Sicurezza Documentale a.a. 2017/2018

DOCENTI: DOTT.SSA VALERIA FIONDA

DOTT. GIUSEPPE PIRRÒ

Sicurezza Informatica

I termini del problema

- Il problema della sicurezza può essere formulato in questi termini:

  Esistono delle informazioni di valore che devono essere protette

- Maggiore è il valore dell'informazione che vogliamo proteggere Maggiore è la complessità dei sistemi di protezione
- I sistemi di protezione sono al servizio della politica di sicurezza.
- Prima si definisce la politica di sicurezza e poi si scelgono i sistemi di protezione.

Sicurezza

- Con il termine “sicurezza” si intende l’insieme delle misure tese ad assicurare a ciascun utente autorizzato (e a nessun altro) tutti e soli i servizi previsti per l’utente, nei tempi e nelle modalità previste.

Sicurezza

- Alcune considerazioni sulla sicurezza:
  - Le regole sono fatte dagli umani
  - Gli algoritmi sono fatti degli umani
  - Una volta individuato il problema devono (o dovrebbero) intervenire gli umani

Evoluzione della tecnologia

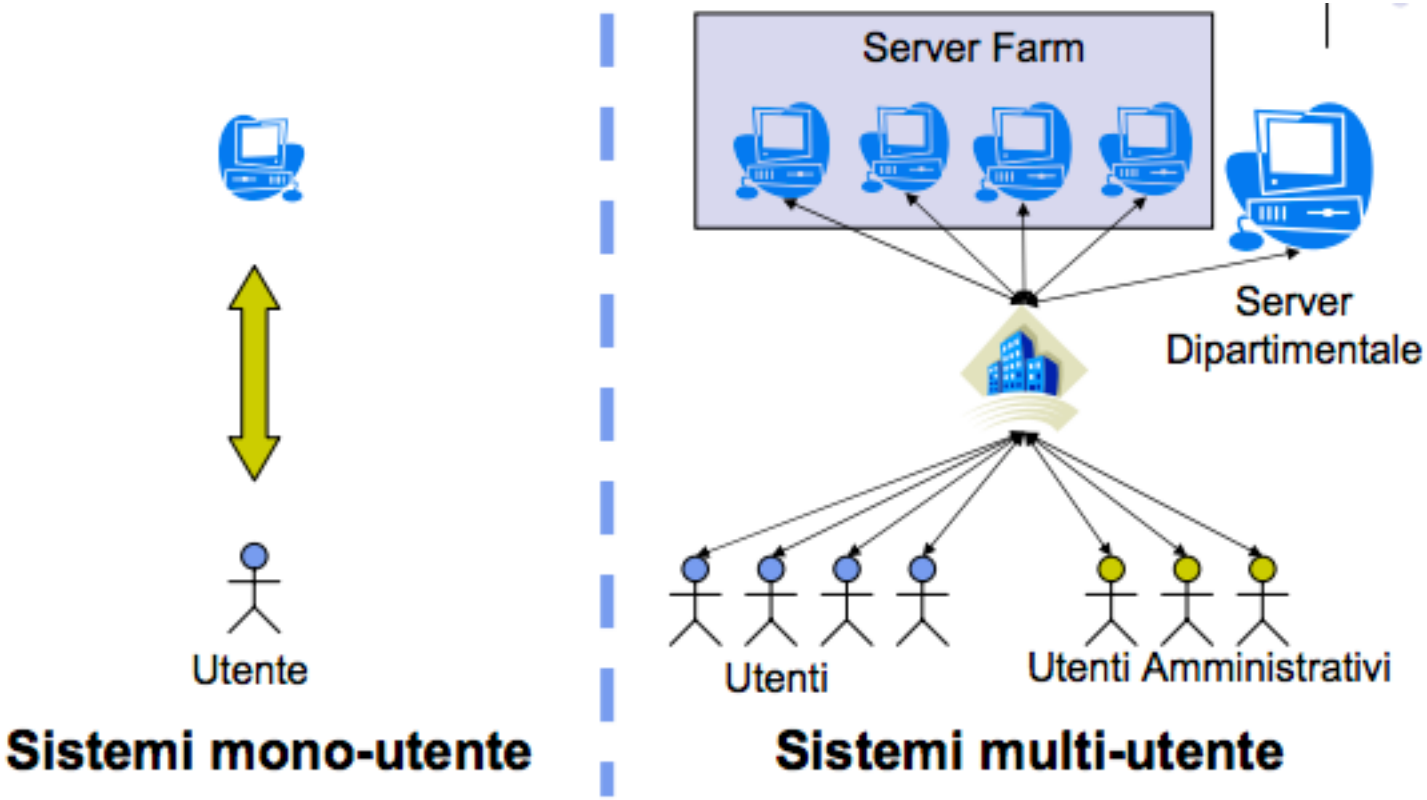
- Passato
  - Tecnologia complessa accessibile a pochi
  - Tecnologia poco diffusa
  - Scarse esposizioni ad attacchi
- Presente
  - Tecnologia semplice e modulare
  - Tecnologia molto diffusa
  - Frequenti esposizioni ad attacchi
- Futuro (?)

Evoluzione dei Sistemi Informatici

Implementazione della Sicurezza

- Passato
  - Mezzi fisici (armadi metallici a combinazione, lucchetti, ecc…)
  - Mezzi amministrativi (procedure di assunzione, impegnative sulla riservatezza, ecc…)
- Presente
  - Criptazione
  - Sistemi anti-intrusione
  - Videosorveglianza
  - …

Evoluzione dei Sistemi Informatici

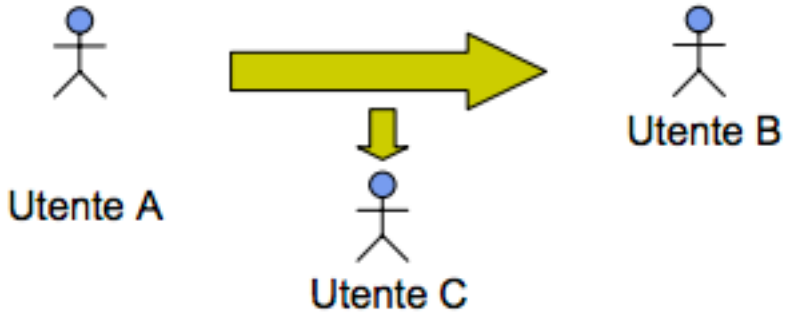


Evoluzione dei Sistemi Informatici

- Sistemi mono-utente
  - Sistema centralizzato
  - Accesso a risorse locali
  - Pochi problemi di sicurezza
- Sistemi multi-utente
  - Sistema distribuito
  - Accesso a risorse remote
  - Molti problemi di sicurezza e di autorizzazione

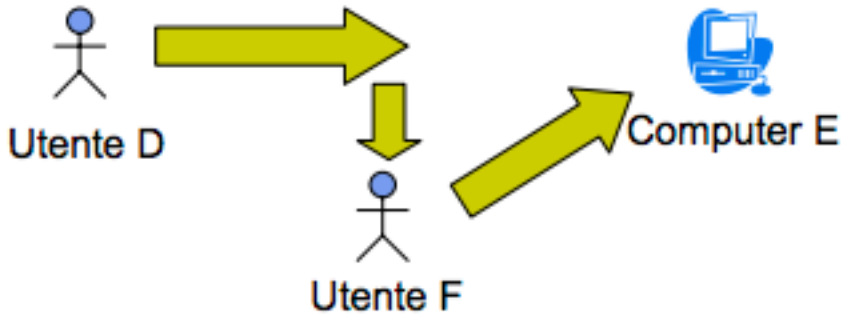
Violazione della Sicurezza: alcuni esempi

- L'utente A trasmette un file all'utente B
- Il file contiene informazioni riservate che non devono essere assolutamente divulgate (stipendi, dati sensibili, numeri di carte di credito)
- L'utente C, non autorizzato a leggere il file, effettua un monitoraggio della trasmissione e cattura un copia del file



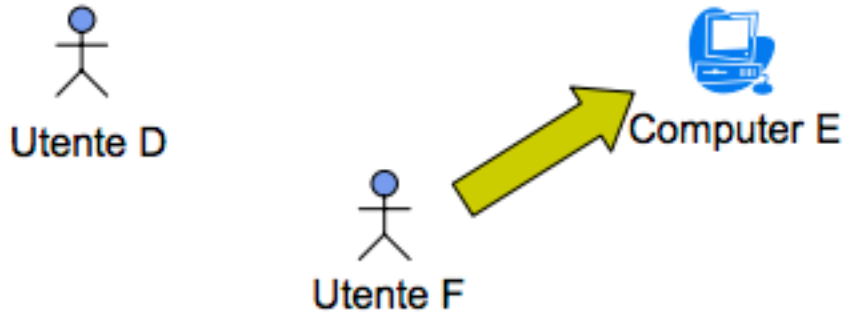
Violazione della Sicurezza: alcuni esempi

- Un amministratore della rete, D, trasmette un messaggio al computer E posto sotto il suo controllo
- Il messaggio ordina al computer E di aggiungere l'autorizzazione all'accesso per un nuovo utente
- L'utente F intercetta il messaggio, altera il suo contenuto (aggiungendo o cancellando delle voci) e poi lo inoltra ad E
- E aggiorna i permessi di accesso come se li avesse ricevuti da D



Violazione della Sicurezza: alcuni esempi

- Invece di intercettare un messaggio, l'utente F costruisce un proprio messaggio specificando le voci desiderate e lo trasmette al computer E fingendosi l'amministratore D
- Il computer E accetta il messaggio some se provenisse da D ed aggiorna il proprio file delle autorizzazioni



Violazione della Sicurezza: alcuni esempi

- Un cliente invia al suo agente di borsa un messaggio chiedendogli di eseguire determinate transazioni
- L'agente esegue ma gli investimenti richiesti perdono valore
- Il cliente nega di avere inviato il messaggio

Definizioni

- Sicurezza di Rete: misure per proteggere i dati e le transazioni durante la loro esistenza in una rete di computer; Contrariamente alla sicurezza informatica, per sistemi autonomi.
- Attacco alla Sicurezza: Qualsiasi azione che comprometta la sicurezza delle informazioni.
- Meccanismo di Sicurezza: Un meccanismo che è stato progettato per rilevare, prevenire o recuperare da un attacco alla sicurezza.
- Servizio di Sicurezza: Un servizio che aumenta la sicurezza dei sistemi di elaborazione dati e dei trasferimenti di informazioni. Un servizio di sicurezza utilizza uno o più meccanismi di sicurezza.

Servizi, meccanismi e attacchi

X.800

- È una “raccomandazione” dell’ITU (International Communication Union)
  - Standard Internazionale
  - Definizione strutturata dei servizi e dei meccanismi
  - Panoramica utile ma astratta
- In generale, secondo la definizione OSI X.800, la sicurezza è l’insieme delle misure atte a garantire :
  - Disponibilità controllata delle informazioni: il sistema deve rendere disponibili a ciascun utente abilitato le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti.
  - Integrità delle informazioni: il sistema deve impedire la alterazione diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali.
  - Riservatezza delle informazioni: il sistema deve impedire a chiunque di ottenere o dedurre, direttamente o indirettamente, informazioni che non è autorizzato a conoscere..

X.800

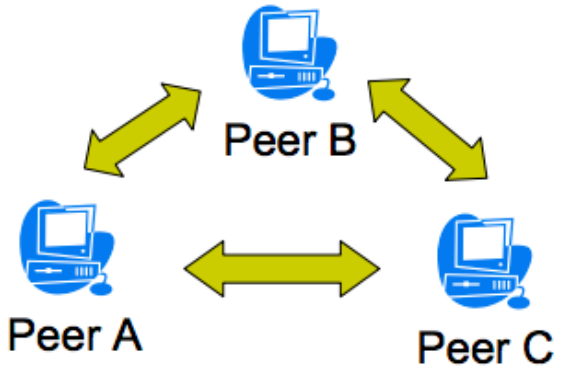
X.800 definisce cinque categorie di servizi di sicurezza:

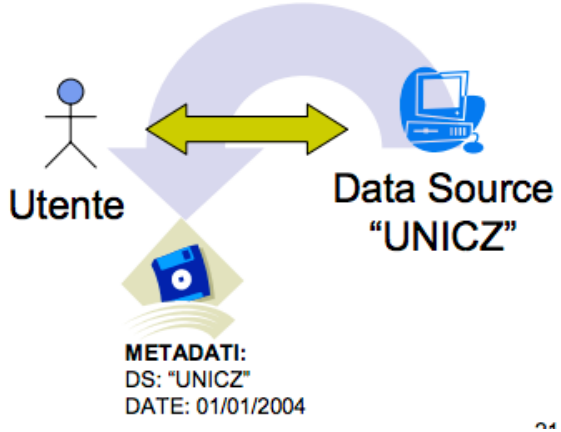
- Autenticazione: sicurezza dell'identita dei soggetti che comunicano
- Controllo degli accessi: prevenire uso non autorizzato di una risorsa
- Segretezza dei dati: protezione dei dati da osservatori non autorizzati
- Integrità dei dati: sicurezza che il dato ricevuto è uguale al dato inviato
- Non-ripudiabilità: sicurezza che il dato inviato sia stato ricevuto

X.800

Autenticazione

- la garanzia che l'entità comunicante è chi sostiene di essere
  - Autenticazione delle entità peer: garantisce l'identità delle entità connesse in una connessione logica
  - Autenticazione dell'origine dei dati: garantisce la provenienza dei dati ricevuti in un trasferimento





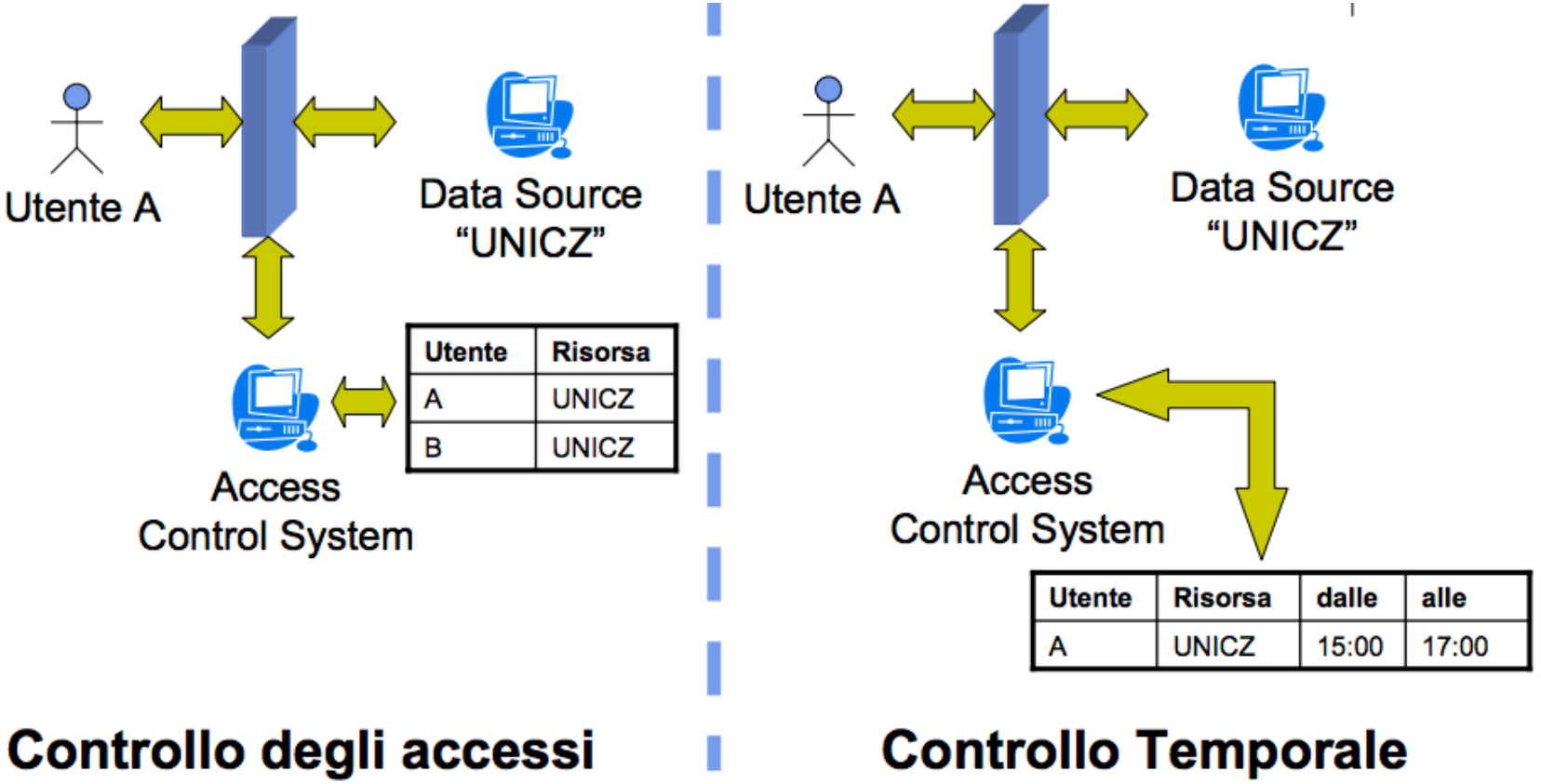
X.800

Controlo degli accessi

- Controlla chi o che cosa può accedere ad una certa risorsa
- Controlla in quali condizioni può avvenire l'accesso alla risorsa
  - Spaziali
  - Temporali
  - Logiche (architettura del sistema, stato del sistema, ecc…)
- Controlla cosa sono autorizzati a fare gli utenti o i sistemi che accedono alla risorsa

X.800

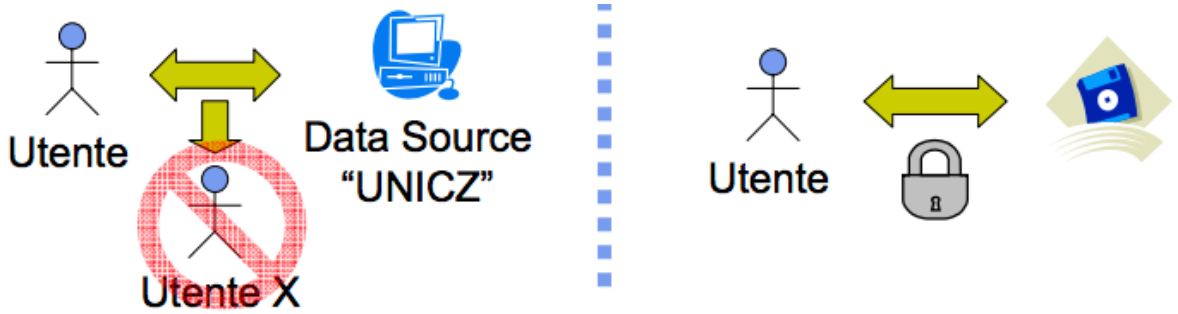
Controllo degli accessi



X.800

Segretezza dei dati

- La protezione dei dati da qualsiasi accesso non autorizzato
  - Segretezza in modalità connessa: La protezione dei dati trasferiti in una connessione
  - Segretezza in modalità non connessa: La protezione dei dati contenuti in un blocco
  - Segretezza selettiva a campi: La segretezza di un sottoinsieme di campi all'interno dei dati sia in modalità connessa che non connessa
  - Segretezza del traffico: La protezione delle informazioni che potrebbero essere ottenute dall'analisi del flusso del traffico



X.800

Integrità dei dati

- La garanzia che i dati ricevuti siano esattamente quelli inviati dall'entità autorizzata, senza essere stati modificati in alcun modo
  - Integrità in modalità connessa con ripristino: Garantisce l'integrità di tutti i dati in una connessione e rileva ogni modifica, inserimento, cancellazione o ripetizione di qualsiasi dato in una sequenza; se necessario effettua tentativi di ripristino
  - Integrità in modalità connessa senza ripristino: Come sopra; i problemi vengono rilevati ma non ripristinati
  - Integrità in modalità non connessa: Garantisce l'integrità di un singolo blocco di dati
  - Integrità selettiva a campi in modalità connessa
  - Integrità selettiva a campi in modalità non connessa

X.800

Non-ripudiabilità

- Protegge dall'eventualità che una delle entità coinvolte in una comunicazione neghi di aver partecipato, in toto o in parte, a detta comunicazione
  - Non ripudiabilità, origine: Prova che il messaggio è stato inviato dal mittente specificato
  - Non ripudiabilità, destinazione: Prova che il messaggio è stato ricevuto dal destinatario indicato