Reti di Calcolatori e Sicurezza

Chi fa cosa contro che

Capp. 3,4,5,20(prima metà) Schneier

Libro kurose

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Cosa? Attacchi

- Parallelo col mondo reale
- Multiformi
  - *Mancato recapito merce*
  - *Doppio pagamento*
  - *Violazione password*
  - *…*
- Classificabili in base all'obiettivo
- Sicurezza ~= prevenzione attacchi

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Che? Elementi di sicurezza

- Molteplici
- “Sicurezza” si traduce in essi
- Alcuni sono primari, altri secondari
- Quanti sono??

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Definizione di Sicurezza Informatica

- Sicurezza:
  - Assenza di rischio o pericolo
- Sicurezza Informatica
  - Prevenzione o protezione contro,
    - Accesso, distruzione o alterazione di risorse/informazioni da parte di utenti non autorizzati

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

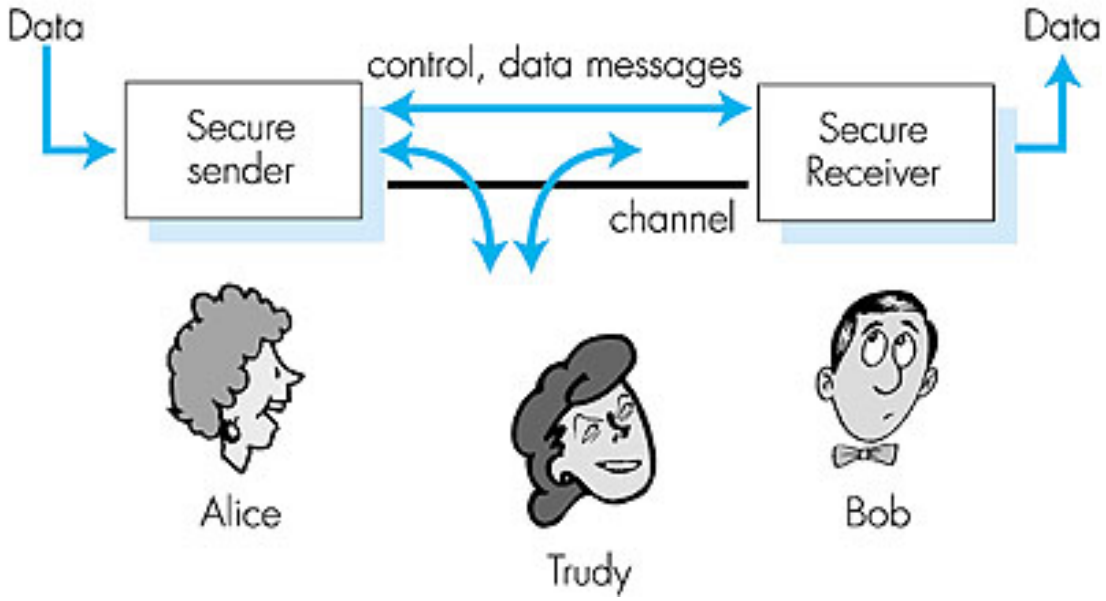
Sicurezza Informatica

- abilità di un sistema di proteggere informazioni, risorse ed il sistema stesso, rispetto alle nozioni di
  - Confidentialità (confidentiality)
  - Integrità (integrity)
  - Autenticazione (authentication)
  - Controllo degli Accessi (control access)
  - Non ripudio (non-repudiaton)
  - Disponibilità (availability)
  - Privatezza (privacy)

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Alice,



- "Hello-world" nel mondo della sicurezza
- Bob e Alice hanno la necessità di comunicare tra loro in modo sicuro
- Trudy, "intruder" è in grado di intercettare e modificare i messaggi

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Security Attacks

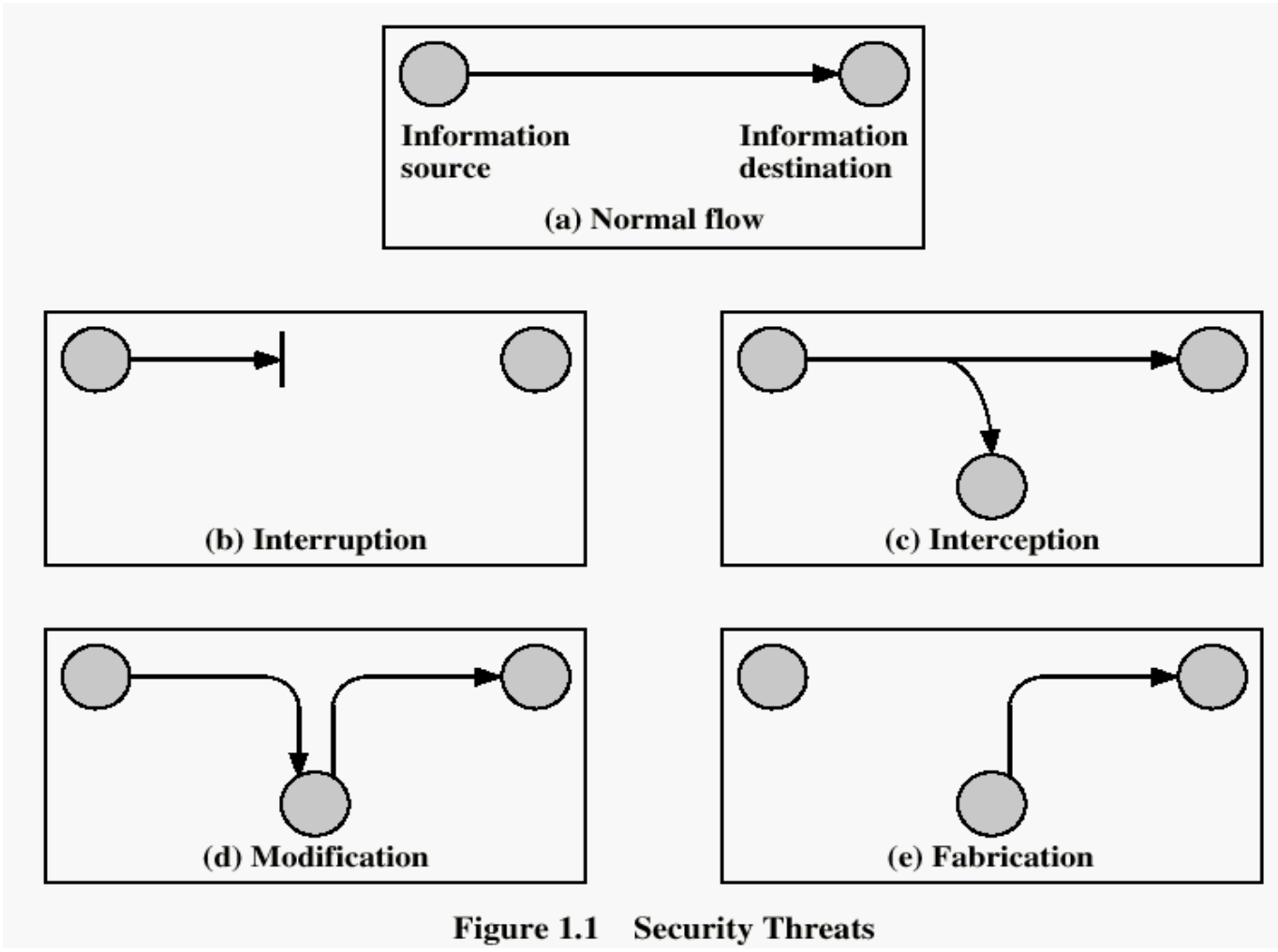


Figure 1.1 Security Threats

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Thanks to Giampaolo Bella for slides draft!!

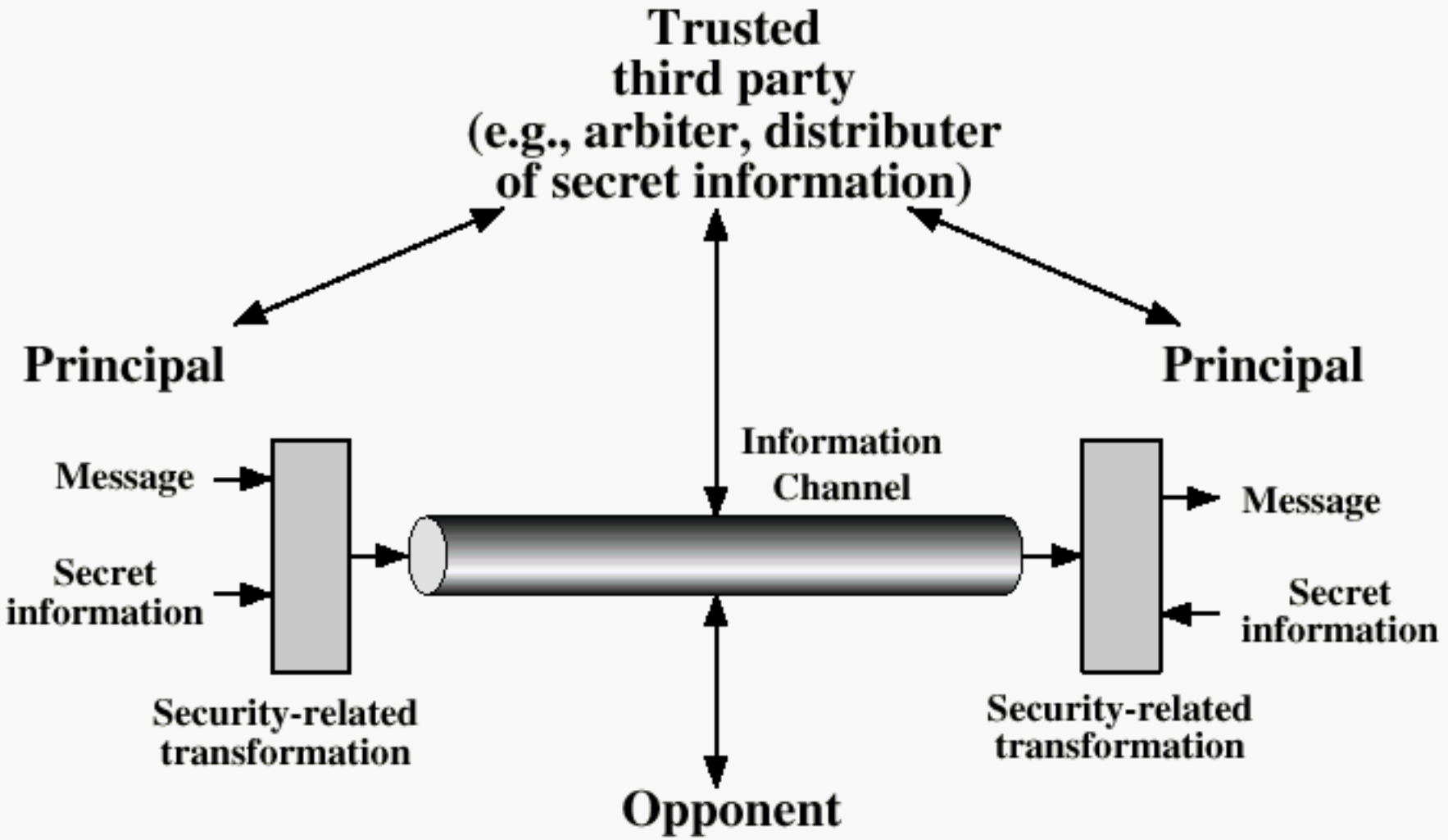
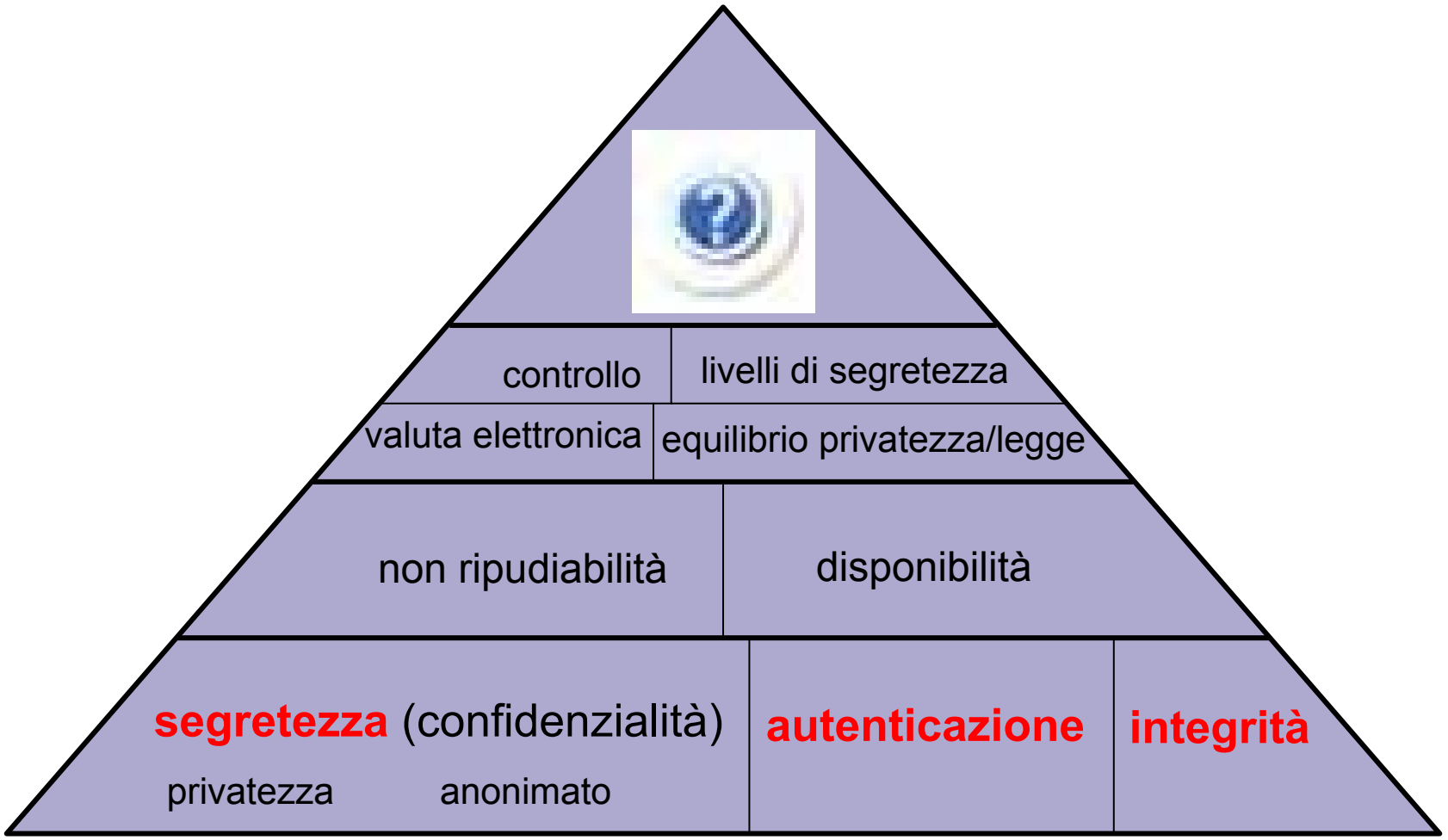


Figure 1.3 Model for Network Security

draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Elementi di sicurezza - tassonomia



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Main goals

- **Confidentialità (confidentiality)**
  - Assicurare che le informazioni non siano accessibili ad utenti non autorizzati
- **Integrità (integrity)**
  - Assicurare che le informazioni non siano alterabili da persona non autorizzate (in maniera invisibile agli utenti autorizzati)
- **Autenticazione (athentication)**
  - Assicurare che gli utenti siano effettivamente chi dichiarano di essere

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

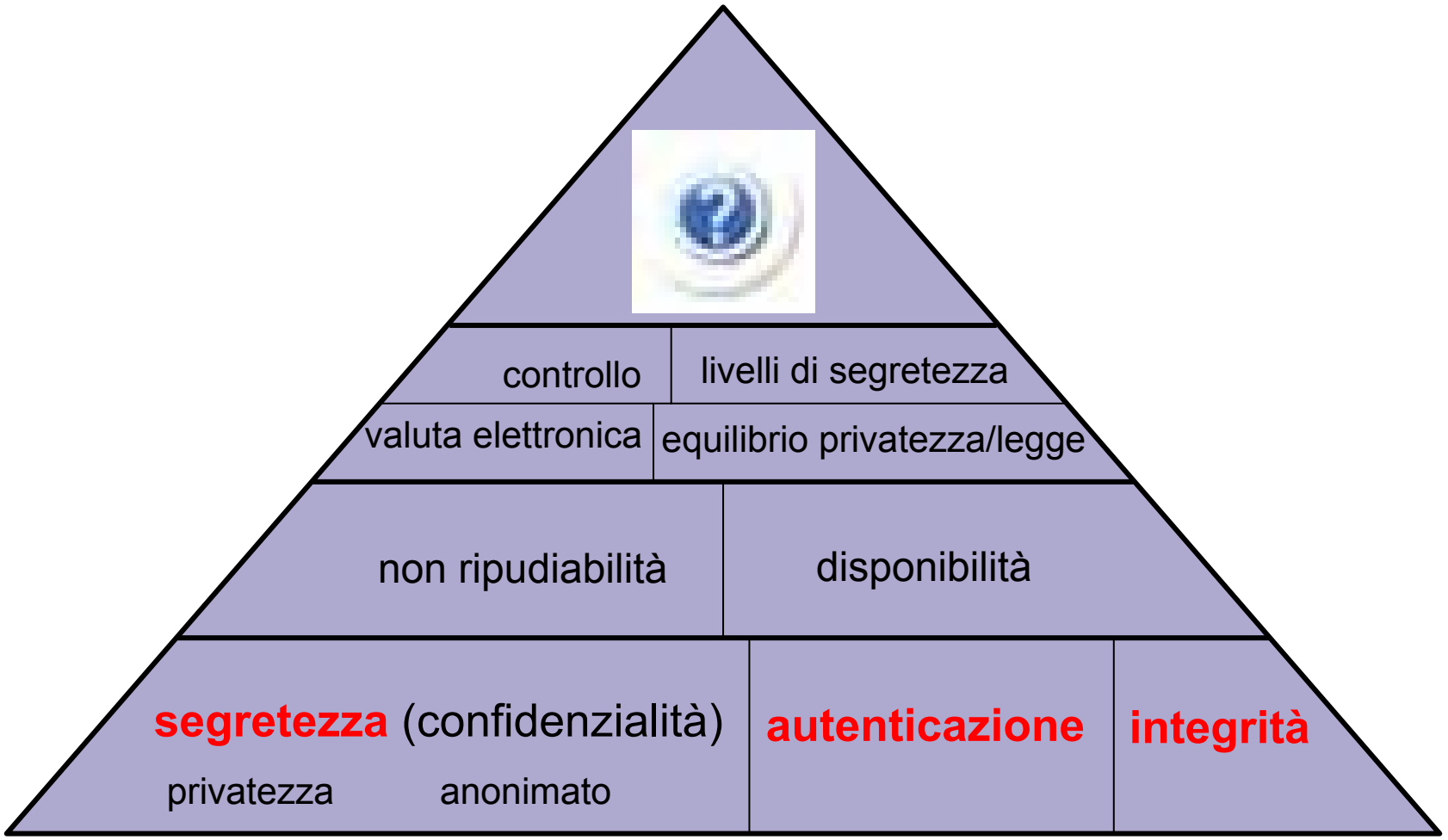
Additional goals

- Privatezza (privacy)
  - Assicurare che gli utenti possano controllare quali informazioni su di lui vengono raccolte, come vengono usate, chi le usa, chi le mantiene, e per quale scopo vengono usate
- Controllo degli accessi (access control)
  - Assicurare che gli utenti abbiano accesso a tutte le risorse ed a tutti i servizi cui sono autorizzati e solo a questi
- Non ripudio (non-repudiation)
  - Assicurare che il mittente di un messaggio non possa negare il fatto di aver spedito il messaggio
- Disponibilità (availability)
  - Assicurare che un sistema sia operativo e funzionale in ogni momento (non deny-of-service)

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Elementi di sicurezza - tassonomia



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

confidentiality/secrecy – privacy - anonimity

Privatezza

Def. Diritto dell'individuo di rilasciare (o meno) le informazioni che lo riguardano.

Anonimato

Def. Diritto dell'individuo di rilasciare (o meno) la propria identità

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Privatezza

- Privacy = diritto di confidentiality
  - *La passwd di Laboratorio è confidentiale, non privata*
- La democrazia si basa sulla privacy
  - *Il voto è privato*
- UE: privatezza dei dati personali. USA: no!
  - *La Doxa non può vendere i vostri dati*
- Temporalità
  - *Privatezza a medio termine del database clienti*

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Anonimato

- Anonimato = privacy dell'identità
- Anonimato commerciale e sanitario
- *Pseudoanonimato*: uso di nome falso
  - Cookies???
- Diritto?
- Difficile da garantire nel mondo digitale
  - *Indirizzo Ethernet unico*
  - *Office inserisce nome autore*
  - *IP trace-back*

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Integrità (coerenza)

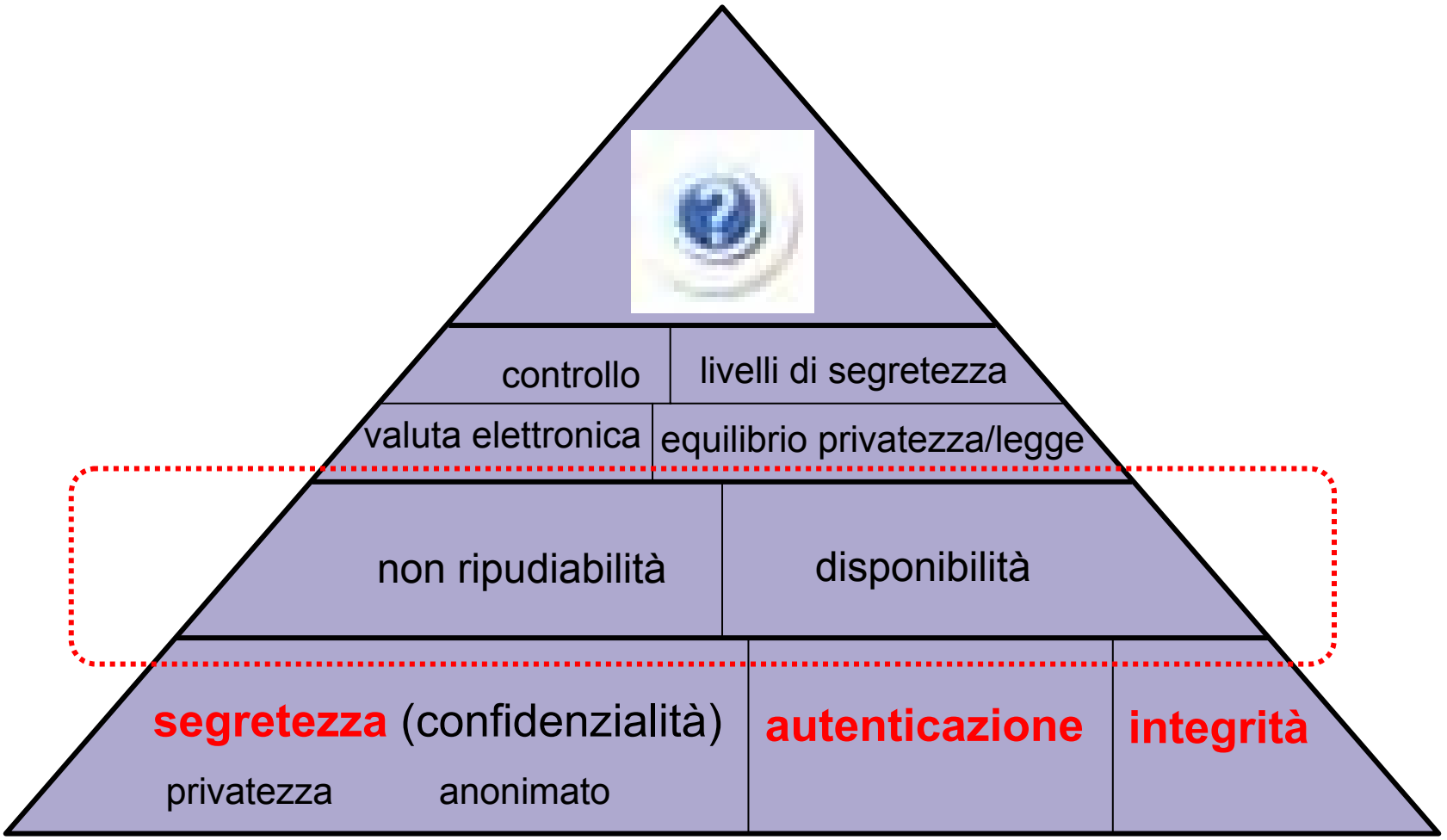
Def. L'informazione non sia alterata da utenti non autorizzati

- Non importa l'origine dei dati (autenticazione
  - *Integrità di un video*
  - *Integrità di un database*
  - *Integrità di una cache*
- Mancanza di integrità spesso sinonimo di falsificazione

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Verso gli elementi di livello 2



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Non-ripudiabilità

Def. L'utente non possa negare la propria partecipazione in una transazione

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Disponibilità (non DoS)

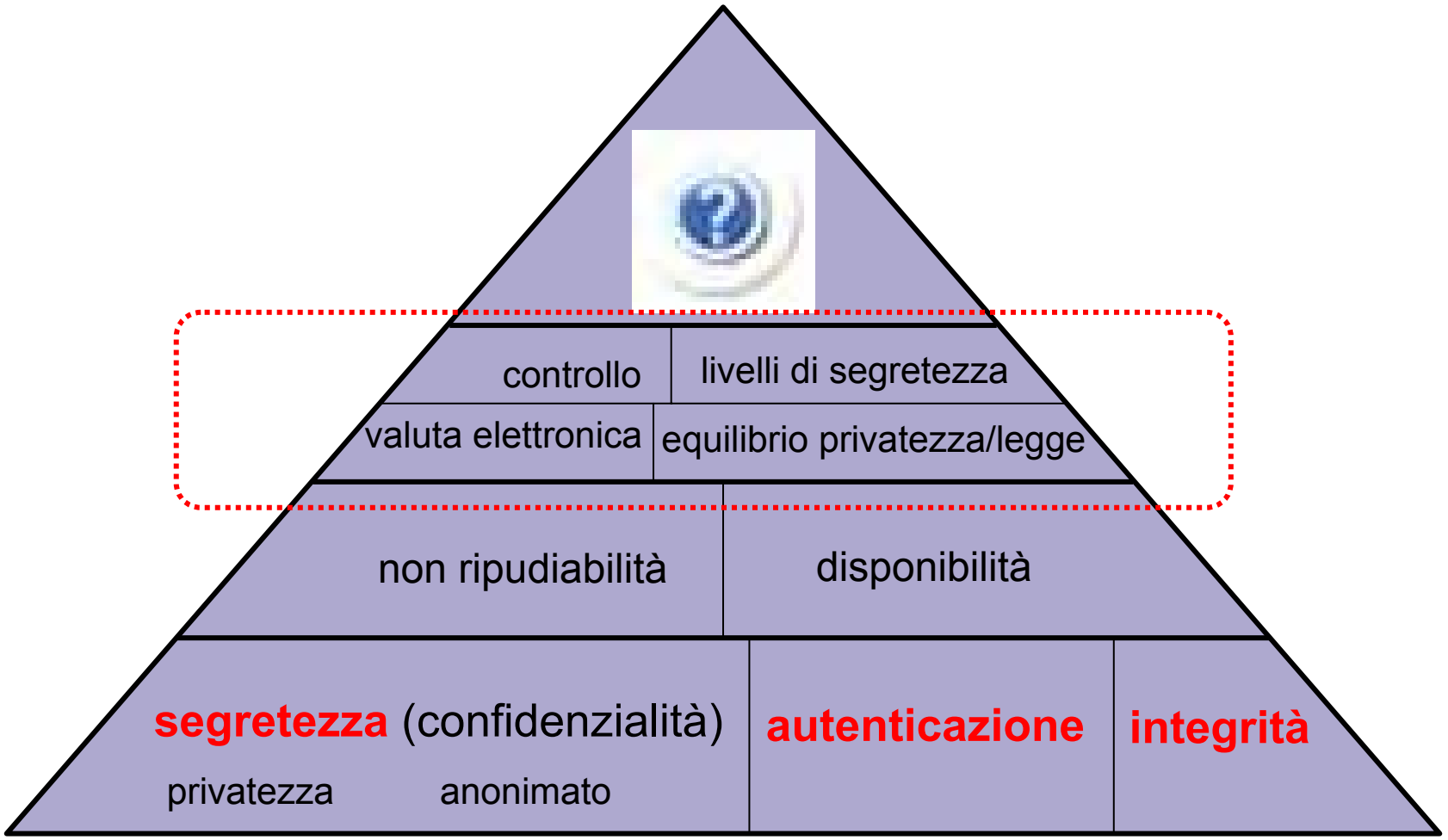
Def. Il sistema sia operante e funzionale in ogni momento

- Minacciata dalle tecniche di automazione
  - *Semplice programma che "saturi" un sito web*
- Favorita complicando l'accesso al sistema
  - *Prima di garantire l'accesso, il sistema risponde con un cookie che vuole indietro compilato*

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Verso gli elementi di livello 3



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Equilibrio privatezza/legge

- Il singolo richiede privacy, la legge richiede l'opposto
  - *Chi possiede capitali in Svizzera?*
  - *In UK le banche hanno "coperto" propri clienti*
- La soluzione serve prima di tutto sul piano etico/legale

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Livelli di segretezza

- Che livello di segretezza?
  1. *Top secret*
  2. *Secret*
  3. *Riservato*
  4. *Non classificato*

  1. *Cruciale*
  2. *Molto importante*
  3. *Importante*
- Sintassi indicativa, semantica importante
  - *Mi presti la tua password?*
  - *Mi mandi via email il tuo progetto di Sicurezza?*

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Valuta elettronica

- Uso di carte di credito su Internet (SET)
  - Il venditore riceve solo l'autorizzazione al pagamento; bonifico consueto
- Proteggere i commercianti
  - *SSL è inaccettabile!*
- Inventare una vera valuta elettronica?
  - Solo SW?
  - Anonima o identificabile?
  - Rischi: double-spending, falsificazione

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Controllo

Def. Verificare che il sistema funzioni come previsto

- Mondo digitale: facile non lasciare tracce
  - *Alterare un file cambiando un bit*

Controllo d'accesso

Def. Garantire che gli utenti abbiano accesso a tutte e sole le risorse o i servizi per i quali sono autorizzati

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Controllo d'accesso richiede

- **Autenticazione** dell'utente al sistema
- **Politiche** di sicurezza: regole di alto livello descriventi gli accessi autorizzati al sistema
  - Chi può fare cosa
  - *Docenti possono accedere al 2° piano sempre; studenti solo per conferire coi docenti*
- **Meccanismi** di basso livello (HW/SW) che implementino le politiche di sicurezza
  - Protetti da alterazioni illecite

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Esempio di politica di sicurezza

1. Un utente ha il permesso di leggere un qualunque file pubblico
2. Un utente ha il permesso di scrivere solo sui file pubblici di sua proprietà
3. Un utente ha il divieto di sostituire un file con una sua versione più obsole
4. Un utente ha l'obbligo di cambiare la propria password quando questa scade
5. Un utente segreto ha il permesso di leggere su un qualunque file non pubblico
6. Un utente segreto ha il permesso di scrivere su un qualunque file non pubblico
7. Un amministratore ha il permesso di sostituire un qualunque file con una sua versione più obsoleta
8. Un utente che non cambia la sua password scaduta (negligente) ha il divieto di compiere qualunque operazione
9. Un utente che non cambia la sua password scaduta (negligente) non ha discrezione di cambiarla

Thanks to Giampaolo Bella for slides

draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

I mattoni dell'esempio

- **Utenti**
- **Ruoli**: utente, utente segreto, sistemista, utente negligente
- **Operazioni**: leggere, scrivere, "downgrade", cambio password
- **Modalità**: obbligo, permesso, divieto, discrezionalità

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Relazioni fra le modalità

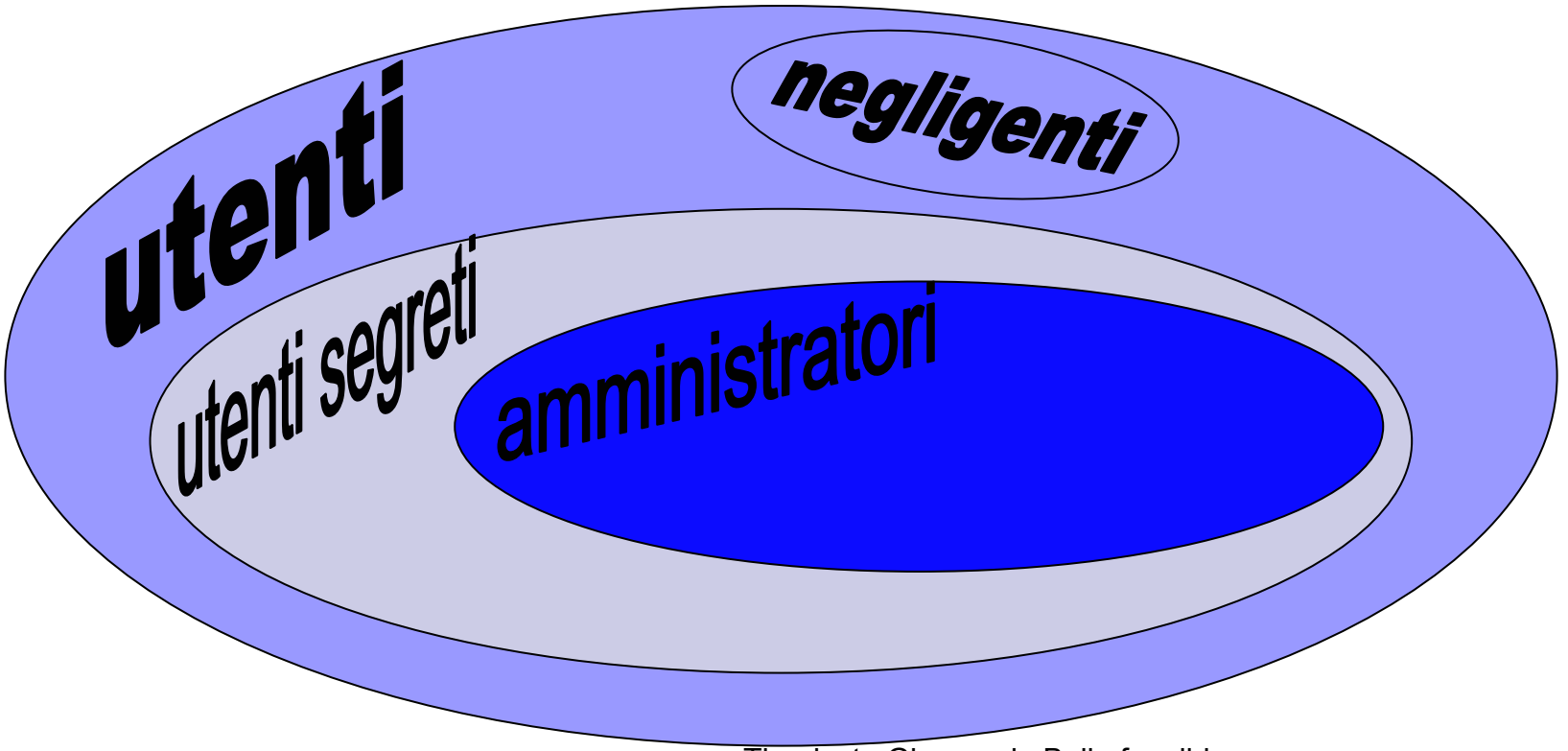
- Modalità base: Obbligatorio(x)
- Permesso(x) = ¬Obbligatorio(¬x)
- Vietato(x) = Obbligatorio(¬x)
- Discrezionale(x) = ¬Obbligatorio(x)

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Intersezione dei ruoli

- Problema: un utente riveste più ruoli



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Inconsistenze di una politica

- **Contraddizione**:
  Obbligatorio(x) $\wedge$ ¬Obbligatorio(x)
- **Dilemma**:
  Obbligatorio(x) $\wedge$ Obbligatorio(¬x)

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Inconsistenze nell'esempio

- Contraddizione da regole 3 e 7
  - Un amministratore ha permesso e divieto di fare downgrade di un file
- Dilemma da regole 8 e 9
  - Un utente negligente ha l'obbligo sia di cambiare sia di non cambiare la propria password

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Esercizio

Trovare tutte le inconsistenze nell'esempio

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Attacchi – ultime!

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Sicurezza dei protocolli di rete

- Il protocollo attualmente più diffuso è il TCP/IP.
- Il protocollo TCP/IP ha delle debolezze intrinseche, perché fu (1974) creato pensando all'efficienza delle connessioni piuttosto che alla sicurezza.
- Queste debolezze permettono attacchi di diverso tipo.

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Attacchi passivi o attivi

- **Attacco passivo**: sottrarre informazioni senza interferire sul sistema
- **Attacco attivo**: interferire sul sitema con vari scopi

Classificazione storica: oggi sono praticamente tutti attivi

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

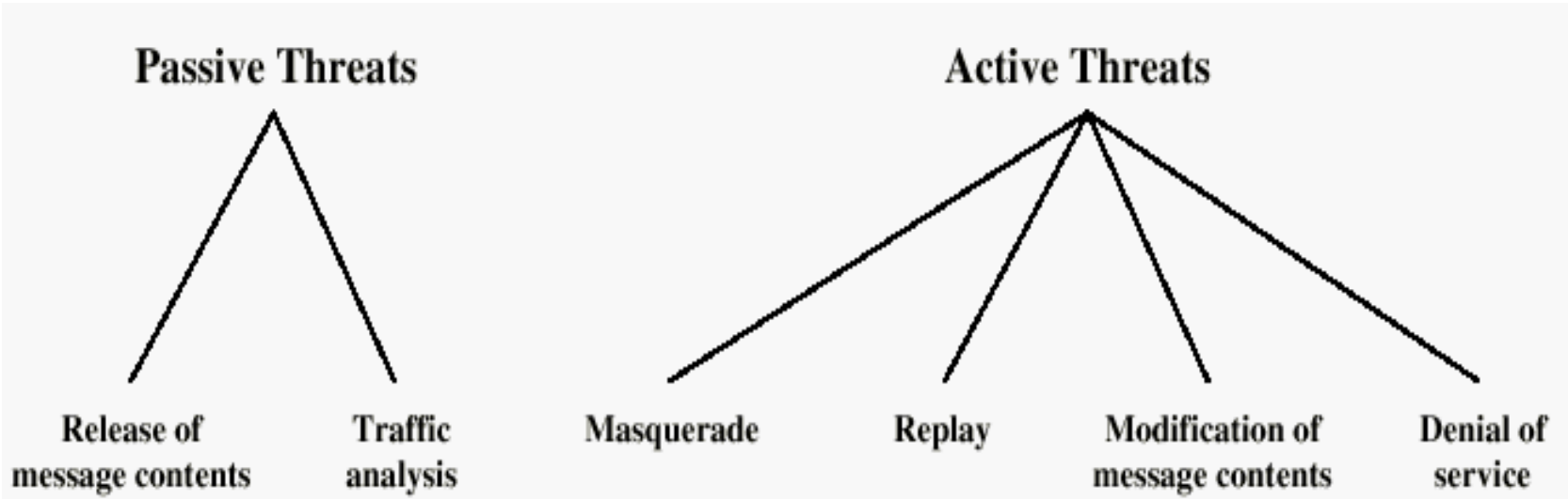
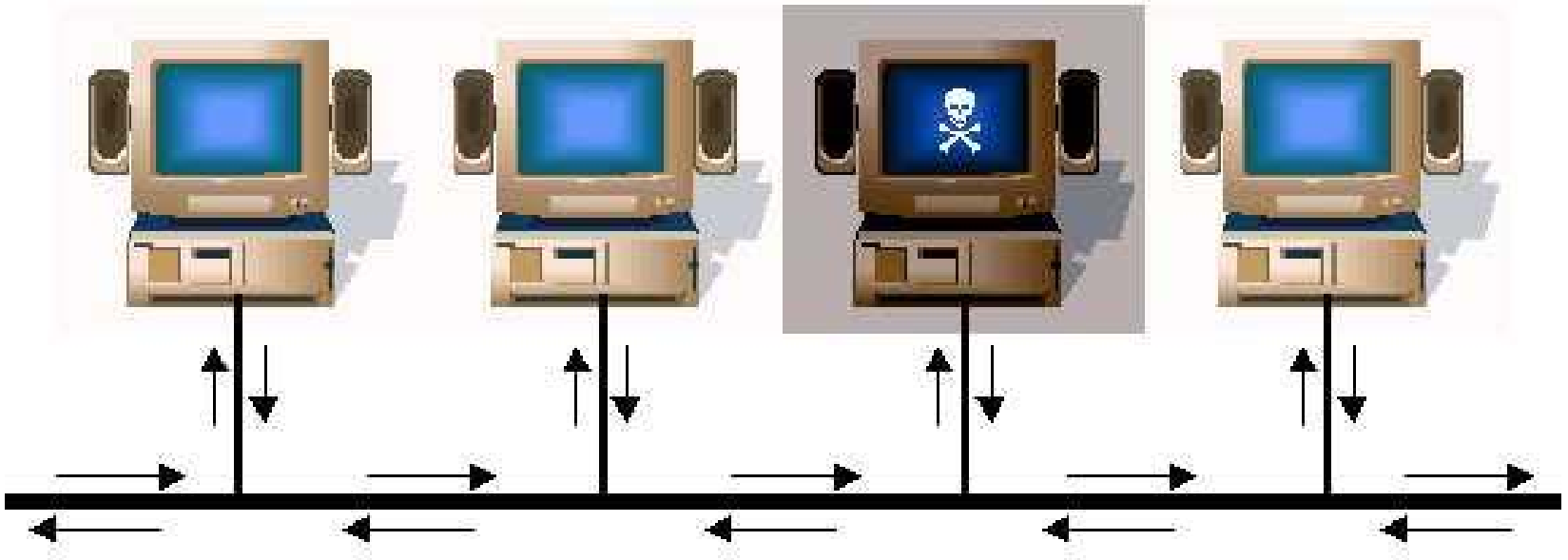


Figure 1.2 Active and Passive Security Threats

Thanks to Giampaolo Bella for slides draft!!

Tipologie di attacchi ai protocolli TCP/IP



Attacco "sniffing"

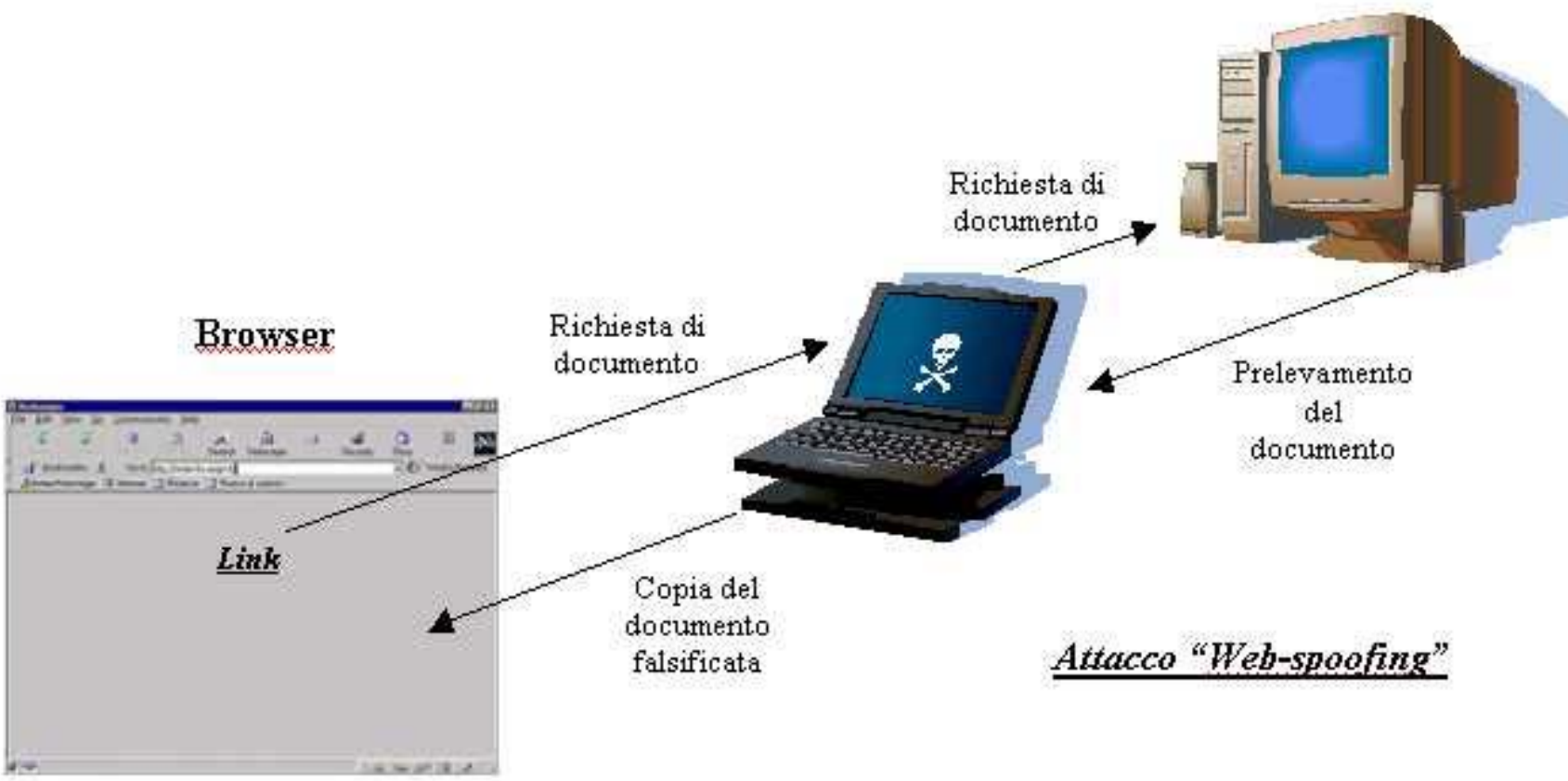
www.stefanobistarelli.com/slides/reti-sicurezza/

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Tipologie di attacchi ai protocolli TCP/IP

- Attacchi attivi (es. web-spoofing)



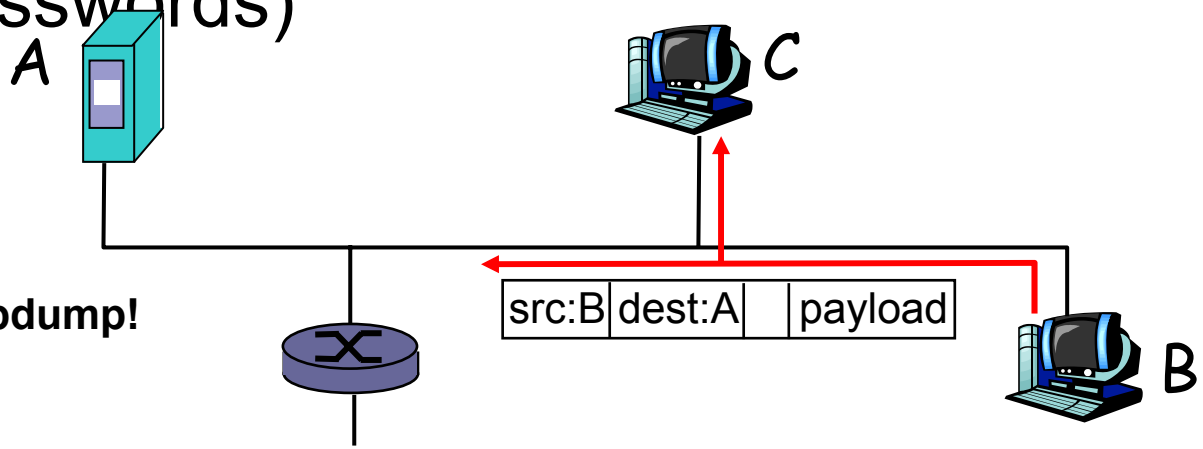
Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Sicurezza e Internet

Packet sniffing:

- LAN di tipo broadcast
- Le schede di rete sono in grado di leggere tutti i pacchetti inviati sulla LAN ed in particolare tutti i dati “in chiaro” (e.g. passwords)



Fai vedere tcpdump!

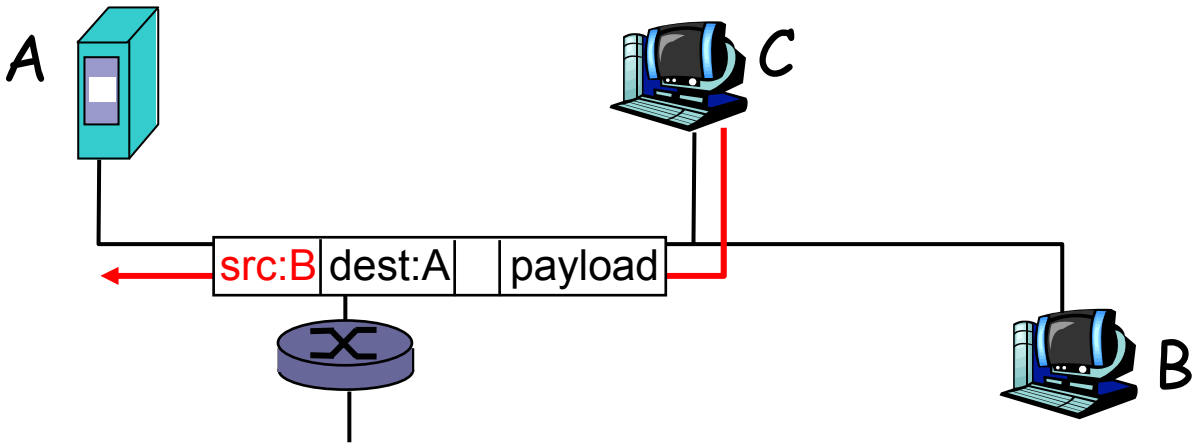
Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Sicurezza e internet

IP Spoofing:

- Un utente non educato potrebbe generare pacchetti IP con un valoro qualsiasi dei campi previsti dalla struttura di IP
- e.g.: C si fa passare per B



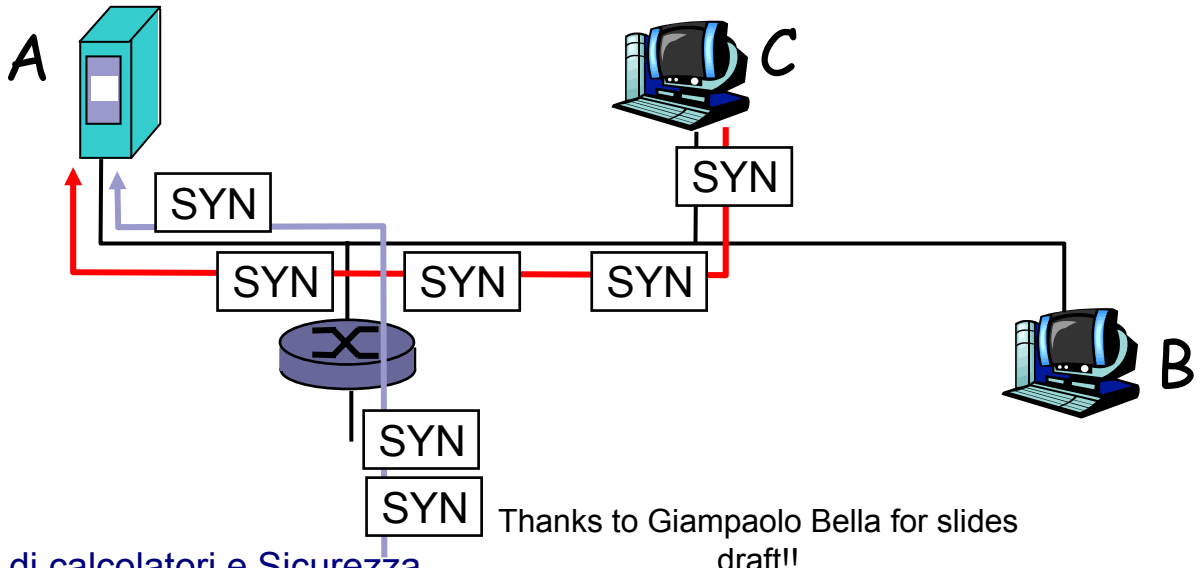
Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Sicurezza e internet

Denial of service (DOS):

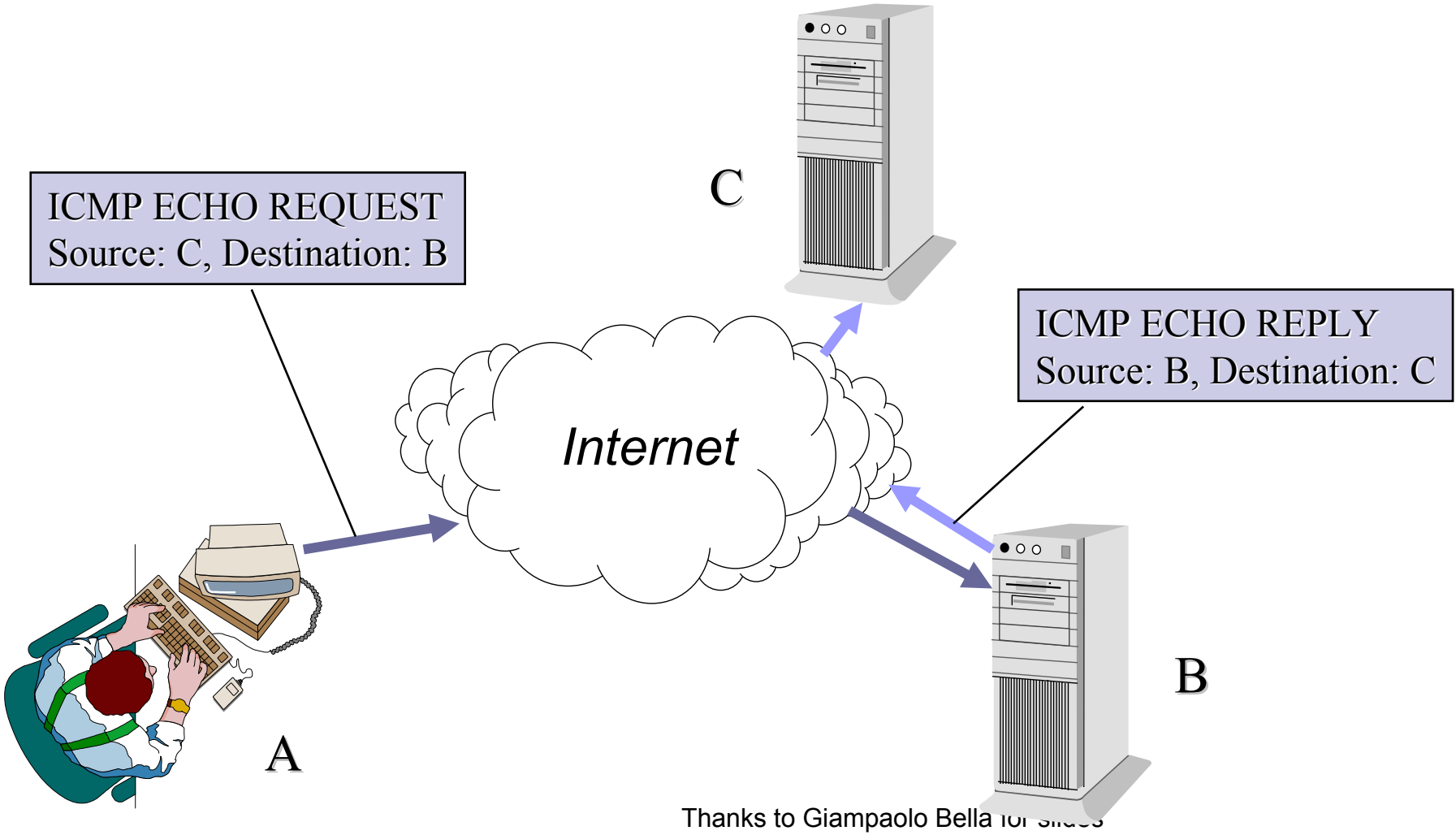
- Creazione di un carico di lavoro elevato tale che il sistema non è in grado di funziuonare
- e.g., C: SYN-attack su A



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

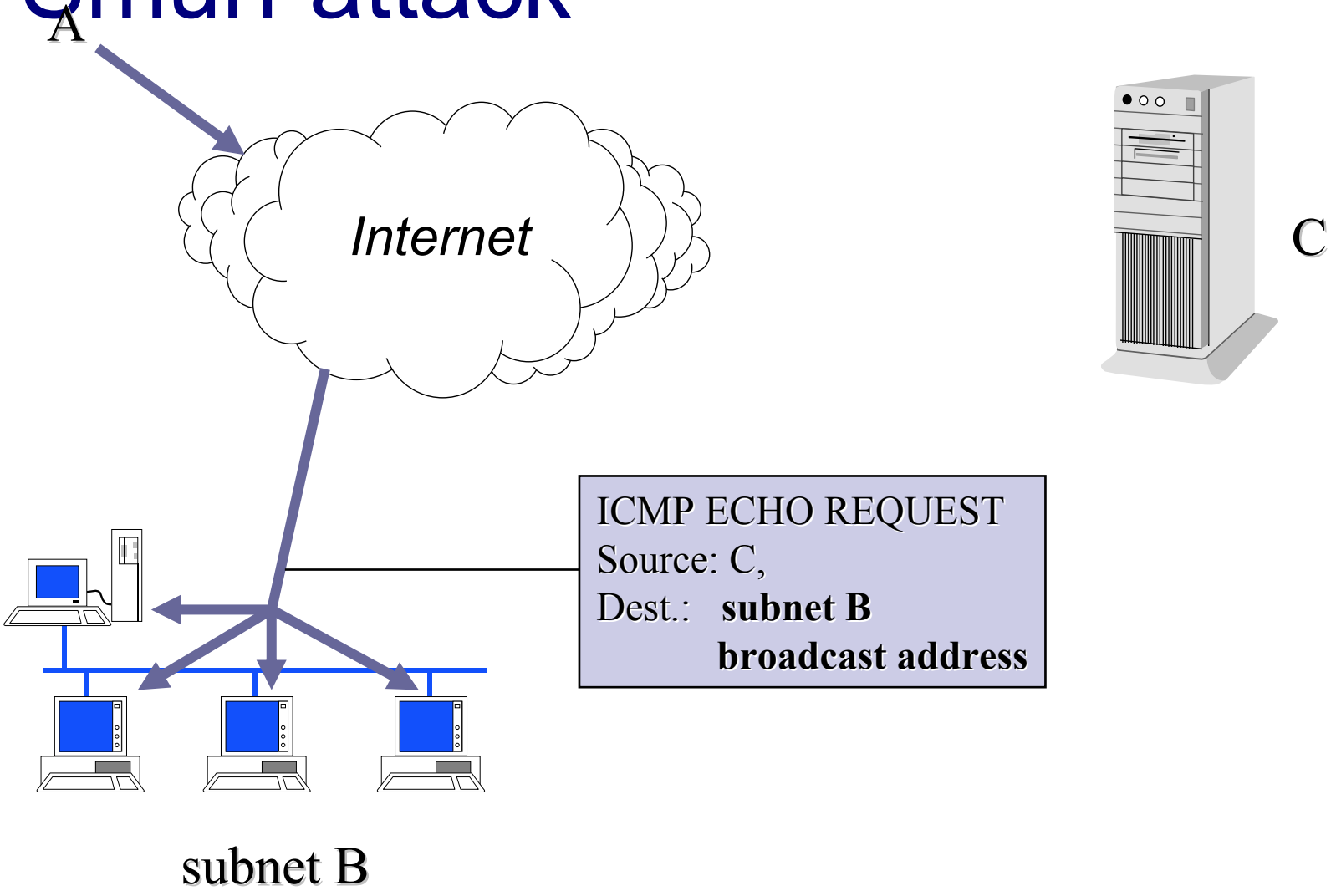
Spoofed ping



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

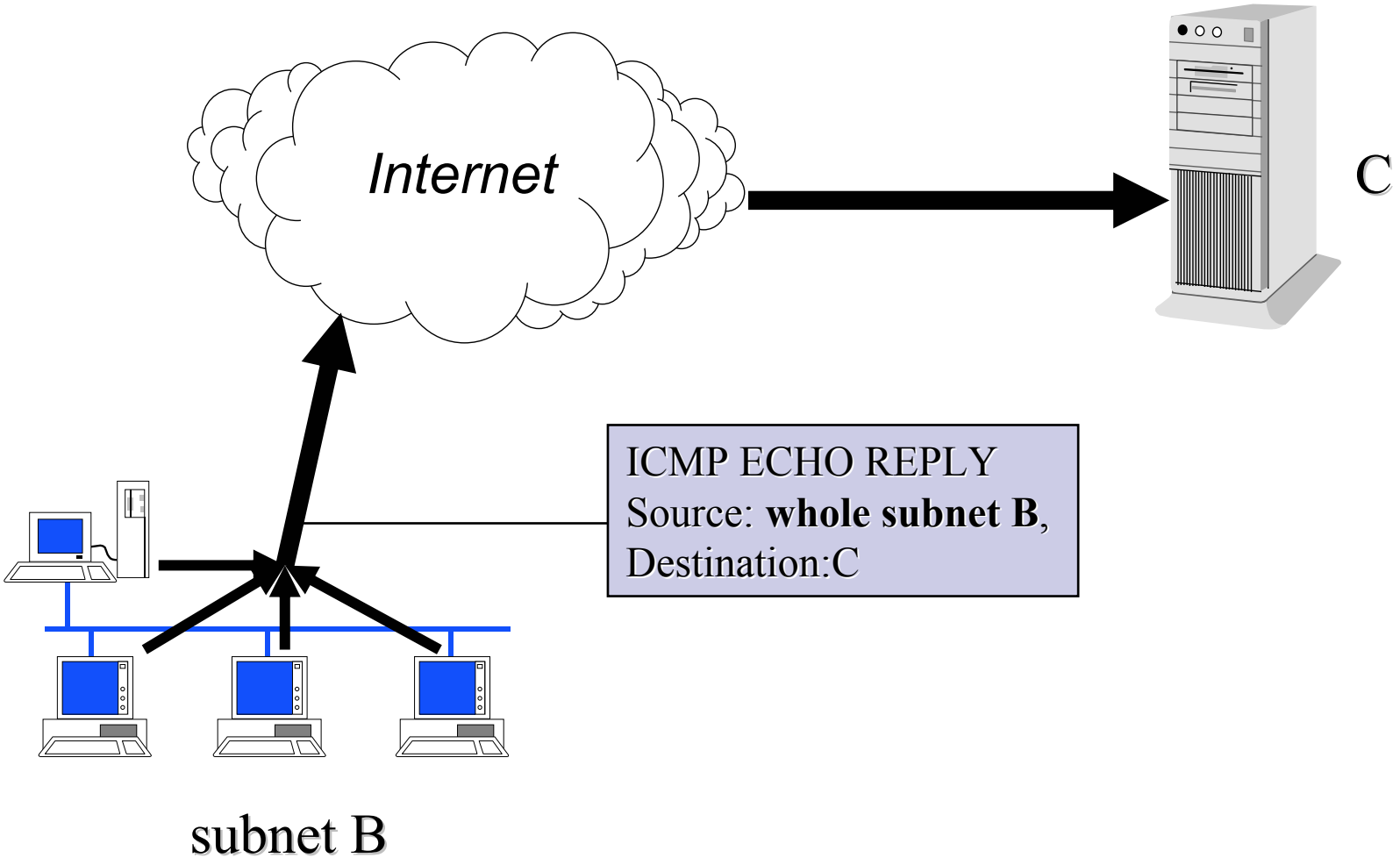
Smurf attack



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

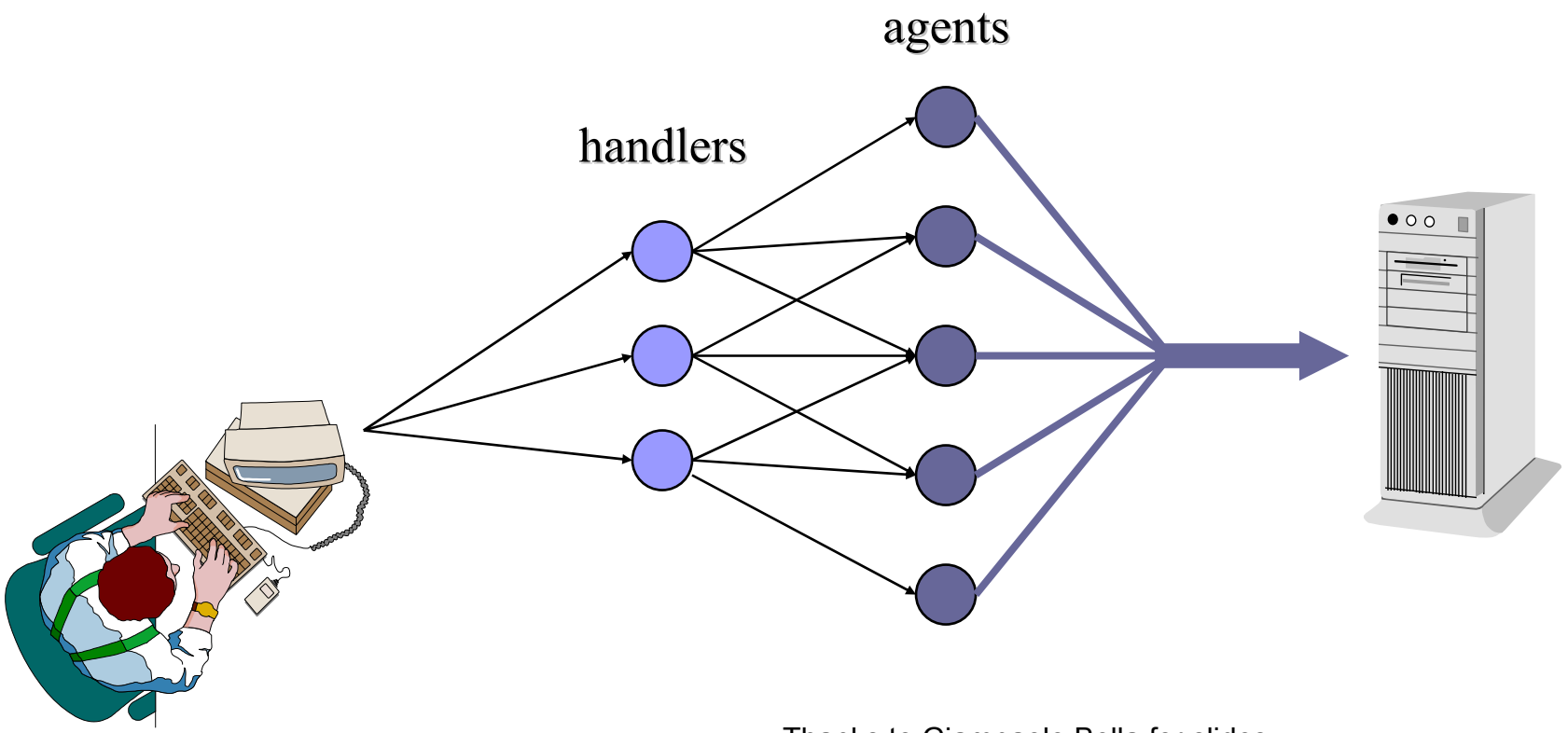
Smurf attack



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Distributed DoS



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Determinare i servizi attivi

port	type	name	
7	TCP/UDP	echo	
9	TCP/UDP	discard	
13	TCP/UDP	daytime	
19	TCP/UDP	chargen	
21	TCP	ftp	●
23	TCP	telnet	●
37	TCP/UDP	time	
53	TCP/UDP	domain	
69	UDP	tftp	
110	TCP	pop3	●
113	TCP/UDP	auth	
161	UDP	snmp	

port	type	name	
513	UDP	who	
514	UDP	syslog	
517	UDP	talk	
2049	TCP/UDP	NFS	
512	TCP	exec	●
513	TCP	login	●
514	TCP	shell	●

services marked with ● use cleartext passwords

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

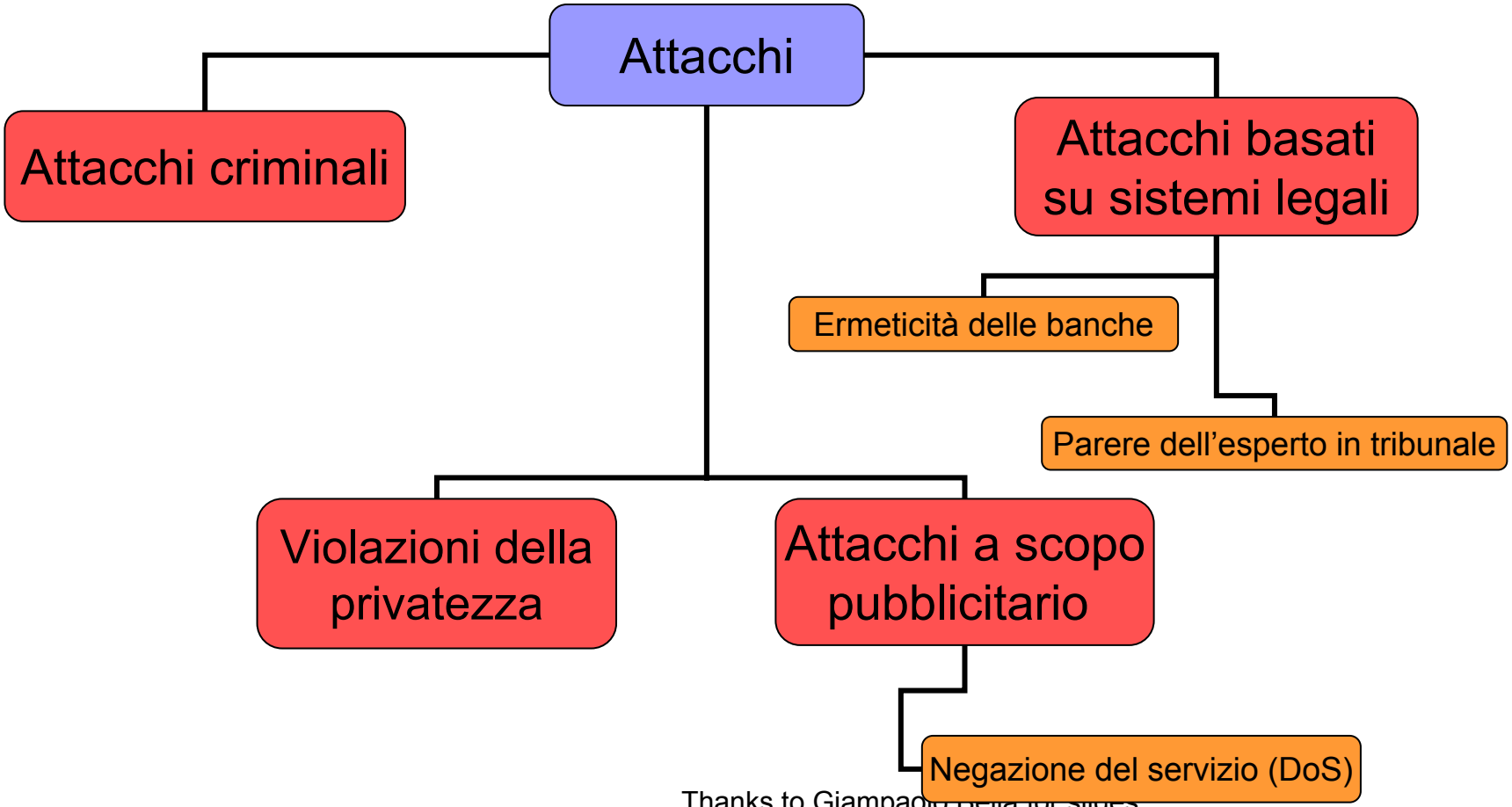
Differenze tra i metodi di attacco

- Gli attacchi passivi sottraggono informazioni senza interferire sul sistema.
- Gli attacchi attivi interferiscono sui sistemi con diversi scopi: DoS, spoofing, ecc.

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

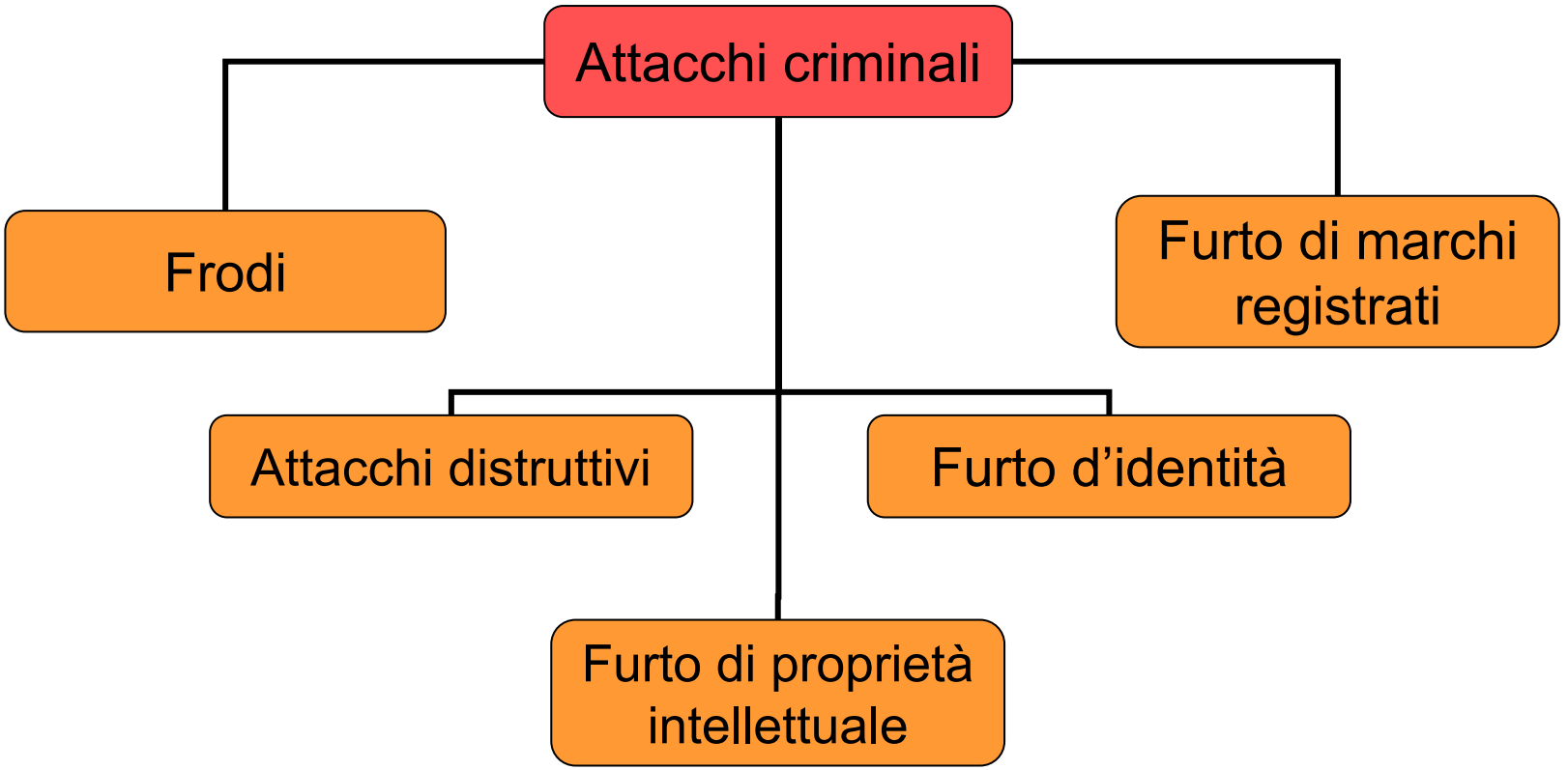
Attacchi – tassonomia



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

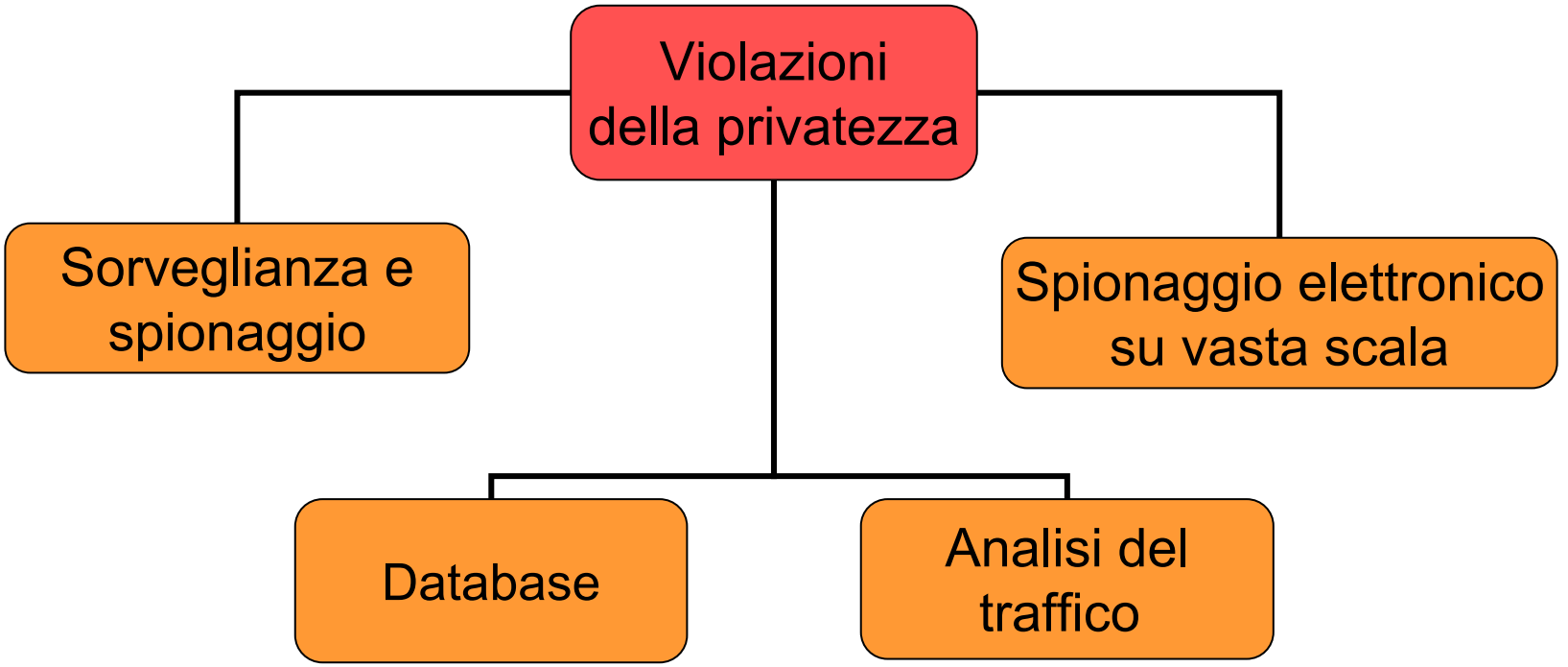
Attacchi criminali



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Violazioni della privatezza



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

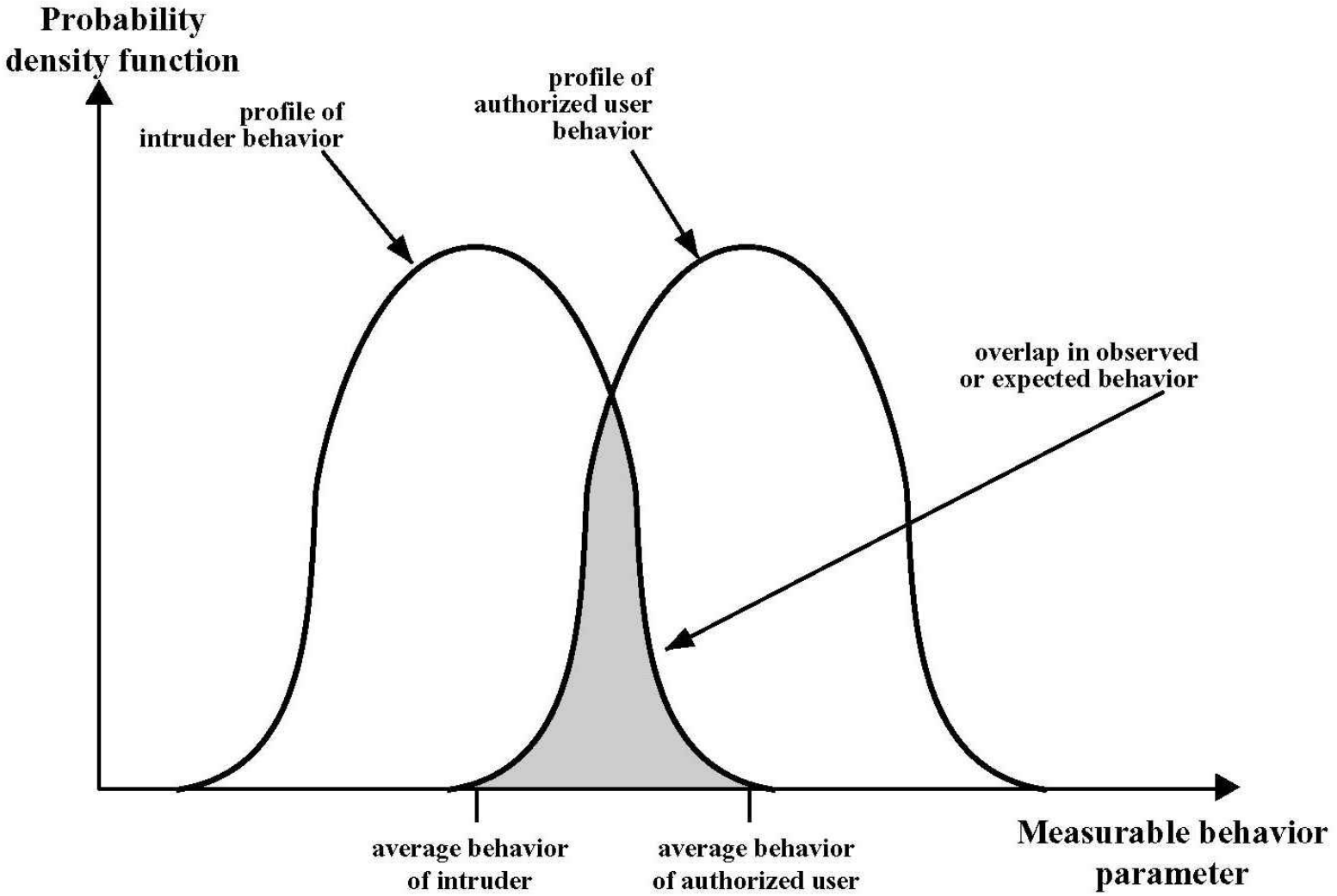
Attaccanti – tassonomia

1. Hacker (cracker)
2. Criminali solitari
3. Attaccanti interni
4. Spie industriali
5. Giornalisti
6. Organizzazioni criminali
7. Forze dell'Ordine
8. Terroristi
9. Servizi segreti
10. Infowarrior

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Profilo comportamentale

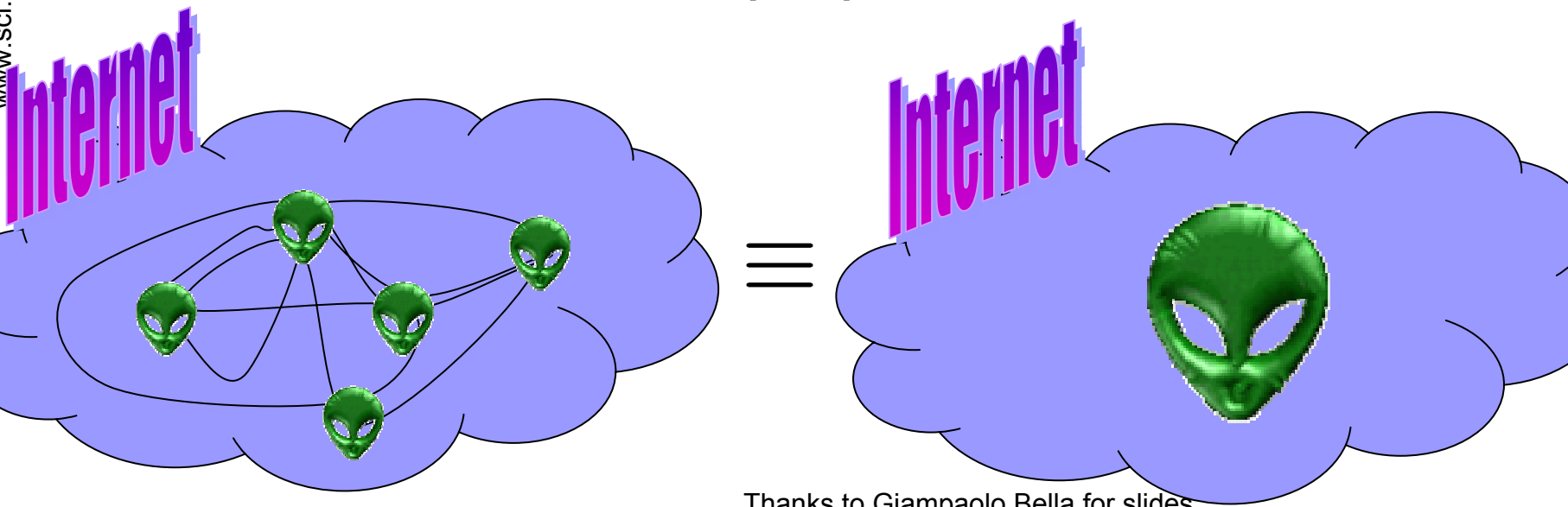


Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Modelli di attaccante

- **DY** (1983). Spia alla Dolev-Yao
  - Unico attaccante
  - Insieme di attaccanti collusi equivale ad unico attaccante superpotente

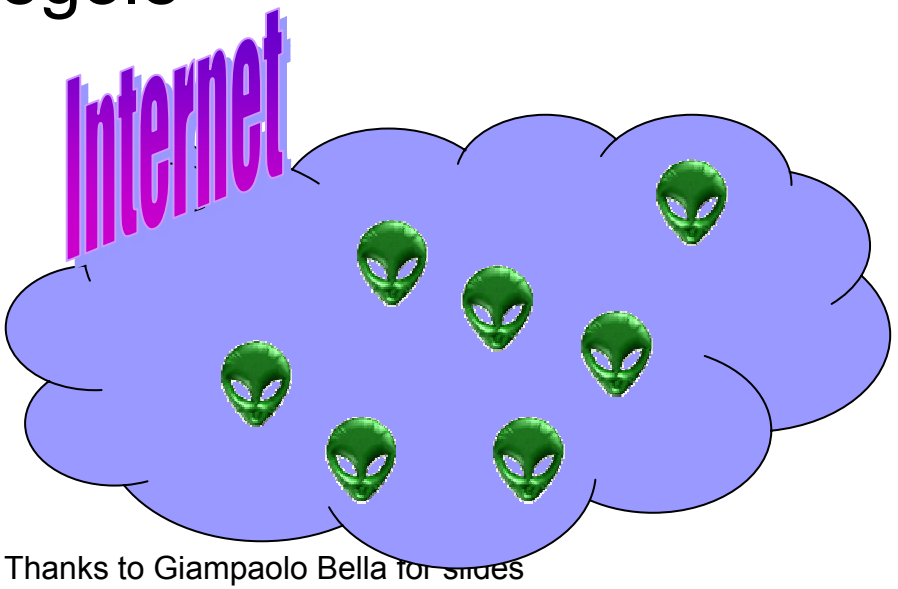


Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Modelli di attaccante

- **BUG** (2003). Tassonomia BUG
  - **B**ad: violano le regole
  - **U**gly: dipende…
  - **G**ood: seguono le regole



Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Security is not safety!!

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Security “is not” Safety (or dependability)

- Reliability (affidabilità)
  - “non sbaglia!”
- Availability (disponibilità)
  - “non da crash!”
- Maintainability (manutenibilità)
  - “E’ facilmente gestibile”
- Safety (sicurezza)
  - “non muore nessuno usandolo”

Thanks to Giampaolo Bella for slides draft!!

www.sci.unich.it/~bista/didattica/reti-sicurezza/

Confidentiality e Integrity (e authenticity)

- Come ottenerle?

- Usando la crittografia!!

Thanks to Giampaolo Bella for slides draft!!