Sicurezza Informatica
Una breve panoramica

Prof. Carlo Blundo
cblundo@unisa.it

Sicurezza Informatica

- Il termine *Sicurezza Informatica* si è evoluto nel corso degli anni
- Tradizionalmente i sistemi informatici(-vi) sono stati protetti per tre motivi
  - Impedire il furto o il danneggiamento dell'hardware
  - Impedire il furto o il danneggiamento del software
  - Impedire l'interruzione del servizio

Sicurezza Informatica

- **Beni (asset) da proteggere**
  - Hardware
  - Software
  - Dati
- **Minacce**
  - Interruzione, intercettazione, modifica, falsificazione, …

- Ricordare che
  - ✓ Security is only as strong as the *weakest link*

Attenzione all'anello debole

Sicurezza Informatica

- La protezione predisposta per un sistema informatico, al fine preservare
  - l'integrità,
  - la disponibilità
  - la riservatezza

  delle risorse del sistema (incluso hardware, software, firmware , informazioni/dati, telecomunicazioni)

NIST An Introduction to Information Security
Computer Security Handbook,
SP800-12, 1995
SP800-12r1, giugno 2017

In questo corso ci concentreremo sul problema della *protezione* dell'informazione (dati rappresentati con stringhe di bit)

Confidenzialità (*Confidentiality*)

- Confidenzialità dei dati
  - Assicura che informazioni riservate non sono rese disponibili (rese note) ad individui non autorizzati

- Privatezza (*privacy*)
  - Assicura che gli individui sono in grado di controllare quale informazione possa essere raccolta e da chi e/o a chi possa essere comunicata

Integrità (*Integrity*)

- Dei dati
  - Assicura che i dati ed i programmi sono stati modificati solo in una specifica ed autorizzata maniera
- Del sistema
  - Assicura che un sistema esegue le sue funzioni in maniera inalterata a prescindere da una manipolazione del sistema deliberata o involontaria

Disponibilità (*Availability*)

- Assicura che il sistema lavora prontamente e il suo servizio non è negato agli utenti autorizzati

- Assicura tempestivo e affidabile accesso ed utilizzo delle informazioni

La triade CIA

- I concetti espressi nelle slide precedenti sono spesso indicati come *triade CIA*
- Lo standard NIST FIPS 199 elenca la *triade CIA* come obiettivo di sicurezza dei sistemi informatici
  - La triade CIA è definita anche nella RFC 4949

~300 pp — 2007 – RFC 4949
Internet Security Glossary, Version 2

Definizioni, abbreviazioni e spiegazioni della terminologia per la sicurezza dei sistemi informatici.

13 pp — 2004 – NIST FIPS 199
Standards for Security Categorization of Federal Information and Information Systems

Livello di impatto

- Nello standard FIPS 199 è anche specificato il livello di impatto sull'organizzazione (sistema informatico) o sull'individuo che ha una violazione della sicurezza (perdita di Confidentiality, Integrity, Availability)
  - Low
  - Moderate
  - Severe

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Sicurezza Informatica

- Per valutare le necessità in termini di sicurezza di un'organizzazione (sistema informatico) e per scegliere prodotti/politiche è necessario un approccio sistematico per
  - Definire i requisiti di sicurezza
  - Caratterizzare gli approcci che soddisfano i requisiti individuati

X.800

- Tale approccio sistematico è definito in ITU-T Recommendation X.800 *Security Architecture for OSI*, 1991
- Utile per organizzare i modi con cui affrontare il problema della sicurezza di un sistema. È necessario concentrarsi su
  - Attacchi alla sicurezza
  - Meccanismi di sicurezza
  - Servizi di sicurezza

International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) è un'agenzia supportata dall'ONU

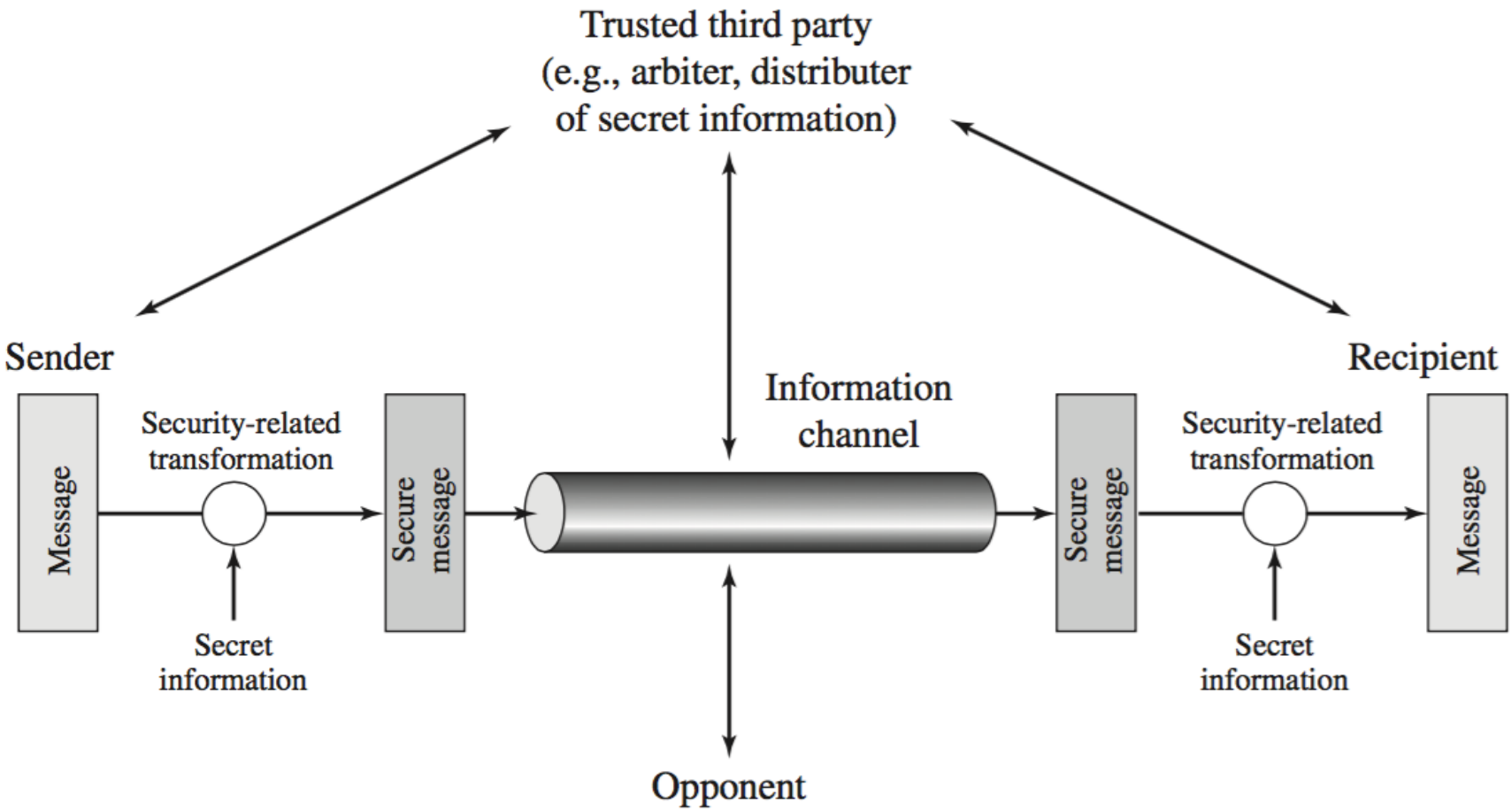
Attacchi alla sicurezza

- Sono definiti come una qualsiasi azione che compromette la sicurezza dell'informazione posseduta dall'organizzazione
- Basati sulla vulnerabilità del sistema stesso
  - La vulnerabilità è una debolezza di un sistema di sicurezza che può essere utilizzata per causare danni

Assunzione

- Supponiamo di caratterizzare il sistema informatico (computer/rete) come un sistema che fornisce informazione
- Esiste un flusso di informazione da una sorgente (file, memoria principale, …) verso una destinazione (file, utente, …)

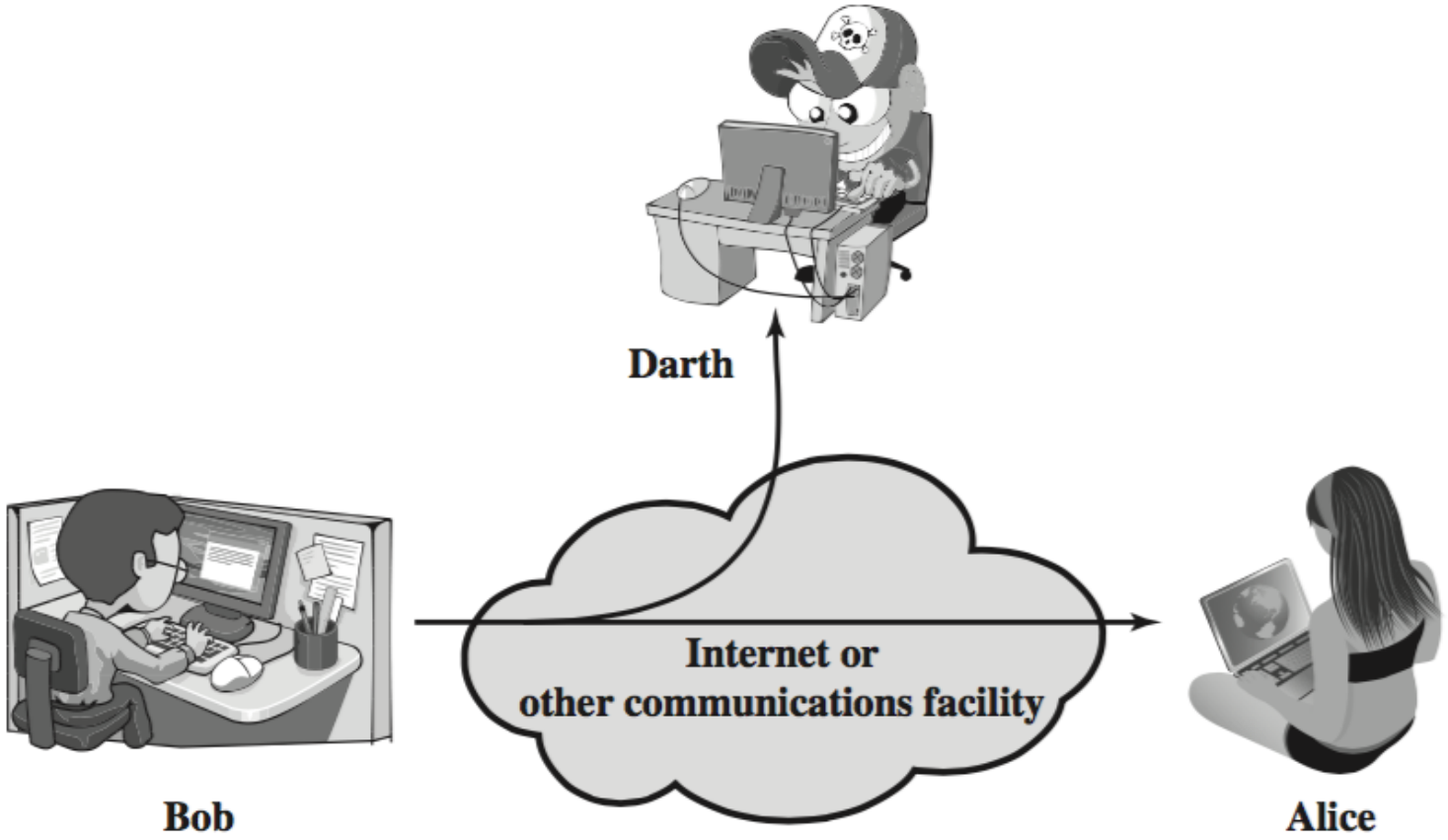
Modello


Trusted third party
(e.g., arbiter, distributer
of secret information)
Sender
Recipient
Information
channel
Message
Security-related
transformation
Secure
message
Secure
message
Security-related
transformation
Message
Secret
information
Secret
information
Opponent

Attacchi passivi

- Non alterano le informazioni in transito
- Scopo dell'attacco è ottenere informazioni sui messaggi trasmessi
  - Accesso al contenuto del messaggio
  - Analisi del traffico di rete
    - Frequenza e lunghezza dei messaggi potrebbero rivelare la natura della comunicazione

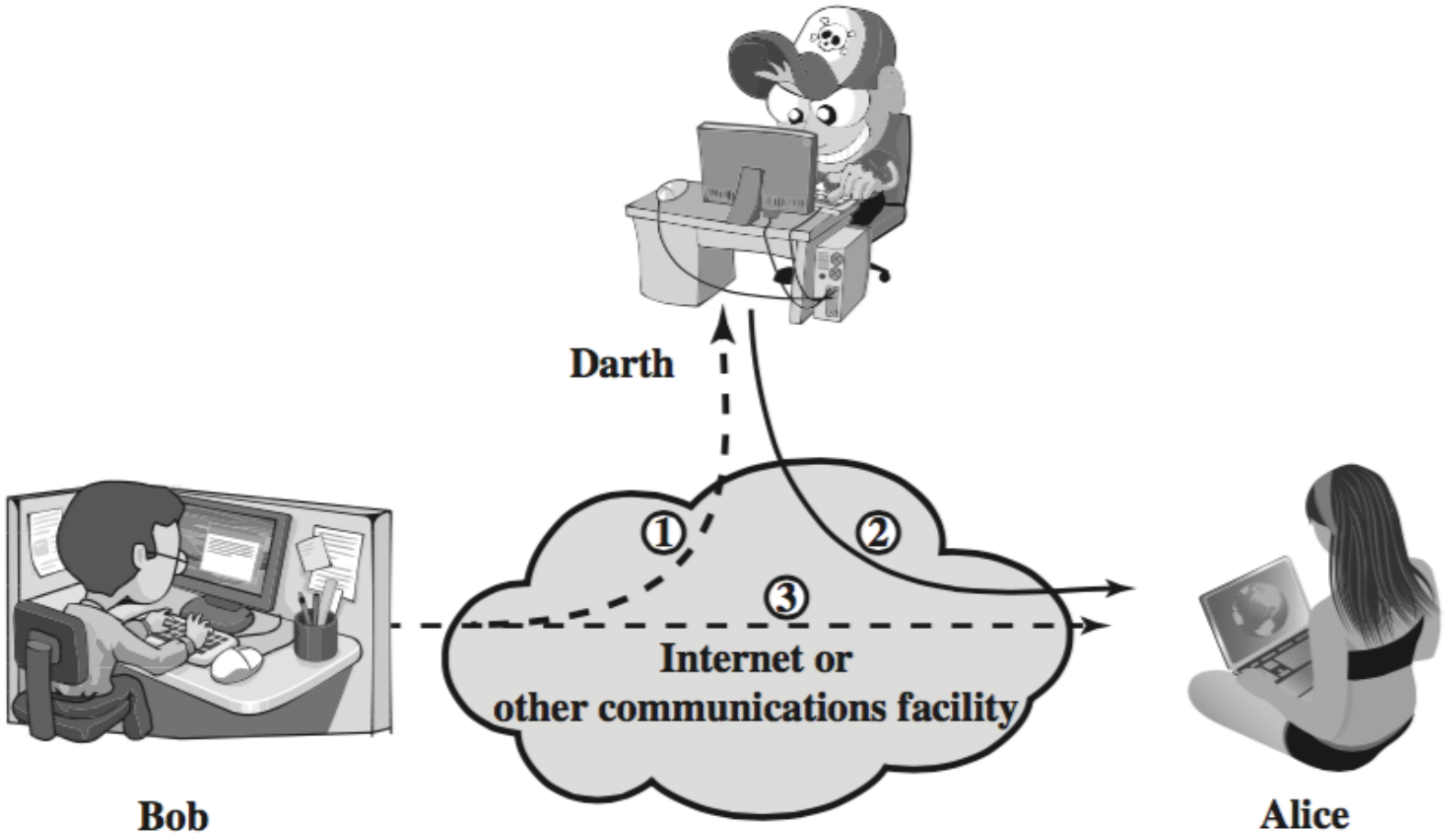
Attacco passivo



Attacchi Attivi

- Modificano il flusso delle informazioni
  - *Questo buono vale ~~€10~~ €100*
- Creano un falso flusso
  - Fingere di essere un'altra entità (*replay attack*)
- Impediscono l'utilizzo del sistema
  - Denial of Service

Attacco attivo



Meccanismo di sicurezza

ITU-T Recommendation X.800, *Security Architecture for OSI*, 1991

- È un processo progettato per
  - Individuare
  - Prevenire un attacco alla sicurezza
  - Ripristinare il *sistema* dopo

Un meccanismo di sicurezza è un metodo, strumento o procedura per far rispettare una politica di sicurezza.
Una politica di sicurezza è un'asserzione di cosa è e cosa non è permesso.

Meccanismo vs Politica

- Meccanismo: indica che cosa si deve fare, descrive come una data funzionalità deve essere realizzata
  - Adozione di AES per *proteggere* i dati
- Politica: descrive quali scelte operare in risposta ad un certo evento, indica quando e come applicare la funzionalità
  - Tutti i messsaggi in *uscita* devono essere cifrati

Accesso ai file

- Politica
  - Un qualsiasi utente che ha accesso ad un filesystem (Unix/Linux/OSX) non deve poter leggere il contenuto dei file di un altro utente

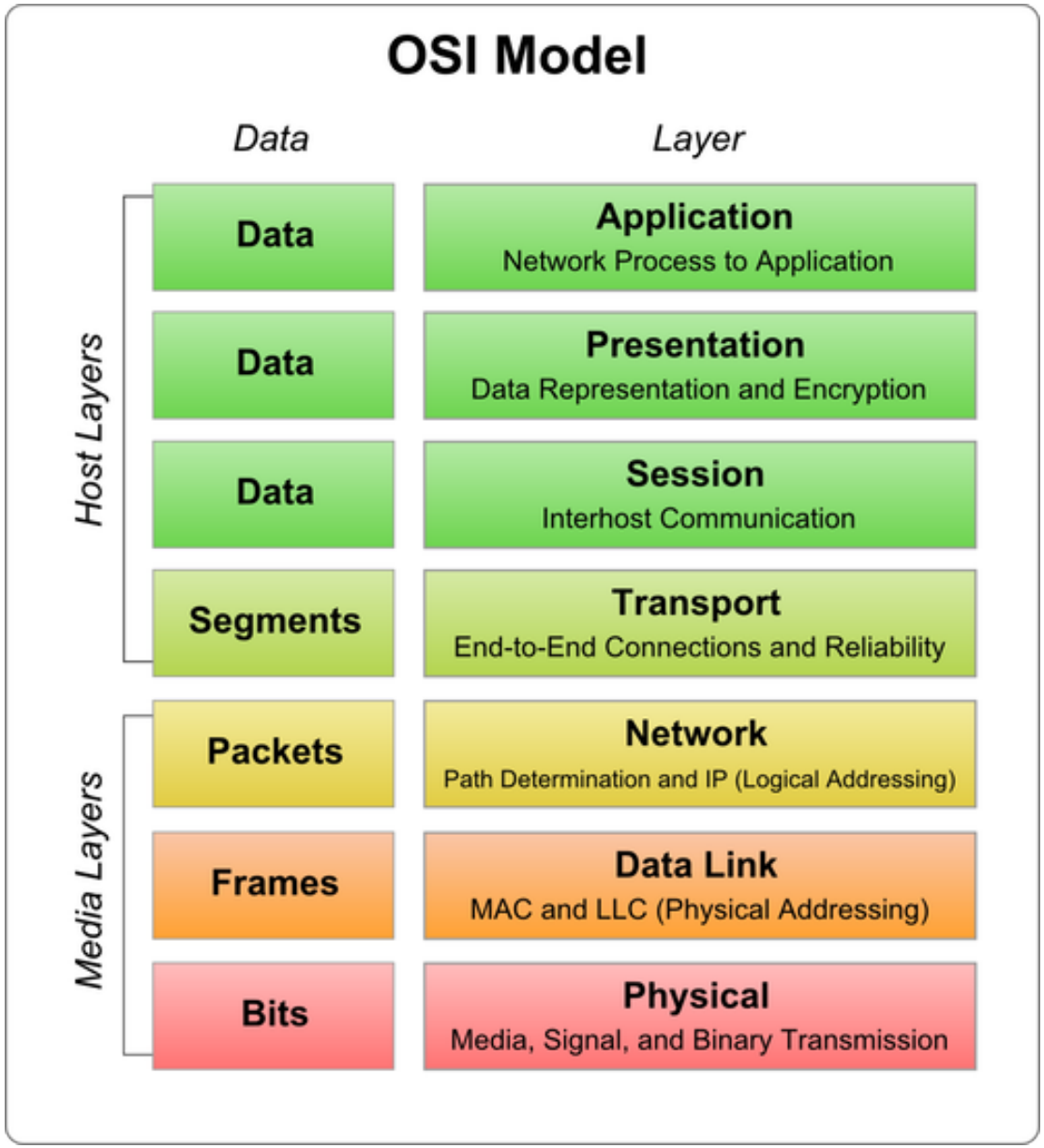
- Meccanismo
  - chmod

!!! -rw-r--r-- 1 carloblundo staff 2 15 Set 15:18 esameSicurezzaInformatica.pdf

-rw------- 1 carloblundo staff 2 15 Set 15:18 esameSicurezzaInformatica.pdf

Meccanismi di sicurezza X.800

- Meccanismi di sicurezza specifici
  - Possono essere incorporati nell'appropriato livello per fornire alcuni dei servizi di sicurezza OSI
  - Encipherment, Digital Signature, Access Control, Data Integrity, Authentication Exchange, Traffic Padding, Routing Control, Notarization


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical Addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Digital Signature – X.800

Meccanismo

Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

Meccanismi di sicurezza X.800

- Meccanismi di sicurezza pervasivi
  - Non sono specifici per un particolare servizio di sicurezza o livello OSI
  - Trusted Functionality, Security Label, Event Detection, Security Audit Trail, Security Recovery.

Security Audit Trial – X.800

Meccanismo

- *Data collected and potentially used to facilitate a security audit.*

- Security audit
  - *An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.*

Servizio di sicurezza

- Un servizio di elaborazione o comunicazione fornito da un livello ISO che incrementa la sicurezza del sistema di elaborazione ed il trasferimento dati di un'organizzazione.
- I servizi di sicurezza sono destinati a contrastare gli attacchi alla sicurezza ed utilizzano uno o più meccanismi di sicurezza per fornire il servizio.

Servizi di sicurezza X.800

- Authentication
- Access Control
- Data Confidentiality
- Data Integrity
- Non repudiation
- Availability Service

I servizi di sicurezza implementano politiche di sicurezza e sono implementati con meccanismi di sicurezza

Non repudiation – X.800

Descritto in due modi

- Non-repudiation with proof of origin
  - *The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents.*
- Non-repudiation with proof of delivery
  - *The sender of data is provided with proof of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents*.

Relazioni tra Meccanismi e Servizi

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Posta Elettronica Certificata

Meccanismi e crittografia

- In questo corso affronteremo lo studio di *primitive* crittografiche utilizzate per la realizzazione di alcuni meccanismi di sicurezza
- Il termine crittografia deriva dall'unione di due parole greche
  - κρυπτός (kryptós) nascosto
  - γραφία (graphía) scrittura
- La crittografia non si occupa soltanto di rendere inintelligibile un messaggio a chi non è autorizzato ad accedere al suo contenuto

Crittografia

- Cryptography is about communication in presence of adversaries" (R. Rivest)

- Communication

- Adversaries

Protocollo/Primitiva

- Sequenza di *passi* che devono essere eseguiti per ottenere una data funzionalità (meccanismo/servizio)

- Un *Protocollo/Primitiva Sicura preserva* la funzionalità anche in presenza di un comportamento *scorretto* (attacco)

Votazione elettronica

- Ogni cittadino può esprimere un solo voto
- Tutti i cittadini vogliono conoscere il risultato
- Alcuni di essi possono imbrogliare o per alterare il risultato delle elezioni o per conoscere il voto di altri votanti
- Un protocollo sicuro garantisce la *correttezza* del risultato e la *privatezza* del voto

Data una funzionalità

- Definire formalmente il problema
  - ***Calcolare la media degli euro che gli studenti presenti oggi a lezione hanno in tasca***
- Definire il modello di sicurezza
  - Tipo di avversario
  - Definire le proprietà che vogliamo che siano soddisfatte da un protocollo generico
  - ***Non si conosce quanto possiede ogni singolo studente***
- Provare che il protocollo proposto calcola la funzionalità (*risolve il problema*) rispetto al modello di sicurezza adottato

Assunzioni sull'avversario

- Potenza computazionale
  - Unbounded potenza computazionale illimitata, risolve il problema immediatamente
    - Unconditionally Secure Setting
  - Bounded potenza computazionale limitata
    - Computationally Secure Setting { Standard assumpion / Random Oracle
- Modalità di azione
  - Attivo/Adattivo/Malevolo
  - Passivo (HBC – Honest But Curious)

Modelli di sicurezza

- Unconditional Security
  - Gli avversari hanno potenza computazionale **illimitata**
  - Tutte le "*soluzioni*" sono possibili. La migliore strategia per l'avversario è indovinare la "*soluzione*"
- Computational Security
  - Gli avversati hanno una potenza computazionale limitata
    - Possono risolvere solo problemi che sono risolvibili in tempo polinomiale

Unconditional Security (esempio)

- Problema: inviare un testo cifrato da A a B
- La conoscenza di un testo cifrato c non fornisce nessuna informazione (nel senso di teoria dell'informazione) sul testo in chiaro m che codifica
  - Prob(M=m | C=c) = Prob(M=m)
- One-time pad
  - c = m ⊗ k (k è la chiave di cifratura)

⊗ è lo xor bit a bit

Esempio di one-time pad

C = M XOR K

M K C

0 XOR 0 → 0

0 XOR 1 → 1

1 XOR 0 → 1

1 XOR 1 → 0

Se C=1, M a cosa corrisponde?

Computational Security

- Se si riesce a "*rompere*" una primitiva (un protocollo) allora si riesce anche a calcolare **efficientemente** la soluzione di un problema che si ritiene difficile da risolvere
  - Fattorizzazione di interi
  - Calcolo del logaritmo discreto

standard cryptographic assumpion

- A volte anche se il protocollo/schema/primitiva si basa su un'assunzione crittografica esso viene *rotto* – dipende dall'implementazione

Cosa significa *rompere*

- Nel caso di un sistema di cifratura, l'avversario non dovrebbe essere in grado di
  - Recuperare la chiave di cifratura
  - Determinare il contenuto di un messaggio
  - Determinare una qualsiasi informazione significativa del messaggio
  - Calcolare una qualsiasi funzione del messaggio
    - *Calcolare funzioni fissate potrebbe essere utile*
      - Dettagli in seguito

Ad esempio riuscire a calcolare la parità di una stringa di bit

Nel caso di primitive crittografiche differenti, i requisiti potrebbero cambiare

Complessità di problemi

- Problemi *facili*
  - Cercare il ***massimo*** di ***n*** numeri — ***O(n)***
  - Ordinare ***n*** elementi — ***O(n lg n)***

- Un problema *difficile*
  - Fattorizzare ***N*** (composto da ***n*** bit) $2^{O(\sqrt{n \cdot \lg n})}$

Implementazione sbagliata => fattorizzazione efficiente

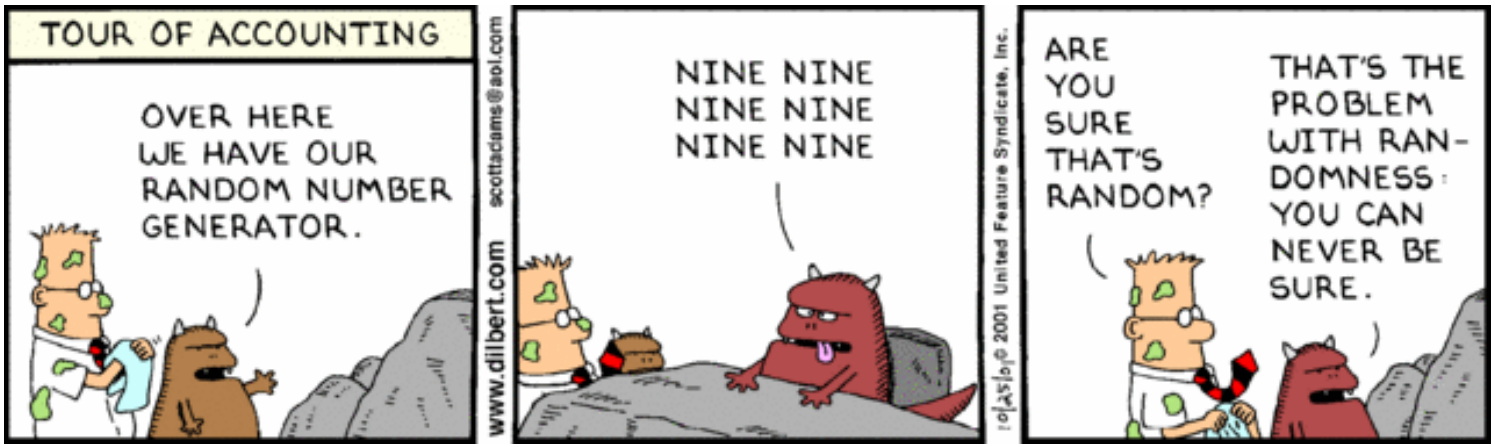
To appear in *Proceedings of the 21st USENIX Security Symposium*, August 2012. Initial public release; July 2, 2012.
For the newest revision of this paper, partial source code, and our online key-check service, visit **https://factorable.net**.

Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices

Nadia Heninger[†*] Zakir Durumeric[‡*] Eric Wustrow[‡] J. Alex Halderman[‡]

[†] *University of California, San Diego*
nadiah@cs.ucsd.edu

[‡] *The University of Michigan*
{zakir, ewust, jhalderm}@umich.edu



Esempi di problemi difficili

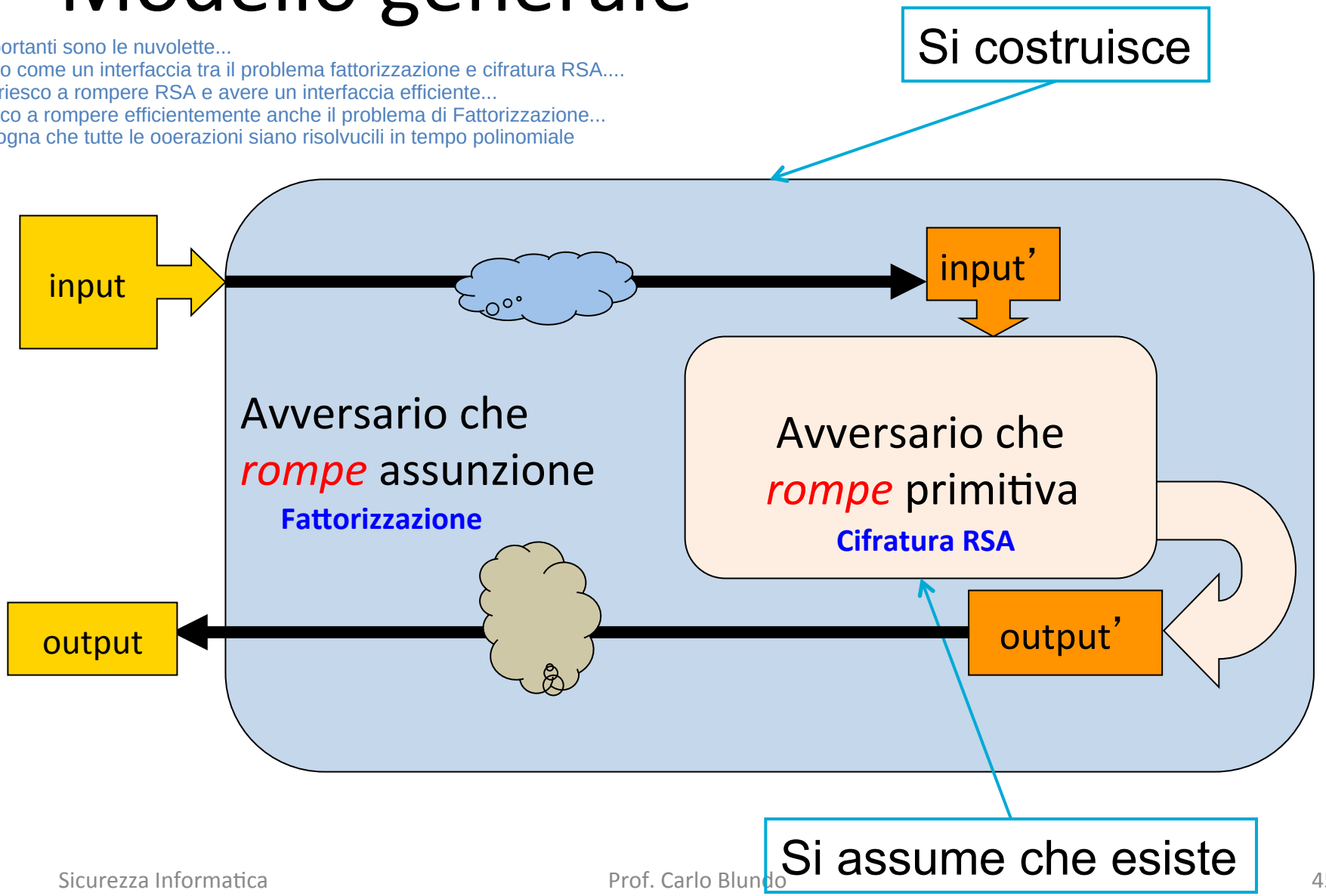
G gruppo di ordine primo

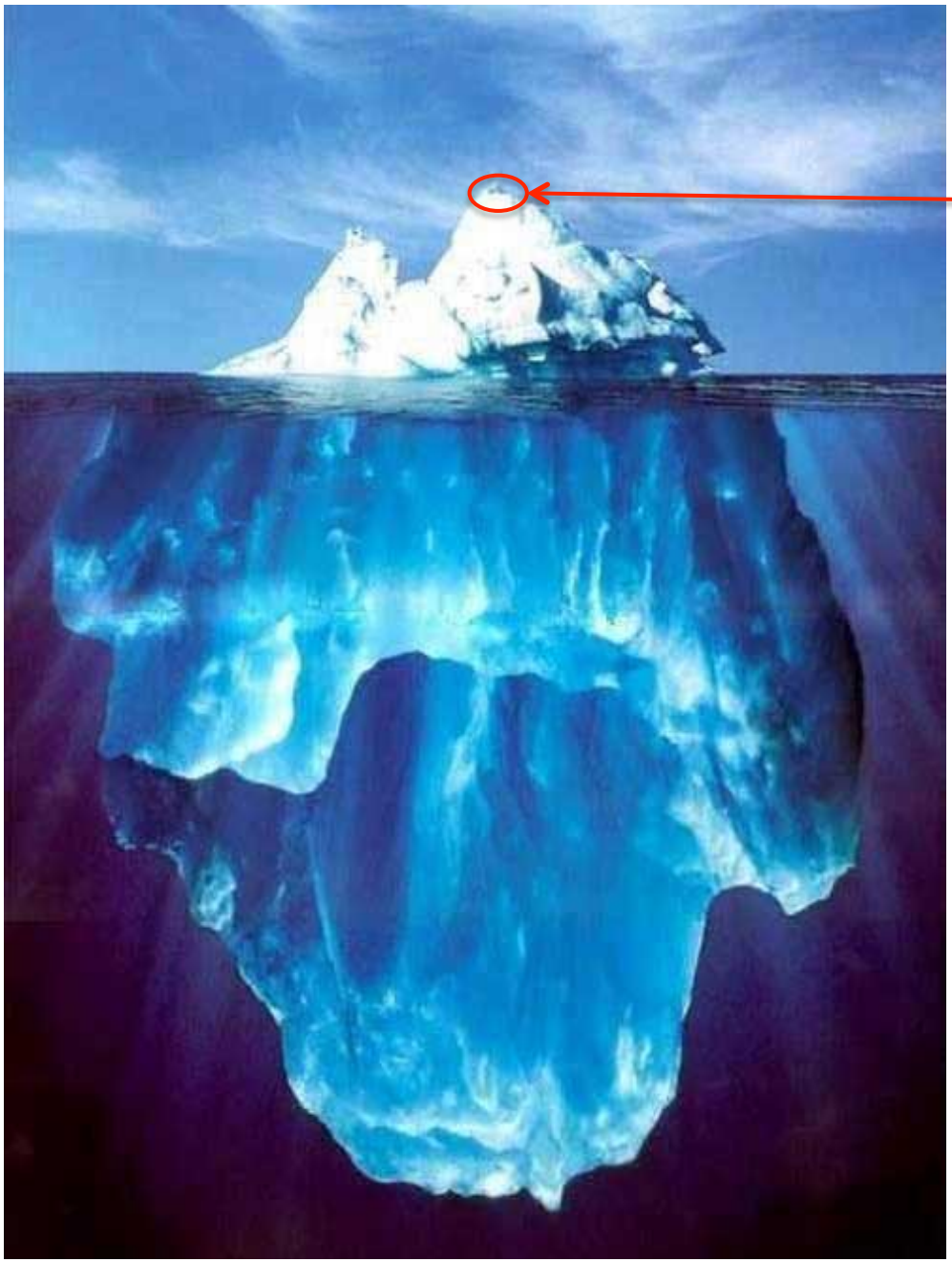
- DLP: discrete logarithm problem
  - Dato un generatore g di G e g^x calcolare x
- CDH: computational Diffie-Hellman
  - Dati un generatore g di G, g^a, e g^b in G, calcolare g^{ab}
- DDH: decision Diffie-Hellman problem
  - Dati un generatore g di G, g^a, g^b, e h in G, decidere se h = g^{ab}
    - $(g, g^a, g^b, g^{ab}) \approx^c (g, g^a, g^b, g^r)$, per r scelto a caso

$\approx^c$ significa indistinguibile computazionalmente

Modello generale

Importanti sono le nuvolette...
sono come un interfaccia tra il problema fattorizzazione e cifratura RSA....
Se riesco a rompere RSA e avere un interfaccia efficiente...
riesco a rompere efficientemente anche il problema di Fattorizzazione...
Bisogna che tutte le ooerazioni siano risolvucili in tempo polinomiale





Argomenti di Sicurezza Informatica che affronteremo in questo corso

Attacchi non ancora individuati

LM66 Laurea Magistrale in Sicurezza Informatica

Riferimenti

- William Stallings
  Cryptography and Network Security: Principles and Practice (6th Edition)
  Capitolo 2 Overview