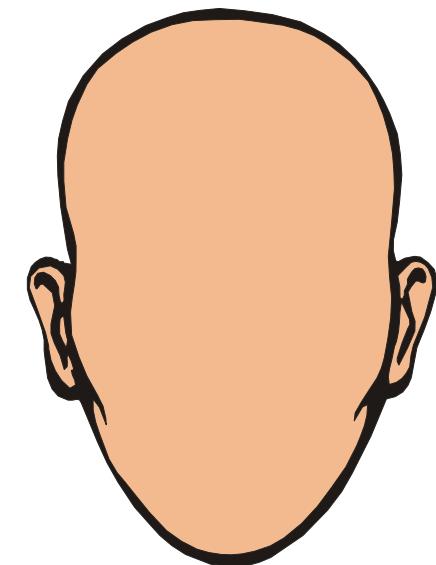
Solo chi è autorizzato può
modificare l'attività di un
sistema o le informazioni
trasmesse



modifica = scrittura, cambiamenti, cancellazione,
creazione, ritardi, replay e riordino
di messaggi, ...

Anonimia

Protezione
dell'identità o del
servizio utilizzato



Disponibilità Risorse

Risorse **disponibili** a chi è
autorizzato quando necessario

Diverse attese:

- presenza di oggetti e servizi utilizzabili
- capacità di soddisfare le richieste di servizi
- progresso: tempo di attesa limitato
- adeguato tempo del servizio

Protezione Proprietà Intellettuale

(Digital Rights Management - DRM)

Controllare l'uso, la modifica e la distribuzione di dati soggetti a forme di copyright



DIGITAL
RIGHTS
MANAGEMENT

Contenuto Corso

➤ Prima parte: Crittografia

- Cifrari simmetrici
- Cifrari asimmetrici
- Firme digitali
- Funzioni hash e integrità dei dati

➤ Seconda parte: Sicurezza su Reti

- PKI
- Autenticazione utenti
- Posta elettronica sicura
- Sicurezza IP e WWW
- Sicurezza sistemi
 - Intrusioni, software malizioso, firewall

Contenuto Corso

➤ Terza parte:

- Crittografia (Curve ellittiche, ...)
- Serrature
- Steganografia
- Watermark
- Wireless Security
- Bluetooth
- Digital Right Management (DRM)
- Digital Video Broadcasting (DVB), Pay Tv
- Radio-Frequency Identification (RFId)
- Anonimia
- Sicurezza del Software
- Buffer Overflow
- Psicologia della Sicurezza
- Economia della Sicurezza
- Elezioni Elettroniche
- Micropagamenti
- Malware
- SPAM
- Analisi del Rischio
- Digital Forensic
- Bitcoin
- Anonimia
- Cloud Storage
- ...

Argomenti (presentazioni)

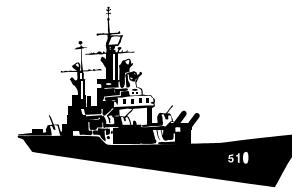
- Introduzione
- Crittografia Classica
- Elementi di Crittoanalisi
- Cifrari a Blocchi
- Advanced Encryption Standard
- Stream Ciphers
- Teoria dei Numeri Computazionale
- Cifrari Asimmetrici
- Accordo su Chiavi
- Crittosistema di ElGamal
- Funzioni Hash
- MAC
- Firme Digitali
- Generatori Pseudocasuali
- Autenticazione
- Curve Ellittiche
- Post Quantum Cryptography
- Identity based Cryptography
- Protocolli Crittografici
- Anonimia
- Certificati e PKI
- Firewall
- Autenticazione Single Sign On
- Protocolli SSL e TLS
- IPsec e VPN
- Codice Malizioso
- Protezione del Software
- Digital Watermarking
- Bitcoin
- Cloud Storage Sicuro
- DVB e PayTV
- Digital Forensics
- Falso Alibi Digitale
- SPID e PEC
- Analisi Sicurezza Serrature
- Social Engineering

Crittografia

Dall'antichità fino a pochi anni fa:

- Essenzialmente comunicazioni private
- Usi Militari e Diplomatici

χρυπτοσ γραφια λογοσ



Oggi: studio di tecniche ed applicazioni che dipendono dall'esistenza di problemi difficili

Strumenti Crittografici: OpenSSL

- Progetto Open Source nato nel dicembre del 1998
- OpenSSL fornisce implementazioni per
 - Funzioni Crittografiche
 - Protocolli Secure Sockets Layer (SSL) e Transport Layer Security (TLS)
- OpenSSL comprende
 - Comandi eseguibili per funzioni crittografiche
 - Una libreria contenente API, mediante la quale i programmatori possono sviluppare le proprie applicazioni crittografiche
- OpenSSL supporta crittografia basata su curve ellittiche
 - Elliptic Curve Cryptography



Alcuni metodi antichi di cifratura

Scitala

- Usata dai Greci antichi, in particolare dagli Spartani, nelle missioni militari
 - Descritta da Plutarco (46-125 d.C.) in "Vita di Lisandro", *Le vite parallele* di Plutarco



Alcuni metodi antichi di cifratura

Quadrato di Polibio o Scacchiera di Polibio

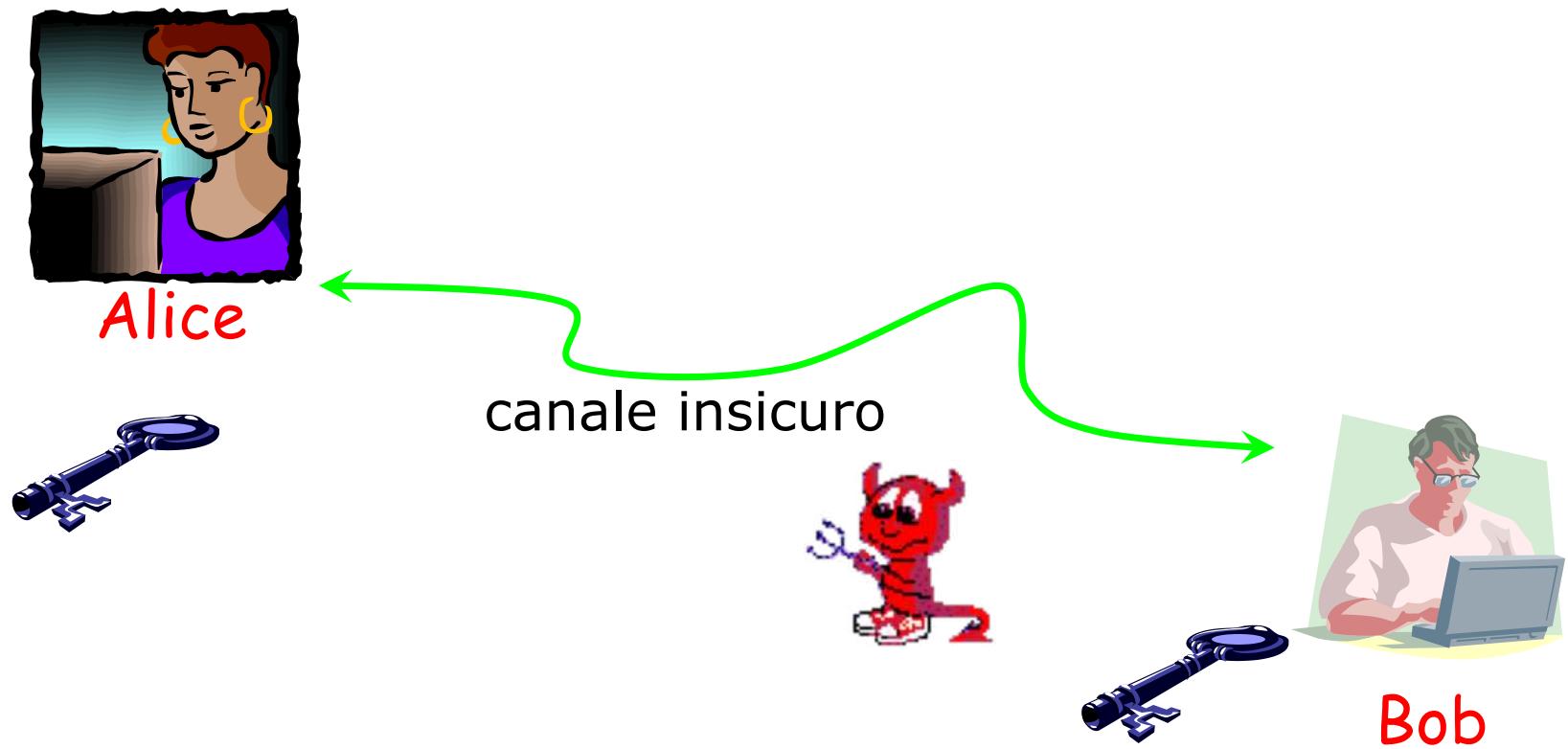
➤ Descritto da Polibio (206-124 a.C.) nelle "Storie"

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I J	K
3	L	M	N	O P	
4	Q	R	S	T	U
5	V	W	X	Y	Z

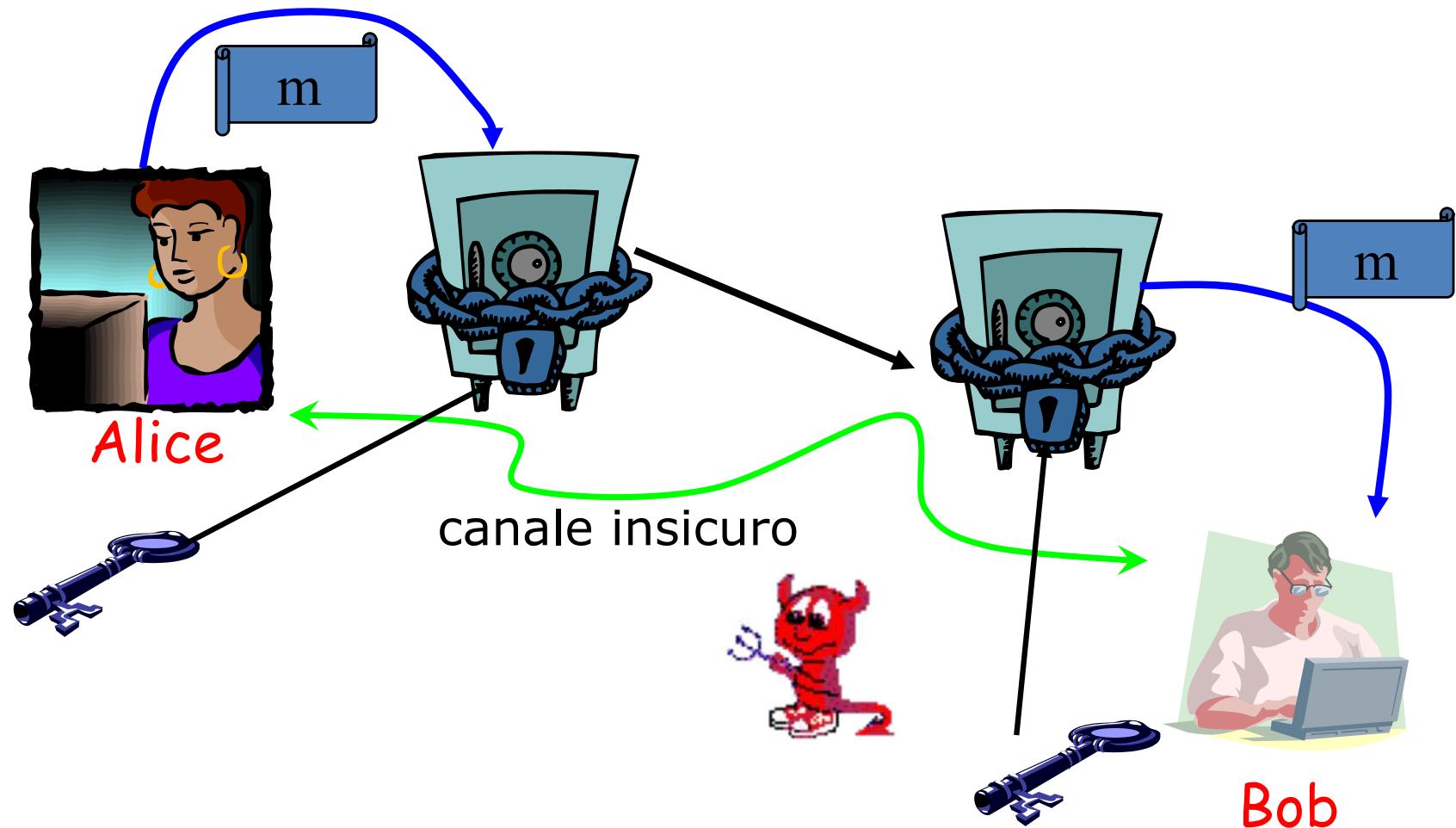


testo in chiaro: C A S A
testo cifrato: (1,3) (1,1) (4,3) (1,1)

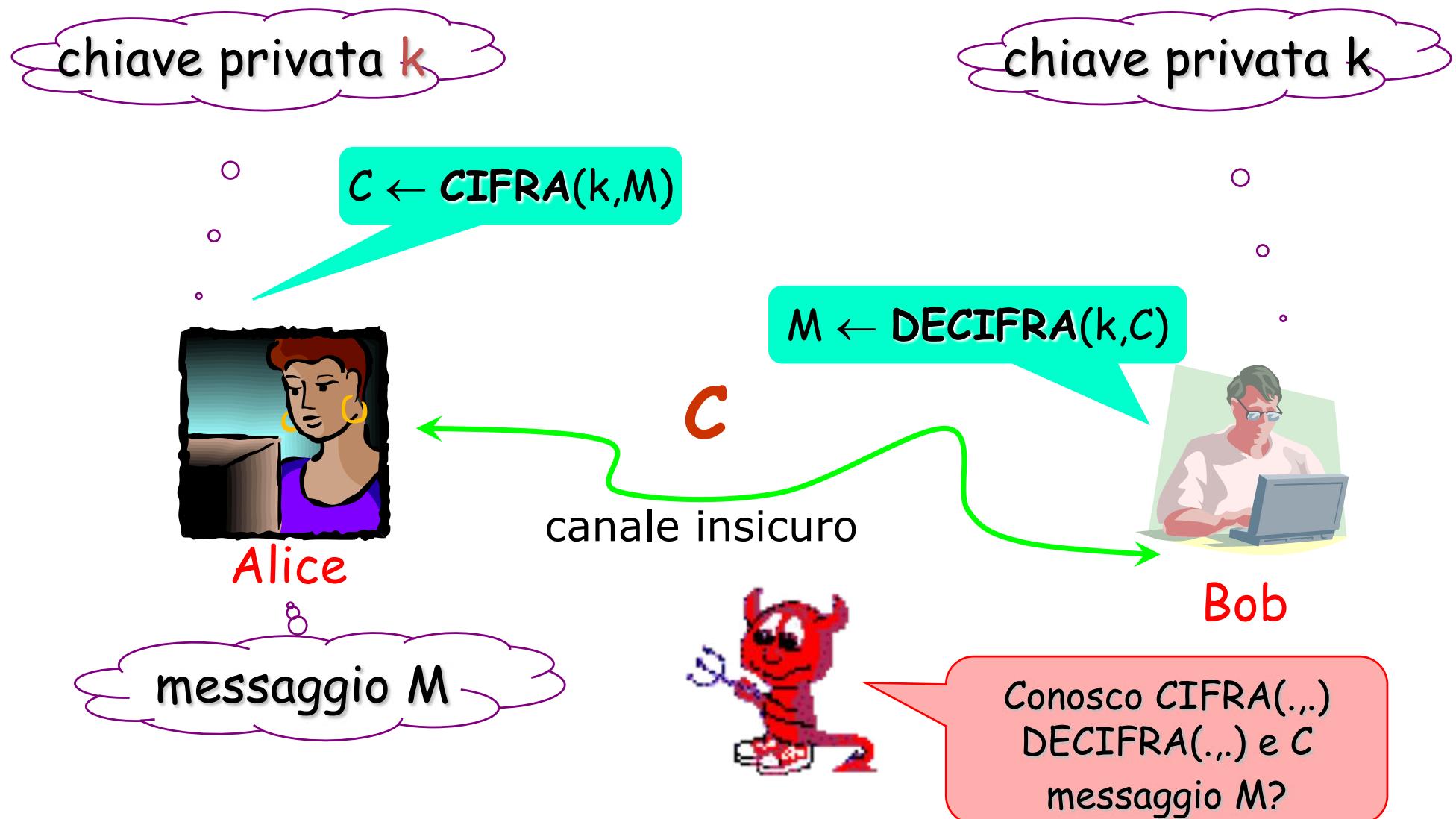
Cifrari simmetrici



Cifrari simmetrici



Cifrari simmetrici



Cifrari simmetrici

➤ Cifrari a blocco

- DES, Triplo DES, AES
- Blowfish, RC5, RC6, ...

Li vedremo ed
utilizzeremo in
OpenSSL

➤ Stream Cipher

- LSFR (Linear Feedback Shift Register)
- RC4

Li vedremo ed
utilizzeremo in
OpenSSL

Benefici di AES

NIST

Search NIST  NIST MENU

NEWS

NIST's Encryption Standard Has Minimum \$250 Billion Economic Benefit, According to New Study

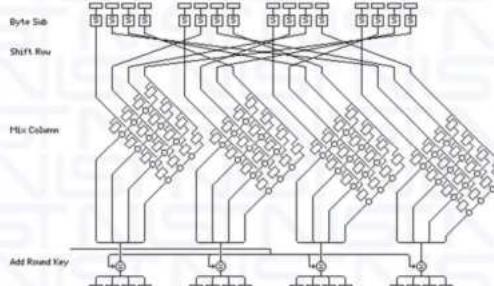
An international competition led to the voluntary standard that today protects millions of IT systems.

September 19, 2018

NIST GCR 18-017

The Economic Impacts of the Advanced Encryption Standard, 1996 - 2017



David P. Leech
Stacey Ferris, CPA
John T. Scott, Ph.D.
September 2018

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

This publication is available free of charge from: <https://doi.org/10.6028/NIST.GCR.18-017>

<https://nvlpubs.nist.gov/nistpubs/gcr/2018/NIST.GCR.18-017.pdf>

Amateurs Produce Amateur Cryptography

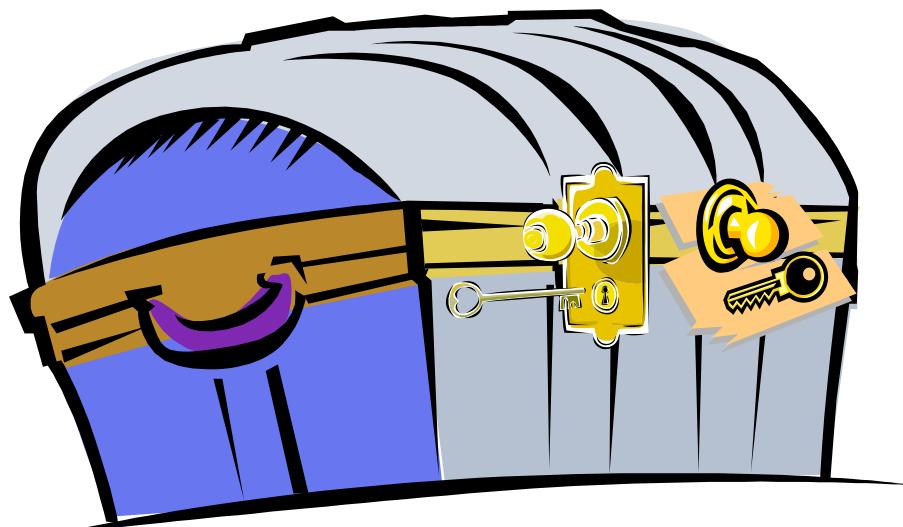
Anyone can design a cipher that he himself cannot break. This is why you should uniformly distrust amateur cryptography, and why you should only use published algorithms that have withstood broad cryptanalysis. All cryptographers know this, but non-cryptographers do not. And this is why we repeatedly see bad amateur cryptography in fielded systems.

Bruce Schneier

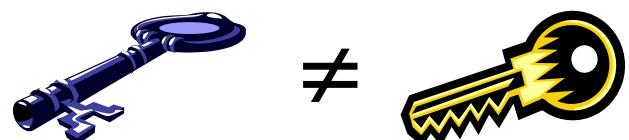
https://www.schneier.com/blog/archives/2015/05/amateurs_produc.html

Cifrari asimmetrici

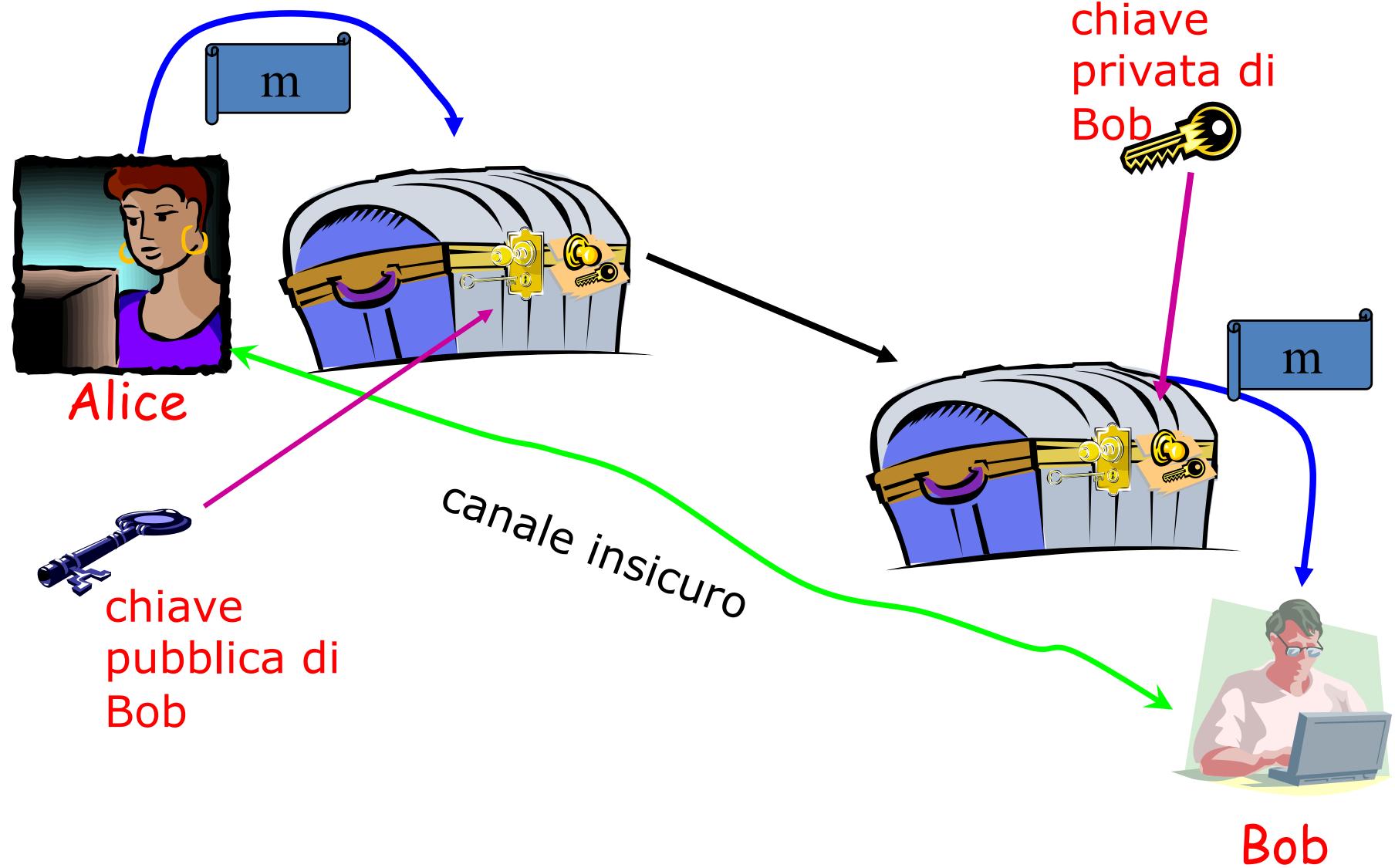
- Usano una cassaforte con due lucchetti
 - Con una chiave (**pubblica**) chiudiamo la cassaforte
 - Con l'altra chiave (**privata**) apriamo la cassaforte



Public key ≠ Private key



Cifrari asimmetrici



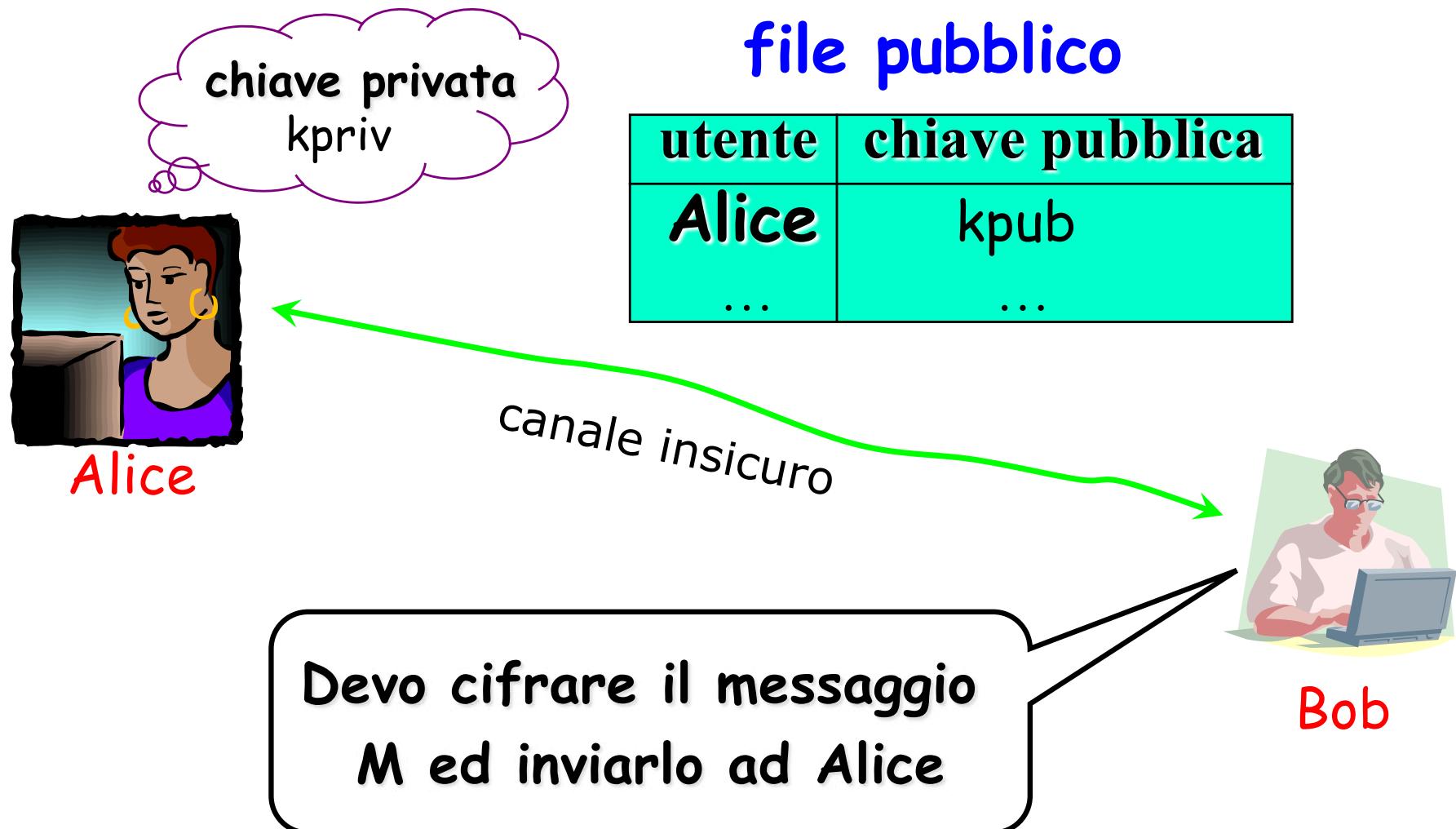
Cifrari asimmetrici



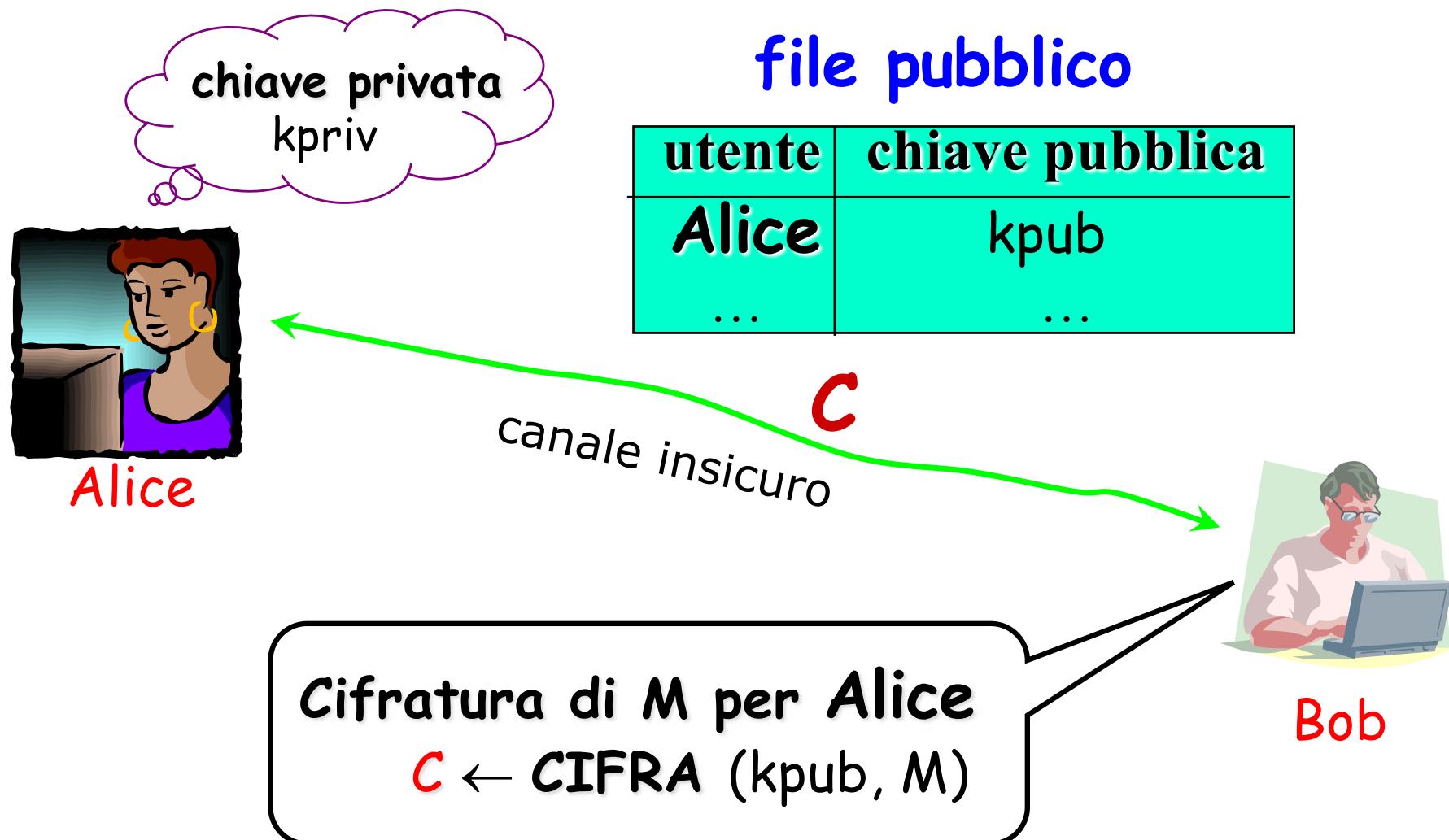
file pubblico

utente	chiave pubblica
Alice	kpub
...	...

Cifratura



Cifratura



Decifratura

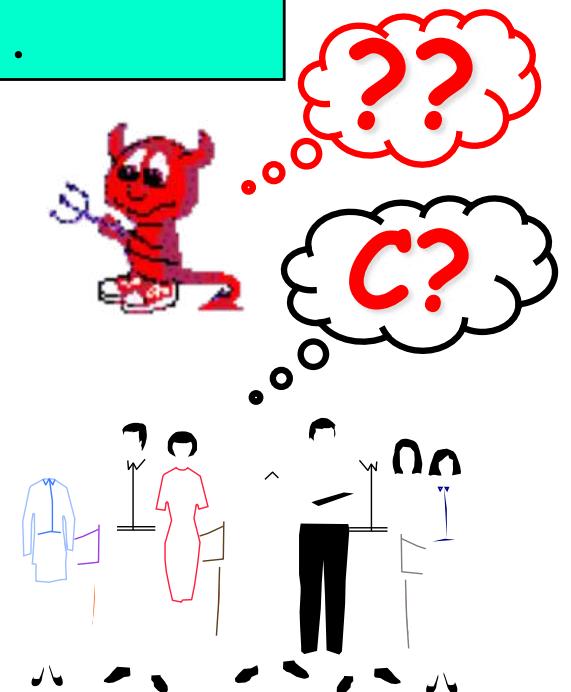
Devo decifrare il messaggio cifrato **C**



Alice

file pubblico

utente	chiave pubblica
Alice	kpub
...	...



Decifratura

chiave privata
kpriv

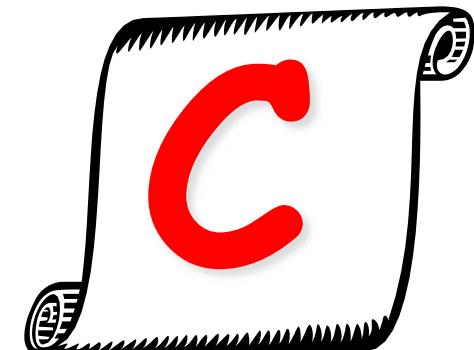


Alice

file pubblico

utente	chiave pubblica
Alice	kpub
...	...

Decifratura di C
 $M \leftarrow \text{DECIFRA} (kpriv, C)$



Cifrari asimmetrici

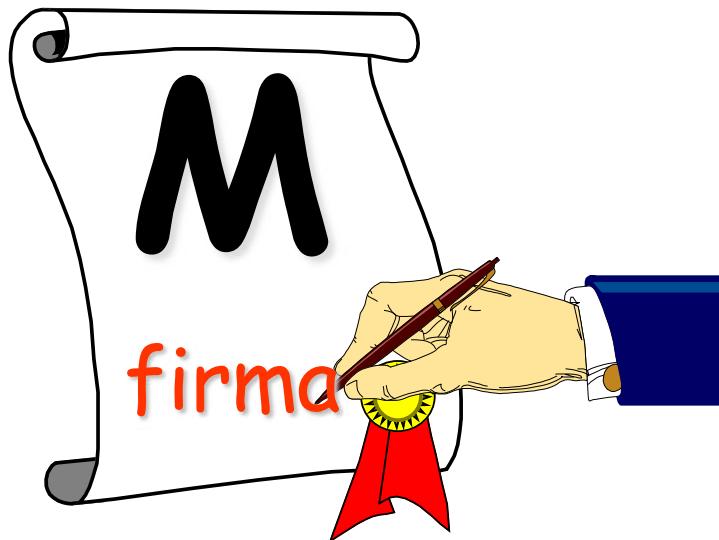
- Chiunque può cifrare un messaggio per Alice
- Solo Alice può decifrare un messaggio cifrato per lei
- Non ci sono chiavi condivise tra Alice e Bob
 - Ciascuno dei due utenti genera da solo la propria coppia di chiavi e rende pubblica la chiave pubblica
- Ogni utente memorizza una sola chiave (privata)

Cifrari asimmetrici

- RSA
- El Gamal
- Sistemi basati su curve ellittiche
- Post-quantum cryptosystem

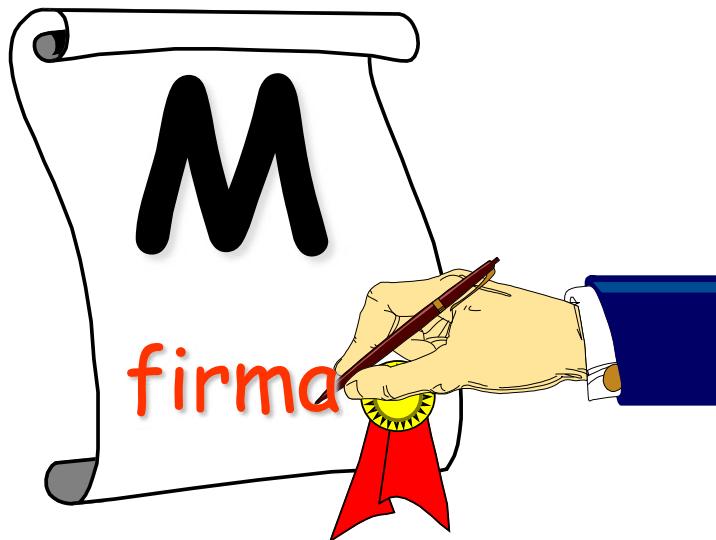
Li vedremo ed
utilizzeremo in
OpenSSL

Firma Digitale



Equivalent alla firma
convenzionale

Firma Digitale

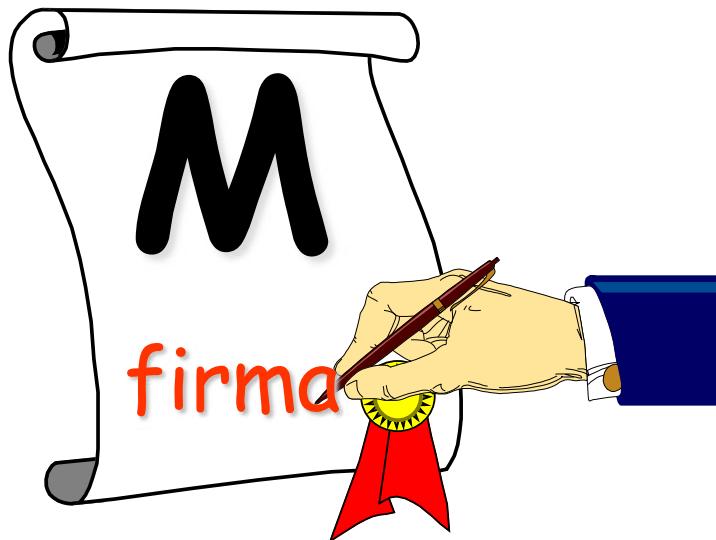


Equivalent alla firma
convenzionale

Soluzione naive:

incollare firma digitalizzata

Firma Digitale



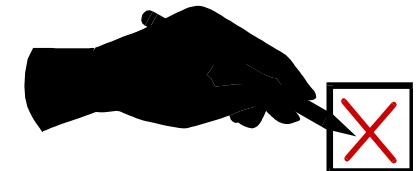
Equivalent alla firma
convenzionale

Soluzione naive:
incollare firma digitalizzata



Requisiti per la Firma Digitale

La firma digitale deve poter essere facilmente prodotta dal legittimo firmatario

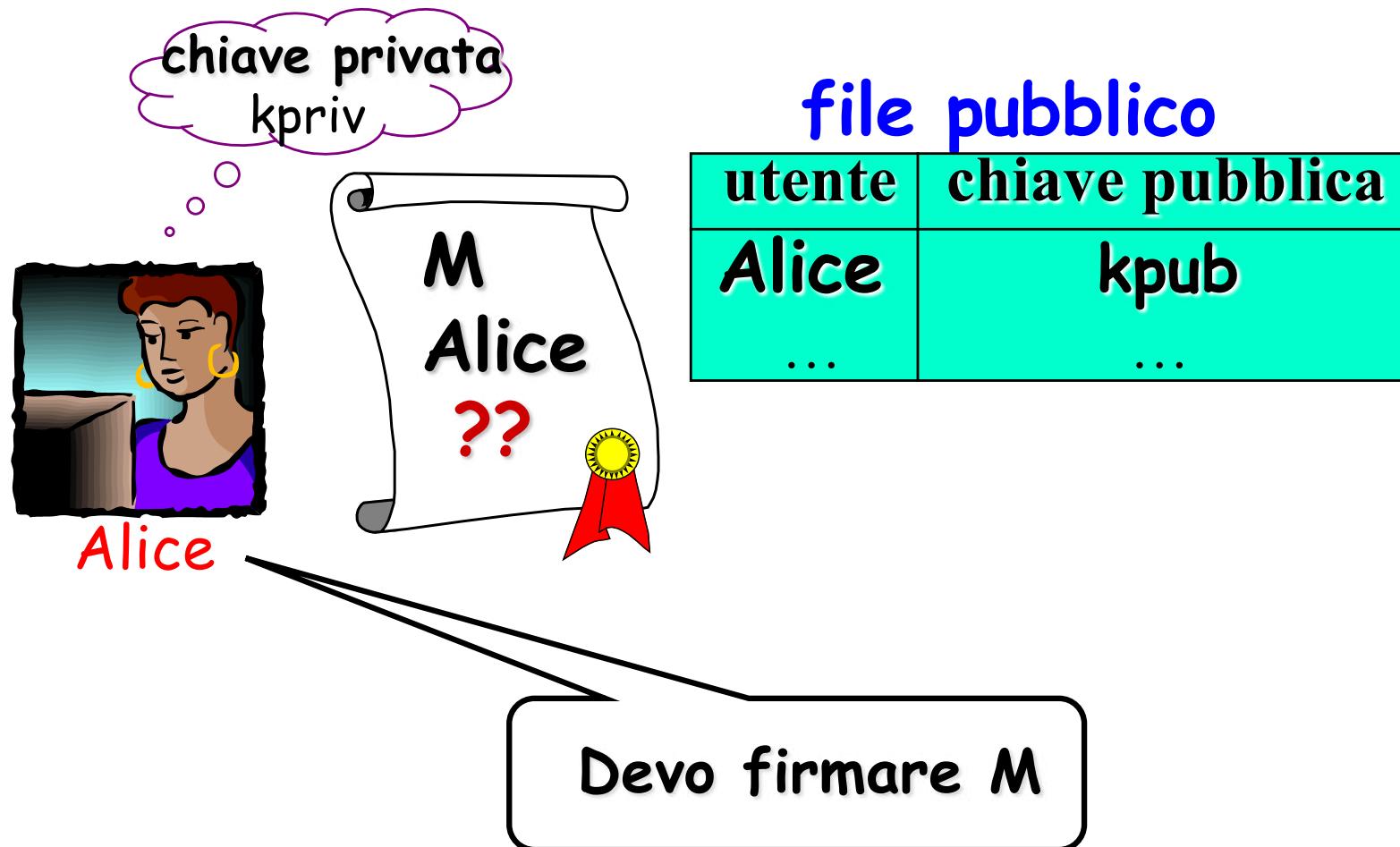


Nessun utente deve poter riprodurre la firma di altri

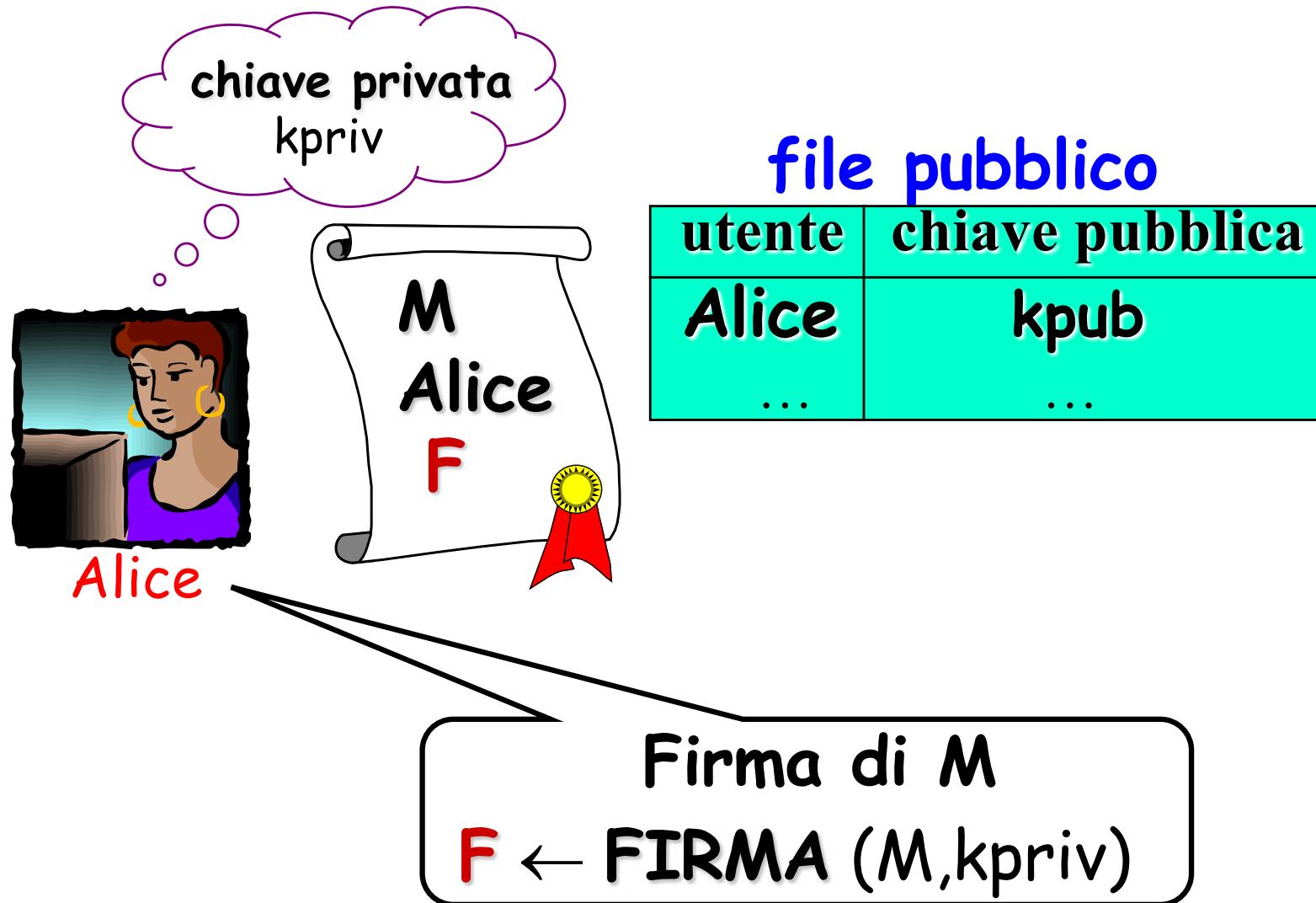
Chiunque può facilmente verificare una firma



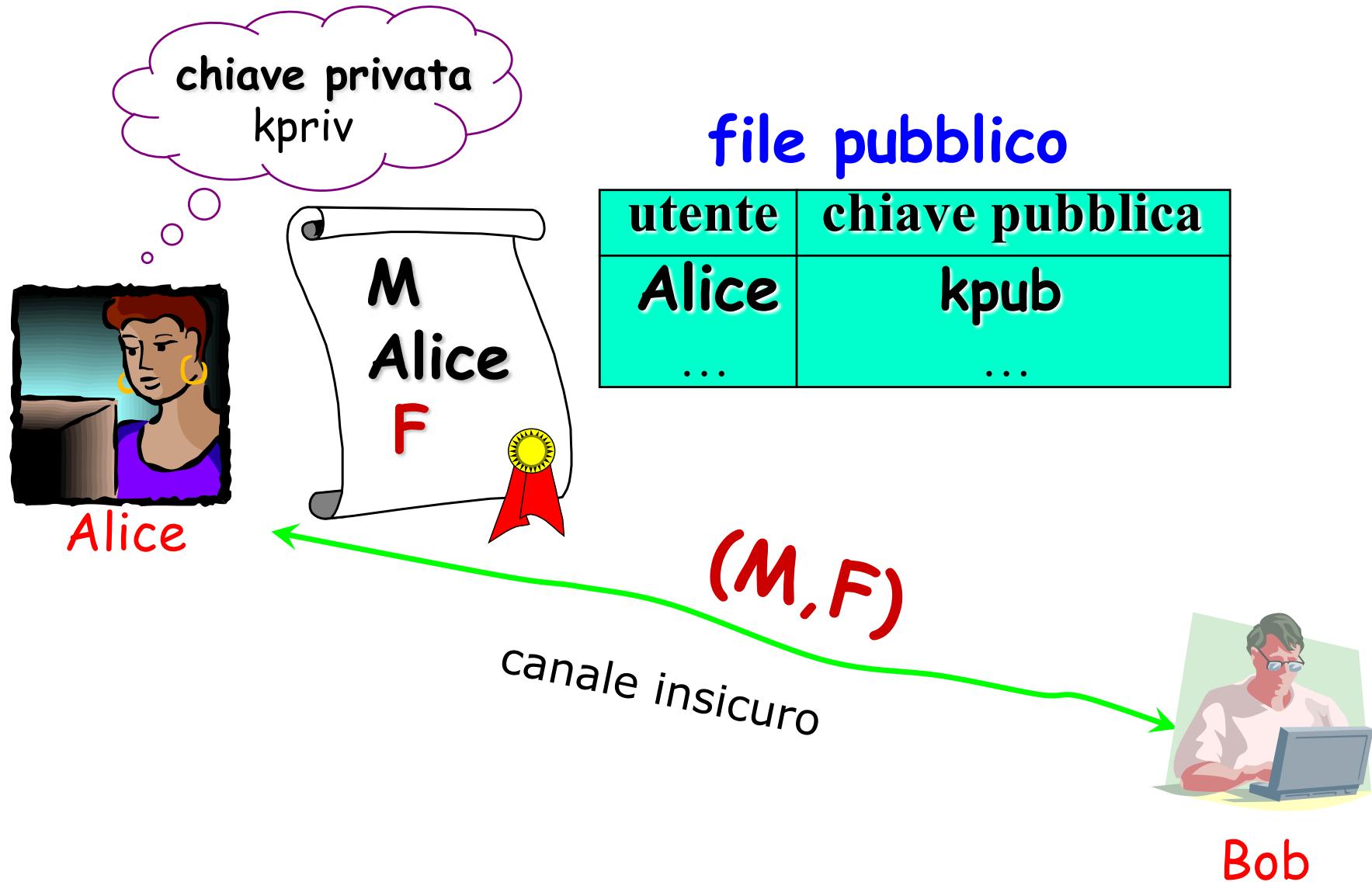
Firma digitale



Firma digitale



Firma digitale



Verifica firma digitale



file pubblico

utente	chiave pubblica
Alice	kpub
...	...

Devo verificare se F
è una firma di Alice per M



Bob

Verifica firma digitale



file pubblico

utente	chiave pubblica
Alice	kpub
...	...

Verifica firma di M

vera se **VERIFICA** (F, M, k_{pub}) = SI
falsa altrimenti



Bob

Firma digitale

- RSA
 - El Gamal
 - DSA
 - ECDSA (basato su curve ellittiche)
 - Post-quantum signature scheme
-
- Li vedremo ed utilizzeremo in OpenSSL

Public Key Infrastructure

- Come vengono distribuite le chiavi pubbliche?
- Chi ci assicura che una chiave pubblica è quella di un prefissato utente?



Public Key Infrastructure

Mondo fisico

- Carta di identità

Un'autorità riconosciuta lega un nome ad una foto



Mondo digitale

- Certificato digitale

Un'autorità riconosciuta lega un nome ad una chiave



Public Key Infrastructure

Insieme di hardware, software, procedure,
politiche, per

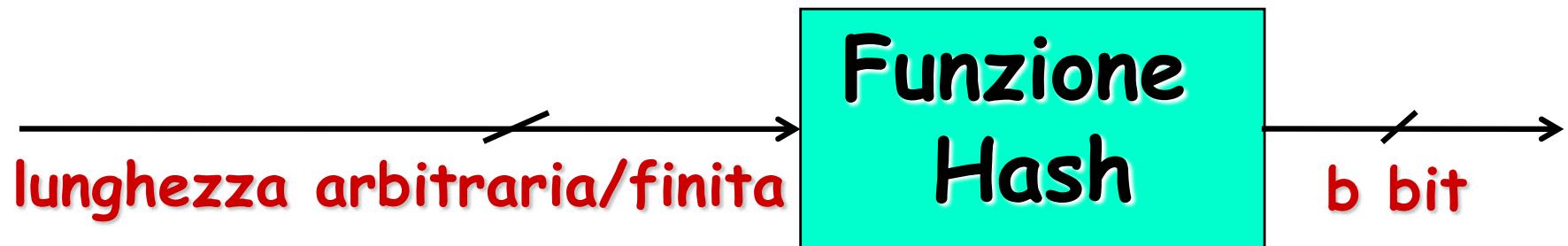
- Creare
- Gestire
- Memorizzare
- Distribuire
- Revocare



certificati digitali

Vedremo come creare e gestire una PKI mediante OpenSSL

Funzioni Hash



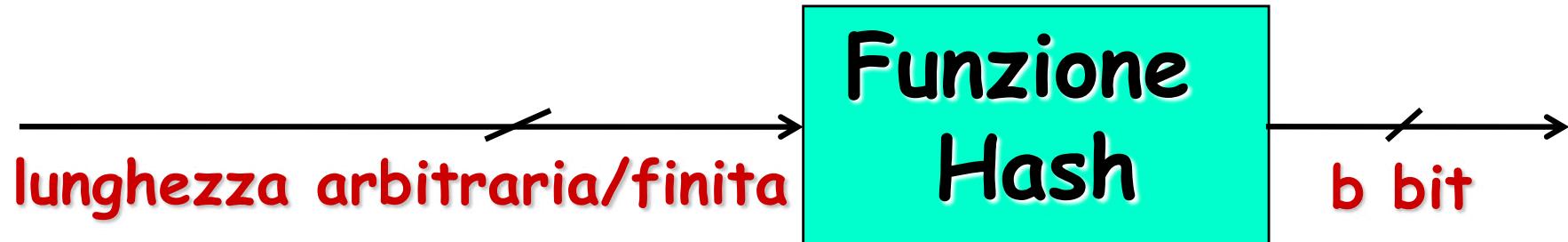
Idea alla base:

il valore hash $h(M)$ è una rappresentazione non ambigua e non falsificabile del messaggio M

Proprietà:

- facile da computare
- difficile trovare una collisione

Funzioni Hash



Le più comuni:

- MD5 (Message Digest Algorithm), valore di 128 bit
- SHA-0, SHA-1 con 160 bit,
- SHA-2, cioè SHA-224, SHA-256, SHA-384 e SHA-512, (Secure Hash Algorithm)

Esempi:

- SHA1("Cantami o diva del pelide Achille l'ira funesta") = 1f8a690b7366a2323e2d5b045120da7e93896f47
- SHA1("Contami o diva del pelide Achille l'ira funesta") = e5f08d98bf18385e2f26b904cad23c734d530ffb

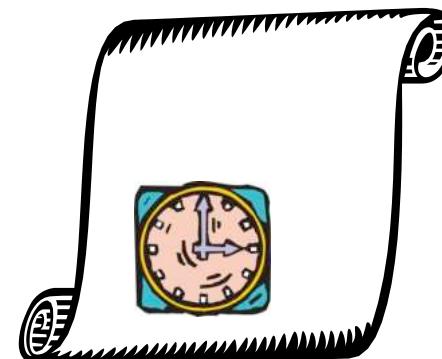
Uso delle funzioni hash

Firme digitali



Integrita' dei dati

Certificazione del tempo



Firme digitali e Funzioni hash

Problema: firma digitale di messaggi lunghi

Soluzione naïve: Divisione in blocchi e firma per ogni blocco
problema per la sicurezza: una permutazione/composizione
delle firme è una nuova firma

Soluzione di uso corrente:

firmare il valore hash del messaggio

$$[\text{firma di } M] = F_k(h(M))$$



Vantaggi: integrità dei dati ed efficienza degli algoritmi

Vedremo come implementare le funzioni hash mediante OpenSSL

Integrità dei dati e Funzioni hash

Tipico uso delle funzioni hash

Computo al tempo T il valore hash del file M

Conservo $H = h(M)$ in un luogo sicuro

Per controllare se il file è stato successivamente
modificato, calcolo $h(M')$ e verifico se $H = h(M')$

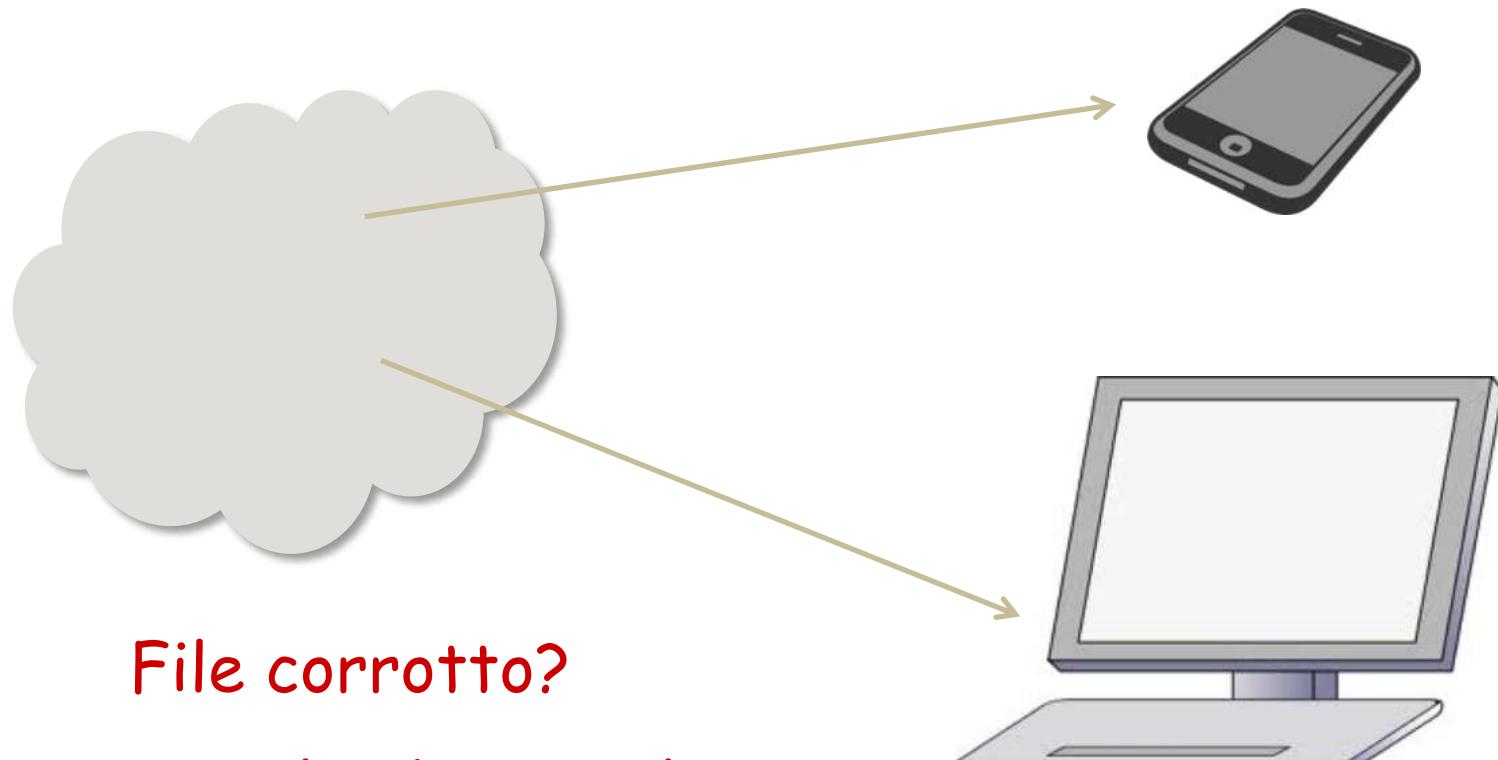
$h(M)$ è l'impronta digitale del file

Assicura se un file è stato modificato!



Integrità dei dati e Funzioni hash

Download file



Factory Images

[Full OTA Images](#)
[Driver Binaries](#)

"coral" for Pixel 4 XL

Version	Download	SHA-256 Checksum
10.0.0 (QD1A.190821.007, Oct 2019)	Link	e915f51a4af2ec6b1a802e105a9e3427613e813d208ae38878a3973f5d0e6b6
10.0.0 (QD1A.190821.011, Oct 2019)	Link	6dbd28f34a2db88e3c4c02104b7ed8ad1338cbe72585a5ac10d435a8a53a3e6c
10.0.0 (QD1A.190821.011.C4, Oct 2019)	Link	6a29be3b076158de063248b1995fc275474d38a1178d67bb34a99df5a592db64
10.0.0 (QD1A.190821.007.A3, Nov 2019)	Link	db77f854196b6a21d99e0cea6e4bee9e70a372423013226ecd7dbe64e1857110
10.0.0 (QD1A.190821.014, Nov 2019)	Link	4ea7d6457f8c9edd59081d6281691522afe61ff3be3dd8b4e9fab893c6c1b5f5
10.0.0 (QD1A.190821.014.C2, Nov 2019)	Link	839d41c9b1b733e9fec112915b376d7f2916a7f4a27625411d7dd0f518780ee7
10.0.0 (QQ1B.191205.011, Dec 2019, EMEA carriers, T-Mobile (US), Google Fi)	Link	0c24f5e0eade8f038dba4a7f6a086575589143f940d0a29dfe06b2af3c4c3cf1
10.0.0 (QQ1B.191205.012.A1, Dec 2019)	Link	a2b67bf7b2dbbb516fcac9f890041cf8aa362ee526eabdb783809635b82abbdb
10.0.0 (QQ1C.191205.016.A1, Dec 2019, Select JP & TW carriers)	Link	fb333d0f15ea6d088bdf2cd0e9d1371fc5bcfc7d97f9b6ef03868cec4b056f3
10.0.0 (QQ1B.200105.004, Jan 2020)	Link	143dfd87bda8e3064f041c1a97b3d4e3a34d0ac79977c79a7829c7df1532edaa
10.0.0 (QQ1C.200105.004, Jan 2020, Select JP & TW carriers)	Link	7dcbe7c415184078308b173a7d4e03f442a214625e62d2d18faa663dfd802348
10.0.0 (QQ1D.200105.002, Jan 2020, NTT DOCOMO)	Link	1e2dd846042f15acf0344b85405750bef08ff7d6d7fbef45e85400d7bb115c4
10.0.0 (QQ1B.200205.002, Feb 2020)	Link	89d8438423ef5398e19bca74e1cc1088900ae2476e208b3b4be2860f8631f732
10.0.0 (QQ1C.200205.002, Feb 2020, Select JP & TW carriers)	Link	2949c30167a4bbb8afe7f5cb291e1acc22211851b3b2ba5e69673044529e3449

maggio 2020

<https://developers.google.com/android/images>

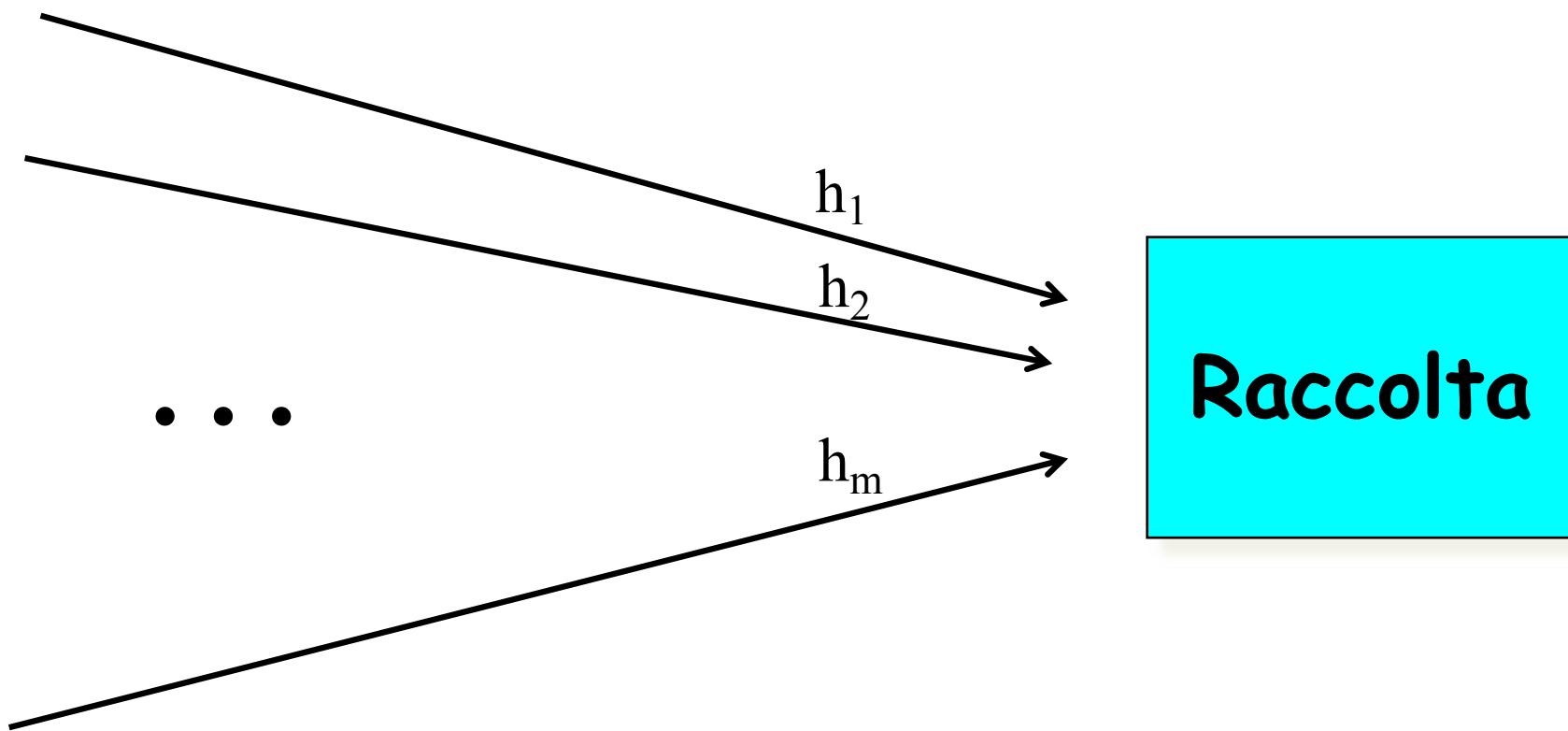
Integrità di più documenti

Utile per

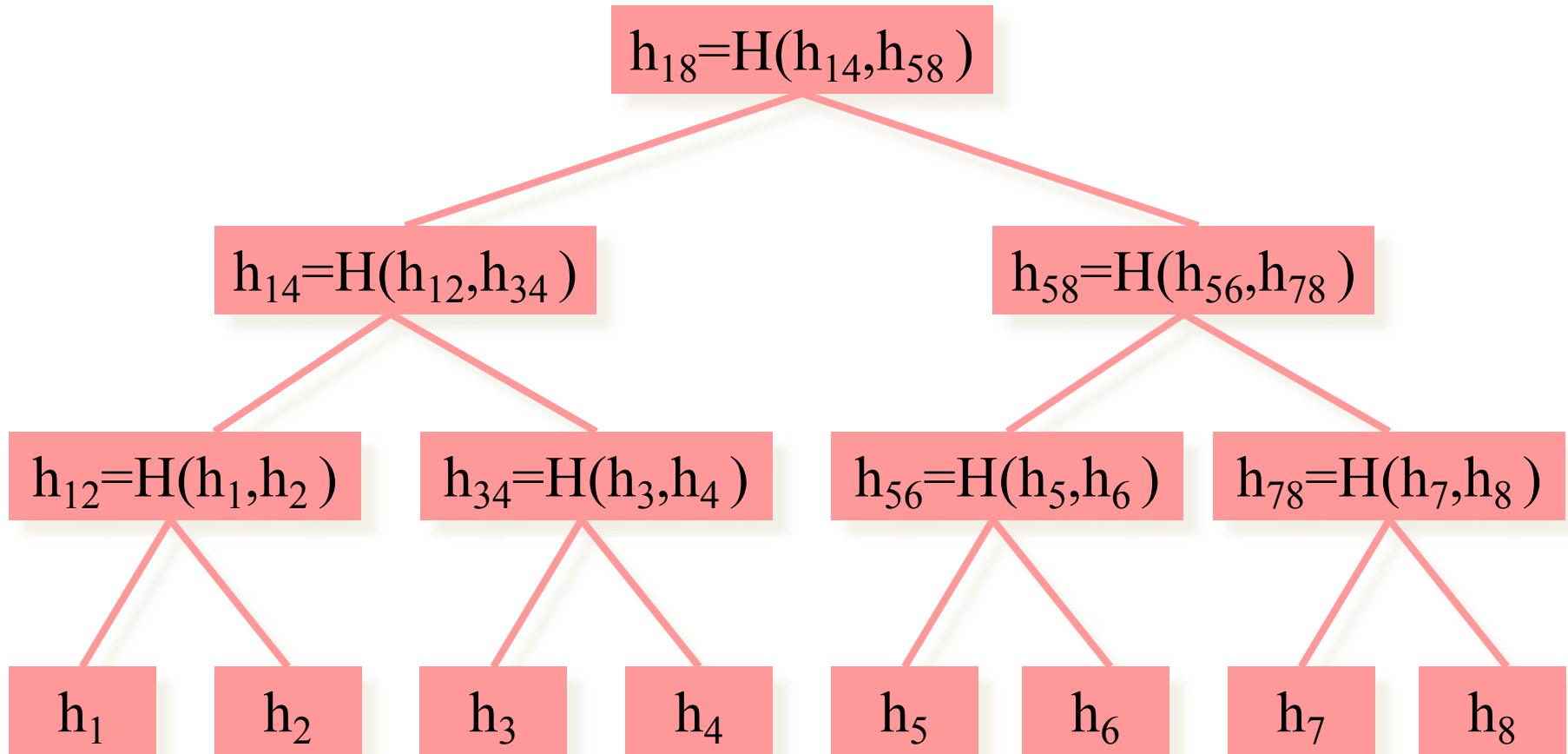
- Certificazione tempo
- Blockchain

Ricezione richieste

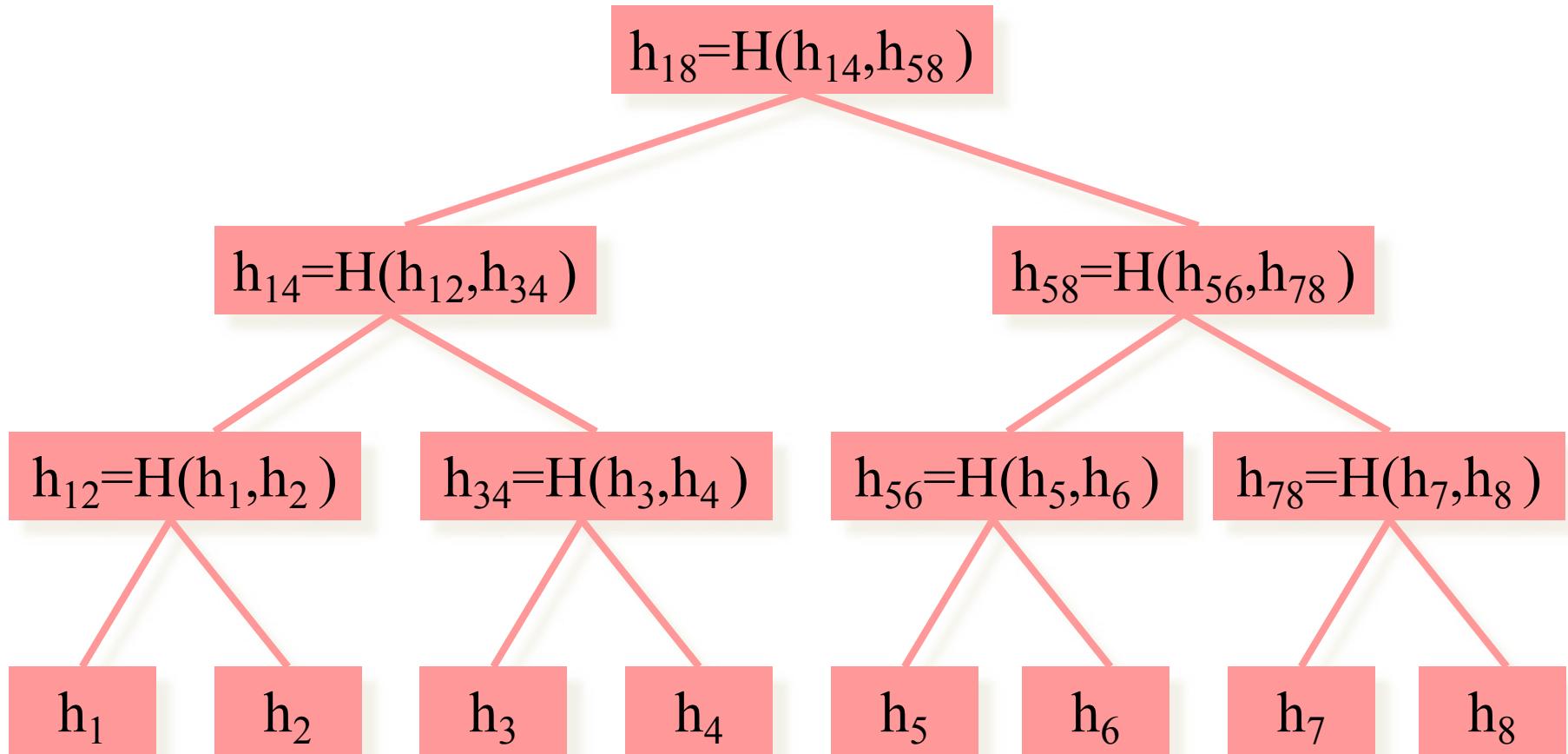
in un prefissato intervallo di tempo



Costruzione albero di hash

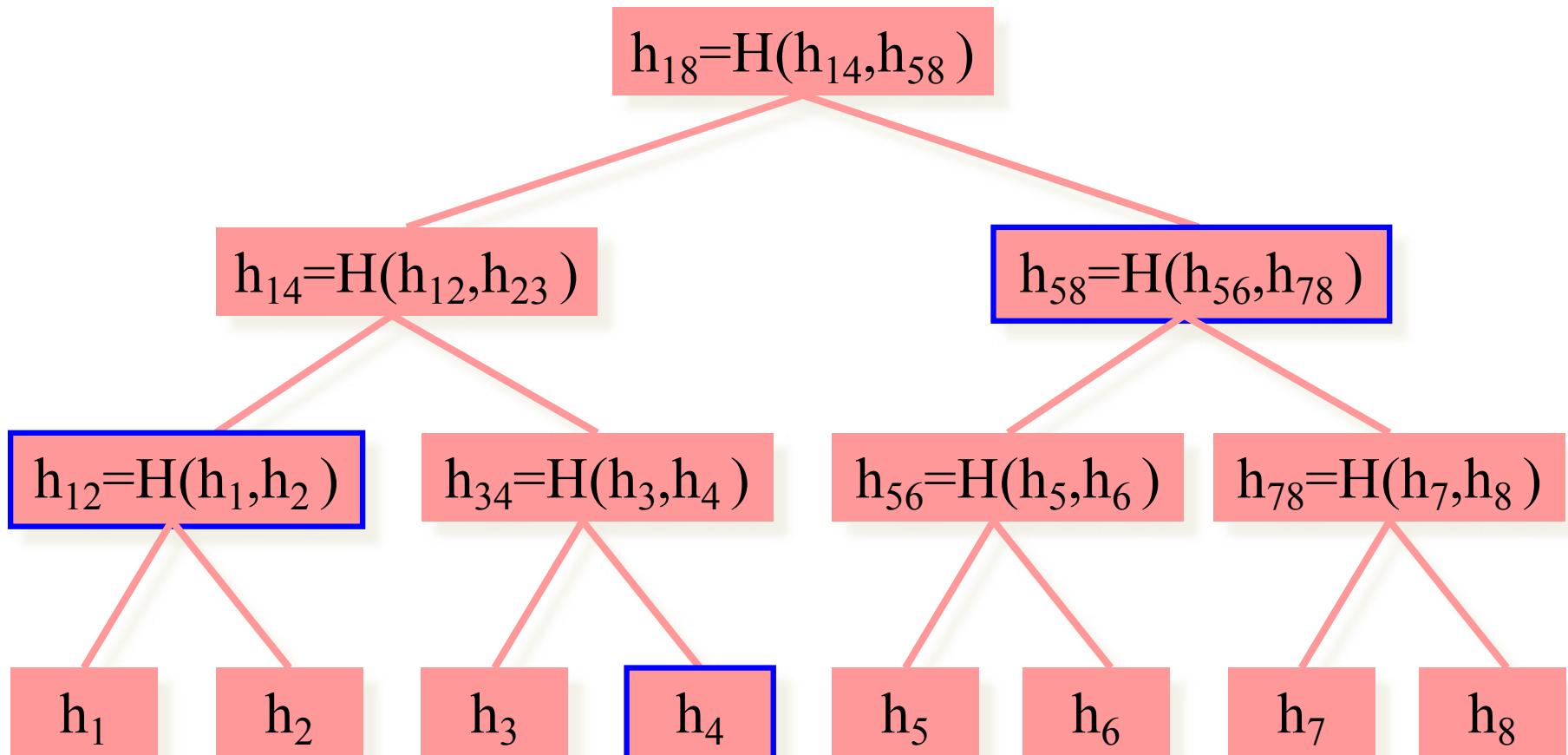


Costruzione albero di hash

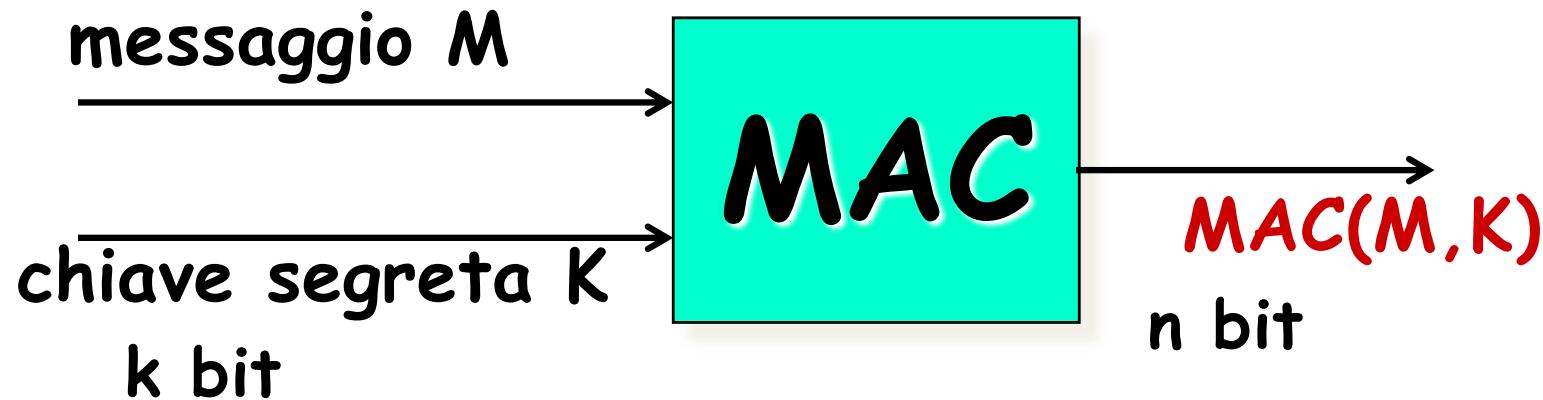


info necessarie per verificare che h_i è stato
utilizzato per costruire l'albero con radice h_{18}

Info per verifica di “ h_3 in albero con radice h_{18} ”



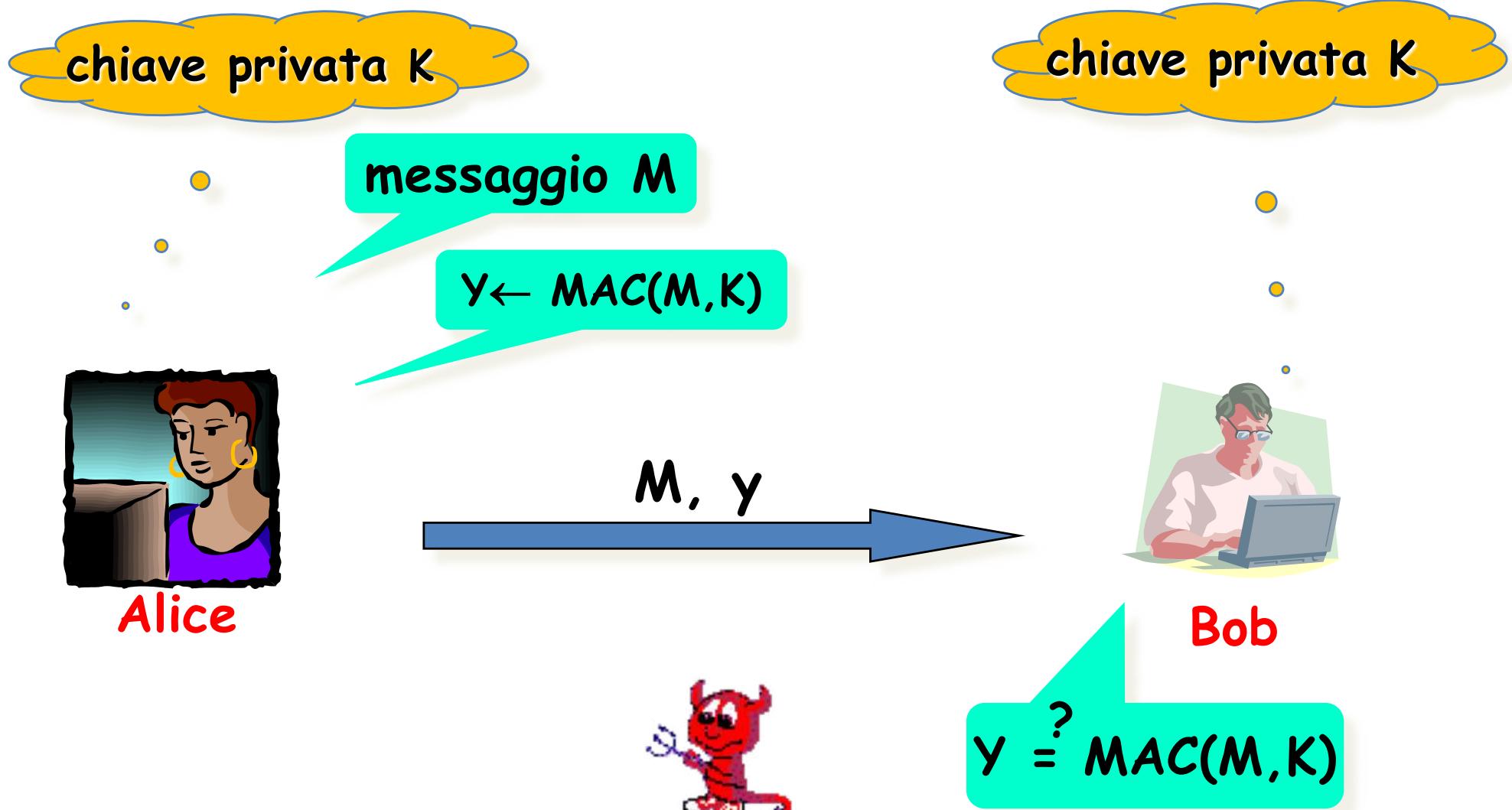
Message Authentication Code (MAC)



Applicazioni

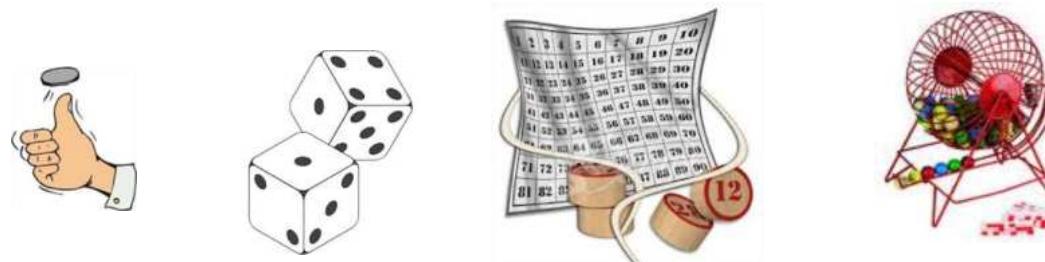
- Autenticità del messaggio M
- Integrità del messaggio M

Utilizzo MAC



Casualità e pseudocausalità

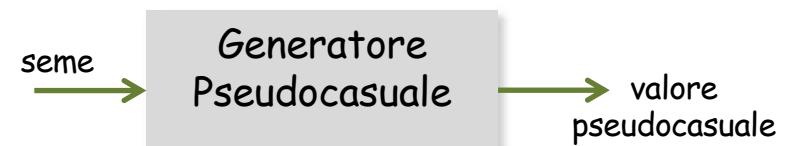
➤ Casuale



➤ Pseudocasuale

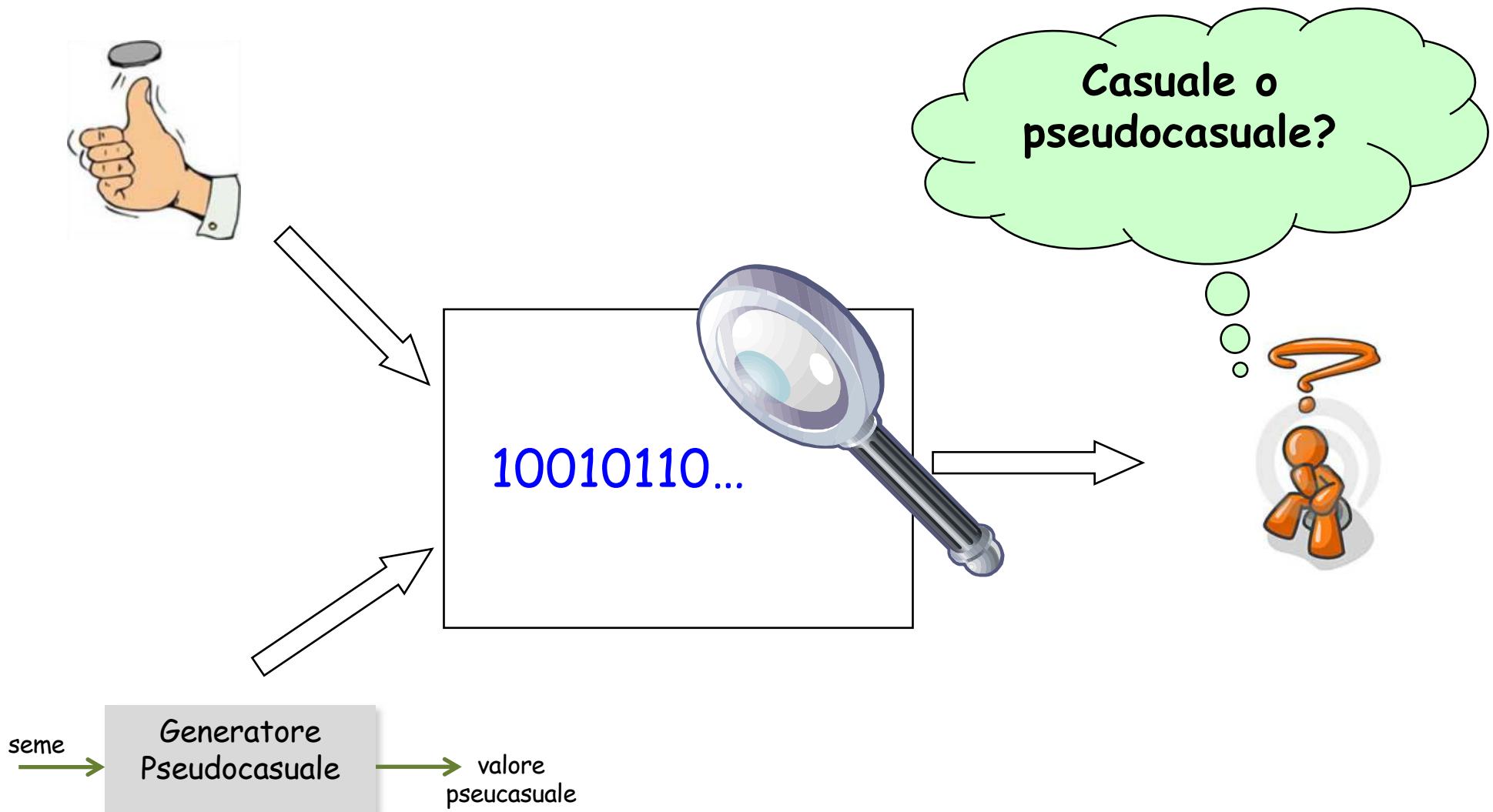
Generazione deterministica da un seme iniziale

Sembra casuale ma non lo è



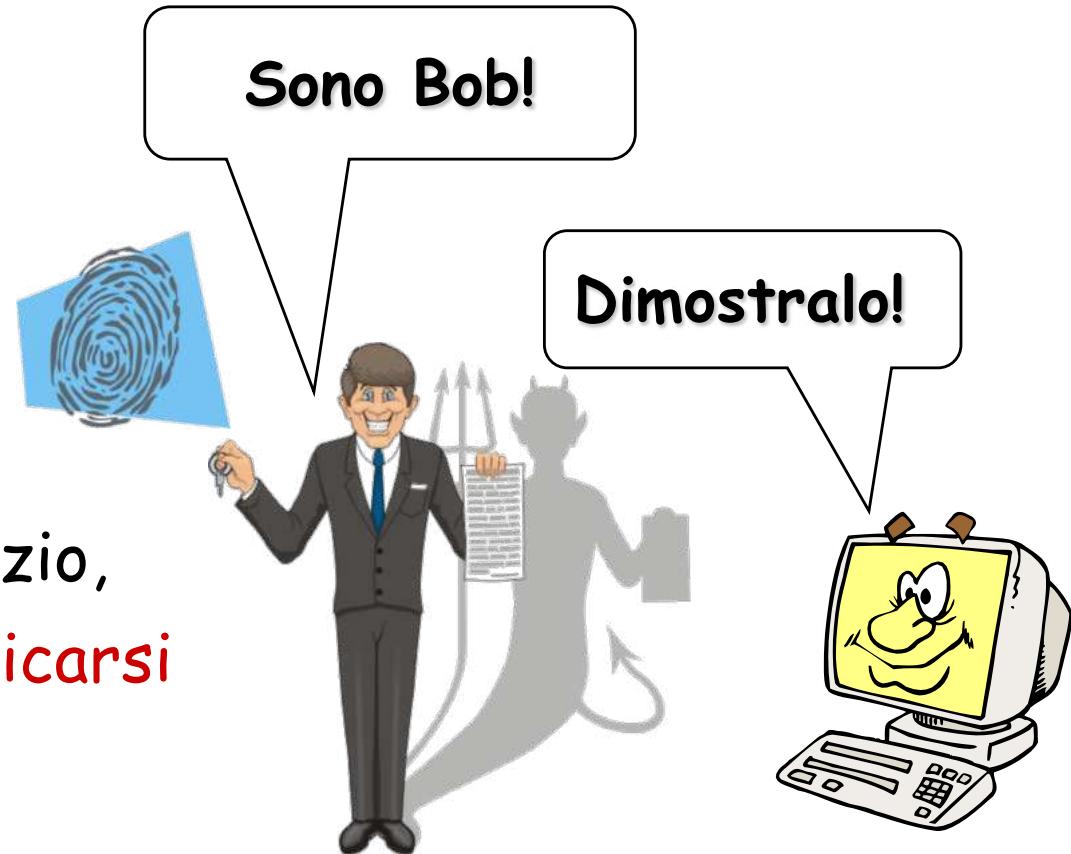
Sicurezza di un generatore pseudocasuale

Indistinguibilità



Autenticazione utente

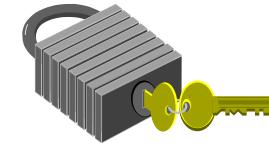
Per utilizzare un servizio,
un utente deve **autenticarsi**



Autenticazione utente: Principi

Qualcosa che l'utente **POSSIEDE**

- cose fisiche o elettroniche, ...



Qualcosa che l'utente **CONOSCE**

- password, PIN,...

.

Qualcosa che l'utente **E'** (o come si comporta)

- biometria, cioè misura di proprietà biologiche



Protocolli Crittografici

- Poker Mentale
- Condivisione di segreti
- Lancio di una moneta
- Blind Signature
- Moneta Elettronica
- Elezioni
- Certified email

Sicurezza IP e WWW

- La sicurezza sul Web ricopre un ruolo importantissimo
- Oggigiorno oltre il 50% del traffico Web è cifrato mediante il protocollo HTTPS
 - Come è emerso dall'analisi telemetrica dei due browser più diffusi
 - Google Chrome
 - Mozilla FireFox
- Questo risultato è stato ottenuto anche grazie alla scelta di utilizzare protocolli sicuri da parte dei principali social network e motori di ricerca



Sicurezza IP e WWW

- La sicurezza sul Web ricopre un ruolo importantissimo
- Oggigiorno oltre il 50% del traffico Web è cifrato mediante il protocollo HTTPS
 - Come è emerso dall'analisi tra i dati metrica dei due browser più diffusi
 - Google Chrome
 - Mozilla FireFox
 - Questo risultato è stato raggiunto dopo la scelta di utilizzare il protocollo HTTPS da parte dei principali social network.



`https://`

HTTPS è anche noto come
HTTP over TLS oppure
HTTP over SSL oppure
HTTP Secure



facebook

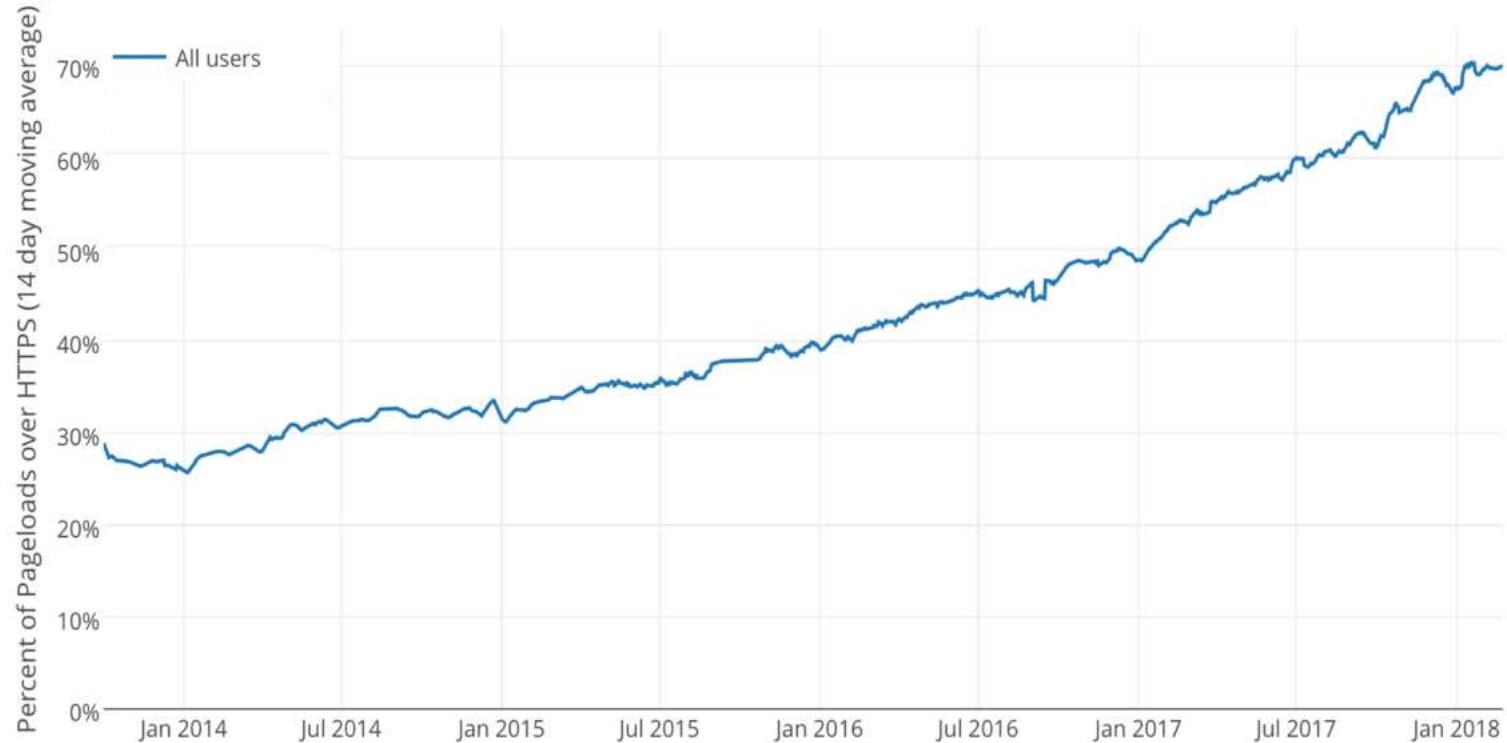


Sicurezza IP e WWW

(Telemetria Mozilla Firefox)



Percentuale di pagine caricate con HTTPS
Telemetria Mozilla Firefox (febbraio 2018)



Fonte: <https://letsencrypt.org/stats/>
<https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web>

Sicurezza IP e WWW

(Telemetria Mozilla Firefox)



Percentuale di pagine caricate con HTTPS
Telemetria Mozilla Firefox (febbraio 2018)



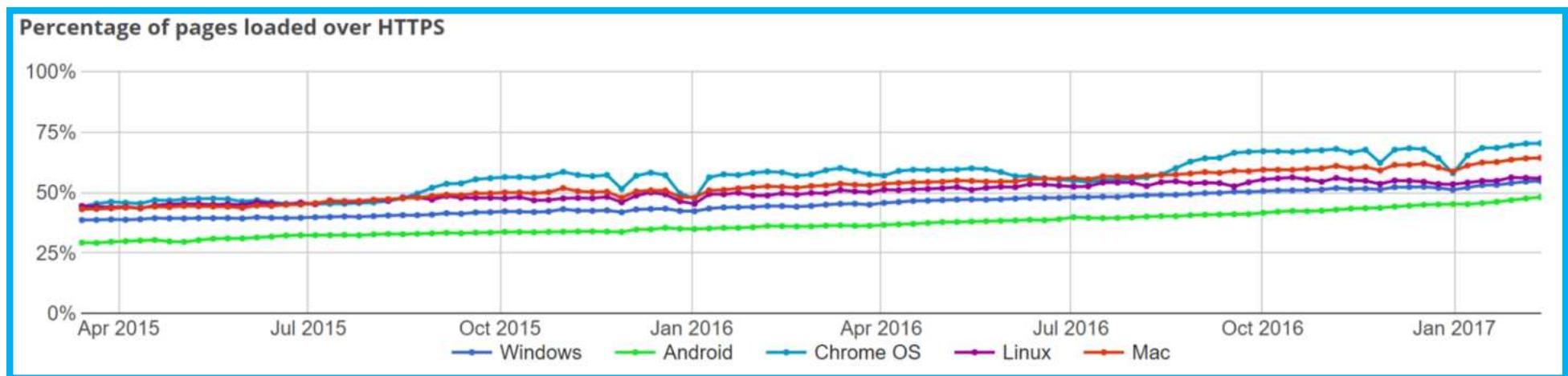
Fonte: <https://letsencrypt.org/stats/>
<https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web>

Sicurezza IP e WWW

(Telemetria Google Chrome)



Percentuale di pagine caricate con HTTPS (Febbraio 2017)
Telemetria Google Chrome su piattaforme



Fonte:

<https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web>

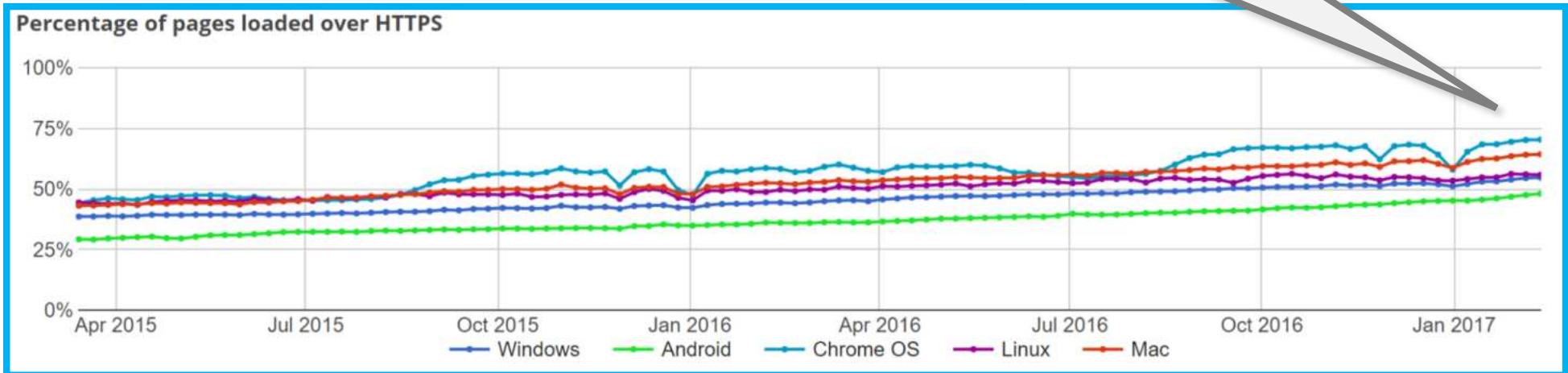
Sicurezza IP e WWW

(Telemetria Google Chrome)

Percentuale pagine caricate con HTTPS per piattaforma

- Windows → ~55% del traffico web
- Android → ~48% del traffico web
- Chrome OS → ~70% del traffico web
- Linux → ~56% del traffico web
- OS X → ~64% del traffico web

In media, circa il 59% del traffico web generato risulta essere cifrato



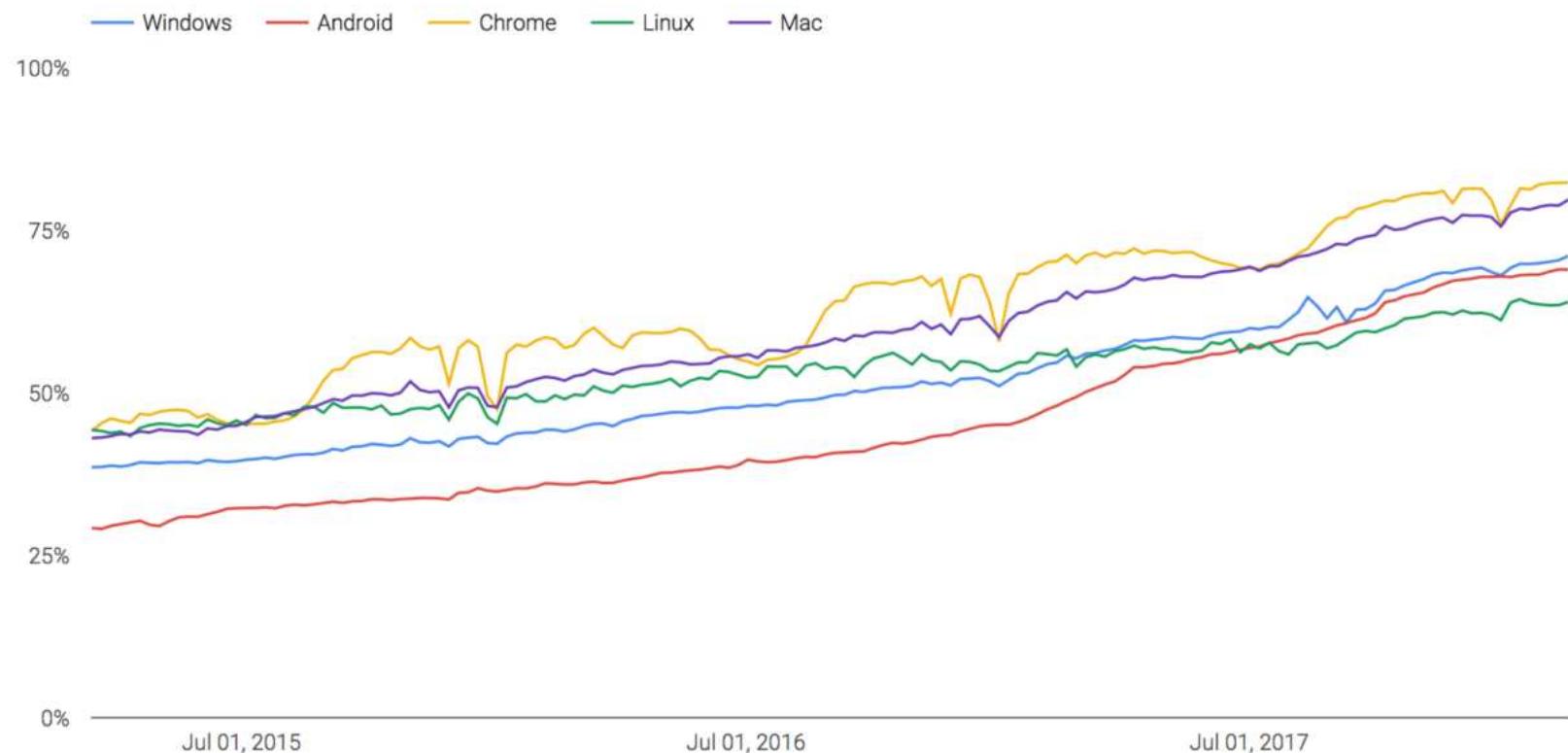
Fonte:

<https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web>

Sicurezza IP e WWW

(Telemetria Google Chrome)

Percentage of pages loaded over HTTPS in Chrome by platform



<https://transparencyreport.google.com/https/overview?hl=en>

Come si ottengono i dati?



Come si ottengono i dati?



I dati sono forniti dagli utenti che scelgono di condividere le statistiche sull'utilizzo

Abilitare Telemetria su Mozilla Firefox

The screenshot shows the Mozilla Firefox preferences window with the sidebar on the left containing icons for Generale, Ricerca, Contenuti, Applicazioni, Privacy, Sicurezza, Sync, and Avanzate. The Avanzate icon is highlighted with an orange border. The main content area has a title "Avanzate" and a subtitle "Condivisione dati". Below this, there are three checkboxes:

- Attiva analisi integrità di Firefox**: Describes how Firefox analyzes its performance and shares information with Mozilla about software integrity. It includes a link to "Ulteriori informazioni".
- Condividi ulteriori dati (telemetria)**: Describes sharing performance, usage, hardware, and customization data with Mozilla to improve Firefox. This option is highlighted with a blue border. It includes a link to "Ulteriori informazioni".
- Consenti a Firefox di inviare automaticamente le segnalazioni di arresto anomalo in sospeso**: Describes sending crash reports to Mozilla to help fix browser issues. It includes a link to "Ulteriori informazioni".

Abilitare Telemetria su Google Chrome

Privacy

[Impostazioni contenuti...](#)

[Cancella dati di navigazione...](#)

Google Chrome potrebbe utilizzare servizi web per migliorare la navigazione. Puoi scegliere di disattivare questi servizi. [Ulteriori informazioni](#)

- Utilizza un servizio web per risolvere gli errori di navigazione
- Utilizza le previsioni per completare i termini di ricerca e gli URL digitati nella barra degli indirizzi
- Utilizza un servizio di previsione per velocizzare il caricamento delle pagine
- Segnala automaticamente a Google i dettagli dei possibili problemi di sicurezza
- Proteggi te stesso e il tuo dispositivo da siti pericolosi
- Utilizza un servizio web per correggere gli errori ortografici
- Invia automaticamente a Google statistiche sull'utilizzo e rapporti sugli arresti anomali
- Invia una richiesta "Non tenere traccia" con il tuo traffico di navigazione

Sicurezza sul WEB

Protocollo **SSL**

- ✓ Consente alle applicazioni client/server di comunicare in modo sicuro
- ✓ Utilizzato per il commercio elettronico e l'accesso riservato ai dati



Votazioni elettroniche

- Cineca u-Vote
- Stati Uniti
- Estonia



Protezione del software dalla copia

- Trovare un metodo contro la pirateria
 - efficiente
 - economico
 - resistente contro i pirati esperti
 - non invasivo
- Compito impossibile!
- Però si può rendere la copia difficile per il pirata esperto ed impossibile per il pirata occasionale



SOCIAL ENGINEERING

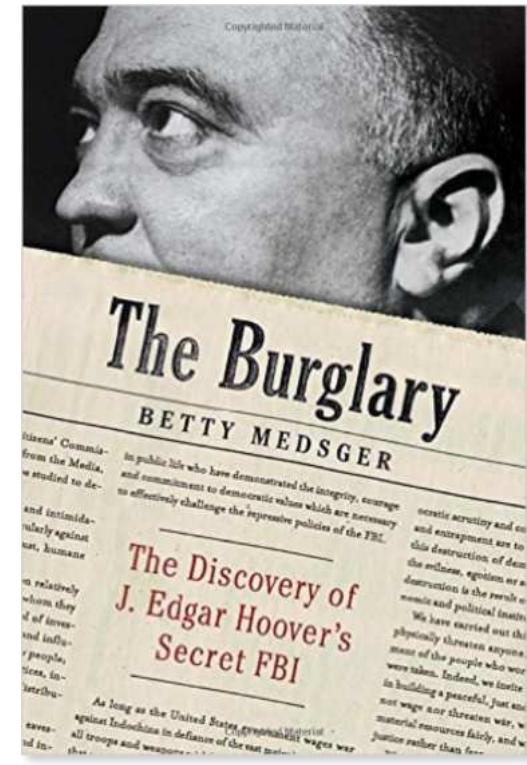
The clever manipulation
of the natural human
tendency to trust.

Attacco social engineering, 1971

- Furto in un ufficio dell'FBI in Media, Pennsylvania, marzo 1971
- Rubati documenti segreti FBI
- Gruppo di attivisti, 8 uomini ed 8 donne
- Scritto nel 2014 da Betty Medsger, giornalista *The Washington Post*, la prima che ebbe i documenti

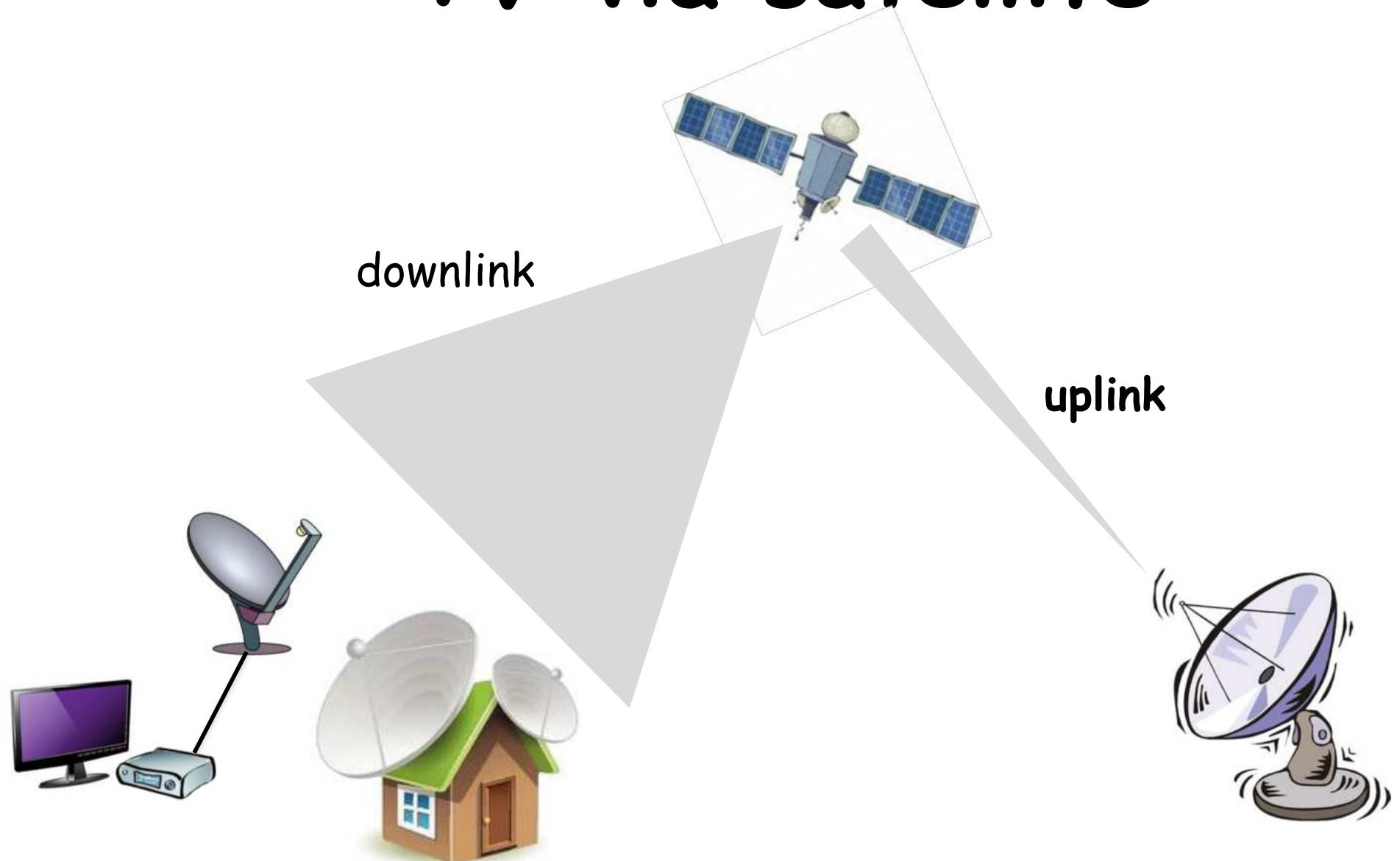
Attacco social engineering, 1971

As burglars, they used some unusual techniques, ones Davidon enjoyed recalling years later, such as what some of them did in 1970 at a draft board office in Delaware. During their casing, they had noticed that the interior door that opened to the draft board office was always locked. There was no padlock to replace, as they had done at a draft board raid in Philadelphia a few months earlier, and no one in the group was able to pick the lock. The break-in technique they settled on at that office must be unique in the annals of burglary. Several hours before the burglary was to take place, one of them wrote a note and tacked it to the door they wanted to enter: "Please don't lock this door tonight." Sure enough, when the burglars arrived that night, someone had obediently left the door unlocked. The burglars entered the office with ease, stole the Selective Service records, and left. They were so pleased with themselves that one of them proposed leaving a thank-you note on the door. More cautious minds prevailed. Miss Manners be damned, they did not leave a note.



The Burglary: The Discovery
of J. Edgar Hoover's Secret
FBI
Gennaio 2014
pag 22

TV via satellite



TV via satellite

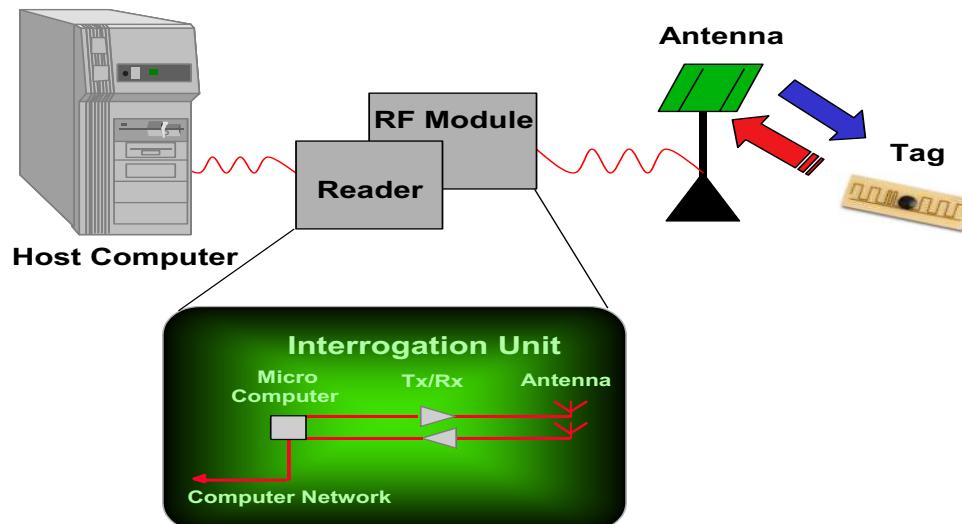


TV via satellite



RFId

- Acronimo di Radio Frequency IDentification
- E' una tecnologia per la identificazione automatica di oggetti, animali o persone
- Il sistema si basa sul leggere a distanza informazioni contenute in un tag RFID usando dei lettori RFID



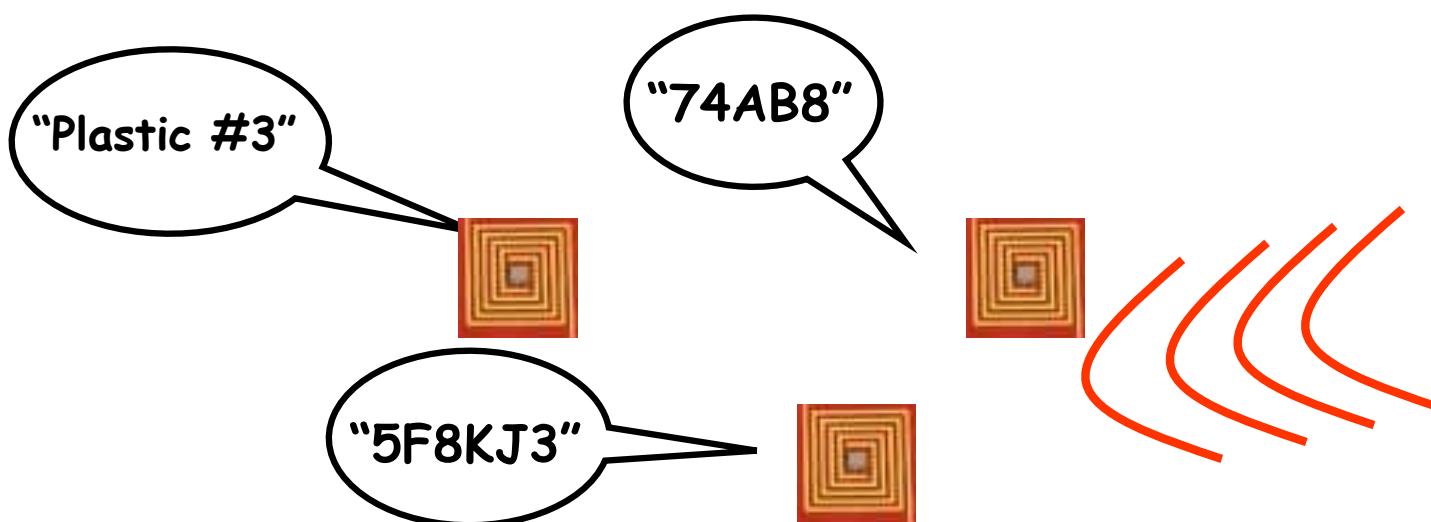
Componenti:

- RFId tag
- Reader o transceiver
- Sistema di elaborazione dati (PC) middleware server

Il tag

Caratteristiche dei tag più semplici:

- Dispositivo passivo
riceve energia dal lettore
- Ha un range di diversi metri
- È un "etichetta intelligente" che grida il suo nome e/o dato



Codici a barre

RFId può sostituire il codice a barra



Problemi di privacy

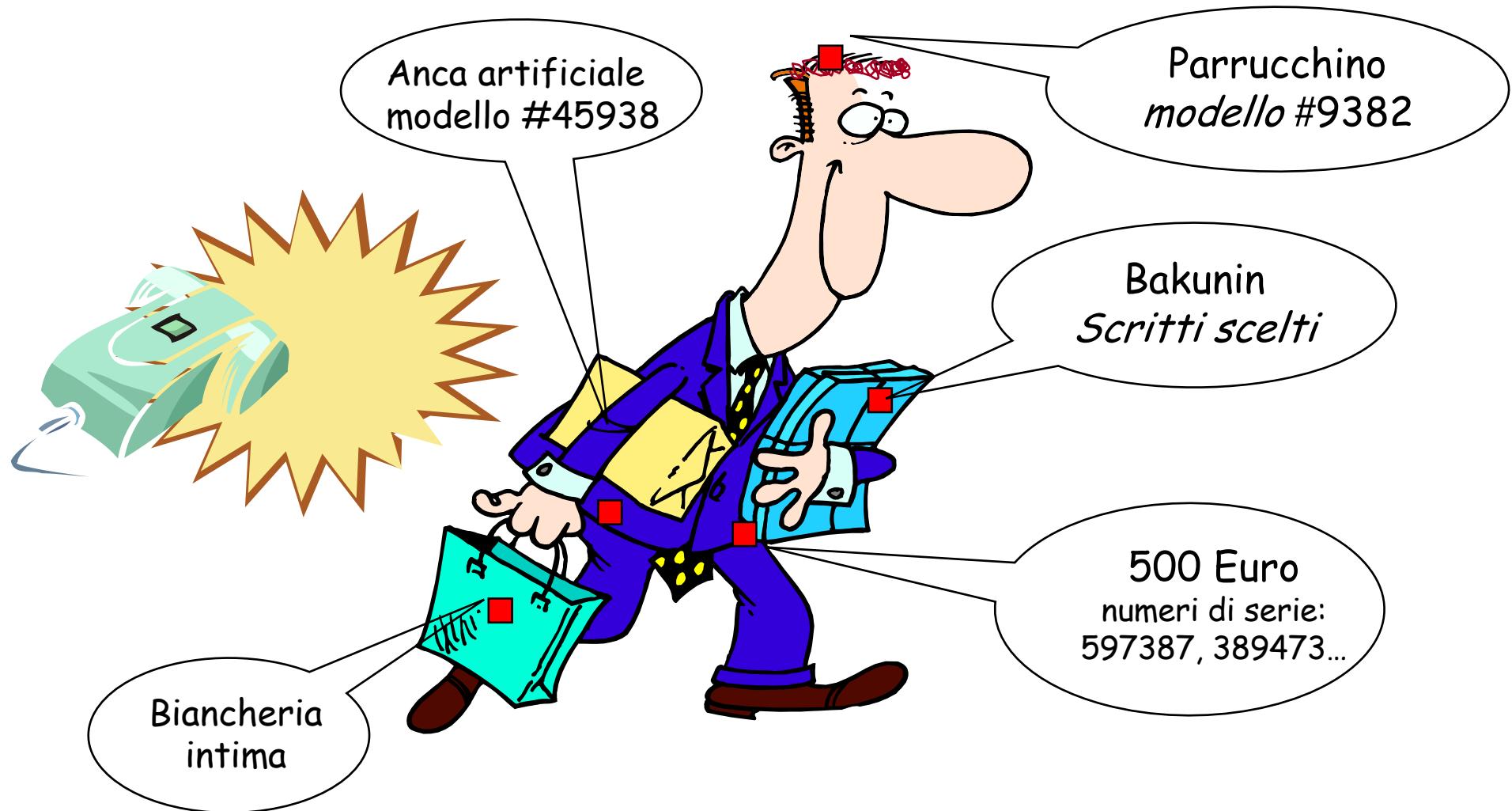
Furto di dati personali



Tracciamento



Problemi di privacy



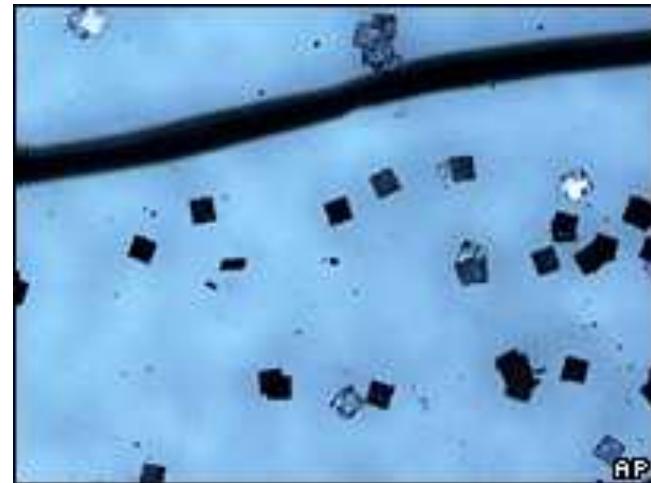
Due esigenze contrastanti

Tutelare la *privacy*

Identificare i beni non acquistati



Tag piccolissimi

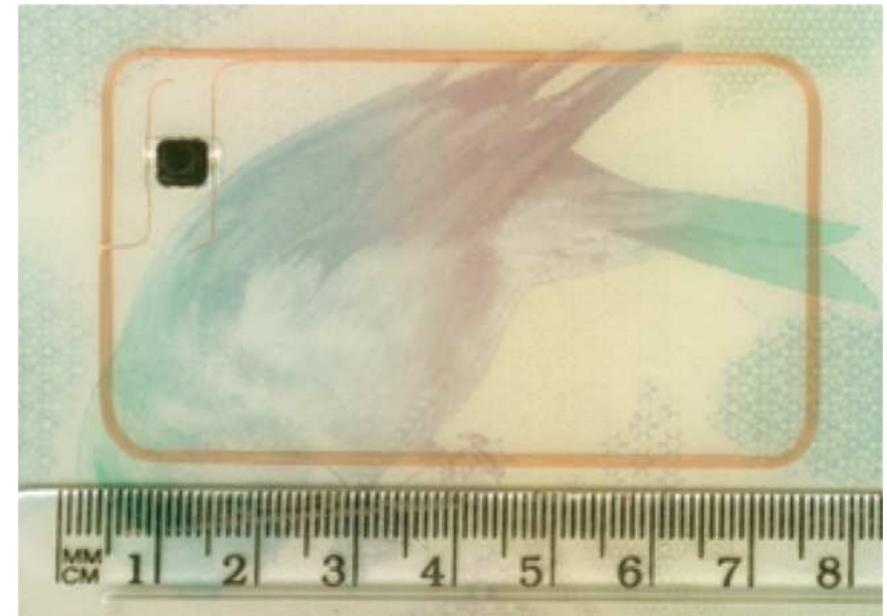


- Hitachi, 2007
- Grandezza: 0,05 mm × 0,05 mm
- Unico problema ... attualmente l'antenna è 80 volte più grande!

Passaporti con RFId

Tag RFID utilizzati nei passaporti

- 2005 Norvegia
- 2006 Giappone, Spagna, Italia, UK, USA
- 2007 Australia
- ...



Tag RFID inserito in un passaporto

Passaporti con RFId

la Repubblica.it | **Tecnologia&Scienze**

[Web](#) | [Immagini](#) | [Video](#) | [News](#) | [Annunci](#) | [Shopping](#) | [Repubblica.it](#)

[Home](#) [Repubblica TV](#) [Politica](#) [Cronaca](#) [Roma](#) [Milano](#) [News](#) [Control](#) [Economia&Finanza](#) [Esteri](#) [Ambiente](#) [Ora per Ora](#) [Foto Multimedia](#) [Annu](#)

[Sport](#) [Motori](#) [Persone](#) [Moda](#) [Star Control](#) [Lavoro](#) [Scuola&Giovani](#) [Spettacoli&Cultura](#) [Tecno&Scienze](#) [Giocchi](#) [Viaggi](#) [Arte](#) [Week-in](#) [Metoo](#)

Tecnologie&Scienze

[Prodotti](#)
[Sicurezza Web](#)
[VideoGiochi](#)
[Mondo Mac](#)
[Software](#)
[Come fare](#)
[Gallerie](#)

SCIENZA & TECNOLOGIA

Lo sostiene un'inchiesta della Bbc che ha effettuato un test.
In cinque minuti è possibile replicare il documento digitale

Passaporto elettronico a rischio clonazione I dati scaricabili dal microchip

Il lettore che cattura le informazioni si acquista su eBay a 200 euro



IL PASSAPORTO elettronico è ad alto rischio clonazione. La denuncia viene dalla Bbc che, attraverso un test, è riuscita a catturare con una certa facilità le informazioni contenute nel microchip del documento di identificazione personale introdotto in Europa dopo l'11 settembre.

Il passaporto testato dal network televisivo è quello britannico, ma la Bbc allarga i rischi anche ai documenti di identificazione degli altri paesi Ue citando la denuncia di un gruppo di ricercatori che ha già sottoposto il problema alle istituzioni di Bruxelles.

Per clonare il passaporto Bbc ha impiegato cinque minuti. Come, è presto detto. Il chip contenuto nel documento digitale è una sorta di codice a barra che può essere letto attraverso frequenze radio a breve distanza. Una caratteristica che ha dei vantaggi, ma anche dei difetti. Gravi, per la Bbc.

In particolare perché il codice permette di scaricare i dati personali contenuti nel passaporto, grazie a un lettore che si acquista su eBay a 200 euro. Una volta trasferiti i dati su un chip vergine è facile avere a disposizione un passaporto digitale clonato.

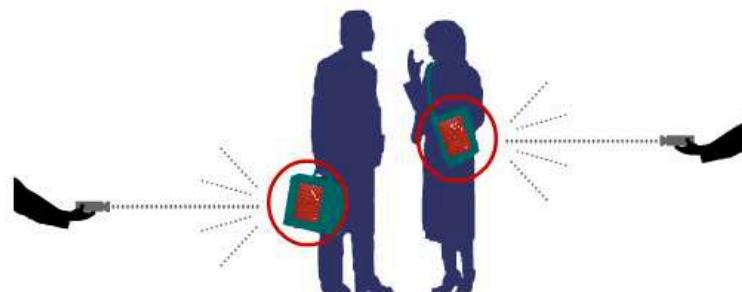
Nonostante il ministero dell'Interno, interpellato dalla Bbc, neghi che clonare un passaporto digitale sia così semplice e alla portata di tutti (in quanto il microchip contiene solo una parte delle informazioni che rendono unico il singolo documento), la rete tv insiste nella sua denuncia. Spiegando che sono molti gli esperti che hanno sollevato il problema della sicurezza dei dati sostenendo che non è troppo tardi per correggere il difetto.

(17 dicembre 2006)

- Potevano essere letti da 10m
- In seguito, i passaporti contengono anche una sottile membrana metallica al fine di rendere difficile le letture non autorizzate (skimming) quando il passaporto è chiuso

Rappresentazione della protezione dalla lettura non autorizzata dei dati

Ritorno alla pagina «[Misure di sicurezza e di protezione dei dati](#)»



Se il passaporto elettronico è chiuso i dati registrati **non** possono essere letti.

Passaporti con RFId

- In Italia dal 2010
- impronte vengono memorizzate solo nel chip del passaporto
- non esiste in Italia una banca dati delle impronte digitali (AFIS, Automated fingerprints identification system) civile
- non per i minori di anni 12



Steganografia

Nasconde l'esistenza di un messaggio

Esempio: immagini Bitmap

Red

Green

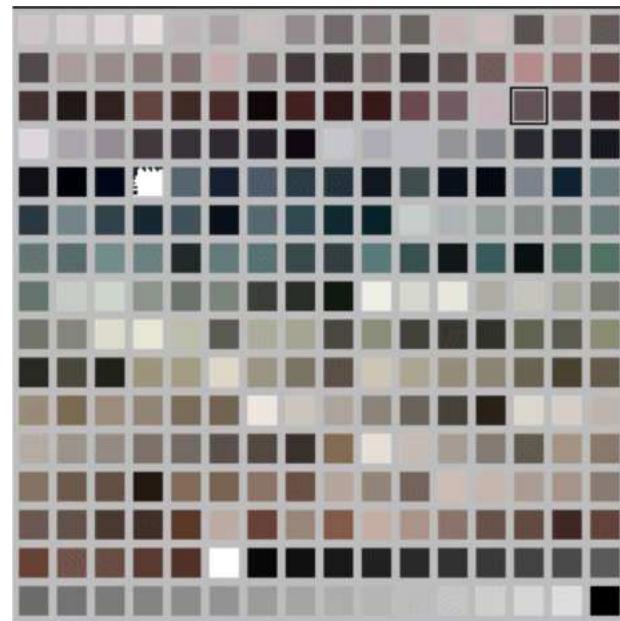
Blue

(11100001, 00000100, 00010111)

- Livello colore primario: 0, ..., 255
- Uso dei bit meno significativi

Steganografia

immagini GIF



palette

Watermark

- Letteralmente "filigrana"
- Assicura autenticità ed integrità ai documenti in cui è immerso
- È una sequenza di bit inseriti all'interno del documento da proteggere con le caratteristiche:
 - **Impercettibile** - Il documento marcato e quello originale devono apparire identici.
 - **Legata al documento** - La marca deve essere funzione del documento e parte integrante di esso.
 - **Robusta** - La marca deve essere in grado di resistere a tutte le più comuni trasformazioni operabili sul documento.

Curve Ellittiche

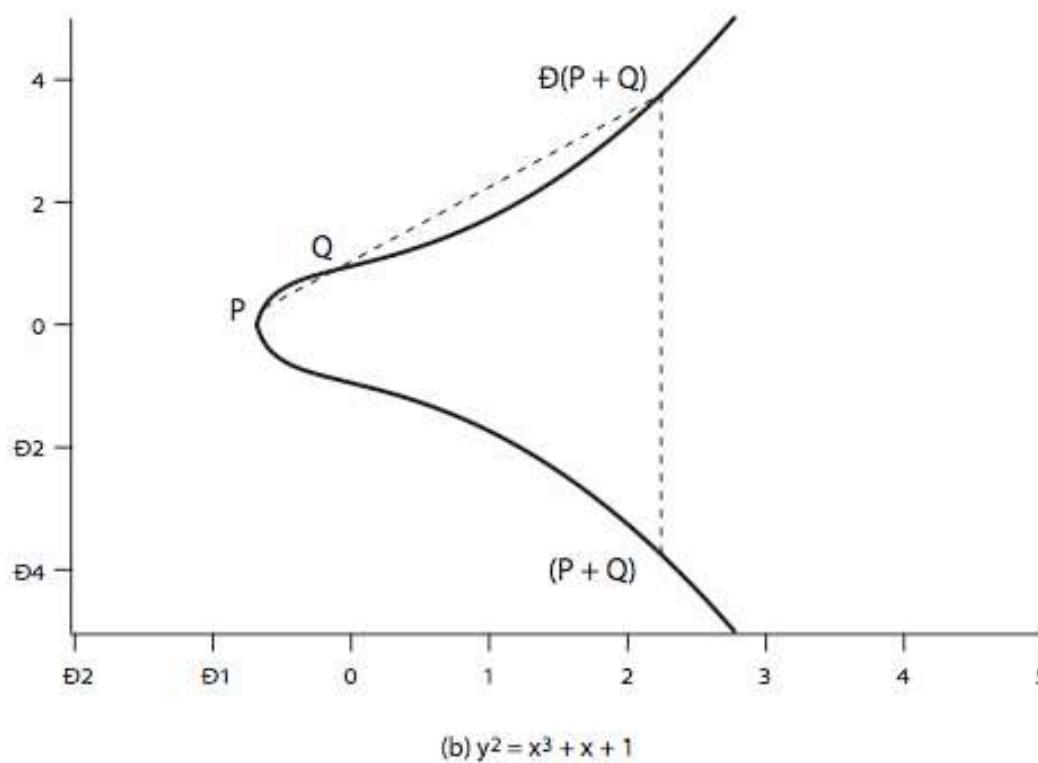
- La maggioranza della crittografia a chiave pubblica (RSA, DH) usa aritmetica sugli interi oppure sui polinomi con numeri/polinomi molto grandi
- “grandi” richieste per memorizzazione e processamento di chiavi e messaggi
- Alternative: usare curve ellittiche
- Offre lo stesso grado di sicurezza con minori lunghezze
- Sistemi più recenti, ma non analizzati come i precedenti

Curve Ellittiche Reali

- Una curva ellittica è definita da una equazione in 2 variabili
- Curva ellittica cubica della forma
 - $y^2 = x^3 + ax + b$
 - dove x, y, a, b sono numeri reali
 - Definisci anche il punto zero O
- Operazione di addizione
 - Somma geometrica dei punti $Q+R$ è il punto riflesso dell'intersezione della curva con la retta QR

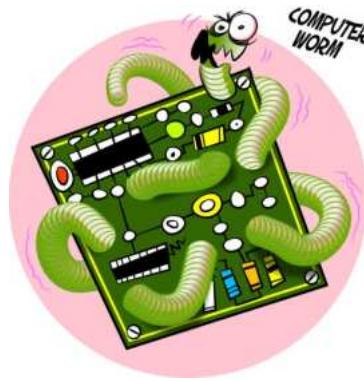
Esempio di una Curva Ellittica

Interpretazione geometrica di una addizione



Comparable Key Sizes for Equivalent Security

Cifrario simmetrico (grandezza chiave in bit)	Schema basato su ECC (grandezza di n in bit)	RSA/DSA (grandezza modulo in bit)
56	112	512
80	160	1.024
112	224	2.048
128	256	3.072
192	384	7.680
256	512	15.360



I Malware

- Un malware (**malicious software**) è una sequenza di codice/programma nocivo
 - Progettato per intenzionalmente causare danni o alterare il normale comportamento di un sistema informatico e i dati in esso contenuti
- Un malware agisce spesso in modo «**subdolo**»
 - Viene eseguito all'insaputa dell'utente

Analisi dei Malware

Analizzare un malware significa cercare di comprenderne il comportamento, al fine di

- Identificare il malware
- Difendersi dal malware
- Eliminare il malware
- Sviluppare adeguate contromisure



BlackEnergy



Identikit

Nome

➤ BlackEnergy

Anno Nascita

➤ 2007

SO Attaccati

➤ Microsoft Windows®

Segni Particolari

➤ Usato per un attacco al settore energetico ucraino (2015)



Sicurezza

Si chiama BlackEnergy il malware che ha spento tre centrali ucraine

Nella notte tra il 23 e il 24 dicembre una minaccia informatica ha lasciato senza elettricità centinaia di migliaia di persone. Ecco in che modo



5 gennaio 2016

BlackEnergy

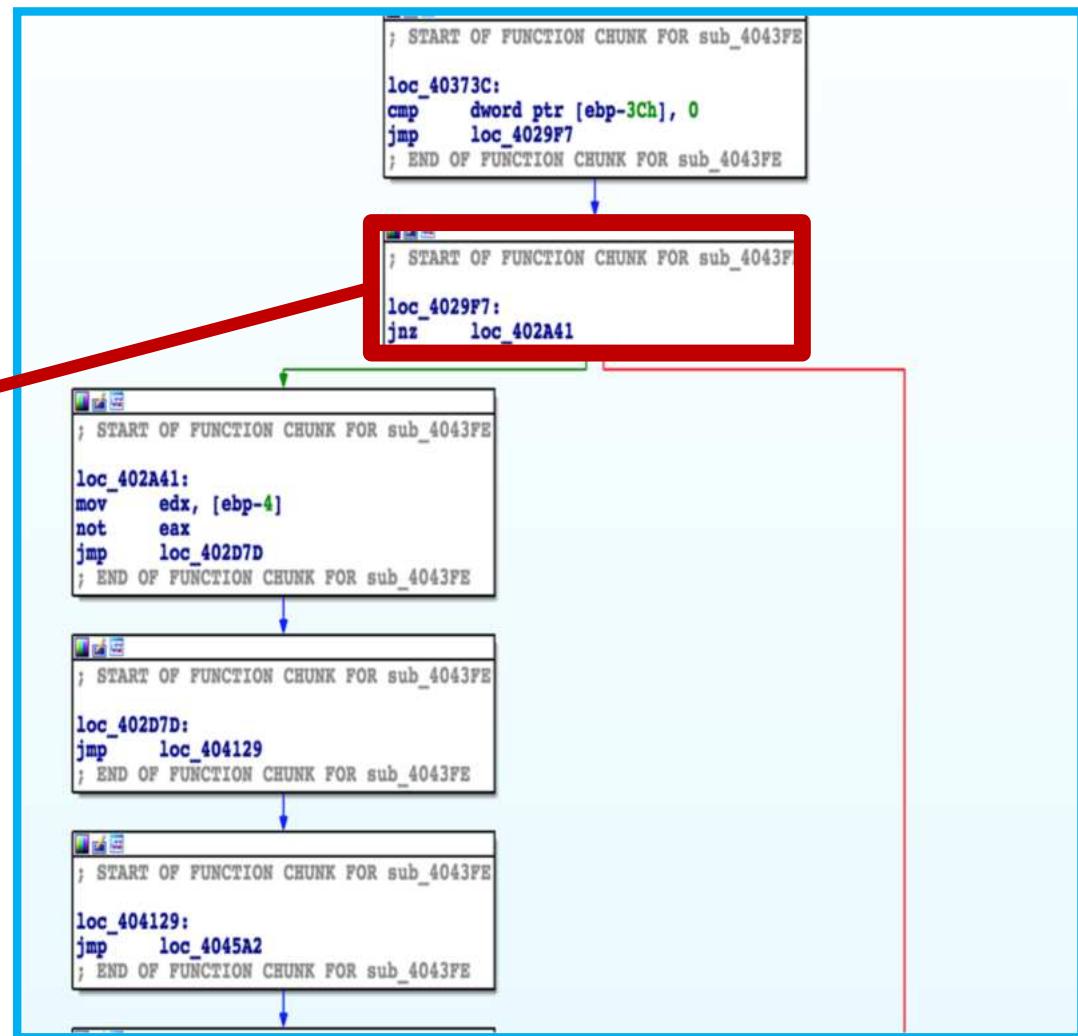
- I danni di BlackEnergy
- Regione Ivano-Frankivsk, Ucraina, Dicembre 2015
 - Assenza di fornitura elettrica per 6 ore
 - La causa è un cyber-attacco
 - Dai rapporti successivi, viene individuata la causa: un malware
 - Il malware definito BlackEnergy sembra aver infettato i sistemi della centrale
 - Grazie alla riuscita di un attacco di phishing

Ci soffermeremo sull'Analisi del Malware BlackEnergy



```
; START OF FUNCTION CHUNK FOR sub_4043FE

loc_4029F7:
jnz    loc_402A41
```

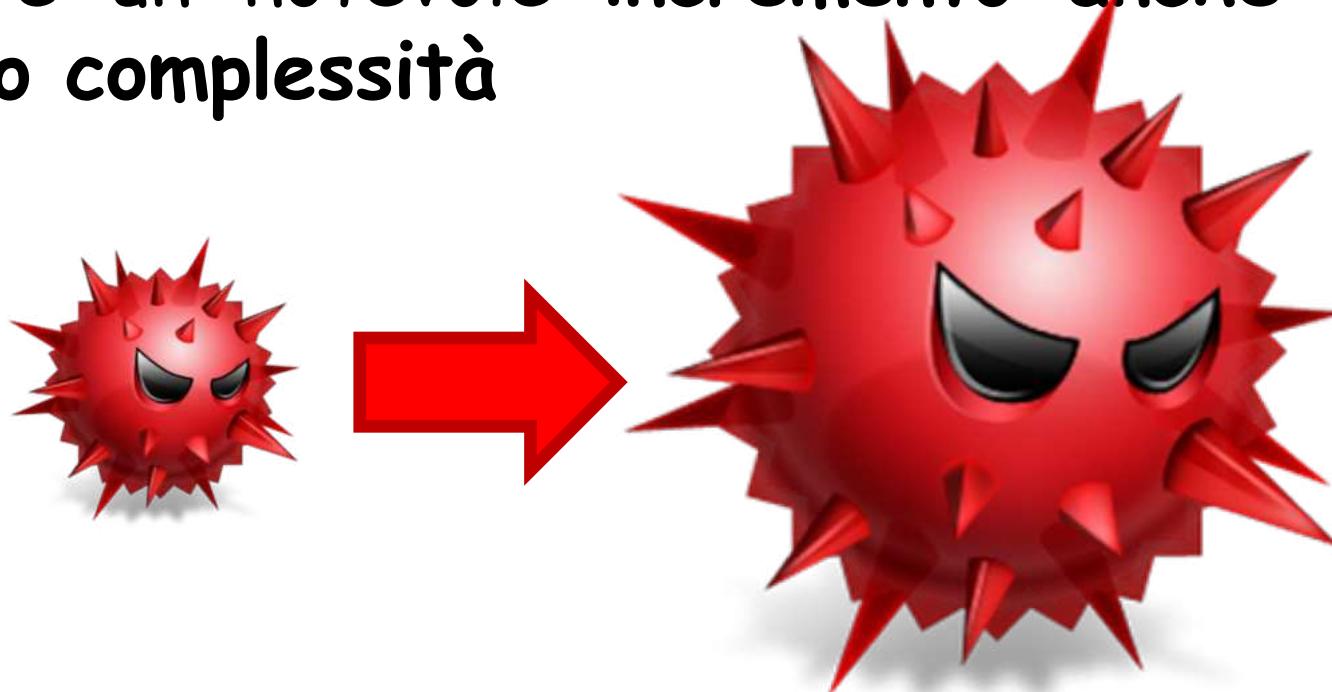


Malware, Dispositivi Mobile e Analisi

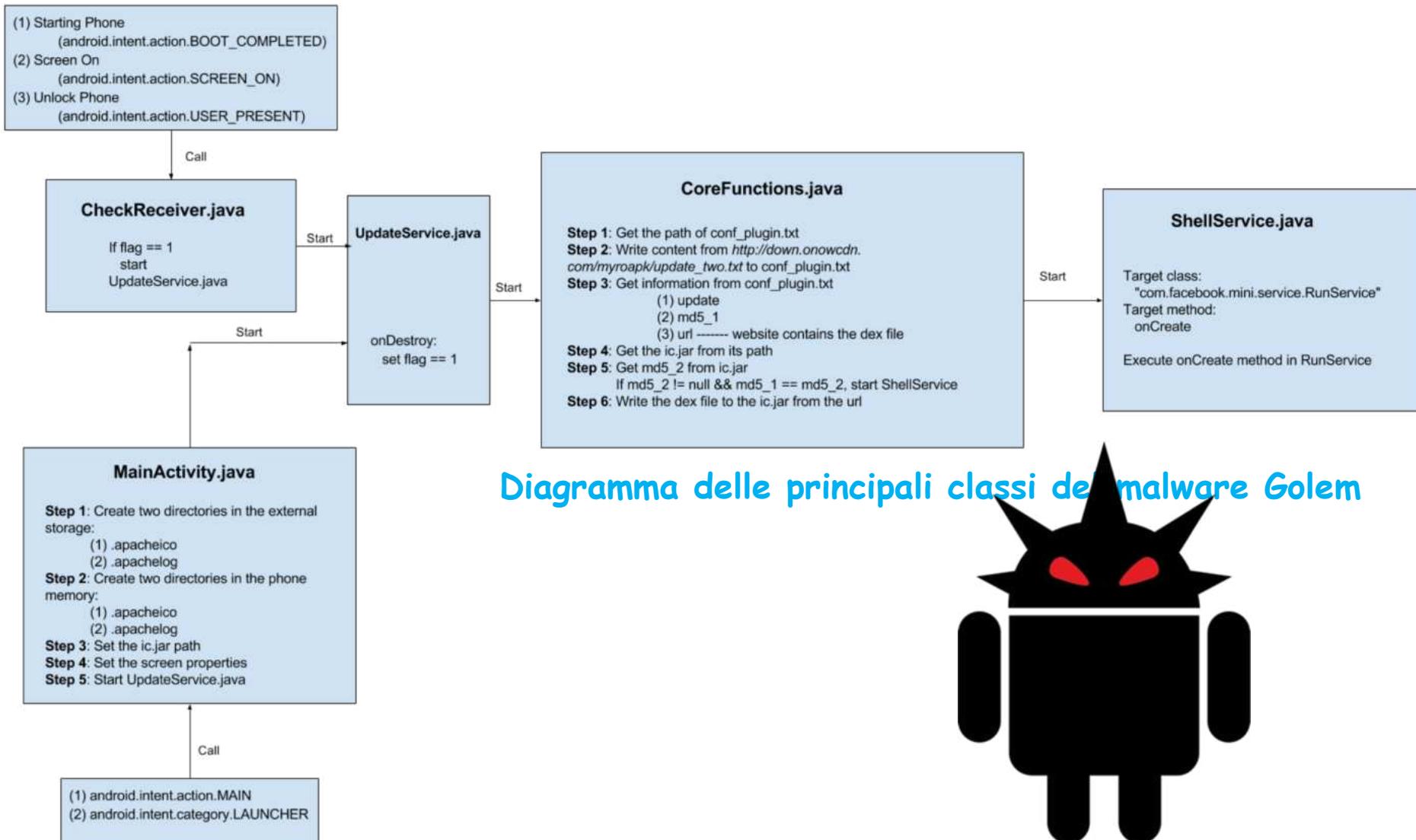
- I malware per dispositivi mobile (smartphone, tablet, etc.)
 - Hanno una struttura ed una diffusione diversa rispetto ai malware per piattaforme desktop
- Con il costante incremento delle tecnologie e l'enorme diffusione globale dei dispositivi mobile
 - Si è verificato un significativo aumento anche per quanto riguarda i malware su tali dispositivi

Malware, Dispositivi Mobile e Analisi

- Oltre il significativo e preoccupante incremento del numero di nuovi malware identificati
 - Vi è un notevole incremento anche della loro complessità



Ci soffermeremo sull'analisi di diversi malware per dispositivi mobile



Watermark e Schemi di Watermarking

- Il *watermark* è essenzialmente una sorta di «*filigrana*»
 - Nell'ambito informatico si parla di digital watermark, che può essere costituito da una sequenza di bit (ottenuta da un logo, una stringa, etc.)
- Con *watermarking* si intende invece la tecnica che permette l'inserimento (*embedding*) del watermark in dati multimediali (video, audio, etc.)

Watermark e Schemi di Watermarking

- Uno schema di watermarking definisce
 - Come il watermark viene immerso nel documento o dato
 - Fase di embedding
 - Come il watermark viene estratto e/o rilevato dal documento o dato marchiato
 - Fase di extraction/detection

Watermark e Schemi di Watermarking

Watermarking su

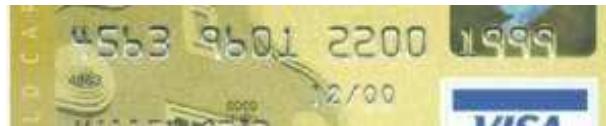
➤ Immagini



➤ Audio



Algoritmo LUHN-10



Card Type	Prefix	Length
MASTERCARD	51-55	16
VISA	4	13, 16
AMEX	34, 37	15
Diners Club/ Carte Blanche	300-305 36, 38	14
Discover	6011	16
JCB	3	16
JCB	2131, 1800	15

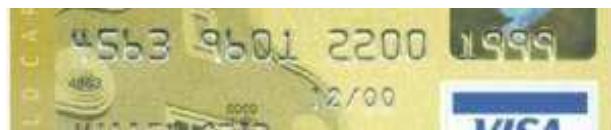
Specificato in ISO-7812-1, standard per il formato delle carte di credito

Ultima cifra per controllo dell'errore

4563 9601 2200 1999



Algoritmo LUHN-10



Position	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Number	4	3	2	1	2	3	4	2	7	5	6	7	8	1	9	0
Multiplier	2		2		2		2		2		2		2		2	
Total	8	3	4	1	4	3	8	2	14	5	12	7	16	1	18	0
Sum	8	3	4	1	4	3	8	2	5	5	3	7	7	1	9	0

Somma = 70 multiplo di 10

Domande?

