

Introduzione ai problemi di sicurezza nei sistemi informatici

rif.:

C.P. Pfleeger & S.L. Pfleeger, Sicurezza in informatica, Cap.1
D. Gollmann, Computer Security, Capp. 1, 2

Giuseppe Scollo

**Corso di Laurea in Informatica applicata
Università di Catania, sede di Comiso (RG)**

6 marzo 2008



Sommario

- 1 **Problemi di sicurezza dei sistemi informatici**
 - Introduzione al problema della sicurezza
 - Attacchi alla sicurezza
 - Significato di sicurezza informatica
 - Crimine informatico
 - Metodi di difesa della sicurezza
- 2 **Esercizi e Problemi**



Sommario

- 1 **Problemi di sicurezza dei sistemi informatici**
 - Introduzione al problema della sicurezza
 - Attacchi alla sicurezza
 - Significato di sicurezza informatica
 - Crimine informatico
 - Metodi di difesa della sicurezza

- 2 **Esercizi e Problemi**



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione di**
 - persone (in espressioni tecniche)
 - beni materiali (dall'hardware al software)
 - informazioni riservate

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - tecnologie rudimentali
 - risorse limitate (umane, materiali, economiche)
 - difficoltà del controllo fisico
 - mancanza di collaborazione e comunicazione



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema...



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema...



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema...



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre

- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema...



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema...



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema. . .

... fenomeno ancora attuale!



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema. . .

... fenomeno ancora attuale!



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema. . .

... fenomeno ancora attuale!



Problemi tradizionali di sicurezza

cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema. . .

... fenomeno ancora attuale!



Problemi tradizionali di sicurezza

cosa significa "sicuro"?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
 - **persone** da aggressioni fisiche
 - **beni materiali** dall'appropriazione indebita
 - **informazioni** riservate da accessi indesiderati

per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
 - **tecnologie rudimentali**
di allarme, identificazione, trasporto, comunicazione
 - **inevitabilità del contatto fisico**
per il trasferimento di beni materiali o informazioni
 - frequente **sottovalutazione** del problema. . .

... fenomeno ancora attuale!



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a:
 - scarsa conoscenza del problema
 - timore del danno all'immagine
 - scarsa conoscenza del danno
 - scarsa conoscenza del costo
- nel seguito si prendono in esame:
 - i rischi di sicurezza nei sistemi informatici
 - le contromisure e controlli adottati
 - le vulnerabilità dei sistemi
 - le aree di rischio informatico
- **intrusione nei sistemi informatici:**
 - significato della vulnerabilità



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di
protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**
grande varietà di: bersagli, tipi di attacchi, vulnerabilità
principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di
protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**
grande varietà di: bersagli, tipi di attacchi, vulnerabilità

principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subìto
 - **carenze legislative** in materia di protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**
grande varietà di: bersagli, tipi di attacchi, vulnerabilità

principio della penetrazione più facile

Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di
protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**
grande varietà di: bersagli, tipi di attacchi, vulnerabilità
principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di
protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**

grande varietà di: bersagli, tipi di attacchi, vulnerabilità
principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di
protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**

grande varietà di: bersagli, tipi di attacchi, vulnerabilità

principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**

grande varietà di: bersagli, tipi di attacchi, vulnerabilità
principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di
protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**

grande varietà di: bersagli, tipi di attacchi, vulnerabilità

principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**

grande varietà di: bersagli, tipi di attacchi, vulnerabilità
principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**

grande varietà di: bersagli, tipi di attacchi, vulnerabilità

principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all’immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**
grande varietà di: bersagli, tipi di attacchi, vulnerabilità

principio della penetrazione più facile



Problemi di sicurezza dei sistemi informatici

cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
 - **sottostima del danno** provocabile da intrusioni
 - **timore del danno all'immagine**
associato alla denuncia di un crimine informatico subito
 - **carenze legislative** in materia di protezione del *diritto di proprietà dell'informazione*
- nel seguito si prendono in esame
 - i **rischi** di sicurezza nei sistemi informatici
 - le **contromisure e controlli** disponibili
 - le **vulnerabilità** dei sistemi informatici
 - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici:**
grande varietà di: bersagli, tipi di attacchi, vulnerabilità
principio della penetrazione più facile



Attacco e difesa: concetti di base

vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione

una risorsa o il

controllo di un

o blocco di

componenti HW/SW del sistema o **dati** contenuti in essi

- una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
- le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*

si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine



Attacco e difesa: concetti di base

vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione

- **accesso a**, ○
- **modifica di**, ○
- **blocco di**

componenti HW/SW del sistema o **dati** contenuti in essi

- una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
- le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*

si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine



Attacco e difesa: concetti di base

vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione

- **accesso a**, o
- **modifica di**, o
- **blocco di**

componenti HW/SW del sistema o **dati** contenuti in essi

- una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
- le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*

si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine



Attacco e difesa: concetti di base

vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione

- **accesso a**, o
- **modifica di**, o
- **blocco di**

componenti HW/SW del sistema o **dati** contenuti in essi

- una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
- le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*

si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine



Attacco e difesa: concetti di base

vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione

- **accesso a**, o
- **modifica di**, o
- **blocco di**

componenti HW/SW del sistema o **dati** contenuti in essi

- una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
- le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*

si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine



Attacco e difesa: concetti di base

vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione

- **accesso a**, o
- **modifica di**, o
- **blocco di**

componenti HW/SW del sistema o **dati** contenuti in essi

- una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
- le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*

si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine

Attacco e difesa: concetti di base

vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione
 - **accesso a**, o
 - **modifica di**, o
 - **blocco di componenti HW/SW** del sistema o **dati** contenuti in essi
 - una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
 - le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*
- si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine

Attacco e difesa: concetti di base

vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione
 - **accesso a**, o
 - **modifica di**, o
 - **blocco di componenti HW/SW** del sistema o **dati** contenuti in essi
- una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
- le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*

si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine

Attacco e difesa: concetti di base

vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione
 - **accesso a**, o
 - **modifica di**, o
 - **blocco di componenti HW/SW** del sistema o **dati** contenuti in essi
 - una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
 - le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*
- si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine



Vulnerabilità, minaccia, controllo

un esempio illustrativo



Vulnerabilità, minaccia, controllo

un esempio illustrativo

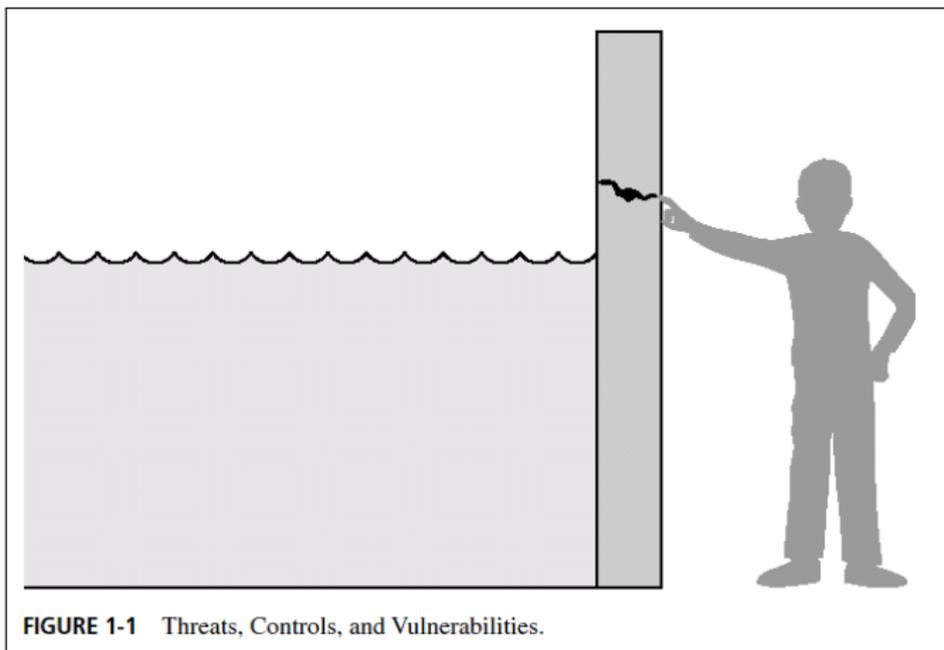


FIGURE 1-1 Threats, Controls, and Vulnerabilities.



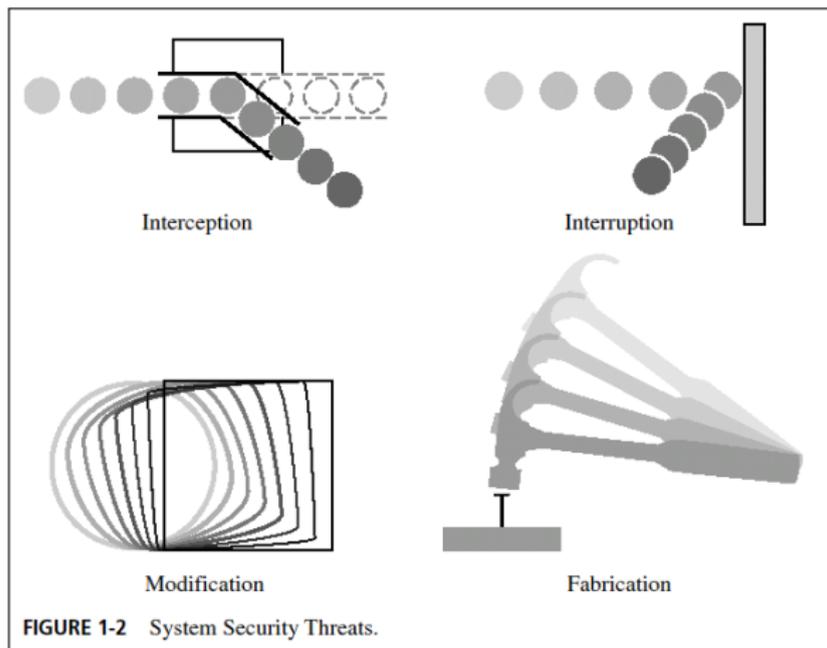
Minacce alla sicurezza di sistema

intercettazione, interruzione, modifica, contraffazione



Minacce alla sicurezza di sistema

intercettazione, interruzione, modifica, contraffazione



Condizioni necessarie all'attacco

metodo, opportunità, motivo (MOM)

un attaccante deve disporre di

- **metodo:**
abilità, conoscenze e strumenti necessari all'attacco
 - **opportunità** di accesso al sistema
 - **motivo** per condurre l'attacco
- condizioni **tutte necessarie**
alla messa in opera dell'attacco, *però...*
*tutte **inerentemente difficili da contrastare!***



Condizioni necessarie all'attacco

metodo, opportunità, motivo (MOM)

un attaccante deve disporre di

- **metodo**:
abilità, conoscenze e strumenti necessari all'attacco
 - **opportunità** di accesso al sistema
 - **motivo** per condurre l'attacco
- condizioni **tutte necessarie**
alla messa in opera dell'attacco, *però* . . .
tutte *inerentemente* **difficili da contrastare!**



Condizioni necessarie all'attacco

metodo, opportunità, motivo (MOM)

un attaccante deve disporre di

- **metodo:**
abilità, conoscenze e strumenti necessari all'attacco
 - **opportunità** di accesso al sistema
 - **motivo** per condurre l'attacco
- condizioni **tutte necessarie**
alla messa in opera dell'attacco, *però* . . .
tutte *inerentemente* **difficili da contrastare!**



Condizioni necessarie all'attacco

metodo, opportunità, motivo (MOM)

un attaccante deve disporre di

- **metodo:**
abilità, conoscenze e strumenti necessari all'attacco
 - **opportunità** di accesso al sistema
 - **motivo** per condurre l'attacco
- condizioni **tutte necessarie**
alla messa in opera dell'attacco, *però* . . .
tutte *inerentemente* **difficili da contrastare!**



Condizioni necessarie all'attacco

metodo, opportunità, motivo (MOM)

un attaccante deve disporre di

- **metodo**:
abilità, conoscenze e strumenti necessari all'attacco
- **opportunità** di accesso al sistema
- **motivo** per condurre l'attacco

condizioni **tutte necessarie**
alla messa in opera dell'attacco, *però* . . .

tutte *inerentemente* **difficili da contrastare!**



Condizioni necessarie all'attacco

metodo, opportunità, motivo (MOM)

un attaccante deve disporre di

- **metodo**:
abilità, conoscenze e strumenti necessari all'attacco
- **opportunità** di accesso al sistema
- **motivo** per condurre l'attacco

condizioni **tutte necessarie**
alla messa in opera dell'attacco, *però* . . .

tutte *inerentemente* **difficili da contrastare!**



Condizioni necessarie all'attacco

metodo, opportunità, motivo (MOM)

un attaccante deve disporre di

- **metodo**:
abilità, conoscenze e strumenti necessari all'attacco
 - **opportunità** di accesso al sistema
 - **motivo** per condurre l'attacco
- condizioni **tutte necessarie**
alla messa in opera dell'attacco, *però* . . .
tutte *inerentemente* **difficili da contrastare!**



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

es. informazioni personali, negoziazioni, privacy
es. documenti riservati, dati della difesa

integrità: **modifica riservata** solo a parti autorizzate

es. mutamenti significativi, documenti
es. dati critici del sistema

disponibilità: **garanzia di servizio** alle parti autorizzate

es. servizi essenziali, servizi di emergenza



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

molteplici significati, dipendenti
dall'*oggetto* e dal *contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- molteplici aspetti, anche *prestazionali*
- area di *ricerca* nello studio della sicurezza



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

molteplici significati, dipendenti
dall'*oggetto* e dal *contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- molteplici aspetti, anche *prestazionali*
- area di *ricerca* nello studio della sicurezza



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

*molteplici significati, dipendenti
dall'oggetto e dal contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- *molteplici aspetti, anche prestazionali*
- *area di ricerca nello studio della sicurezza*



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

*molteplici significati, dipendenti
dall'oggetto e dal contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- *molteplici aspetti, anche prestazionali*
- *area di ricerca nello studio della sicurezza*



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

*molteplici significati, dipendenti
dall'oggetto e dal contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- *molteplici aspetti, anche prestazionali*
- *area di ricerca nello studio della sicurezza*



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

*molteplici significati, dipendenti
dall'oggetto e dal contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- *molteplici aspetti, anche prestazionali*
- *area di ricerca nello studio della sicurezza*



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

molteplici significati, dipendenti
dall'*oggetto* e dal *contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- molteplici aspetti, anche *prestazionali*
- area di *ricerca* nello studio della sicurezza



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

molteplici significati, dipendenti
dall'*oggetto* e dal *contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- molteplici aspetti, anche *prestazionali*
- area di *ricerca* nello studio della sicurezza



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

molteplici significati, dipendenti
dall'*oggetto* e dal *contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- molteplici aspetti, anche *prestazionali*
- area di *ricerca* nello studio della sicurezza

Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

molteplici significati, dipendenti
dall'*oggetto* e dal *contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- molteplici aspetti, anche *prestazionali*
- area di *ricerca* nello studio della sicurezza



Proprietà caratteristiche della sicurezza

riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
 - visibilità
 - lettura
 - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

molteplici significati, dipendenti
dall'*oggetto* e dal *contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- molteplici aspetti, anche *prestazionali*
- area di *ricerca* nello studio della sicurezza

Relazione tra caratteristiche di sicurezza minacce e contromisure specifiche

attacchi alla
riservatezza:

intercettazione
furto

integrità:

modifica
distruzione

disponibilità:

denegazione
distruzione



Relazione tra caratteristiche di sicurezza minacce e contromisure specifiche

attacchi alla

riservatezza:

indebito
accesso

integrità:

indebita
modifica

disponibilità:

diniego
di
servizio



Relazione tra caratteristiche di sicurezza minacce e contromisure specifiche

attacchi alla
riservatezza:

**indebito
accesso**

integrità:

**indebita
modifica**

disponibilità:

**diniego
di
servizio**



Relazione tra caratteristiche di sicurezza minacce e contromisure specifiche

attacchi alla
riservatezza:

**indebito
accesso**

integrità:

**indebita
modifica**

disponibilità:

**diniego
di
servizio**



Relazione tra caratteristiche di sicurezza minacce e contromisure specifiche

attacchi alla
riservatezza:

**indebito
accesso**

integrità:

**indebita
modifica**

disponibilità:

**diniego
di
servizio**



Relazione tra caratteristiche di sicurezza

minacce e contromisure specifiche

attacchi alla
riservatezza:

**indebito
accesso**

integrità:

**indebita
modifica**

disponibilità:

**diniego
di
servizio**

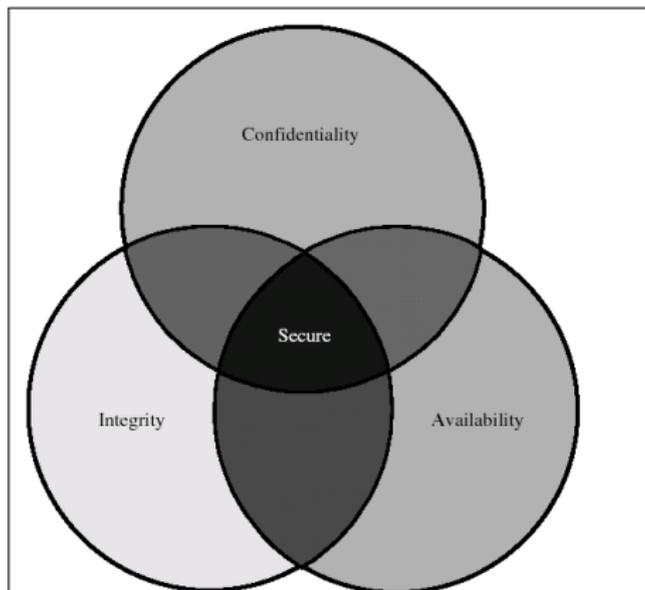


FIGURE 1-3 Relationship Between Confidentiality, Integrity, and Availability.



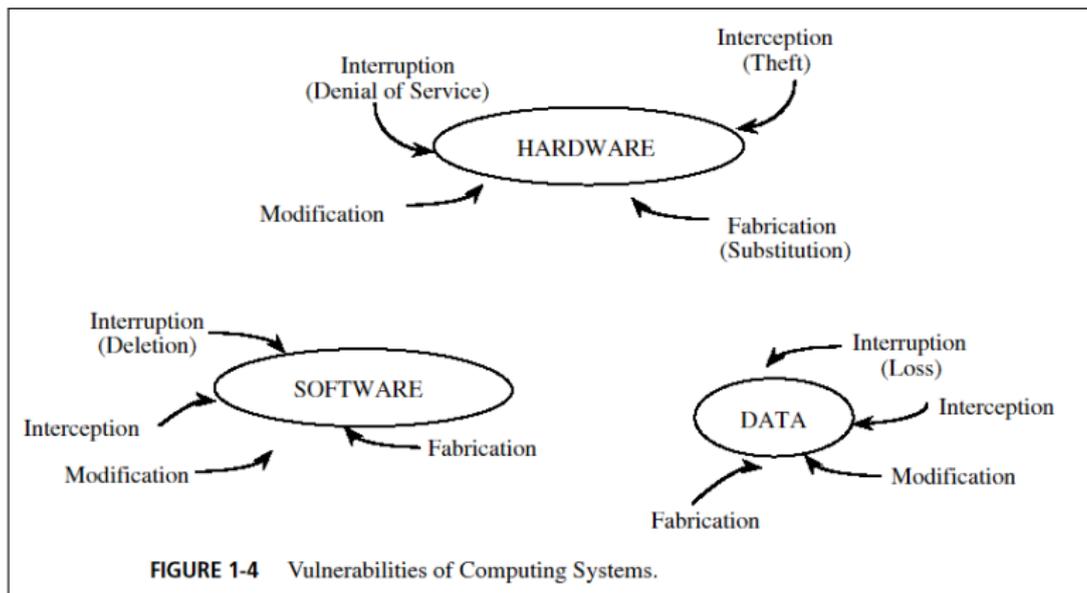
Vulnerabilità dei sistemi informatici

un quadro generale



Vulnerabilità dei sistemi informatici

un quadro generale



Vulnerabilità hardware

esposizione a . . .

- minacce intenzionali, e.g.:
 - furto di componenti fisici
 - sabotaggio del hardware, o della struttura costituzionale o aggiunta di componenti
 - introduzione del virus di compromissione
 - sovraccarico di traffico o di energia
- minacce non intenzionali, e.g.:
 - degradazione di componenti operative (temperatura, umidità, umidità, elettromagnetismo, interferenze, materiali dannosi)



Vulnerabilità hardware

esposizione a . . .

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a . . .

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a...

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali** (temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi** (polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a . . .

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a...

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico ⇒ *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a...

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a . . .

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a...

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a...

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a...

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a...

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniego di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori tecnici**, uso di **strumenti impropri**



Vulnerabilità hardware

esposizione a...

- **minacce intenzionali**, e.g.:
 - **furto** di componenti, dispositivi, sistemi
 - **sabotaggio** del funzionamento, fino alla *distruzione*
 - **sostituzione o aggiunta** di componenti o dispositivi
 - **intercettazione** del flusso di informazione
 - **sovraccarico** di traffico \Rightarrow *diniogo di servizio*
- **minacce non intenzionali**, e.g.:
 - alterazione di condizioni operative **ambientali**
(temperatura, umidità, alimentazione elettrica, etc.)
 - commistione con **materiali dannosi**
(polvere, fumi, bevande, olio, etc.)
 - **usura** dei materiali
 - intrusione di **roditori**
 - **errori** tecnici, uso di **strumenti impropri**



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di backup e ripristino
 - controllo di versione
 - parti della più recente gestione delle configurazioni
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - bomba logica
 - cavallo di Troia, virus
 - trojan
 - targa informatica
 - modifica di sistema ← carenze di controllo
 - installazione di programmi non autorizzati
- **furto**



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ← carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ← carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - bomba logica
 - cavallo di Troia, virus
 - trapdoor
 - falla informativa
 - **modifica di sistema** ← carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ⇐ carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ⇐ carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ⇐ carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ⇐ carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ⇐ carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ⇐ carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia non autorizzata**,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ⇐ carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright*, brevetti, *copyleft*. . .



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ⇐ carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright, brevetti, copyleft. . .*



Vulnerabilità software

facilità di . . .

- **cancellazione**: lacune nel (o assenza di)
 - sistema di **backup** periodico
 - **controllo di versione**,
parte della più generale **gestione delle configurazioni**
- **modifica** ⇒ arresto o (mal)funzionamento [improprio]
 - **bomba logica**
 - **cavallo di Troia, virus**
 - **trapdoor**
 - **falla informativa**
 - **modifica di sistema** ⇐ carenza di controllo
su installazione e/o esecuzione di programmi
- **furto**
 - più precisamente: **copia** non autorizzata,
violazione del *diritto di proprietà intellettuale*
 - si discute di: *copyright*, brevetti, *copyleft*. . .



Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

• *durata limitata*

• *fonti multiple*

di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*



Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
di *difficile misura!*
 - **costo** di ricostruzione,
in caso di perdita
 - **danno** per intercettazione,
modifica, indisponibilità

di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*



Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
di *difficile misura!*
 - costo di ricostruzione,
in caso di perdita
 - danno per intercettazione,
modifica, indisponibilità

di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*



Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
di *difficile misura!*
 - **costo** di ricostruzione,
in caso di perdita
 - **danno** per intercettazione,
modifica, indisponibilità

di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*



Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
di *difficile misura!*
 - **costo** di ricostruzione,
in caso di perdita
 - **danno** per intercettazione,
modifica, indisponibilità

di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*



Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
di *difficile misura!*
 - **costo** di ricostruzione,
in caso di perdita
 - **danno** per intercettazione,
modifica, indisponibilità

di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*

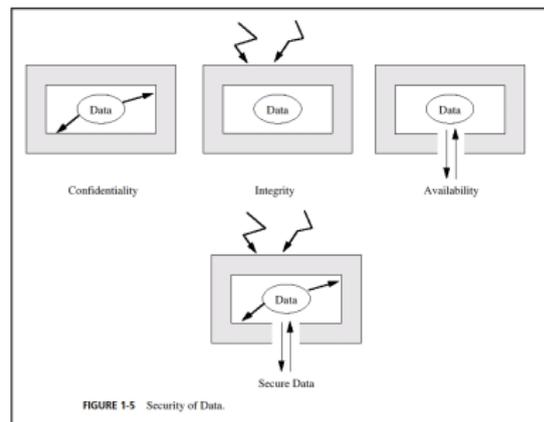


Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
di *difficile misura!*
 - **costo** di ricostruzione,
in caso di perdita
 - **danno** per intercettazione,
modifica, indisponibilità



di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*

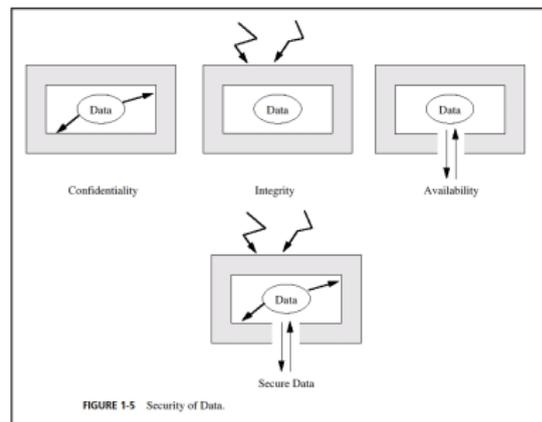


Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
di *difficile misura!*
 - **costo** di ricostruzione,
in caso di perdita
 - **danno** per intercettazione,
modifica, indisponibilità



di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*

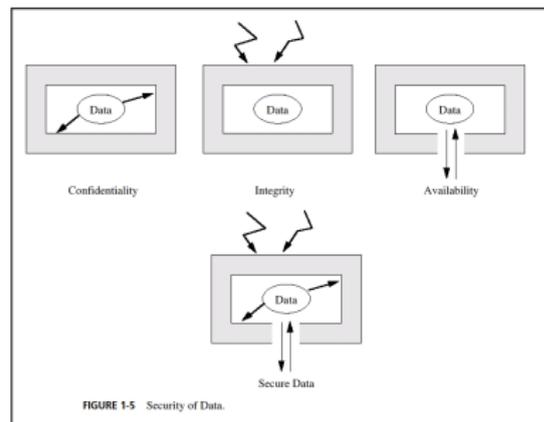


Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
di *difficile misura!*
 - **costo** di ricostruzione,
in caso di perdita
 - **danno** per intercettazione,
modifica, indisponibilità



di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*

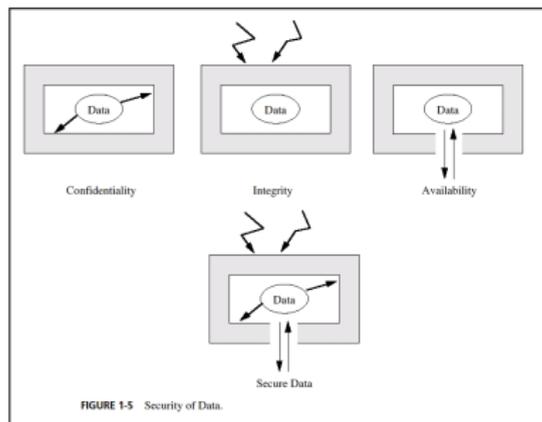


Vulnerabilità dei dati

... ⇒ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
di *difficile misura!*
 - **costo** di ricostruzione,
in caso di perdita
 - **danno** per intercettazione,
modifica, indisponibilità



di *durata limitata*: ⇒ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*



Crimine informatico

una definizione molto ampia. . .

crimine che riguarda un sistema informatico
o messo in opera con l'ausilio di uno

- definizioni migliori richiedono la precisazione del concetto di *norma sui sistemi informatici*, ad es:

violazione di norma penale sui sistemi informatici

- inesistenza di **statistiche** sul crimine informatico
- tuttavia, fenomeno di crescente **rilevanza sociale**, per la rapida diffusione dell'informatica nella vita quotidiana
- chi sono i "*criminali informatici*"?



Crimine informatico

una definizione molto ampia. . .

crimine che riguarda un sistema informatico o messo in opera con l'ausilio di uno

- definizioni migliori richiedono la precisazione del concetto di *norma sui sistemi informatici*, ad es:

violazione di norma penale sui sistemi informatici

- inesistenza di **statistiche** sul crimine informatico
- tuttavia, fenomeno di crescente **rilevanza sociale**, per la rapida diffusione dell'informatica nella vita quotidiana
- chi sono i "*criminali informatici*"?



Crimine informatico

una definizione molto ampia. . .

crimine che riguarda un sistema informatico o messo in opera con l'ausilio di uno

- definizioni migliori richiedono la precisazione del concetto di *norma sui sistemi informatici*, ad es:

violazione di norma penale sui sistemi informatici

- inesistenza di **statistiche** sul crimine informatico
- tuttavia, fenomeno di crescente **rilevanza sociale**, per la rapida diffusione dell'informatica nella vita quotidiana
- chi sono i "*criminali informatici*"?



Crimine informatico

una definizione molto ampia. . .

**crimine che riguarda un sistema informatico
o messo in opera con l'ausilio di uno**

- definizioni migliori richiedono la precisazione del concetto di *norma sui sistemi informatici*, ad es:

violazione di norma penale sui sistemi informatici

- inesistenza di **statistiche** sul crimine informatico
- tuttavia, fenomeno di crescente **rilevanza sociale**, per la rapida diffusione dell'informatica nella vita quotidiana
- chi sono i "*criminali informatici*"?



Crimine informatico

una definizione molto ampia. . .

**crimine che riguarda un sistema informatico
o messo in opera con l'ausilio di uno**

- definizioni migliori richiedono la precisazione del concetto di *norma sui sistemi informatici*, ad es:

violazione di norma penale sui sistemi informatici

- inesistenza di **statistiche** sul crimine informatico
- tuttavia, fenomeno di crescente **rilevanza sociale**, per la rapida diffusione dell'informatica nella vita quotidiana
- chi sono i "*criminali informatici*"?



Crimine informatico

una definizione molto ampia. . .

crimine che riguarda un sistema informatico o messo in opera con l'ausilio di uno

- definizioni migliori richiedono la precisazione del concetto di *norma sui sistemi informatici*, ad es:

violazione di norma penale sui sistemi informatici

- inesistenza di **statistiche** sul crimine informatico
- tuttavia, fenomeno di crescente **rilevanza sociale**, per la rapida diffusione dell'informatica nella vita quotidiana
- chi sono i "*criminali informatici*"?



Crimine informatico

una definizione molto ampia. . .

crimine che riguarda un sistema informatico o messo in opera con l'ausilio di uno

- definizioni migliori richiedono la precisazione del concetto di *norma sui sistemi informatici*, ad es:

violazione di norma penale sui sistemi informatici

- inesistenza di **statistiche** sul crimine informatico
- tuttavia, fenomeno di crescente **rilevanza sociale**, per la rapida diffusione dell'informatica nella vita quotidiana
- chi sono i "*criminali informatici*"?



Criminali informatici

tipologie e caratteristiche

- **dilettanti**

- sono i più numerosi
- sono i più "sinceri"
- sono i più "variabili"
- sono i più "pericolosi"

- **crackers** (non "hackers"!)

- sono persone disoccupate con un'istruzione superiore
- sono "hackers" come hobby, "crackers" come professione
- sono i più "pericolosi"

- **criminali professionisti...**

- sono i più "pericolosi"
- sono i più "variabili"
- sono i più "sinceri"
- sono i più numerosi



Criminali informatici

tipologie e caratteristiche

● **dilettanti**

- *maggioranza* degli autori di crimini informatici noti
- “criminali per caso”
- *motivazioni*: vantaggio personale, ripicca, ...

● **crackers** (non “hackers”!)

- perpetrano *accesso non autorizzato*
- *motivazioni* come sopra, inoltre:
gusto della trasgressione, delirio di onnipotenza, ...

● **criminali professionisti...**

- ...in altri “settori” del crimine
scoprono opportunità e prospettive nel crimine informatico
- problema sociale: *timore del danno all'immagine*
associato alla denuncia di un crimine informatico subito



Criminali informatici

tipologie e caratteristiche

● **dilettanti**

- *maggioranza* degli autori di crimini informatici noti
- “criminali per caso”
- *motivazioni*: vantaggio personale, ripicca, ...

● **crackers** (non “*hackers*”!)

- perpetrano *accesso non autorizzato*
- *motivazioni* come sopra, inoltre:
gusto della trasgressione, delirio di onnipotenza, ...

● **criminali professionisti...**

- ...in altri “settori” del crimine
scoprono opportunità e prospettive nel crimine informatico
- problema sociale: *timore del danno all'immagine*
associato alla denuncia di un crimine informatico subito



Criminali informatici

tipologie e caratteristiche

- **dilettanti**

- *maggioranza* degli autori di crimini informatici noti
- “criminali per caso”
- *motivazioni*: vantaggio personale, ripicca, ...

- **crackers** (non “hackers”!)

- *perpetrano accesso non autorizzato*
- *motivazioni* come sopra, inoltre:
gusto della trasgressione, delirio di onnipotenza, ...

- **criminali professionisti...**

- ...in altri “settori” del crimine
scoprono opportunità e prospettive nel crimine informatico
- problema sociale: *timore del danno all'immagine*
associato alla denuncia di un crimine informatico subito



Criminali informatici

tipologie e caratteristiche

● **dilettanti**

- *maggioranza* degli autori di crimini informatici noti
- “criminali per caso”
- *motivazioni*: vantaggio personale, ripicca, ...

● **crackers** (non “*hackers*”!)

- perpetrano *accesso non autorizzato*
- *motivazioni* come sopra, inoltre:
gusto della trasgressione, delirio di onnipotenza, ...

● **criminali professionisti...**

- ...in altri “settori” del crimine
scoprono opportunità e prospettive nel crimine informatico
- problema sociale: *timore del danno all'immagine*
associato alla denuncia di un crimine informatico subito



Criminali informatici

tipologie e caratteristiche

- **dilettanti**
 - *maggioranza* degli autori di crimini informatici noti
 - “criminali per caso”
 - *motivazioni*: vantaggio personale, ripicca, ...
- **crackers** (non “*hackers*”!)
 - perpetrano *accesso non autorizzato*
 - *motivazioni* come sopra, inoltre:
gusto della trasgressione, delirio di onnipotenza, ...
- **criminali professionisti...**
 - ... in altri “settori” del crimine
scoprono opportunità e prospettive nel crimine informatico
 - problema sociale: *timore del danno all'immagine*
associato alla denuncia di un crimine informatico subito



Criminali informatici

tipologie e caratteristiche

- **dilettanti**
 - *maggioranza* degli autori di crimini informatici noti
 - “criminali per caso”
 - *motivazioni*: vantaggio personale, ripicca, ...
- **crackers** (non “*hackers*”!)
 - perpetrano *accesso non autorizzato*
 - *motivazioni* come sopra, inoltre:
gusto della trasgressione, delirio di onnipotenza, ...
- **criminali professionisti...**
 - ... in altri “settori” del crimine
scoprono opportunità e prospettive nel crimine informatico
 - problema sociale: *timore del danno all'immagine*
associato alla denuncia di un crimine informatico subito



Criminali informatici

tipologie e caratteristiche

- **dilettanti**
 - *maggioranza* degli autori di crimini informatici noti
 - “criminali per caso”
 - *motivazioni*: vantaggio personale, ripicca, ...
- **crackers** (non “*hackers*”!)
 - perpetrano *accesso non autorizzato*
 - *motivazioni* come sopra, inoltre:
gusto della trasgressione, delirio di onnipotenza, ...
- **criminali professionisti...**
 - ... in altri “settori” del crimine
scoprono opportunità e prospettive nel crimine informatico
 - problema sociale: *timore del danno all'immagine*
associato alla denuncia di un crimine informatico subito



Criminali informatici

tipologie e caratteristiche

- **dilettanti**
 - *maggioranza* degli autori di crimini informatici noti
 - “criminali per caso”
 - *motivazioni*: vantaggio personale, ripicca, ...
- **crackers** (non “*hackers*”!)
 - perpetrano *accesso non autorizzato*
 - *motivazioni* come sopra, inoltre:
gusto della trasgressione, delirio di onnipotenza, ...
- **criminali professionisti...**
 - ... in altri “settori” del crimine
scoprono opportunità e prospettive nel crimine informatico
 - problema sociale: *timore del danno all'immagine*
associato alla denuncia di un crimine informatico subito



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - di prevenzione del danno
 - di limitazione di vulnerabilità
 - determinati, rispetto l'attacco più grave
 - difensivi, rispetto il danno
 - di rivelazione del danno, non capaci di evitare il danno
 - di recupero degli effetti del danno (post-mortem)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - natura del bersaglio
 - vulnerabilità e criticità del bersaglio
 - natura e gravità dell'attacco



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Obiettivi della difesa

disposti in cascata. . .

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
 - **di prevenzione** dell'attacco
e.g. rimozione di vulnerabilità
 - **deterrenti**, rendendo l'attacco più *arduo*
 - **devianti**, spostando il bersaglio
 - **di rivelazione** dell'attacco, non appena avviene o dopo
 - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
 - valore del **bersaglio**
 - rapporto **costi/benefici** dei controlli
 - maggior onere causato dai controlli all'**attaccante**



Controlli di sicurezza

Controlli multipli



Controlli di sicurezza

Controlli multipli

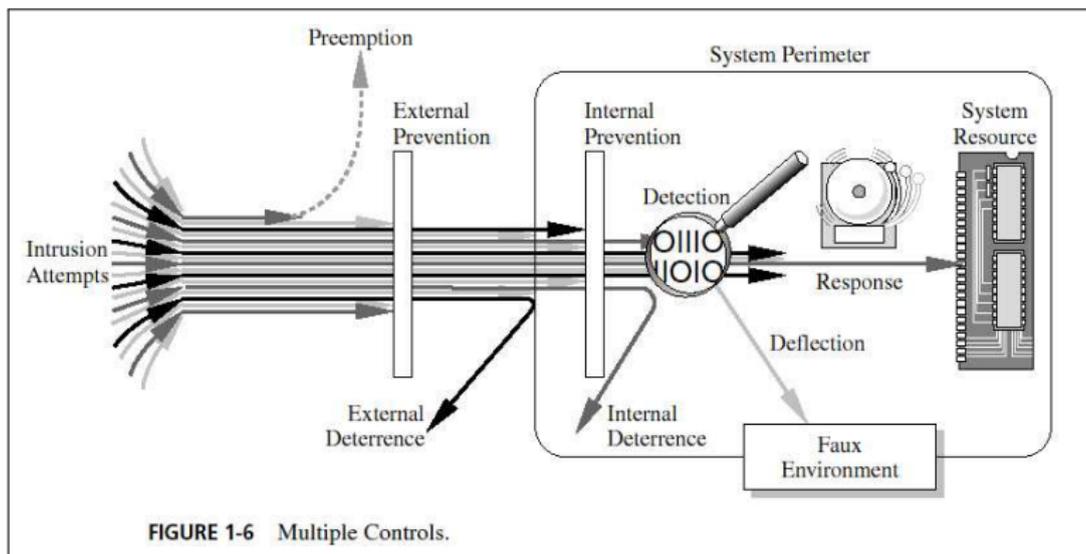


FIGURE 1-6 Multiple Controls.



Tipi di controllo

controlli crittografici, ma non solo. . .

- **codifica crittografica**

● *controlli di integrità*: verificano l'assenza di alterazioni non autorizzate
● *controlli di autenticità*: verificano l'identità del mittente
● *controlli di riservatezza*: verificano che l'informazione disponibile solo agli autorizzati

● *controlli di accesso*: verificano l'identità dell'utente
● *controlli di controllo*: verificano l'identità del sistema
● *controlli di controllo*: verificano l'identità del sistema
● *controlli di controllo*: verificano l'identità del sistema

- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, . . .
- **procedurali**: basati su *politiche e consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, . . .



Tipi di controllo

controlli crittografici, ma non solo. . .

● **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{E_k}$ cifrato $\xrightarrow{D_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
- protegge *riservatezza*, *integrità* e *disponibilità*, dunque
- **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, . . .
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, . . .



Tipi di controllo

controlli crittografici, ma non solo. . .

● **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
- protegge *riservatezza*, *integrità* e *disponibilità*, dunque
- **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, . . .
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, . . .



Tipi di controllo

controlli crittografici, ma non solo...

● **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
- protegge *riservatezza*, *integrità* e *disponibilità*, dunque
- **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, ...
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, ...



Tipi di controllo

controlli crittografici, ma non solo...

● **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
 - spesso realizzata in *hardware* per efficienza prestazionale
 - protegge *riservatezza*, *integrità* e *disponibilità*, dunque
 - **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, ...
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, ...



Tipi di controllo

controlli crittografici, ma non solo...

● **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
 - protegge *riservatezza*, *integrità* e *disponibilità*, dunque
 - **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, ...
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, ...



Tipi di controllo

controlli crittografici, ma non solo...

● **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
- protegge *riservatezza*, *integrità* e *disponibilità*, dunque
- **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, ...
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, ...



Tipi di controllo

controlli crittografici, ma non solo...

- **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
- protegge *riservatezza*, *integrità* e *disponibilità*, dunque
- **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, ...
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, ...



Tipi di controllo

controlli crittografici, ma non solo. . .

- **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
- protegge *riservatezza*, *integrità* e *disponibilità*, dunque
- **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, . . .
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, . . .



Tipi di controllo

controlli crittografici, ma non solo. . .

● **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
- protegge *riservatezza*, *integrità* e *disponibilità*, dunque
- **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, . . .
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, . . .



Tipi di controllo

controlli crittografici, ma non solo. . .

● **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
- protegge *riservatezza*, *integrità* e *disponibilità*, dunque
- **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, . . .
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, . . .



Tipi di controllo

controlli crittografici, ma non solo...

● **codifica crittografica**

- *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

in chiaro $\xrightarrow{e_k}$ cifrato $\xrightarrow{d_k}$ decifrato

- protegge non solo i *dati* ma anche il *software*
- spesso realizzata in *hardware* per efficienza prestazionale
- protegge *riservatezza*, *integrità* e *disponibilità*, dunque
- **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, ...
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, ...



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
ogni componente controllata deve essere sottoposta a
controlli di diversa natura

principio dell'angolo più debole

- **revisione periodica** dell'efficacia dei controlli



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
 - può compensare eventuali inefficacie di singoli controlli
 - altrimenti detta **difesa stratificata**
 - OK, però. . .

principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
 - può compensare eventuali inefficacie di singoli controlli
 - altrimenti detta **difesa stratificata**
 - OK, però. . .

principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
 - può compensare eventuali inefficacie di singoli controlli
 - altrimenti detta **difesa stratificata**
 - OK, però. . .

principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
 - può compensare eventuali inefficacie di singoli controlli
 - altrimenti detta **difesa stratificata**
 - OK, però. . .

principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
 - può compensare eventuali inefficacie di singoli controlli
 - altrimenti detta **difesa stratificata**
 - OK, però. . .

principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
 - può compensare eventuali inefficacie di singoli controlli
 - altrimenti detta **difesa stratificata**
 - OK, però. . .

principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
 - può compensare eventuali inefficacie di singoli controlli
 - altrimenti detta **difesa stratificata**
 - OK, però. . .

principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
 - può compensare eventuali inefficacie di singoli controlli
 - altrimenti detta **difesa stratificata**
 - OK, però. . .

principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli



Efficacia dei controlli di sicurezza

la sola predisposizione di controlli non basta. . .

- occorre **consapevolezza del problema** di sicurezza
prerequisito perché i controlli siano *effettivamente in uso*

principio di efficacia dei controlli

- **sovrapposizione** di controlli:
 - può compensare eventuali inefficacie di singoli controlli
 - altrimenti detta **difesa stratificata**
 - OK, però. . .

principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli



Esercizi

controllo della comprensione e dell'apprendimento

1. Distinguere fra vulnerabilità, minaccia, controllo.
2. Si considerano vari tipi di danni, ad es. a seguito di un furto: perdita economica, disagio pratico, sconvolgimento emotivo. Identificare almeno tre tipi di danni che un'azienda può soffrire a seguito del furto di apparecchiature informatiche.
3. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia alla riservatezza di suoi dati.
4. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia all'integrità di programmi o dati.
5. Fornire due esempi di vulnerabilità in automobili per le quali i costruttori hanno installato controlli; esprimere un giudizio sull'efficacia di tali controlli: buona, parziale, nulla.



Esercizi

controllo della comprensione e dell'apprendimento

- 1. Distinguere fra vulnerabilità, minaccia, controllo.**
2. Si considerano vari tipi di danni, ad es. a seguito di un furto: perdita economica, disagio pratico, sconvolgimento emotivo. Identificare almeno tre tipi di danni che un'azienda può soffrire a seguito del furto di apparecchiature informatiche.
3. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia alla riservatezza di suoi dati.
4. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia all'integrità di programmi o dati.
5. Fornire due esempi di vulnerabilità in automobili per le quali i costruttori hanno installato controlli; esprimere un giudizio sull'efficacia di tali controlli: buona, parziale, nulla.



Esercizi

controllo della comprensione e dell'apprendimento

1. Distinguere fra vulnerabilità, minaccia, controllo.
2. Si considerano vari tipi di danni, ad es. a seguito di un furto: perdita economica, disagio pratico, sconvolgimento emotivo. Identificare almeno tre tipi di danni che un'azienda può soffrire a seguito del furto di apparecchiature informatiche.
3. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia alla riservatezza di suoi dati.
4. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia all'integrità di programmi o dati.
5. Fornire due esempi di vulnerabilità in automobili per le quali i costruttori hanno installato controlli; esprimere un giudizio sull'efficacia di tali controlli: buona, parziale, nulla.



Esercizi

controllo della comprensione e dell'apprendimento

1. Distinguere fra vulnerabilità, minaccia, controllo.
2. Si considerano vari tipi di danni, ad es. a seguito di un furto: perdita economica, disagio pratico, sconvolgimento emotivo. Identificare almeno tre tipi di danni che un'azienda può soffrire a seguito del furto di apparecchiature informatiche.
3. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia alla riservatezza di suoi dati.
4. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia all'integrità di programmi o dati.
5. Fornire due esempi di vulnerabilità in automobili per le quali i costruttori hanno installato controlli; esprimere un giudizio sull'efficacia di tali controlli: buona, parziale, nulla.



Esercizi

controllo della comprensione e dell'apprendimento

1. Distinguere fra vulnerabilità, minaccia, controllo.
2. Si considerano vari tipi di danni, ad es. a seguito di un furto: perdita economica, disagio pratico, sconvolgimento emotivo. Identificare almeno tre tipi di danni che un'azienda può soffrire a seguito del furto di apparecchiature informatiche.
3. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia alla riservatezza di suoi dati.
4. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia all'integrità di programmi o dati.
5. Fornire due esempi di vulnerabilità in automobili per le quali i costruttori hanno installato controlli; esprimere un giudizio sull'efficacia di tali controlli: buona, parziale, nulla.



Esercizi

controllo della comprensione e dell'apprendimento

1. Distinguere fra vulnerabilità, minaccia, controllo.
2. Si considerano vari tipi di danni, ad es. a seguito di un furto: perdita economica, disagio pratico, sconvolgimento emotivo. Identificare almeno tre tipi di danni che un'azienda può soffrire a seguito del furto di apparecchiature informatiche.
3. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia alla riservatezza di suoi dati.
4. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia all'integrità di programmi o dati.
5. Fornire due esempi di vulnerabilità in automobili per le quali i costruttori hanno installato controlli; esprimere un giudizio sull'efficacia di tali controlli: buona, parziale, nulla.



Problemi

applicazioni dei concetti proposti

8. **Ipotesi:** un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, **Ipotesi:** considerare un programma che

17. visualizza ed elabora dati sulla personale Pavia e le informazioni della propria città;

18. calcola e visualizza il 30% di un numero intero;

19. accetta e stampa dati decimali;

20. genera dati relativi al 30% di un numero intero e li stampa con un formato personalizzato.

17–20, **Problema:** in ciascuna delle ipotesi proposte sopra



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

- 17.** visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
- 18.** permette a consumatori di ordinare prodotti via web;
- 19.** accetta e tabula voti elettorali;
- 20.** permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?



Problemi

applicazioni dei concetti proposti

8. Ipotesi: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.

Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, Ipotesi: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, Problema: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?

