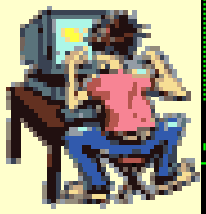


Sicurezza e Internet 02

La Sicurezza

Gli argomenti inerenti la sicurezza sono generalmente raggruppabili all'interno delle seguenti aree:

1. Sicurezza Fisica
2. Sicurezza Logica
3. Sicurezza Organizzativa
4. Piano di Continuità Operativa

Sicurezza Fisi

- Il ruolo della sicurezza fisica è quello di proteggere le persone che operano sui sistemi, le aree e le componenti del sistema informativo.

I requisiti di sicurezza fisica possono variare considerevolmente in funzione delle dimensioni e dell'organizzazione del Sistema Informativo.

- Generalmente le contromisure di sicurezza fisica possono essere ricondotte in:

1. **Sicurezza di area**

   La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi IT.

2. **Sicurezza delle apparecchiature hardware**

   Protezioni da danneggiamenti accidentali o intenzionali. Sicurezza degli impianti di alimentazione e di condizionamento. Manutenzione dell'hardware alla protezione da manomissione o furti.

Sicurezza Logica

- La sicurezza logica è una componente particolarmente critica della Sicurezza del Sistema Informativo.
- Il campo di applicazione della Sicurezza Logica riguarda principalmente la protezione dell'informazione, e di conseguenza di **dati**, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. (vedi Servizi di Sicurezza)
- Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di **misure di sicurezza** di carattere tecnologico (ICT - *Information and Communication Technology*) e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere. (vedi Meccanismi di Sicurezza)

Sicurezza Organizzativa

- Il Processo della Sicurezza del Sistema Informativo richiede che, accanto all'adozione di misure tecnologiche precedentemente illustrate, vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo medesimo.

- Gli aspetti organizzativi della Sicurezza del Sistema Informativo riguardano principalmente:
- La definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo Sicurezza;
- L'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate

Sicurezza Organizzativa

- in relazione alla propria particolare struttura organizzativa e ruoli del personale, definirà specifici compiti e responsabilità.

- In relazione al secondo aspetto elenchiamo le principali procedure organizzative per la Sicurezza del Sistema Informativo:
  - Procedure di Gestione delle Contromisure di Sicurezza Logica.
  - Procedure di Gestione specifiche per la Sicurezza della Rete.
  - Procedure di Controllo dei Sistemi di Sicurezza.
  - Procedure di Controllo del Ciclo di Vita del Software.
  - Procedure di Controllo per la Gestione delle Operazioni.
  - Procedure per la Gestione degli Incidenti.
  - Procedure per la Continuità Operativa.
  - Procedure per il Personale.

Sicurezza Organizzativa

Un’altra serie di aspetti si riferiscono a:

Documenti: Accesso ai documenti, Conservazione dei documenti, Consegna documenti, Distruzione.

Utilizzo del software: installazione, licenze d’uso, modalità d‘uso.

Password: Modalità di assegnazione, gestione ed utilizzo, validità nel tempo.

I virus informatici: Misure preventive, Regole operative, Norme sull'utilizzo dei programmi antivirus.

La posta elettronica: Norme generali, Utilizzo corretto, Attivazione del servizio.

Le risorse informatiche: Generalità, Diritto d'Uso, Autorizzazioni, Dismissione, Installazione delle postazioni, Ergonomia e salute del lavoratore, Sicurezza ambientale, Protezione da furti, Blocco fisico dell’apparato, Blocco dell’avvio da disco floppy, Protezioni logiche della risorsa.

I Supporti rimovibili, magnetici e ottici: Supporto di memorizzazione fisso o rimovibile, Distruzione dei supporti magnetici e ottici.

La rete: Gli utenti di rete, Directory condivise, Monitoraggio e Gestione, Backup Centralizzato di rete, Utilizzo della rete.

Sicurezza dei Personal Computer portatili.

Comportamenti illegali.

Norme disciplinari.

Riferimenti Normativi.

Oltre a regolamentare il comportamento dei propri utenti è necessario anche regolamentare quello di utenti esterni (ad esempio consulenti e fornitori) che operano con il Sistema Informativo o comunque che sono abilitati a connettersi con esso.

Piano di Continuità Operativa

- Il piano di continuità operativa rappresenta l'aspetto della Sicurezza principalmente orientata a garantire la continuità e la disponibilità del Sistema Informativo rispetto a danneggiamenti causati da eventi accidentali, sabotaggi, disastri naturali.
- In considerazione del fatto che i Piani di Continuità in genere richiedono investimenti significativi per la loro realizzazione, e' importante che vengano definiti, tenendo continuamente presente un corretto rapporto costi/benefici, nei limiti della loro effettiva necessità.
- L'obiettivo del Piano di Continuità Operativa è quello di **ripristinare i servizi** informatici entro un tempo prestabilito, in funzione dei livelli di servizio attesi, e di rendere minime le perdite causate dall'interruzione dell'attività.
- Ciò vuol dire che il Piano di Continuità Operativa non deve essere inteso come misura alternativa a quelle di prevenzione, ma a completamento di queste ultime, al fine di:
- Garantire la continuità dei principali processi assicurando l'erogazione dei servizi essenziali.
- Limitare gli impatti degli eventi a carattere distruttivo sulla posizione finanziaria.

Piano di Continuità Operativa

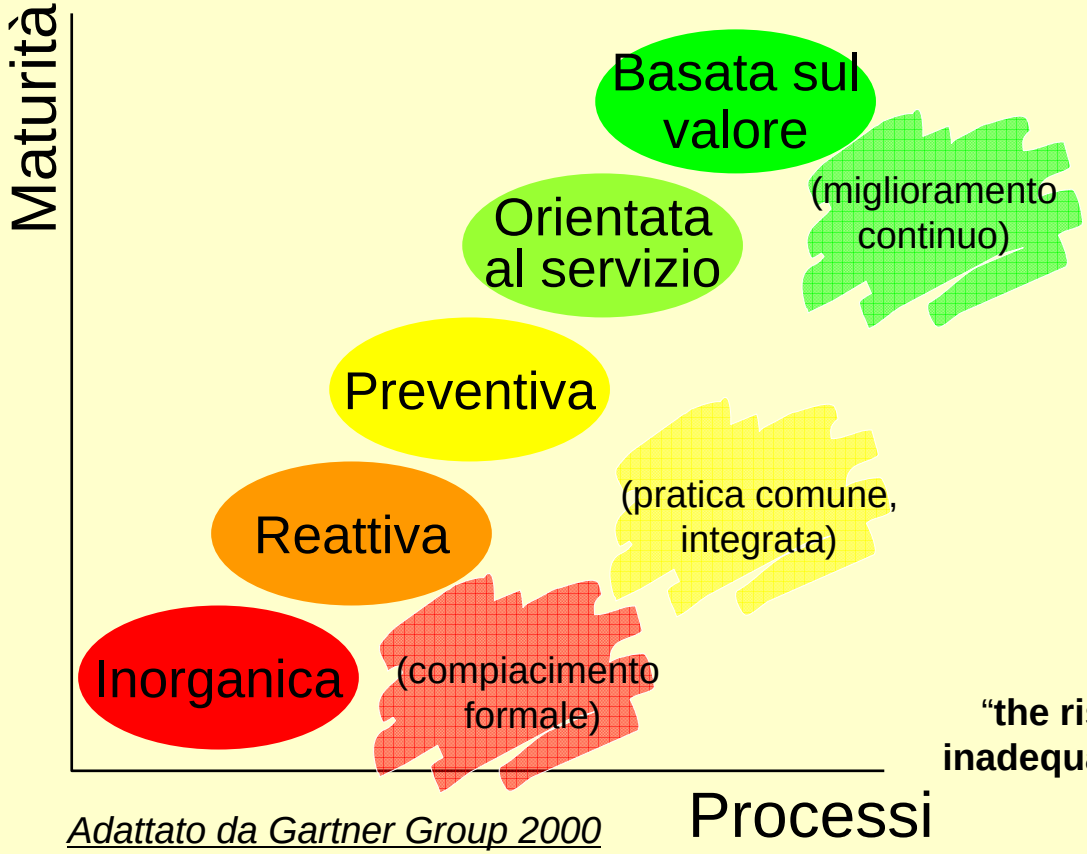
- Il processo di pianificazione della Continuità Operativa dovrebbe essere visto come un quadro di riferimento per la gestione di più procedure di ripristino orientate a coprire scenari di impatto differenziati in relazione ai diversi eventi dannosi: dalla semplice caduta di alimentazione fino agli eventi catastrofici che richiederebbero un vero e proprio Piano di *Disaster Recovery*.
- I principali *aspetti organizzativi* del piano dovranno comprendere:
  - L'assegnazione delle responsabilità individuali.
  - Le procedure di rilevamento e segnalazione.
  - Il Piano di gestione dell'emergenza.
  - L'organizzazione della ripartenza dei servizi essenziali (ripartenza automatica).
  - Il Piano di gestione della comunicazione verso le Direzioni, le altre Aziende, i terzi in genere.
  - Corsi di Sensibilizzazione e Formazione periodici.
  - La manutenzione del Piano: organizzazione di test regolari e revisioni di tutte le contromisure, le procedure ed i recovery plan.

Piano di Continuità Operativa

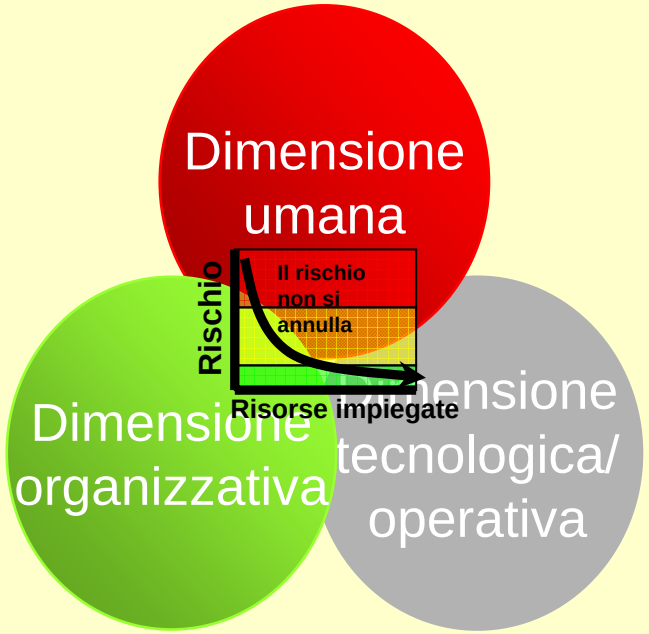
- L’attività di manutenzione del piano dovrà rivestire particolare importanza per evitare che il sistema stesso divenga rapidamente **obsoleto** ed inefficace a causa della:
  - **Evoluzione tecnologica** dei sistemi hardware e software sia del proprio Sistema Informativo che, eventualmente, del Centro di Back-up.
  - **Evoluzione organizzativa** e logistica dell’Azienda.
  - **Caduta di attenzione** delle persone coinvolte.
  - **Cambiamento delle persone** che occupano i ruoli interessati.

Gestione della sicurezza: maturità del piano

Gestione della sicurezza



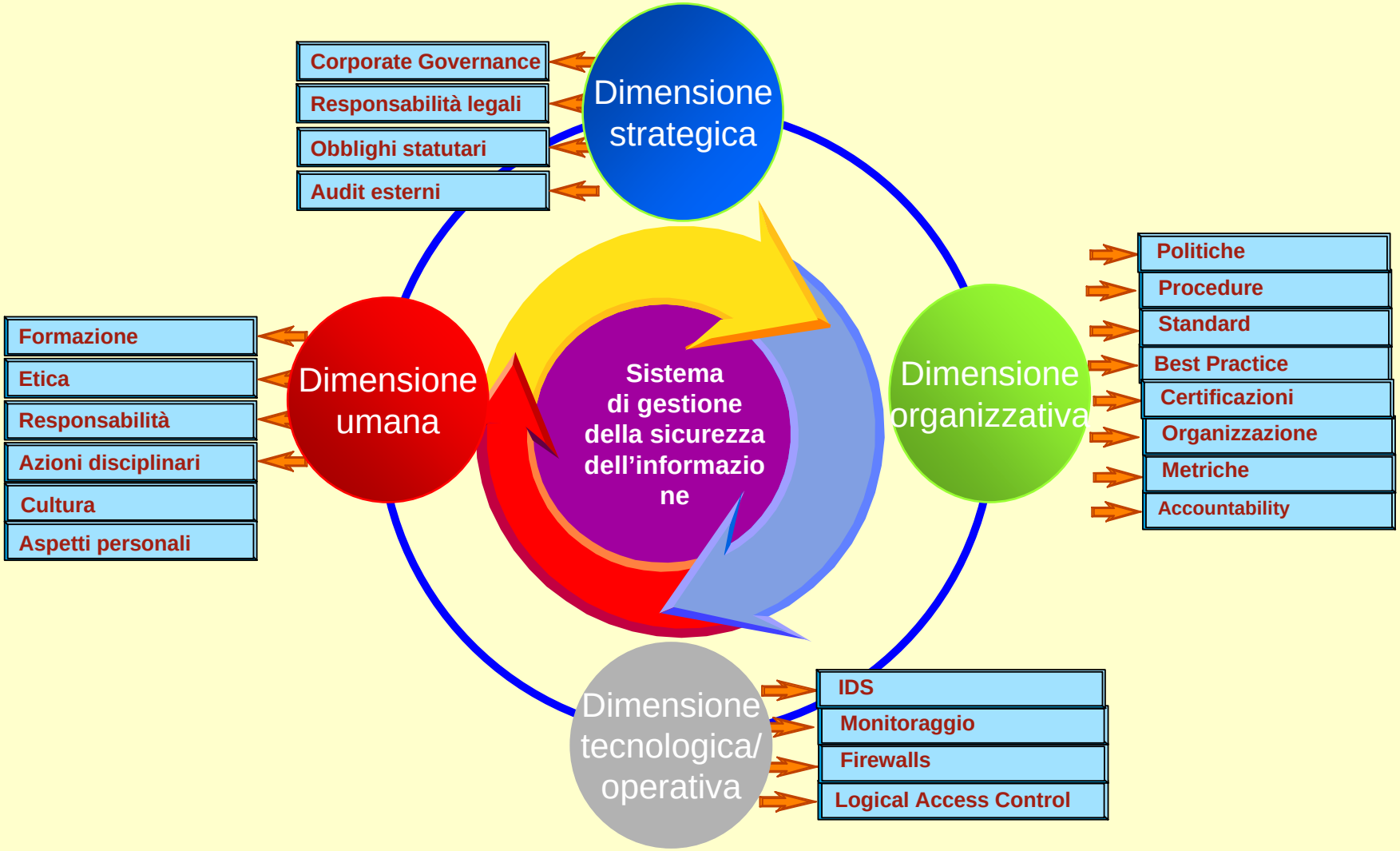
Adattato da Gartner Group 2000



“ Operational Risk “

“the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events”

Gestione della sicurezza: il ciclo virtuoso



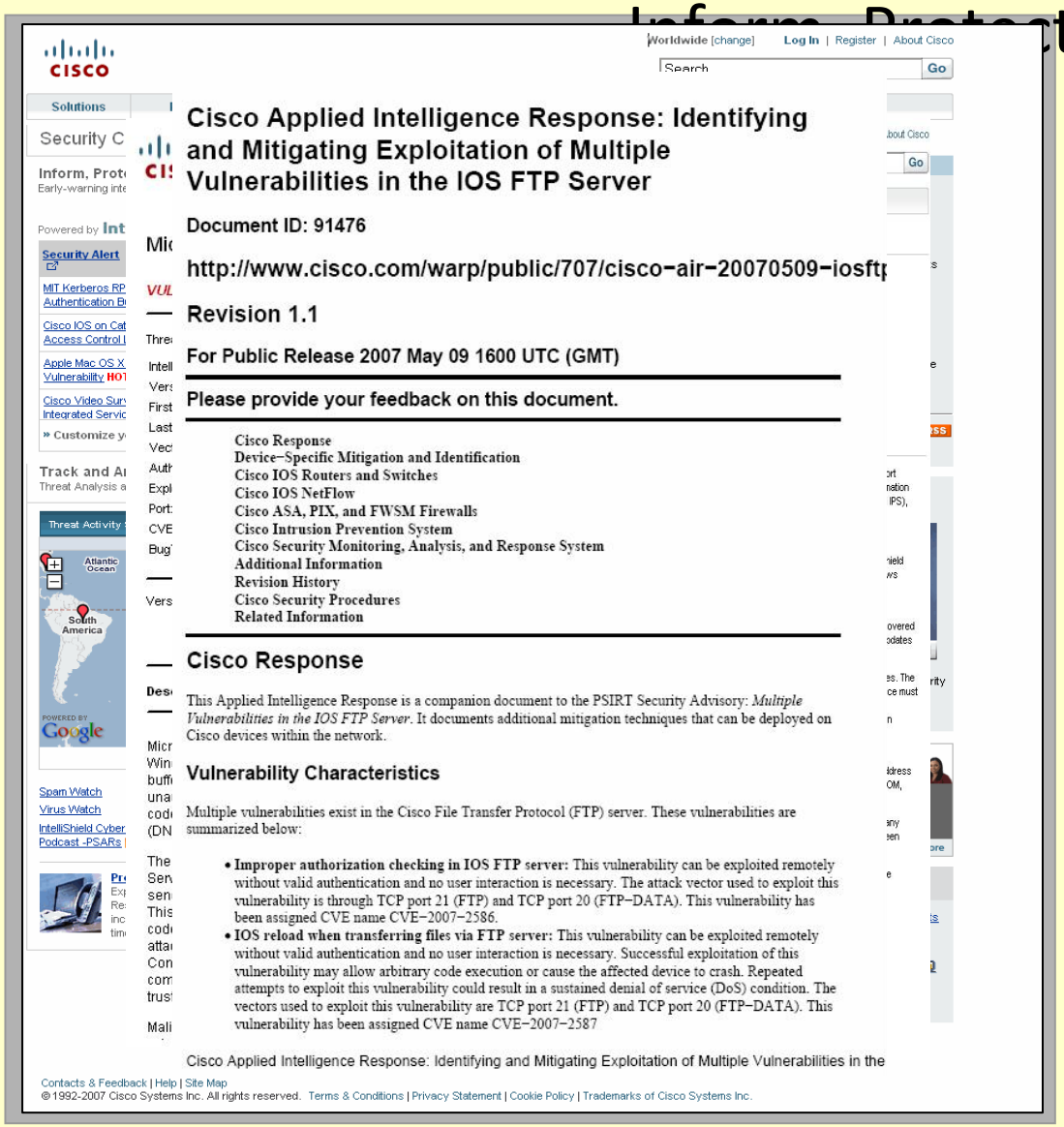
Mappa di corrispondenza

Corporate: Policy & Standards	BS7799: Key Control Areas	CISSP: Domains
Network	Section 1: Security Policy.	Domain1: Access Control Systems & Methodology
Mail	Section 2: Security Organisation.	Domain 2: Applications & Systems Development
Data Classification	Section 3: Assets Classification and Control.	Domain 3: Business Continuity Planning
Incident Handling	Section 4: Personnel Security.	Domain 4: Cryptography
Malicious Software	Section 5: Physical and Environmental Security.	Domain 5: Law, Investigation & Ethics
User Access Management	Section 6: Computer and Network Management.	Domain 6: Operations Security
Internet	Section 7: Systems Access Control.	Domain 7: Physical Security
Personnel Security	Section 8: Systems Development and Maintenance.	Domain 8: Security Architecture & Models
Physical Security	Section 9: Business Continuity Planning.	Domain 9:Security Management Practices
Software Development	Section 10: Compliance.	Domain 10: Telecommunications, Network & Internet Security
Encryption		

INFORMAZIONE AGGIORNATA

Cisco Security Center

Inform, Protect, and Respond



www.cisco.com/security

- **Vendor neutral Event-based, early-warning security intelligence**
- **Comprehensive alert analysis and mitigation solutions**
- **Real-time e-mail threat, virus, and spam tracking and trending**
- **Easy access to comprehensive security best-practice guidance**

Featured Content

- **Cisco® 2007 Security Annual Report**
  - **2008 major risk categories**
  - **2008 Cisco expert outlook**
- **Cisco Security IntelliShield Cyber Risk Report podcast**
- **Cisco Security IntelliShield Event Response reports**

Informatevi

http://www.sans.org/top20/

http://tools.cisco.com/security/center/home.x

http://www.cert.org/

http://security.dsi.unimi.it/

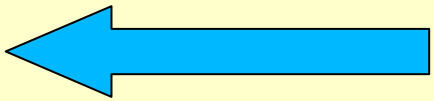
http://www.owasp.org/index.php/Top_10_2007

http://cert.uni-stuttgart.de/

http://www.poliziadistato.it/pds/informatica/uaci.html

La Sicurezza

Gli argomenti inerenti la sicurezza sono generalmente raggruppabili all'interno delle seguenti aree:

1. Sicurezza Fisica
2. Sicurezza Logica 
3. Sicurezza Organizzativa
4. Piano di Continuità Operativa

Servizi di Sicurezza

- sono le funzioni di sicurezza che il sistema dovrà garantire su tutte le piattaforme ed a tutti i livelli di elaborazione.
- ISO(*) individua i seguenti servizi di sicurezza:
  A. Autenticazione (reciproca)
  B. Controllo accessi
  C. Confidenzialità (riservatezza)
  D. Integrità
  E. Non ripudio

(*) ISO - *International Organization for Standardization*

Table 1.2 Security Services (X.800)

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

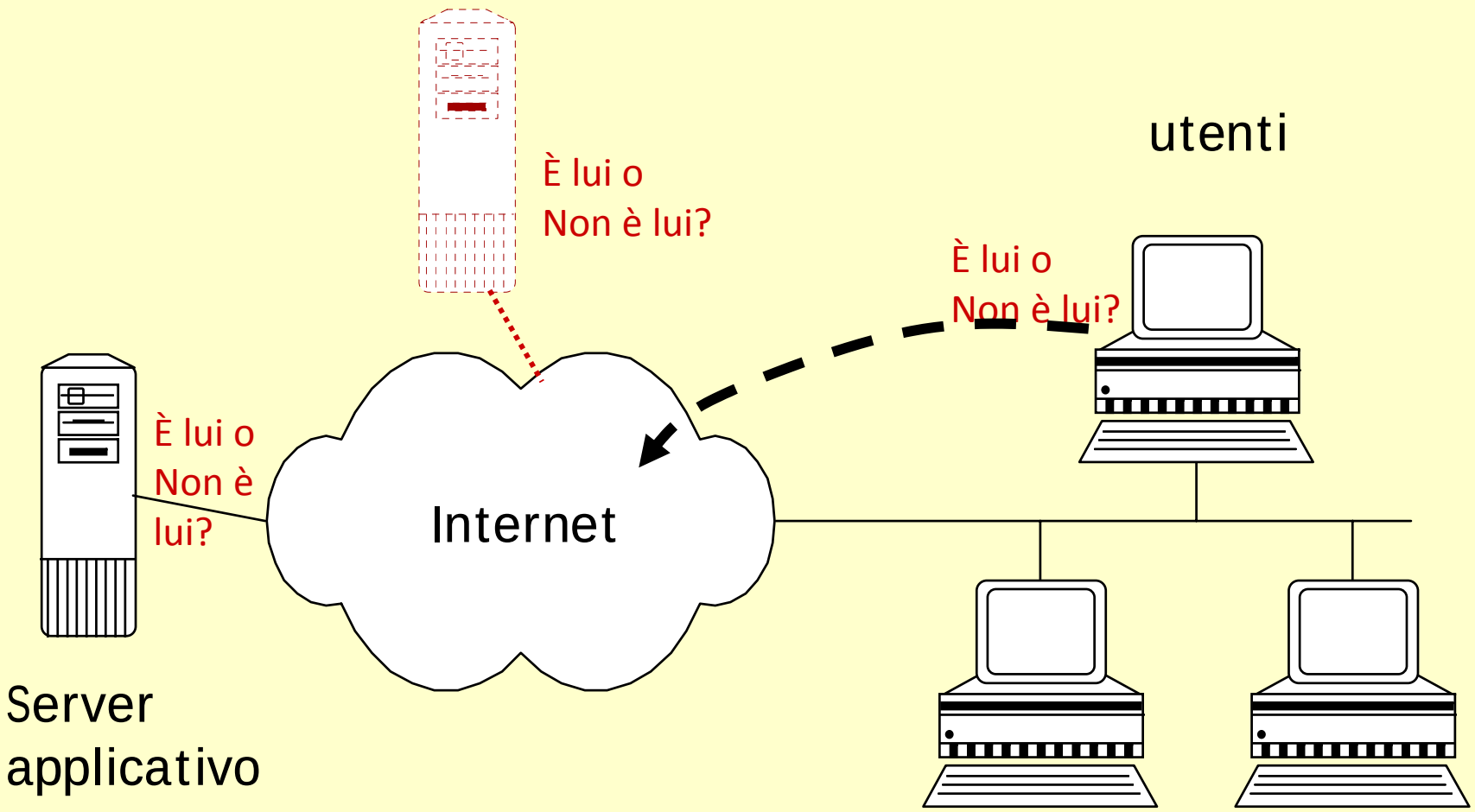
Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

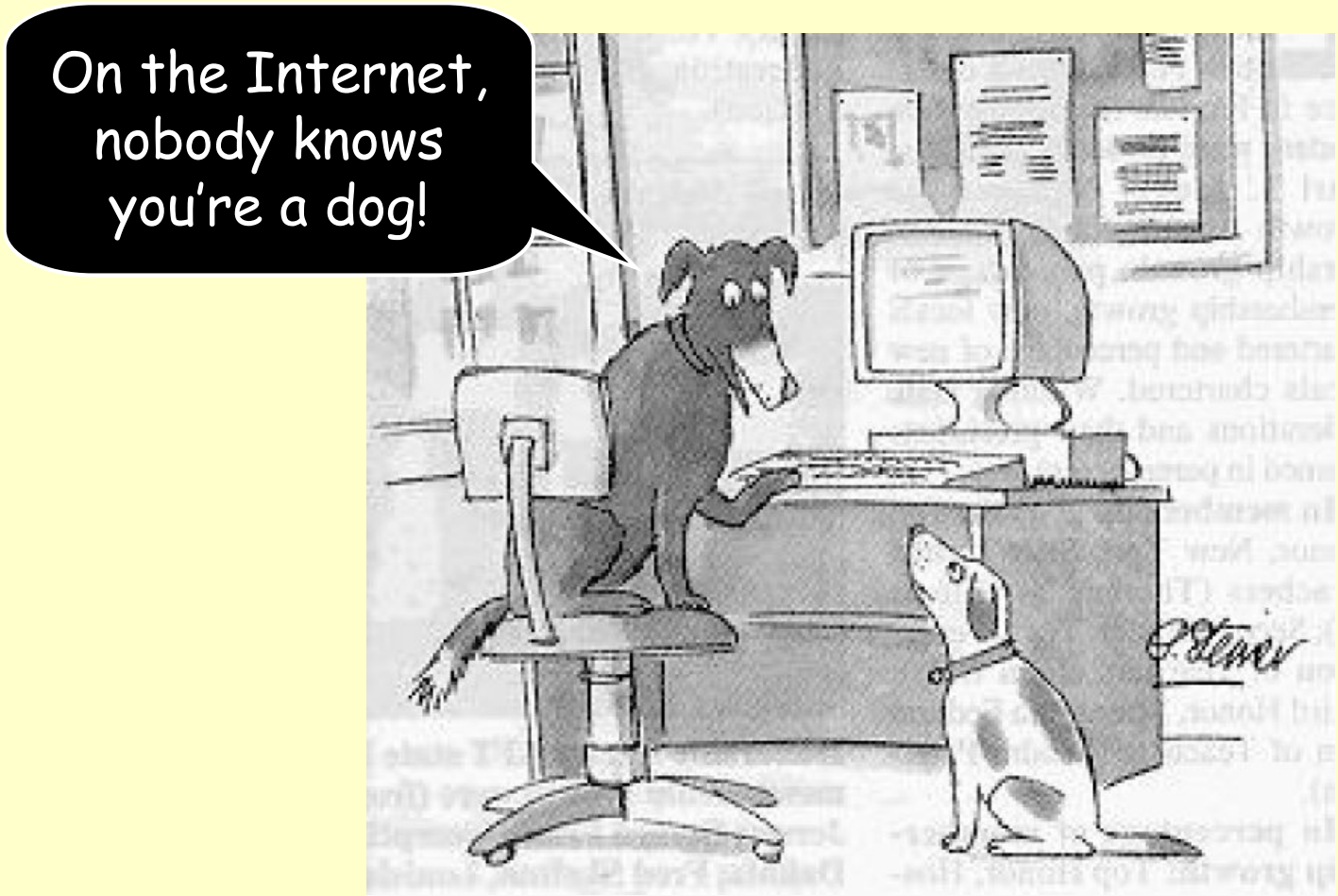
Nonrepudiation, Destination
Proof that the message was received by the specified party.

Più preci same nte

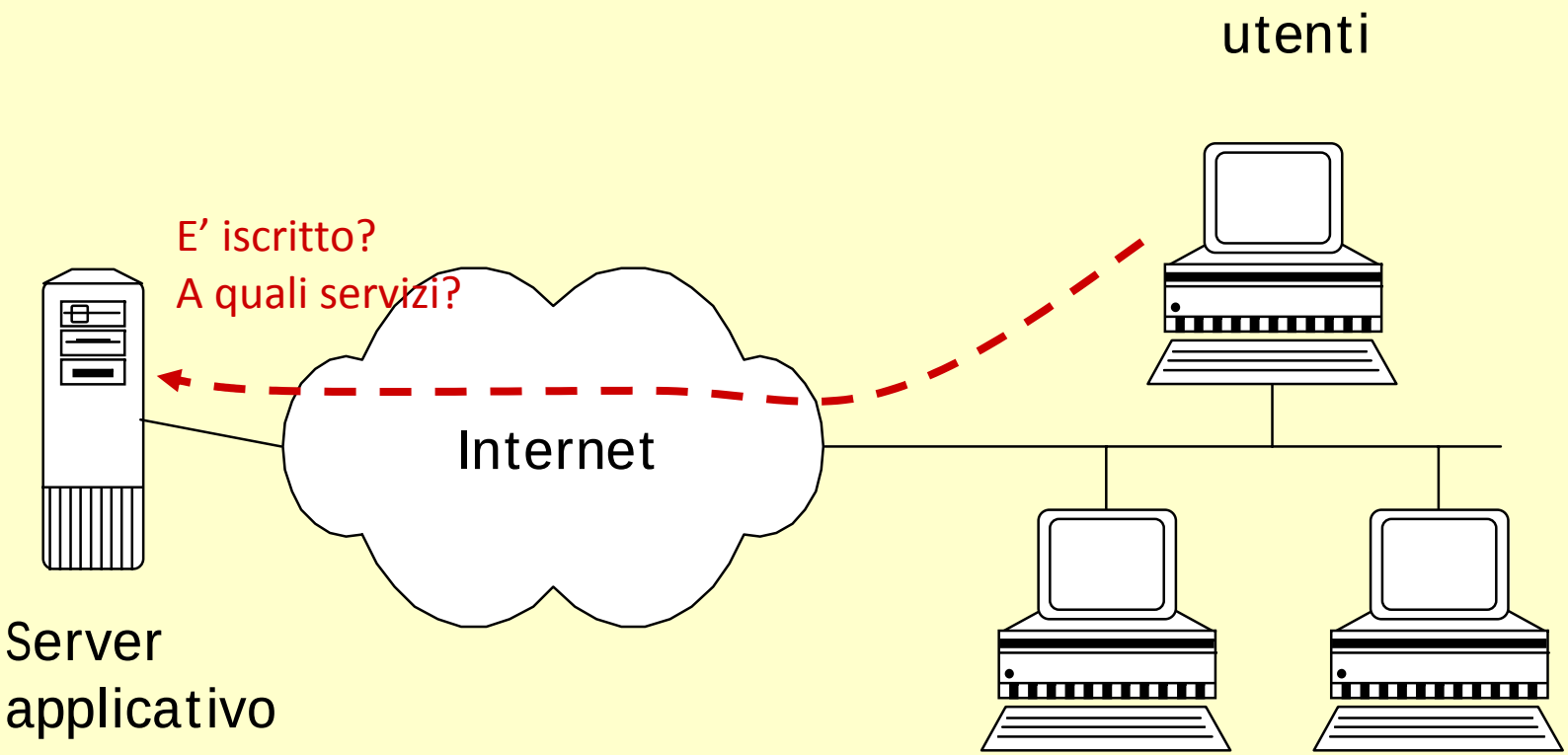
Autenticazione (reciproca)



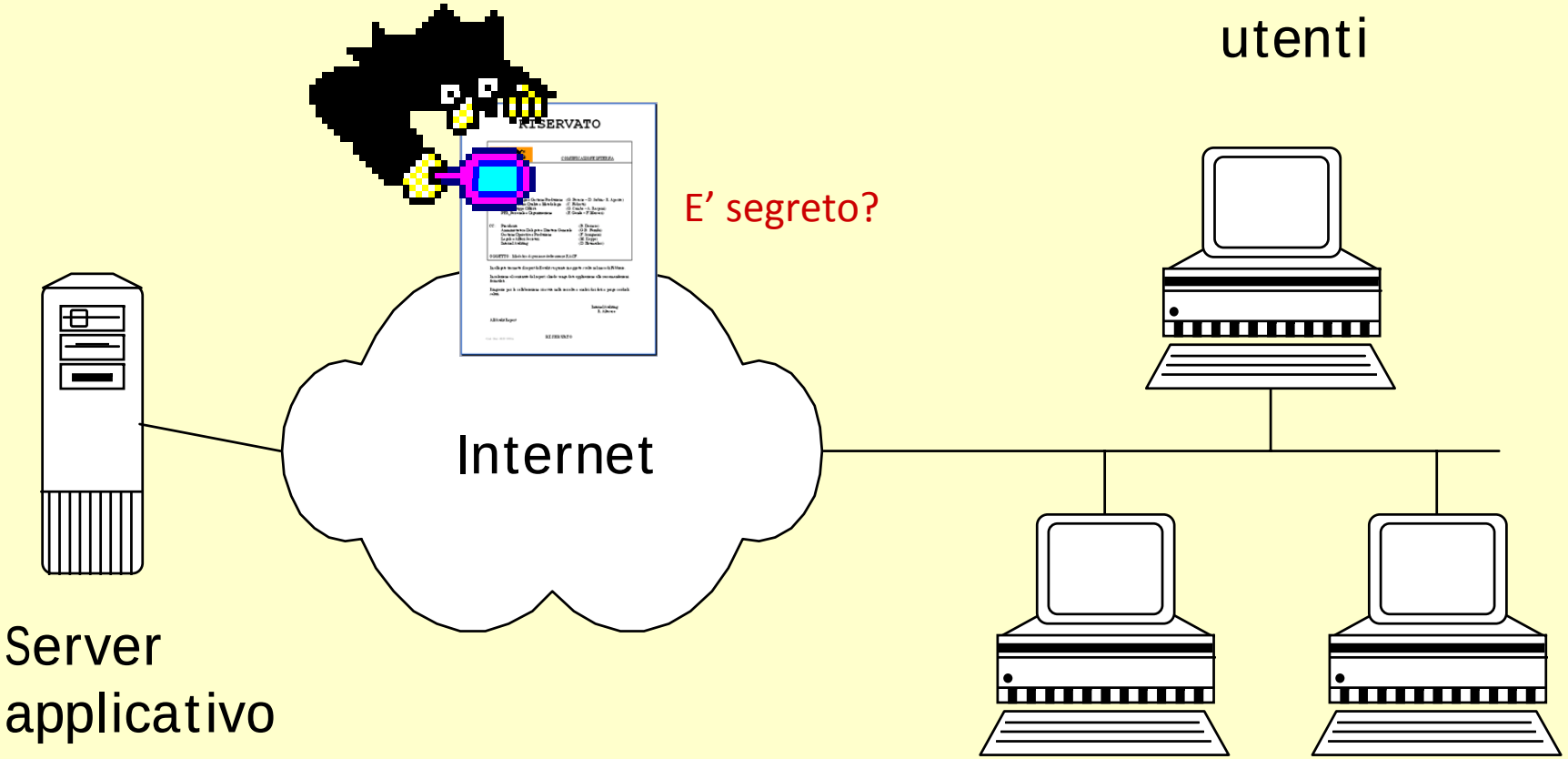
Il solito, vecchio problema



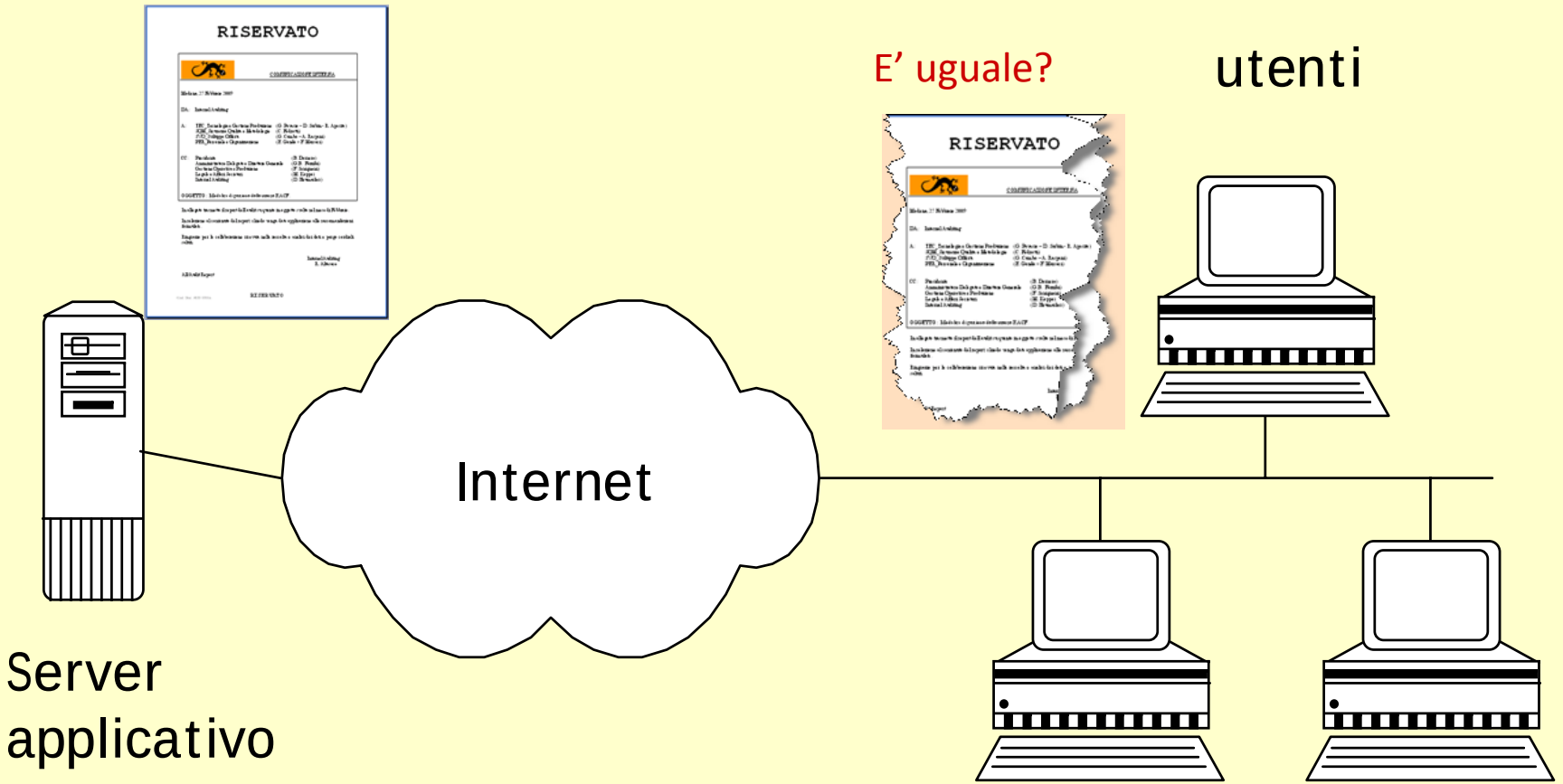
Controllo accessi



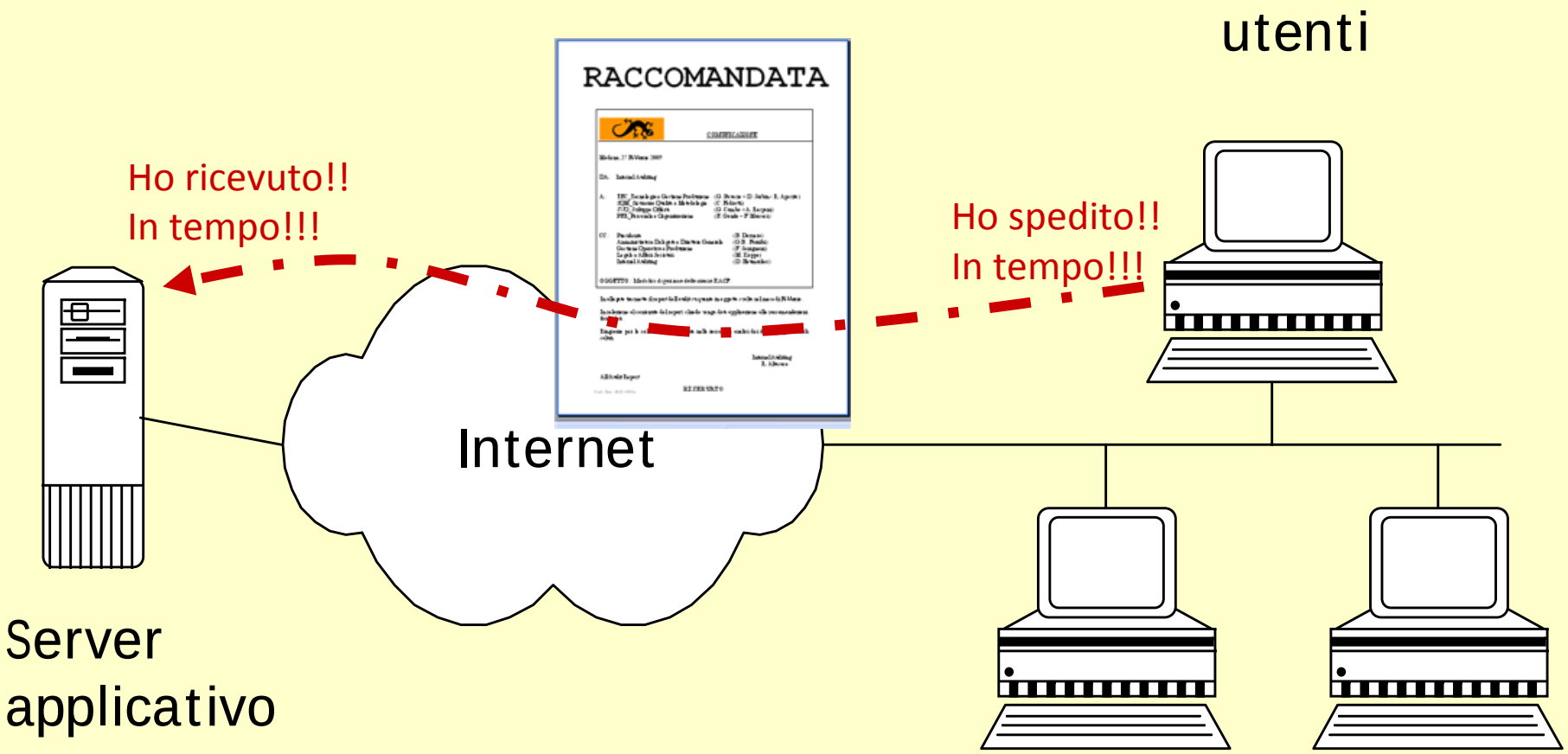
Confidenzialità (riservatezza)



Integrità


RISERVATO
E' uguale?
RISERVATO
utenti
Internet
Server
applicativo

Non ripudio


utenti
RACCOMANDATA
Ho ricevuto!!
In tempo!!!
Ho spedito!!
In tempo!!!
Internet
Server
applicativo

Meccanismi di Sicurezza

- rappresentano le modalità tecniche attraverso le quali è possibile realizzare i servizi di sicurezza.
- ISO individua (tra altri) i seguenti meccanismi di sicurezza:
  - Meccanismi per l'autenticazione (A)
  - Meccanismi per il controllo degli accessi (B)
  - Cifratura (crittografia)(C)
  - Firma digitale (D)
  - Notarizzazione (E)

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation 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).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

Più precisamente

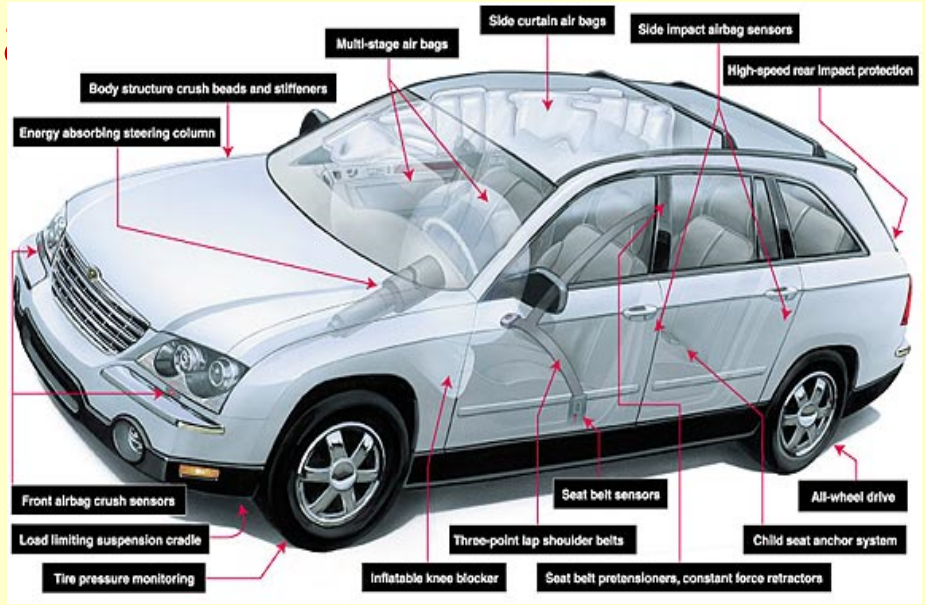
Le relazioni servizi/meccanismi

Table 1.4 Relationship Between Security Services and Mechanisms

	Mechanism							
Service	**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				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Value of Integrated Security System

Security Is No Longer an Option—It's



Security as an Option

- Security is an add-on
- Challenging integration
- Not cost-effective
- Cannot focus on core priority

Security as Integral to a System

- Security is built-in
- Intelligent collaboration
- Appropriate security
- Direct focus on core priority


The 12 Layer Matrix
Building a Cyber Fortress
OCTAVE
Chief Security Officer
Policy Management Software
Proper Systems Administration
Firewall
Authentication
Incident Response Plan
Virus Scanners
Intrusion Detection Systems (IDS)
Cyber Intelligence
Encyrption
Active Content Filtering