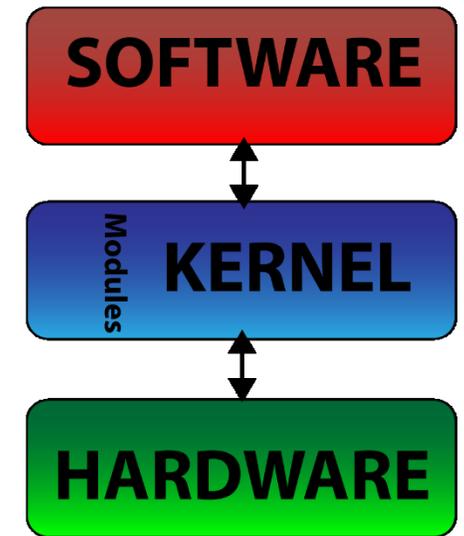
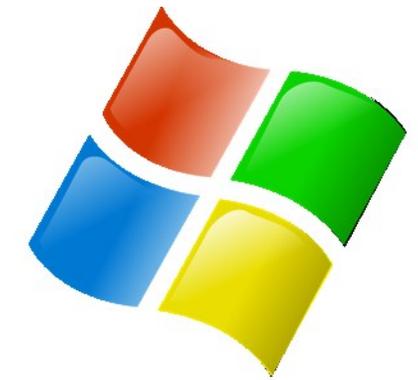




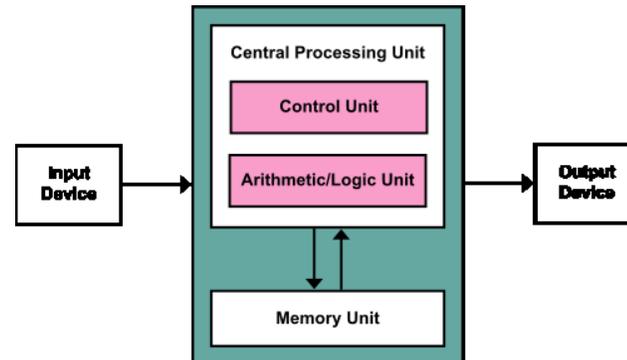
**UNIVERSITÀ DEGLI STUDI
DELLA BASILICATA**

*Corso di Sistemi Operativi
A.A. 2019/20*

Sicurezza



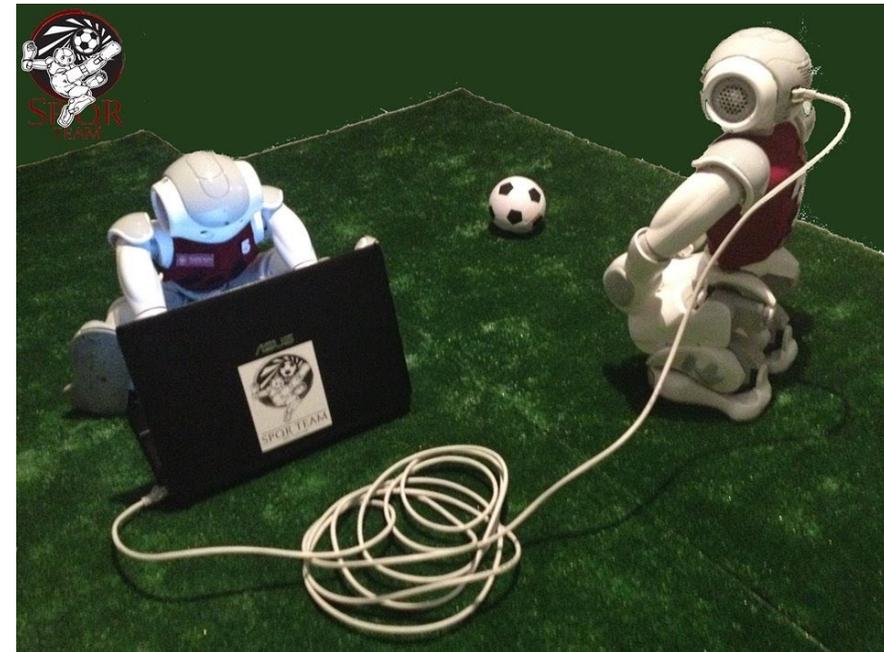
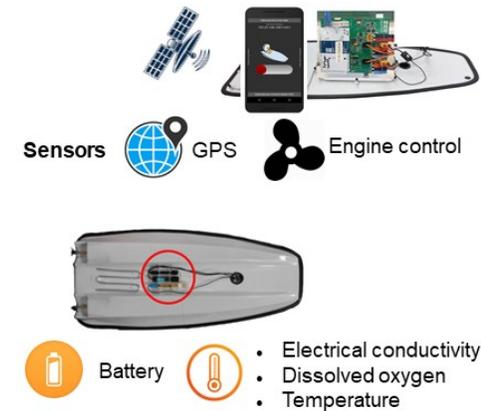
Docente:
**Domenico Daniele
Bloisi**



Gennaio 2020

Domenico Daniele Bloisi

- Ricercatore RTD B
Dipartimento di Matematica, Informatica ed Economia
Università degli studi della Basilicata
<http://web.unibas.it/bloisi>
- SPQR Robot Soccer Team
Dipartimento di Informatica, Automatica e Gestionale Università degli studi di Roma “La Sapienza”
<http://spqr.diag.uniroma1.it>



Ricevimento

- In aula, subito dopo le lezioni
- Martedì dalle 11:00 alle 13:00 presso:
Campus di Macchia Romana
[Edificio 3D](#) (Dipartimento di Matematica,
Informatica ed Economia)
[Il piano, stanza 15](#)

Email: domenico.bloisi@unibas.it



Programma – Sistemi Operativi

- Introduzione ai sistemi operativi
- Gestione dei processi
- Sincronizzazione dei processi
- Gestione della memoria centrale
- Gestione della memoria di massa
- File system
- Sicurezza e protezione

Sicurezza e protezione

La sicurezza misura la fiducia nel fatto che l'integrità di un sistema e dei suoi dati siano preservati

La protezione è l'insieme di meccanismi che controllano l'accesso di processi e utenti alle risorse di un sistema informatico

Sicurezza

La sicurezza si occupa di preservare le risorse del sistema da:

- accessi non autorizzati
- distruzione o alterazione dolosa
- involontaria introduzione di elementi di incoerenza

Le risorse da preservare includono:

- informazione memorizzata nel sistema sotto forma di dati e programmi
- CPU
- memoria
- dischi
- connessioni di rete

Il problema della sicurezza

Le violazioni della sicurezza del sistema si possono classificare come *intenzionali (dolose)* o *accidentali*. Nell'elenco che segue sono comprese sia le *intrusioni accidentali* sia le *violazioni dolose*.

Violazione della riservatezza

Compromissione dell'integrità

Violazione della disponibilità

Appropriazione del servizio

Rifiuto del servizio
DOS (*Denial-Of-Service*)

Il problema della sicurezza

Violazione
della
riservatezza

- Lettura non autorizzata di dati
- Furto di informazioni

Compromissione
dell'integrità

- Modifica non autorizzata di dati
- Modifica codice sorgente

Violazione
della
disponibilità

- Distruzione non autorizzata di dati
- Sabotaggio di siti web

Il problema della sicurezza

Appropriazione
del servizio

- Uso non autorizzato delle risorse

Rifiuto del
servizio

- Blocco dell'utilizzo legittimo del sistema
- Attacchi DOS (Denial-Of-Service)

Sicurezza del sistema

Per proteggere il sistema è necessario prendere misure di sicurezza a quattro livelli:

Fisico

Rete

Sistema
operativo

Applicazione

Sicurezza del sistema

Fisico

- Edifici
- Macchine
- Stazioni di lavoro
- Terminali

Rete

- Linee di comunicazione private
- Linee condivise
- Connessioni Wi-Fi

Sicurezza del sistema

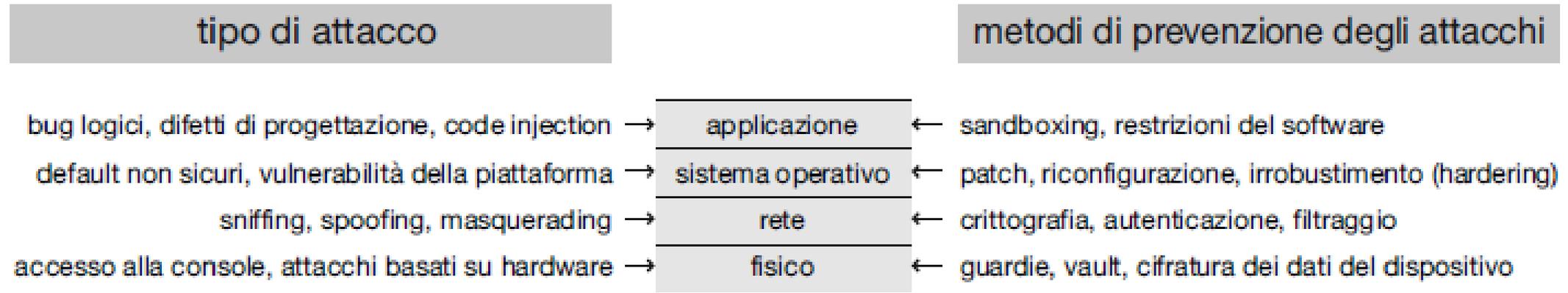
SO

- Impostazioni predefinite
- Parametri di configurazione
- Bug di sicurezza

Applicazione

- Programmi di terze parti
- Bug di sicurezza

Modello di sicurezza a quattro livelli



Il **modello di sicurezza a quattro livelli** è come una catena formata da anelli collegati: una vulnerabilità in uno qualsiasi dei suoi livelli può compromettere l'intero sistema.

Fattore umano

Le tecniche di ingegneria sociale utilizzano l'inganno per convincere le persone a rivelare informazioni riservate

Phishing

consiste nel contraffare e-mail o pagine web rendendole simili a quelle autentiche per spingere gli utenti tratti in inganno a comunicare informazioni confidenziali

Phishing

The screenshot shows the top section of the Italia news website. At the top left, there is a search bar and the word "Italia" followed by "Attualità". On the right, there are social media icons for Facebook, Twitter, and LinkedIn, along with a "24+" logo and an "ABBONATI" button. Below this, a navigation bar lists "Temi Caldi" such as Libia, Usa 2020, Piano Autostrade, Taglio cuneo fiscale, and Debito Italia. A row of three video thumbnails is displayed: "ITALIA Reddito di cittadinanza, ecco che lavori faranno i percettori", "MONDO L'abbattimento del Boeing 737-800 nei cieli di Teheran", and "IL MILANESE IMBRUTTITO L'economia spiegata dal Nano: il mutuo".

The main article is dated "23 dicembre 2019" and is categorized under "CYBER SICUREZZA". The title is "Truffa di Natale: hacker contro NoiPA, rubati stipendi e tredicesime a dipendenti pubblici". The sub-headline reads: "Operazione basata su tecniche di phishing, che riguarderebbe un numero non definito di dipendenti pubblici. Un furto che lascia spazio a molti interrogativi e al pesante dubbio di non poter recuperare il maltolto". The author is "di Biagio Simonetta". Below the text is a photograph of a person's hands typing on a keyboard at a desk, with an "ANSA" logo in the corner.

On the left side of the article, there is a sidebar with a list of tags: "Natale", "Iban", "Ing Bank", "NoiPA", and "CONSOB". Below the tags are buttons for "Salva" and "Commenta", and social media sharing icons for Facebook, Twitter, and LinkedIn.

On the right side, there is a section titled "Il meglio di 24+" containing a list of five featured articles:

- OCCUPAZIONE**
Lavoro, richiesta record di laureati. Quali sono i titoli più gettonati
- 24PLUS**
Auto elettriche, perché è urgente l'alternativa al cobalto nelle batterie
- REDDITI**
Negli ultimi 20 anni le pensioni italiane sono cresciute più degli stipendi
- L'INCHIESTA DELLA DOMENICA**
Quali sono le scuole che fanno trovare più velocemente il lavoro
- INDUSTRIA SOSTENIBILE**
La sfida difficile di Volkswagen, Daimler e Bmw verso l'auto elettrica

Minacce legate ai programmi

Il **malware** è un software progettato per *sfruttare, disabilitare o danneggiare* i sistemi informatici.

1. Un programma che agisce in modo clandestino o malevolo, anziché eseguire semplicemente la sua funzione dichiarata, è chiamato **cavallo di Troia**.
2. Una variante è un programma (detto “**trojan mule**”) che emula una procedura di login: l’ignaro utente, nella fase d’accesso a un terminale, crede di aver scritto erroneamente la propria password; prova ancora e, questa volta, ha successo → sottrazione del nome utente e password.
3. **Spyware** → talvolta accompagna un programma che l’utente ha scelto di installare

Ransomware

☰ MENU | 🔍 CERCA

la Repubblica

R+ | Rep: | ABBONATI | ACCEDI 👤

Tecnologia

HOME NEWS SPECIALI MOBILE SOCIAL NETWORK SICUREZZA PRODOTTI INTERATTIVI VIDEO



Il ransomware "terrorista": chiede il riscatto in bitcoin e minaccia un attacco bomba



Il messaggio che compare sul computer bloccato intima di pagare 20.000 dollari in bitcoin, altrimenti "una persona reclutata" appositamente farà esplodere la bomba in quell'edificio. Ma i dubbi sono tanti

Minimo privilegio



IL PRINCIPIO DEL MINIMO PRIVILEGIO

“Il principio del minimo privilegio: in un sistema, ogni programma e ogni utente dotato di privilegi dovrebbero operare con il minimo privilegio necessario per completare il proprio lavoro, allo scopo di ridurre il numero di potenziali interazioni tra programmi privilegiati al minimo necessario per poter operare correttamente, in modo che si possa essere ragionevolmente fiduciosi del non verificarsi di usi non intenzionali, indesiderati o impropri del privilegio.” Jerome H. Saltzer, nella descrizione di un principio di progettazione del sistema operativo Multics nel 1974:

<https://pdfs.semanticscholar.org/1c8d/06510ad449ad24fbdd164f8008cc730cab47.pdf>.

Trap door

Una trap door è un tipo di malware in cui il progettista di un programma o di un sistema può lasciare nel programma un buco segreto che solo lui è in grado di utilizzare

Logic bomb: trap door che si attiva solo al verificarsi di uno specifico insieme di condizioni logiche

Trap door nei compilatori: Malware XCodeGhost



The image shows a screenshot of a news article from the Italian newspaper LA STAMPA. The article is in the 'TECNOLOGIA' (Technology) section. The title is 'Attacco hacker contro l'App Store di Apple, a rischio anche WeChat'. The author is ANDREA NEPORI. The article was published on October 20, 2015, and last modified on June 24, 2019. The article text states: 'Il malware cinese XcodeGhost è riuscito a infettare applicazioni per iOS disponibili sull'App store. Colpite anche alcune app diffuse in Europa e negli Stati Uniti'. Below the text is an image of an iPhone home screen with various app icons like Clock, Calendar, Photos, and Maps. At the bottom of the screenshot, there is a URL: '/www.lastampa.it/promozioni/lettori/top-news/presentazione?ref=lastampa.abbonati.tntop_off'.

MENU TOP NEWS

LA STAMPA

TECNOLOGIA

NEWS GIOCHI IDEE PROVE TUTORIAL

ANDREA NEPORI

PUBBLICATO IL
20 Ottobre 2015

ULTIMA MODIFICA
24 Giugno 2019
ora: 10:06

f t e

Attacco hacker contro l'App Store di Apple, a rischio anche WeChat

Il malware cinese XcodeGhost è riuscito a infettare applicazioni per iOS disponibili sull'App store. Colpite anche alcune app diffuse in Europa e negli Stati Uniti



/www.lastampa.it/promozioni/lettori/top-news/presentazione?ref=lastampa.abbonati.tntop_off

Code injection

Overflow di un buffer: il più semplice vettore di code injection

```
#include <stdio.h>
#include <string.h>
#define BUFFER_SIZE 0

int main(int argc, char *argv[])
{
    int j = 0;
    char buffer[BUFFER_SIZE];
    int k = 0;
    if (argc < 2) {return -1;}

    strcpy(buffer,argv[1]);
    printf("K is %d, J is %d, buffer is %s\n",j,k,buffer);
    return 0;
}
```

Figura 16.2 Programma C che esemplifica il buffer overflow.

Buffer overflow

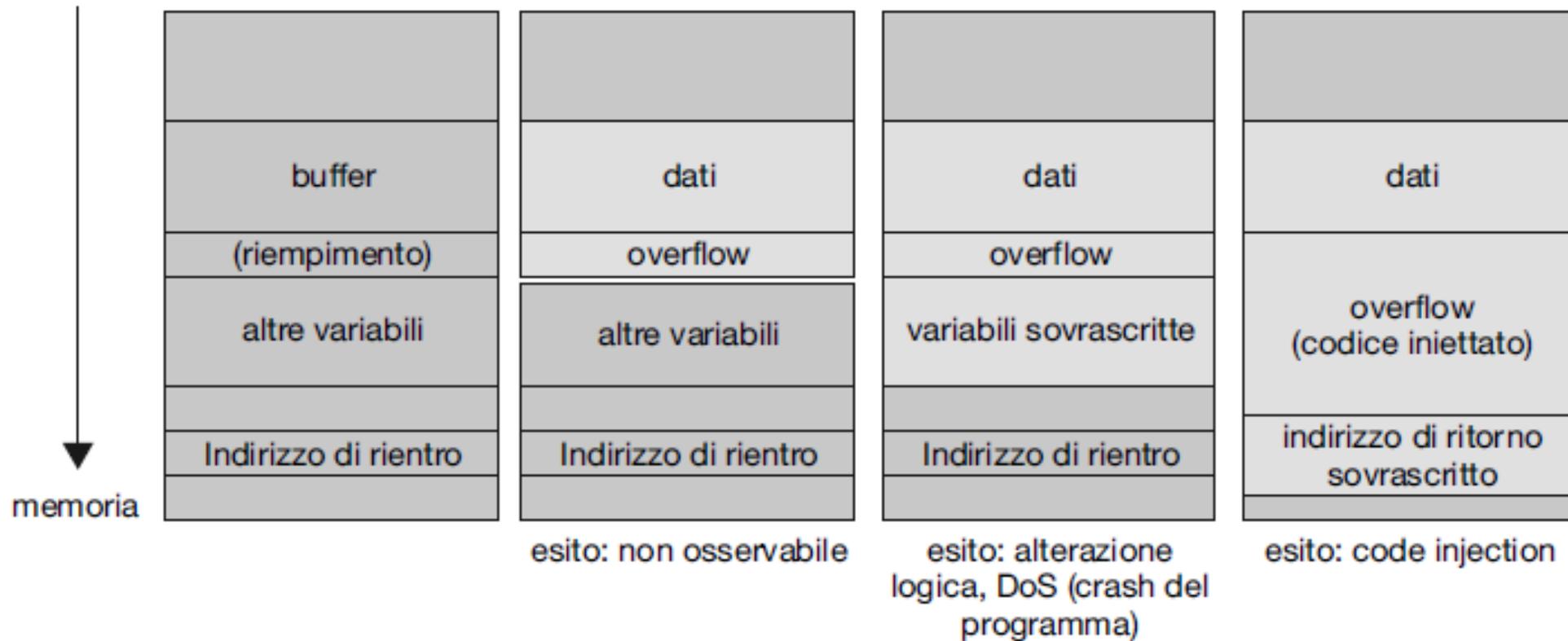


Figura 16.3 Possibili esiti di un buffer overflow.

Exploit shellcode

Un **exploit shellcode** è mostrato nella Figura 16.4.

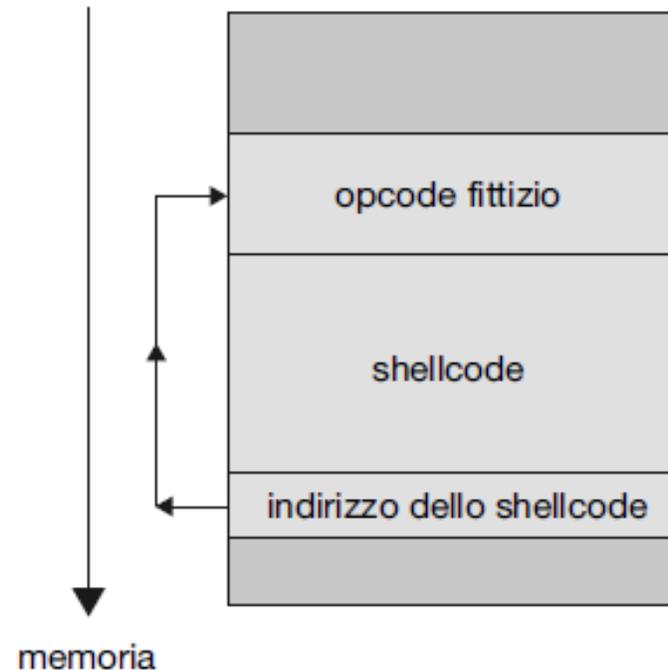


Figura 16.4 “Trampolino” per l’esecuzione di codice sfruttando un buffer overflow.

SQL injection

SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

SQL in web pages

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

Look at the following example which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):

Example

```
txtUserId = getRequestString("UserId");  
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

SQL injection based on 1 = 1

Look at the example above again. The original purpose of the code was to create an SQL statement to select a user, with a given user id.

If there is nothing to prevent a user from entering "wrong" input, the user can enter some "smart" input like this:

UserId: 105 OR 1=1

Then, the SQL statement will look like this:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

The SQL above is valid and will return ALL rows from the "Users" table, since **OR 1=1** is always TRUE.

SQL injection based on 1 = 1

Does the example above look dangerous? What if the "Users" table contains names and passwords?

The SQL statement above is much the same as this:

```
SELECT UserId, Name, Password FROM Users WHERE UserId = 105 or 1=1;
```

A hacker might get access to all the user names and passwords in a database, by simply inserting 105 OR 1=1 into the input field.

Virus

Virus: frammento di codice inserito in un programma legittimo.

I **virus** si autoriproducono e sono concepiti in modo da “contagiare” altri programmi → *crash del sistema*

Normalmente i **virus** si trasmettono per posta elettronica, tramite posta indesiderata (*SPAM*), e utilizzando tecniche di *phishing*.

Dopo che un virus raggiunge la macchina presa di mira, un programma chiamato **portatore di virus** (*virus dropper*) inserisce il virus nel sistema.

Worm

Si può fare una distinzione tra i virus, che richiedono attività da parte dell'uomo, e i **worm**, che usano una rete per replicarsi, senza l'aiuto dell'uomo.

Categoria di Virus

Esistono **migliaia di virus**, che tuttavia possono essere ricondotti ad alcune categorie principali:



Virus del boot sector

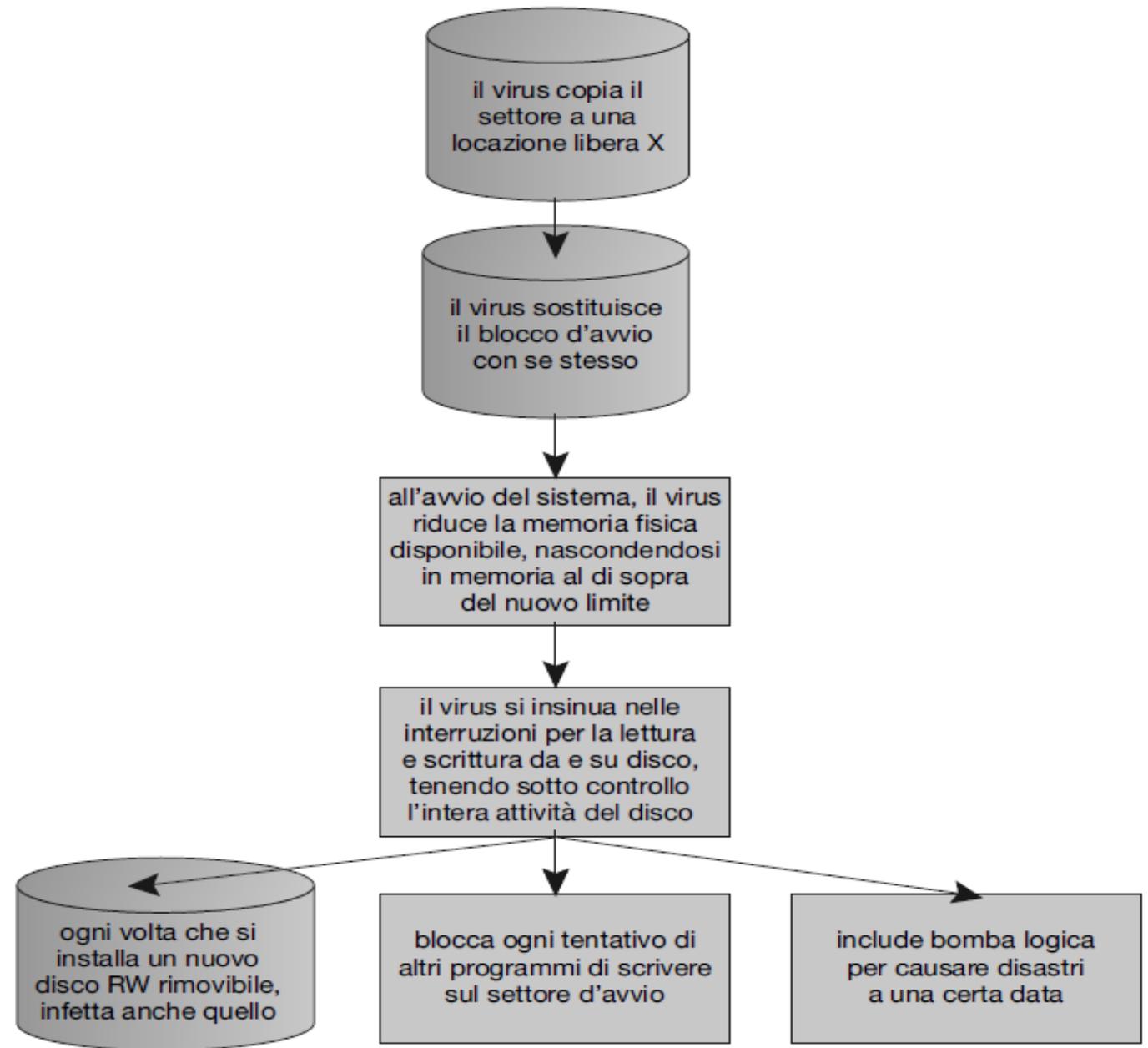


Figura 16.5 Virus del boot sector di un computer.

Macrovirus



Office

Windows

Surface

Xbox

Deals

Support

More ▾

Microsoft Support

Frequently asked questions about Word macro viruses

Summary

This article answers some of the more frequently asked questions concerning Word macro viruses.

More Information

1. Q. What are Word macro viruses?

Macro viruses are computer viruses that use an application's own macro programming language to distribute themselves. These macros have the potential to inflict damage to the document or to other computer software. These macro viruses can infect Word files as well as any other application that uses a programming language.

Minacce relative al sistema e alla rete

Attaccare il traffico di rete

Un utente malintenzionato può scegliere:

1. di rimanere passivo e intercettare il traffico di rete (questo attacco è comunemente indicato come **sniffing**);
2. di assumere un ruolo più attivo, mascherandosi come una delle parti (**spoofing**);
3. di diventare un **man-in-the-middle** (*uomo nel mezzo*) completamente attivo, che intercetta ed eventualmente modifica le transazioni tra due soggetti comunicanti.

Attacchi alla sicurezza

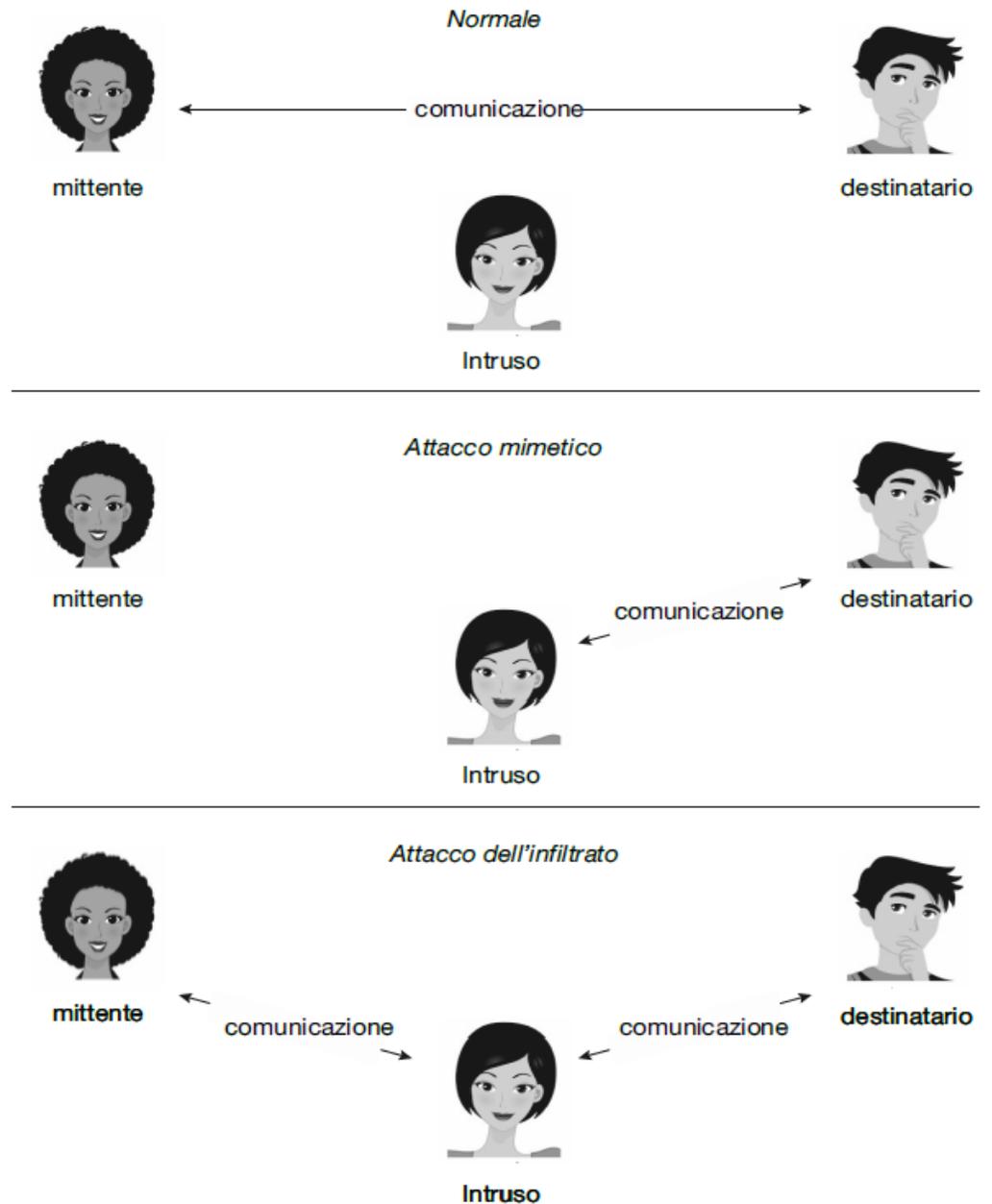


Figura 16.6 Attacchi comuni alla sicurezza.³

Attacchi denial of service

Attacco **denial-of-service (DoS)**: non mirano a ottenere informazioni o a sottrarre risorse, bensì a impedire l'uso corretto di un sistema o di una funzionalità.

Due categorie:

1. l'aggressore occupa un numero così alto di risorse di un servizio da bloccarne completamente la funzionalità;
2. il sabotaggio di una rete che ospita un servizio.

È impossibile impedire gli **attacchi denial-of-service**, poiché essi sfruttano gli stessi meccanismi del funzionamento normale.

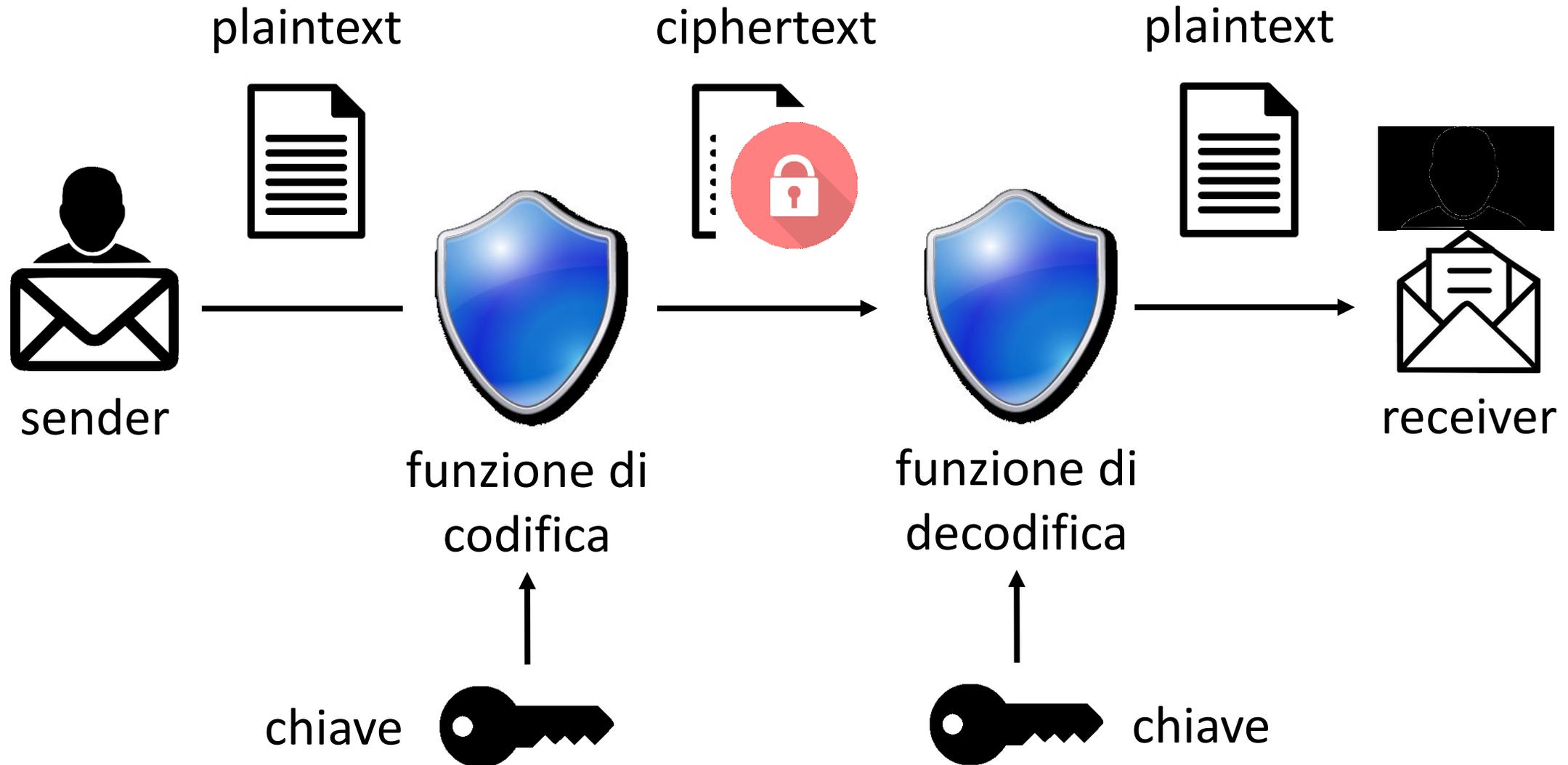
Ancor peggio: **attacchi denial-of-service distribuiti** (*distributed denial-of-service*, **DDOS**)

Crittografia

La crittografia è la scienza che studia le tecniche e le metodologie per cifrare (codificare) un testo in chiaro (*plaintext*), al fine di produrre un testo cifrato (*ciphertext*) comprensibile solo ad un destinatario legittimo (*receiver*)

Il receiver deve possedere l'informazione sufficiente (*chiave*) per decifrare il testo cifrato, recuperando così il testo in chiaro

Sistema Crittografico



Chiavi

La **crittografia** moderna si fonda su codici segreti, chiamati **chiavi**, che si distribuiscono selettivamente ai calcolatori di una rete e si usano per elaborare i messaggi.

La **crittografia** permette al destinatario di un messaggio di verificare che il messaggio sia stato creato da un calcolatore che possiede **una certa chiave**.

Cifratura

Cifratura
simmetrica

Cifratura
asimmetrica

Autenticazione

Cifratura

La **cifratura dei messaggi**, come si sa, è una pratica antica; alcuni algoritmi di cifratura risalgono all'antichità.

Un **algoritmo di cifratura** permette al mittente di un messaggio di imporre che solo un calcolatore che possiede una certa chiave possa leggere il messaggio.

La **cifratura** delimita l'insieme di coloro i quali ricevono informazioni, mentre l'**autenticazione** circoscrive il dominio di chi le trasmette.

La **cifratura simmetrica** richiede una chiave condivisa, mentre la **cifratura asimmetrica** è effettuata con una chiave pubblica e una chiave privata.

L'uso combinato dell'**autenticazione** e delle **funzioni hash** permette di verificare che i dati non abbiano subito modifiche.

Cifratura simmetrica

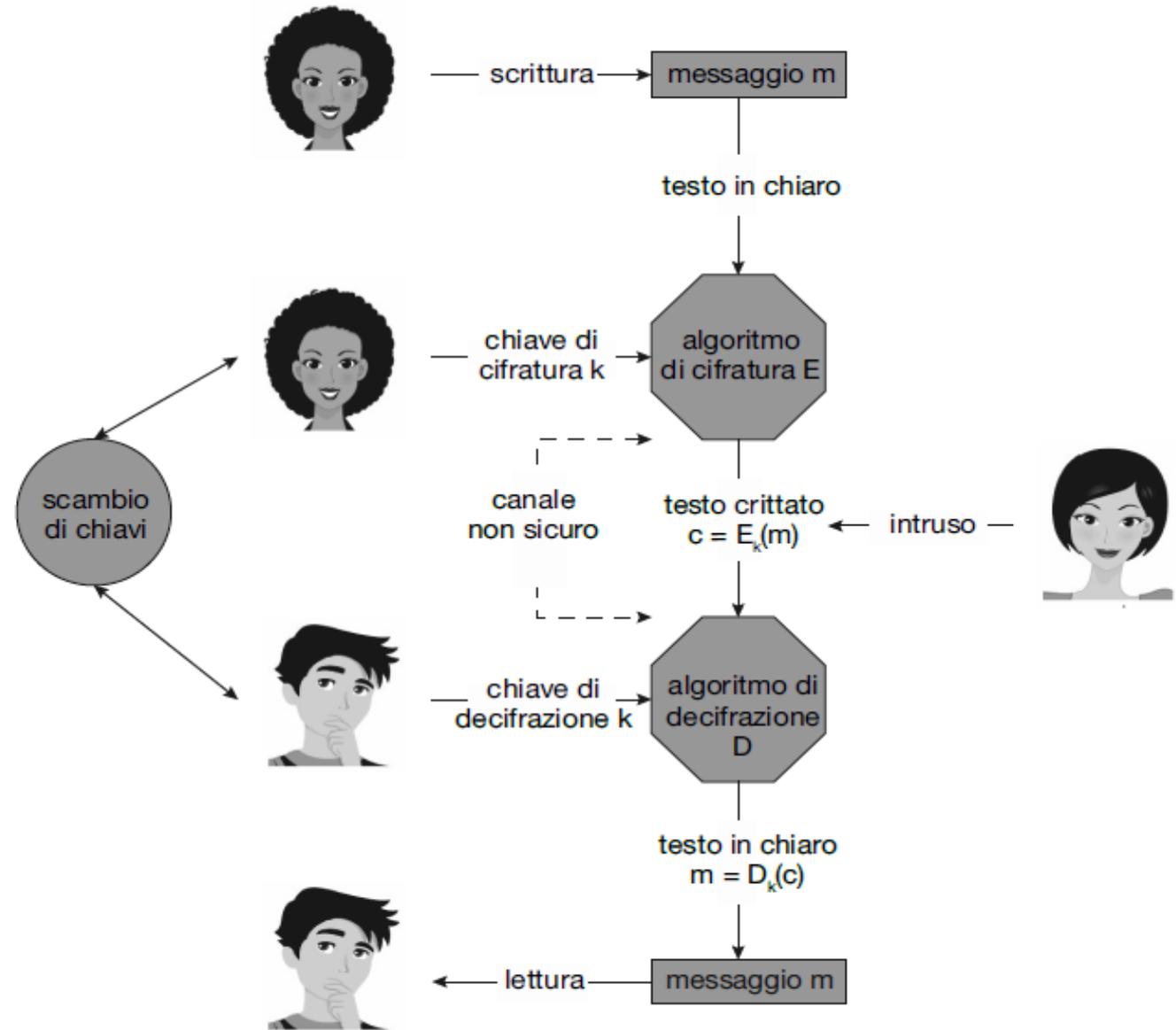


Figura 16.7 Comunicazione sicura su un canale non sicuro.⁴

Cifratura a chiave pubblica

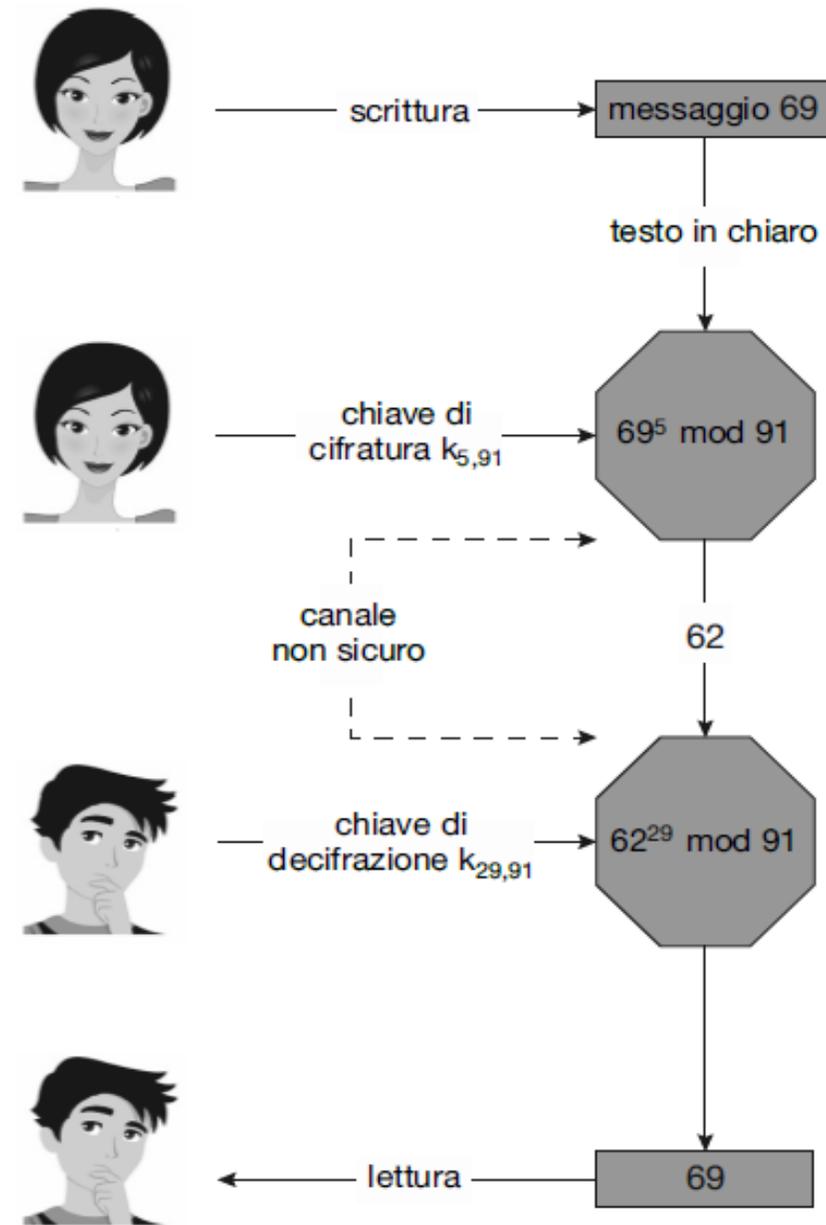


Figura 16.8 Cifratura e decifrazione per mezzo della crittografia asimmetrica RSA.⁵

Attacco alla cifratura a chiave pubblica

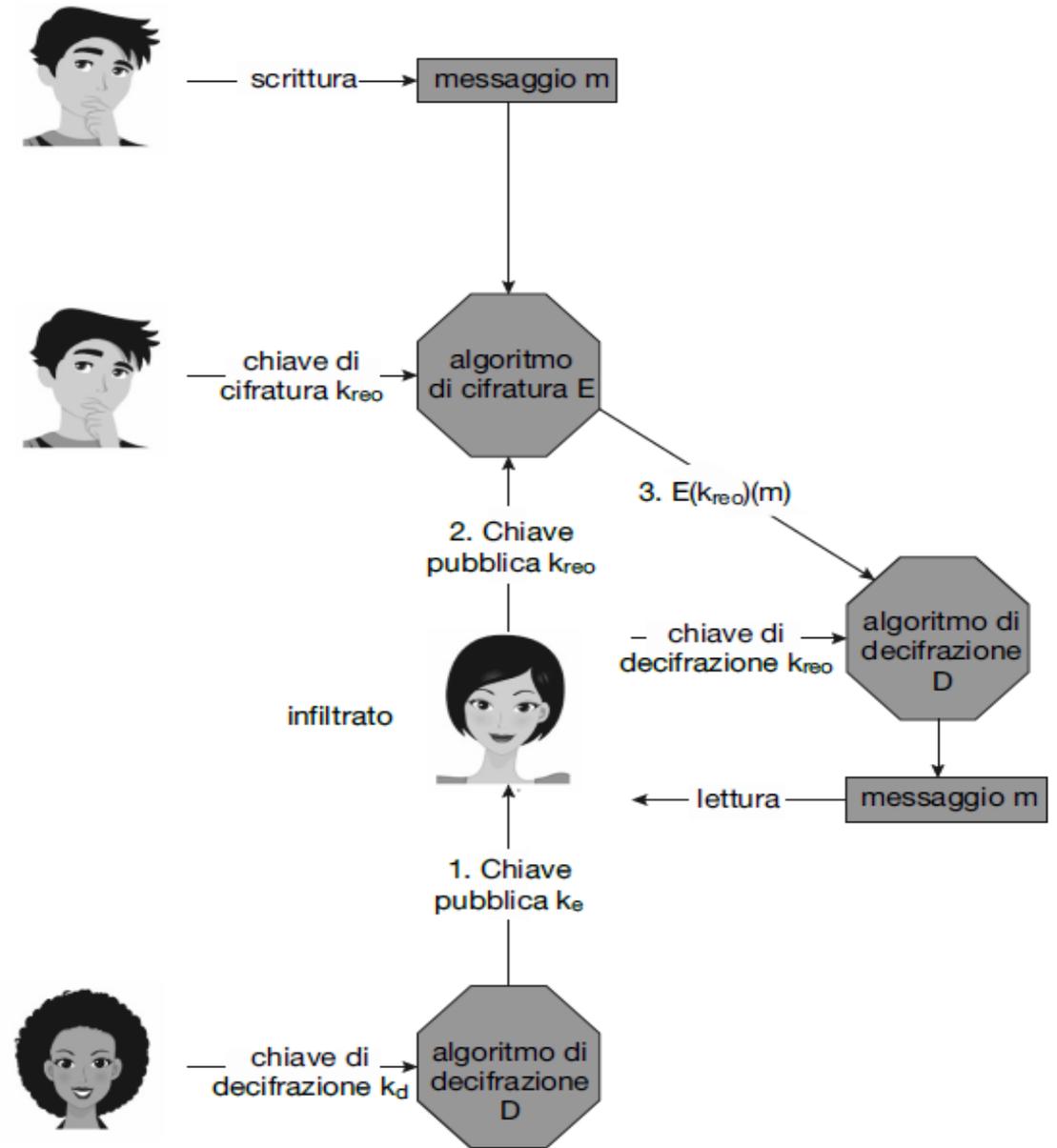


Figura 16.9 Attacco di interposizione alla cifratura asimmetrica.⁶

Autenticazione degli utenti

Le **password** si possono considerare un caso particolare di *chiavi* o di *abilitazioni*.

Ai tradizionali metodi di protezione basati su nome-utente e password, se ne possono affiancare altri:

Password monouso. Esse cambiano da sessione a sessione per evitare attacchi replay.

Autenticazione a due fattori richiede due elementi di autenticazione, per esempio un dispositivo hardware insieme a un PIN di attivazione.

Autenticazione multifattoriale impiega tre o più elementi. I metodi citati riducono fortemente le possibilità di falsificare l'autenticazione.

Misure di sicurezza

I metodi per prevenire o rilevare le violazioni alla sicurezza comprendono:

Politica di
sicurezza

Sistemi di
rilevamento
delle intrusioni

Programmi
antivirus

Auditing e il
log delle
attività

Monitoraggio
delle chiamate
di sistema

Firma digitale
del codice

Sandbox

Firewall

Firewall

Un **firewall** può separare una rete in più *domini*. Uno schema comune considera la rete Internet come *dominio non fidato*; prevede una rete parzialmente fidata, la cosiddetta **zona smilitarizzata** (*demilitarized zone, DMZ*), come *secondo dominio*; e un *terzo dominio* che comprende i calcolatori aziendali.

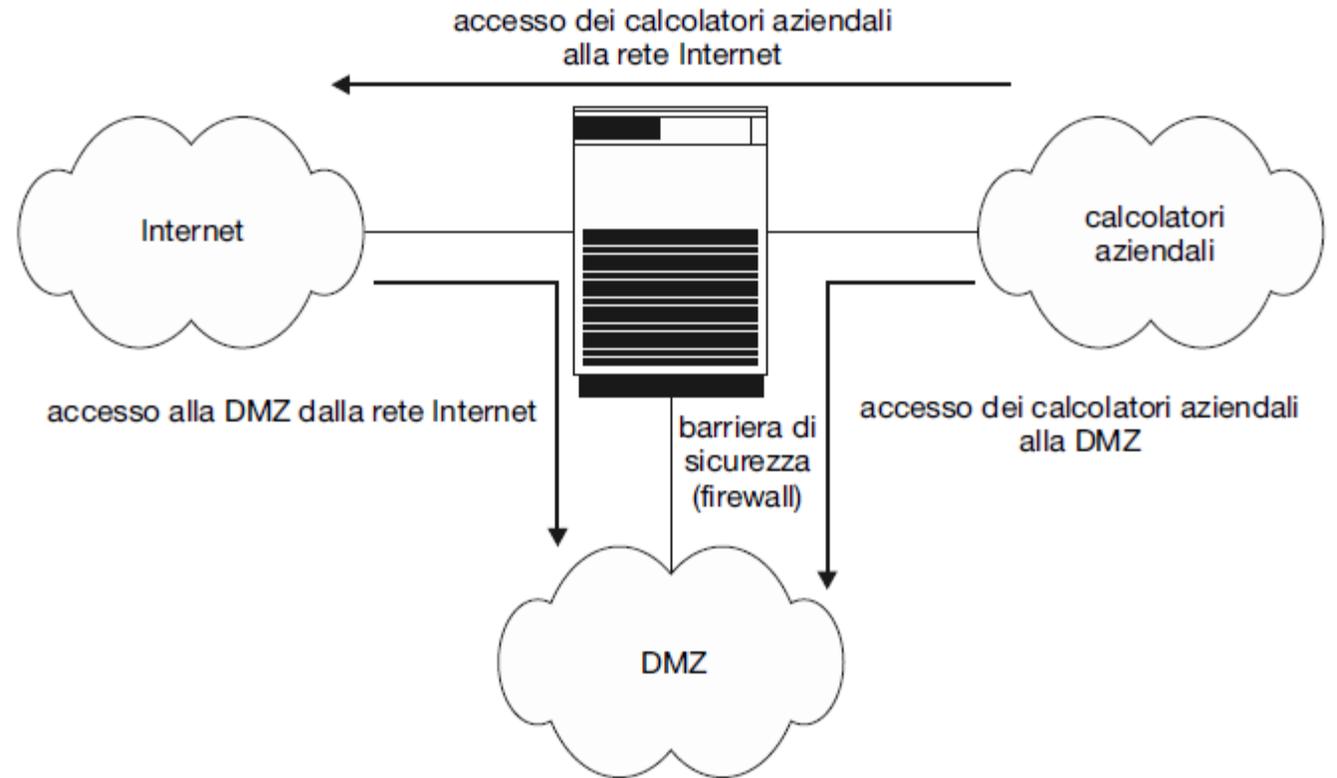


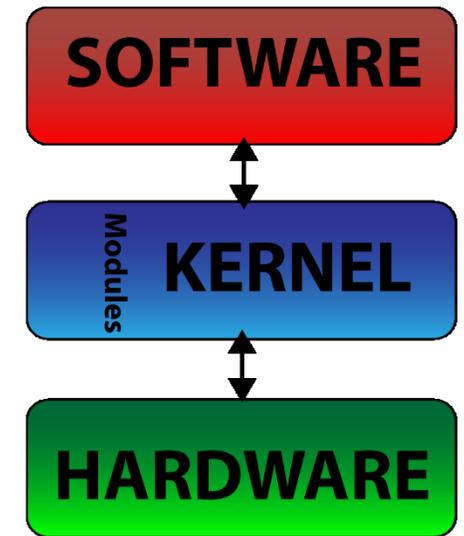
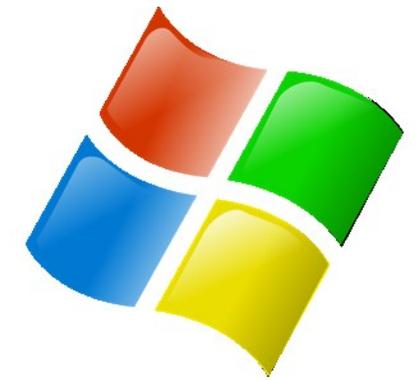
Figura 16.10 Sicurezza di rete con separazione in domini tramite firewall.



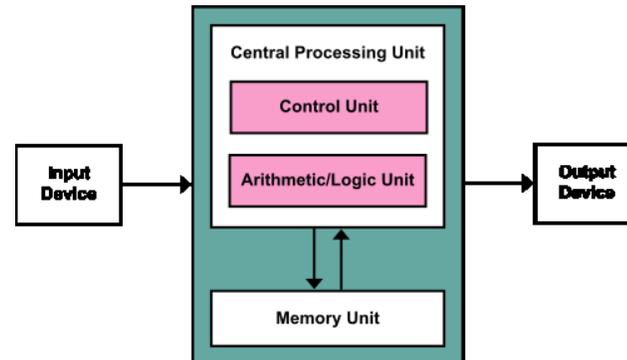
**UNIVERSITÀ DEGLI STUDI
DELLA BASILICATA**

*Corso di Sistemi Operativi
A.A. 2019/20*

Sicurezza



Docente:
**Domenico Daniele
Bloisi**



Gennaio 2020