



Operazione Rif PA **2021-15946/RER**

approvata con DGR **1263/2021 del 02/08/2021**

Progetto n. **1** - Edizione n. **1**

TECNICO PER LA PROGETTAZIONE E LO SVILUPPO DI APPLICAZIONI INFORMATICHE

**MODULO: N. 6 Titolo: AMMINISTRAZIONE DI SISTEMI SERVER
DURATA : 34 ORE DOCENTE: MARCO PRANDINI**

Introduzione alla sicurezza



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Introduzione alla Sicurezza Informatica

Marco Prandini

Dipartimento di Informatica – Scienza e Ingegneria

Introduzione

■ Inquadramento della materia

- Perché interessarsi alla sicurezza informatica?
- Elementi di base: minacce, vulnerabilità, exploit e rischio
- Tipologie di attacco e loro conseguenze
- Panoramica delle metodologie di difesa

La sicurezza informatica ci riguarda?

■ Sì, ben prima che come professionisti. Nelle nostre vite

- Infrastrutture critiche per la “civiltà”
- Sistemi di comunicazione ed elaborazione delle informazioni
- Archivi di informazioni personali

sono tutti elementi *informatizzati* ormai irrinunciabili e in molti casi, se **danneggiati**, insostituibili (in assoluto o in tempo utile per evitare conseguenze gravi)

■ Sicurezza informatica è tutto ciò che ha a che fare col contrasto di **azioni deliberate** che provochino danni

- Termini diversi hanno sfumature specifiche, ma spesso sono usati “popolarmente” in modo intercambiabile: sicurezza dell’informazione, IT security, cybersecurity, ...
- Useremo sicurezza nel senso del termine inglese *security* ricordando che in italiano significa anche contrasto di eventi accidentali che provochino danni (in inglese tradotto *safety*)

Impatto sociale della cyber(in)security

Woman dies during a ransomware attack on a German hospital



The Verge, Sep 17, 2020



2000: Maroochy waste management

...

2008: Refahiye pipeline

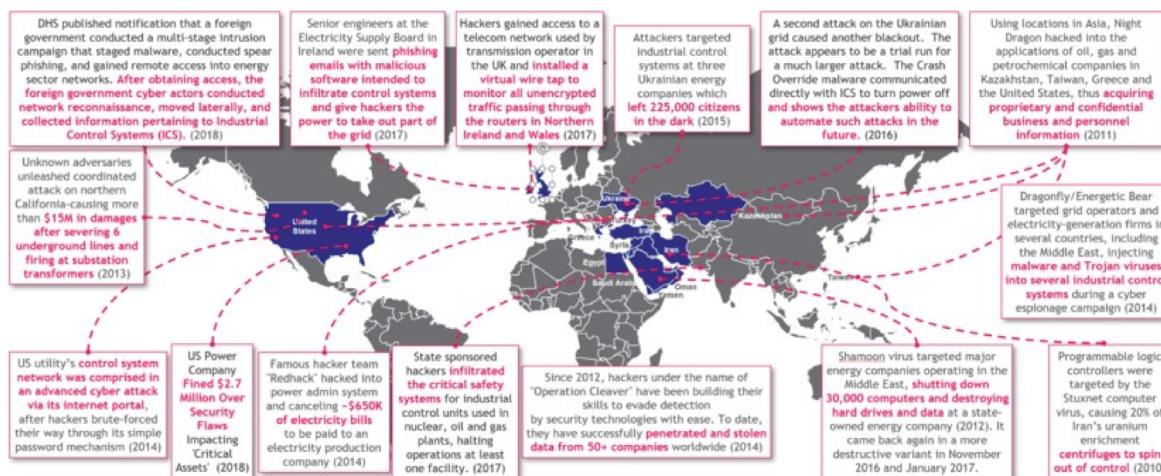
...

2018: Saudi Chemical Company

...

2020: Natanz “stuxnet 2”

Hackers are causing blackouts. It's time to boost our cyber resilience. World Economic Forum, Mar 27, 2019



Impatto economico della cyber(in)security

- Se il cybercrime fosse una nazione, farebbe parte del G3, con un GDP>10T\$ previsto per il 2025
- Un business criminale in crescita
 - Più lucrativo del mercato mondiale della droga
 - Più dannoso di tutti i disastri naturali cumulati
- Un modello criminale attrattivo
 - Utilizzabile in innumerevoli settori
 - A basso rischio (0,05%) di individuazione e prosecuzione legale
- Sono richiesti investimenti ingenti per la difesa
 - Dal 2004 al 2017 il mercato è cresciuto di 35 volte
 - Spesa stimata nel quadriennio 2018-2021: 1T\$



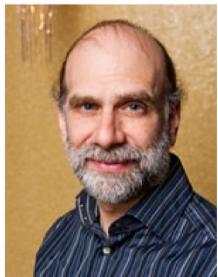
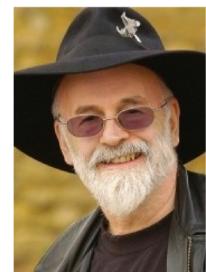
Il rischio cyber

- Affrontare i problemi di sicurezza informatica è sostanzialmente un esercizio di **gestione del rischio**
"il potenziale danno immateriale, perdita economica, o distruzione di risorse che risulterebbe da un evento (malevolo)"
- Semplificando in modo estremo:
RISCHIO = PROBABILITÀ x IMPATTO
es. se nell'arco di un anno c'è una probabilità del 4% di subire un danno di 15.000€ dovuto a un'azione malevola, il rischio è pari a 600€/anno
- Per gestire il rischio dobbiamo conoscerlo
 - valutare le probabilità di ogni evento potenzialmente dannoso
 - quantificare l'impatto di ogni possibile azione malevola
- Per mitigare il rischio si progettano e implementano contromisure (che devono essere convenienti!)
 - bisogna saperne valutare l'efficacia, in termini di riduzione della probabilità degli eventi dannosi e/o del loro impatto

Detto così sembra facile...

“Progress just means bad things happen faster.”

– Terry Pratchett (from *Witches Abroad*)

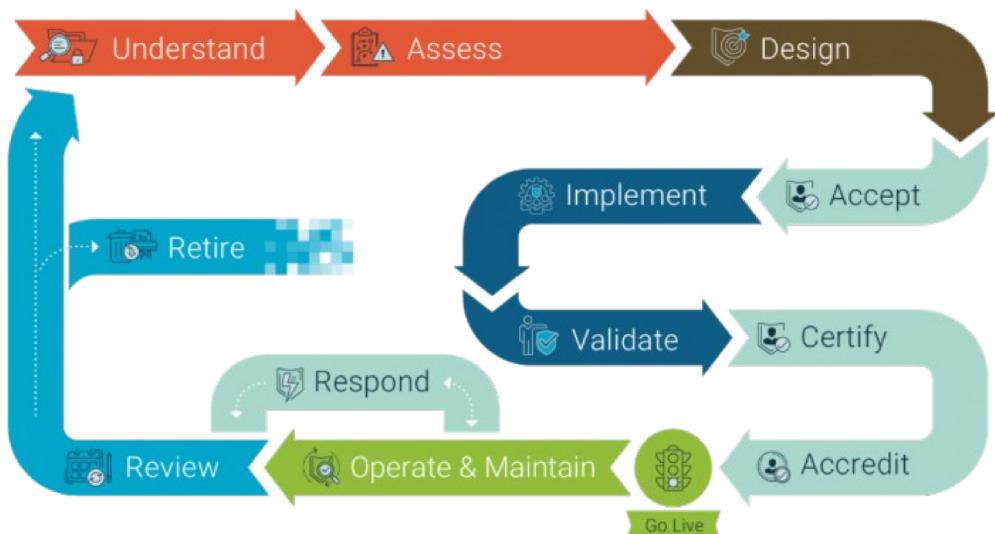


“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.”

– Bruce Schneier

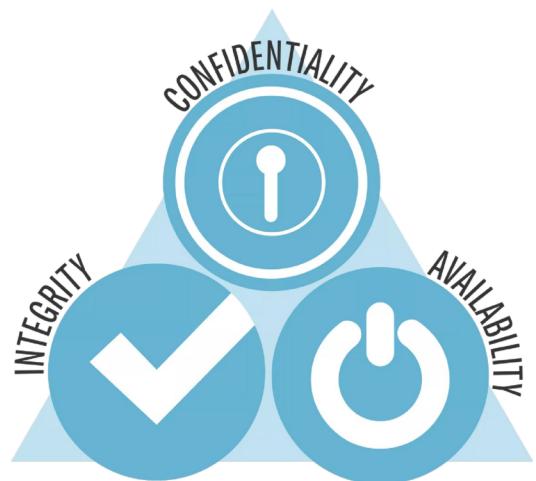
Un processo continuo

Sicurezza non è valutare la situazione presente e comprare un **prodotto**, bensì definire un **processo** per tenere traccia delle continue evoluzioni dei rischi e dell'efficacia delle contromisure



Proprietà di sicurezza

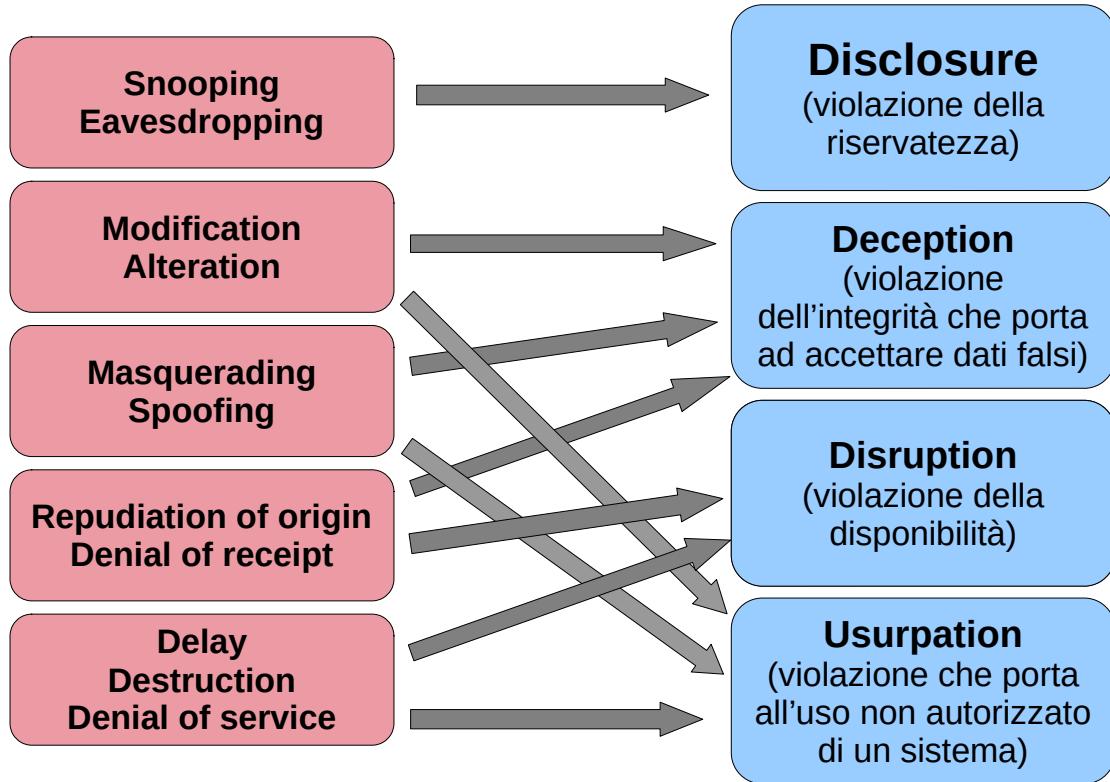
- La sicurezza di un sistema può essere scomposta in tre proprietà chiave, riassunte dalla sigla **CIA**
- Confidentiality (riservatezza)
 - Mantenere inaccessibili dati, o proprietà di un sistema, a chi non sia autorizzato a conoscerli
- Integrity (integrità)
 - Poder garantire che il contenuto e/o l'origine di un dato corrispondano a quanto si ritiene corretto
- Availability (disponibilità)
 - Poder garantire la possibilità effettiva di accedere a dati e servizi quando necessario



Le minacce e gli attacchi

- **Minaccia (threat)**: una condizione che potenzialmente può compromettere una o più delle proprietà di sicurezza
 - Esiste indipendentemente dal fatto che venga concretizzata
 - **Attacco (attack)**: l'azione che porta al concretizzarsi di una minaccia
 - **Attaccante (attacker)**: l'entità che sferra l'attacco
- Le minacce sono indissolubilmente legate alle intenzioni dei potenziali attaccanti
 - Script kiddies
 - Criminali comuni
 - Insider disonesti e impiegati vendicativi
 - Reporter
 - Ricercatori
 - Attivisti
 - Criminali organizzati
 - Spie industriali
 - Governi ed eserciti

Tipologie di attacchi e minacce



Politiche e meccanismi

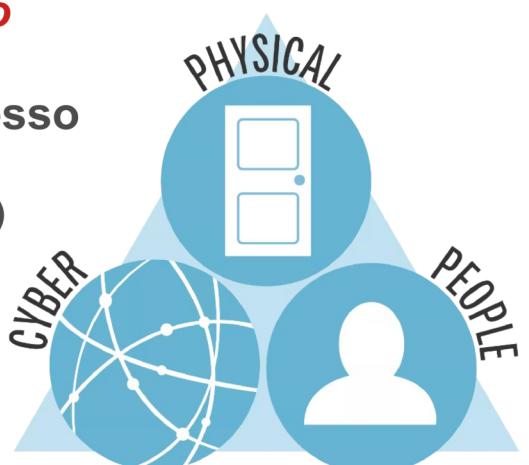
- Una **politica di sicurezza** (*security policy*) è la dichiarazione di ciò che è consentito o proibito fare
- Un **meccanismo di sicurezza** (*security mechanism*) è un metodo, uno strumento o una procedura per far rispettare una politica di sicurezza
- Non sono necessariamente tecnici, anzi molto spesso, tra i più importanti, ci sono comportamenti e regole di interazione tra persone

Obiettivi delle politiche e dei meccanismi

- Le politiche dichiarano qual è il fine della sicurezza
- I meccanismi specificano il mezzo per contrastare gli attacchi, e possono combinare diverse strategie:
 - **Prevenzione (prevention)**: l'attacco deve fallire
 - Meccanismi invasivi
 - Implementazione inalterabile e non aggirabile
 - **Rilevazione (detection)**: l'attacco potrebbe avere successo ma deve essere notato e riportato
 - Inefficace rispetto ad alcune minacce, es. disclosure
 - **Reazione (response)**: l'attacco rilevato viene mitigato per ridurre la gravità o l'estensione del danno
 - **Ripristino (recovery)**: le conseguenze dell'attacco vengono ridotte o azzerate, ripristinando le proprietà di sicurezza violate

Superficie di attacco

- Politiche e meccanismi si applicano a ogni interazione del sistema col mondo esterno (o tra sottosistemi)
- Ogni modo reso accessibile a un attaccante per stimolare un'interazione è un **vettore di attacco**
- Ogni vettore può essere realizzato combinando uno o più canali di accesso
 - Fisico
 - “Cyber” (accesso remoto via cavo o wireless)
 - Umano
- L'insieme dei vettori costituisce la superficie di attacco



Vulnerabilità ed exploit

- Se le politiche e i meccanismi di protezione di un sistema fossero perfetti, le minacce non potrebbero concretizzarsi
 - Neutralizzano i vettori di attacco
- Gli attacchi hanno successo se esistono errori
 - Nell'individuazione della superficie di attacco (porosità – un vettore esiste là dove non dovrebbe)
 - Nella definizione di una politica o nell'implementazione di un meccanismo (**vulnerabilità / vulnerability**)
 - Può essere strutturale nell'hardware o software
 - Puo dipendere dalla configurazione
 - Può dipendere da un uso scorretto
- Exploit
 - Uno strumento per trarre vantaggio da una vulnerabilità concretizzando una minaccia
 - Tecnico (cracking)
 - Umano (social engineering)

Qualche esempio di vulnerabilità

- Uno switch propaga pacchetti a destinatari non designati se la tabella di switching è satura (vincolo hardware)
- Un router accetta qualsiasi annuncio gli pervenga riguardante la topologia della rete (caratteristica intrinseca del protocollo)
- Un utente clicca un link di un messaggio non verificando la fonte (errore umano di applicazione di una procedura)
- Un processo non controlla prima di sovrascrivere un'area di memoria che non gli appartiene (errore di implementazione del software)
- Un processo interpreta sequenze di byte come comandi anche se dovrebbero essere considerate puri dati (errore di progetto del software)
- Un computer che gestisce dati riservati può avere le porte USB abilitate (errore di definizione della politica di sicurezza)

I vettori umani, fisici e software che permettono di accedere a un computer sono normalmente usati per installare *malware*

- Worm
- Spyware
- Ransomware
- Trojan horse

Cybersecurity Kill Chain

Lockheed-Martin, 2011

Un modello per descrivere le fasi di un attacco



MITRE ATT&CK

Una base di conoscenza di come queste fasi vengono realmente eseguite <https://attack.mitre.org/>

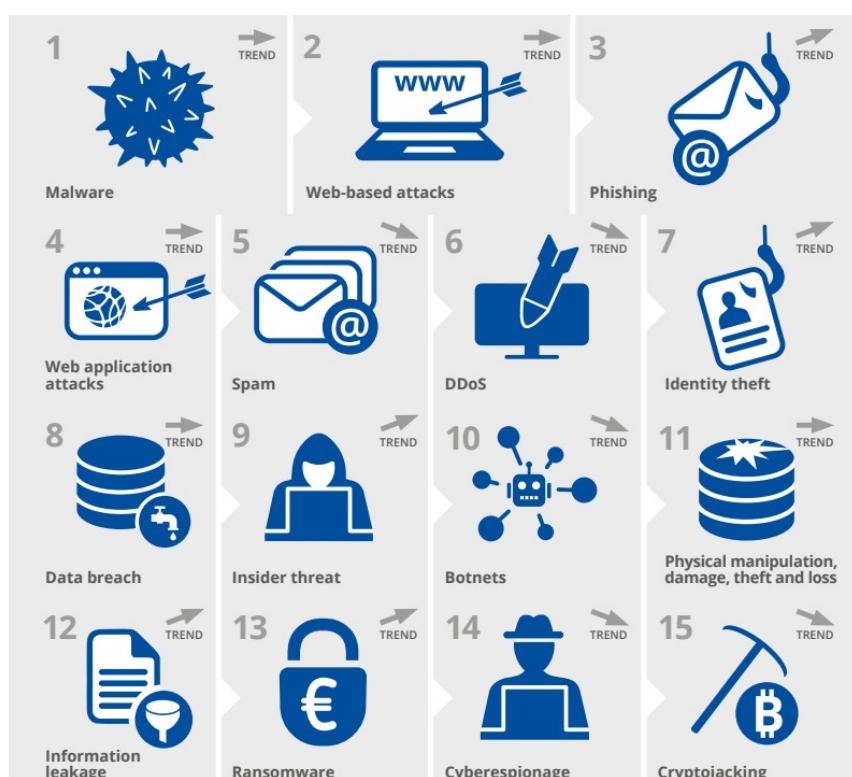
Il panorama delle minacce

ENISA Threat Landscape

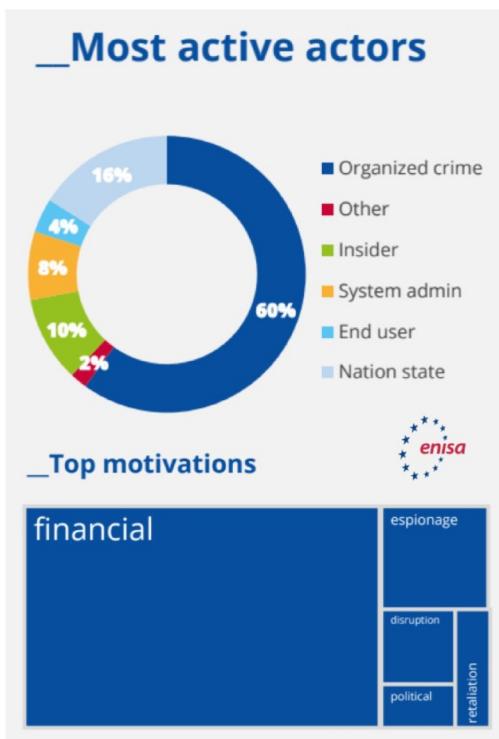
15 Top Threats in 2020

EUROPEAN UNION AGENCY FOR CYBERSECURITY

www.enisa.europa.eu



Chi, perché e come



■ I punti di ingresso sono ancora principalmente legati all'elemento umano

- Furto di credenziali
- Social engineering
- Errori di configurazione
- Abuso di privilegi

■ L'azione conseguente più comune è l'installazione di malware

- Con 230.000 varianti nuove ogni giorno, la rilevazione è ancora un punto dolente
- Dopo l'ingresso, il movimento all'interno dell'organizzazione è rapido ed efficace

I bersagli

_Five most desired assets by cybercriminals

01 Industrial property and trade secrets

Industrial property and trade secrets are the most desirable assets because of their high value to their owners, the market and some cases the criminal world.

02 State/military classified information

This asset includes any information that a state deems sensitive. In 2019, the trade and diplomatic tensions between countries made this type of information even more attractive.

03 Server infrastructure

Server infrastructure is the first sensitive asset that is not data. In many attacks, taking over the victim's server infrastructure, is the primary objective.

04 Authentication data

Authentication data is valuable assets for generating profits but also as an objective to support an attack.

05 Financial data

Financial data such as credit card, banking and payment information is always value to cybercriminals.

_Most targeted sectors

Digital Services Services such as e-mail, social and collaborative platforms and cloud providers were under attack during 2019. These were also used as proxies for further attacks.

Government Administration The financial returns from ransoms paid makes the public sector one of the most attractive targets for ransomware attacks.

Technology Industry The technology industry was under attack in 2019 mainly through supply chain attacks trying to compromise the development of software through zero-day exploits and backdoors attacks.

Financial The number of incidents with financial organisations and not necessarily banks, increased substantially during the reporting period.

Healthcare The number of attacks against the healthcare sector continues to grow.



L'effetto COVID

■ Lockdown =

- Telelavoro → maggiore utilizzo di dispositivi e reti non gestiti
- Incremento dell'uso dei servizi online personali → e-commerce, e-banking, social network, più usati da utenti esperti e più nuovi utenti non consapevoli dei rischi

■ **Coronavirus is alone blamed for a 238% rise in cyber attacks on banks.**

■ **Phishing attacks have seen a dramatic increase of 600% since the end of February.**

■ **Ransomware attacks rose 148% in March and the average ransomware payment rose by 33% to \$111,605 as compared to Q4 2019.**

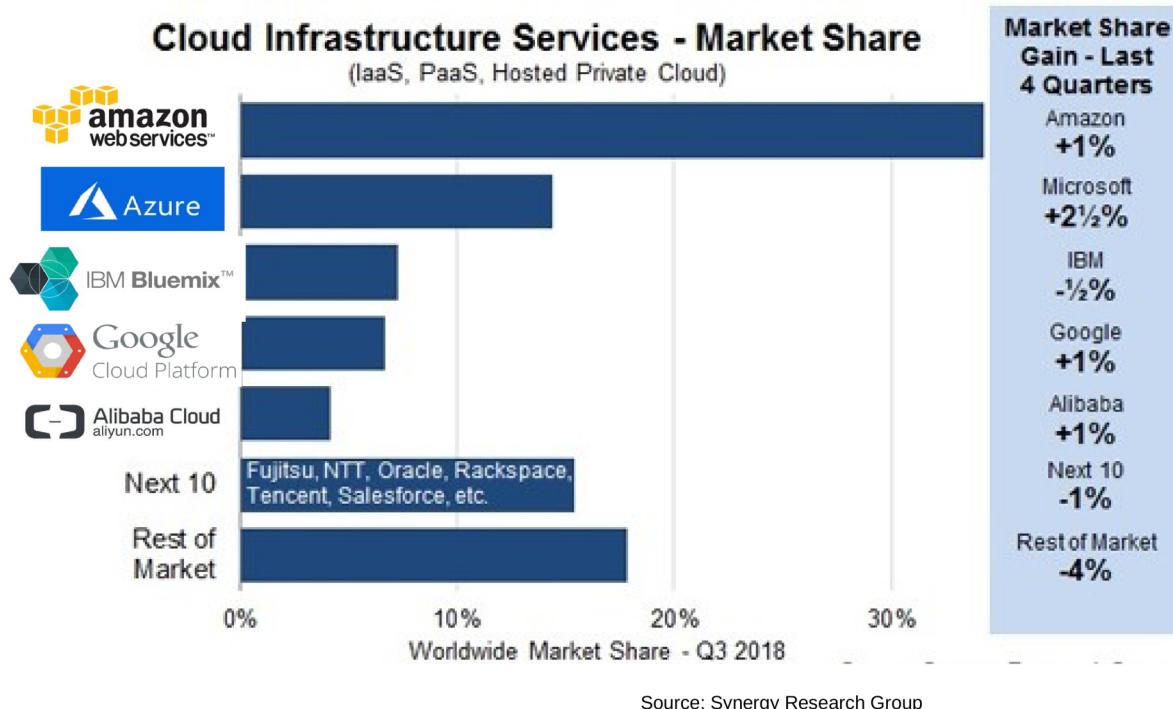
(Source: Fintech News)

I maggiori incidenti

Data breaches	Ransomware	Sabot/Espion	Cyberwar
Mitsubishi (employees, projects) CheckPeople (56M US citizens) Wawa (30M credit cards)	J	Travelex (6M\$) US def. contr. CPI (500k\$ - 2 months to recover)	J
Clearview AI 3bn photos + customer list (law enforcement) Tetrad (747GB data on households)	F	UK Redcar Council (10M£)	F
Virgin Media (900k users) US Census (200M citizens)	M	UK Durham fire/police/govt.svcs	M
Nintendo (160k accounts) Zoom (500k accounts)	A	Energias de Portugal (9.9M€)	A
EasyJet (9M records) CAM4 adult live (10M+ users)	M	21 incidents reported, including Fresenius hospital operator & NYC law firm representing celebs	M
	J	UC Covid-19 research data (1.14M\$) Most Honda offices shut down (Enel blocked a similar attack)	J
	J	Telecom Argentina (7.5M\$) Garmin (3 days down)	J
235M Instagram, TikTok and YouTube user profiles Carnival customers & employees	A	NL CWT travel (4.5M\$) Konica Minolta (1 week down)	A
SK Covid tracing (390k patients)	S	31 incidents, including (DE) Duesseldorf University H. (AG) Dir. Nac. Migraciones (4M\$) (PK) electric company (4M\$)	S
Marriott fined 18M£ for 2014-2018 leak of 339M customer data	O	40 incidents, including ERT (disrupted vaccine tests) DE Software AG (20M\$)	O
			7 events (IR,TK,RU,IL)
		IR DDoS of interet infrastr.	4 events (RU,CN)
		SA exploit global telco bug to track citizens CN espionage on 75 org. ww.	3 mass surveillance (KP,KR,UZ) 2 wide industry attaks (CN,US)
		AZ SCADA wind turbines	9 events (VN,RU,CN,IR)
		JP/IT/DE/UK industrial suppliers RU→DE spl.ch.→energy/water NO state fund empl. tricked 10M\$	11 events (RU,CN,IR,IL)
		Backdoor found in mandatory tax-filing software for foreign companies operating in China	8 events (KP,CN,IN)
		IL water infrastructure	5 events (RU,CN,US)
		NZ Stock Exchange DdoS KP worldwide ATM robbery IR→US mf backdoor injection CN→TW code&design theft	9 events (KP,IR,RU,CN,IN)
		Georgia COVID research espion.	9 events (IR,CN,RU)
			24 events (IR,CN,RU,GR,KP)

Piccola digressione: sovranità

- Evidente necessità: difendersi da attacchi esterni
- Per la normale operatività, nessuna preoccupazione?



Lo scenario degli attacchi in sintesi

01 Attack surface in cybersecurity continues to expand as we are entering a new phase of the digital transformation.

02 There will be a new social and economic norm after the COVID-19 pandemic even more dependent on a secure and reliable cyberspace.

03 The use of social media platforms in targeted attacks is a serious trend and reaches different domains and types of threats.

04 Finely targeted and persistent attacks on high-value data (e.g. intellectual property and state secrets) are being meticulously planned and executed by state-sponsored actors.

05 Massively distributed attacks with a short duration and wide impact are used with multiple objectives such as credential theft.

06 The motivation behind the majority of cyberattacks is still financial.

07 Ransomware remains widespread with costly consequences to many organisations.

08 Still many cybersecurity incidents go unnoticed or take a long time to be detected.

09 With more security automation, organisations will be invest more in preparedness using Cyber Threat Intelligence as its main capability.

10 The number of phishing victims continues to grow since it exploits the human dimension being the weakest link.

With all the changes observed in the cyber threat landscape and the challenges created by the COVID-19 pandemic, there is still a long way before cyberspace becomes a trustworthy and safe environment for everyone.

Difesa

- La messa in sicurezza deve essere un processo metodico
- I *framework* e le *metodologie* possono aiutare nella sistematizzazione
- Le *certificazioni* possono dare evidenza, fornita da una terza parte disinteressata, che misure efficaci siano state adottate da una controparte
 - La sicurezza della supply chain è diventata un elemento cruciale
- Vediamo solo una minuscola panoramica di alcuni elementi importanti



<https://www.nist.gov/cyberframework/framework>
Credit: N. Hanacek/NIST

Prevenzione

- Come tutti i processi ingegneristici, politiche e meccanismi derivano da
 - Analisi di requisiti
 - Progetto
 - Implementazione
 - Test
- Devono essere applicati a
 - Processi organizzativi
 - Contesto fisico
 - Sistemi
 - Reti
 - Applicazioni

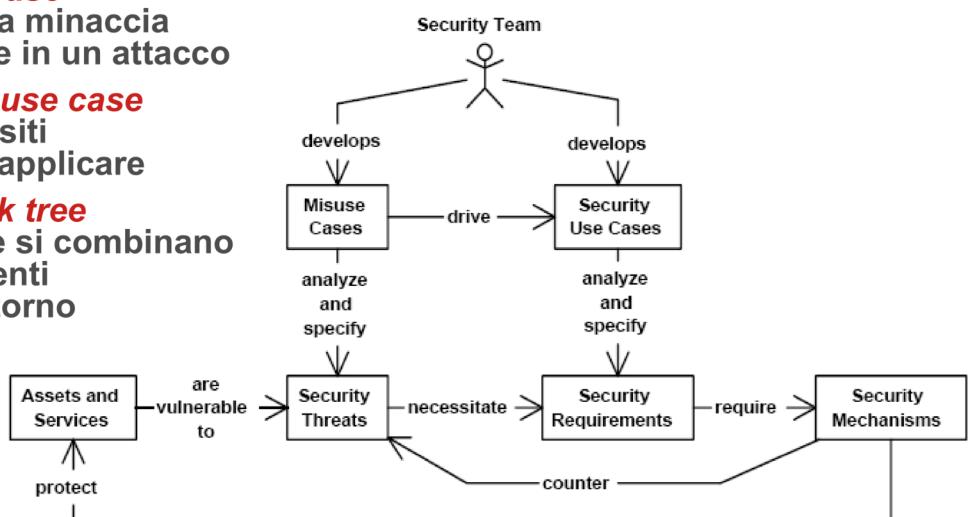
Prevenzione - Security Engineering

■ Prima sfida: non trascurare nemmeno un dettaglio

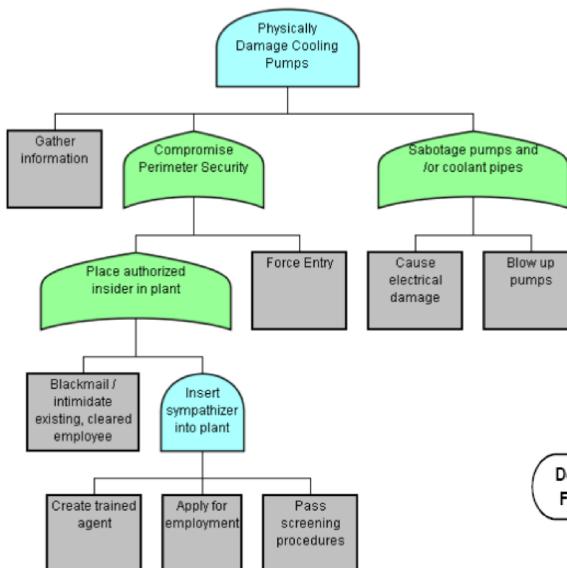
- Inventario di tutti i componenti fisici
- Catalogo di tutti i servizi

■ Raccolta dei requisiti

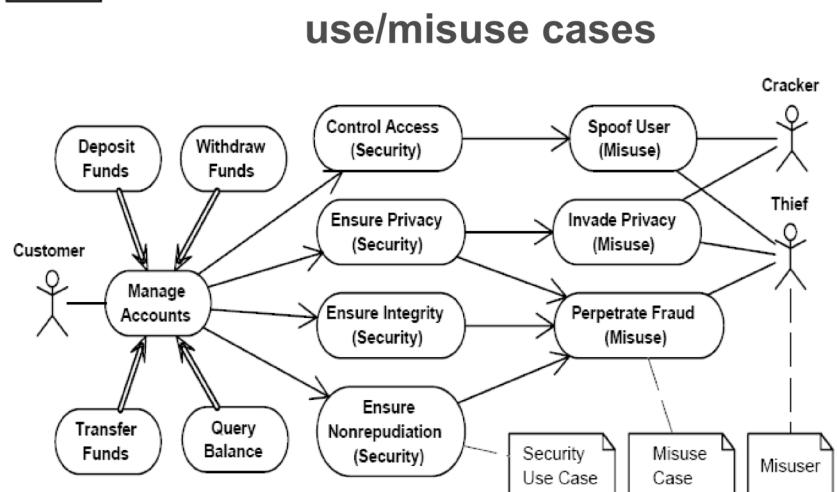
- Molto diversa da quella tradizionale: focalizzata sul “non deve accadere” invece che sul “deve funzionare”
- Studio dei ***misuse case*** per verificare se una minaccia si può concretizzare in un attacco
- Studio dei ***security use case*** per distillare i requisiti dei meccanismi da applicare
- Definizione di ***attack tree*** per modellare come si combinano diversi possibili eventi e condizioni al contorno



Security Engineering - esempi



attack tree



Security Engineering – migliori pratiche

- 1) Basare le decisioni della sicurezza su una esplicita politica**
 - a) Identity
 - b) Access control
 - c) Content-specific
 - d) Network and infrastructure
 - e) Regulatory
 - f) Advisor and information
- 2) Evitare un singolo punto di fallimento (defense in depth)**
- 3) Fallire in modo certo**
- 4) Bilanciare sicurezza e usabilità**
- 5) Essere consapevoli dell'esistenza dell'ingegneria sociale**
- 6) Usare ridondanza e diversità riduce i rischi**
- 7) Validare tutti gli input**
- 8) Dividere in compartimenti i beni**
- 9) Progettare per il deployment**
- 10) Progettare per il ripristino**

Prevenzione - Testing

- **Fondamentale per**
 - verificare se sono sfuggite vulnerabilità
 - verificare se il sistema è esposto a rischi nuovi rispetto al momento della progettazione
- **Problema concettuale: copertura**
 - Non su può dimostrare l'assenza di problemi
 - Solo tentare di sollecitare il sistema nel modo più completo possibile per trovare eventuali problemi esistenti
- **Tre livelli di approfondimento**
 - Vulnerability Assessment
 - Penetration Testing
 - Red Team Operations

Rilevazione

- **Osservare il sistema durante tutte le fasi del suo funzionamento**
- **IDS = Intrusion Detection System**
 - qualsiasi sistema in grado di rilevare i tentativi di attacco
 - basato sulla firma → cerca gli attacchi noti
 - rilevamento delle anomalie → cerca le deviazioni dai comportamenti sicuri
- **IPS = Sistema di prevenzione delle intrusioni**
 - in poche parole: un IDS che può attivare contromisure
- **SIEM = Informazioni sulla sicurezza e gestione degli eventi**
 - un'etichetta commerciale e completa per strumenti, politiche e processi che gestiscono origini dati e incidenti

Certificazioni

- **Di processo per le aziende**
 - ISO 27000
 - ITIL (Information Technology Infrastructure Library)
 - COBIT (Control Objectives for Information and Related Technologies)
- **Di competenza per i professionisti – una pletora, ad esempio TIBER-EU suggerisce per i Red Team**

– CCITM, CCSAM	→ CREST - UK
– CISSP, SSCP, CCSP	→ ISC2 - origini USA
– CSX-P, CISM, CRISC, CISA	→ ISACA - origini USA
– Security+, CySA+	→ CompTIA – USA
– ECSA, CEH, LPT, CHFI	→ EC Council - USA
– GPEN, GWAPT, GXPN, GMOB, GAWN	→ SANS institute - USA
– OSCP, OSWP, OSEE, OSWE, OSCE	→ Offensive Security – USA
– eCCPT, eWPT, eWPTX, eMAPT, eCXD, eCPTX	→ eLearnSecurity - USA



Lo scenario europeo e italiano

- Gli attaccanti si organizzano, devono farlo anche i difensori
- È indispensabile un cambiamento di scala
 - singola impresa → supply chain → sistema paese → digital single market
- Va tutelato l'interesse nazionale in un quadro di alleanze UE
 - Quadro strategico nazionale per la sicurezza dello spazio cibernetico (Pres. CdM, 2013)
 - Direttiva "NIS" recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (n. 2016/1148 del Parlamento Europeo del Consiglio)
 - Piano nazionale per la protezione cibernetica e la sicurezza informatica (Pres. CdM, 2017)
 - Attuazione della Direttiva NIS (DLGS n.65 , 18 maggio 2018)
- Ci sono due problemi incisivi:
 - Skill shortage
 - Capacity building

Agredire lo skill shortage

- I numeri
 - Numero stimato di posizioni lavorative disponibili e non coperte in ambito cybersecurity
 - Worldwide: 2.93 milioni (2018) -> 4.07 milioni (2019)
 - Europa: 142.000 (2018) -> 291.000 (2019)
 - Deficit stimato in Europa per il 2022 pari a 350.000 addetti
- Come agire?
 - Nuove forme di innovazione didattica
 - supporto alle comunità di studenti appassionati di cybersecurity
 - Allargare la ricerca anche a personale con formazione non prettamente informatica ed ingegneristica
 - Iniziative nazionali che avviano alla cybersecurity anche i più giovani

Capacity building – due esempi

■ Cyber Ranges

- Una federazione di “poligoni di tiro” cyber
- Oggetto di lavoro in ECSO, nei 4 progetti pilota, nel CSNL

■ Certificazioni

- Definire criteri armonici per riconoscimento mutuo
- Sfruttare le esperienze di **composability** maturate in altri settori
- ECSO WG5 - EHR4CYBER:
 - *The certification market is dominated by non-European, especially US, companies. A European wide certification scheme including an education framework is lacking.*

Cosa fa Unibo

■ Altre competenze di ricerca legate a cybersecurity del Dipartimento di Informatica – Scienza e Ingegneria (DISI)

- Visione artificiale
- Sistemi biometrici
 - Impronte digitali
 - Riconoscimento del volto
- IoT e Cloud
 - Next generation networks
 - Orchestrazione di microservizi e sistemi serverless
- Computazione Quantistica
- Crittografia
- Analisi statica dei programmi
- Sistemi di gestione delle reti basati su politiche
- Modelli di controllo dell'accesso
- Metodologie di Vulnerability Assessment e Red Teaming

Community building

- Studenti in Informatica e TLC Bologna-Cesena
- Gruppi di lavoro autogestito
 - Discussione
 - Addestramento
 - Competizione
 - DEFCON quals 2012
CeSeNA
72° posto su 414
 - DEFCON quals 2019
ULISSe
97° posto su 1261
 - DEFCON quals 2020
ULISSe+CeSeNA
60° posto su 1399



ULISSE

Unibo Laboratory
of Information and
System SEcurity



UNIBO MAGAZINE

[Home](#) • [Innovazione e ricerca](#) • [A scuola di hacking: studiare la sicurezza informatica sfidando gli esperti di...](#)

2 Luglio 2013

A scuola di hacking: studiare la sicurezza informatica sfidando gli esperti di tutto il mondo

Computer security e hacking: sono i temi di cui si occupa un gruppo di studenti di informatica a Cesena, attraverso l'organizzazione di seminari autogestiti e la partecipazione a competizioni internazionali

Cosa fa Unibo

- Non si può lavorare in isolamento!
 - nodo del Laboratorio Nazionale di Cybersecurity del CINI



cini

Cyber Security National Lab

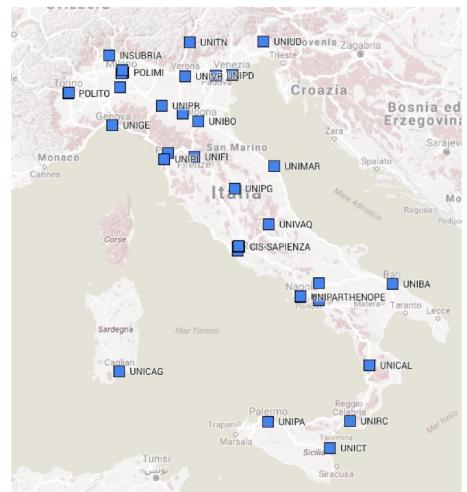
- membro di ECSO



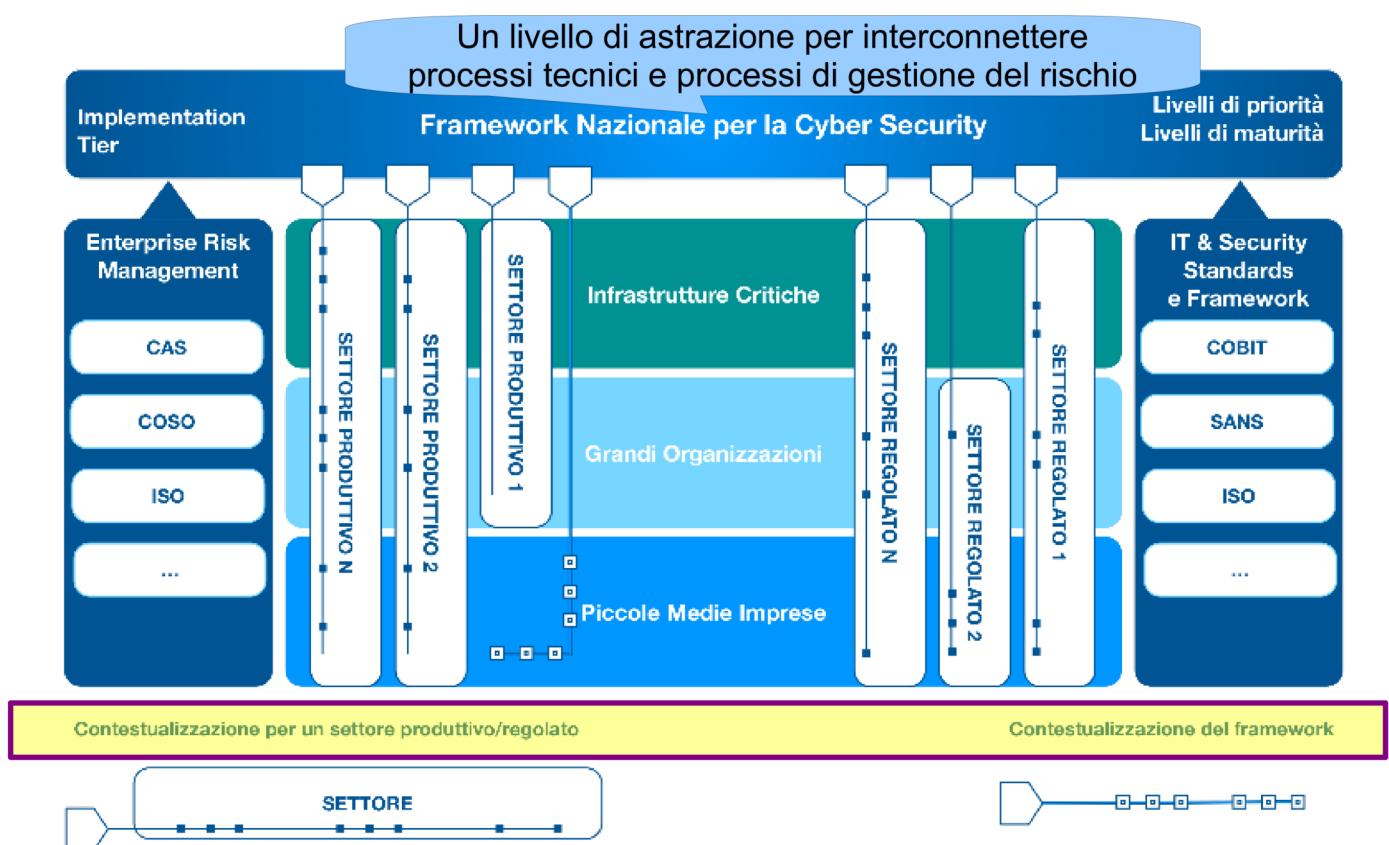
- Non può prescindere dalla missione formativa
 - Ha attivato percorsi di alta formazione specifici

Il Laboratorio Nazionale di Cyber Security

- Fondatore e primo direttore:
Prof. Roberto Baldoni
Università di Roma La Sapienza
 - attualmente vicedirettore generale del Dipartimento delle Informazioni per la Sicurezza (DIS) con delega alla cyber security
- Missione:
 - Coordinare eccellenze a livello scientifico e industriale
 - Aiutare il sistema paese ad essere più resiliente alla minaccia cibernetica
 - Aumentare consapevolezza del rischio e misure di protezione
 - Definire standard e metodologie
 - Armonizzare iniziative nazionali ed europee



Framework Nazionale per la Cyber Security



Non solo framework per le imprese: CyberReadiness individuale

What

- A project aimed at assessing the cybersecurity posture of *individuals*, taking care of their roles and positions

Assets

- Complete anonymization
- Versatile platform to collect results
- Sound methodology to propose personalized remediation actions

How

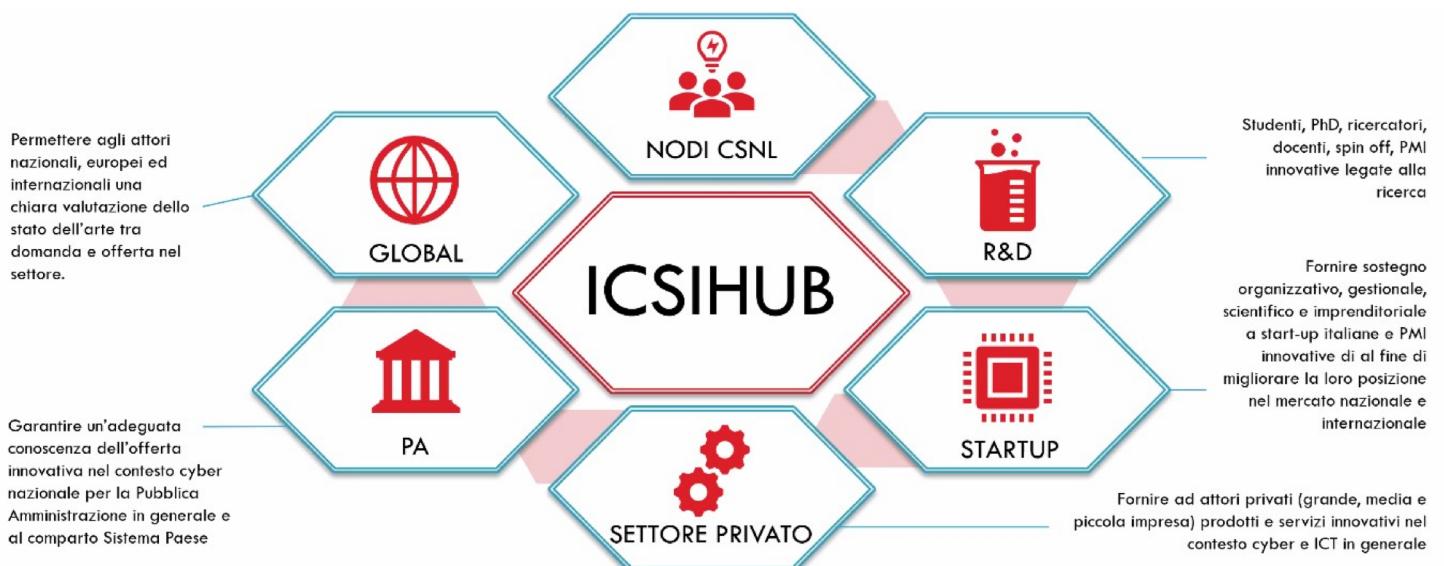
- A Survey
- Set of questions, properly customized according to roles, positions, company, administration, ...

Remediations

- Based on a qualitative and quantitative methodology
- A personal dashboard suggests remediation actions



Non solo framework: verso un Italian CyberSecurity Innovation Hub



La ricerca su scala europea – i grandi temi

- Approfondire la comprensione dell'elemento umano
- Integrare la sicurezza mentre nasce la rete 5G
 - Agire su tutti gli strati
 - HW/SDN/SW – tolleranza alle intrusioni nella supply chain
 - Standardizzare i controlli di sicurezza
 - Sviluppare sistemi AAA compatibili con le “thing”
- Privacy nell'era del cloud
 - Crittografia omomorfa
 - Secure multiparty computation
 - User-centric privacy
- Aumentare l'efficienza della Cyber Threat Intelligence
 - Migliorare la disseminazione di metodi e strumenti
 - Adottare approcci open
 - Automatizzare i processi
 - Passare dall'analisi al supporto alle decisioni
 - Integrare i dettagli specifici dei diversi domini

Un punto di incontro europeo



ECSO is the private counterpart to the European Commission in implementing the contractual Public-Private Partnership (cPPP) on cybersecurity.

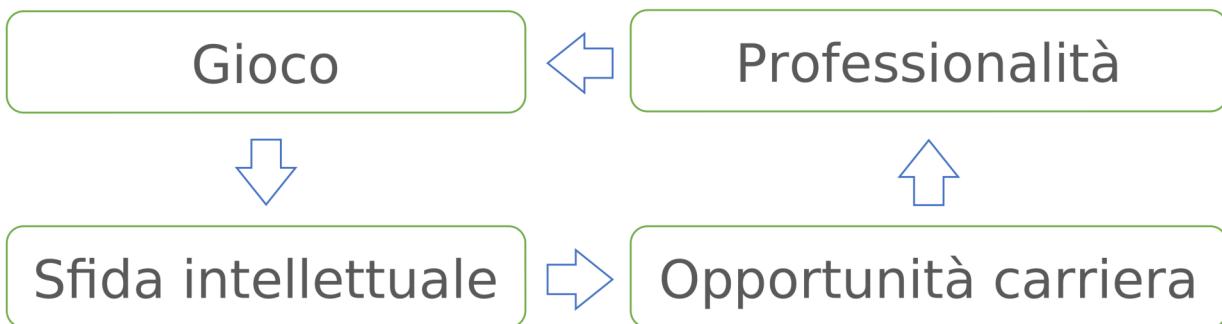
The main goal of ECSO is to coordinate the development of the European Cybersecurity Ecosystem

- Due esempi di iniziative
 - Sostenere le aziende cyber EU sul mercato



an industry-driven marketing tool, designed to promote European cybersecurity companies and increase their visibility on the European and on the global market.

- Indicare alla Commissione Europea le priorità nel finanziamento di bandi di ricerca e innovazione
 - WG6 → Strategic Research and Innovation Agenda



- **Percorso gratuito per giovani da 16 a 23 anni**
 - Docenti DISI
 - Volontari ULISSe
- **24 ore di fondamenti e 48 di esercitazioni in 12 weekend**
- **Sfida finale locale (jeopardy)**
 - Formazione dei team coi migliori 4 di ogni sede
- **Sfida finale nazionale (attack-defense)**
 - Scontro diretto tra i team

- **Edizione 2019**
 - 18 sedi
 - 3200+ candidati
 - 360 ammessi



**Finale nazionale
Chiavari 27-6-2019**

UNIBO MAGAZINE

[Home](#) • [Incontri e iniziative](#) • [Cyber challenge italiana, medaglia d'argento per i cyber-defender Unibo](#)



1 Luglio 2019 | [Premi e riconoscimenti](#)

Cyber challenge italiana, medaglia d'argento per i cyber-defender Unibo

Il team dell'Alma Mater ha sbaragliato le altre squadre, composte da studenti universitari provenienti da tutta Italia, in una sfida sulla gestione della sicurezza di sistemi informatici di tipo attacco-difesa

■ Edizione 2020

- 28 sedi
- 4452 candidati
 - Unibo: 188 domande
- 560 ammessi + eventuali riserve
 - Unibo: 20 ammessi + 5 riserve
 - 5 da fuori provincia
 - **6 studenti delle scuole superiori**
 - 14 iscritti a LT
 - 5 iscritti a LM
- Challenge locale
 - 8 giugno (online)
- Challenge nazionale
 - 1-2 ottobre (online) →
 - **5° posto**
(a un soffio dal podio!)



■ Edizione 2021

- 32 sedi
- **4868 domande (Unibo: 211)**

■ Edizione 2022

- 32 sedi
- Iscrizioni fino al 2 febbraio 2022

- <https://cyberchallenge.it>
- Se avete domande per la sede di Bologna*: disi.ulisse@unibo.it



Master Universitario di I livello *Cybersecurity: from design to operations*

■ Internazionale

- Insegnamenti in inglese (salvo caso solo studenti italiani)

■ Impegno

- 288 ore di aula (teoria ed esercitazioni)
- 500 ore di tirocinio (o project work per studenti lavoratori)
- seminari offerti dalle aziende partner

■ Weekend formula

- 4 ore ogni venerdì
- 8 ore ogni sabato

■ Calendario

- Autunno/inverno: moduli introduttivi
- Inverno/primavera:
 - Lezioni nel weekend
 - Tirocinio durante la settimana

Master Universitario di I livello

Cybersecurity: from design to operations

- **Intro track – 24 ore**
 - Fundamentals of Security and Cryptography (24h)
- **Infrastructure security track – 80 ore**
 - Computer security and administration
 - Network security and administration
- **Software security track – 72 ore**
 - Secure coding I - software engineering
 - Secure coding II - web app security and testing
 - Secure coding III - mobile security and testing
- **Attack detection track – 64 ore**
 - Security monitoring I - Malware analysis and detection (32h)
 - Security monitoring II - information correlation (32h)
- **Response & recovery track – 48 ore**
 - Incident response (16h)
 - Cyber Forensics (32h)

Dove trovarmi

- E-mail/Teams: marco.prandini@unibo.it
- Telefono: 05120 93867

Cenni di crittografia

*Marco Prandini
DISI – Università di Bologna*

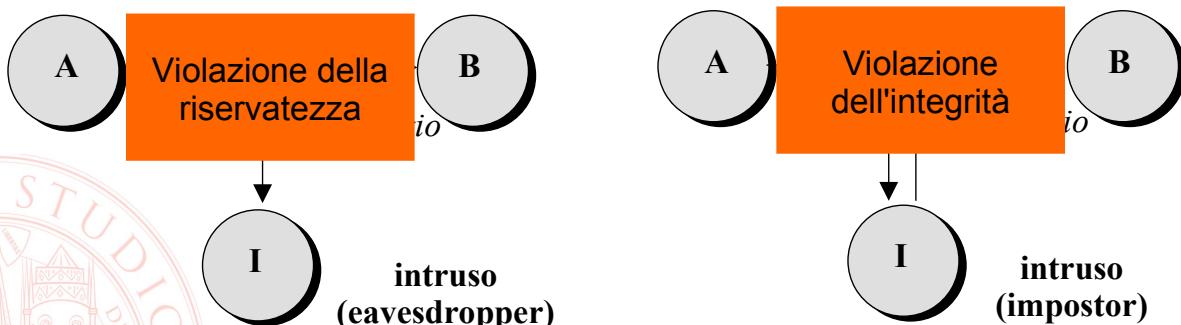


Da cosa è fatta la sicurezza delle informazioni

- ⇒ Confidentiality (riservatezza)
- ⇒ Integrity (integrità)
 - Authenticity (paternità)
- ⇒ Availability (disponibilità)



Mondi ideali e reali



Soluzione: crittografia

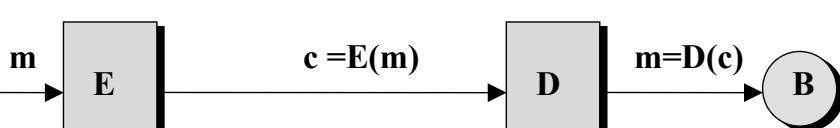
- ⇒ Un'elaborazione matematica e algoritmica della codifica delle informazioni
- ⇒ Prevenire la violazione della riservatezza (una rilevazione a posteriori sarebbe inefficace!):
→ alterare il codice in modo da renderlo incomprensibile a chi non ha diritto di apprendere le informazioni
- ⇒ Rilevare la violazione dell'integrità e autenticità (non può essere prevenuta!) → aggiungere al codice elementi che permettano la verifica delle informazioni ricevute

Una novità introdotta da Internet?

- ⇒ VI sec. a.C. - Il cifrario Atbash degli Ebrei
 - Sostituzione monoalfabetica
- ⇒ V sec. a.C. - La tavoletta di Demarato
 - Steganografia
- ⇒ IV sec. a.C. - La scitala degli Spartani
 - Trasposizione
- ⇒ IV sec. a.C. - Lo schiavo rapato di Istieo
 - Steganografia
- ⇒ I sec. a.C. - Il cifrari di Cesare
 - Sostituzione monoalfabetica
- ⇒ VIII sec. d.C. - Il trattato di Al-Kindi
 - Studio sistematico della **crittoanalisi**

Cifrari per la riservatezza

- ⇒ Due operazioni
 - Cifratura
 converte il testo in chiaro in testo cifrato
 - Decifrazione
 converte il testo cifrato in testo in chiaro



I principi di Kerckhoffs (1883)

- 
- 1) Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
 - Sicurezza *computazionale* o *assoluta*
 - 2) Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
 - **segreto=algoritmo segreto=chiave!**
 - 3) La clef doit pouvoir en être communiquée et etenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants;
 - Cifratura = ricordare un segreto semplice per poter scambiare molti segreti arbitrari

Crittoanalisi

- 
- ⇒ Di fronte a un testo cifrato con algoritmo noto, cosa può sempre fare un crittoanalista?
 - Analizzare le proprietà statistiche del testo
 - robustezza = capacità dell'algoritmo di **occultare le proprietà del testo in chiaro**
 - Cercare la chiave tra tutte quelle possibili
 - sicurezza assoluta = rendere totalmente **indistinguibile** la chiave giusta dalle altre
 - sicurezza computazionale = rendere il processo di ricerca della chiave **trop poco oneroso**

Sostituzione monoalfabetica

- ⌚ Cifrario di Cesare, Agony Columns del Times, parole crociate crittografate della Settimana Enigmistica, ...

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

- ⌚ CRITTOGRAFIA → ESOZZGUSQYOOQ

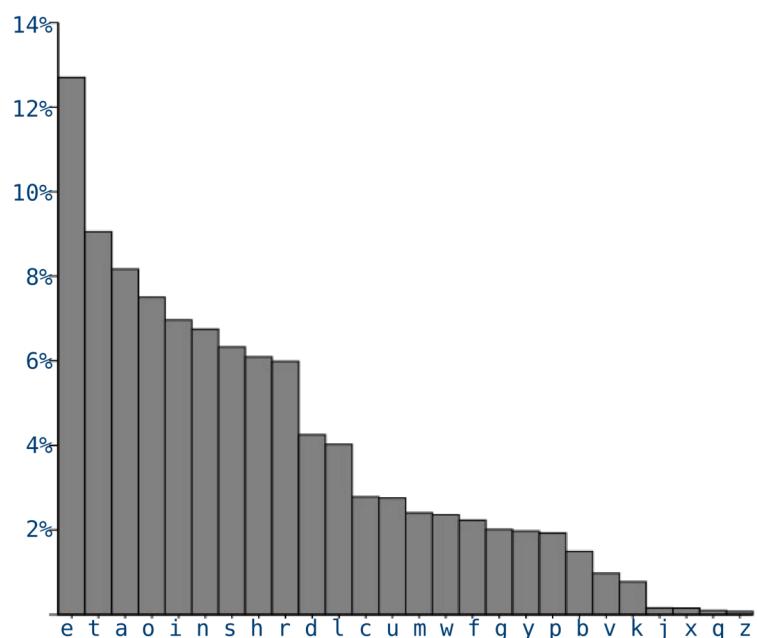
⌚ Ricerca della chiave: spazio di $26! \approx 4 \cdot 10^{26} \approx 2^{88}$

⌚ Robustezza...

Attacco alla sostituzione

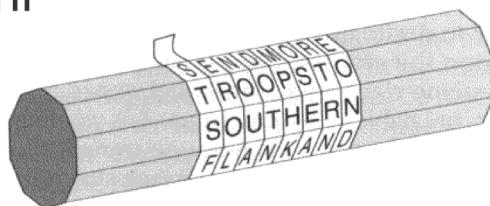
Nel linguaggio naturale, estremamente facile con le statistiche di frequenza dei caratteri (in figura il grafico per la lingua inglese)

Nel mondo binario, la “lettera” può essere un lungo blocco di bit
→ frequenze basse e uniformi (compressione)
→ buona efficacia!



Trasposizione

- ⇒ La scitala degli Spartani



- ⇒ Algoritmamente basta una tabella scritta per colonne e letta per righe

ALLE PROSSIME ELEZIONI MI PRESENTO ANCHE IO

A	P	I	L	N		E	A	
L	R	M	E	I	P	N	N	I
L	O	E	Z		R	T	C	O
E	S		I	M	E	O	H	
S	E	O	I	S		E		

APILN EA LRMEIPNNI LOEZ RTCOES IMEOH SEOIS E

Trasposizione

- ⇒ Ricerca della chiave:

- dimensione della tabella
- ordine di lettura delle righe

- ⇒ Robustezza

- Statistiche dei *digrammi* e *trigrammi*
 - Permettono di dedurre la dimensione della tabella
- Per nulla banale se applicata ripetutamente

Sostituzione polialfabetica

- ⇒ Leon Battista Alberti (1466)
 - Forma generale e implementazione meccanica
- ⇒ Bellaso/Vigenère (1553)
 - Forma semplificata usata per 4 secoli (es. la macchina Enigma - WWII)



Sostituzione polialfabetica

Es. si consideri $A=0, B=1, \dots, Z=25$ e si sommi modulo 26 la chiave al testo

Le frequenze di un carattere in chiaro vengono sparse su più caratteri cifrati

Le frequenze di un carattere cifrato derivano da contributi di diversi caratteri in chiaro

Key flow:	C I A O C I A O C I A O C I A O C I A O
Message:	D O M A N I N O N P O S S O P A S S A R
	F W M O P Q N D P X O H U W P O U B A G

Attaccabile grazie al ripetersi periodico delle sostituzioni

Attaccabile facendo ipotesi sul contenuto del messaggio (*cribs*)
- Trattato sulla crittoanalisi di Charles Babbage (1853)
- Decifrazione rapida di Enigma ad opera di Alan Turing (WWII)

One-time pad

- ⌚ Vernam/Mauborgne (1917)
- ⌚ Polialfabetica con chiave
 - Scelta perfettamente a caso
 - Lunga quanto il messaggio
 - Mai riutilizzata

Ma che fatica!

Testo in chiaro **FRA**, Testo cifrato: **WPE**

Tutte equiprobabili

Chiavi possibili

AAA ... EVT ... DYE ... RYE ... FHQ ...

Testi in chiaro

WPE ... SUL ... TRA ... **FRA** ... RIO ...

Ipotesi valide: **tutte** quelle della lingua considerata
→ Quella giusta è indistinguibile

Sicurezza perfetta!

Cifrari simmetrici moderni

- ⌚ Applicano gli stessi principi di confusione e diffusione
 - Reiterando sostituzioni e trasposizioni
 - ⌚ Operano sull'alfabeto binario invece che naturale
 - ⌚ Sono studiati per essere computazionalmente sicuri
 - ⌚ La sicurezza risiede nella lunghezza della chiave
-
- ⌚ Standard storico: DES (National Bureau of Standards degli U.S.A in collaborazione con IBM, pubblicato nel 1977, chiave di 56 bit)
 - ⌚ Standard attuale: AES/Rijndael (chiave variabile di oltre 64 bit)
<http://csrc.nist.gov/encryption/aes/rijndael/>

Robustezza dei cifrari simmetrici

- Il miglior attacco è la forza bruta.

Esempi di tempi di ricerca con tecnologie recenti:

	Lunghezza della chiave in bit		
Budget	56	80	128
1 K€ (individuo)	38 anni	640 milioni di anni	10^{21} anni
1 M€ (impresa)	19 giorni	100.000 anni	10^{18} anni
1 G€ (NSA)	12 secondi	6 anni	10^{14} anni

- Attenzione alle ricerche con tempo di calcolo gratis (lotteria cinese, virus) e alla sfortuna!

- C'è un limite invalicabile: la termodinamica

Limite di Landauer: per cambiare 1 bit almeno $k \times T \times \ln(2)$ (3×10^{-23} J a 3°K)

Tutta l'energia emessa dal Sole in un anno = 1.2×10^{34} J

→ 4×10^{56} bit flip, come contare da 0 a 2^{188}

Energia emessa dall'esplosione di una supernova = 2×10^{44} J

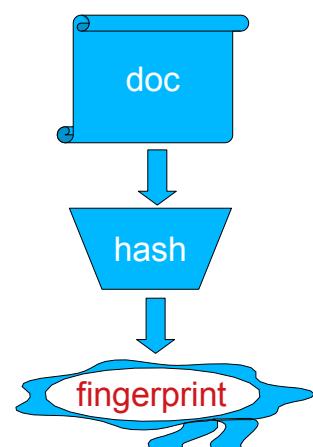
→ 7×10^{66} bit flip, come contare da 0 a 2^{222}

Funzioni hash

- Gli stessi principi possono essere usati senza chiave per ottenere “impronte digitali” compatte di documenti di dimensione arbitraria

- Fingerprint:

- dimensione fissa (f. non biunivoca)
- f. pubblica, senza chiave
- difficili da falsificare
 - Non si riesce a trovare doc dato fingerprint
 - Non si riesce a trovare coppia di doc con lo stesso fingerprint

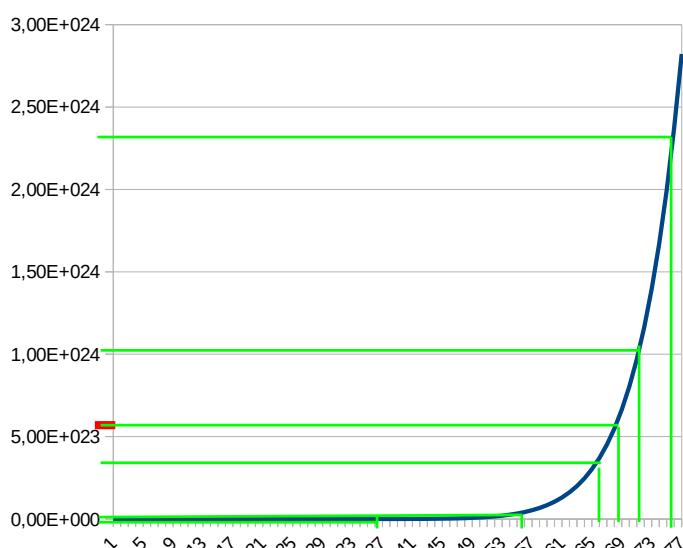


- Uso: autenticazione
(memorizzazione password, firma digitale)

Problemi difficili e trabocchetti

- ⇒ Operazioni facili in un verso e (speriamo) computazionalmente infattibili nell'altro
 - A meno di conoscere un segreto
- ⇒ Fattorizzazione di grandi numeri
- ⇒ Molte operazioni in aritmetica modulare
 - Numeri interi
 - Come risultato di un'operazione si prende il resto della divisione per un *modulo* fisso

Intuitivamente



$$y=x^{13}$$

Su R, se non conosco l'inversa di una funzione "regolare", mi avvicino per approssimazioni successive (es. bisezione)

Per una funzione monotona, si parte dagli estremi del dominio, e si valuta la funzione nel punto medio del dominio.

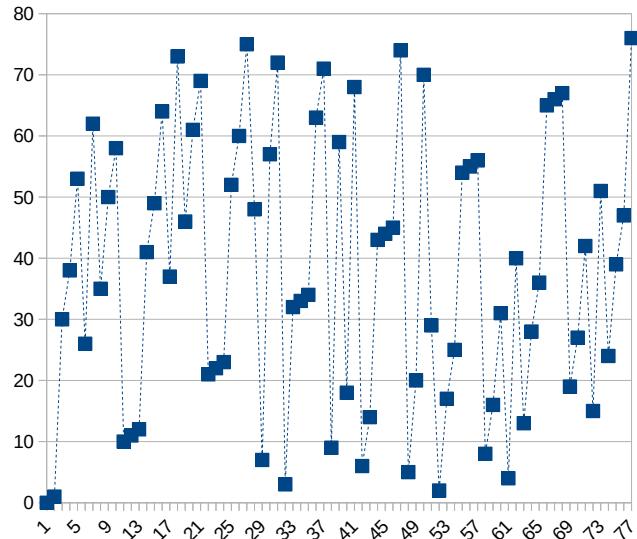
In questo esempio, valutiamo la funzione per $\{0,76\} \rightarrow \{38,76\} \rightarrow \{57,76\} \rightarrow \{66,5,76\} \rightarrow \{66,5,71,25\}$

Per $x=68,875$ otteniamo il risultato

Intuitivamente

$$y = x^{13} \bmod 77$$

Su Z_{77} , (il campo di Galois con 77 numeri, in cui le operazioni si effettuano modulo 77) l'effetto di riduzione modulare rende estremamente irregolare la funzione → non è possibile una ricerca efficiente



Crittografia asimmetrica: RSA (1977)

- ⇒ Generazione delle chiavi:
 1. si scelgono due numeri primi p e q
 2. il modulo viene calcolato come $n = p \cdot q$
 3. si sceglie a caso un numero d e si calcola un numero e tale che $e \cdot d \bmod (p-1)(q-1) = 1$
 - Facile solo conoscendo p e q , che vengono poi dimenticati

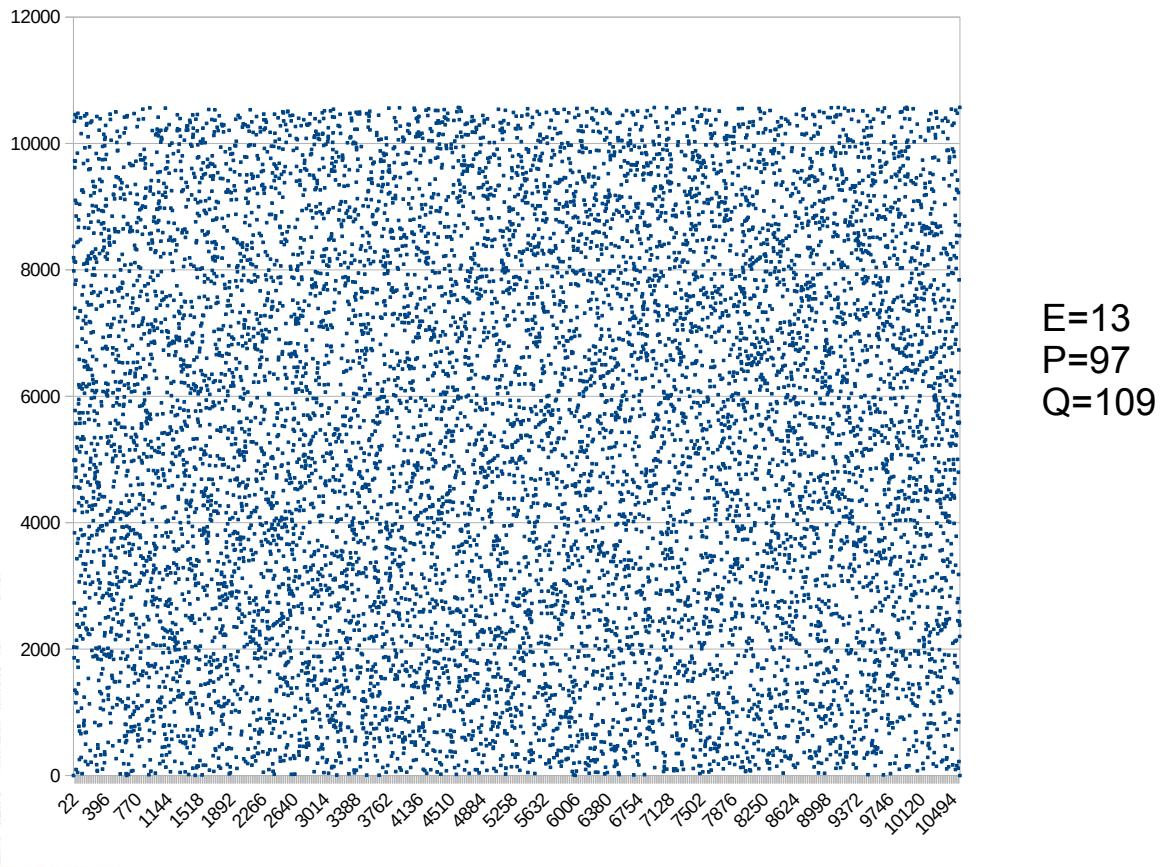
⇒ La chiave pubblica è (e, n) , la chiave privata (d, n)

Cifratura: $c = m^e \bmod n$

Decifrazione $m = c^d \bmod n$



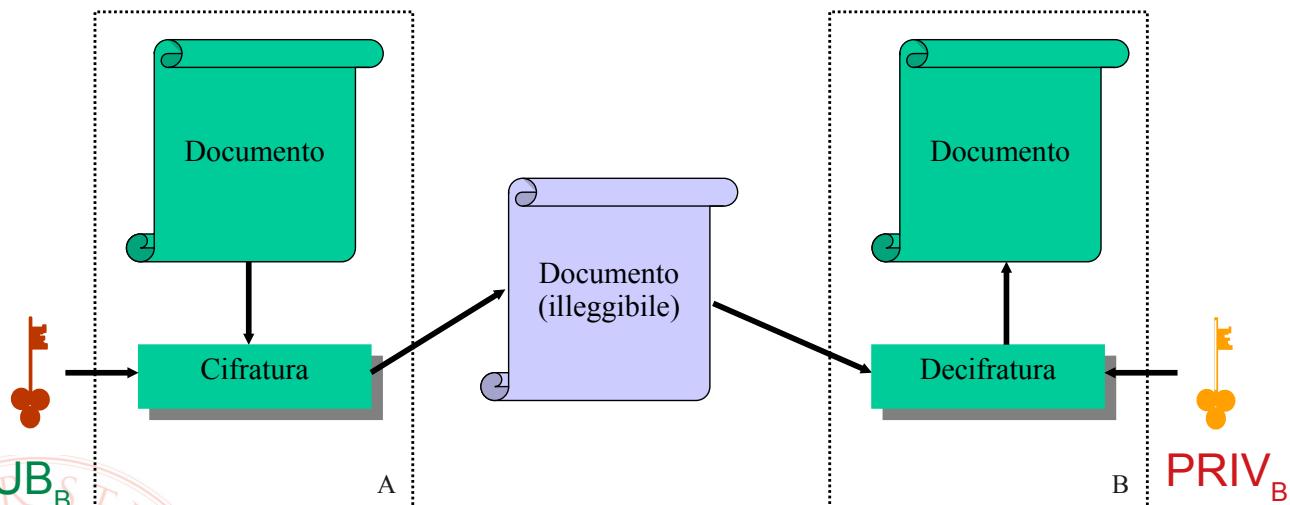
Visivamente



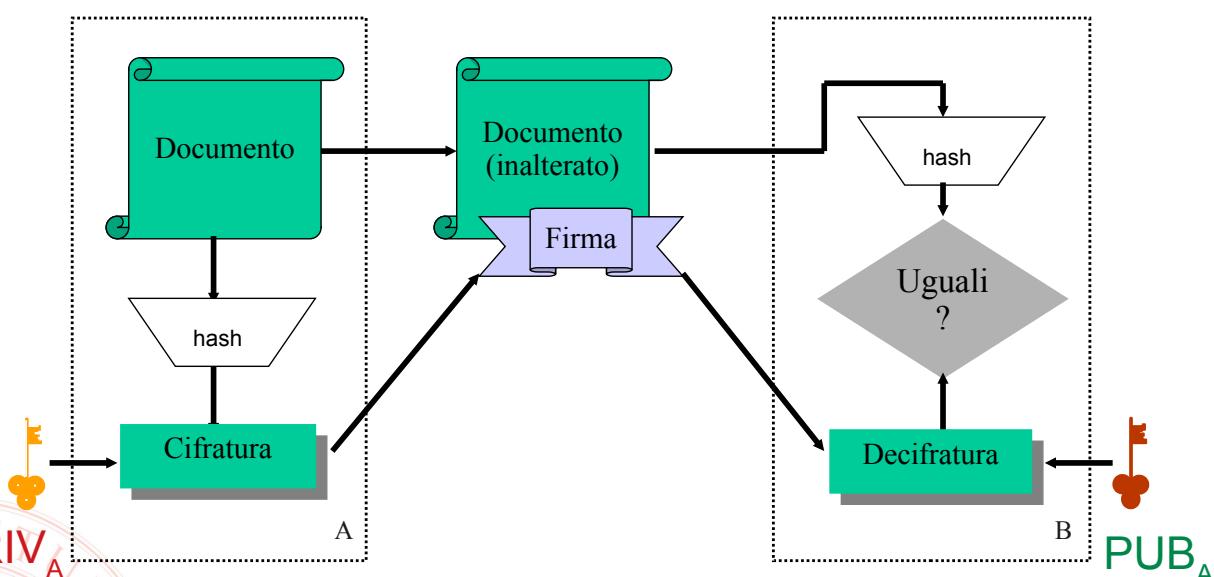
Vantaggi della c. asimmetrica

- ⇒ Le chiavi usate per cifrare e decifrare sono diverse
- ⇒ La chiave pubblica può essere distribuita
 - Da essa non è derivabile la chiave privata
 - Chiunque può usarla per cifrare
- ⇒ La chiave privata corrispondente è l'unica che può decifrare
- ⇒ La chiave privata è specifica di un solo utente quindi utile anche per *autenticare*

C. asimmetrica per la riservatezza



C. asimmetrica per l'integrità e l'autenticità



Il successo della verifica garantisce che si è usata la chiave pubblica corrispondente a quella privata usata per firmare... ma chi garantisce che sia davvero dell'utente A?

C. asimmetrica - pregi e difetti

⇒ Grandi vantaggi:

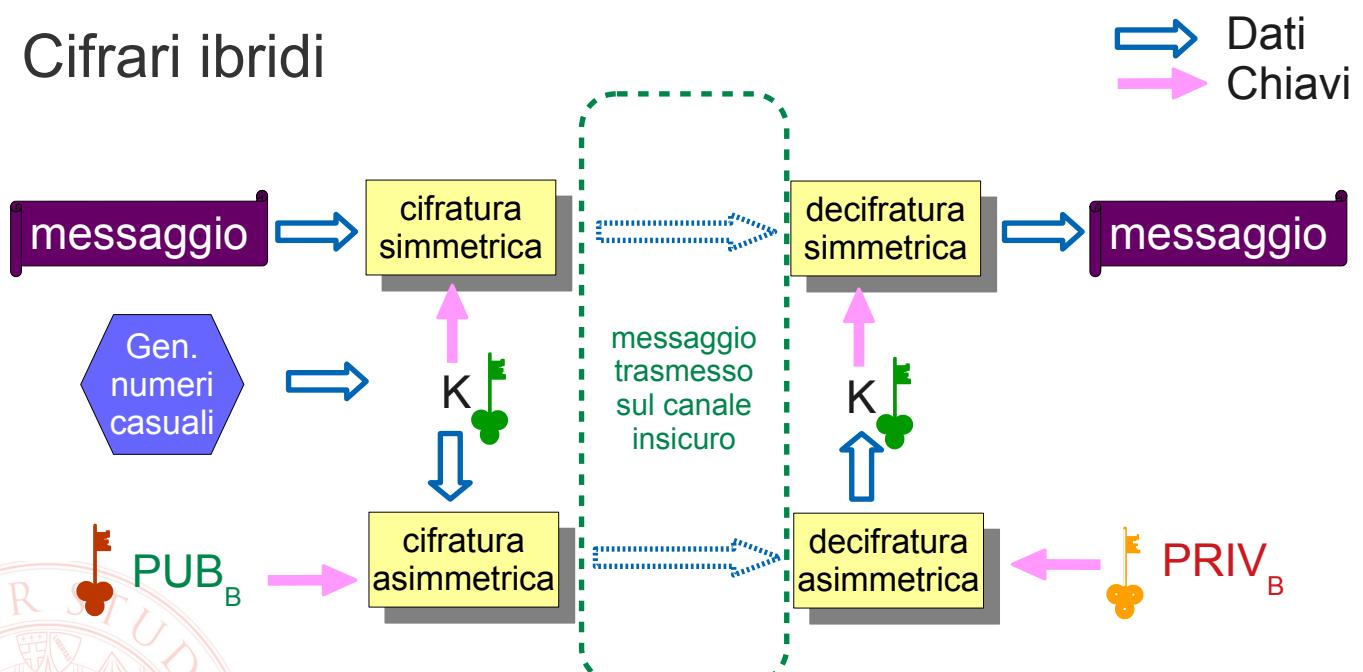
- distribuzione delle chiavi
- utilità per tutte le proprietà di sicurezza

⇒ Punti deboli:

- Prestazioni (5-10 volte più lento di AES)
 - Sistemi ibridi
- alcuni attacchi specifici (known plaintext)

Aggiungere prestazioni e flessibilità

Cifrari ibridi



Più destinatari = un solo messaggio cifrato & più copie di K cifrate con la chiave pubblica di ognuno

Utilizzo della c. asimmetrica per l'autenticazione

- ⇒ Autenticazione passiva (es. password)
 - svela il proprio segreto a chi verifica
 - sempre uguale → replay attack (una password intercettata può essere riutilizzata)
- ⇒ Autenticazione attiva con cifrari asimmetrici (in principio)
 - il possesso della chiave privata identifica univocamente un utente o sistema, poiché non viene mai condivisa
 - il *prover* (P) dimostra al *Verifier* (V) di possedere una certa chiave privata rispondendo a una *sfida*:
 - V genera un numero random grande R
 - V cifra R con la chiave pubblica di P
 - V manda a P la sfida
 - P se è autentico riesce a decifrare e risponde con R
 - Non svela il segreto!
 - R non prevedibile, non riutilizzato, intercettarlo e rigiocarlo è inutile
 - Come nella firma, chi garantisce a V di detenere effettivamente la chiave pubblica di P e non quella di un impostore?

Robustezza della c. asimmetrica

- ⇒ Le chiavi non sono numeri casuali, esiste una relazione matematica che facilita l'attacco
- ⇒ Il metodo più efficiente è tentare la fattorizzazione del modulo (SNFS)
- ⇒ Per questo la lunghezza consigliata del modulo è di **2048 bit e oltre**
- ⇒ Esiste inoltre un problema di **autenticità della chiave**

Secure Shell

- ⇒ Necessità: amministrazione remota
- ⇒ Predecessori: TELNET
 - Nessuna confidenzialità del canale
 - Nessuna autenticazione dell'host
 - Autenticazione passiva dell'utente



Secure Shell

- ⇒ Il collegamento SSH tra client (ssh) e server (sshd) avviene attraverso questi passi essenziali
 - Negoziazione dei cifrari disponibili
 - Autenticazione dell'host remoto per mezzo della sua chiave pubblica
 - Inizializzazione di un canale di comunicazione cifrato
 - Negoziazione dei metodi disponibili per l'autenticazione dell'utente
 - Autenticazione dell'utente
- ⇒ Ognuno dei passi elencati può essere portato a termine in modo configurabile, al fine di garantire il compromesso tra sicurezza e flessibilità più adatto al contesto.



Secure Shell – host authentication

- ⇒ L'autenticazione dell'host remoto è importante per evitare di cadere nella trappola tesa da un eventuale uomo nel mezzo, che potrebbe così catturare la password dell'amministratore spacciandosi per l'host su cui egli vuole effettuare il login
 - Non è previsto un sistema centralizzato di attestazione dell'autenticità della chiave dell'host
 - Alla prima connessione l'amministratore deve utilizzare un metodo out-of-band per determinare la correttezza della chiave pubblica presentata dall'host
 - Alle connessioni successive la chiave pubblica memorizzata dal client dell'amministratore permette di effettuare un'autenticazione attiva
- ⇒ Le chiavi pubbliche vengono memorizzate nel file `known_hosts` nella directory `.ssh` posta nella home dell'utente sul client.

Secure Shell – user authentication

- ⇒ Ci sono due possibilità per l'autenticazione dell'utente sull'host remoto
 - Autenticazione passiva, tradizionale, con username e password – i dati sono trasmessi all'host autenticato su di un canale cifrato, quindi con buon livello di sicurezza
 - Autenticazione attiva, per mezzo di un protocollo challenge-response a chiave pubblica – presuppone che l'utente si doti della coppia di chiavi, e che installi correttamente sull'host remoto la chiave pubblica

Secure Shell – user authentication

- ⇒ In entrambi i casi, l'identità dell'utente con cui viene tentato il login sull'host remoto può essere selezionata
 - in assenza di indicazioni specifiche verrà usato lo stesso nome utente con cui l'operatore sta lavorando sul client

Es:

- utente "marco" sul client esegue "ssh remoteserver"
 - si presenta come utente "marco" su "remoteserver" e si deve autenticare di conseguenza
- utente "marco" sul client esegue "ssh root@remoteserver"
 - si presenta come utente "root" su "remoteserver" e si deve autenticare di conseguenza

Secure Shell – key generation

- ⇒ Per poter effettuare l'autenticazione attiva un utente deve
 - generare una coppia di chiavi asimmetriche
 - comando **ssh-keygen -t rsa -b 2048**
 - installare sull'host remoto la chiave pubblica.
 - file locale **.ssh/id_rsa.pub**
 - copia su host remoto
 - **scp .ssh/id_rsa.pub user@remote:**
 - append alla lista di utenti autorizzati (su *remote*)
 - **cat id_rsa.pub >> .ssh/authorized_keys**

Secure Shell – avvertenze

Il ruolo autenticante della password viene sostituito dalla presenza della chiave privata dell'utente sul client – la segretezza della password è quindi sostituita dalla riservatezza del file che contiene la chiave privata

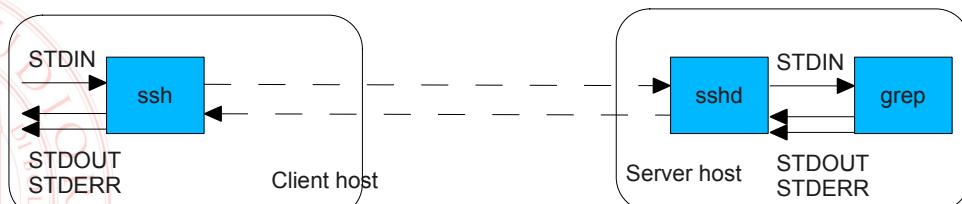
- ⇒ Grande cura nell'impostazione dei permessi di file e directory (nota di tipo pratico: spesso il passwordless login non funziona semplicemente perché i permessi sulla directory `.ssh` dell'host remoto sono troppo larghi, e quindi il server sshd “non si fida” dell'integrità del suo contenuto)
- ⇒ Possibilità di proteggere la chiave privata con una password
 - Vi priva della possibilità di passwordless login
 - Più sicuro comunque che utilizzare direttamente la password dell'account remoto, e più pratico se si amministrano molti host remoti

Secure Shell – esecuzione remota

- ⇒ Lanciando `ssh utente@host` si ottiene un *terminale remoto* interattivo.
- ⇒ Aggiungendo un ulteriore parametro, viene interpretato come **comando** da eseguire sull'host remoto al posto della shell interattiva; gli stream di I/O di tale comando vengono riportati attraverso il canale cifrato sul client.

Es: `ssh root@server "grep pattern"`

- I dati forniti attraverso STDIN al processo ssh sul client vengono resi disponibili sullo STDIN del processo grep sul server
- STDOUT e STDERR prodotti dal processo grep sul server “fuoriescono” dagli analoghi stream dal processo ssh sul client



Attacchi/2

Qualche esempio delle tecniche usate per violare le reti, e relative contromisure

Net security:
pagine 47-61

Marco Prandini

Sicurezza dei protocolli di rete

- Alcuni esempi di attacchi portati attraverso i protocolli di rete
 - Classico attacco: hijacking, cioè dirottamento della connessione perché passi attraverso i sistemi dell'attaccante
 - sfruttando i protocolli applicativi
 - direttamente (Es. HTTP attraverso manipolazione del browser)
 - attraverso i protocolli ausiliari (es. DNS)
 - sfruttando la mancanza di sicurezza di IP stesso

DNS spoofing

- Query e risposta

www.amazon.com?

207.171.166.48



DNS spoofing

- Risposta falsificata

www.amazon.com?

207.171.166.48



DNS spoofing (pharming)

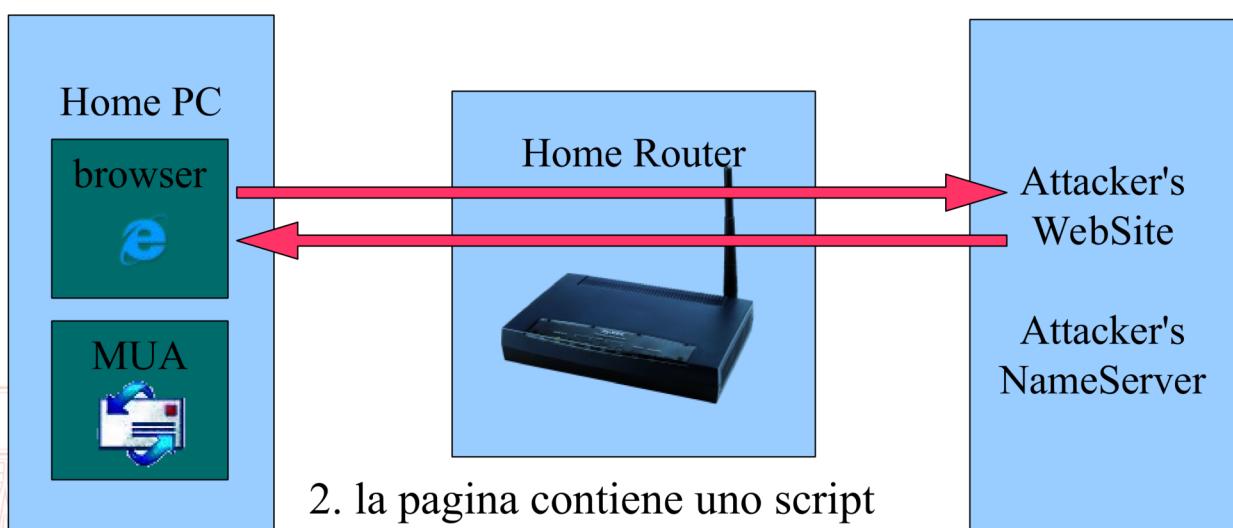
- Sembra difficile falsificare una risposta DNS?



1. L'utente visita una pagina HTML, consapevolmente o no

DNS spoofing (pharming)

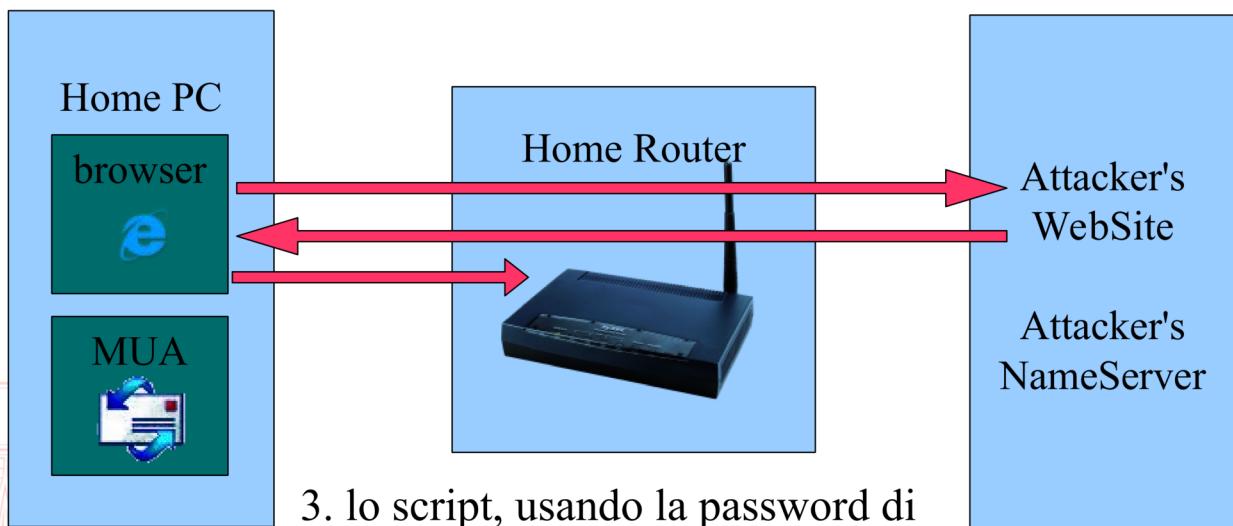
- Sembra difficile falsificare una risposta DNS?



2. la pagina contiene uno script

DNS spoofing (pharming)

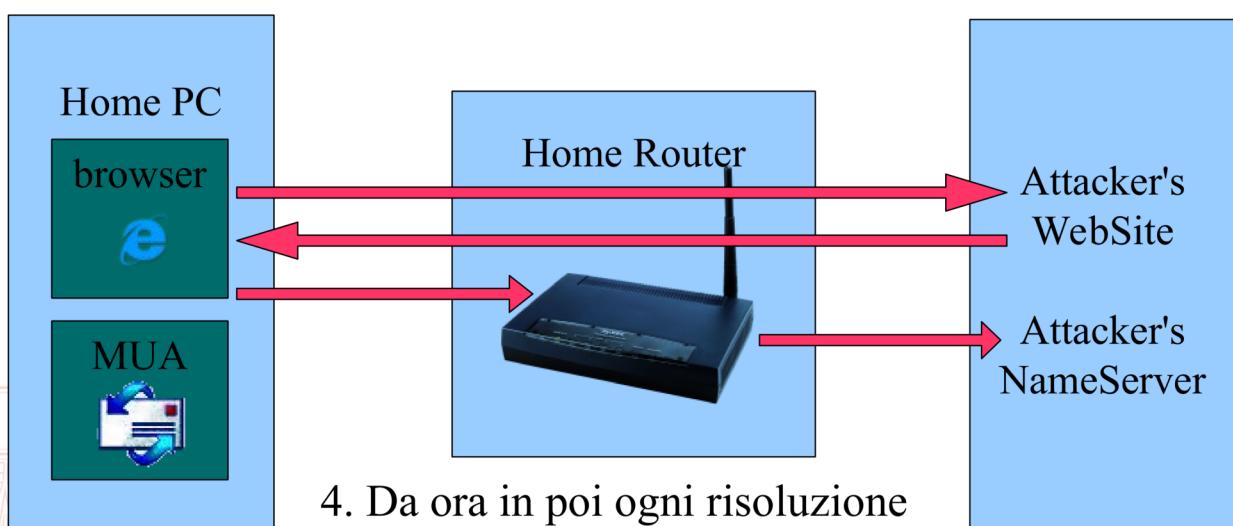
- Sembra difficile falsificare una risposta DNS?



3. lo script, usando la password di default del router, riprogramma il DNS

DNS spoofing (pharming)

- Sembra difficile falsificare una risposta DNS?



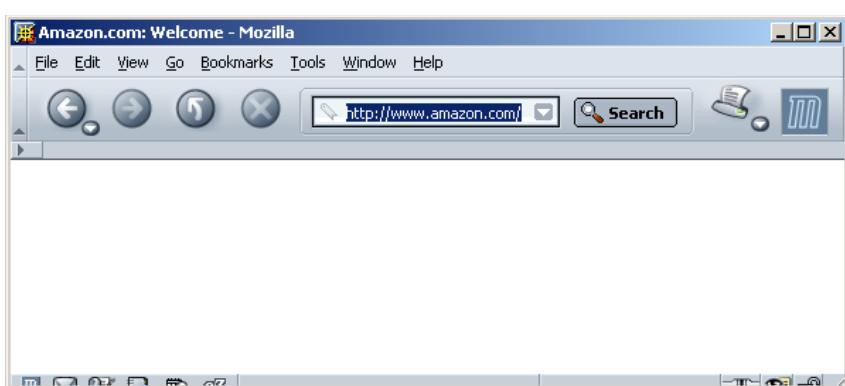
4. Da ora in poi ogni risoluzione sarà eseguita dal NS dell'attaccante

Contromisure e contro-contromisure

- HTTPS permette di bloccare questi attacchi
- ... ma esistono modi
 - per evitare che venga visualizzata l'URL effettivamente visitata
 - o per far accettare al browser qualsiasi certificato



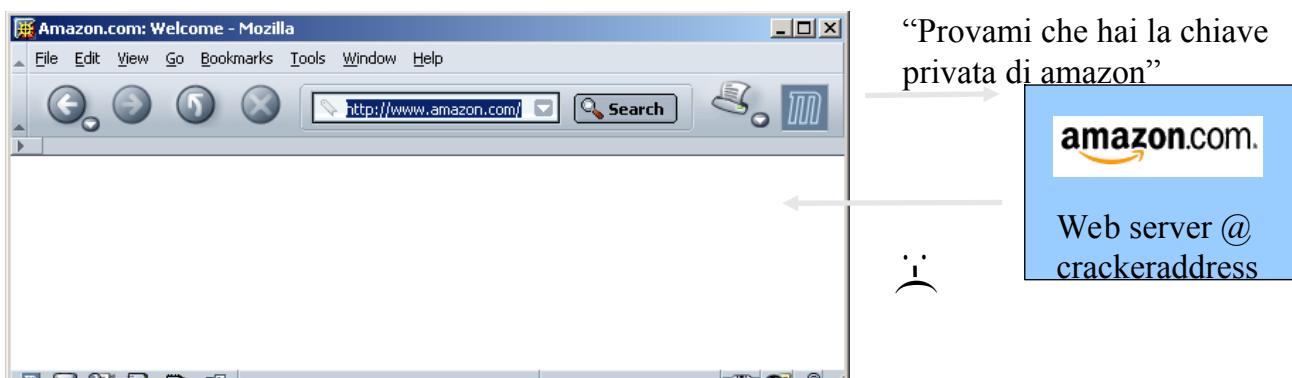
HTTPS



“Provami che hai la chiave
privata di amazon”



HTTPS



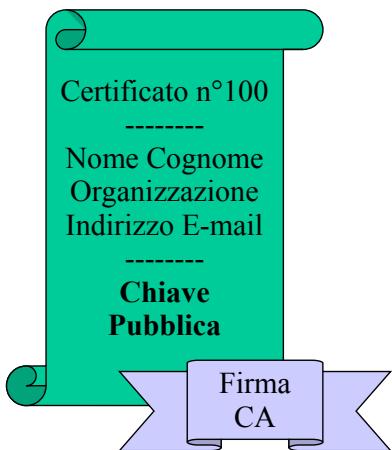
HTTPS



- Come fa il browser a verificare la prova fornita dal web server?
 - Certificate store
 - Trusted CAs



Certificazione della chiave pubblica



■ Certificato X.509

- Associa chiave e titolare
- Autenticità e integrità garantite dalla firma digitale di una terza parte fidata (**Certification Authority**)

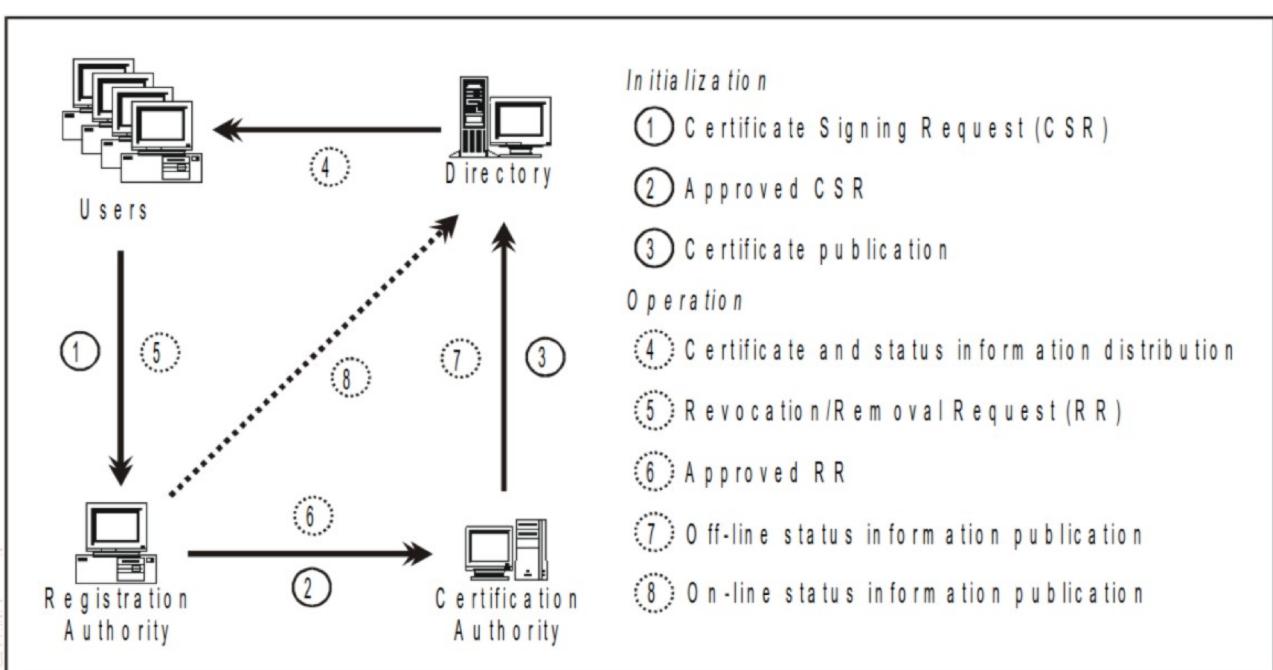
■ Per verificare la firma serve la chiave pubblica della CA

- Chi ci garantisce che questa sia autentica?

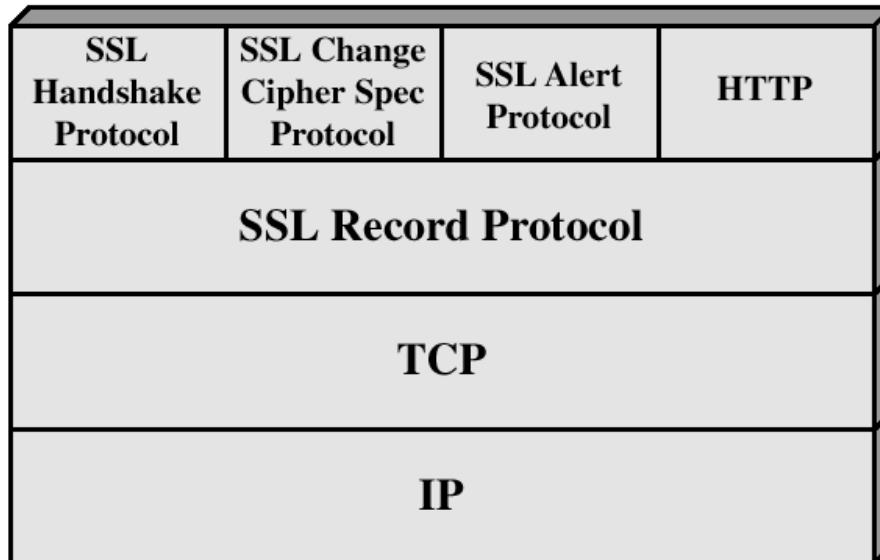
■ Serve una **Root of Trust**



PKI – ciclo di vita dei certificati

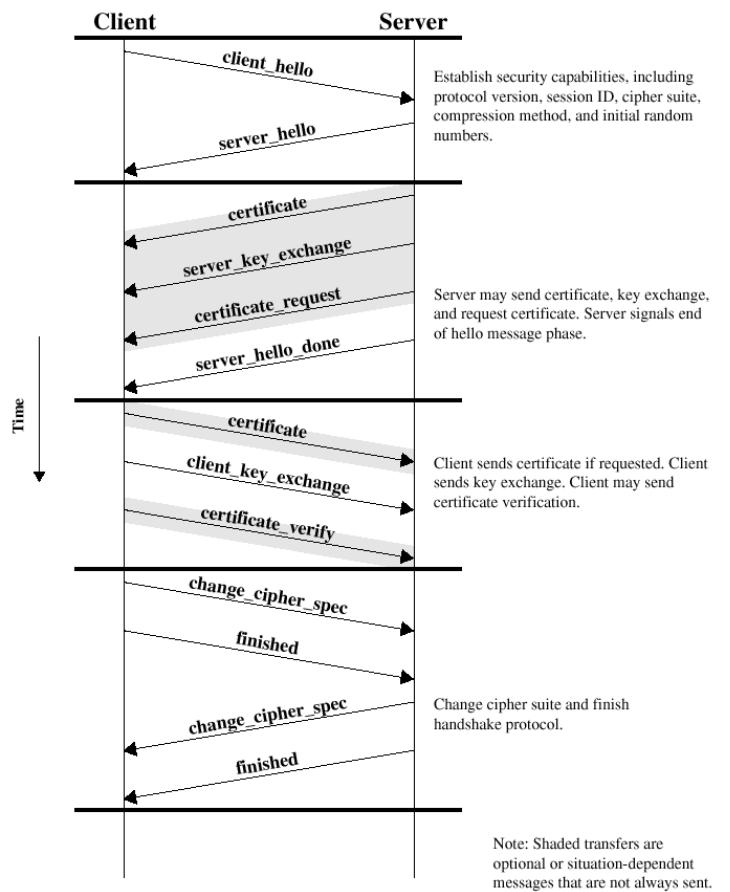


Architettura di SSL



Handshake Protocol

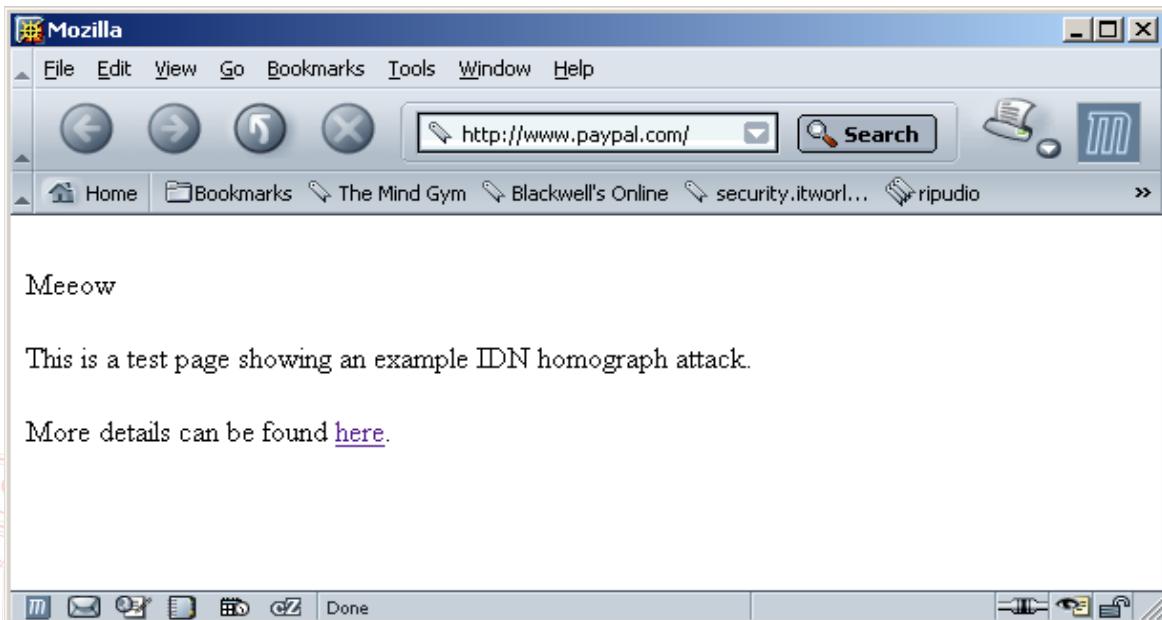
- La parte più complessa di SSL.
- Consente al server ed al client di autenticarsi reciprocamente
 - nelle applicazioni web è comune che il server provi la sua autenticità ed il client no
- Negozia gli algoritmi e le chiavi per la cifratura ed i controlli di integrità
- Interviene prima che qualsiasi dato sia trasmesso



Occultamento dell'URL

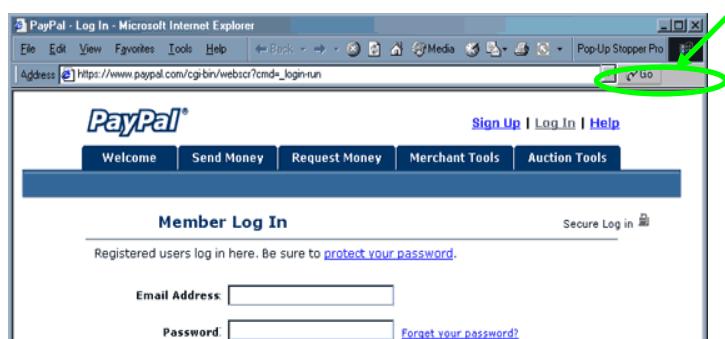
RFC3490/1/2: International Domain Names

ad esempio: <http://www.palypal.com/>



Occultamento della barra degli indirizzi

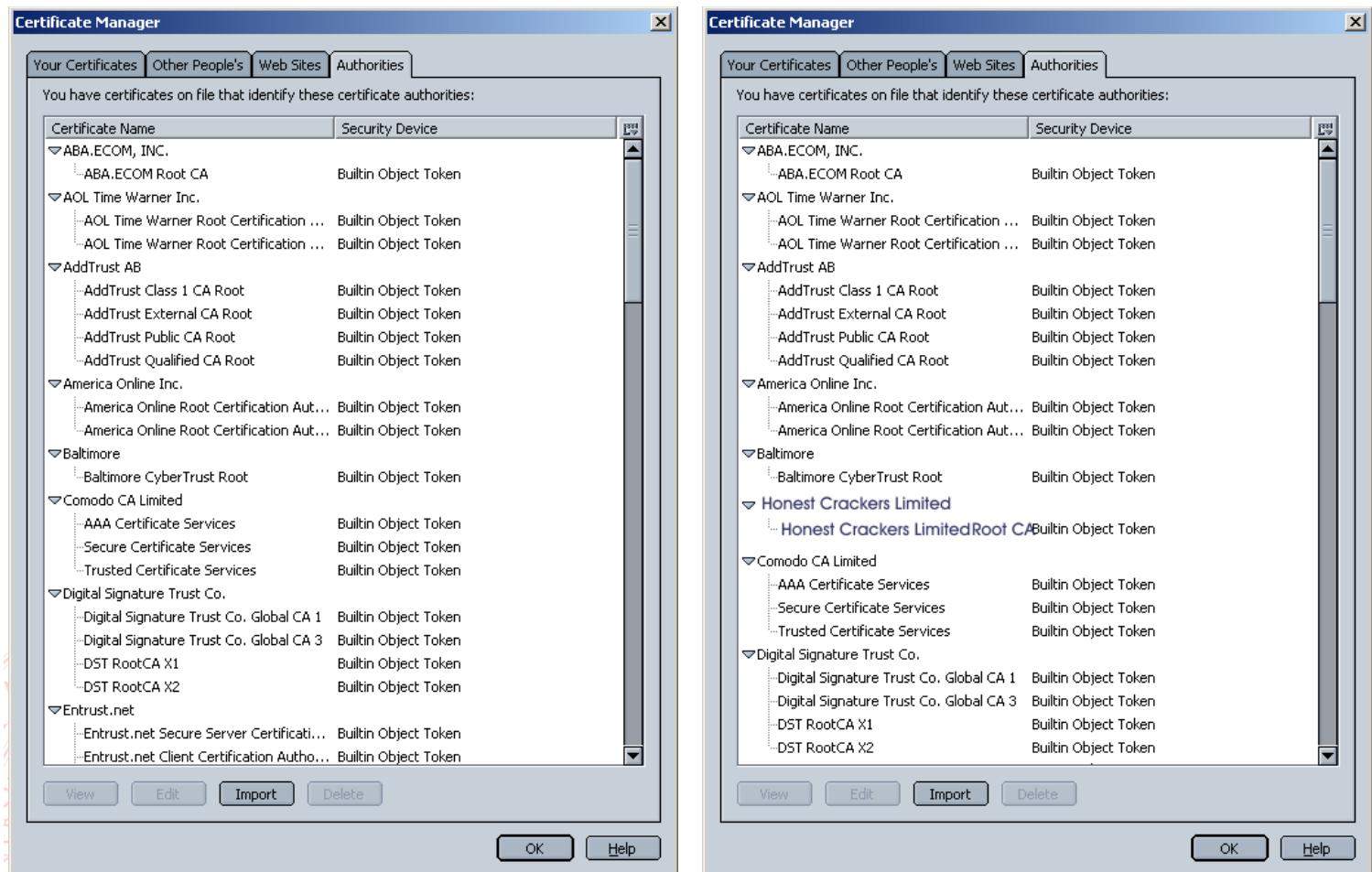
Il vecchio: qualche riga di codice js o activeX



Il nuovo: auto-hiding della barra nei browser mobili

<https://jamesfisher.com/2019/04/27/the-inception-bar-a-new-phishing-method/>

Iniezione di CA nel certificate store



Vulnerabilità di SSL – a livello di protocollo

■ DROWN (2016) - <https://drownattack.com/>

- Gravi vulnerabilità note nella vecchia versione SSLv2, originata dalle restrizioni imposte dal governo USA all'esportazione di crittografia forte
 - Possibile inviare probe che limitano lo spazio di ricerca delle chiavi a 40 bit
- Se tale versione è supportata su un server con una certa chiave privata, tutti i server che usano tale chiave sono vulnerabili
- Impatto: **controllo completo, impersonamento del server**

■ POODLE (2014)

- Un attaccante in grado di posizionarsi *in the middle* (ad esempio contro gli utenti di un hotspot pubblico) può forzare il downgrade delle connessioni verso SSLv3
- SSLv3 ha varie vulnerabilità sfruttabili
- Impatto: **controllo completo della connessione**

Vulnerabilità di SSL – a livello di implementazione

- Heartbleed (2014) - <http://heartbleed.com/>
 - Implementazione errata della rinegoziazione delle chiavi
 - Consente di leggere pezzi di memoria del sistema target
 - Impatto: possibile leak di materiale sensibile, come le chiavi
- Attacchi a livello IP
 - IP non può garantire nessuna proprietà di sicurezza ...
 - autenticità
 - integrità
 - riservatezza
 - ... di nessuna parte del pacchetto
 - header
 - payload
 - Esistono varianti che conferiscono queste proprietà, ma richiedono uno stack modificato

IP Hijacking

- Vari modi di *informare internet che la rotta verso una data subnet passa dal proprio AS, attraverso il protocollo BGP*
 - Autorità apparente di annunciare
 - Annuncio spontaneo (nessuno filtra!)
- Usi differenti:
 - Non malevolo: più veloce che chiedere IP al RIR :-)
 - Spamma e fuggi
 - DoS attivo o passivo
 - Impersonare un bersaglio
 - Man In The Middle
- Dirottamenti accidentali avvengono spesso: quindi basse probabilità di essere notati
- Qualche esempio storico disponibile su completowhois.com



Un esempio recente: Youtube & Pakistan Telecom

Dalla presentazione di Pilosov e Kapela a DEFCON16 (Las Vegas 2008)

- YouTube announces 5 prefixes:
- A /19, /20, /22, and two /24s
- The /22 is 208.65.152.0/22
- Pakistan's government decides to block YouTube
- Pakistan Telecom internally nails up a more specific route (208.65.153.0/24) out of YouTube's /22 to null0 (the routers discard interface)
- Somehow redists from static bgp, then to PCCW
- Upstream provider sends routes to everyone else...
- Most of the net now goes to Pakistan for YouTube, gets nothing!
- YouTube responds by announcing both the /24 and two more specific /25s, with partial success
- PCCW turns off Pakistan Telecom peering two hours later
- 3 to 5 minutes afterward, global bgp table is clean again

Link interessanti:

http://news.cnet.com/8301-10784_3-9878655-7.html

<http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf>

Come risolvere il problema?

- Reagendo:
 - Per avere l'attenzione dei grossi provider upstream possono volerci giorni, se non siete Youtube
- Prevenendo:
 - Filtrando gli annunci sulla base del contenuto (come essere certi della ragionevolezza?)
 - Autenticando i singoli pacchetti: ad esempio con IPSec

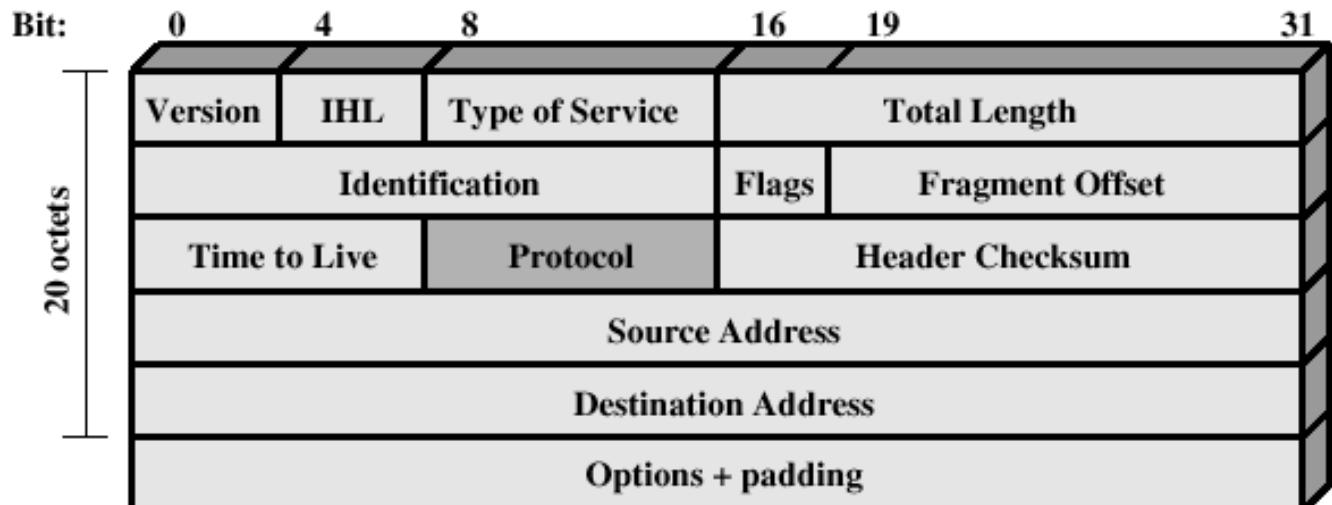


IP Security Overview

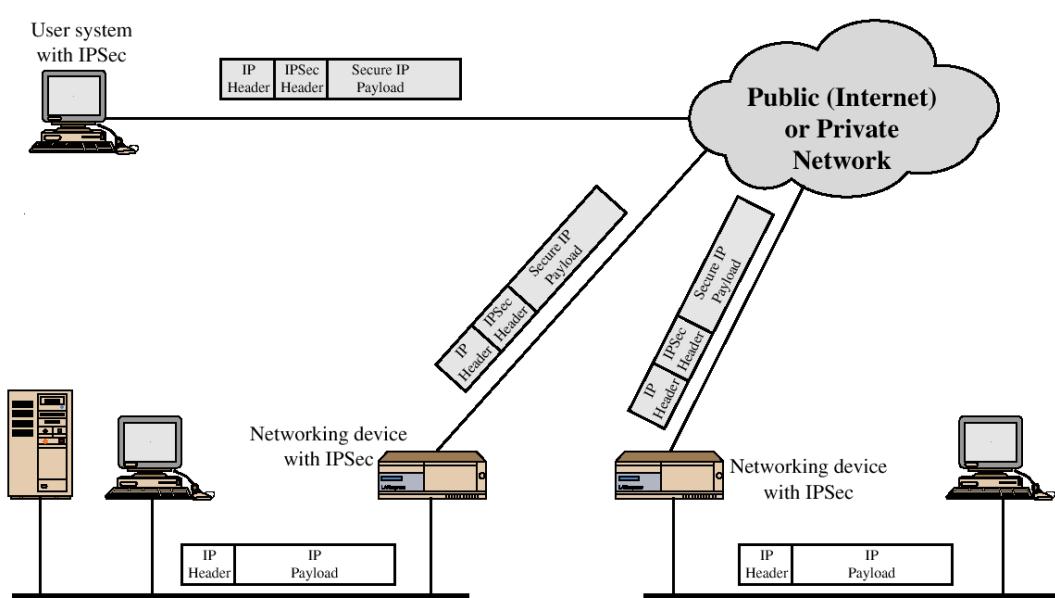
- IPSec non è un protocollo singolo
 - set di algoritmi di sicurezza
 - framework per la negoziazione degli algoritmi
 - specifiche per la gestione delle chiavi
- Applicazioni di IPSec
 - Interconnessione di sedi remote attraverso Internet
 - Accesso di client alla rete aziendale attraverso Internet
 - Creazione di reti complesse con criteri di protezione differenziati
- Vantaggi di IPSec
 - Trasparente alle applicazioni
 - Applicabile al traffico infrastrutturale di Internet, come i messaggi che i router si scambiano per aggiornare le tabelle di instradamento



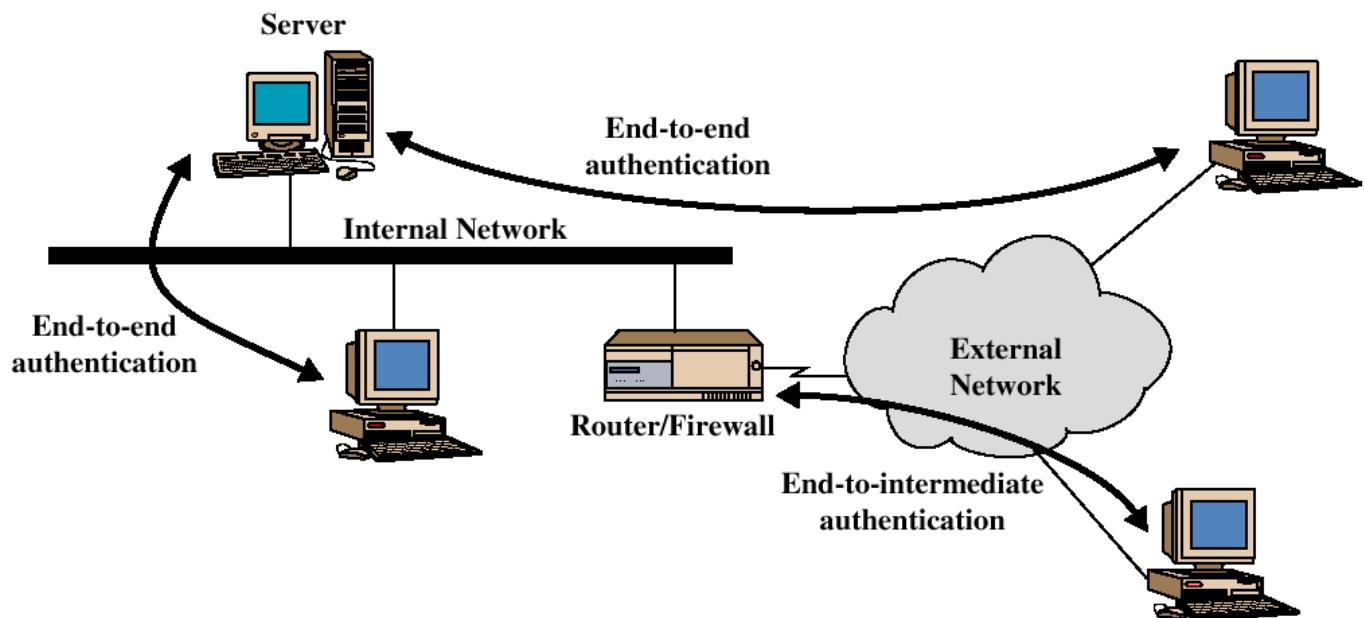
IPv4 Header



IPSec Scenario

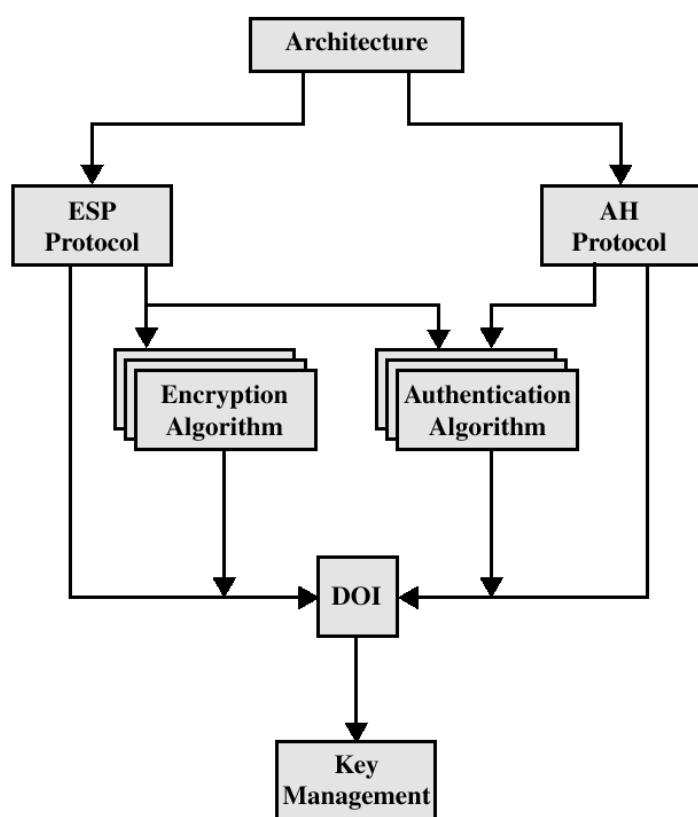


Utilizzo End-to-end / End-to-Intermediate

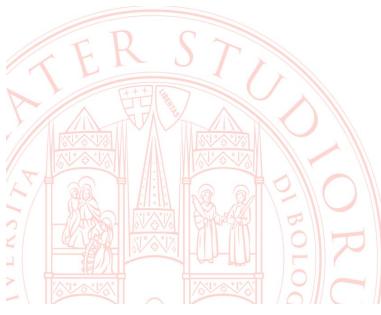


Gli standard di IPSec

- **IPSec documents:**
 - RFC 2401: An overview of security architecture
 - RFC 2402: Description of a packet encryption extension to IPv4/IPv6
 - RFC 2406: Description of a packet encryption extension to IPv4/IPv6
 - RFC 2408: Specification of key management capabilities



Servizi offerti ed algoritmi utilizzati

- 
- Controllo dell'accesso
 - Integrità anche senza connessione
 - Autenticazione dell'origine dei dati
 - Rilevazione dei replay
 - Riservatezza dei dati
 - Parziale riservatezza dei flussi di traffico
 - Cifratura:
 - Three-key triple DES
 - RC5
 - IDEA
 - Three-key triple IDEA
 - CAST
 - Blowfish
 - Autenticazione:
 - HMAC-MD5-96
 - HMAC-SHA-1-96
 - Gestione chiavi:
 - Manuale
 - Automatizzata
 - Oakley Key Determination Protocol
 - Internet Security Association and Key Management Protocol (ISAKMP)

Terminologia di base

- SA (Security Association)
 - relazione unidirezionale tra mittente e destinatario, definita da
 - Security Parameter Index (SPI)
 - IP Destination address
 - Security Protocol Identifier
 - due modalità possibili di SA
 - Transport Mode
 - Tunnel Mode
- Protocolli di sicurezza
 - AH (Authentication Header)
 - ESP (Encapsulating Security Payload)



Autentication Header

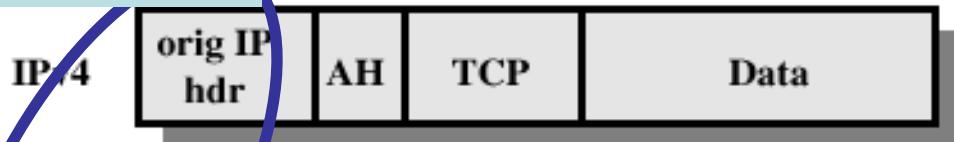
Gli indirizzi, giustamente, non sono considerati campi variabili

- vengono autenticati
- le alterazioni del NAT vengono percepite come violazioni dell'integrità



authenticated except for mutable fields →

Mode



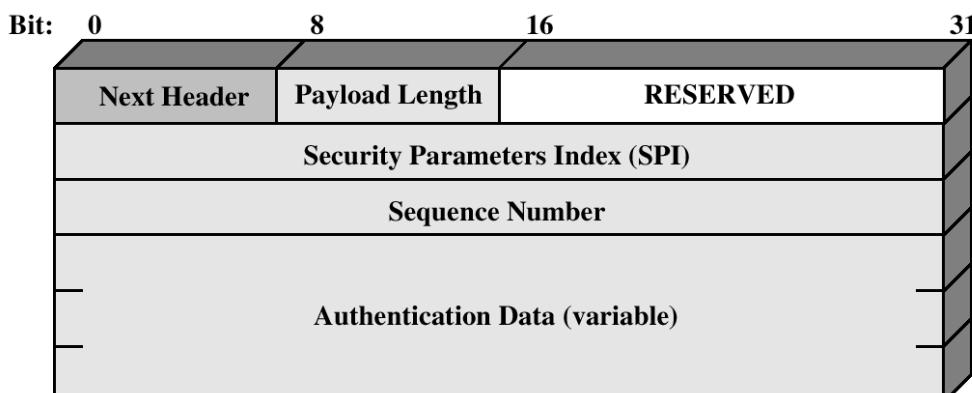
authenticated except for mutable
fields in the new IP header →

Tunnel
Mode



Authentication Header

- Garantisce l'autenticazione e l'integrità dei pacchetti IP
- Protegge dai replay attacks

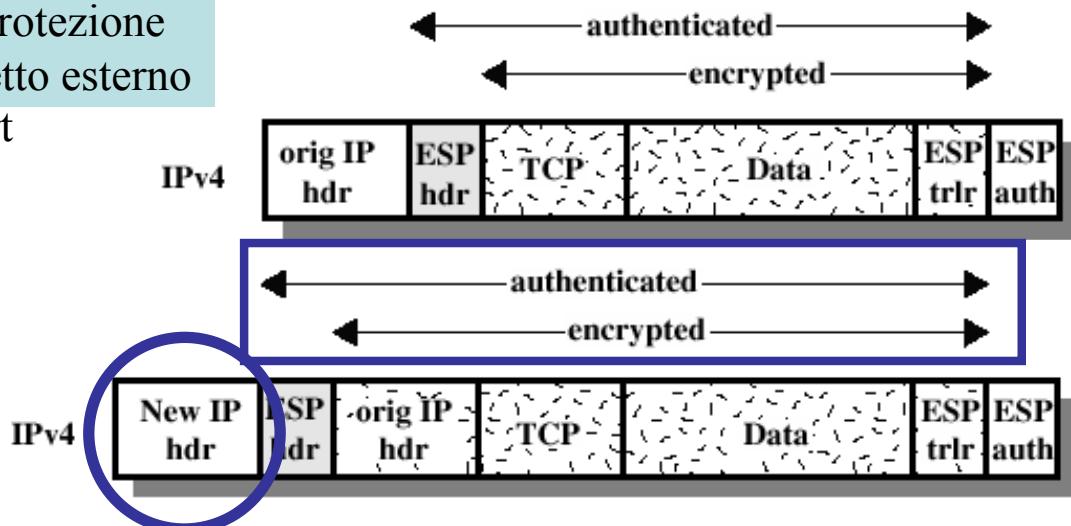


ESP con cifratura ed autenticazione

Nessuna protezione
del pacchetto esterno

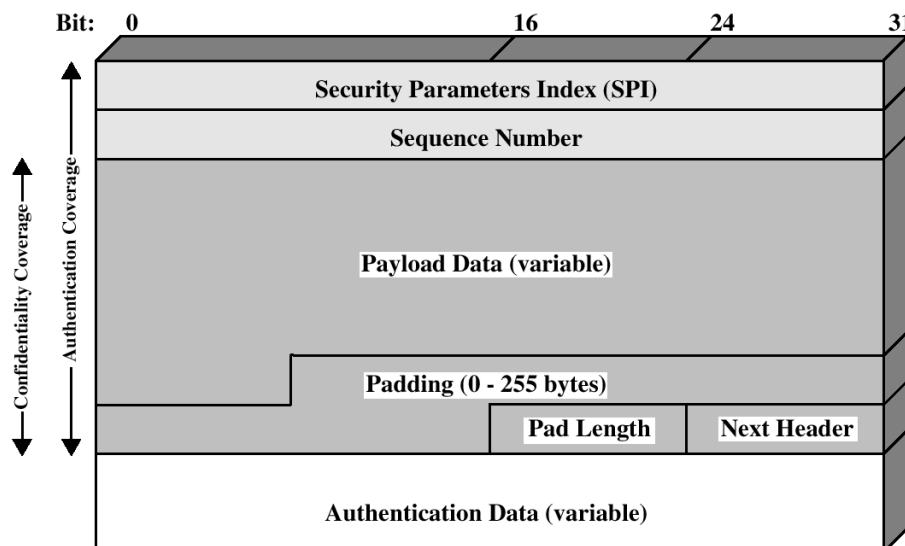
Transport
Mode

Tunnel
Mode



Encapsulating Security Payload

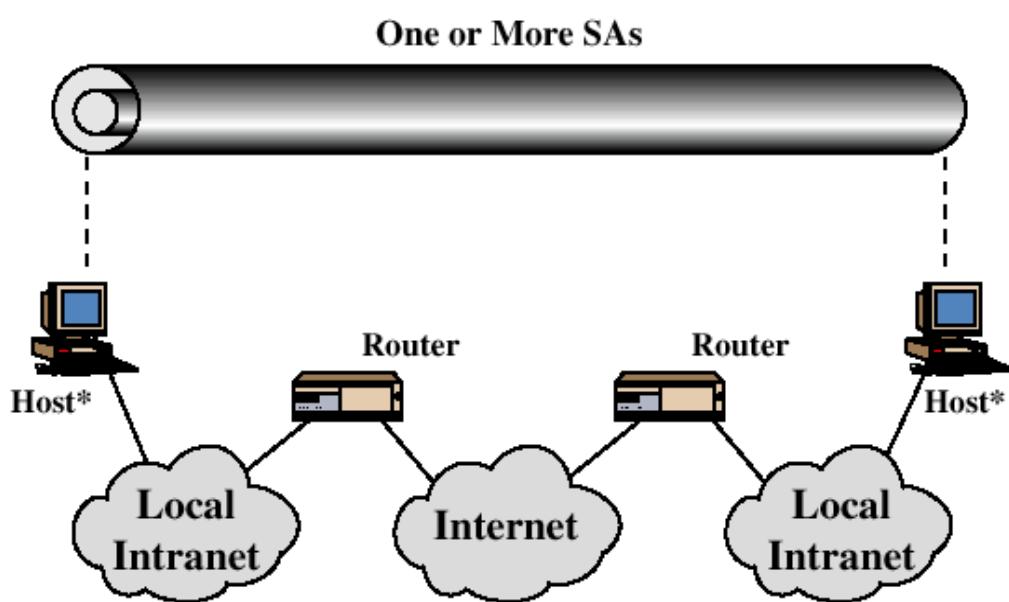
- ESP offre essenzialmente servizi per la riservatezza



Riassunto delle combinazioni dei modi di protezione

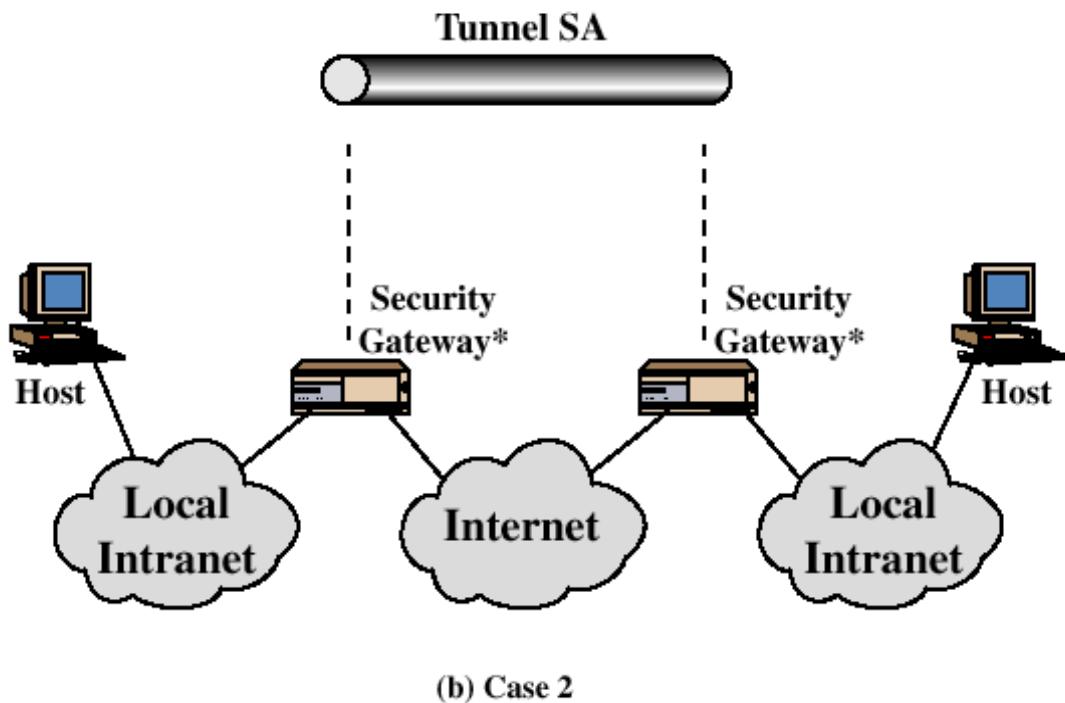
	Transport Mode SA	Tunnel Mode SA
AH	Autentica il payload del pacchetto IP ed alcuni campi dell'header IP	Autentica l'intero pacchetto IP interno ed alcuni campi del pacchetto IP esterno
ESP	Cifra il contenuto del pacchetto	Cifra l'intero pacchetto IP interno
ESP with authentication	Cifra il contenuto del pacchetto. Autentica il payload del pacchetto ma non l'header IP	Cifra ed autentica l'intero pacchetto IP interno.

Combinazione di Security Associations

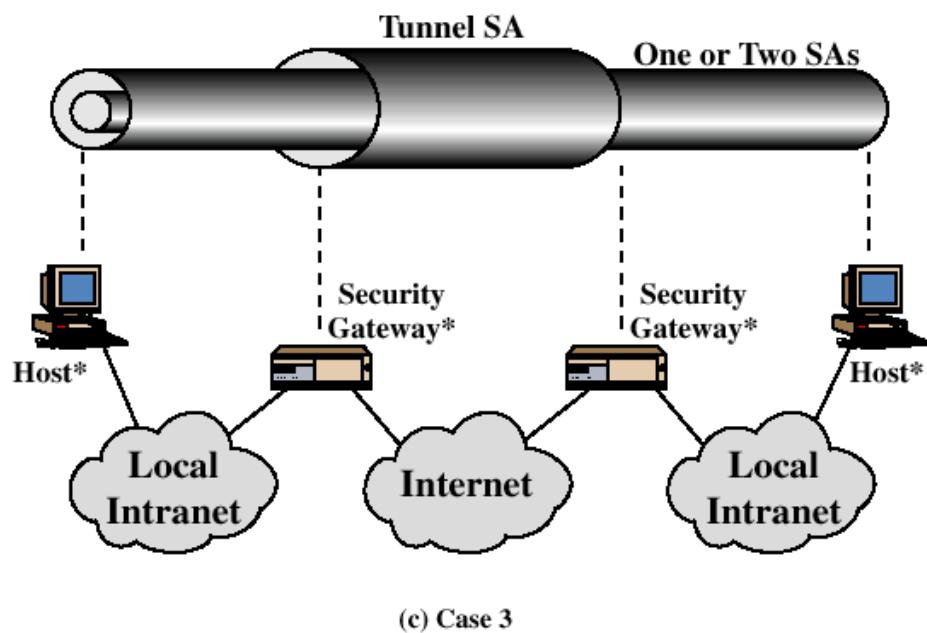


(a) Case 1

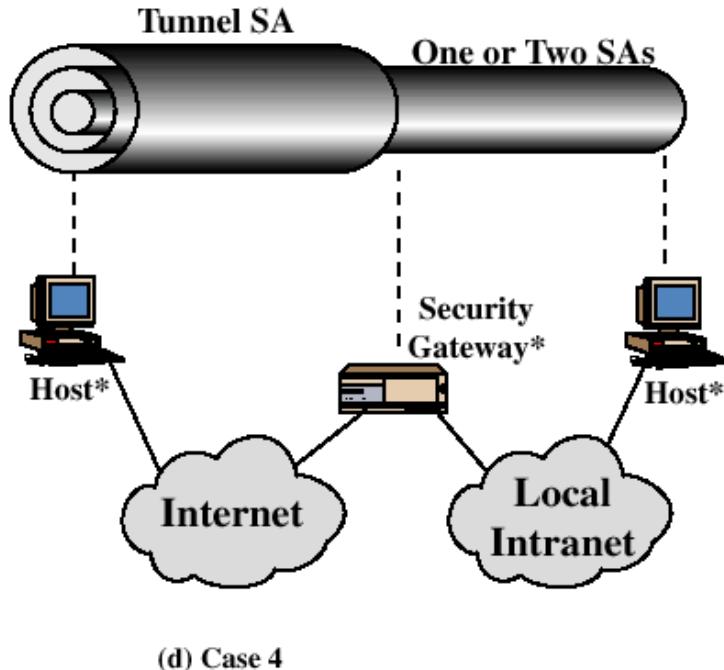
Combinazione di Security Associations



Combinazione di Security Associations



Combinazione di Security Associations



Considerazioni comparative

- **SSL/TLS**
 - è specifico di un dominio applicativo ☹
 - è semplice e realmente standard ☺
- **IPSec**
 - è generale e trasparente alle applicazioni ☺
 - è tipicamente implementato nello stack TCP/IP del sistema operativo, con variazioni che rendono difficile l'interoperabilità ☹
- **Soluzioni "ibride"**
 - utilizzo di varianti di SSL per il trasporto di pacchetti IP analogo al tunnel mode di IPSec
 - implementazione user space, indipendente dal S.O.
 - Es: OpenVPN

Laboratorio di Sicurezza Informatica



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Sicurezza fisica e collocazione delle risorse

Marco Prandini

Dipartimento di Informatica – Scienza e Ingegneria

On premises vs. in the cloud

- Abbiamo visto sistemi di controllo dell'accesso alle informazioni; ricordiamo che sono tutti "mediati"
 - dal sistema operativo (es. permessi su file)
 - dalla gestione di segreti (es. chiavi crittografiche)
- Come influsce la collocazione delle risorse?
- On premises:
 - nessuna condivisione
 - relativa semplicità di separazione tra segreti e sistemi e dati
 - inserimento manuale di password e chiavi
 - necessità di garantire
 - il corretto funzionamento dell'hardware
 - l'esecuzione di sistemi operativi e software integri e autentici
- In the cloud
 - gestione hw/sw di altissimo livello
 - ambienti di memorizzazione ed elaborazione condivisi
 - delocalizzazione



On premises - messa in sicurezza fisica

- Un server è prima di tutto un sistema di calcolo, collocato in un ambiente e connesso a una varietà di dispositivi
 - Normalmente si concentrano le difese sul fronte degli attacchi via rete, a componenti software come applicazioni e sistema operativo
 - Le corrispondenti contromisure possono facilmente essere scavalcate da un attaccante con accesso fisico al sistema!
 - Le minacce principali sono:
 - Furto dello storage o dell'intero calcolatore
 - Connessione di sistemi di raccolta dati alle interfacce
 - Avvio del sistema con un sistema operativo arbitrario
 - La gravità di queste minacce dipende fortemente dallo specifico ambiente
- Molti di questi problemi sono cambiati nello scenario sempre più comune di virtualizzazione sul Cloud, ma altri concettualmente simili sono apparsi, e la logica delle stesse contromisure si può adattare

3

Fattori non informatici

- Vedremo che l'accesso a sistema permette attacchi specifici
- Come si ottiene l'accesso?
 - Insider
 - Tailgating
 - Errata identificazione di visitatori
 - Social engineering
 - Effrazione
- La sicurezza fisica “tradizionale” è essenziale!
 - Regolamenti chiari e condivisi
 - Perimetro robusto
 - Sorveglianza e procedure

<https://docs.microsoft.com/it-it/azure/security/fundamentals/physical-security>

- La disponibilità è il terzo vertice della triade CIA
 - Alimentazione
 - Connettività
 - Condizionamento
 - Incidenti, disastri, attentati <https://goo.gl/maps/5Ukzcorg5pZNmbzW7>

4

Alcune vulnerabilità sfruttabili in presenza

■ BadUSB e simili

<https://threatpost.com/badusb-attack-code-publicly-disclosed/108663/>

■ Thunderspy

<https://thunderspy.io/>

■ Keylogging e videoghosting

<https://www.keelog.com/>

■ Key injection

<https://www.blackhillsinfosec.com/executing-keyboard-injection-attacks/>

■ Disk un/plugging

<https://www.blackhat.com/docs/eu-15/materials/eu-15-Boteanu-Bypassing-Self-Encrypting-Drives-SED-In-Enterprise-Environments-wp.pdf>

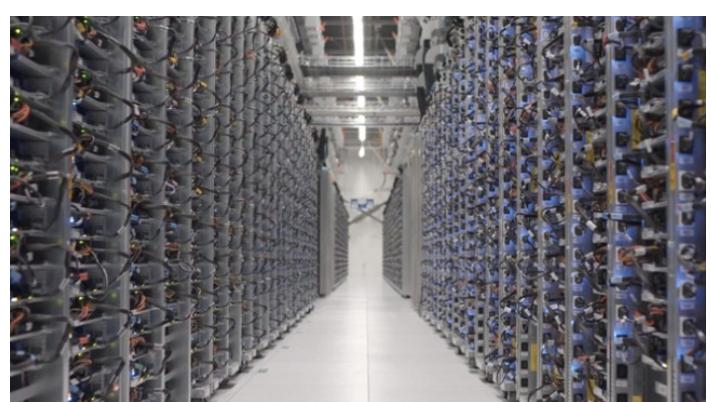
■ Power glitching

<https://www.darkreading.com/edge/theedge/glitching-the-hardware-attack-that-can-disrupt-secure-software-/b/d-id/1336119>



5

In remoto



■ Se la collocazione è fuori dalla possibilità di controllo diretto, si può considerare di:

- Scegliere un case che possa essere chiuso e fissato al rack
- Installare dispositivi di rilevazione delle intrusioni
- Adottare misure di protezione dei dati che rendano inutile il furto
 - L'accesso ai dati va però abilitato manualmente
- Disabilitare le periferiche non utilizzate
 - Salvo poi averne bisogno per esigenze nuove

6

Attacchi fisici alle risorse logiche

- Per andare a regime il sistema attraversa un processo di boot, che può essere diviso in queste fasi:
 - (1) BIOS – Individua i dispositivi di possibile caricamento del boot loader e l'ordine per esaminarli
 - Molti BIOS prevedono la possibilità di proteggere con password l'avvio o la modifica della configurazione
 - (2) Boot Loader – Sceglie il sistema operativo e gli passa eventuali parametri
 - Gestione della “maintenance mode”
 - Stesso tipo di protezione con password come descritto per BIOS
 - (3) Sistema operativo – carica i device driver (da non sottostimare) e avvia il processo *init*
 - (4) *init* – gestisce i *runlevel* o i *target* per coordinare l'inizializzazione del sistema, cioè avviare i servizi nell'ordine corretto
- Ognuna di queste fasi potrebbe essere **dirottata** da un attaccante con accesso fisico, per far caricare software malevolo

7

Boot

- Password pro e contro:
 - Se serve una password per l'avvio del sistema, il funzionamento non supervisionato può essere problematico: ad esempio può non ripartire per ore dopo una semplice mancanza di alimentazione
 - In sistemi con gravi esigenze di sicurezza, non sarà comunque l'unica password da fornire, quindi meglio proteggere tutti gli strati
 - Almeno la protezione contro i cambi di configurazione è sempre consigliabile
- MAI affidarsi a un unico strato di protezione
 - Le password del BIOS hanno meccanismi semplici di reset
 - Possono essere indovinate...

8

Bootloader – configurazione (runtime)

- LILO, the Linux Loader
 - Usato fin dagli albori di Linux
- GRUB, the Grand Unified Bootloader
 - GRUB è più potente e flessibile di LILO, è dotato di una shell che permette di eseguire vari comandi per modificare al volo la procedura di avvio: naturalmente questo permette molti abusi
- Entrambi permettono di passare parametri al kernel, i più importanti ai fini della sicurezza sono
 - single
 - Init=...
- Alcune distribuzioni hanno default rischiosi, ad esempio se si riesce a innescare un *maintenance mode* aprono una shell di root senza chiedere password

9

Boot Loader passwords

■ LILO

`password=YourPasswordHere`

Imposta una password richiesta al boot, a meno che

`restricted`

non sia `is` specificato, in tal caso la password è richiesta solo per modificare i parametri durante il boot.

■ Global vs. Single-entry

- `password` e `restricted` nella “global section”: chiede la password prima di consentire l’aggiunta di parametri – attenzione alle entry non sicure (`cd`)
- `password` e `restricted` in una “image section”: chiede la password prima di consentire l’aggiunta di parametri, solo per l’immagine specificata
- `password` nella “global section” e `restricted` in una “image section”: chiede la password prima di consentire l’aggiunta di parametri, solo per l’immagine specificata, mentre chiede sempre la password per avviare altre immagini

10

Boot Loader passwords

■ GRUB

`password [--md5] passwd [new-config-file]`

Se specificato nella “global section”, imposta una password che sarà richiesta per attivare l’*interactive operation* del bootloader. Opzionalmente può innescare il caricamento di un file di configurazione alternativo

Se specificata per un item specifico del menu, imposta una password che sarà richiesta per avviare quell’item

`lock`

Se specificata per un item specifico del menu, subito dopo `title`, contrassegna quell’item come password-protected.

Funziona solo se esiste una direttiva `password` nella “global section”

`md5crypt`

Comando utilizzabile al grub prompt per calcolare il password hash da usare con `--md5`



11

Sicurezza del processo di boot

■ Problema: come assicurarsi che ogni componente software eseguito da un computer sia autentico, integro e benevolo?

- Anti-malware verificano le applicazioni
- Chi verifica gli anti-malware?? Il S.O. (idealemente rendendo AM inutile)
- Chi verifica il S.O.? Il boot loader potrebbe
- Chi verifica il boot loader? Il BIOS potrebbe, specialmente se assistito da HW speciale, che non possa essere modificato dal S.O., e quindi sia immune da infezioni

→ *hardware root of (a chain of) trust*

https://medium.com/@martin_24447/trusted-boot-b1ae7e6d2890



<https://dl.acm.org/doi/pdf/10.1145/3380774.3382016>

12

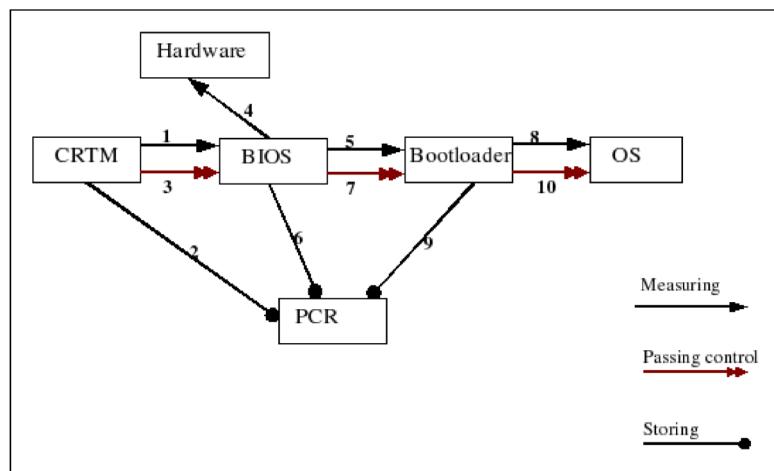
Measured / Trusted / Secure Boot

- **Measured Boot** si riferisce a un processo generale, che tipicamente usa un **TPM** come hardware root of trust
 - TPM = Trusted Platform Module: chip con funzionalità crittografiche
 - fa parte delle specifiche del *Trusted Computing Group*
<https://trustedcomputinggroup.org/>
 - M.B. non definisce come prevenire un avvio malevolo
- **Trusted Boot** è un processo che usa gli strumenti del M. B. e riesce a bloccare il boot non appena individua un componente non fidato
- **Secure Boot** è il nome specifico dato all'implementazione di trusted boot basata su **UEFI**
 - UEFI = Unified Extensible Firmware Interface
<http://www.uefi.org/>
 - Implementazione Software + chiavi in firmware
 - Serve un BIOS standard per la fase di POST
 - Può avvalersi del TPM per velocizzare e migliorare i controlli di integrità

13

Measured boot

- Basato sul TPM
 - Core Root of Trust for Measurement (**CRTM**)
 - Registers (**PCR**)
- Raccoglie hash di ogni componente caricato
 - nei PCR che sono fisicamente non modificabili una volta scritti
- Pospone i controlli fintanto che non dispone
 - Delle crypto keys
 - Di abbastanza memoria per fare i calcoli necessari
- Si può decidere chi fa i controlli e quando
 - per esempio dall'esterno (sistema fidato) per abilitare funzioni critiche
 - **remote attestation!**



14

UEFI e secure boot

- UEFI (Intel) nasce come interfaccia più flessibile del BIOS tra S.O. e firmware
- UEFI forum standardizza e aggiorna la specifica
- UEFI è un “mini OS”
 - milioni di righe di codice
 - standard per molte piattaforme
 - bersaglio ideale degli attaccanti!

https://media.kaspersky.com/en/business-security/Threats_to_UEFI.pdf

<https://www.csoonline.com/article/3599908/trickbot-gets-new-uefi-attack-capability-that-makes-recovery-incredibly-hard.html>

<https://www.debian.org/security/2021-GRUB-UEFI-SecureBoot/>

- UEFI verifica ogni componente software prima di passare il controllo a BootLoader/SistemaOperativo
 - Richiede la disponibilità di un database di chiavi
 - Blocca il boot appena rileva una difformità

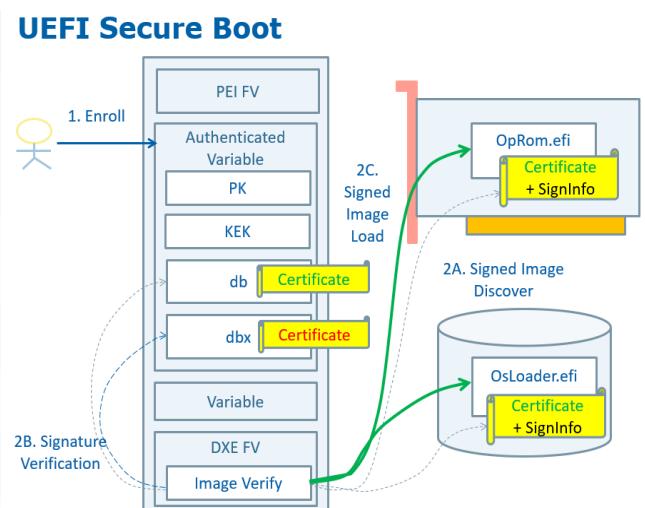
15

Le chiavi di UEFI Secure Boot

https://edk2-docs.gitbook.io/understanding-the-uefi-secure-boot-chain/secure_boot_chain_in_uefi/uefi_secure_boot

- UEFI Secure Boot definisce due processi di sicurezza:
 - verifica dell’immagine di boot
 - verifica degli aggiornamenti al database della sicurezza delle immagini
- Per fare questo si avvale di differenti database e set di chiavi

Key	Verifies	Update is verified by	NOTES
PK	New PK New KEK New db/dbx/dbt/dbr New OsRecoveryOrder New OsRecovery#####	PK	Platform Key
KEK	New db/dbx/dbt/dbr New OsRecoveryOrder New OsRecovery#####	PK	Key Exchange Key
db	UEFI Image	PK/KEK	Authorized Image Database
dbx	UEFI Image	PK/KEK	Forbidden Image Database
dbt	UEFI Image + dbx	PK/KEK	Timestamp Database
dbr	New OsRecoveryOrder New OsRecovery#####	PK/KEK	Recovery Database



16

UEFI Secure Boot Image Verification

https://edk2-docs.gitbook.io/understanding-the-uefi-secure-boot-chain/secure_boot_chain_in_uefi/uefi_secure_boot

- Entità coinvolte nel processo di verifica delle immagini al boot
 - TP = trusted platform, procedura di verifica
 - CDI = UEFI Secure Boot Image Security Database
 - UDI = qualsiasi firmware di terze parti, inclusi boot loader, PCI option ROMs, o UEFI shell tool.
- Al boot, TP verifica l'integrità di UDI utilizzando le policy CDI
 - se ok, UDI entra a far parte di CDI e il firmware di terze parti viene eseguito
- Il CDI, cioè il database delle politiche di sicurezza da applicare alle immagini software da caricare, è quindi aggiornabile.
 - Il fornitore del componente deve firmarlo con la propria chiave privata e rendere disponibile la chiave pubblica.
 - La chiave pubblica deve essere iscritta (enrolled) nel firmware del sistema
 - normalmente questo passaggio richiede un reboot in una modalità speciale e l'intervento sulla console, bloccando quindi l'azione di utenti malevoli ma senza accesso fisico al sistema

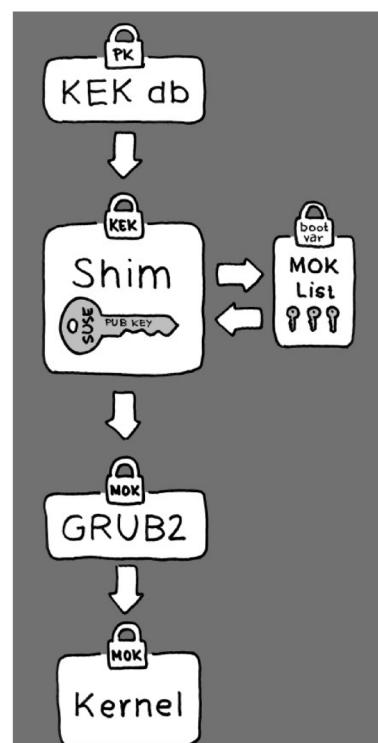
Item	Entity	Provider	Location
TP	UEFI Secure Boot Image Verification	OEM	Originally on flash, loaded into DRAM
CDI	Manufacture Firmware Code	OEM	Originally on flash, loaded into DRAM
	UEFI Secure Boot Image Security Database (Policy)	End user (or OEM default)	Originally on flash, authenticated variable region, loaded into DRAM
UDI	3rd party Firmware Code, (OS boot loader)	OSV	Originally on external storage (e.g. Hard drive, USB), loaded into DRAM
	3rd party Firmware Code, (PCI Option ROM)	IHV	Originally on PCI card, loaded into DRAM
	3rd party Firmware Code, (UEFI Shell Tool)	Any	External Storage (e.g. hard drive, USB), loaded into DRAM

7

UEFI e secure boot in Linux

https://www.suse.com/media/presentation/uefi_secure_boot_webinar.pdf
<https://wiki.ubuntu.com/UEFI/SecureBoot>

- 1) La Platform Key ufficiale verifica un piccolo pre-boot-loader, **shim**
 - La chiave key usata per “firmare” shim deve essere fornita dal costruttore HW
 - È una chiave Microsoft!
 - 2) Shim può usare o trasferire MOKs (Machine Owner Keys)
 - Per validare il bootloader
 - Per validare moduli custom del kernel
- Componenti aggiuntivi del kernel devono essere firmati per poterli caricare
 - L'utente genera le MOKs
 - L'utente deposita le MOKs in shim
 - Al boot successivo, shim trova le chiavi nella fase di setup, e chiede conferma per salvarle in firmware → **consenso esplicito e basato su password sempre richiesto!**



<https://www.suse.com/communities/blog/uefi-secure-boot-details/>

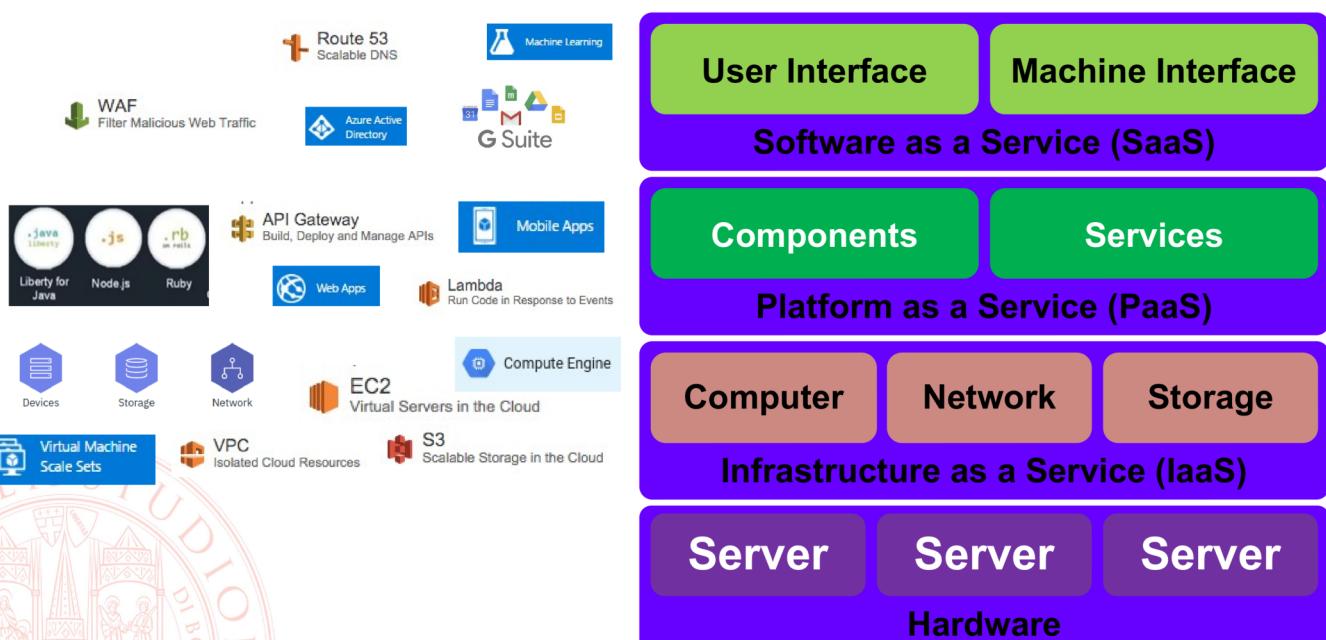
UEFI / Secure boot links

- E-book con schemi chiari e riferimenti a proprietà formali di sicurezza secondo il modello di Clark-Wilson garantite dal procedimento
 - <https://edk2-docs.gitbook.io/understanding-the-uefi-secure-boot-chain/>
- Documentazione originale
 - https://uefi.org/sites/default/files/resources/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2013.pdf
- Articoli datati ma illustrano i problemi incontrati all'introduzione di UEFI
 - <http://www.rodsbooks.com/linux-uefi/>
 - <http://www.linux-magazine.com/Online/Features/Coping-with-the-UEFI-Boot-Process>
 - <https://help.ubuntu.com/community/UEFI>
 - <http://askubuntu.com/questions/760671/could-not-load-vboxdrv-after-upgrade-to-ubuntu-16-04-and-i-want-to-keep-secure>
 - <https://www.suse.com/communities/blog/uefi-secure-boot-details/>
 - <https://lwn.net/Articles/519618/>
- Guide alla personalizzazione
 - <https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF>
 - <https://www.linuxjournal.com/content/take-control-your-pc-uefi-secure-boot>



Due parole su cloud security

- A seconda del livello utilizzato, molti problemi “svaniscono”



Sicurezza: cloud vs. on-premise

- I problemi di sicurezza del cloud riguardano raramente la sicurezza dell'host e della rete
- Impatto "emotivo" della distanza
 - perdita di controllo
- Osservazione razionale
 - il più delle volte, i fornitori di cloud hanno team di sicurezza di livello mondiale che quasi nessuna azienda può permettersi di assumere per i propri data center
- La due diligence suggerisce di verificare questa affermazione quando si seleziona un fornitore di servizi cloud!
 - Certificazione ISO27001 + ambito di applicazione
 - risultati di un audit SAS70 di tipo II
- Paradossalmente, alcune minacce reali riguardano la disponibilità
 - lock-in
 - dipendenza dalla rete
 - cessazione dell'attività

I benefici potenziali del cloud per la sicurezza

- Le misure di sicurezza sono più economiche se implementate su scala più ampia:
 - Collocazioni multiple = ridondanza di istanze e dati = indipendenza dai guasti dovuti a comportamenti dannosi, opportunità di ripristino
 - Tempestività migliorata: è possibile utilizzare sistemi su scala più ampia per sviluppare capacità di risposta agli incidenti più efficaci
 - Gestione delle minacce: i fornitori di servizi cloud possono coinvolgere specialisti nella gestione di minacce alla sicurezza specifiche
- La sicurezza come elemento di differenziazione sul mercato
 - Il cliente del servizio cloud (CSC) effettuerà le scelte di acquisto di servizi e risorse sulla base della reputazione di riservatezza, integrità e resilienza del fornitore di servizi cloud (CSP), nonché dei servizi di sicurezza offerti da CSP
 - Questo è un forte motore per i CSP per migliorare le pratiche di sicurezza

I benefici potenziali del cloud per la sicurezza

■ Aggiornamenti più tempestivi ed efficaci

- Le immagini delle macchina virtuale possono essere pre-rafforzate e aggiornate con le ultime patch e impostazioni di sicurezza in modo centralizzato, riducendo al minimo le vulnerabilità
- IaaS può fornire un servizio per consentire l'acquisizione regolare di istantanee dell'infrastruttura virtuale, nonché la rapida implementazione di numerosi aggiornamenti su piattaforme omogenee

■ Concentrazione delle risorse e rapido ridimensionamento

- La concentrazione delle risorse consente l'applicazione più semplice ed economica di controlli di sicurezza completi e policy sui processi di manutenzione, gestione degli incidenti e gestione delle patch
- CSP può scalare dinamicamente i meccanismi difensivi su richiesta per il traffic shaping, il filtraggio, la crittografia, ecc., al fine di aumentare il supporto per le misure di riparazione durante un attacco
- Quando queste capacità sono combinate con un appropriato schema di ottimizzazione delle risorse, il CSP può limitare l'effetto che alcuni attacchi potrebbero avere sulla disponibilità delle risorse che ospitano i servizi cloud, nonché limitare l'uso delle risorse necessarie per affrontare tali attacchi

I benefici potenziali del cloud per la sicurezza

■ Sicurezza come servizio e raccolta di prove

- I CSP di grandi dimensioni possono offrire come servizio interfacce standardizzate per la sicurezza gestita; questo potenzialmente crea un mercato per i servizi di sicurezza, dove i CSC possono facilmente acquisire controlli di sicurezza preconfigurati con costi di set-up inferiori
- IaaS può offrire supporto per la sicurezza su richiesta, clonare macchine virtuali (VM) e fornire uno storage conveniente per i log, che può essere utilizzato per analisi forensi offline, senza compromettere le prestazioni

■ Gli SLA impongono una migliore gestione del rischio

- I CSP implementano procedure di audit interno e valutazione del rischio più rigorose per quantificare le sanzioni per gli scenari di rischio negli SLA e definire azioni correttive per ridurre il possibile impatto delle violazioni della sicurezza sulla propria reputazione

Attori e minacce nel cloud

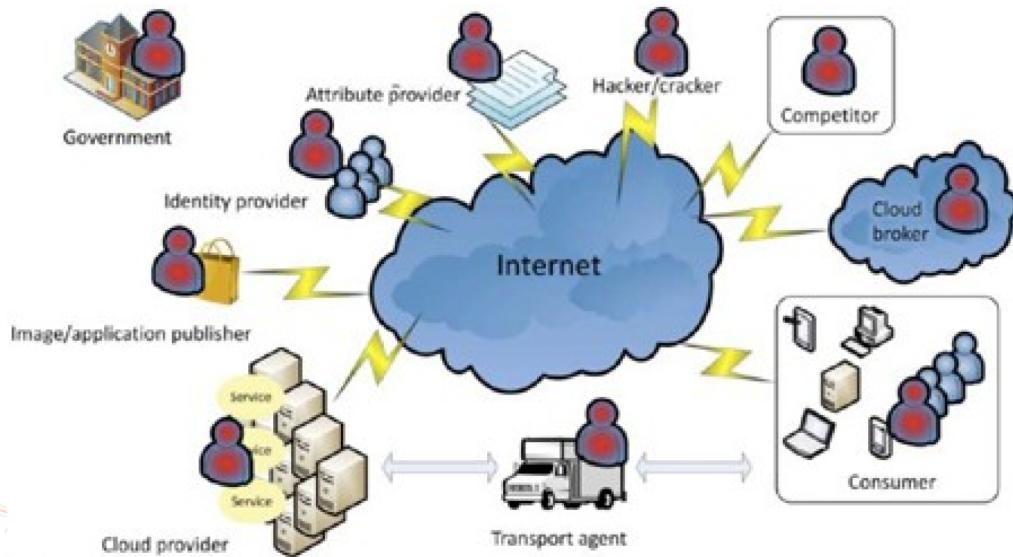


Image from "Securing Cloud Services: A pragmatic approach to security architecture in the Cloud"
by Lee Newcombe - IT Governance Publishing

I rischi specifici del cloud

- Tre categorie principali
- Rischi Organizzativi
 - Perdita di controllo
 - Lock-in
 - Supply Chain Failure
 -
- Rischi Tecnici
 - Economic denial of service (EDoS)
 - Cedimento dell'isolamento
 -
- Rischi legali
 - Rischi riguardanti la protezione dei dati
 - Rischi riguardanti la giurisdizione

Rischi Organizzativi

■ Perdita di controllo

- forse il rischio considerato più grave
- CSC cede il controllo a CSP su molti aspetti critici per la sicurezza
- se la SLA di CSP lascia un gap rispetto alle necessità, non c'è modo di chiuderlo
- outsourcing e subcontracting potrebbero mettere in gioco attori non fidati
- CSC non può verificare autonomamente la compliance di CSP

■ Lock-in

- molti aspetti proprietari rendono difficile la migrazione
- anche on premise, ma almeno i dati restano in mano al CSC...

■ Supply Chain Failure

- outsourcing crea catene di fornitura dei servizi: forti quanto l'anello più debole

■ Interferenze tra politiche di sicurezza CSC-CSP

- CSC potrebbe desiderare controlli in conflitto con l'ambiente CSP, quindi non implementabili
- insicurezze di un CSC potrebbero diventare vulnerabilità di tutta la piattaforma che lo ospita

Rischi Tecnici

■ Economic denial of service (EdoS)

- Servizi pay-per-use che scalano automaticamente → un attacco di sovraccarico, invece di degradare le prestazioni, aumenta i costi

■ Vulnerabilità della piattaforma

- Un attacco all'infrastruttura potrebbe consentire l'accesso a tutte le VM
- Molto improbabile, ma devastante
- Più plausibile: compromissione dell'interfaccia di gestione

■ Cedimento dell'isolamento

- Multi-tenancy teoricamente permette di installare una VM malevola accanto a quelle della vittima

- Possibili attacchi cross-VM via side channel
- Possibile forzatura di migrazioni saturando l'host

– Intercettazione dei dati in transito

- non tanto quelli dell'utente (che deve cauterarsi cifrando end-to-end)
- operazioni trasparenti del CSP: sincronizzazioni, migrazioni, ecc.
- raramente CSP fornisce garanzie di sicurezza su questi aspetti

Rischi legali

- Rischi riguardanti la protezione dei dati
 - legislazioni differenti
 - potrebbe essere illegale trasferire alcuni tipi di dati in alcuni paesi
 - CSP potrebbe spostare i dati tra i propri datacenter senza dirlo a CSC
- Rischi riguardanti la giurisdizione
 - CSP potrebbe essere costretto ad azioni dagli organi giudiziari sulla base di leggi del paese della sede legale, del paese dove sono collocati i datacenter, ecc...
 - CSC potrebbe subire interruzioni di servizio o sequestro di dati sulla base di motivi che non sussistono nel proprio paese



Laboratorio di Sicurezza Informatica



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Autorizzazione: modelli e implementazioni

Marco Prandini

Dipartimento di Informatica – Scienza e Ingegneria

Il processo di controllo dell'accesso

- Un soggetto autenticato deve essere autorizzato a svolgere operazioni sulle risorse del sistema
- Tre passaggi:
 - definire il modello del sistema controllato
(limitatamente ai fattori critici per il controllo degli accessi)
 - definire la politica di accesso
(le regole in base alle quali l'accesso è regolamentato)
 - attuare la politica
(tramite opportuni meccanismi HW / SW)
- Come già detto è molto utile separare politiche e meccanismi
 - per confrontare diverse politiche senza essere sommersi dai dettagli di implementazione
 - per modellare i componenti al livello di astrazione più appropriato e identificare la serie minima di requisiti che qualsiasi sistema di controllo degli accessi dovrebbe rispettare
 - per progettare meccanismi come elementi costitutivi, utilizzabili per diversi tipi di politiche



Caratteristiche delle politiche

- **Principio del privilegio minimo**
 - qualsiasi accesso deve avvenire concedendo l'insieme di autorizzazioni più ristretto possibile
- **Consistenza**
 - deve esistere uno schema di risoluzione non ambiguo da impiegare quando è possibile applicare autorizzazioni diverse alla stessa richiesta di accesso
 - nessuna soluzione unica!
 - la regola più / meno specifica vince
 - default allow vs. default deny
 - vince la prima / ultima regola incontrata in ordine spazio / temporale
 - gerarchia degli autori delle regole
- **Completezza e correttezza**
 - qualsiasi richiesta di accesso deve ricevere risposta entro un limite di tempo predeterminato
 - ci deve essere una regola predefinita da applicare quando non è possibile trovare un'autorizzazione esplicita per una richiesta

3

Caratteristiche dei meccanismi

- **Resistenza alle manomissioni**
 - deve essere impossibile sabotare un meccanismo di controllo degli accessi senza che nessuno se ne accorga
- **Principio di mediazione completa**
 - ogni accesso alle risorse deve essere sottoposto al controllo e alla decisione del meccanismo
- **Piccolo e autonomo**
 - deve essere facile da testare e riparare
- **Ragionevolmente economico**
 - il suo costo non deve superare i danni causati da accessi non autorizzati

4

Parametri di decisione

- Identità del soggetto
 - ovvio
- Ruolo del soggetto
 - i soggetti possono assumere ruoli diversi
 - le decisioni di accesso vengono prese in base al ruolo attuale di un soggetto, indipendentemente dalla sua identità
- Modalità di accesso
 - la decisione è presa non solo in base all'identità / dal ruolo, ma anche al tipo di operazione che il soggetto vuole eseguire
- Vincoli spaziali e temporali
 - l'accesso può dipendere da dove si trova il soggetto e da quando viene effettuata la richiesta
- Storia delle attività svolte
 - possono essere imposti limiti alla quantità di attività di un soggetto e al tipo di utilizzo della risorsa

5

Modelli di controllo dell'accesso

- I due paradigmi fondamentali sono
 - **DAC (Discretionary access control):**
 - Ogni oggetto ha un proprietario
 - Il proprietario decide i permessi
 - **MAC (Mandatory access control):**
 - La proprietà di un oggetto non consente di modificarne i permessi
 - C'è una policy centralizzata decisa da un *security manager*
- Ci sono modelli più complessi
 - **RBAC (Role-based access control):**
 - I permessi sono assegnati ai *ruoli*
 - Utile se i soggetti possono assumere dinamicamente ruoli differenti a seconda del contesto (cosa devono fare, dove si trovano, in che tempi operano...)
 - e varianti...

6

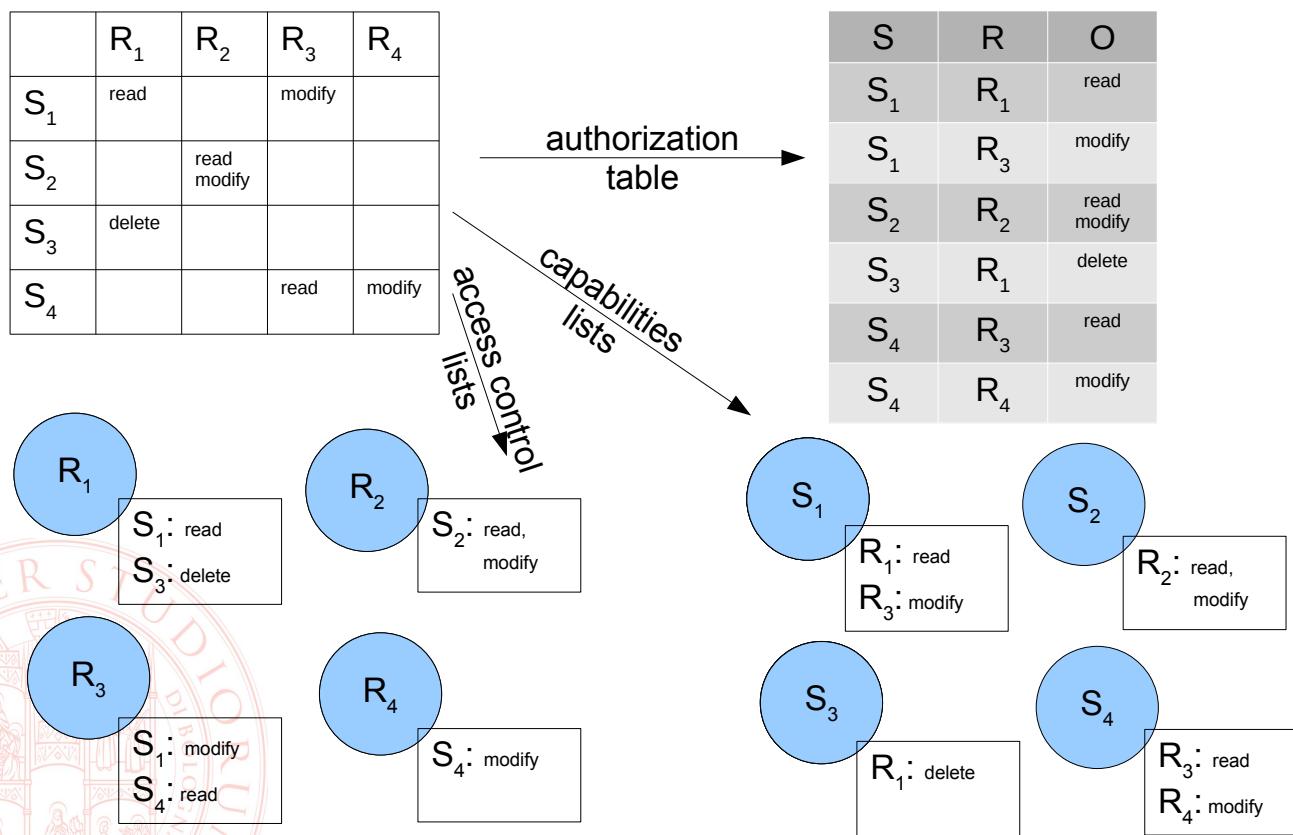
Generalità sui meccanismi

- In principio, il controllo dell'accesso è decidere se un soggetto può eseguire una specifica operazione su di un oggetto
- Il modo più banale per esprimere i permessi sarebbe una matrice completa
 - Migliaia di soggetti, milioni di oggetti!
 - La maggior parte delle “celle” è sempre al valore di default → potrebbe essere omessa

Subject	User1	User2	Group3
Object					
File1	read	read write	--
Dir2	list	modify	--
Socket3	write	--	read
...
...

7

Implementazioni efficienti



8

Implementazioni comuni

- Partizionare la matrice per soggetto: *capability lists*
 - Una lista associata a ogni soggetto del sistema
 - Contiene solo gli oggetti su cui il soggetto ha permessi ≠ default
- Partizionare la matrice per oggetto: *access control lists (ACL)*
 - Una lista associata a ogni oggetto del sistema
 - Contiene solo i soggetti che hanno permessi ≠ default sull'oggetto
 - Esplicitamente implementata da POSIX e MS Windows
 - Il filesystem Unix tradizionale ha negli inode una ACL “rigida”, che elenca sempre e solo tre soggetti:
 - L'utente proprietario (U)
 - Il gruppo proprietario (G)
 - Il gruppo隐式 che contiene tutti gli utenti ≠ U e ∉ G e i relativi permessi



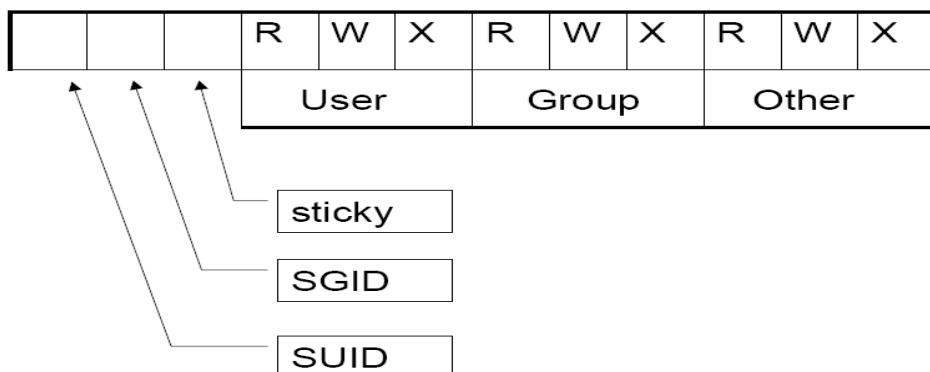
9

DAC nei sistemi Linux

- Gli utenti/gruppi possono essere creati con tool grafici o a riga di comando
 - `adduser`, `addgroup`
- Ogni utente DEVE appartenere almeno a un gruppo
 - Normalmente il sistema ne crea uno omonimo, con solo l'utente dentro
- Ogni utente può appartenere a un numero variabile di altri gruppi
- Gli account utente possono essere in uno stato *locked*, che impedisce di usarli per l'accesso interattivo, ma consente ai processi di girare con tale identità
 - Minimo privilegio!
- Il comando *passwd* si usa
 - Per cambiare le password (proprie, salvo root che può cambiarle a tutti)
 - Per settare l'account allo stato lock (-l) o unlock (-u)
 - Ovviamente solo root può farlo

Autorizzazioni su Unix Filesystem

- Ogni file (regolare, directory, link, socket, block/char special) è descritto da un i-node
- Un set di informazioni di autorizzazione, tra le altre cose, è memorizzato nell'i-node
 - (esattamente un) utente proprietario del file
 - (esattamente un) gruppo proprietario del file
 - Un set di 12 bit che rappresentano permessi standard e speciali



11

Significato dei bit di autorizzazione

- Leggermente diverso tra file e directory, ma in gran parte deducibile ricordando che
 - Una directory è semplicemente un file
 - Il contenuto di tale file è un database di coppie (nome, i-node)

R = **read (lettura del contenuto)**

Lettura di un file

Elenco dei file nella directory

W = **write (modifica del contenuto)**

Scrittura dentro un file

Aggiunta/cancellazione/rinomina
di file in una directory

NOTA che il permesso 'W' in una directory
consente a un utente di cancellare file sul
contenuto dei quali non ha alcun diritto

X = **execute**

Esegui il file come programma

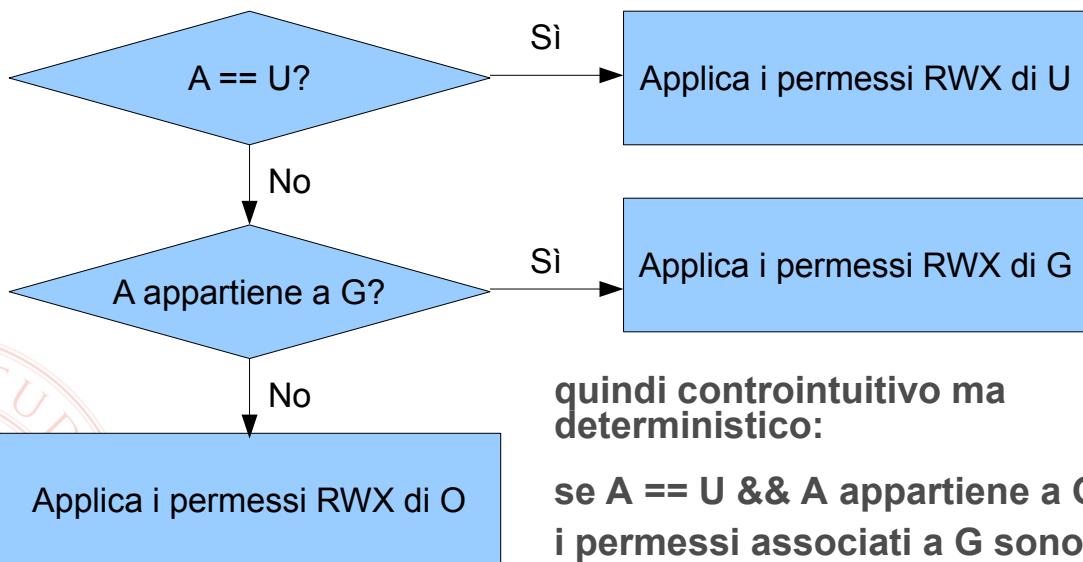
Esegui il lookup dell'i-node nella

NOTA: l'accesso a un file richiede il lookup
di tutti gli i-node corrispondenti ai nomi
delle directory nel path → serve il
permesso 'X' per ognuna, mentre 'R'
non è necessario

12

Composizione dei permessi

- Quando un utente “A” vuole eseguire un’operazione su di un file, il sistema operativo controlla i permessi secondo questo schema:



quindi contorto ma deterministico:

se $A == U \&\& A \text{ appartiene a } G$
i permessi associati a G sono ignorati anche se più favorevoli

13

Controllo dei permessi predefiniti

- Servono automatismi per assegnare i permessi alla creazione
- Ownership
 - l’utente creatore è assegnato come proprietario del file
 - Il gruppo attivo dell’utente creatore è assegnato come gruppo proprietario
 - Default = gruppo predefinito, da /etc/passwd
 - L’utente lo può cambiare a mano nella sessione con **newgrp**
 - Può cambiare automaticamente nelle directoy con SGID settato
- Permessi = “tutti quelli sensati” tolta la umask
 - “tutti quelli sensati”
 - **rw-rw-rw-** (666) per i file, l’eseguibilità è un’eccezione
 - **rwxrwxrwx** (777) per le directory, la possibilità di entrarci è la regola
 - la **umask** quindi può essere unica: una maschera che toglie i permessi da non concedere
 - poiché in Linux il gruppo di default group di un utente contiene solo l’utente stesso, una umask sensata è **006** (toglie agli “other” lettura e scrittura)
 - È un settaggio utile per collaborare, crea file manipolabili da tutti i membri del gruppo, a patto che questo sia settato correttamente
 - col comando **umask** si può interrogare e settare interattivamente, per rendere persistente la scelta si usano i file di configurazione della shell

14

Bit speciali / per i file

I tre bit più significativi della dozzina (11, 10, 9) configurano comportamenti speciali legati all'utente proprietario, al gruppo proprietario, e ad altri rispettivamente

■ BIT 11 – SUID (Set User ID)

- Se settato a 1 su di un programma (file eseguibile) fa sì che al lancio il sistema operativo generi un processo che esegue con l'identità dell'utente proprietario del file, invece che quella dell'utente che lo lancia

■ BIT 10 – SGID (Set Group ID)

- Come SUID, ma agisce sull'identità di gruppo del processo, prendendo quella del gruppo proprietario del file

■ BIT 9 – STICKY

- OBSOLETO, suggerisce al S.O. di tenere in cache una copia del programma



15

Permessi delicati da tenere sotto controllo

■ SUID e SGID sono un modo efficace di implementare interfacce per utenti standard verso processi privilegiati

- Cambio password: guardare `/usr/bin/passwd`
- Pianificazione di attività: guardare `/usr/bin/crontab` e `/var/spool/cron/`
- etc.

■ I programmi con questi permessi vanno sorvegliati, perché chiunque li lancia acquisisce temporaneamente privilegi elevati

- Pochi programmi e molto vincolati
- Rischi: bug di questi programmi che porti a eseguire operazioni arbitrarie invece di quelle progettate, programmi diversi a cui sono dati per errore questi privilegi

■ Usare `find` per trovarli

- `find / -type f -perm +6000`

■ Altre ricerche interessanti per la sicurezza

- file world-writable (`-perm +2`)
- file senza proprietario, rimasti da account cancellati (`-nouser`)



16

Bit speciali / per le directory

- Bit 11 per le directory non viene usato
- Bit 10 – SGID
 - Precondizioni
 - un utente appartiene (anche) al gruppo proprietario della directory
 - il bit SGID è impostato sulla directory
 - Effetto:
 - l'utente assume come gruppo attivo il gruppo proprietario della directory
 - I file creati nella directory hanno quello come gruppo proprietario
 - Vantaggi (mantenendo umask 0006)
 - nelle aree collaborative i file sono automaticamente resi leggibili e scrivibili da tutti i membri del gruppo
 - nelle aree personali i file sono comunque privati perché proprietà del gruppo principale dell'utente, che contiene solo l'utente medesimo
- Bit 9 – Temp
 - Le “directory temporanee” cioè quelle world-writable predisposte perché le applicazioni dispongano di luoghi noti dove scrivere, hanno un problema: chiunque può cancellare ogni file
 - Questo bit settato a 1 impone che nella directory i file siano cancellabili solo dai rispettivi proprietari

17

Attributi

- Gli attributi sono primariamente utili per il fs tuning
 - compressed (c), no dump (d), extent format (e), data journalling (j), no tail-merging (t), undeletable (u), no atime updates (A), synchronous directory updates (D), synchronous updates (S), and top of directory hierarchy (T)
- Alcuni sono rilevanti per la sicurezza
 - append only (a) – utile per impedire il taglio dei logfile
 - immutable (I) – vieta cancellazione, creazione di link verso il file, rinomina e scrittura, utile per i file di sistema
 - secure deletion (s) – sovrascrive con zeri i blocchi dei file cancellati (sicurezza molto limitata ma valida contro strumenti in linea)
- Tools
 - **chattr** per modificarli
 - **lsattr** per visualizzarli

18

POSIX Access Control Lists

■ Le ACL estendono la flessibilità di autorizzazione

■ Vantaggi:

- Specificare una lista arbitraria di utenti e gruppi coi relativi permessi (comunque scelti tra rwx) in aggiunta agli owner
- Ereditare la maschera di creazione dalla directory
- Limitare tutti i permessi simultaneamente (esempio mask sotto)

■ Esempio:

```
user::rw-
user:lisa:rwt          #effective:r--
group::r--              #effective:r--
group:toolies:rwt       #effective:r--
mask::r--                
```

other::r--

■ Strumenti:

- **setfacl** per impostare, **getfacl** per visualizzare le ACL (ls -l mostra un '+' dopo i permessi se ACL è presente per un file)
- **man acl**

19

Il super-utente nei modelli DAC

■ Esiste tipicamente un utente con privilegi illimitati, che può scavalcare i meccanismi di controllo dell'accesso

- **root** in Unix
- **administrator** in Windows

■ L'account va difeso contro ingressi abusivi ma va anche minimizzata la probabilità di fare errori

- Usare un account non-privilegiato, basta per il 99% del tempo
- Disabilitare l'accesso diretto da GUI e console
- Ottenere temporaneamente i diritti di super-utente solo per eseguire i task di amministrazione
 - **sudo** in Linux
 - “**esegui come amministratore**” in Windows

Capabilities in Linux

(da non confondere con le capability list tipiche dei modelli MAC)

- I poteri di *root* non sono “monolitici”
- Ci sono ben 41 diverse *capability* (al kernel 5.9)
 - rappresentano autorizzazioni normalmente negate agli utenti standard
 - riguardano molteplici aspetti di controllo delle risorse di calcolo e dei processi e dell'accesso alla rete
 - una nello specifico è CAP_DAC_OVERRIDE: la possibilità di ignorare i permessi sul filesystem
- È possibile assegnare specifiche capability a processi lanciati da utenti standard
 - autorizzazione a svolgere azioni privilegiate senza accesso a root
 - implementazione del principio di minimo privilegio
- [man \(7\) capabilities \(8\) getcap \(8\) setcap](#)

DAC nei sistemi Microsoft

- Utenti e loro proprietà
- Tipi di gruppi
- Estensione dei gruppi sui domini
- Gruppi predefiniti
- Generalità NTFS
- Implementare la sicurezza di NTFS
- Implementare la condivisione di risorse
- Permessi locali e permessi sulle condivisioni NTFS



Premessa: i domini

- Nell'uso più comune, i sistemi Microsoft sono raggruppati in un **dominio**: un insieme di computer, comunicanti tra loro e che condividono un directory database comune
- Nella directory sono memorizzati vari tipi di oggetti
 - I computer che fanno parte del dominio
 - Le risorse condivise dai computer (cartelle, stampanti)
 - Gli utenti validi sul dominio
 - I gruppi di utenti
 - I raggruppamenti di altre entità
 - ...



Utenti

- Local user accounts
 - ristretti al sistema su cui sono creati
 - possono avere moderati permessi amministrativi (che non si estendono alla possibilità di accedere ai dati di altri utenti) --> Power Users Group
- Domain user accounts
 - appartiene ad un dominio
 - profilo memorizzato in AD
 - può accedere a risorse non locali, limitatamente ai privilegi che gli sono concessi
 - del proprio dominio
 - dei domini trusted



Proprietà dell'utente

■ Sono moltissime, accessibili dai tab del wizard qui elencati:

- | | |
|----------------------------|--|
| – Member Of | The user's defined group membership |
| – Dial-in | Remote access and callback options |
| – General | User's first name, last name, display name description, office location, telephone, e-mail, and Web pages |
| – Address | User's post office mailing address |
| – Account | Logon name, domain, logon hours, logon to server name, account options, and account expiration date |
| – Profile | User profile path, profile script, home directory path and server, and shared document folder location |
| – Telephones/Notes | Home, pager, and mobile phone numbers and comments on where to contact user |
| – Organization who | Job title, company, department, manager, and people report to user Environment Applications to run from Terminal server client |
| – Sessions | Timeouts for Terminal Services |
| – Remote Control | Permissions for monitoring Terminal Service sessions |
| – Terminal Service Profile | Location for Terminal Service home directory |

Gruppi

- Ogni oggetto di AD può essere membro di uno o più gruppi (di tipo e scope appropriato)
- Distribution Groups
 - possono essere usati da qualsiasi applicazione abbia bisogno di una lista di utenti
 - il sistema operativo non li utilizza
 - non appesantiscono il logon ticket dell'utente
- Security Groups
 - come i DG, ma possono essere soggetti nelle regole che controllano l'accesso alle risorse del sistema
- In Windows 2003 funzionante in Native Mode è possibile la conversione da un tipo all'altro

Group scopes

- Sia per i Distribution Group che per i Security Group vale il concetto di scope (estensione), che definisce
 - oggetti di quali domini possono far parte del gruppo
 - in quali domini può essere usato un gruppo per definire regole d'accesso
- La prima suddivisione è tra
 - Machine Local (locali ad una singola macchina)
 - Gruppi validi nel dominio
 - Domain Local
 - Global
 - Universal
- Nesting: è possibile solo *in native mode* rendere gruppi membri di altri gruppi

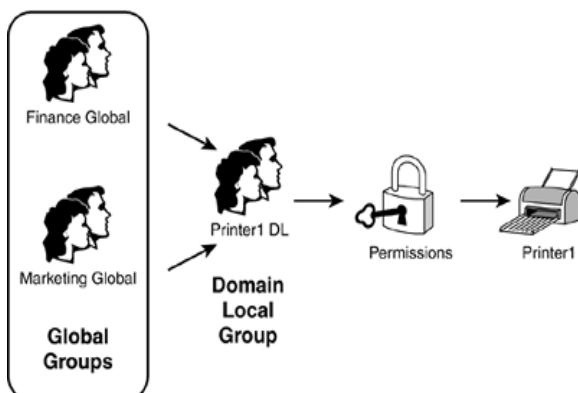
Group scopes

	Può contenere	Può essere membro di	Gli possono essere assegnati permessi su
Domain Local Group (DLG)	Utenti, GG, UG, computer di qualsiasi dominio, DLG dello stesso dominio	Altri DLG dello stesso dominio	Risorse dello stesso dominio
Global Group (GG)	Utenti ed altri GG dello stesso dominio	Qualsiasi DLG e UG, GG dello stesso dominio	Risorse di qualsiasi dominio
Universal Group (UG)	Utenti, GG, UG di qualsiasi dominio	DLG e UG di qualsiasi dominio	Risorse di qualsiasi dominio

Utilizzo tipico e consigliato

- Sebbene sia possibile assegnare diritti su risorse direttamente a UG e GG, la struttura consigliata è (caso più semplice):

- individuare in ogni dominio utenti con esigenze analoghe e metterli in un GG
- rendere i GG membro degli opportuni DLG
- assegnare i permessi d'uso delle risorse ai DLG



Utilizzo tipico e consigliato

- In realtà molto ampie è possibile sfruttare gli UG per aggiungere un livello di nesting che consenta all'*enterprise administrator* di raggruppare i GG

- individuare in ogni dominio utenti con esigenze analoghe e metterli in un GG
 - in questo modo si delega al *domain administrator* che conosce bene la propria realtà il compito di popolare i GG
- raggruppare i GG omologhi in un UG
 - in questo modo si evita che alla riorganizzazione dei domini, o in generale alla comparsa/scomparsa di GG, i singoli amministratori delle risorse debbano agire sui DLG, ripopolandoli di conseguenza. Sarà l'*enterprise administrator* a sapere quali GG è opportuno assegnare agli UG, mentre questi ultimi saranno creati o distrutti solo in casi eccezionali.
- rendere l'UG membro degli opportuni DLG
- assegnare i permessi d'uso delle risorse ai DLG
 - gli amministratori delle singole risorse possono scegliere i soggetti (GG e UG) preconfigurati ai passi precedenti come membri di DLG, anzichè come soggetti cui attribuire direttamente permessi, in modo che l'aggiunta o la rimozione di un UG/GG da un DLG si applichi automaticamente a tutte le risorse su cui tale DLG può operare

Gruppi predefiniti – domain local

Gruppo	Caratteristiche
Administrators	Controllo completo della macchina locale con tutti i privilegi; membri di default comprendono i Domain Admins, gli Enterprise Admins, e l'account Administrator.
Account Operators	Amministrazione degli utenti del dominio.
Backup Operators	Back up e restore dei file sulla macchina locale indipendentemente dai permessi ad essi associati; log on e shut down. Le Group policies possono limitare questi privilegi di default.
Guests	Logon/shutdown limitato sulla macchina locale.
Print Operators	Amministrazione delle stampanti locali.
Replicator	Gestione delle funzioni e dei servizi di replica di Active Directory.
Server Operators	Amministrazione del sistema locale.
Users	Esecuzione di applicazioni, accesso alle stampanti, logon/shutdown/locking, creazione e modifica fi gruppi locali; tutti gli utenti del dominio sono membri di default.

Gruppi predefiniti – global

Gruppo	Caratteristiche
Domain Admins	Privilegi di amministrazione su tutti i sistemi appartenenti al dominio
Domain Computers	Tutti i computer del dominio
Domain Controllers	Tutti i domain controller
Domain Guests	Appartiene al DLG "Guest"
Domain Users	Appartiene al DLG "Users"
Enterprise Admins	Appartiene al gruppo "Domain Admins" di ciascun dominio, concedendo quindi i privilegi di amministrazione a livello di foresta.
Group Policy Creators Owners	Ai membri è consentito modificare le group policy
Schema Admins	Ai membri è consentito modificare lo schema di Active Directory

Group Policy

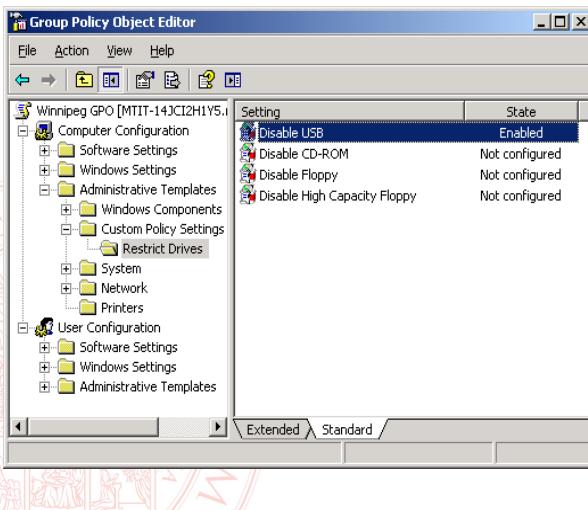
- Group Policy fornisce un quadro di riferimento per controllare l'ambiente di utenti e computer, cioè per assegnare quel tipo di privilegi o restrizioni che non sono legati a risorse fisiche ovvie quali file, cartelle, ecc.
- Le regole vengono definite in un Group Policy Object, che può essere collegato a qualsiasi contenitore di oggetti (una OU, un Site, un Domain) per applicarle a tutti gli oggetti in esso contenuti.
- Ogni GPO contiene due sezioni distinte
 - impostazioni per gli utenti (user settings)
 - impostazioni per i computer (computer settings)
- In ciascuna delle due sezioni le impostazioni sono ulteriormente classificate in:
 - impostazioni software (software settings)
 - impostazioni di Windows (Windows settings)
 - modelli per l'amministrazione (administrative templates)

Group Policy - impostazioni

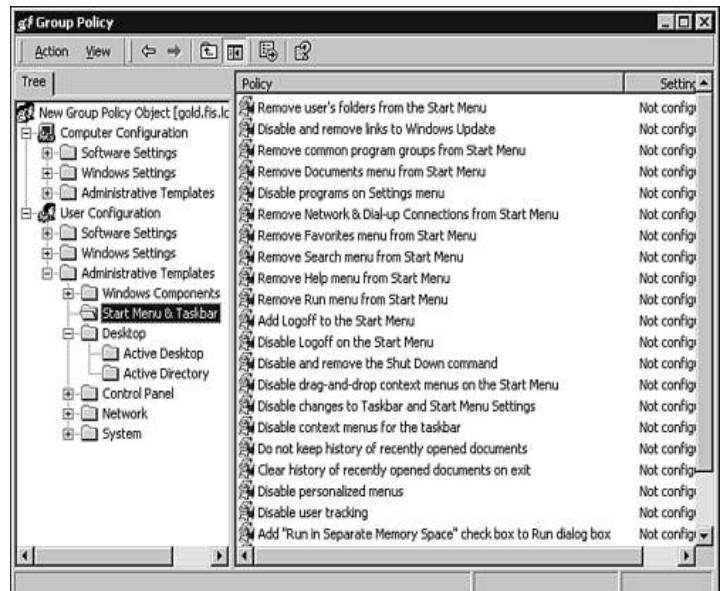
Categoria	Finalità	Disponibile per computer?	Disponibile per utenti?
Software settings	Installare, aggiornare, rimuovere applicazioni	Sì	Sì
Windows settings	Definire scripts ed impostazioni di sicurezza (vedi colonne a fianco)	Start-up e shutdown scripts, numerose impostazioni di sicurezza	Logon e logoff scripts, alcune impostazioni di sicurezza, impostazioni di Internet Explorer, folder redirection
Administrative templates	Definire in modo centralizzato le impostazioni del registro di sistema	Sì	Sì

Group Policy - esempi

Limitare l'uso di una intera categoria di dispositivi, come le porte USB



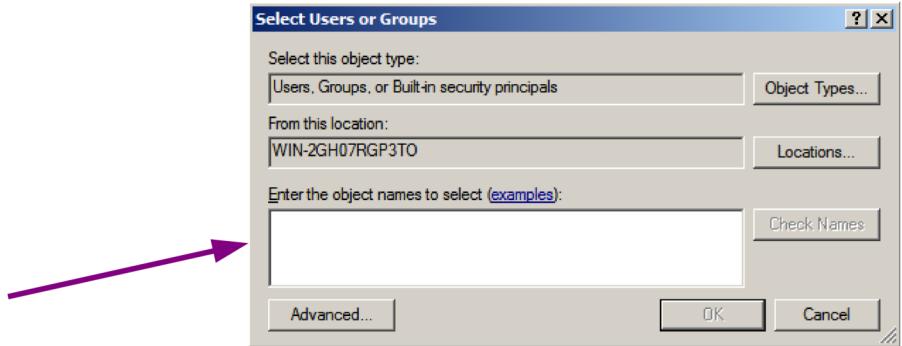
Configurare il contenuto del desktop o del menu avvio



Controllo dell'accesso

- Le autorizzazioni sono assegnate sotto forma di ACL: ad ogni risorsa è associata una lista di soggetti (utenti o gruppi) e dei relativi permessi che essi detengono sulla risorsa
- Le ACL sono disponibili
 - su partizioni NTFS (non FAT)
 - sulle condivisioni di risorse in rete
- Per modificare le ACL è necessario
 - o detenere l'Ownership
 - o che nell'ACL medesima siano assegnati i permessi 'Full Control' o 'Change Permissions'

Esempio di modifica delle ACL



Aggiunta di soggetti alla lista
collegata ad una risorsa
(da “Edit” della finestra precedente)



Ownership ed autorizzazioni

■ Ownership

- L'Owner di files e directories ha il pieno controllo (Full Control)
- Administrator può sempre prendere l'ownership
- L'Owner può assegnare le permissions per prendere l'Ownership
- Nota: gli utenti che creano un file o una directory ne detengono l' Ownership

■ Autorizzazioni NTFS predefinite

- Ad Everyone viene assegnato automaticamente Full Control
- I nuovi file ereditano le autorizzazioni della cartella in cui vengono creati (questo vale anche per i files che vengono copiati in un direttorio)



Accesso ed auditing

- Le ACL per il controllo dell'accesso fanno sì che, ad ogni tentativo di utilizzo di una risorsa, il sistema risponda autorizzando o negando l'operazione
- Ad ogni risorsa è inoltre associata una SACL utilizzata per l'auditing, che si presenta come una normale ACL, ma permette di tracciare gli esiti dei tentativi di utilizzo
- Le regole nella SACL possono essere impostate in modo che
 - quando un determinato soggetto tenta un'operazione e, grazie alla configurazione della ACL standard, riesce, questo evento sia registrato
 - quando un determinato soggetto tenta un'operazione e, grazie alla configurazione della ACL standard, viene bloccato, questo evento sia registrato



Autorizzazioni standard e speciali

- L'obiettivo del sistema di controllo delle autorizzazioni è duplice
 - elevata precisione nel controllo dell'accesso
 - in termini di tipo di azioni da concedere/negare
 - in termini di gestione delle complesse relazioni tra utenti e gruppi che possono essere titolari delle autorizzazioni
 - facilità d'uso
 - il sistema è Discretionary Access Control (DAC), quindi consente ad ogni utente anche non tecnico di manipolare le autorizzazioni sulle proprie risorse
 - anche l'utente più esperto per il 90% del tempo fa cose semplici



Autorizzazioni standard e speciali (cont.)

■ La soluzione ai due problemi è realizzata con un sistema che prevede tre strati di interfaccia utente per “svelare” all'occorrenza i dettagli che servono:

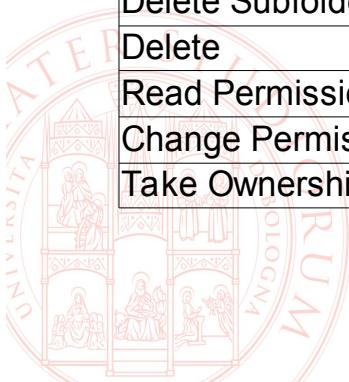
- a basso livello il sistema supporta
 - molte autorizzazioni (*autorizzazioni speciali*) --> possibilità di controllo fine sui permessi
 - con una logica a tre valori (*allow*, *deny*, *not set*) --> possibilità di definire regole di interazione quando diverse ACL vengono combinate
- le autorizzazioni speciali sono aggregate in un set più ridotto di *autorizzazioni standard*
- le autorizzazioni standard possono essere visualizzate a due valori (*allow*, *not set*) o mostrando esplicitamente i tre valori



Autorizzazioni standard (elenco)

Abbreviation	Type	Description
R	Read	Provides the designated user or group the ability to read the file or the contents of the folder.
W	Write	Provides the designated user or group the ability to create or write files and folders.
RX	Read & Execute	Provides the designated user or group the ability to read file and folder attributes, view folder contents, and read files within the folder. If this permission is applied to a folder, files with inheritance set will inherit it (see the inheritance discussion).
L	List Folder Contents	Same as Read & Execute, but not inherited by files within a folder. However, newly created subfolders will inherit this permission.
M	Modify	Provides the ability to delete, write, read, and execute.
F	Full Control	Provides the ability to perform any action, including taking ownership and changing permissions. When applied to a folder, the user or group may delete subfolders and files within a folder.

Corrispondenza tra autorizzazioni standard e speciali



Types	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder/Execute File	X	X	X	X		
List Folder/Read Data	X	X	X	X	X	
Read Attributes	X	X	X	X	X	
Read Extended Attributes	X	X	X	X	X	
Create Files/Write Data	X	X				X
Create Folders/Append Data	X	X				X
Write Attributes	X	X				X
Write Extended Attributes	X	X				X
Delete Subfolders and Files	X					
Delete	X	X				
Read Permissions	X	X	X	X	X	
Change Permissions	X					
Take Ownership	X					

ACL editing - esempi

special
standard

Software Config Properties

General | Sharing | Security | Web Sharing | Customize |

Group or user names:

- Engineers (ENTCERT2\Engineers)
- Joe Engineer (jengineer@Entcert2.com)
- Software Config (ENTCERT2\Software Config)
- SYSTEM
- Users (ENTCERT2\Users)

Permissions for Software Config

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Modify	<input type="checkbox"/>	<input type="checkbox"/>
Read & Execute	<input type="checkbox"/>	<input type="checkbox"/>
List Folder Contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or for advanced settings, click Advanced.

OK Cancel Apply

Permission Entry for Software Config

Name: Joe Engineer (jengineer@Entcert2.com) Change...

Apply on: This folder, subfolders and files

Permissions:

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Traverse Folder / Execute File	<input type="checkbox"/>	<input type="checkbox"/>
List Folder / Read Data	<input type="checkbox"/>	<input type="checkbox"/>
Read Attributes	<input type="checkbox"/>	<input type="checkbox"/>
Read Extended Attributes	<input type="checkbox"/>	<input type="checkbox"/>
Create Files / Write Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create Folders / Append Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write Extended Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete Subfolders and Files	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input type="checkbox"/>	<input type="checkbox"/>
Read Permissions	<input type="checkbox"/>	<input type="checkbox"/>
Change Permissions	<input type="checkbox"/>	<input type="checkbox"/>
Take Ownership	<input type="checkbox"/>	<input type="checkbox"/>

Apply these permissions to objects and/or containers within this container only

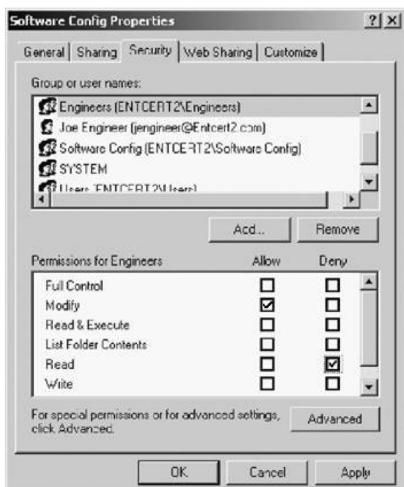
OK Cancel Clear All

Composizione

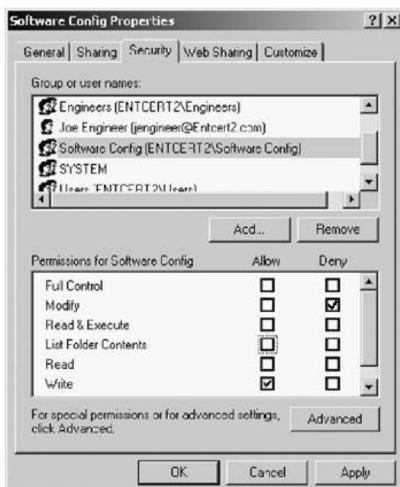
- Come si può vedere, ogni permesso può essere impostato in tre modi
 - esplicitamente **allow**
 - esplicitamente **deny**
 - o **non impostato**
- Windows segue un modello default deny: ciò che non è esplicitamente concesso è proibito
 - quindi **non impostato == deny** ?
 - a cosa servono due modi diversi di proibire l'accesso?
- Un utente può appartenere a molti gruppi!
 - ogni gruppo può avere permessi distinti nell'ACL di una risorsa
 - il permesso complessivo dell'utente sarà la somma, bit a bit, di tutti i permessi ottenuti in quanto membro dei propri gruppi
- **non impostato** (sia allow che deny sono bit a zero) presente nei permessi di un gruppo consente che un **allow** ottenuto da un altro gruppo possa avere effetto: **non impostato == deny “debole”/scavalcabile**
- un **deny** esplicito prevarrà sempre su di un eventuale **allow** ottenuto da un altro gruppo: **deny esplicito == deny “forte”/non scavalcabile**

45

Composizione



permessi dei membri del gruppo Engineers



permessi dei membri del gruppo Software Config

i membri del gruppo Software Config non potrebbero ottenere **modify** anche se appartenessero a un gruppo (come Engineers) che lo ha (**strong deny**)

i membri di Engineers non hanno il permesso **write** ma lo potrebbero ottenere se appartenessero a un gruppo (come Software config) che lo ha

Full Control	<input type="checkbox"/>
Modify	<input checked="" type="checkbox"/>
Read & Execute	<input type="checkbox"/>
List Folder Contents	<input type="checkbox"/>
Read	<input type="checkbox"/>
Write	<input type="checkbox"/>

- ← non imp. resta non imp. == deny
- ← **deny prevale su allow == deny**
- ← deny esplicito == deny
- ← allow esplicito == allow

46

Esempio di manipolazione delle ACL (vecchia interfaccia semplificata)



Nelle nuove versioni di Windows, tutte le interfacce mostrano le colonne Allow e Deny, nelle vecchie esisteva una vista ancor più semplificata per scegliere

- una delle autorizzazioni standard (implicitamente equivalente a settare "Allow" su tutte le autorizzazioni speciali corrispondenti)
- oppure "Nessun accesso", equivalente a deny su tutti i permessi

Autorizzazioni di accesso alle cartelle

- Sulle cartelle è possibile impostare una delle seguenti autorizzazioni standard:
 - Nessun accesso
 - Elenco
 - Lettura
 - Aggiunta
 - Aggiunta e Lettura
 - Modifica
 - Controllo completo
- Nota: I gruppi o gli utenti a cui è stata concessa l'autorizzazione 'Controllo completo' su una cartella sono in grado di eliminarne i file, indipendentemente dall'autorizzazione che li protegge.

Autorizzazioni di accesso ai file

- Sui file è possibile impostare le seguenti autorizzazioni standard:
 - Nessun accesso
 - Lettura
 - Modifica
 - Controllo completo
- Impostando le autorizzazioni di accesso a un file sarà possibile specificare il tipo di accesso al file consentito a un gruppo o a un utente. Altrimenti, un file eredita le autorizzazioni proprie della cartella in cui è stato creato.
- Nota I gruppi o gli utenti cui si concede l'autorizzazione Controllo completo su una cartella possono eliminarne i file, indipendentemente dall'autorizzazione che li protegge.



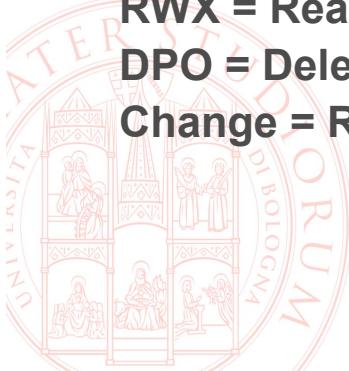
Esempio di composizione di permessi

Permessi di Michael	Permessi di Research	Permessi di Development	Permessi di Michael (effettivi)
Read	Read	-	Read
Write	-	Read	Change
Take Ownership	Read	Change	Take Ownership & Change
No Access	Read	Change	No Access
Change	No Access	Change	No Access

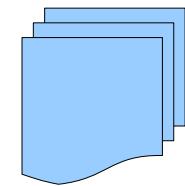
RWX = Read, Write, Execute

DPO = Delete, Permissions, Ownership

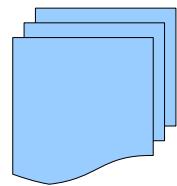
Change = RWXD



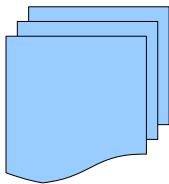
Permessi dopo un copy/move di file



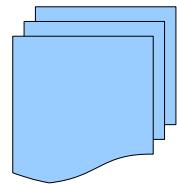
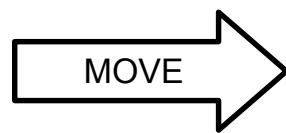
File1 = RWX



File1 = diritti del directory

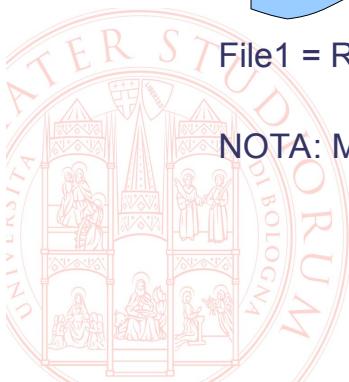


File1 = RWX



File1 = RWX

NOTA: MOVE verso una partizione diversa dalla sorgente = COPY (+delete)!



Condivisione di risorse

- Share = directory (folder) condivisa
- I diritti necessari per attivare le condivisioni sono concessi di default ai gruppi
 - Administrators
 - Server Operators (se in un dominio)
 - Power Users (se in un workgroup)
- Gli Users devono avere almeno il permesso List per fruire della directory condivisa



Condividere una cartella



Permessi locali vs. Permessi sulla condivisione

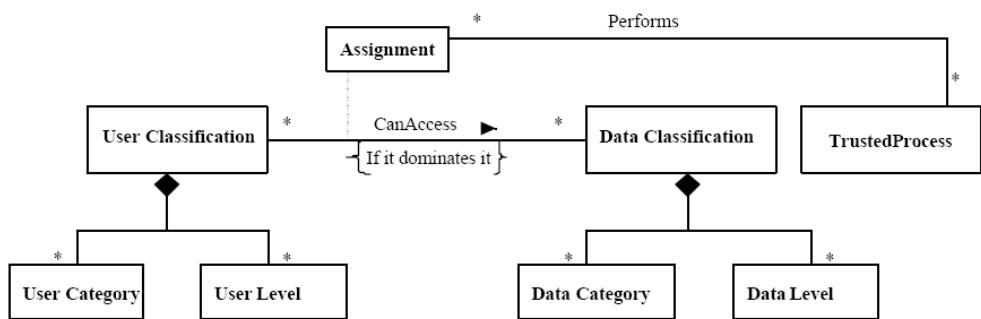
	Permessi assegnati	Permessi di Michael
Permessi Share	Everyone: Read Michael: Change	Change (RWXD)
Permessi locali	Everyone: Read Michael: Read	Read (RX)
Permessi effettivi		Read (RX)

Le ACL di Share si comportano come quelle di NTFS in termini di composizione di permessi, però vengono applicate in serie una all'altra, per cui complessivamente l'autorizzazione effettiva è quella più restrittiva tra le due



Un breve cenno a MAC

- **MANDATORY:** le regole di controllo degli accessi sono dettate da un'autorità centrale e i soggetti non possono modificarne alcun dettaglio
- Ad ogni soggetto o risorsa viene assegnata una **classe di accesso** che specifica tipicamente
 - un livello di sicurezza all'interno di un insieme ordinato di valori, ad es {TopSecret ► Segreto ► Riservato ► Non classificato}
 - una categoria (**compartment**) all'interno di un insieme non ordinato, ad es. {armi, piani di battaglia, unità di combattimento, ...} che riflette le aree funzionali del sistema



Come si usano le classi

- le **risorse** sono etichettate (**classification**) con un livello di sicurezza (**sensitivity**) che rappresenta la gravità delle conseguenze di una violazione delle policy che le riguarda
- i **soggetti** sono etichettati con un livello di sicurezza che rappresenta la loro affidabilità: **clearance**
- le categorie sono utilizzate per raffinare le politiche
- vengono stabilite relazioni di dominanza tra classi; detti
 - S un livello di sicurezza
 - C un insieme di categorie
 - $L_1 = \langle S_1, C_1 \rangle$
 - $L_2 = \langle S_2, C_2 \rangle$

L_1 domina L_2 se e solo se $S_1 \geq S_2$ e $C_1 \supseteq C_2$

Come si usano le classi

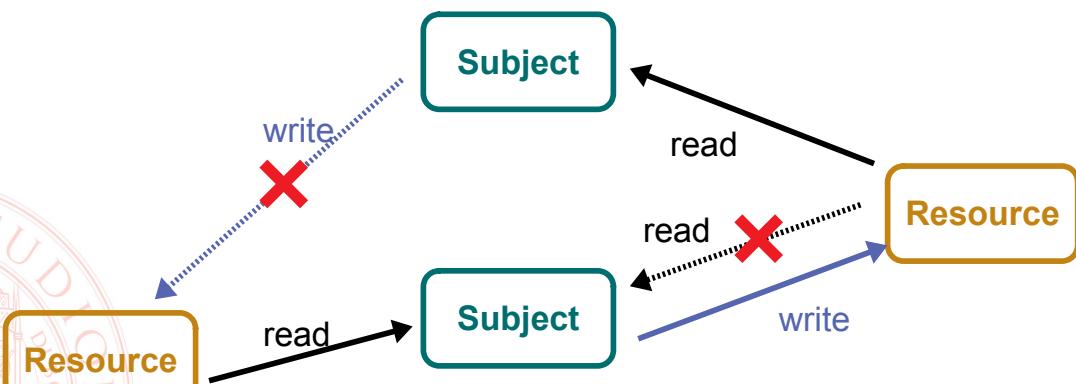
- Le relazioni di dominanza vengono usate in modo diverso a seconda della proprietà di sicurezza da proteggere
 - riservatezza → Bell-LaPadula model
 - integrità → Biba model
- L'applicazione simultanea dei due modelli è possibile assegnando due classi di accesso a ogni soggetto e risorsa, una usata per controllare la riservatezza e l'altra per controllare l'integrità



BLP (Bell-LaPadula)

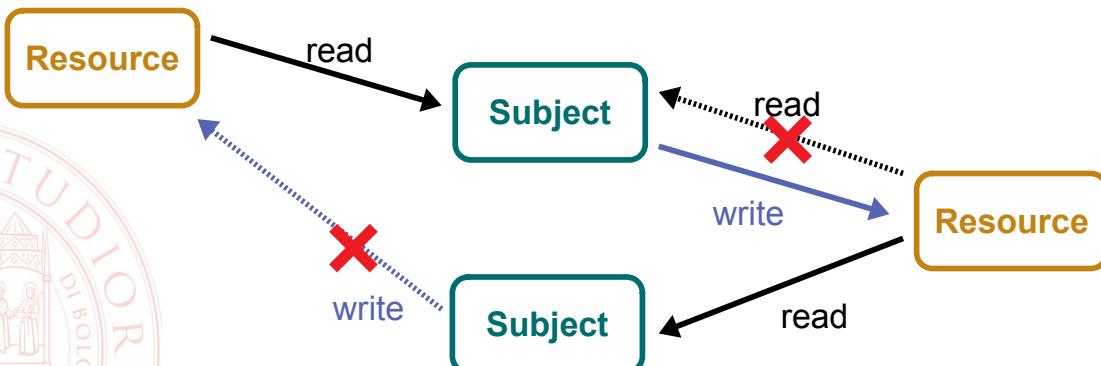
■ Due regole per proteggere la riservatezza

- **NO-READ-UP**: un soggetto può leggere una risorsa solo se la sua classe di accesso domina la classe di accesso della risorsa (altrimenti leggerebbe una risorsa troppo sensibile per il suo livello)
- **NO-WRITE-DOWN**: un soggetto può modificare una risorsa solo se la sua classe di accesso è dominata dalla classe di accesso della risorsa (altrimenti potrebbe far trapelare un segreto in luoghi accessibili a soggetti con minor clearance)



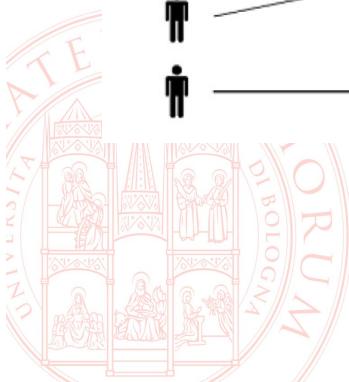
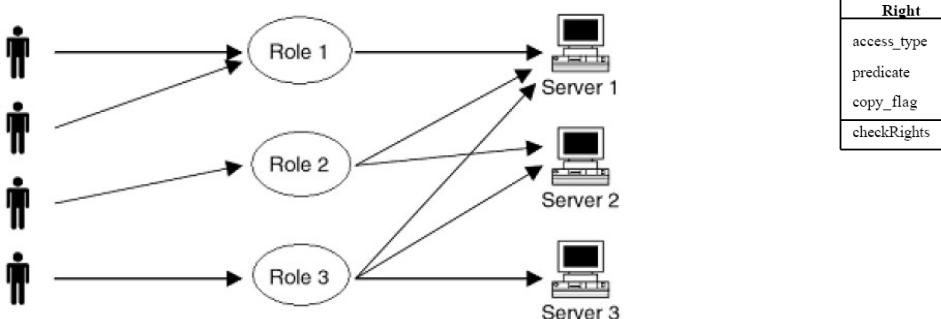
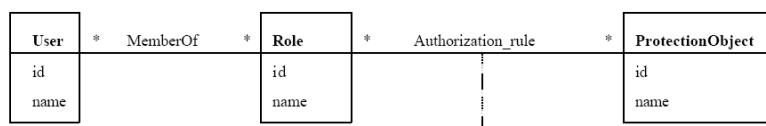
■ Due regole per proteggere l'integrità:

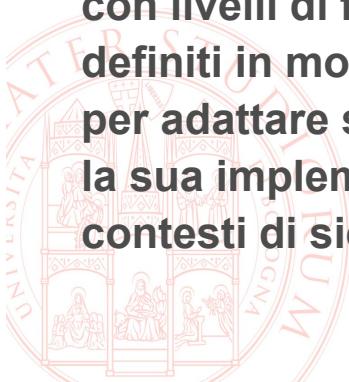
- **NO-READ-DOWN**: un soggetto può leggere una risorsa solo se la sua classe di accesso è dominata dalla classe di accesso della risorsa (altrimenti utilizzerebbe informazioni meno attendibili al proprio livello di fiducia più elevato)
- **NO-WRITE-UP**: un soggetto può scrivere una risorsa solo se la sua classe di accesso domina la classe di accesso della risorsa (altrimenti modificherebbe una risorsa troppo sensibile per il suo livello)



Un brevissimo cenno a RBAC

- le autorizzazioni non sono concesse a utenti, ma a *ruoli*
- il ruolo ricoperto da un utente può cambiare dinamicamente
 - nel tempo
 - secondo il contesto





- RBAC è un modello "policy neutral" che permette di esprimere tutti i principi fondamentali per la sicurezza:
 - minimo privilegio
 - separazione delle responsabilità
 - astrazione (es. usando generici "debiti" e "crediti" al posto di permessi specifici delle risorse come "possibilità di lettura/scrittura")
 - Vantaggio: le autorizzazioni cambiano poco o per nulla, se correttamente modellate
 - il ruolo dell'amministratore della sicurezza diventa essenzialmente quello di assegnare il ruolo appropriato ai soggetti
 - Esiste un modello standard (ANSI/INCITS 359-2004) con livelli di funzionalità definiti in modo incrementale per adattare semplicemente la sua implementazione in contesti di sicurezza differenziati

