

Sicurezza

a.a. 2019/20

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

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



Marzo 2020

Informazioni sul Corso

➤ Insegnamento dal 24 febbraio al 5 giugno 2020
– 48 ore

➤ Orario lezioni:
– Lunedì 16:00 - 18:00, Aula F/8
– Venerdì 14:00 - 16:00, Aula F/8



➤ Home-page del corso:
– http://www.di.unisa.it/~ads/ads/Sicurezza_su_Reti.htm

Anni precedenti

Corsi precedenti prof. Alfredo De Santis

- a.a. 2013/14, ..., 2018/19
- Modalità esame inalterate

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](#)

Organizzazione

➤ Bibliografia

- Libri
- Materiale/Appunti dalle lezioni



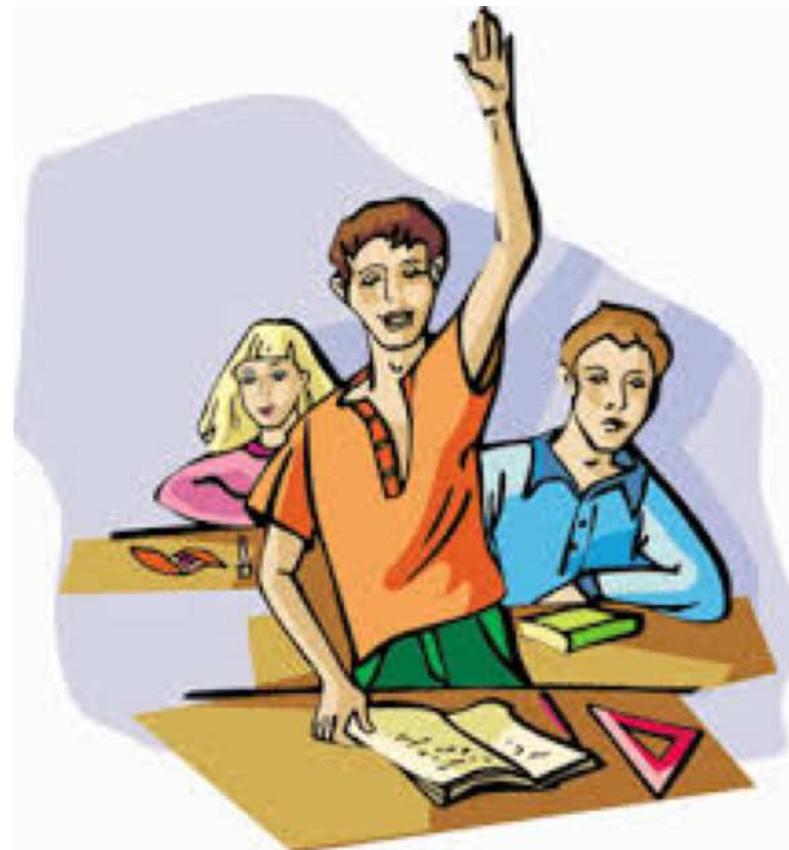
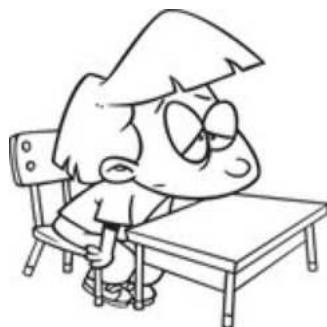
➤ Progetti e presentazioni di argomenti specifici (anni precedenti)



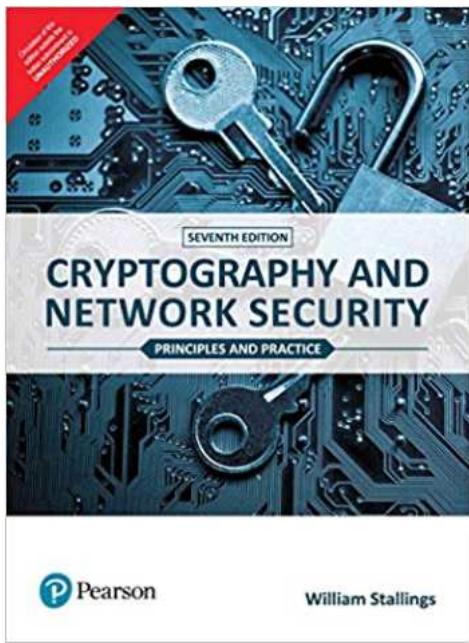
Interazione

Domande

Interesse



Testi di riferimento

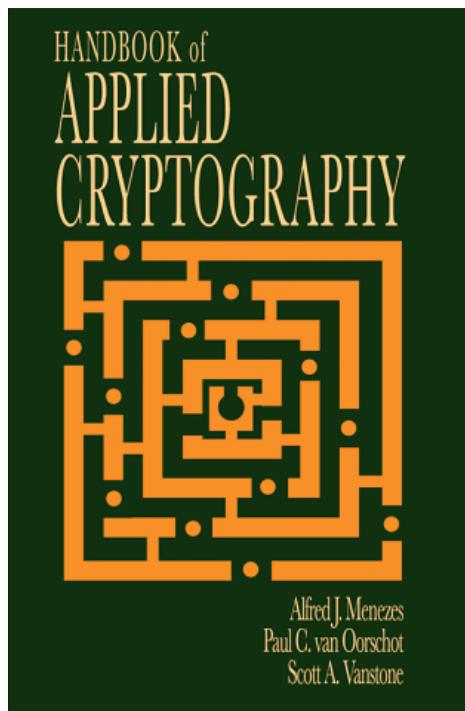


Cryptography and Network Security:
Principles and Practices
Prentice-Hall (7/Ed)
by William Stallings, 2016

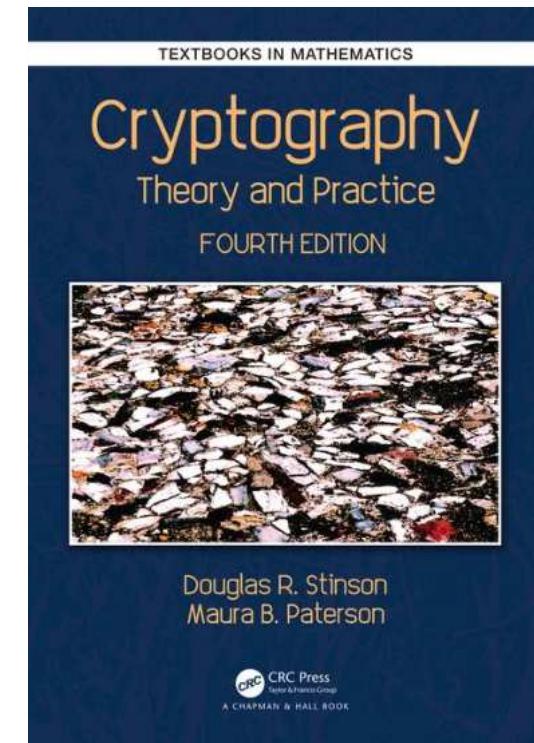
Crittografia e Sicurezza delle Reti
McGraw-Hill (2/Ed)
by William Stallings, 2007



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

Esami

- L'esame prevede una prova scritta e una prova orale
- Sono previsti **sette appelli** suddivisi come segue:
 - Preappello, 10-13 giugno 2020
 - I appello, 24 giugno - 7 luglio 2020
 - II appello, 8-31 luglio 2020
 - 1-11 settembre 2020
 - Un appello straordinario Novembre 2020
 - Due appelli nel periodo Gennaio 2021 - Febbraio 2021



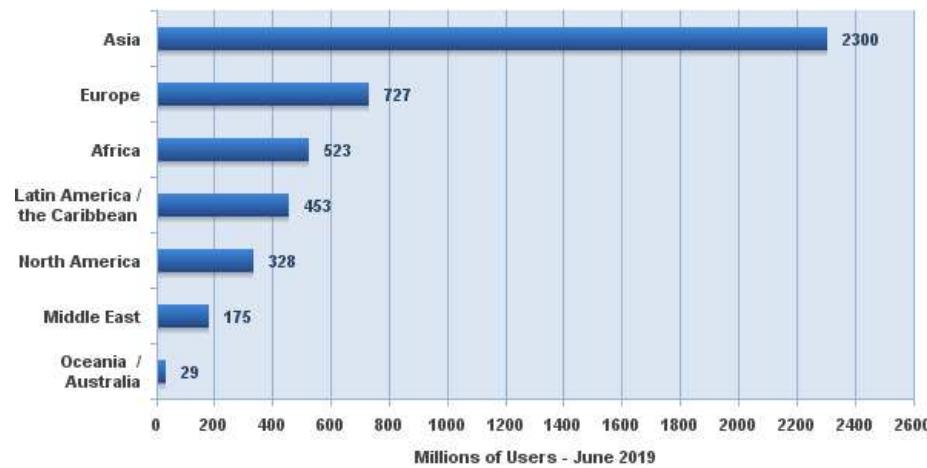
Nessuna prova intercorso



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

Utenti Internet nel mondo

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

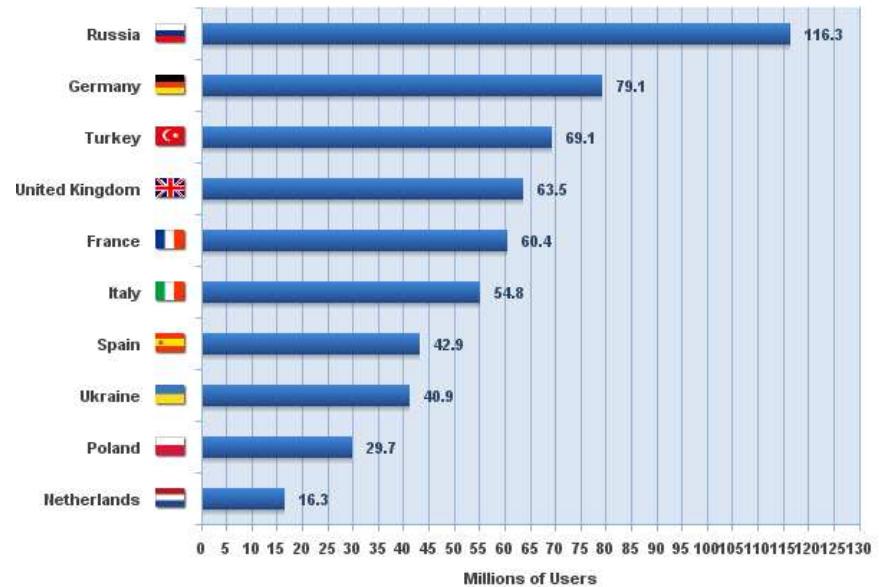


Source: Internet World Stats - www.internetworldstats.com/stats.htm

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

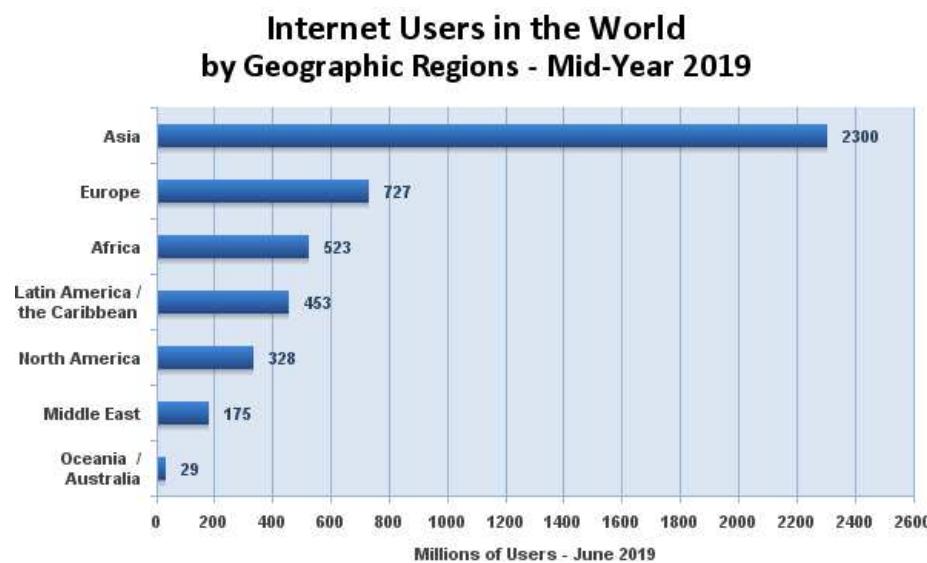
Basis: 727,559,682 estimated Internet Users in Europe on June 2019

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

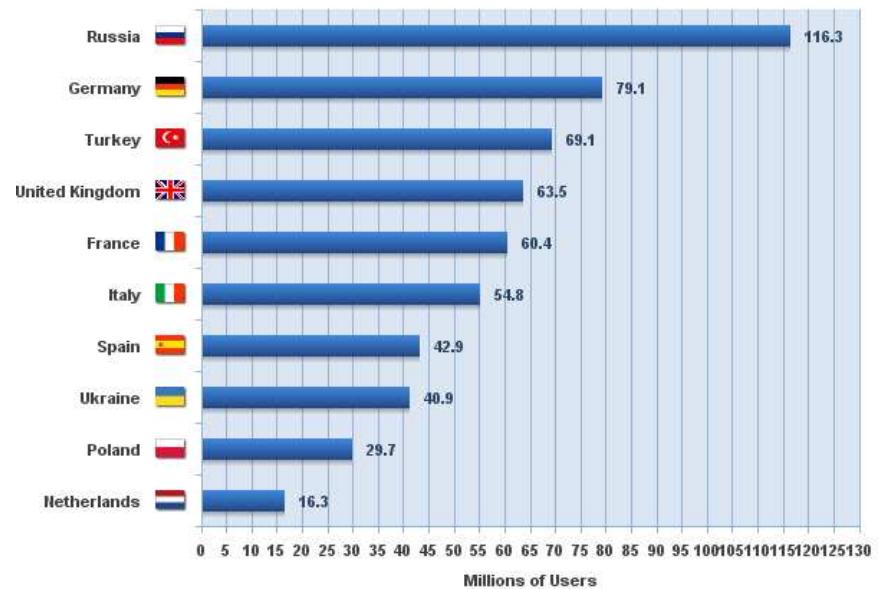
Utenti Internet nel mondo

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

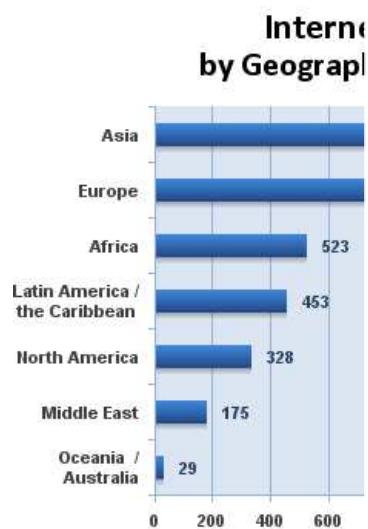
**Internet Top 10 Countries in Europe
June 30, 2019**



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

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



...tuttavia...

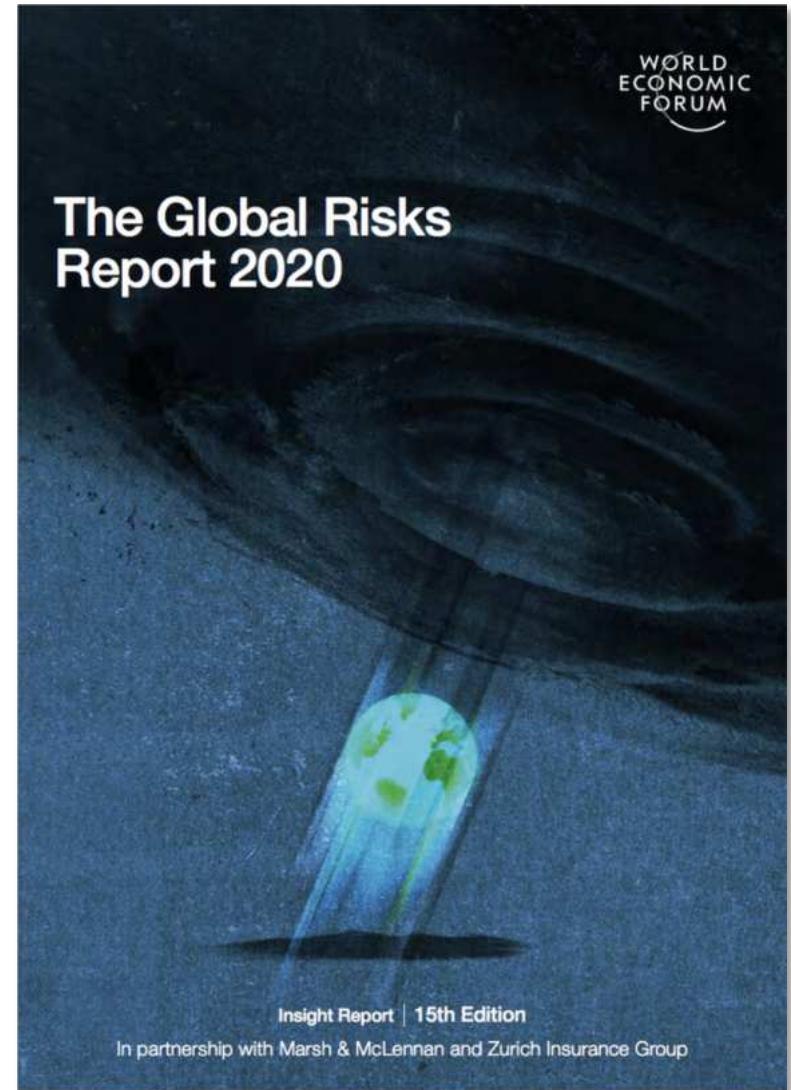
... espone i computer all'azione di attacchi da parte di malintenzionati

- 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

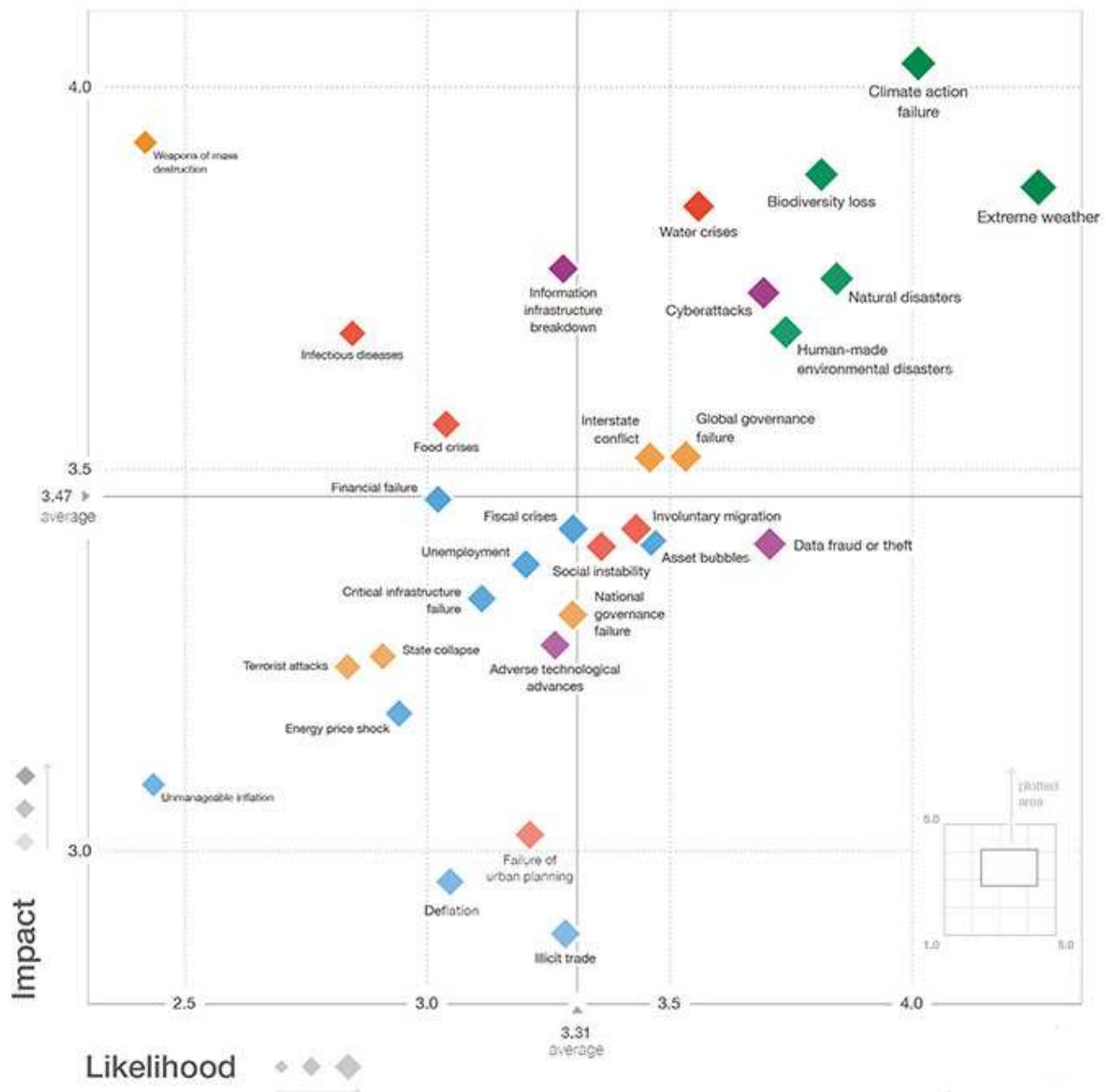
Top 10 risks in terms of

Impact

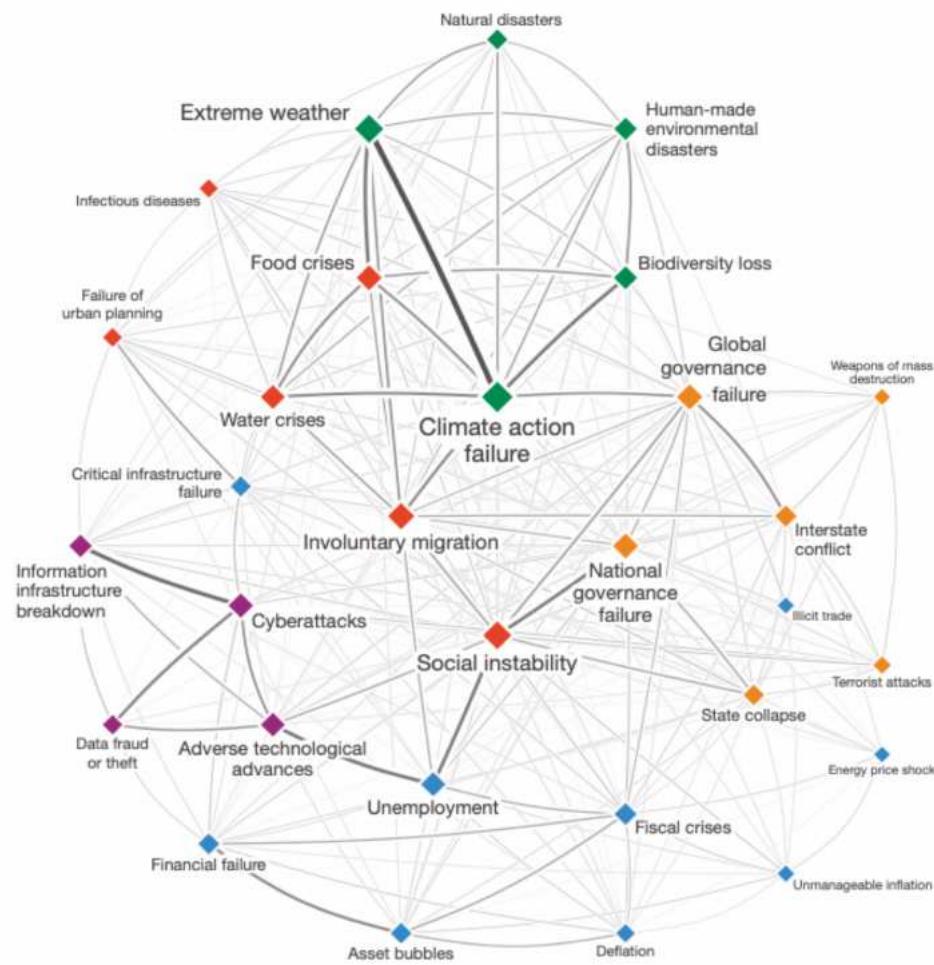
- 1 Climate action failure
- 2 Weapons of mass destruction
- 3 Biodiversity loss
- 4 Extreme weather
- 5 Water crises
- 6 Information infrastructure breakdown
- 7 Natural disasters
- 8 Cyberattacks
- 9 Human-made environmental disasters
- 10 Infectious diseases

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological



The Risk-Trends Interconnections Map 2020



Economic
Risks

Environmental
Risks

Societal
Risks

Geopolitical
Risks

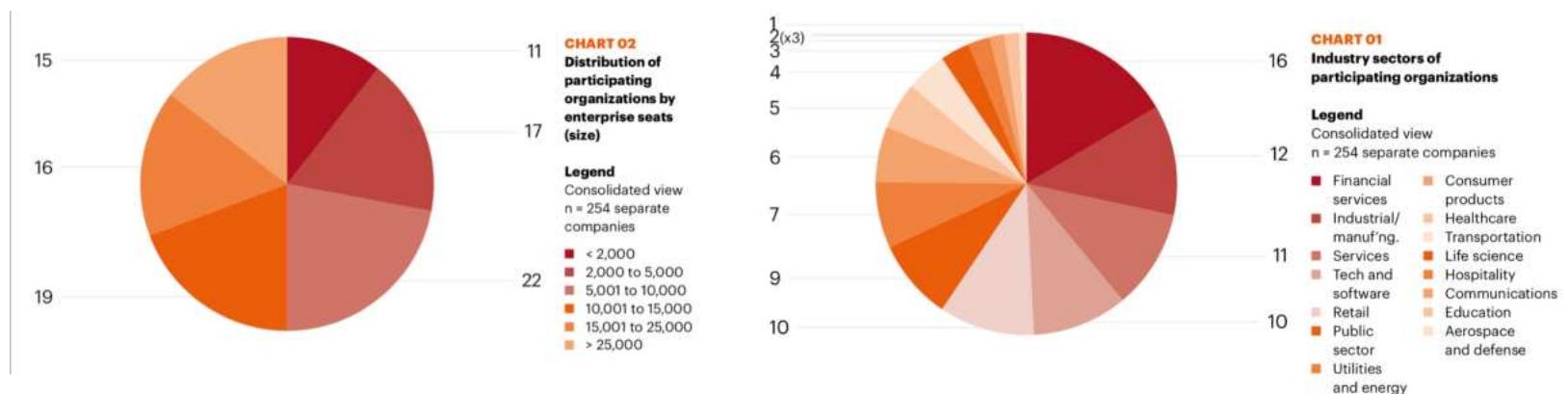
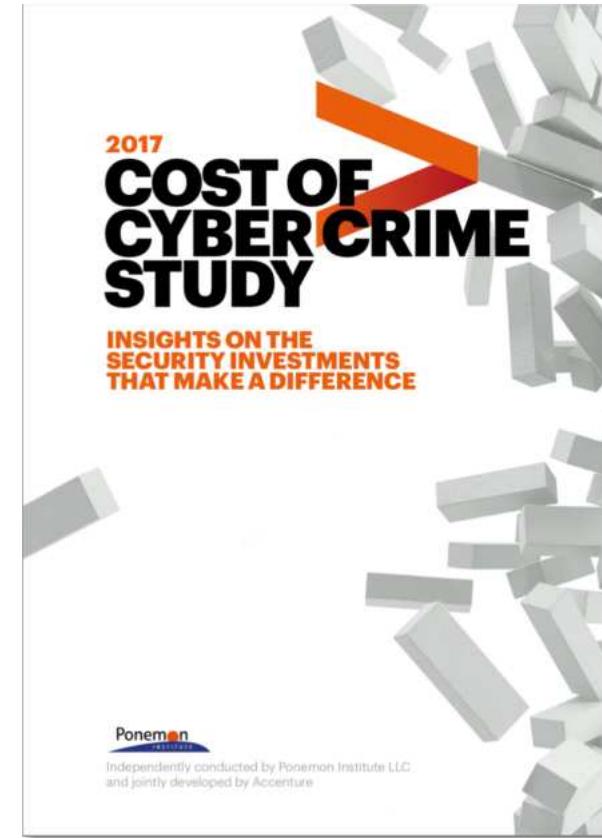
Technological
Risks



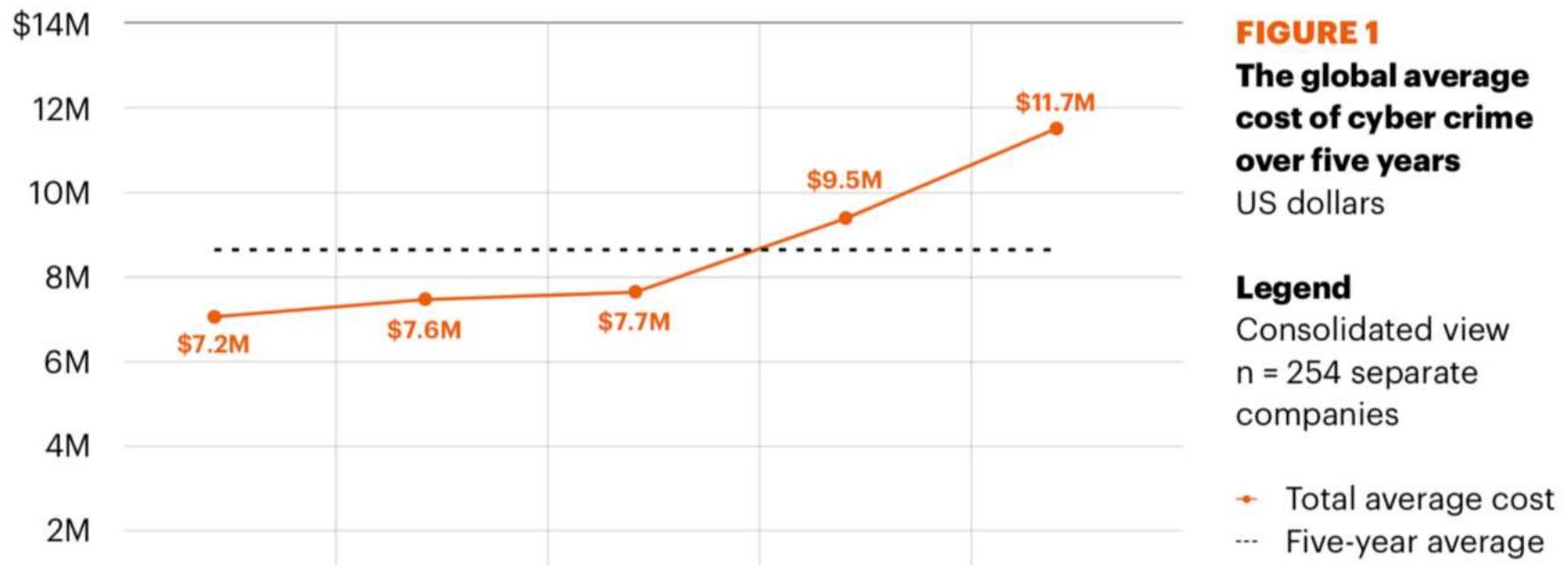
Number and strength
of connections
("weighted degree")

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

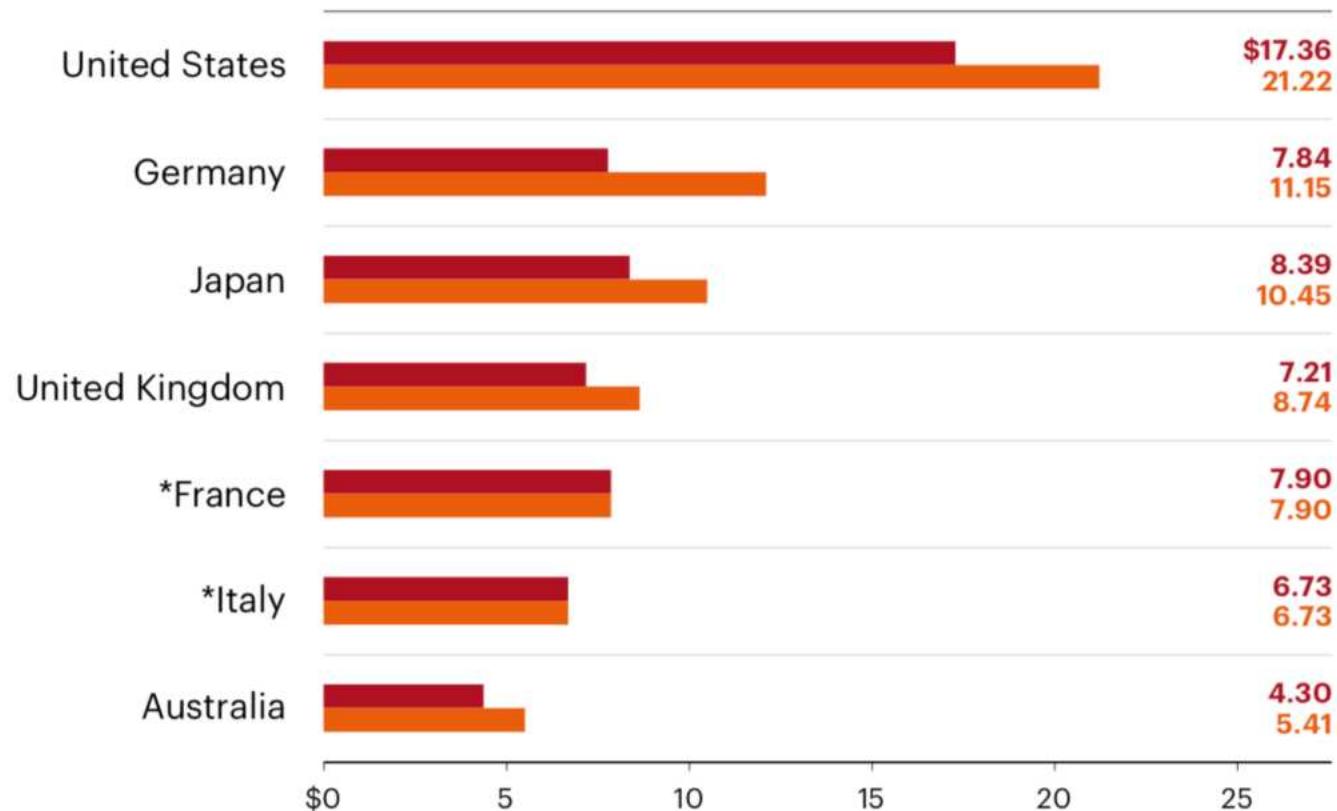


FIGURE 2

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

*Historical data does
not exist for newly added
country samples

Legend

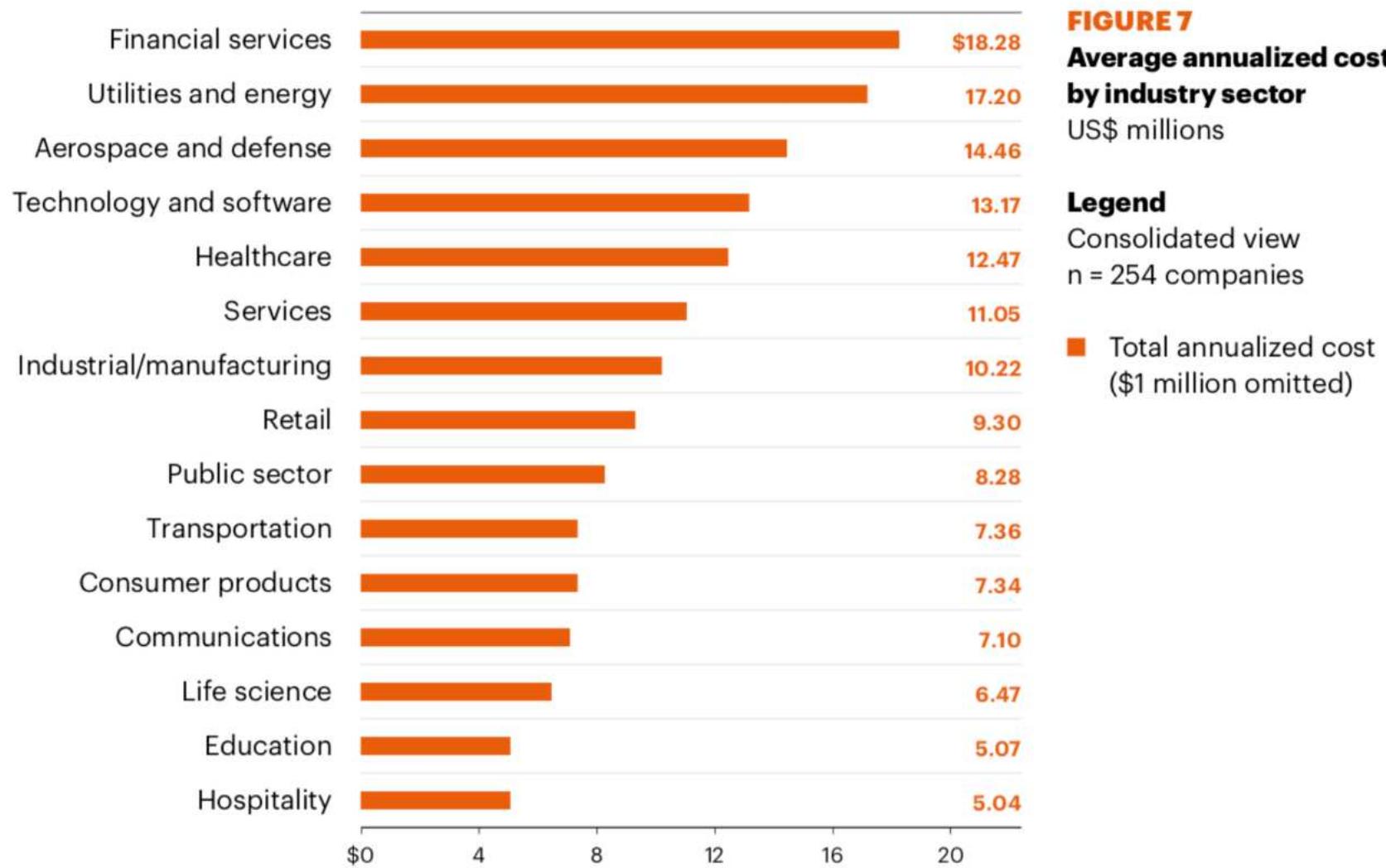
US\$ millions

n = 254

■ FY2016 (US\$ millions)

■ FY 2017 (US\$ millions)

Costo Cybercrime per settore industriale



Costo Cybercrime per tipo di attacco

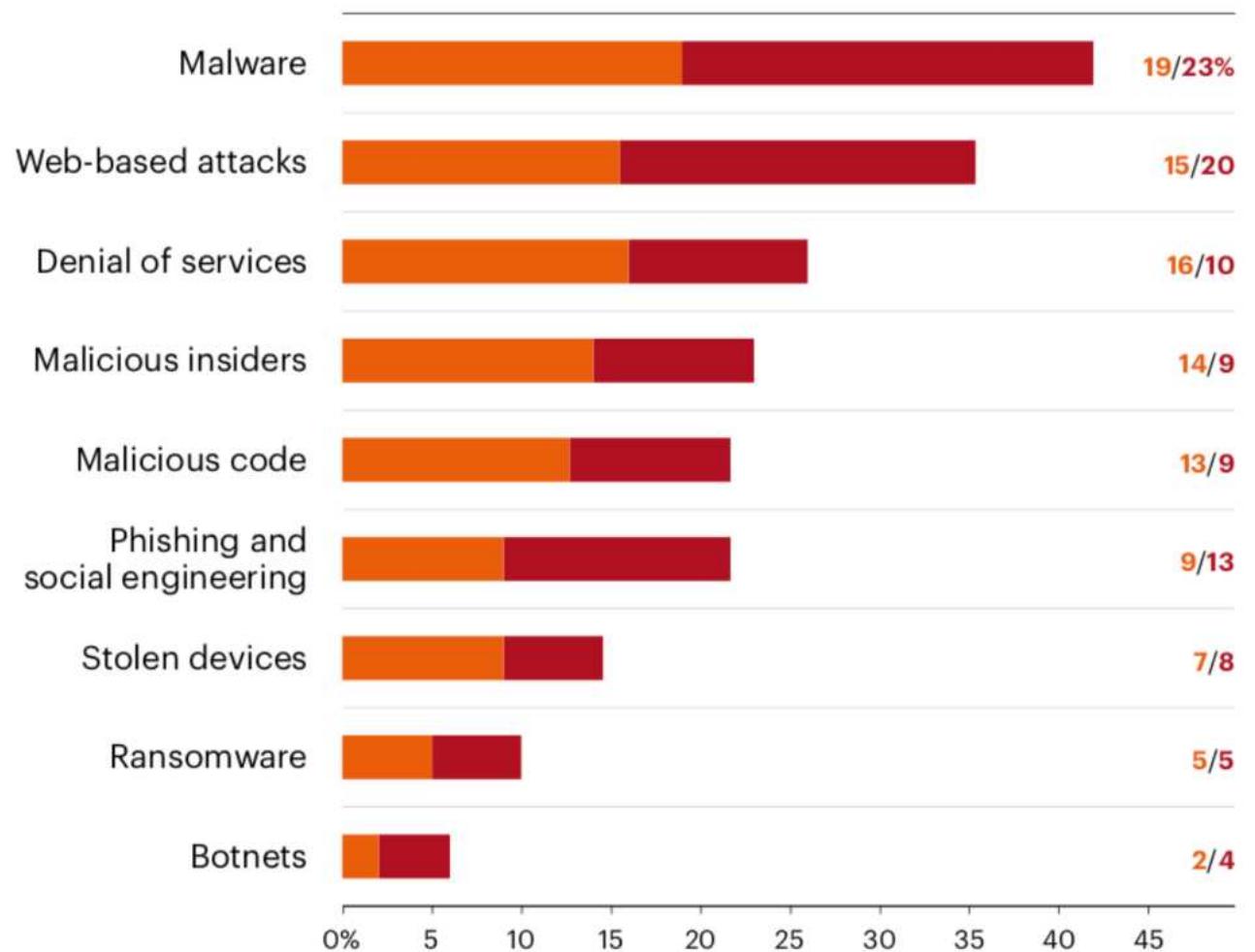


FIGURE 8
**Organizational size
affects the cost of nine
attack types**
Size measured according
to the number of
enterprise seats within
the participating
organizations

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

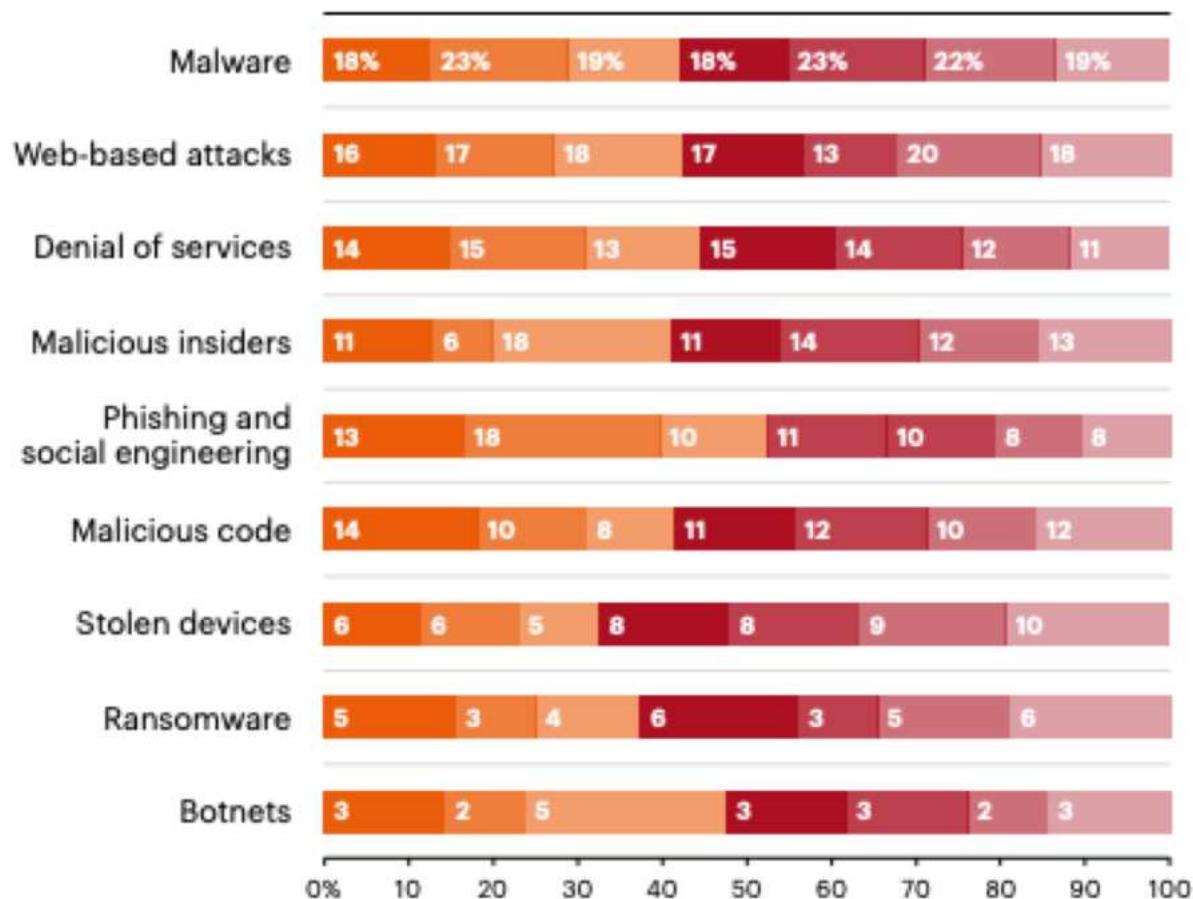


FIGURE 10
Percentage annualized
cyber crime cost by
attack type and country

Legend

Consolidated view
n = 254 companies

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

Costo Cybercrime per attività interna

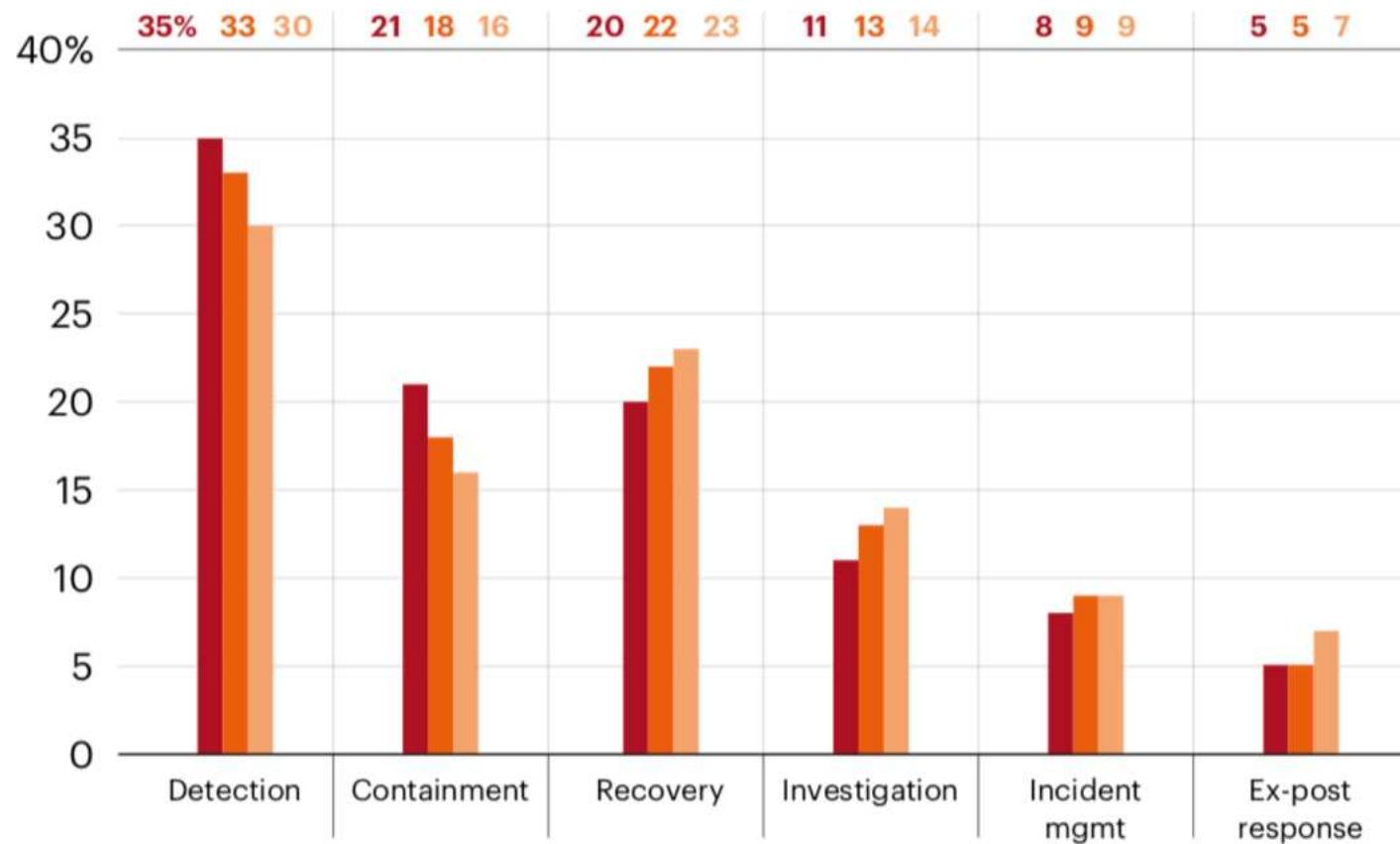


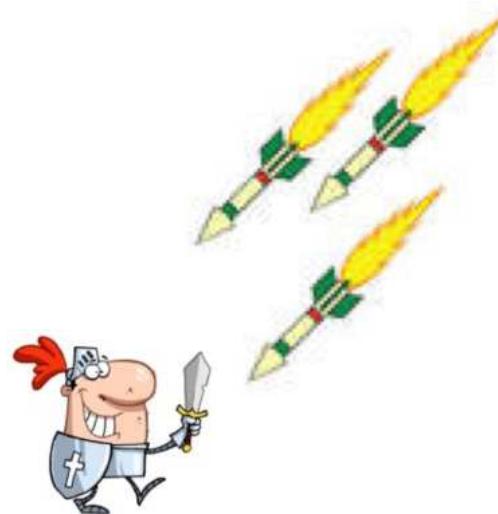
FIGURE 16
Percentage cost by internal activities

Legend
Consolidated view
n = 254 companies

- FY 2017
- FY 2016
- FY 2015

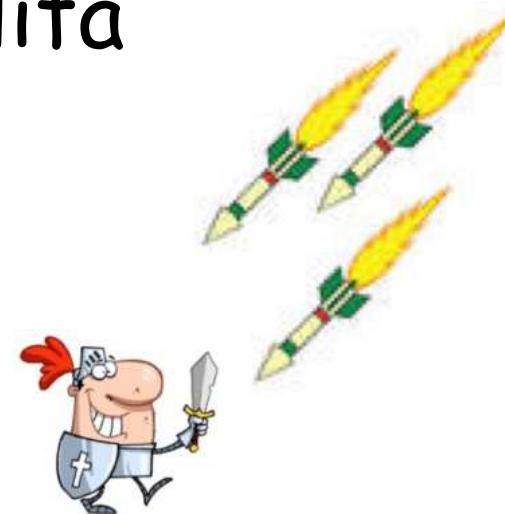
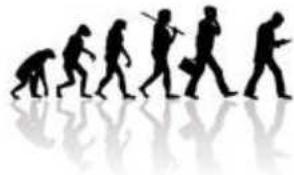
Difese statiche e dinamiche

- Difesa statica prima o poi cede
dopo nuovi attacchi



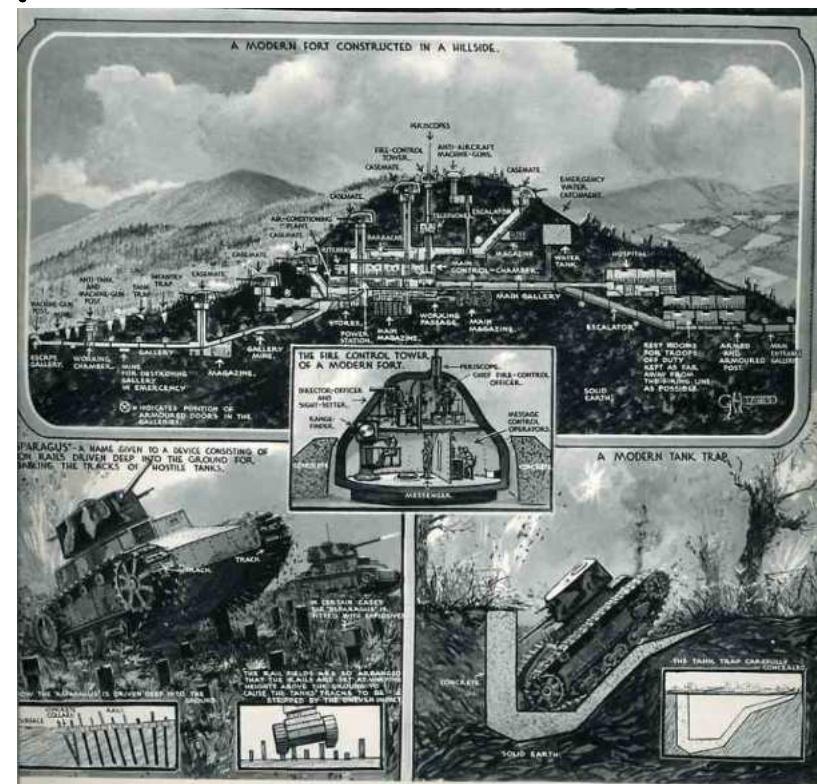
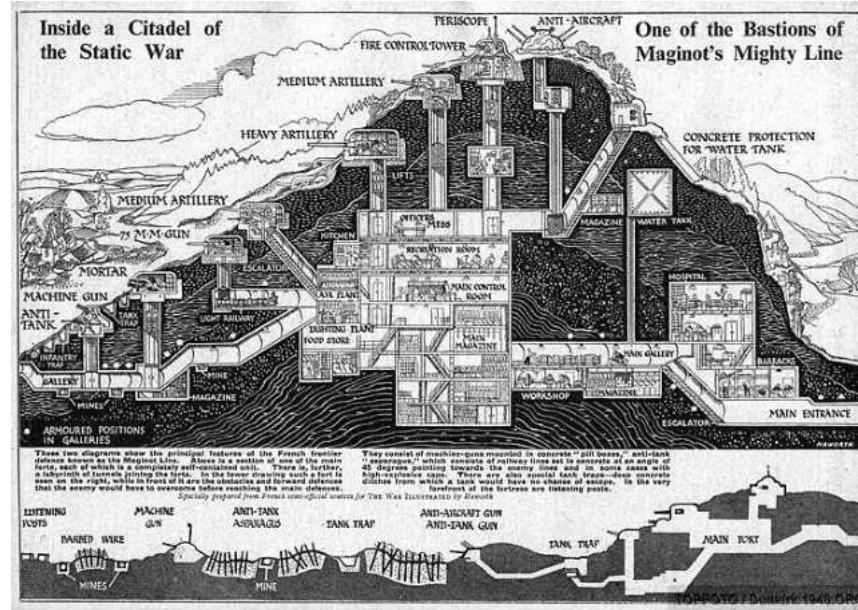
Difese statiche e dinamiche

- 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."



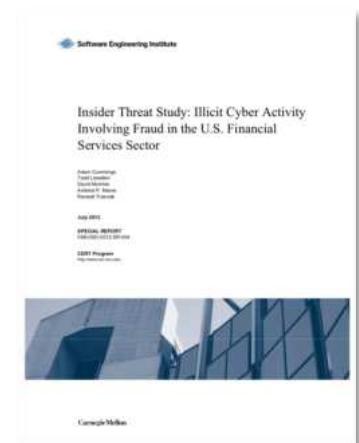
Muraglia cinese

- 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
 - Circular Error Probability 1100m a 440 km
- Molto mobile e difficile da individuare



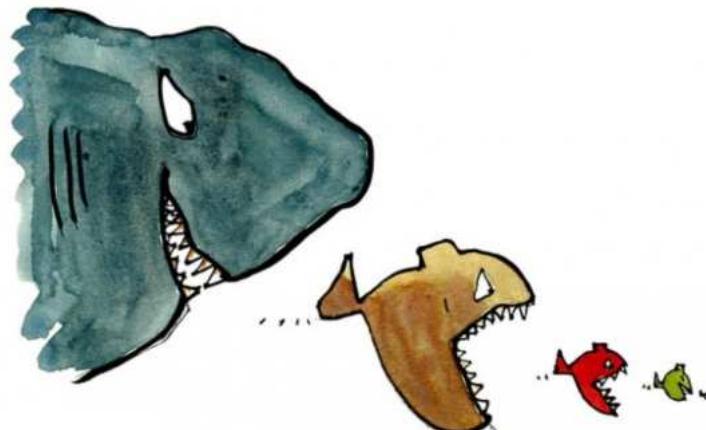
Prede e predatori

- Teoria dell'evoluzione
- Evoluzione dei predatori

Canini ed artigli più grandi ed affilati,

... ed evoluzione prede

corazze più resistenti e zampe più veloci



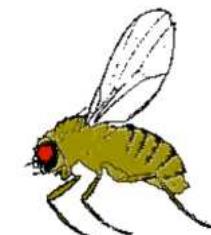
Antilocapra americana



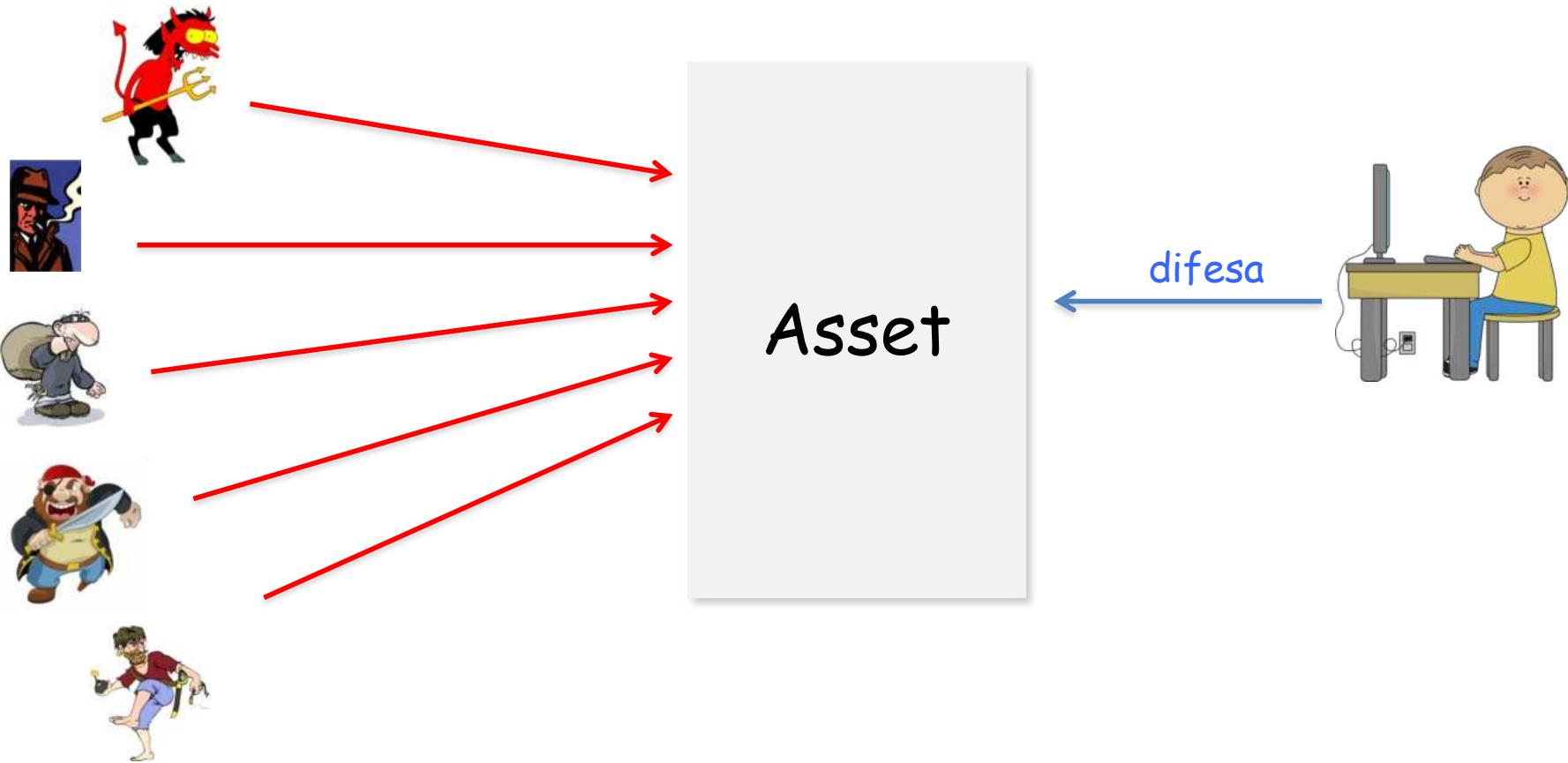
- Habitat: prateria
- Predatori: lupo, coyote, lince rossa
- Animale terrestre più veloce dopo il ghepardo
 - Raggiunge i 100 km/h (superato solo su brevi distanze)
- Rileva movimenti ad una distanza di 4-5 km

Drosofilia (moscerino della frutta)

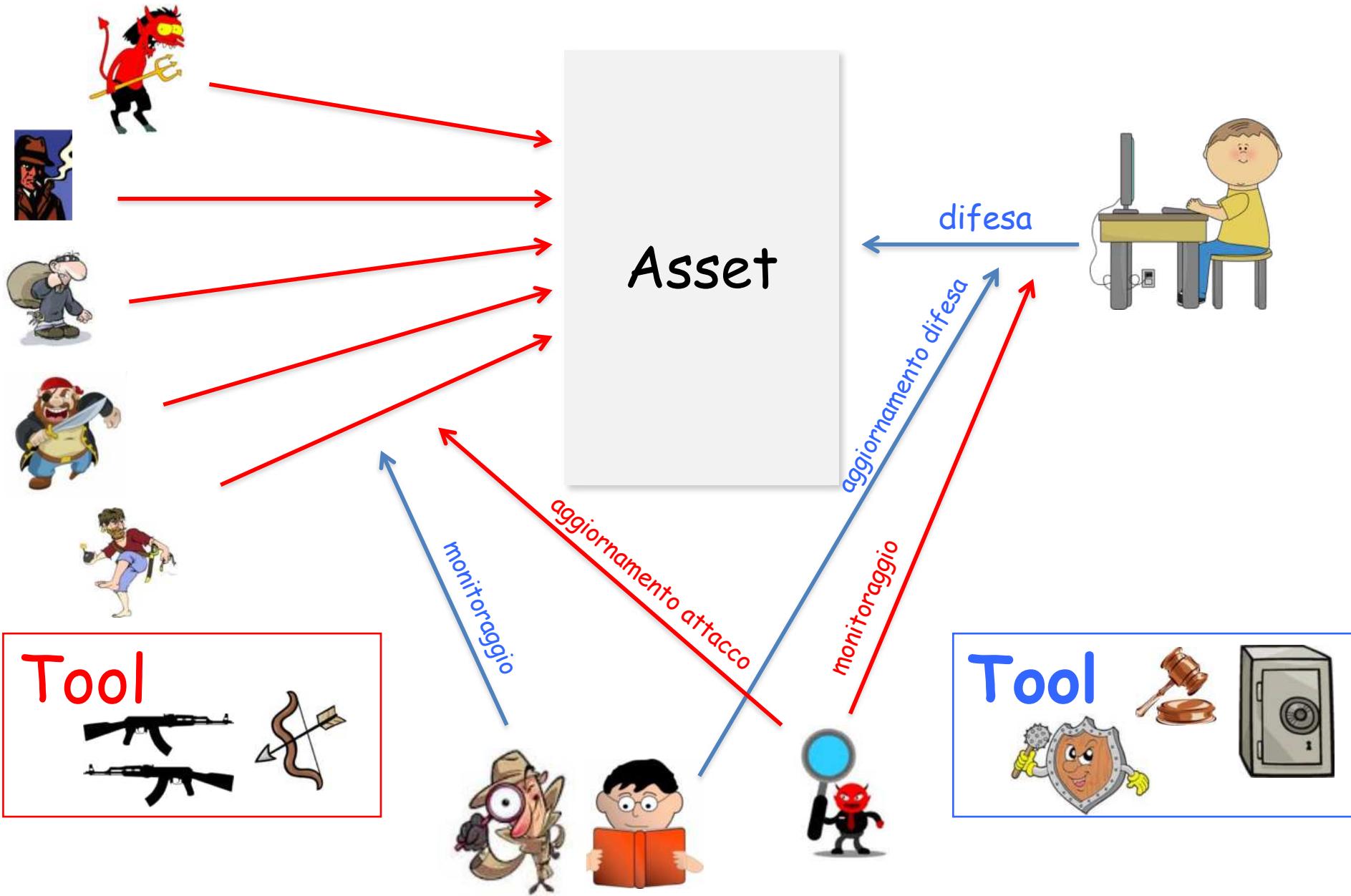
- Le ali possono battere fino a 250 volte al secondo
- Volo con tratti lineari, con rapidi cambi di direzione
 - Può ruotare di 90 gradi in meno di 50 millisecondi
- Presenta nervi ottici collegati direttamente ai muscoli delle ali
 - mentre in altri insetti c'è in ogni caso un passaggio attraverso il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



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:

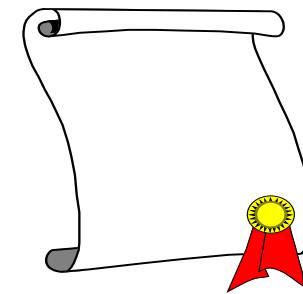
- Riproduzione
- Modifica dei messaggi
- Denial of service



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

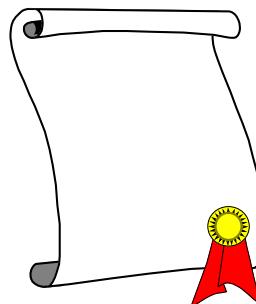


Informazioni { trasmesse
memorizzate

sono accessibili in lettura
solo da chi è autorizzato

Autenticazione

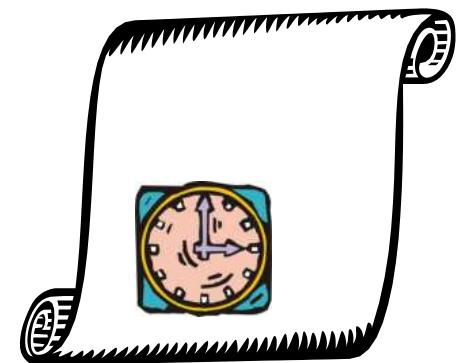
messaggi



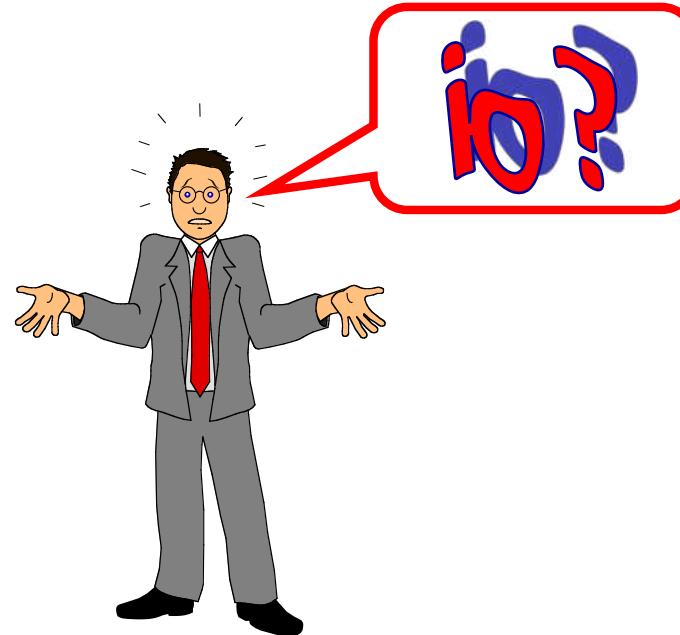
entità
(Identificazione)



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

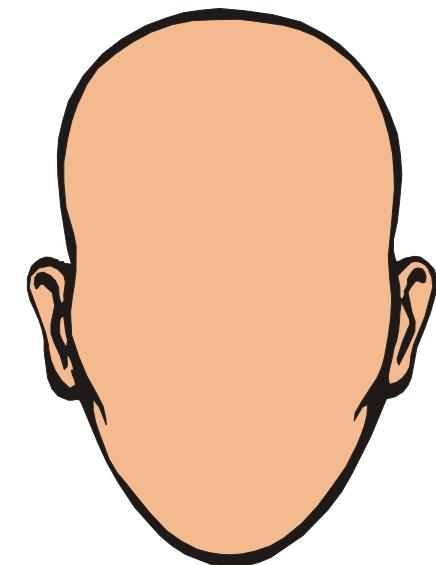
Solo chi è autorizzato può
modificare l'attività di un
sistema o le informazioni
trasmesse



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

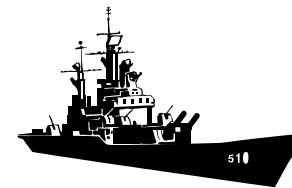
- Prima parte: Crittografia e Strumenti Crittografici
 - Cifrari simmetrici
 - Cifrari asimmetrici
 - Firme digitali
 - Funzioni hash e integrità dei dati
 - OpenSSL
- Seconda parte: Sicurezza su Reti ed Applicazioni
 - Public Key Infrastructure (PKI)
 - Autenticazione utenti
 - Sicurezza IP e WWW
 - Malware
 - Protezione dati multimediali

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

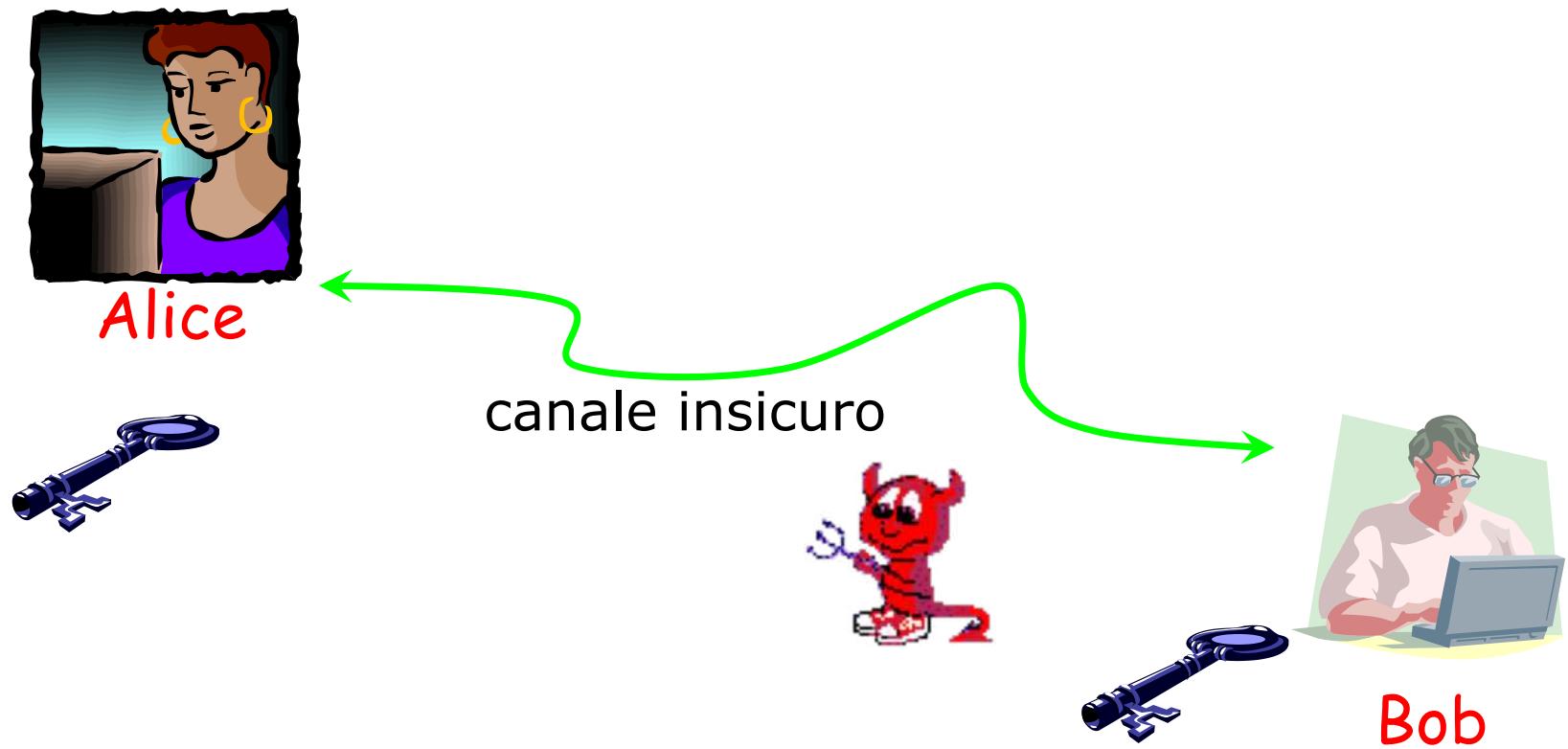
➤ Descritto da Polibio (206-124 a.C.) nelle "Storie"

	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

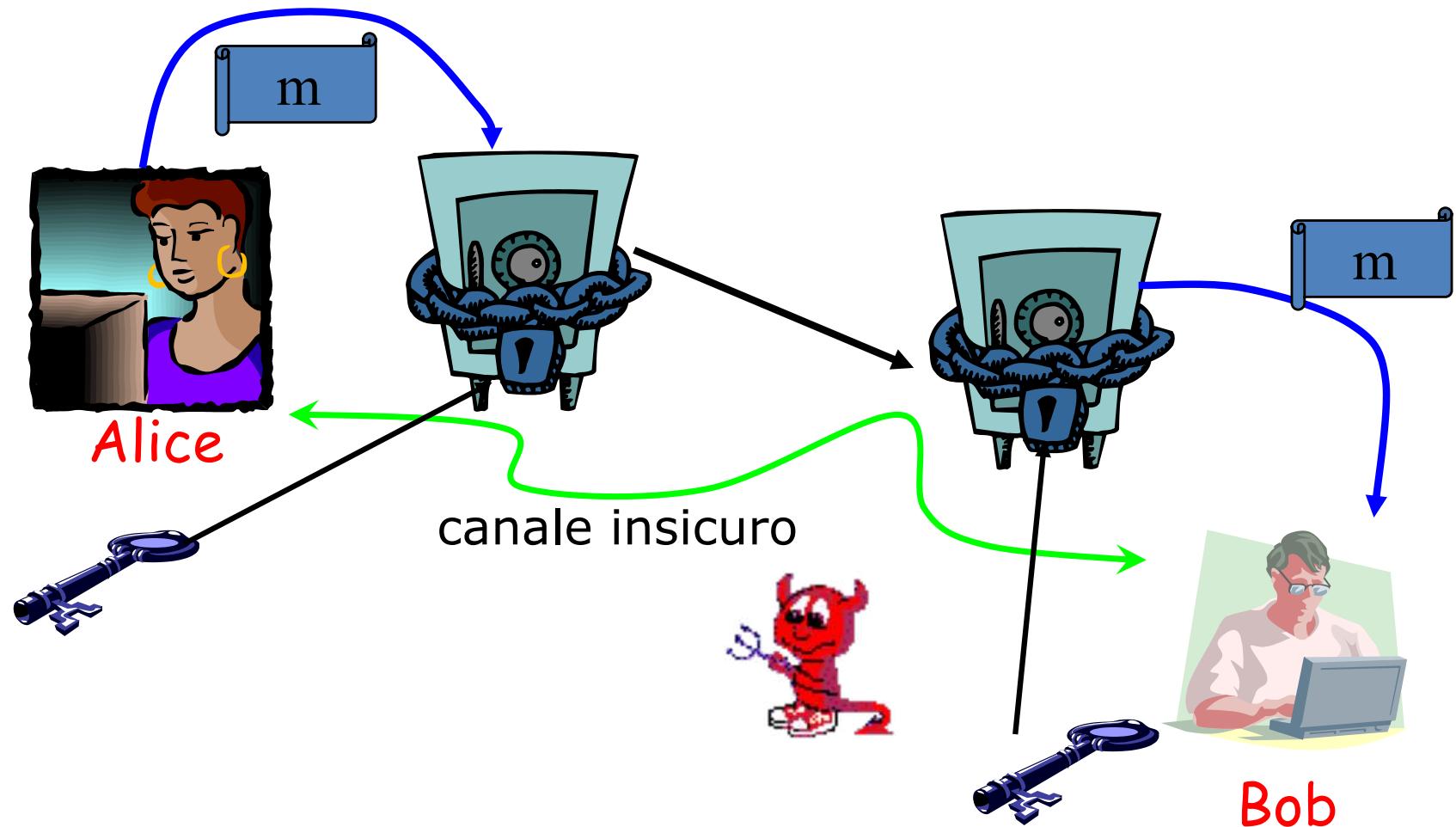


testo in chiaro: C A S A
testo cifrato: (1,3) (1,1) (4,3) (1,1)

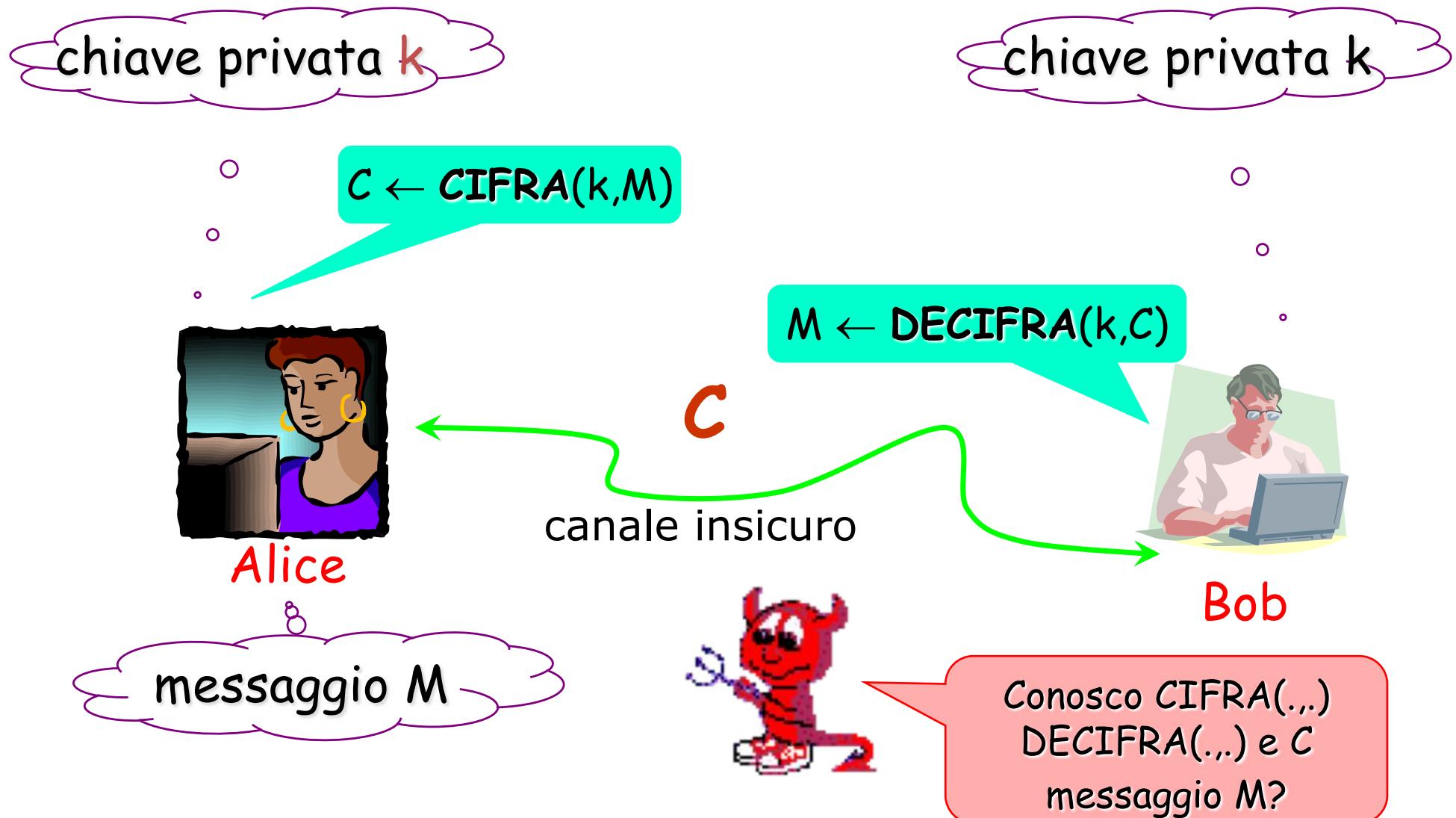
Cifrari simmetrici



Cifrari simmetrici



Cifrari simmetrici



Cifrari simmetrici

- Cifrari a blocco
 - DES, Triplo DES, AES
 - Blowfish, RC5, RC6, ...
- Stream Cipher
 - LSFR (Linear Feedback Shift Register)
 - RC4

Li vedremo ed
utilizzeremo in
OpenSSL

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

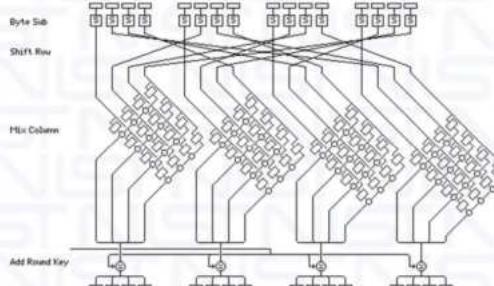
An international competition led to the voluntary standard that today protects millions of IT systems.

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

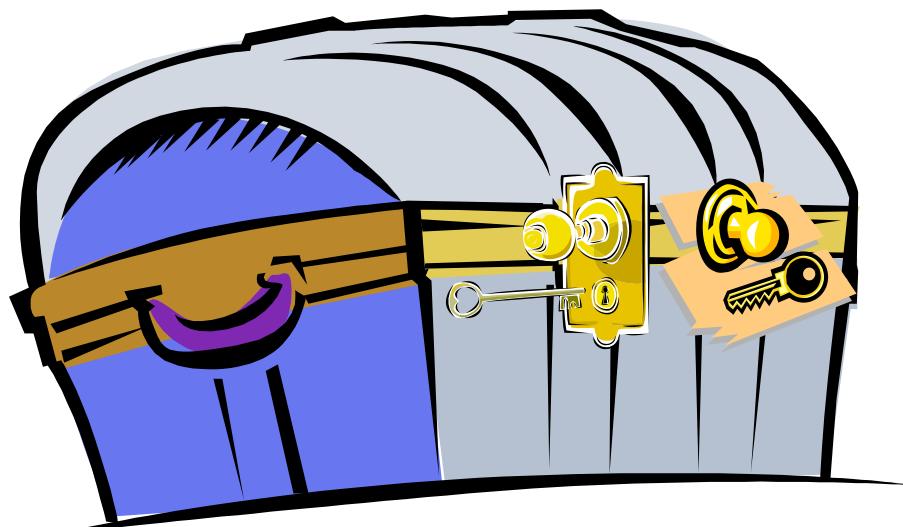
Anyone can design a cipher that he himself cannot break. This is why you should uniformly distrust amateur cryptography, and why you should only use published algorithms that have withstood broad cryptanalysis. All cryptographers know this, but non-cryptographers do not. And this is why we repeatedly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

Bruce Schneier

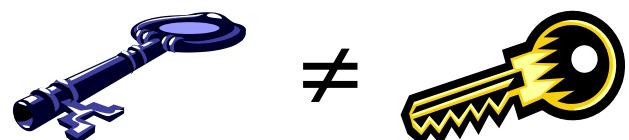
https://www.schneier.com/blog/archives/2015/05/amateurs_produc.html

Cifrari asimmetrici

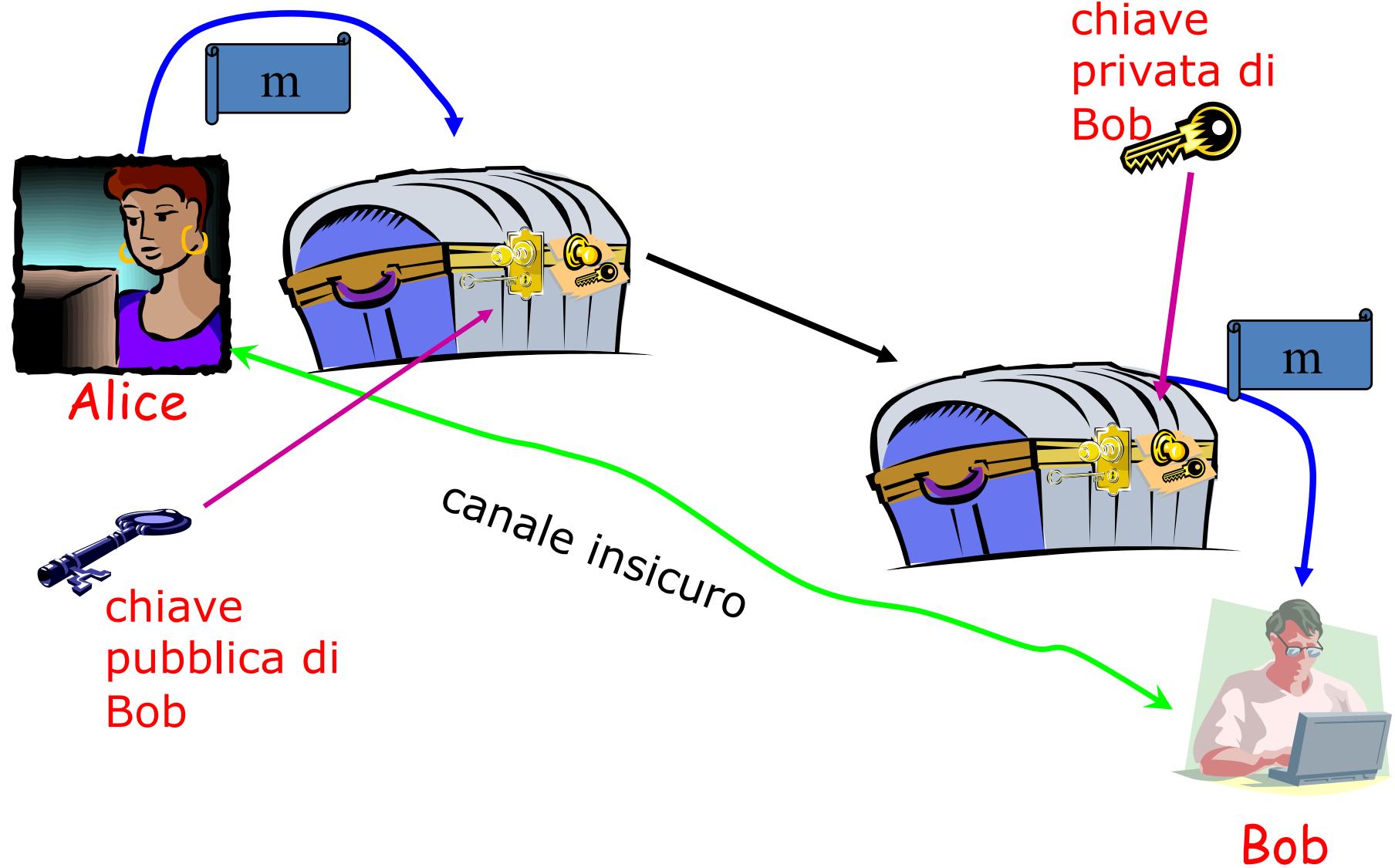
- Usano una cassaforte con due lucchetti
 - Con una chiave (**pubblica**) chiudiamo la cassaforte
 - Con l'altra chiave (**privata**) apriamo la cassaforte



Public key ≠ Private key



Cifrari asimmetrici



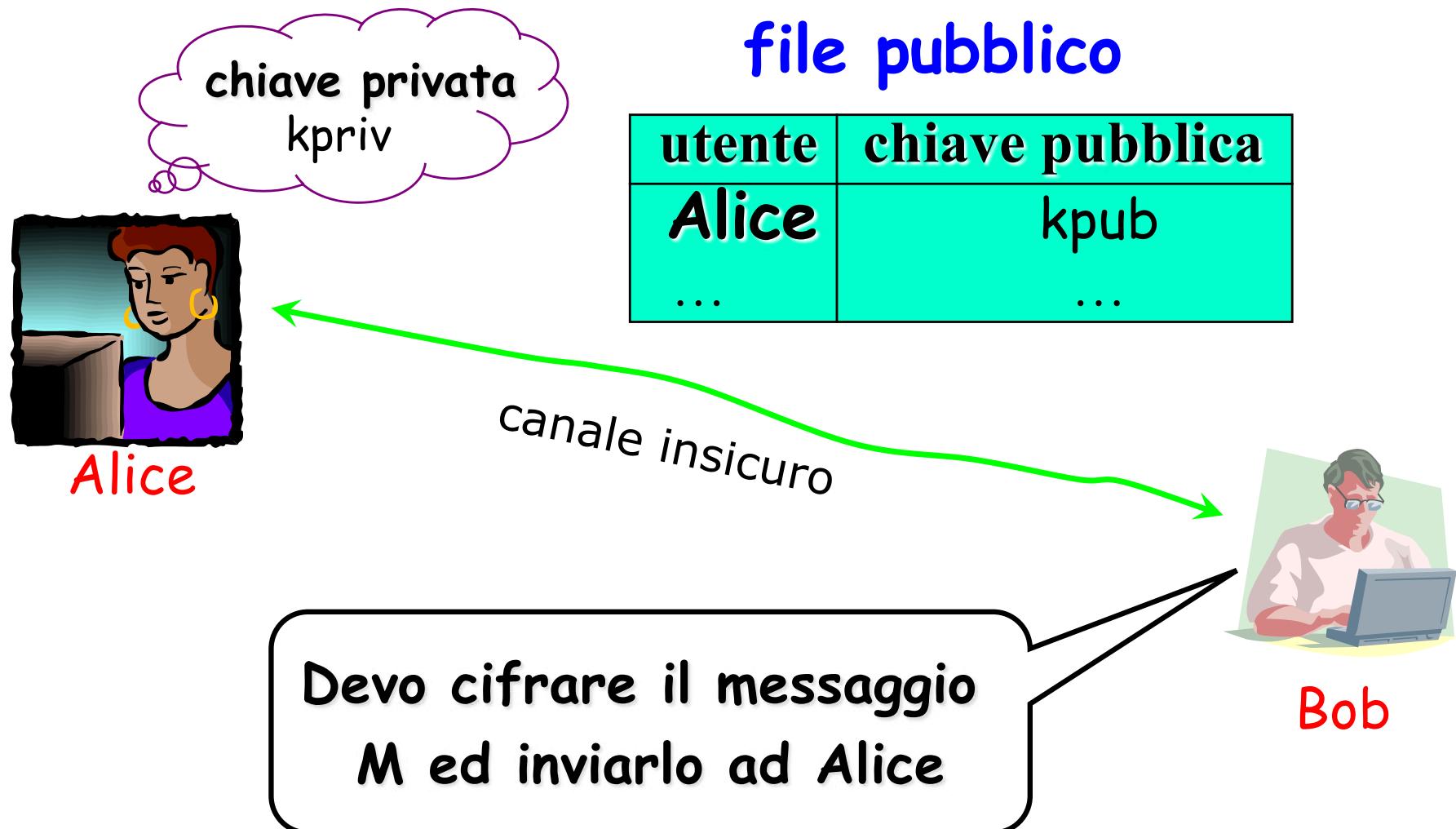
Cifrari asimmetrici



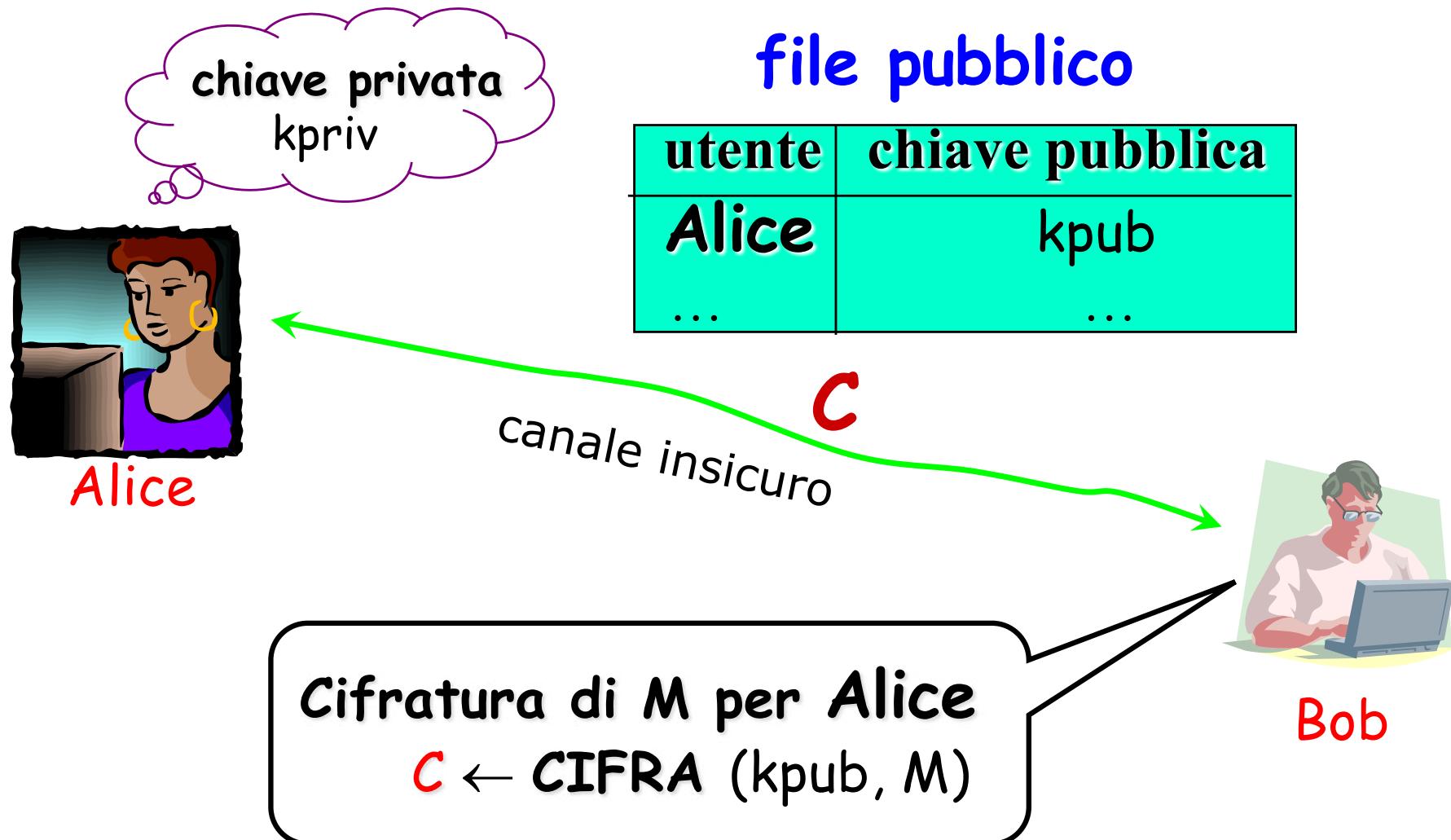
file pubblico

utente	chiave pubblica
Alice	kpub
...	...

Cifratura



Cifratura



Decifratura

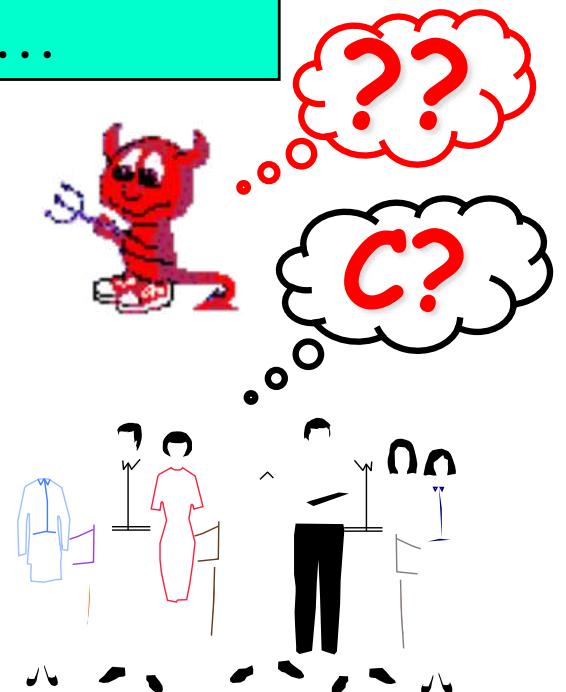
Devo decifrare il messaggio cifrato **C**



Alice

file pubblico

utente	chiave pubblica
Alice	kpub
...	...



Decifratura

chiave privata
kpriv

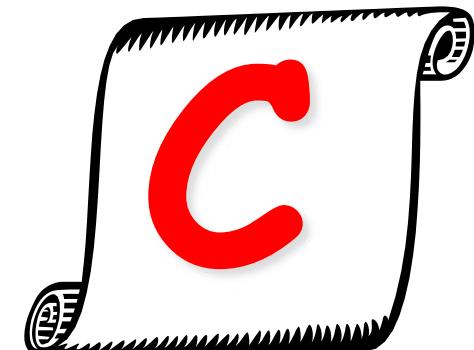


Alice

file pubblico

utente	chiave pubblica
Alice	kpub
...	...

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



Cifrari asimmetrici

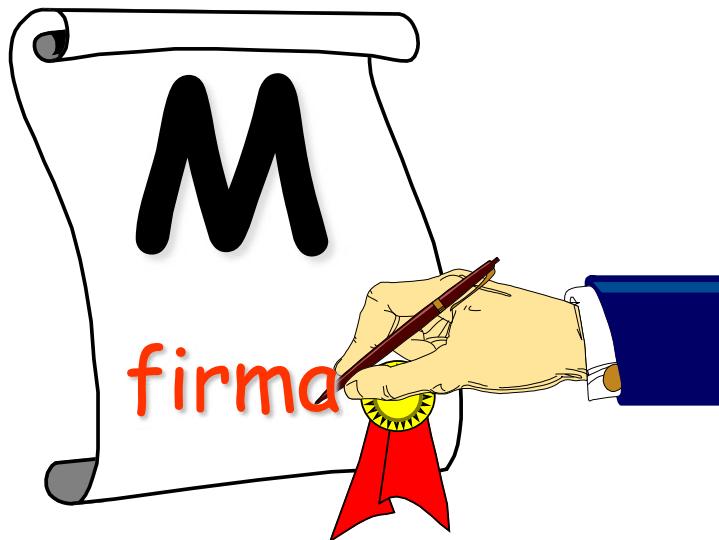
- Chiunque può cifrare un messaggio per Alice
- Solo Alice può decifrare un messaggio cifrato per lei
- Non ci sono chiavi condivise tra Alice e Bob
 - Ciascuno dei due utenti genera da solo la propria coppia di chiavi e rende pubblica la chiave pubblica
- Ogni utente memorizza una sola chiave (privata)

Cifrari asimmetrici

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

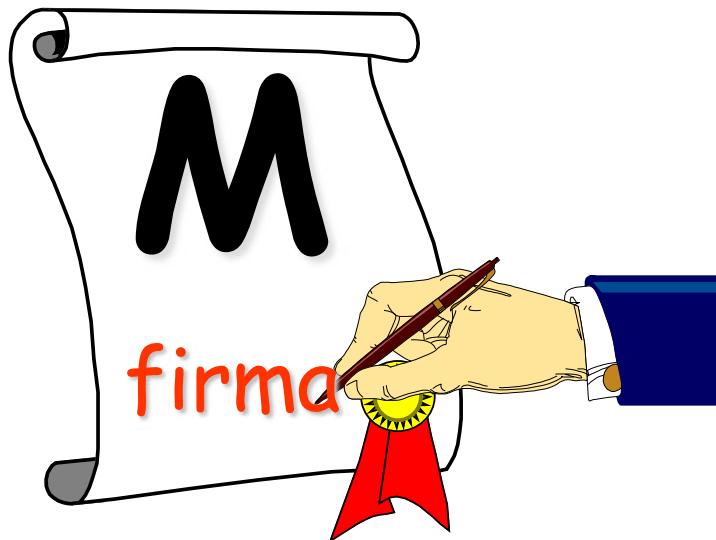
Li vedremo ed
utilizzeremo in
OpenSSL

Firma Digitale



Equivalent alla firma
convenzionale

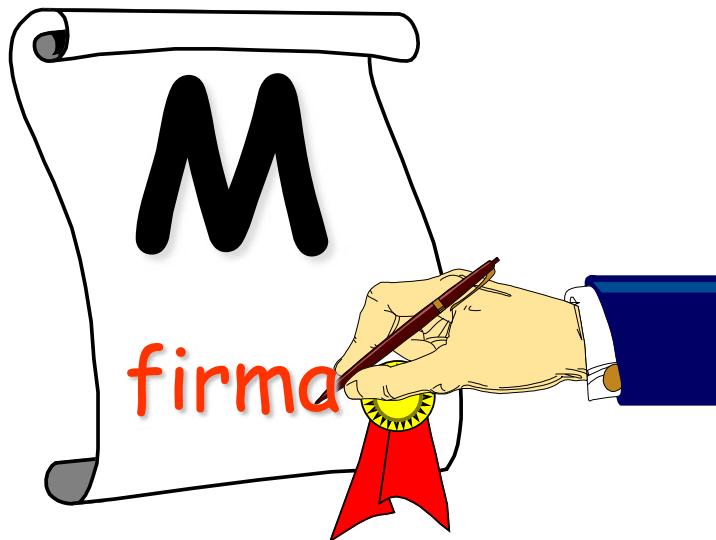
Firma Digitale



Equivalent alla firma
convenzionale

Soluzione naive:
incollare firma digitalizzata

Firma Digitale



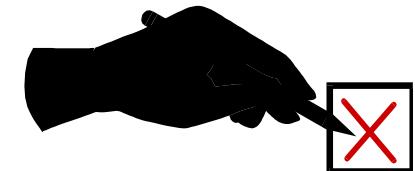
Equivalent alla firma
convenzionale

Soluzione naive:
incollare firma digitalizzata



Requisiti per la Firma Digitale

La firma digitale deve poter essere facilmente prodotta dal legittimo firmatario

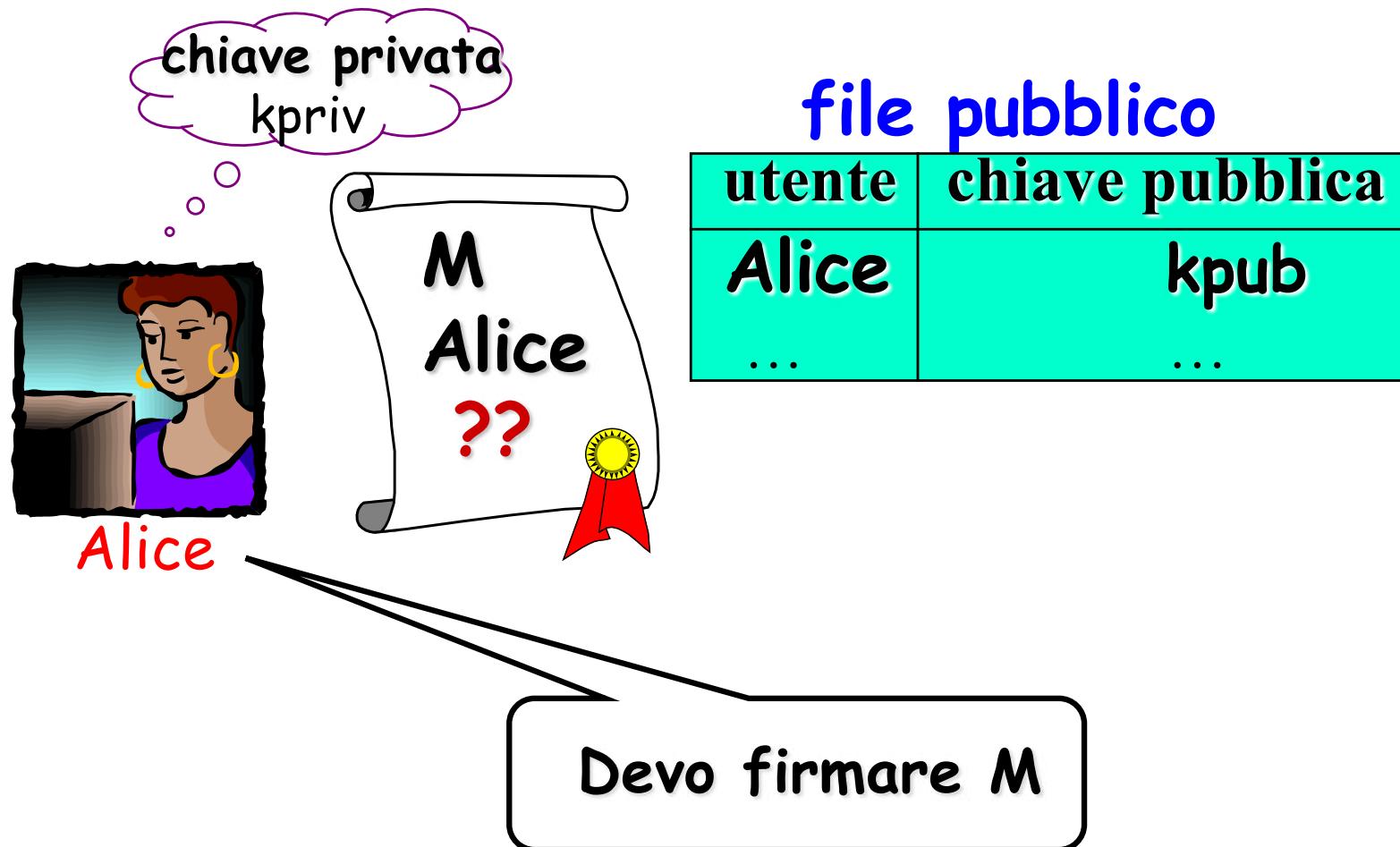


Nessun utente deve poter riprodurre la firma di altri

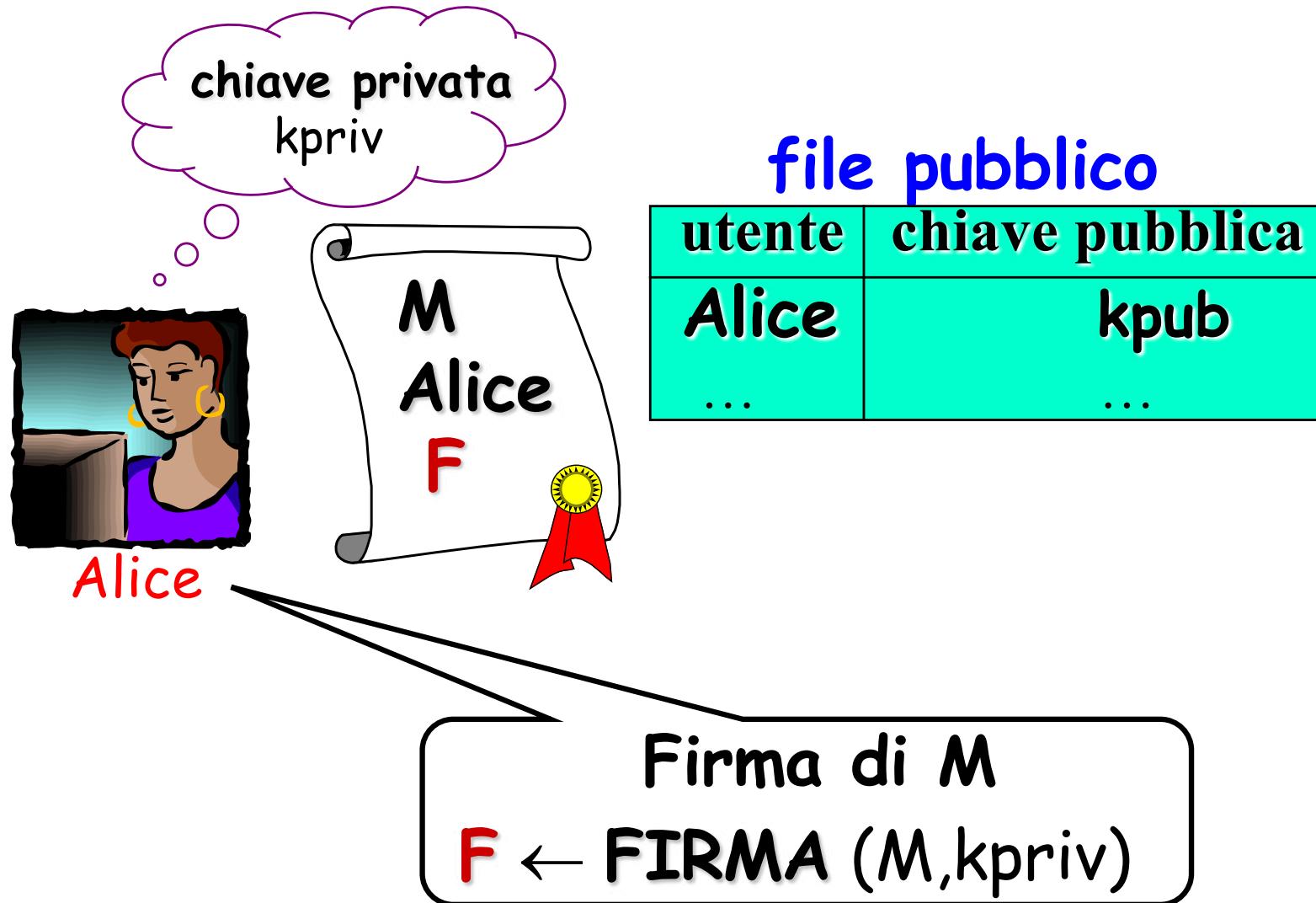
Chiunque può facilmente verificare una firma



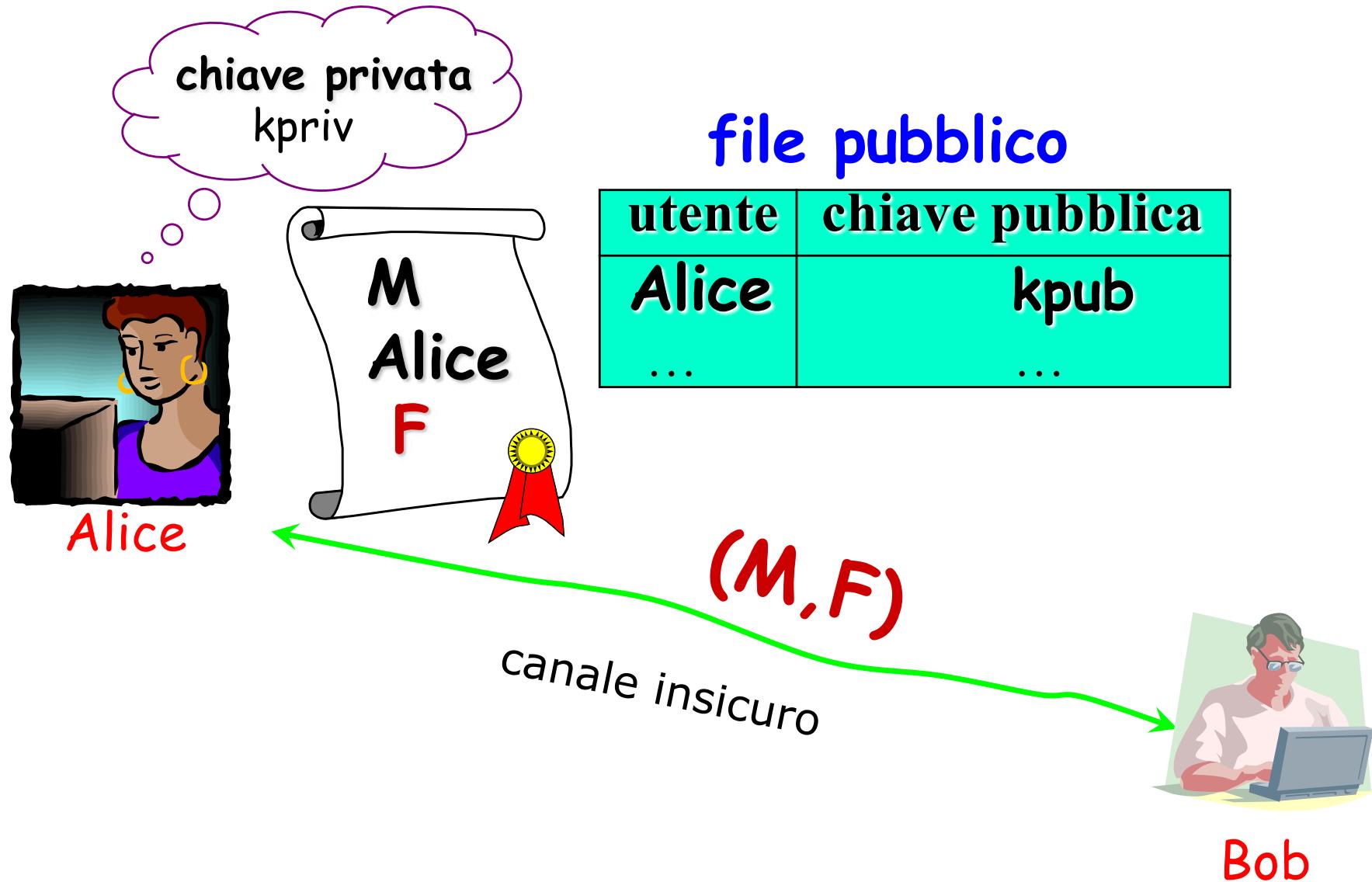
Firma digitale



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
-
- A diagram illustrating the relationship between various digital signature schemes. Five blue arrows originate from the list items above and point towards a light orange rectangular callout box. The box contains the text: "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

Homepage area pubblica, Università di Salerno

Safari utilizza una connessione a esse3web.unisa.it codificata.

La codifica con un certificato digitale mantiene private le informazioni quando vengono inviate al/dal sito web https://esse3web.unisa.it.

MENU

Area Strutturale

DA QUESTA PAGINA E' POSSIBILE ACCEDERE ALLA SEZIONE DI CUI ALDO A DESTRA, PER OTTENERE I DOCUMENTI DI CUI ALLA NOTA.

GLI STUDENTI CHE ACCEDONO A QUESTA PAGINA SONO IDENTIFICATI DA UN COLORE DIVERSO DA QUELLO DEGLI STUDENTI CHE SONO IDENTIFICATI DA UN COLORE DIVERSO.

I DOCENTI NON DEVONO RICORDARSI DI ACCEDERE ALLA SEZIONE DI CUI ALDO A DESTRA.

Home

DigiCert Assured ID Root CA
└ TERENA SSL CA 3
└ esse3web.unisa.it

esse3web.unisa.it

Emesso da: TERENA SSL CA 3
Scade: mercoledì 19 maggio 2021 02:00:00 Ora legale dell'Europa centrale
 Il certificato è valido

► Attendibilità

▼ Dettagli

Nome soggetto _____

Paese o regione IT
Località Fisciano
Società Università degli Studi di Salerno
Unità organizzativa unisa.it
Nome comune esse3web.unisa.it

Nome emittente _____

Paese o regione NL
Stato/Provincia Noord-Holland
Località Amsterdam
Società TERENA
Nome comune TERENA SSL CA 3

Numero di serie 07 2F 3A DC A6 FF A9 42 26 01 7C 24 C3 29 25 F0
Versione 3
Algoritmo firma SHA-256 con codifica RSA (1.2.840.113549.1.1.11)
Parametri Nessuno

Non valido prima di giovedì 14 febbraio 2019 01:00:00 Ora standard dell'Europa centrale
Non valido dopo mercoledì 19 maggio 2021 02:00:00 Ora legale dell'Europa centrale

Informazioni chiave pubblica _____

Algoritmo Codifica RSA (1.2.840.113549.1.1.1)
Parametri Nessuno

Chiave pubblica 256 byte: B1 2E F6 F3 4A B6 B8 0A E2 E5 43 4A 01 BB EF 38 BC AE 8F C3 5F 49 74
44 70 05 36 AE 6D DE 1B 18 EC 14 B8 4C 1B D9 44 18 BF 22 33 F2 7A 5C 21 B1 92
37 25 2E 0A BC 1F D3 C2 EC AB B8 14 9C E8 90 B5 31 58 2D D3 30 63 18 31 29 0C
FA CD E8 EE B0 D3 14 E5 7B F8 72 5C 01 61 97 65 A3 23 BB 6F 0D 9D 4A 3D 29

?

Nascondi certificato

OK

NE' DAL MENU' IN ALTO A DESTRA

'LOGIN' DAL MENU' IN ALTO A DESTRA

INFORMATIVA UTILIZZO COOKIE | © CINECA



UNIVERSITÀ



Safari utilizza una connessione a esse3web.unisa.it codificata.

La codifica con un certificato digitale mantiene private le informazioni quando vengono inviate al/dal sito web
<https://esse3web.unisa.it>

MENU

Area Strutturale

DA QUESTA PAGINA E' POSSIBILE:

GLI STUDENTI CHE ACCEDONO AL SITO DA QUESTA PAGINA SONO AUTORIZZATI A

GLI STUDENTI CHE SONO CONNETTI ALLA RETE SONO AUTORIZZATI A

I DOCENTI NON DEVONO FARLO MA SONO AUTORIZZATI A

ALTO A DESTRA

Home

DigiCert Assured ID Root CA

TERENA SSL CA 3

esse3web.unisa.it

TERENA SSL CA 3
Autorità di certificazione intermedia
Scade: lunedì 18 novembre 2024 13:00:00 Ora standard dell'Europa centrale
Il certificato è valido

Attendibilità

Dettagli

Nome soggetto _____
Paese o regione NL
Stato/Provincia Noord-Holland
Località Amsterdam
Società TERENA
Nome comune TERENA SSL CA 3

Nome emittente _____
Paese o regione US
Società DigiCert Inc
Unità organizzativa www.digicert.com
Nome comune DigiCert Assured ID Root CA

Numero di serie 08 70 BC C5 AF 3F DB 95 9A 91 CB 6A EE EF E4 65
Versione 3
Algoritmo firma SHA-256 con codifica RSA (1.2.840.113549.1.1.11)
Parametri Nessuno

Non valido prima di martedì 18 novembre 2014 13:00:00 Ora standard dell'Europa centrale
Non valido dopo lunedì 18 novembre 2024 13:00:00 Ora standard dell'Europa centrale

Informazioni chiave pubblica

Algoritmo Codifica RSA (1.2.840.113549.1.1.1)
Parametri Nessuno
Chiave pubblica 256 byte: C5 76 0F 0F D9 43 29 3B ...
Esponente 65537
Dimensione chiave 2.048 bit
Utilizzo chiave Verifica

? Nascondi certificato OK

NE' DAL MENU' IN ALTO A

STRADA

'LOGIN' DAL MENU' IN

mativa utilizzo cookie | © CINECA



UNIVERSITÀ



Safari utilizza una connessione a esse3web.unisa.it codificata.

La codifica con un certificato digitale mantiene private le informazioni quando vengono inviate al/dal sito web
https://esse3web.unisa.it.≡
MENU

Area Strutturale

DA QUESTA PAGINA E' POSSIBILE:

GLI STUDENTI CHE ACCEDONO DA QUESTA PAGINA SONO A DESTRA, PER OTTENERE I CERTIFICATI DI CONSEGUIMENTO

GLI STUDENTI CHE SONO CONSIDERATI COME AUTORIZZATI SONO A DESTRA

I DOCENTI NON DEVONO FARE NIENTE, SONO A DESTRA, ALCUNI SONO A SINISTRA, ALCUNI SONO A ALTO A DESTRA

Home

DigiCert Assured ID Root CA

TERENA SSL CA 3

esse3web.unisa.it

DigiCert Assured ID Root CA
Autorità di certificazione principale
Scade: lunedì 10 novembre 2031 01:00:00 Ora standard dell'Europa centrale
 Il certificato è valido

► Attendibilità

▼ Dettagli

Nome soggetto _____
Paese o regione US
Società DigiCert Inc
Unità organizzativa www.digicert.com
Nome comune DigiCert Assured ID Root CA

Nome emittente _____
Paese o regione US
Società DigiCert Inc
Unità organizzativa www.digicert.com
Nome comune DigiCert Assured ID Root CA

Numero di serie 0C E7 E0 E5 17 D8 46 FE 8F E5 60 FC 1B F0 30 39
Versione 3
Algoritmo firma SHA-1 con codifica RSA (1.2.840.113549.1.1.5)
Parametri Nessuno

Non valido prima di venerdì 10 novembre 2006 01:00:00 Ora standard dell'Europa centrale
Non valido dopo lunedì 10 novembre 2031 01:00:00 Ora standard dell'Europa centrale

Informazioni chiave pubblica
Algoritmo Codifica RSA (1.2.840.113549.1.1.1)
Parametri Nessuno
Chiave pubblica 256 byte: AD 0E 15 CE E4 43 80 5C ...
Esponente 65537
Dimensione chiave 2.048 bit
Utilizzo chiave Verifica

Firma 256 byte: A2 0F BC DF E2 FD F0 F3

? Nascondi certificato OK

NE' DAL MENU' IN ALTO A SINISTRA

'LOGIN' DAL MENU' IN ALTO A SINISTRA

Informativa utilizzo cookie | © CINECA

Chain of trust

End-entity Certificate

Owner's name
Owner's public key
Issuer's (CA's) name
Issuer's signature

reference

Intermediate Certificate

Owner's (CA's) name
Owner's public key
Issuer's (root CA's) name
Issuer's signature

sign

reference

Root CA's name
Root CA's public key
Root CA's signature

sign

self-sign

Root Certificate

Quanti certificati?

Per esempio, la sola Let's Encrypt:



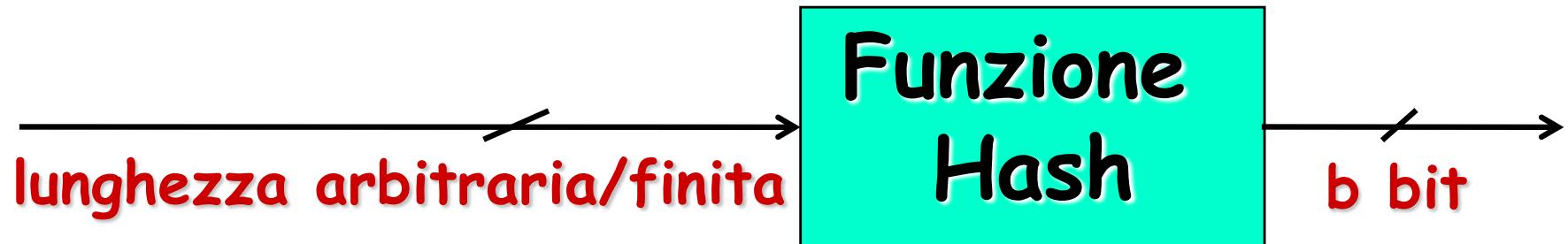
Let's Encrypt Has Issued a Billion Certificates

Feb 27, 2020 • Josh Aas and Sarah Gran

We issued our billionth certificate on February 27, 2020. We're going to use this big round number as an opportunity to reflect on what has changed for us, and for the Internet, leading up to this event. In particular, we want to talk about what has happened since the last time we talked about a big round number of certificates - [one hundred million](#).

One thing that's different now is that the Web is much more encrypted than it was. In June of 2017 approximately 58% of page loads used HTTPS globally, 64% in the United States. Today 81% of page loads use HTTPS globally, and we're at 91% in the United States! This is an incredible achievement. That's a lot more privacy and security for everybody.

Funzioni Hash



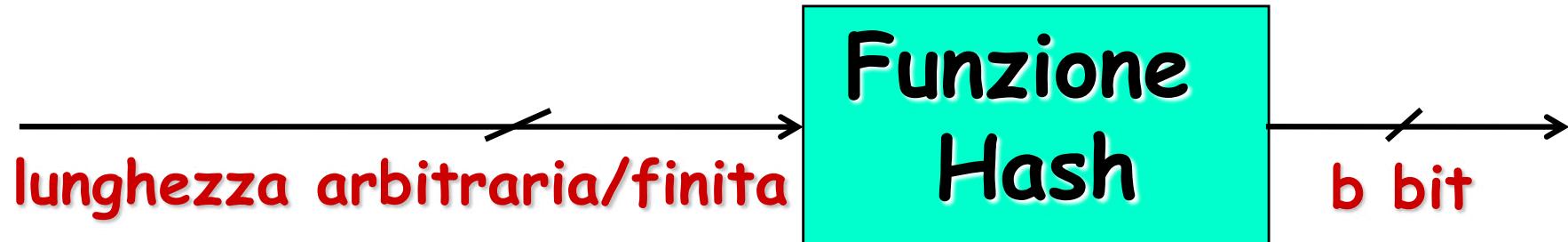
Idea alla base:

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

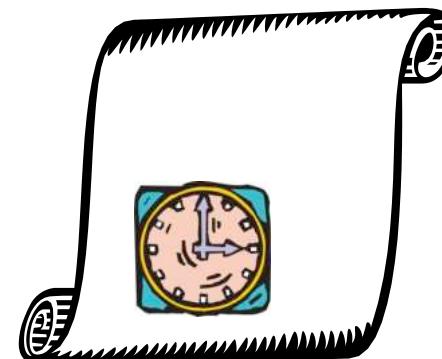
Uso delle funzioni hash

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

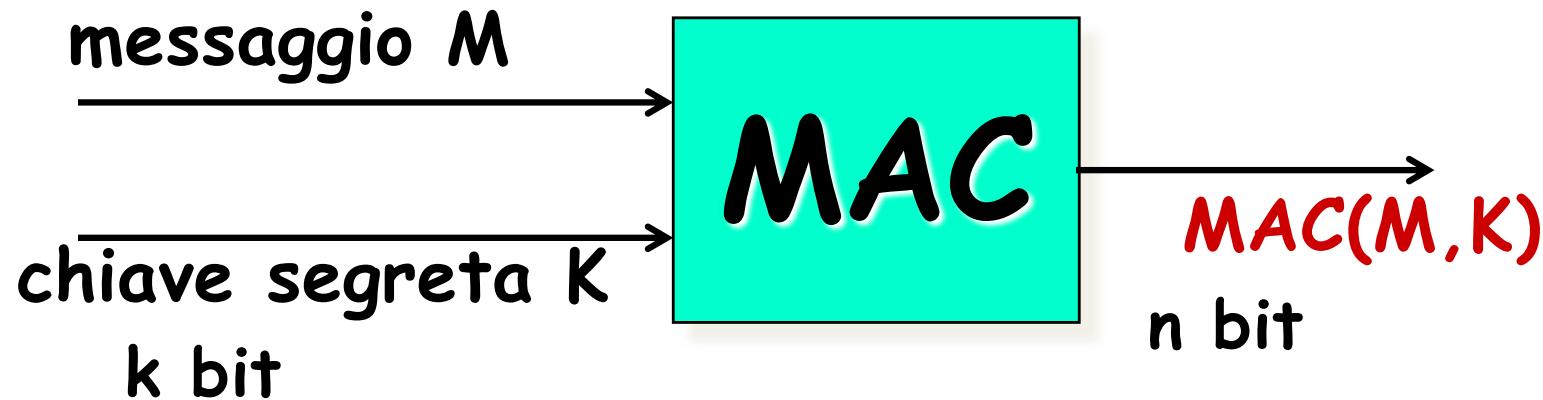
Per controllare se il file è stato successivamente
modificato, calcolo $h(M')$ e verifico se $H = h(M')$

$h(M)$ è l'impronta digitale del file

Assicura se un file è stato modificato!



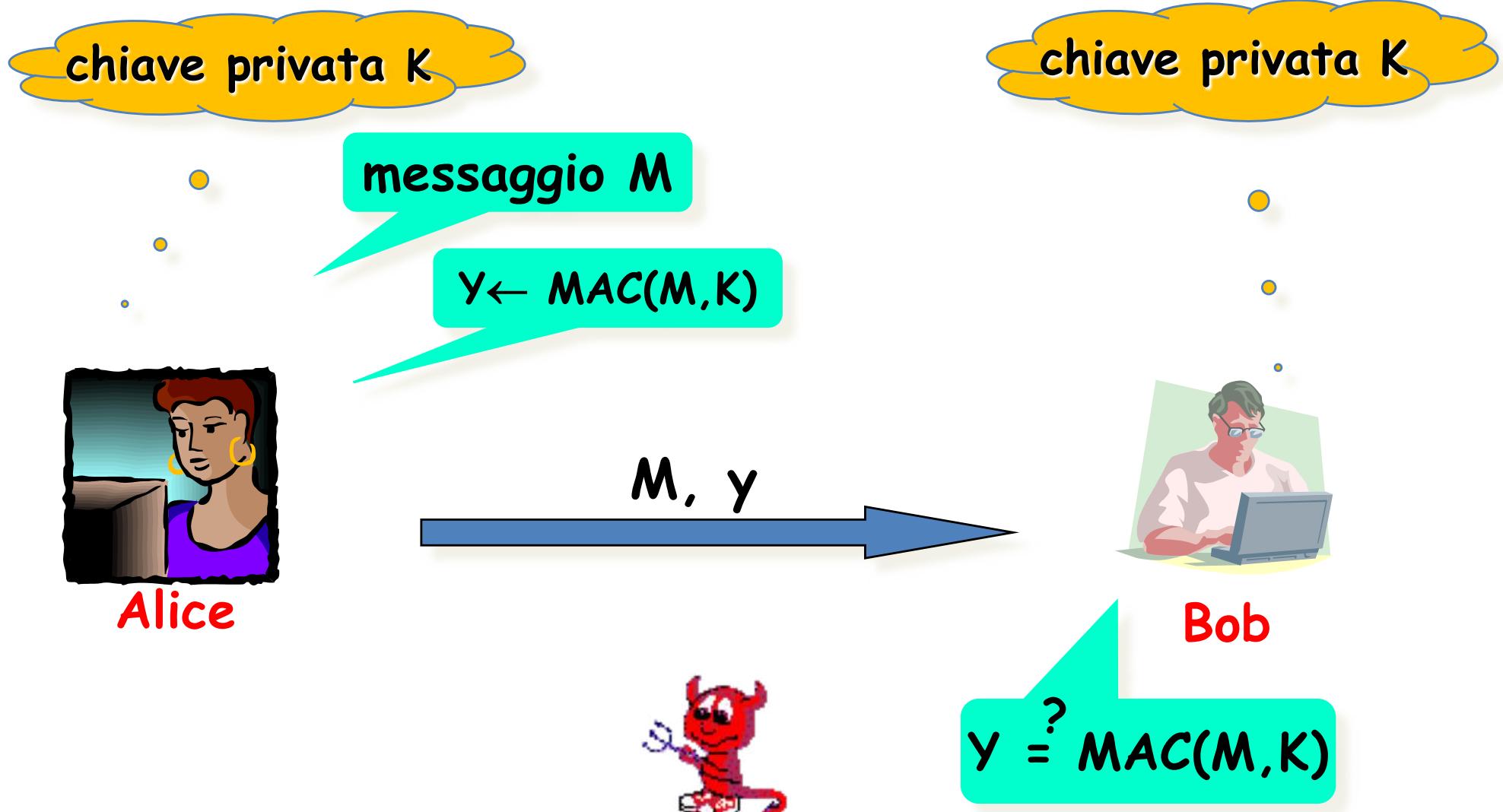
Message Authentication Code (MAC)



Applicazioni

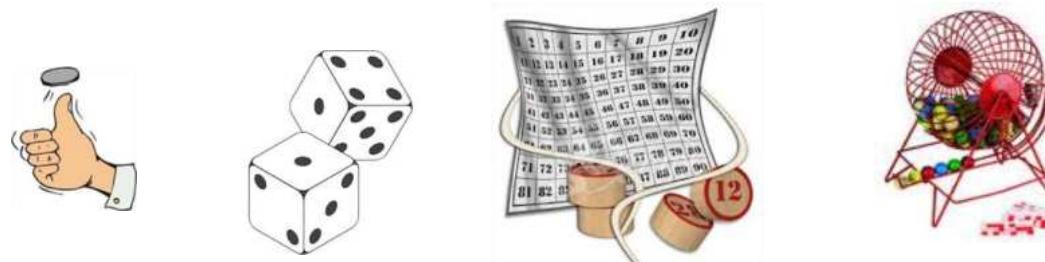
- Autenticità del messaggio M
- Integrità del messaggio M

Utilizzo MAC



Casualità e pseudocausalità

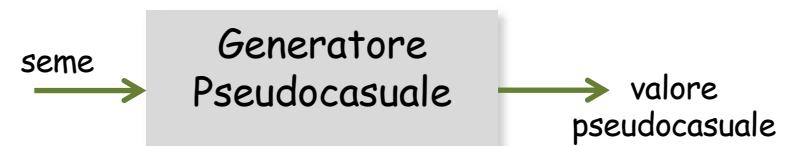
➤ Casuale



➤ Pseudocasuale

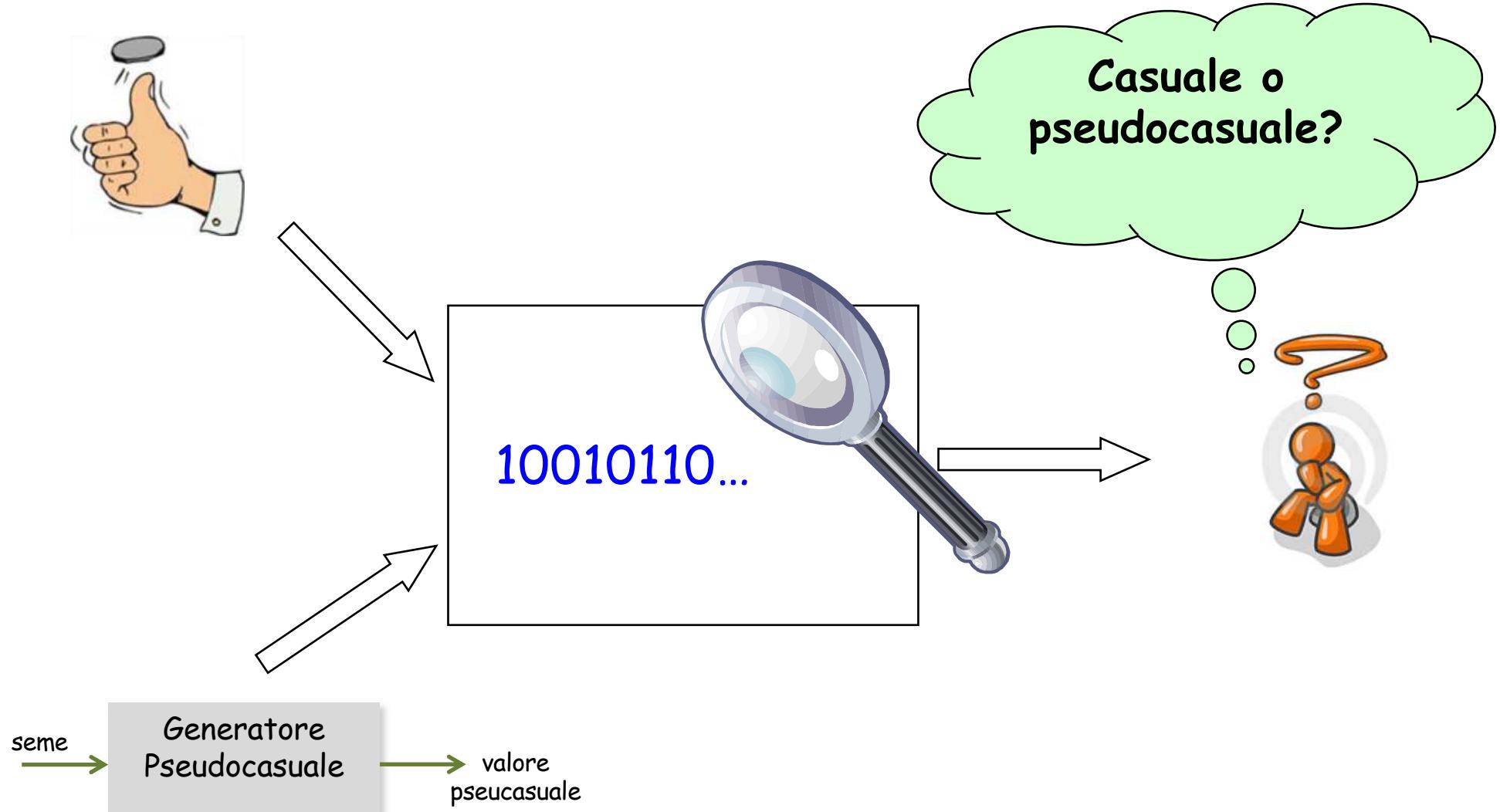
Generazione deterministica da un seme iniziale

Sembra casuale ma non lo è



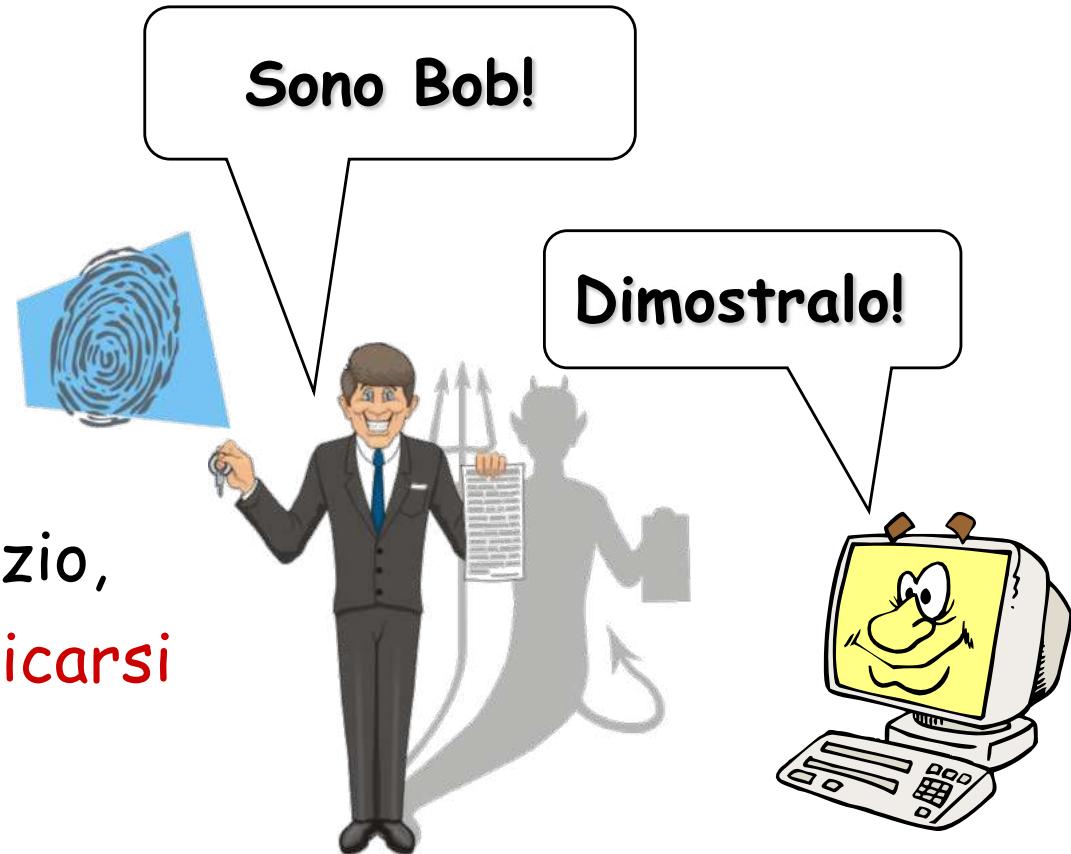
Sicurezza di un generatore pseudocasuale

Indistinguibilità



Autenticazione utente

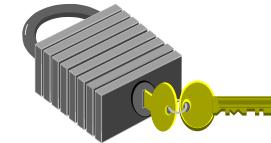
Per utilizzare un servizio,
un utente deve **autenticarsi**



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



Autenticazione a due fattori



Sicurezza IP e WWW

- La sicurezza sul Web ricopre un ruolo importantissimo
- Oggigiorno oltre l'80% 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 l'80% del traffico Web è cifrato mediante il protocollo HTTPS
 - Come è emerso dall'analisi  della metrica dei due browser più diffusi
 - Google Chrome
 - Mozilla FireFox
 - Questo risultato è stato ottenuto scelta di utilizzare i principali social network.



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



Sicurezza IP e WWW

(Telemetria Mozilla Firefox)



Percentuale di pagine caricate con HTTPS
Telemetria Mozilla Firefox (febbraio 2020)



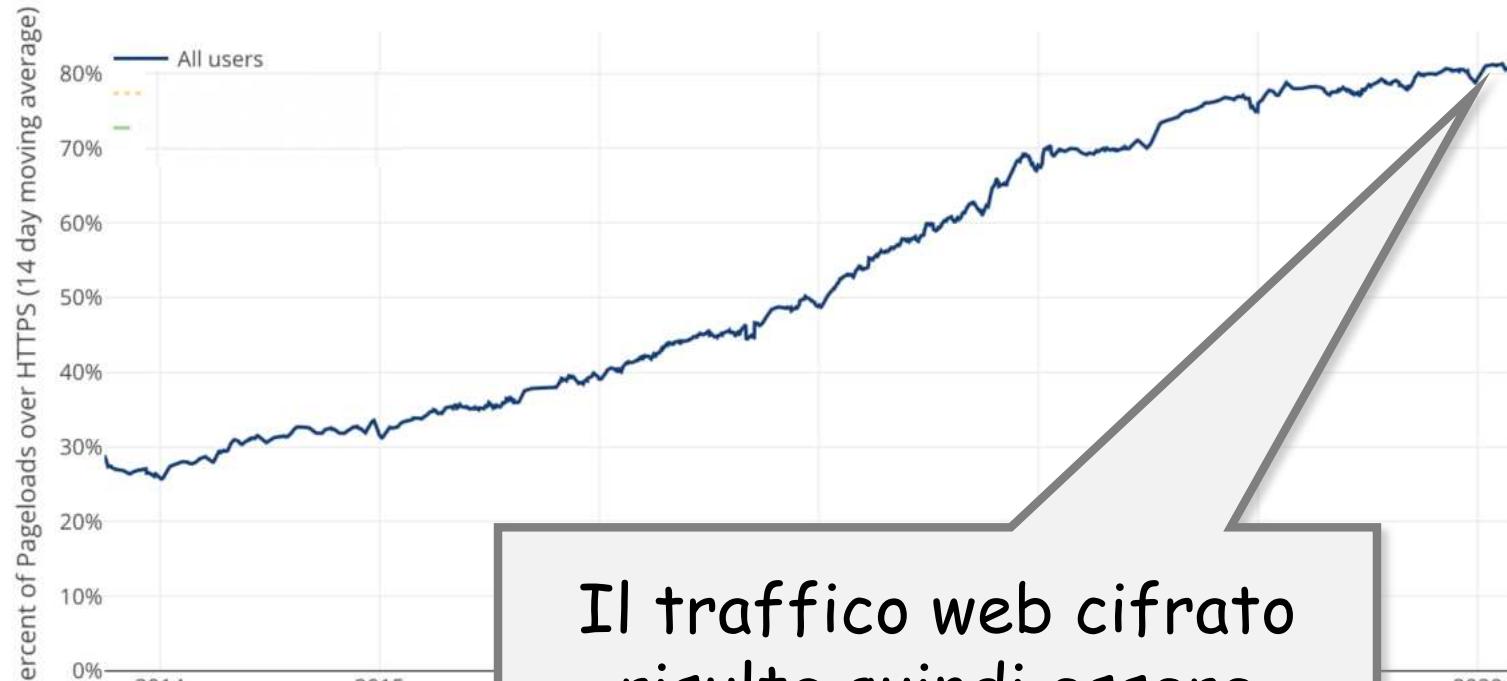
Fonte: <https://letsencrypt.org/stats/>
<https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web>

Sicurezza IP e WWW

(Telemetria Mozilla Firefox)



Percentuale di pagine caricate con HTTPS
Telemetria Mozilla Firefox (febbraio 2020)



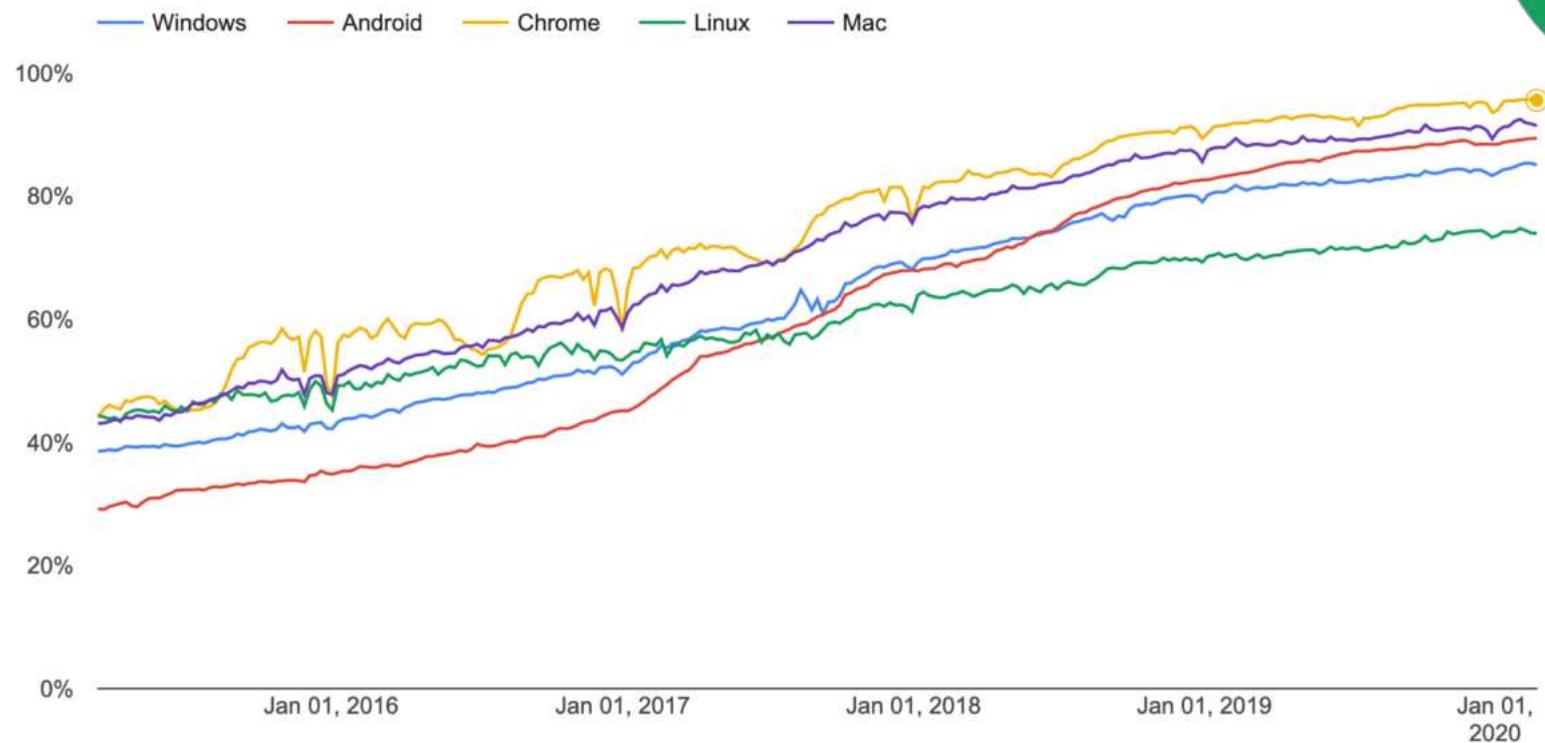
Il traffico web cifrato
risulta quindi essere
superiore all'80%

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 (1 gennaio 2020)
Telemetria Google Chrome su piattaforme

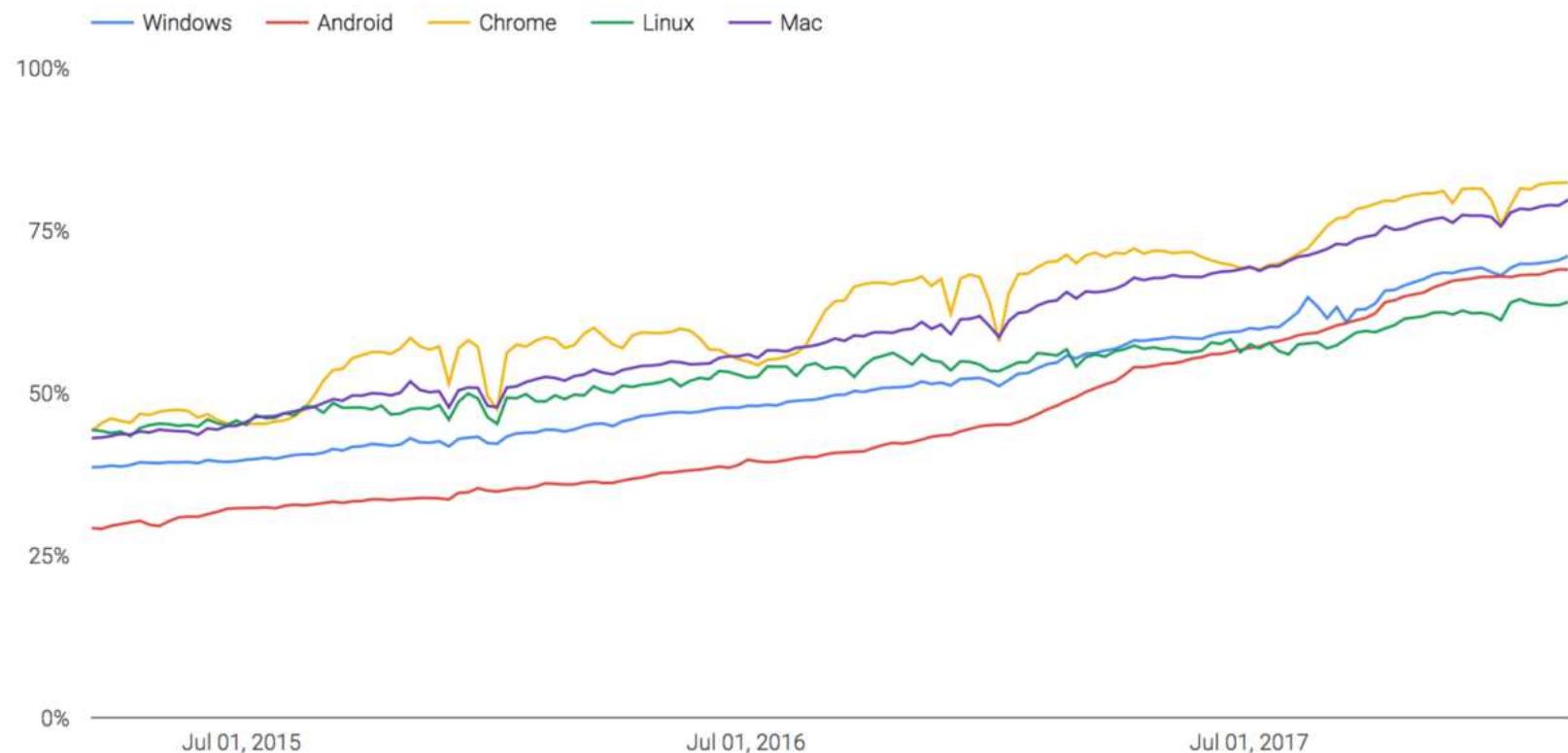


<https://transparencyreport.google.com/https/overview?hl=en>

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 panel has a title "Avanzate" and a sub-navigation bar with tabs: Generale, Condivisione dati (which is selected and highlighted with an orange bar), Rete, Aggiornamenti, and Certificati. The "Condivisione dati" tab is active.

Attiva analisi integrità di Firefox

Analizza le prestazioni del browser e condividi informazioni con Mozilla sullo stato di integrità del software [Ulteriori informazioni](#)

Condividi ulteriori dati (telemetria)

Condividi con Mozilla informazioni relative a prestazioni, utilizzo, hardware e personalizzazioni del browser per contribuire al miglioramento di Firefox [Ulteriori informazioni](#)

Consenti a Firefox di inviare automaticamente le segnalazioni di arresto anomalo in sospeso

Le segnalazioni di arresto anomalo permettono a Mozilla di risolvere i problemi del browser e renderlo più stabile e sicuro [Ulteriori informazioni](#)

Abilitare Telemetria su Google Chrome

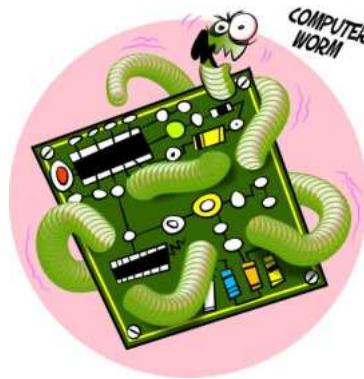
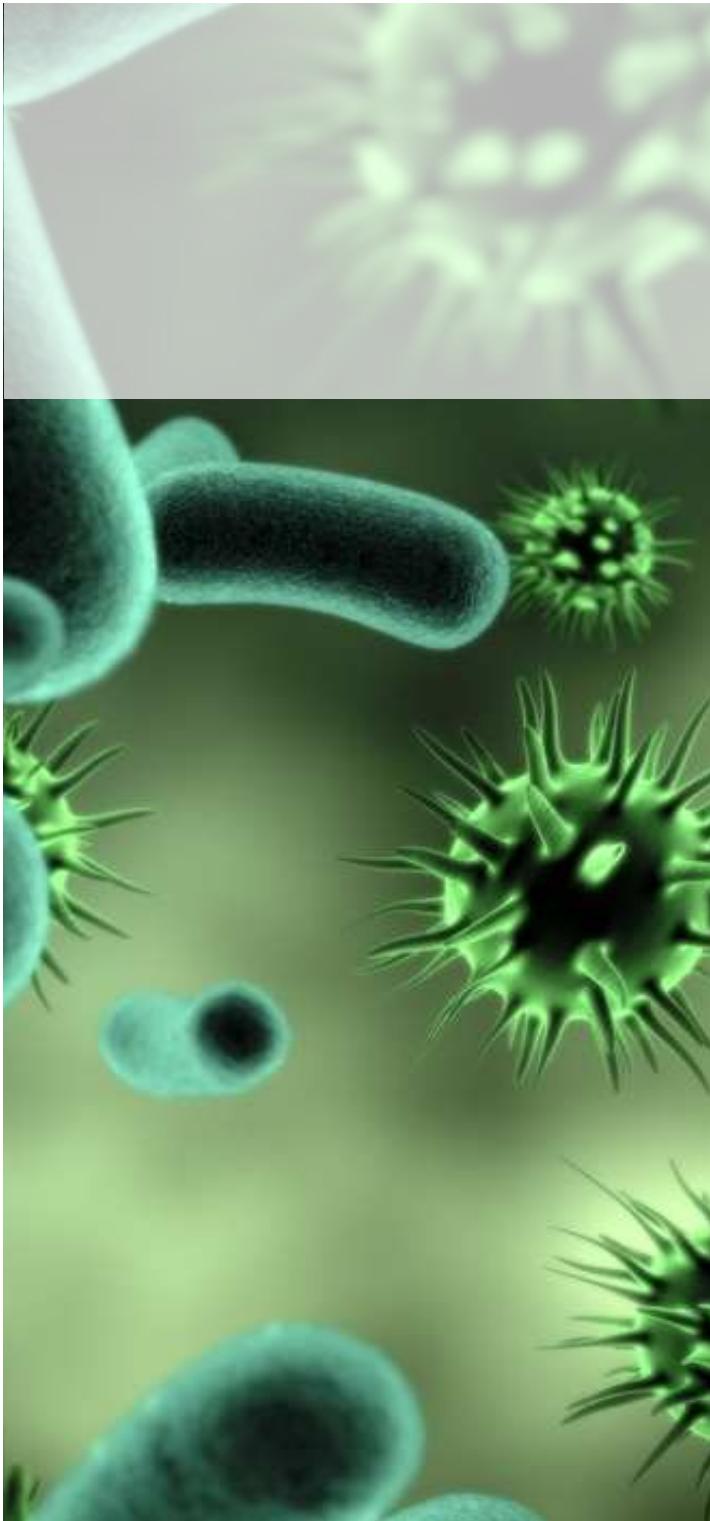
Privacy

[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



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

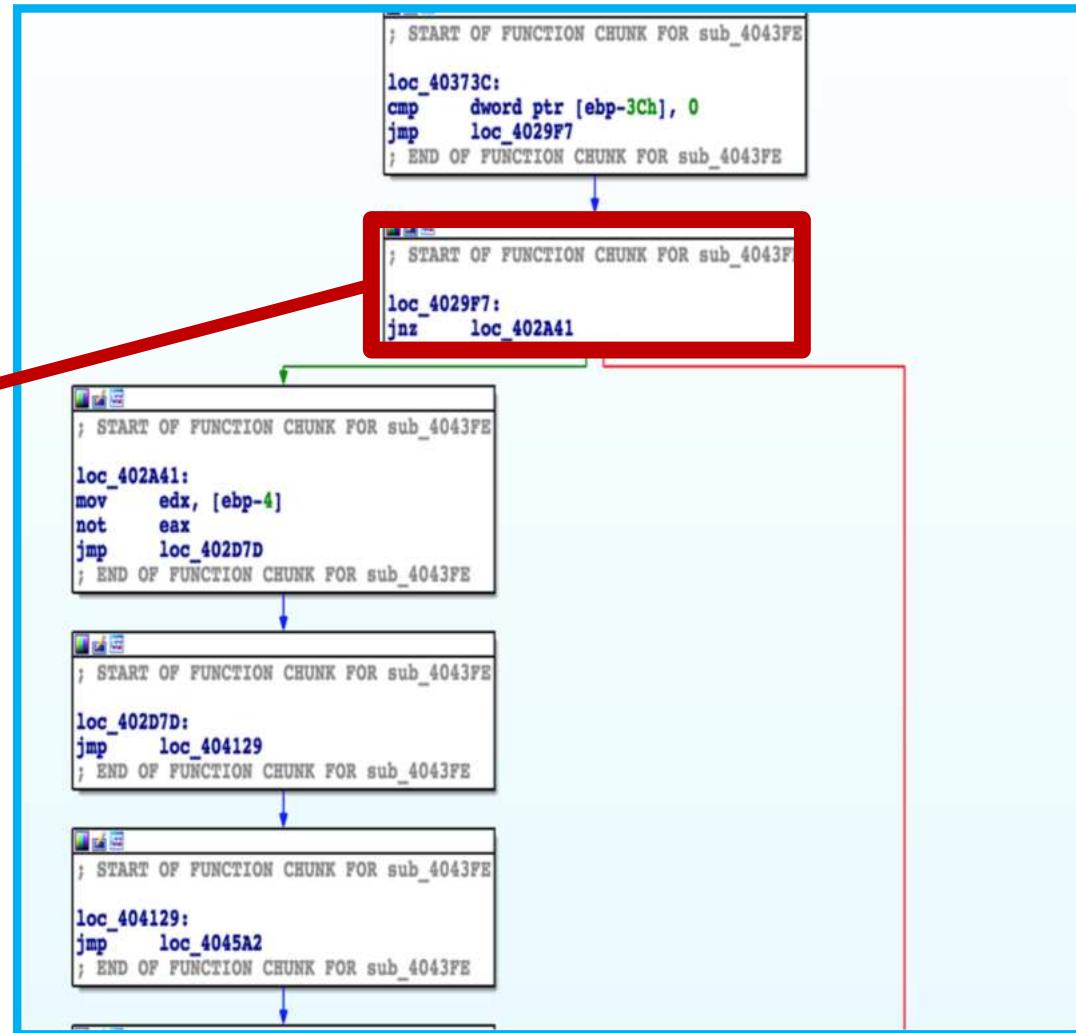
- I danni di BlackEnergy
- Regione Ivano-Frankivsk, Ucraina, Dicembre 2015
 - Assenza di fornitura elettrica per 6 ore
 - La causa è un cyber-attacco
 - Dai rapporti successivi, viene individuata la causa: un malware
 - Il malware definito BlackEnergy sembra aver infettato i sistemi della centrale
 -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

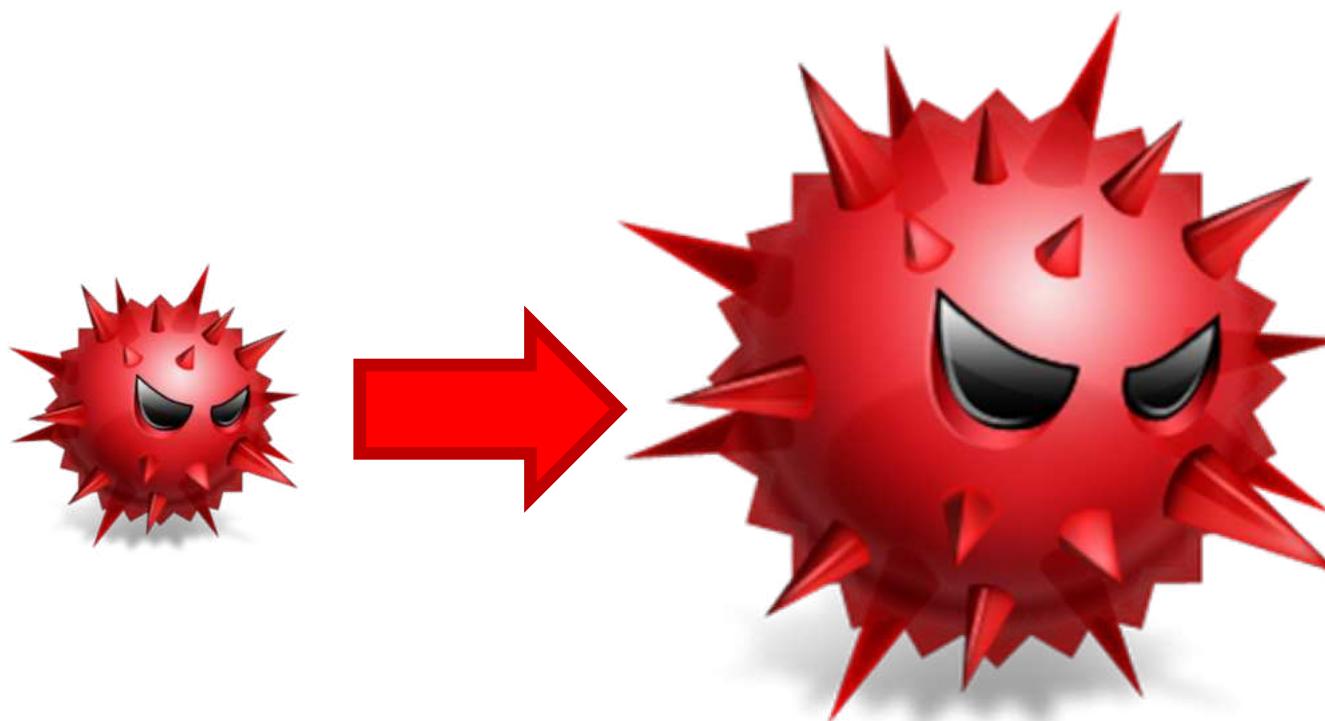


Malware, Dispositivi Mobile e Analisi

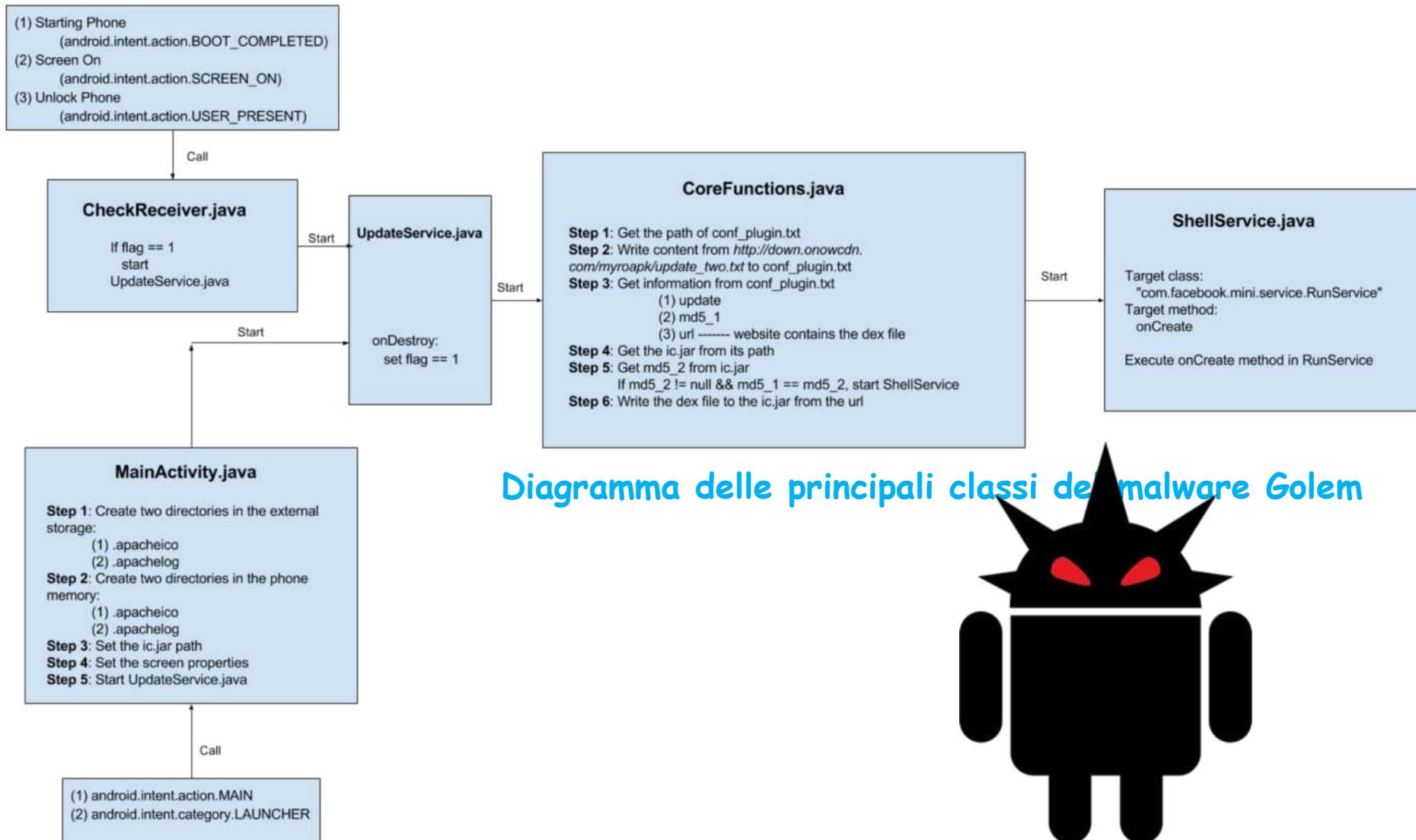
- I malware per dispositivi mobile (smartphone, tablet, etc.)
 - Hanno una struttura ed una diffusione diversa rispetto ai malware per piattaforme desktop
- Con il costante incremento delle tecnologie e l'enorme diffusione globale dei dispositivi mobile
 - Si è verificato un significativo aumento anche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



Domande?

