Autenticazione

Gregorio D'Agostino

4 Maggio 2021

Comunicazioni

- Gli esami saranno in presenza

Autenticazione

- L'autenticazione è il processo tramite il quale un autenticatore si assicura dell'identità di un soggetto (umano o processo) utente.

Autenticazione

- L'autenticazione è il processo tramite il quale un autenticatore si assicura dell'identità di un soggetto (umano o processo) utente.
- Il processo può svolgersi anche in due passi distinti: l'identificazione e la verifica

Autenticazione

- L'autenticazione è il processo tramite il quale un autenticatore si assicura dell'identità di un soggetto (umano o processo) utente.
- Il processo può svolgersi anche in due passi distinti: l'identificazione e la verifica
- L'dentificazione è la presentazione di un identificatore al sistema di sicurezza. Esempio non informatico: si mostra un documento di identità ad un addetto alla sicurezza, il quale verifica la corrispondenza della fotografia. In campo informatico l'esempio più semplice è la coppia userid o username (identificatore presente in una lista) e parola d'ordine o password.

Autenticazione

- L'autenticazione è il processo tramite il quale un autenticatore si assicura dell'identità di un soggetto (umano o processo) utente.
- Il processo può svolgersi anche in due passi distinti: l'identificazione e la verifica
- L'dentificazione è la presentazione di un identificatore al sistema di sicurezza. Esempio non informatico: si mostra un documento di identità ad un addetto alla sicurezza, il quale verifica la corrispondenza della fotografia. In campo informatico l'esempio più semplice è la coppia userid o username (identificatore presente in una lista) e parola d'ordine o password.
- La verifica consiste nella ulteriore presentazione di elementi identificativi (password) o nella elaborazione di dati già ricevuti. Esempio all'aeroporto oltre al passaporto si controllano le impronte digitali.

Autenticazione di una piattaforma

- Abbiamo visto un esempio comune di autenticazione, nel caso dell'accesso wireless.

Autenticazione di una piattaforma

- Abbiamo visto un esempio comune di autenticazione, nel caso dell'accesso wireless.
- Ogni scheda di rete viene identificata tramite il suo MAC address.

Autenticazione di una piattaforma

- Abbiamo visto un esempio comune di autenticazione, nel caso dell'accesso wireless.
- Ogni scheda di rete viene identificata tramite il suo MAC address.
- La verifica si ottiene chiedendo username e password. Senza l'autenticazione la connessione non viene concessa.

Autenticazione di una piattaforma

- Abbiamo visto un esempio comune di autenticazione, nel caso dell'accesso wireless.
- Ogni scheda di rete viene identificata tramite il suo MAC address.
- La verifica si ottiene chiedendo username e password. Senza l'autenticazione la connessione non viene concessa.
- La stessa procedura si applica nel protocollo IEEE 802.1x per le reti cablate.

Strumenti per l'autenticazione

- L'autenticazione si basa sui seguenti strumenti:

Strumenti per l'autenticazione

- L'autenticazione si basa sui seguenti strumenti:
  - Una informazione in possesso dell'utente: password, numero identificativo PIN (Personal Identifcation Number) o conoscenza specifica (risposta ad una domanda riservata o una serie di domande ovvie solo per il vero utente).

Strumenti per l'autenticazione

- L'autenticazione si basa sui seguenti strumenti:
  - Una informazione in possesso dell'utente: password, numero identificativo PIN (Personal Identifcation Number) o conoscenza specifica (risposta ad una domanda riservata o una serie di domande ovvie solo per il vero utente).
  - Un oggetto fisico in possesso dell'utente: carte elettroniche, smart cards, tabelline e chiavi fisiche. Questi oggetti si chiamano token (gettoni).

Strumenti per l'autenticazione

- L'autenticazione si basa sui seguenti strumenti:
  - Una informazione in possesso dell'utente: password, numero identificativo PIN (Personal Identifcation Number) o conoscenza specifica (risposta ad una domanda riservata o una serie di domande ovvie solo per il vero utente).
  - Un oggetto fisico in possesso dell'utente: carte elettroniche, smart cards, tabelline e chiavi fisiche. Questi oggetti si chiamano token (gettoni).
  - Caratteristiche biometriche: impronte digitali, scansione del viso o dell'iride, timbro vocale; analisi campioni biologici (DNA) in casi estremi.

Strumenti per l'autenticazione

- L'autenticazione si basa sui seguenti strumenti:
  - Una informazione in possesso dell'utente: password, numero identificativo PIN (Personal Identifcation Number) o conoscenza specifica (risposta ad una domanda riservata o una serie di domande ovvie solo per il vero utente).
  - Un oggetto fisico in possesso dell'utente: carte elettroniche, smart cards, tabelline e chiavi fisiche. Questi oggetti si chiamano token (gettoni).
  - Caratteristiche biometriche: impronte digitali, scansione del viso o dell'iride, timbro vocale; analisi campioni biologici (DNA) in casi estremi.
  - Caratteristiche specifiche funzionali: scrittura in corsivo (firma), sequenza vocale (modo di parlare), ritmo di battitura.

Strumenti per l'autenticazione

- L'autenticazione si basa sui seguenti strumenti:
  - Una informazione in possesso dell'utente: password, numero identificativo PIN (Personal Identifcation Number) o conoscenza specifica (risposta ad una domanda riservata o una serie di domande ovvie solo per il vero utente).
  - Un oggetto fisico in possesso dell'utente: carte elettroniche, smart cards, tabelline e chiavi fisiche. Questi oggetti si chiamano token (gettoni).
  - Caratteristiche biometriche: impronte digitali, scansione del viso o dell'iride, timbro vocale; analisi campioni biologici (DNA) in casi estremi.
  - Caratteristiche specifiche funzionali: scrittura in corsivo (firma), sequenza vocale (modo di parlare), ritmo di battitura.
- Gli elementi possono essere combinati richiedendone almeno uno (o vel, o inclusivo) oppure più di uno (e).

Strumenti per l'autenticazione

- Consentendo uno tra più possibili metodi alternativi la sicurezza globale è data dal più debole degli elementi identificativi. Esempio: sui nuovi portatili (e gli ultimi i-phone) si può accedere sia via password che con la scansione dell'impronta digitale. La sicurezza è data dal più debole dei due metodi (l'impronta).

Strumenti per l'autenticazione

- Consentendo uno tra più possibili metodi alternativi la sicurezza globale è data dal più debole degli elementi identificativi. Esempio: sui nuovi portatili (e gli ultimi i-phone) si può accedere sia via password che con la scansione dell'impronta digitale. La sicurezza è data dal più debole dei due metodi (l'impronta).
- Se invece si chiede di superare due diversi test di identificazione, la sicurezza è maggiore di entrambi gli elementi. Nel caso in cui siano totalmente indipendenti la probabilità di autentificazione erronea è il prodotto delle probabilità.

Vulnerabilità specifiche

- Ogni metodo presenta le sue vulnerabilità.

Vulnerabilità specifiche

- Ogni metodo presenta le sue vulnerabilità.
  - Le password possono essere scoperte, trafugate o estorte.

Vulnerabilità specifiche

- Ogni metodo presenta le sue vulnerabilità.
  - Le password possono essere scoperte, trafugate o estorte.
  - I tokens possono essere smarriti, rubati o danneggiati.

Vulnerabilità specifiche

- Ogni metodo presenta le sue vulnerabilità.
  - Le password possono essere scoperte, trafugate o estorte.
  - I tokens possono essere smarriti, rubati o danneggiati.
  - I caratteri biometrici possono essere emulati (sia ingannando la macchina, che simulando con perizia).

Vulnerabilità specifiche

- Ogni metodo presenta le sue vulnerabilità.
  - Le password possono essere scoperte, trafugate o estorte.
  - I tokens possono essere smarriti, rubati o danneggiati.
  - I caratteri biometrici possono essere emulati (sia ingannando la macchina, che simulando con perizia).
- L'istallazione dei dispositivi di sicurezza per l'autenticazione implica costi, allocazione di memoria e tempo di elaborazione.

Affidabilità dei metodi autenticativi

- Quando un processo identificativo (test) identifica un soggetto inappropriato si dice che incorre in un falso positivo.

Affidabilità dei metodi autenticativi

- Quando un processo identificativo (test) identifica un soggetto inappropriato si dice che incorre in un falso positivo.
- Quando un processo identificativo (test) non identifica un soggetto appropriato si dice che incorre in un falso negativo.

Affidabilità dei metodi autenticativi

- Quando un processo identificativo (test) identifica un soggetto inappropriato si dice che incorre in un falso positivo.
- Quando un processo identificativo (test) non identifica un soggetto appropriato si dice che incorre in un falso negativo.
- La probabilità di rifiutare l'identificazione ad un soggetto inappropriato si chiama "potere di reiezione". E' il complementare della probabilità di commettere un errore del primo tipo.

Affidabilità dei metodi autenticativi

- Quando un processo identificativo (test) identifica un soggetto inappropriato si dice che incorre in un falso positivo.
- Quando un processo identificativo (test) non identifica un soggetto appropriato si dice che incorre in un falso negativo.
- La probabilità di rifiutare l'identificazione ad un soggetto inappropriato si chiama "potere di reiezione". E' il complementare della probabilità di commettere un errore del primo tipo.
- La probabilità di eseguire l'identificazione ad un soggetto appropriato si chiama "efficienza". E' il complementare della probabilità di commettere un errore del secondo tipo.

Affidabilità dei metodi autenticativi

- Quando un processo identificativo (test) identifica un soggetto inappropriato si dice che incorre in un falso positivo.
- Quando un processo identificativo (test) non identifica un soggetto appropriato si dice che incorre in un falso negativo.
- La probabilità di rifiutare l'identificazione ad un soggetto inappropriato si chiama "potere di reiezione". E' il complementare della probabilità di commettere un errore del primo tipo.
- La probabilità di eseguire l'identificazione ad un soggetto appropriato si chiama "efficienza". E' il complementare della probabilità di commettere un errore del secondo tipo.
- Di solito si realizza un compromesso tra le due esigenze per evitare che un errore umano accettabile dell'utente renda le risorse irraggiungibili e limitare le fruizioni non autorizzate.

Identificazione per password

- Tipicamente funziona su interrogazione. All'utente (o al processo) viene chiesto il suo nome (codice identificativo) ID e poi la password ad esso relativa.

Identificazione per password

- Tipicamente funziona su interrogazione. All'utente (o al processo) viene chiesto il suo nome (codice identificativo) ID e poi la password ad esso relativa.
- Le password vengono memorizzate in forma cifrata in opportuni file di sistema.

Identificazione per password

- Tipicamente funziona su interrogazione. All'utente (o al processo) viene chiesto il suo nome (codice identificativo) ID e poi la password ad esso relativa.
- Le password vengono memorizzate in forma cifrata in opportuni file di sistema.
- L'ID definisce l'insieme delle risorse a cui un determinato utente è autorizzato ad accedere. In particolare può essere negata ogni forma di accesso (l'utente non esiste) o gli si possono attribuire dei privilegi specifici.

Identificazione per password

- Tipicamente funziona su interrogazione. All'utente (o al processo) viene chiesto il suo nome (codice identificativo) ID e poi la password ad esso relativa.
- Le password vengono memorizzate in forma cifrata in opportuni file di sistema.
- L'ID definisce l'insieme delle risorse a cui un determinato utente è autorizzato ad accedere. In particolare può essere negata ogni forma di accesso (l'utente non esiste) o gli si possono attribuire dei privilegi specifici.
- Nei sistemi linux gli utenti possono essere super-user con nessun limite di accesso o utenti ordinari (users). Gli utenti (tutti) possono far parte di gruppi.

Identificazione per password

- Tipicamente funziona su interrogazione. All'utente (o al processo) viene chiesto il suo nome (codice identificativo) ID e poi la password ad esso relativa.
- Le password vengono memorizzate in forma cifrata in opportuni file di sistema.
- L'ID definisce l'insieme delle risorse a cui un determinato utente è autorizzato ad accedere. In particolare può essere negata ogni forma di accesso (l'utente non esiste) o gli si possono attribuire dei privilegi specifici.
- Nei sistemi linux gli utenti possono essere super-user con nessun limite di accesso o utenti ordinari (users). Gli utenti (tutti) possono far parte di gruppi.
- Gli utenti ordinari possono avere accesso solo alle risorse proprie, del proprio gruppo o accessibili a tutti.

Identificazione per password

- Tipicamente funziona su interrogazione. All'utente (o al processo) viene chiesto il suo nome (codice identificativo) ID e poi la password ad esso relativa.
- Le password vengono memorizzate in forma cifrata in opportuni file di sistema.
- L'ID definisce l'insieme delle risorse a cui un determinato utente è autorizzato ad accedere. In particolare può essere negata ogni forma di accesso (l'utente non esiste) o gli si possono attribuire dei privilegi specifici.
- Nei sistemi linux gli utenti possono essere super-user con nessun limite di accesso o utenti ordinari (users). Gli utenti (tutti) possono far parte di gruppi.
- Gli utenti ordinari possono avere accesso solo alle risorse proprie, del proprio gruppo o accessibili a tutti.
- Nei sistemi windows esistono gli utenti, l'amministratore e le aree di condivisione che realizzano gli stessi meccanismi.

Identificazioni collettive

- Nell'ultima lezione abbiamo visto un esempio di accesso ad una rete wireless in cui si chiedeva una password collettiva ad ogni utente per consentire l'accesso alla rete.

Identificazioni collettive

- Nell'ultima lezione abbiamo visto un esempio di accesso ad una rete wireless in cui si chiedeva una password collettiva ad ogni utente per consentire l'accesso alla rete.
- Esistono vari metodi di questo genere quello usato era uno WAP (Wi-fi Protected Access), in particolare WAP2. Fa parte dello standard IEEE 802.11i già menzionato per la gestione delle reti wireless.

Identificazioni collettive

- Nell'ultima lezione abbiamo visto un esempio di accesso ad una rete wireless in cui si chiedeva una password collettiva ad ogni utente per consentire l'accesso alla rete.
- Esistono vari metodi di questo genere quello usato era uno WAP (Wi-fi Protected Access), in particolare WAP2. Fa parte dello standard IEEE 802.11i già menzionato per la gestione delle reti wireless.
- WPA2 usa uno standard di crittografia simmetrica AES Advanced Encryption Standard (una cifratura a chiave simmetrica che vedremo la prossima lezione).

Identificazioni collettive

- Nell'ultima lezione abbiamo visto un esempio di accesso ad una rete wireless in cui si chiedeva una password collettiva ad ogni utente per consentire l'accesso alla rete.
- Esistono vari metodi di questo genere quello usato era uno WAP (Wi-fi Protected Access), in particolare WAP2. Fa parte dello standard IEEE 802.11i già menzionato per la gestione delle reti wireless.
- WPA2 usa uno standard di crittografia simmetrica AES Advanced Encryption Standard (una cifratura a chiave simmetrica che vedremo la prossima lezione).
- Dal 2016 è entrato in uso il WPA3 dello standard IEEE 802.11-2016

Identificazioni collettive

- Nell'ultima lezione abbiamo visto un esempio di accesso ad una rete wireless in cui si chiedeva una password collettiva ad ogni utente per consentire l'accesso alla rete.
- Esistono vari metodi di questo genere quello usato era uno WAP (Wi-fi Protected Access), in particolare WAP2. Fa parte dello standard IEEE 802.11i già menzionato per la gestione delle reti wireless.
- WPA2 usa uno standard di crittografia simmetrica AES Advanced Encryption Standard (una cifratura a chiave simmetrica che vedremo la prossima lezione).
- Dal 2016 è entrato in uso il WPA3 dello standard IEEE 802.11-2016
- Altre reti wireless usano TKIP (Temporal Key Integrity Protocol) sempre dello standard 802.11i in cui si genera una chiave per ogni pacchetto in modo dinamico.

Identificazioni collettive

- Nell'ultima lezione abbiamo visto un esempio di accesso ad una rete wireless in cui si chiedeva una password collettiva ad ogni utente per consentire l'accesso alla rete.
- Esistono vari metodi di questo genere quello usato era uno WAP (Wi-fi Protected Access), in particolare WAP2. Fa parte dello standard IEEE 802.11i già menzionato per la gestione delle reti wireless.
- WPA2 usa uno standard di crittografia simmetrica AES Advanced Encryption Standard (una cifratura a chiave simmetrica che vedremo la prossima lezione).
- Dal 2016 è entrato in uso il WPA3 dello standard IEEE 802.11-2016
- Altre reti wireless usano TKIP (Temporal Key Integrity Protocol) sempre dello standard 802.11i in cui si genera una chiave per ogni pacchetto in modo dinamico.
- Vecchi protocolli basati su IEEE 802.11a e 802.11b usavano la cifratura WEP (Wire Equivalente Privacy), qualche vecchio router li usa ancora.

Identificazioni individuali

- Esistono gli analoghi di protocolli WPA2 e WPA3 in cui ad ogni utente viene assegnato un nome (username) e utilizzando gli stessi protocolli di cifratura simmetrica devono fornire una propria parola d'ordine (password) di uso esclusivo.

Identificazioni individuali

- Esistono gli analoghi di protocolli WPA2 e WPA3 in cui ad ogni utente viene assegnato un nome (username) e utilizzando gli stessi protocolli di cifratura simmetrica devono fornire una propria parola d'ordine (password) di uso esclusivo.
- I WPA-personal hanno il vantaggio di rendere identificabile l'utente che utilizza una connessione avendo ricevuto un nome in maniera esclusiva.

Identificazioni individuali

- Esistono gli analoghi di protocolli WPA2 e WPA3 in cui ad ogni utente viene assegnato un nome (username) e utilizzando gli stessi protocolli di cifratura simmetrica devono fornire una propria parola d'ordine (password) di uso esclusivo.
- I WPA-personal hanno il vantaggio di rendere identificabile l'utente che utilizza una connessione avendo ricevuto un nome in maniera esclusiva.
- Anche nei semplici WPA l'utente viene identificato (o meglio la sua scheda di rete wireless) tramite il MAC, ma questo può essere soggetto a spoofing.

Identificazioni individuali

- Esistono gli analoghi di protocolli WPA2 e WPA3 in cui ad ogni utente viene assegnato un nome (username) e utilizzando gli stessi protocolli di cifratura simmetrica devono fornire una propria parola d'ordine (password) di uso esclusivo.
- I WPA-personal hanno il vantaggio di rendere identificabile l'utente che utilizza una connessione avendo ricevuto un nome in maniera esclusiva.
- Anche nei semplici WPA l'utente viene identificato (o meglio la sua scheda di rete wireless) tramite il MAC, ma questo può essere soggetto a spoofing.
- Quando si effettua uno spoofing di un MAC usando un MAC di un altro dispositivo noto si dice che in dispositivo vittima è stato clonato (cloning).

Attacchi alle password

- Attacchi senza interazione con il meccanismo di sicurezza (Offline dictionary attack): se l'attaccante riesce ad ottenere il file delle password (in formato hash) può usare i meccanismi noti di hash e le password più naturali (contenute in un "dizionario") per verificare se coincidono.
  Le contromisure sono volte ad impedire la lettura del file delle password, sollecitare la scelta di password non banali e la loro frequente modifica (reissuance).

Attacchi alle password

- Attacchi senza interazione con il meccanismo di sicurezza (Offline dictionary attack): se l'attaccante riesce ad ottenere il file delle password (in formato hash) può usare i meccanismi noti di hash e le password più naturali (contenute in un "dizionario") per verificare se coincidono.
  Le contromisure sono volte ad impedire la lettura del file delle password, sollecitare la scelta di password non banali e la loro frequente modifica (reissuance).
- Attacchi contro un account (user) specifico: l'attaccante prova ad entrare sempre con lo stesso ID ma con passwd diverse.
  La contromisura tipica è il blocco dell'account dopo un numero modesto di tentativi fallitti (3 in genere e meno di 5). Di solito il blocco è temporaneo.

Attacchi alle password cont

- Attacchi basati su passwd comuni: l'attaccante prova ad entrare sempre con la stessa passwd (comune) ma con ID diversi.
  La contromisura tipica è la richiesta agli utenti di evitare passwd banali e verificare se da una stessa origine si tenta di entrare con diverse ID.

Attacchi alle password cont

- Attacchi basati su passwd comuni: l'attaccante prova ad entrare sempre con la stessa passwd (comune) ma con ID diversi.
  La contromisura tipica è la richiesta agli utenti di evitare passwd banali e verificare se da una stessa origine si tenta di entrare con diverse ID.
- Scoperta di password di un utente tramite il suo profilo umano. La contromisura consiste nell'insegnare agli utenti come crearsi passwd mnemoniche ma non riconducibili a fatti notori che li riguardano. Si impongono lunghezze minimali, la presenza di caratteri non alfabetici, maiuscole etc.

Attacchi alle password -cont

- Workstation hijacking: si usa una macchina in cui si è assentato il soggetto autorizzato.
  La contromisura istallata sulle macchine client (che chiedono l'accesso - vittime potenziali di hijacking) è il log-out dopo un periodo di inattività; mentre dalla macchina ospite si possono usare sofisticati meccanismi di analisi di comportamento che possono identificare il cambiamento dell'utente umano che usa il dispositivo remoto.

Attacchi alle password -cont

- Workstation hijacking: si usa una macchina in cui si è assentato il soggetto autorizzato.
  La contromisura istallata sulle macchine client (che chiedono l'accesso - vittime potenziali di hijacking) è il log-out dopo un periodo di inattività; mentre dalla macchina ospite si possono usare sofisticati meccanismi di analisi di comportamento che possono identificare il cambiamento dell'utente umano che usa il dispositivo remoto.
- Scopertura di copie di passwd su carta come backup della memoria dell'utente. Passwd troppo difficili si prestano a questo problema.
  Contromisura non chiedere uso di passwd impossibili da ricordare.

Attacchi alle password -cont

- Uso di passwd scoperte per un altro sistema. Contromisura non usare le stesse passwd dovunque. Diventa sempre più difficile perché la gente chiede passwd per ragioni inutili, quindi (vedremo oltre) si aggiunge una spolverata di pepe.

Attacchi alle password -cont

- Uso di passwd scoperte per un altro sistema. Contromisura non usare le stesse passwd dovunque. Diventa sempre più difficile perché la gente chiede passwd per ragioni inutili, quindi (vedremo oltre) si aggiunge una spolverata di pepe.
- Origliamento eavesdropping: si osserva un canale di comunicazione e si scoprono i caratteri inviati per l'autenticazione. La criptazione della passwd impedisce all'origliatore di conoscerla, ma non di acquisire l'accesso in nostra vece (attacco reply).
  Contromisure: evitare questi origliamenti e rendere difficile distinguere i pacchetti dove si chiede la passwd. Oppure realizzare autenticazioni a tempo definito.

Aggiungiamo un pizzico di sale alle passwd

- Per rendere più difficili gli attacchi con dizionario si aggiunge il sale alla passwd: cioè si genera una sequenza random (o pseudo-tale) e si calcola l'o esclusivo con la passwd, solo dopo si calcola l'hash function.

Aggiungiamo un pizzico di sale alle passwd

- Per rendere più difficili gli attacchi con dizionario si aggiunge il sale alla passwd: cioè si genera una sequenza random (o pseudo-tale) e si calcola l'o esclusivo con la passwd, solo dopo si calcola l'hash function.
- I vantaggi di questa tecnica sono diversi:

Aggiungiamo un pizzico di sale alle passwd

- Per rendere più difficili gli attacchi con dizionario si aggiunge il sale alla passwd: cioè si genera una sequenza random (o pseudo-tale) e si calcola l'o esclusivo con la passwd, solo dopo si calcola l'hash function.
- I vantaggi di questa tecnica sono diversi:
  - Se le passwd di due utenti sono uguali appaiono comunque diverse

Aggiungiamo un pizzico di sale alle passwd

- Per rendere più difficili gli attacchi con dizionario si aggiunge il sale alla passwd: cioè si genera una sequenza random (o pseudo-tale) e si calcola l'o esclusivo con la passwd, solo dopo si calcola l'hash function.
- I vantaggi di questa tecnica sono diversi:
  - Se le passwd di due utenti sono uguali appaiono comunque diverse
  - Si rende più complesso l'attacco a dizionario perché bisogna ispezionare anche il possibile sale.

Aggiungiamo un pizzico di sale alle passwd

- Per rendere più difficili gli attacchi con dizionario si aggiunge il sale alla passwd: cioè si genera una sequenza random (o pseudo-tale) e si calcola l'o esclusivo con la passwd, solo dopo si calcola l'hash function.
- I vantaggi di questa tecnica sono diversi:
  - Se le passwd di due utenti sono uguali appaiono comunque diverse
  - Si rende più complesso l'attacco a dizionario perché bisogna ispezionare anche il possibile sale.
- Per rendere più difficile l'acquisizione del file con le hash delle passwd questo è collocato in un aree di memoria riservata al super-user (administrator). Si parla di file ombra (shadow password file)

Aggiungiamo un pizzico di pepe

- Oltre al sale, prima di calcolare la hash function delle password si include anche il pepe: un ulteriore sequenza random, questa volta caratteristica della piattaforma ospite e uguale per tutti gli utenti.

Aggiungiamo un pizzico di pepe

- Oltre al sale, prima di calcolare la hash function delle password si include anche il pepe: un ulteriore sequenza random, questa volta caratteristica della piattaforma ospite e uguale per tutti gli utenti.
- Questo consente di usare la stessa password su piattaforme diverse, ottenendo digest diversi nei file ombra (shadow file). Chi violasse una piattaforma ottenendo la sequenza relativa ad un utente, non potrebbe comunque usarla in un altra piattaforma.

Aggiungiamo un pizzico di pepe

- Oltre al sale, prima di calcolare la hash function delle password si include anche il pepe: un ulteriore sequenza random, questa volta caratteristica della piattaforma ospite e uguale per tutti gli utenti.
- Questo consente di usare la stessa password su piattaforme diverse, ottenendo digest diversi nei file ombra (shadow file). Chi violasse una piattaforma ottenendo la sequenza relativa ad un utente, non potrebbe comunque usarla in un altra piattaforma.
- Riassumendo:

Aggiungiamo un pizzico di pepe

- Oltre al sale, prima di calcolare la hash function delle password si include anche il pepe: un ulteriore sequenza random, questa volta caratteristica della piattaforma ospite e uguale per tutti gli utenti.
- Questo consente di usare la stessa password su piattaforme diverse, ottenendo digest diversi nei file ombra (shadow file). Chi violasse una piattaforma ottenendo la sequenza relativa ad un utente, non potrebbe comunque usarla in un altra piattaforma.
- Riassumendo:
  - Il server invia la sequenza risultante da sale e pepe al client

Aggiungiamo un pizzico di pepe

- Oltre al sale, prima di calcolare la hash function delle password si include anche il pepe: un ulteriore sequenza random, questa volta caratteristica della piattaforma ospite e uguale per tutti gli utenti.
- Questo consente di usare la stessa password su piattaforme diverse, ottenendo digest diversi nei file ombra (shadow file). Chi violasse una piattaforma ottenendo la sequenza relativa ad un utente, non potrebbe comunque usarla in un altra piattaforma.
- Riassumendo:
  - Il server invia la sequenza risultante da sale e pepe al client
  - Il client appone sale e pepe alla passwd utente, calcola la hash function e la invia al server

Aggiungiamo un pizzico di pepe

- Oltre al sale, prima di calcolare la hash function delle password si include anche il pepe: un ulteriore sequenza random, questa volta caratteristica della piattaforma ospite e uguale per tutti gli utenti.
- Questo consente di usare la stessa password su piattaforme diverse, ottenendo digest diversi nei file ombra (shadow file). Chi violasse una piattaforma ottenendo la sequenza relativa ad un utente, non potrebbe comunque usarla in un altra piattaforma.
- Riassumendo:
  - Il server invia la sequenza risultante da sale e pepe al client
  - Il client appone sale e pepe alla passwd utente, calcola la hash function e la invia al server
  - Il server verifica che sia uguale alla sequenza nel file ombra.

Aggiungiamo un pizzico di pepe

- Oltre al sale, prima di calcolare la hash function delle password si include anche il pepe: un ulteriore sequenza random, questa volta caratteristica della piattaforma ospite e uguale per tutti gli utenti.
- Questo consente di usare la stessa password su piattaforme diverse, ottenendo digest diversi nei file ombra (shadow file). Chi violasse una piattaforma ottenendo la sequenza relativa ad un utente, non potrebbe comunque usarla in un altra piattaforma.
- Riassumendo:
  - Il server invia la sequenza risultante da sale e pepe al client
  - Il client appone sale e pepe alla passwd utente, calcola la hash function e la invia al server
  - Il server verifica che sia uguale alla sequenza nel file ombra.
- Si noti che nemmeno l'amministratore può conoscere la passwd. Può cambiarla (e rimane traccia nei registri), ma non conoscerla.

Strumenti di difesa

- Educazione degli utenti

Strumenti di difesa

- Educazione degli utenti
- Vincoli sulle passwd. Vincolo di lunghezza (più di 8 byte); sulla varietà dei caratteri.

Strumenti di difesa

- Educazione degli utenti
- Vincoli sulle passwd. Vincolo di lunghezza (più di 8 byte); sulla varietà dei caratteri.
- Generazione di passwd robuste da parte del sistema.

Strumenti di difesa

- Educazione degli utenti
- Vincoli sulle passwd. Vincolo di lunghezza (più di 8 byte); sulla varietà dei caratteri.
- Generazione di passwd robuste da parte del sistema.
- Controllo reattivo (reactive control): se la passwd è debole si chiede di cambiarla. Ci si finge hacker di se stessi, le passwd scoperte vengono cambiate. (molto costoso)

Strumenti di difesa

- Educazione degli utenti
- Vincoli sulle passwd. Vincolo di lunghezza (più di 8 byte); sulla varietà dei caratteri.
- Generazione di passwd robuste da parte del sistema.
- Controllo reattivo (reactive control): se la passwd è debole si chiede di cambiarla. Ci si finge hacker di se stessi, le passwd scoperte vengono cambiate. (molto costoso)
- Controllo preventivo (proactive control) si usano sistemi esperti per giungere a passwd che siano sia mnemoniche che robuste.

Buone pratiche per le passwd

- Indipendentemente dall'uso di un sistema esperto o di una lista di raccomandazioni le regole di buon senso

Buone pratiche per le passwd

- Indipendentemente dall'uso di un sistema esperto o di una lista di raccomandazioni le regole di buon senso
  - Lunghezza minima 8 caratteri.

Buone pratiche per le passwd

- Indipendentemente dall'uso di un sistema esperto o di una lista di raccomandazioni le regole di buon senso
  - Lunghezza minima 8 caratteri.
  - Obbligo dell'inclusione di almeno: una maiuscola, una minuscola, un numero, un segno di interpunzione, un carattere dei rimanenti.

Buone pratiche per le passwd

- Indipendentemente dall'uso di un sistema esperto o di una lista di raccomandazioni le regole di buon senso
  - Lunghezza minima 8 caratteri.
  - Obbligo dell'inclusione di almeno: una maiuscola, una minuscola, un numero, un segno di interpunzione, un carattere dei rimanenti.
- Aggiungo: non usare parole comuni con 5, 3, 1 e 0 al posto di s,e, i ed o. Oppure @ al posto di at; & al posto di e, @ al posto di a, etc
  Non è difficile associare 5u0n@r3 a suonare.

Il filtro di Bloom

- Dato un grande dizionario (di passwd inadatte) di dimensione D: $\mathcal{D} = \{X_1, X_2, \ldots, X_D\}$ ed un insieme di K hash function $H_1, H_2, \ldots, H_k$ a valori da zero ad $N - 1$, si costruisce la tabella di hash (una sequenza di N valori). L'elemento m-esimo della tabella assume valore unitario solo se esiste una hash function di un elemento del dizionario che è uguale all'indice della tabella:

$$\mathcal{T}(m) = 1 \Leftrightarrow \exists i, j : H_i(X_j) = m. \tag{1}$$

Il filtro di Bloom

- Dato un grande dizionario (di passwd inadatte) di dimensione D: $\mathcal{D} = \{X_1, X_2, \ldots, X_D\}$ ed un insieme di K hash function $H_1, H_2, \ldots, H_k$ a valori da zero ad $N - 1$, si costruisce la tabella di hash (una sequenza di N valori). L'elemento m-esimo della tabella assume valore unitario solo se esiste una hash function di un elemento del dizionario che è uguale all'indice della tabella:

$$\mathcal{T}(m) = 1 \Leftrightarrow \exists i, j : H_i(X_j) = m. \tag{1}$$

- Il filtro di Bloom ha esito positivo (reiezione cioè scarto della passwd) su una passwd X se tutte le sue hash function hanno valore unitario nella tabella.

$$\forall i : \mathcal{T}(H_i(X)) = 1. \tag{2}$$

Il filtro di Bloom

- Il filtro ha un buon potere di reiezione: (immagine presa dal William Stalling):

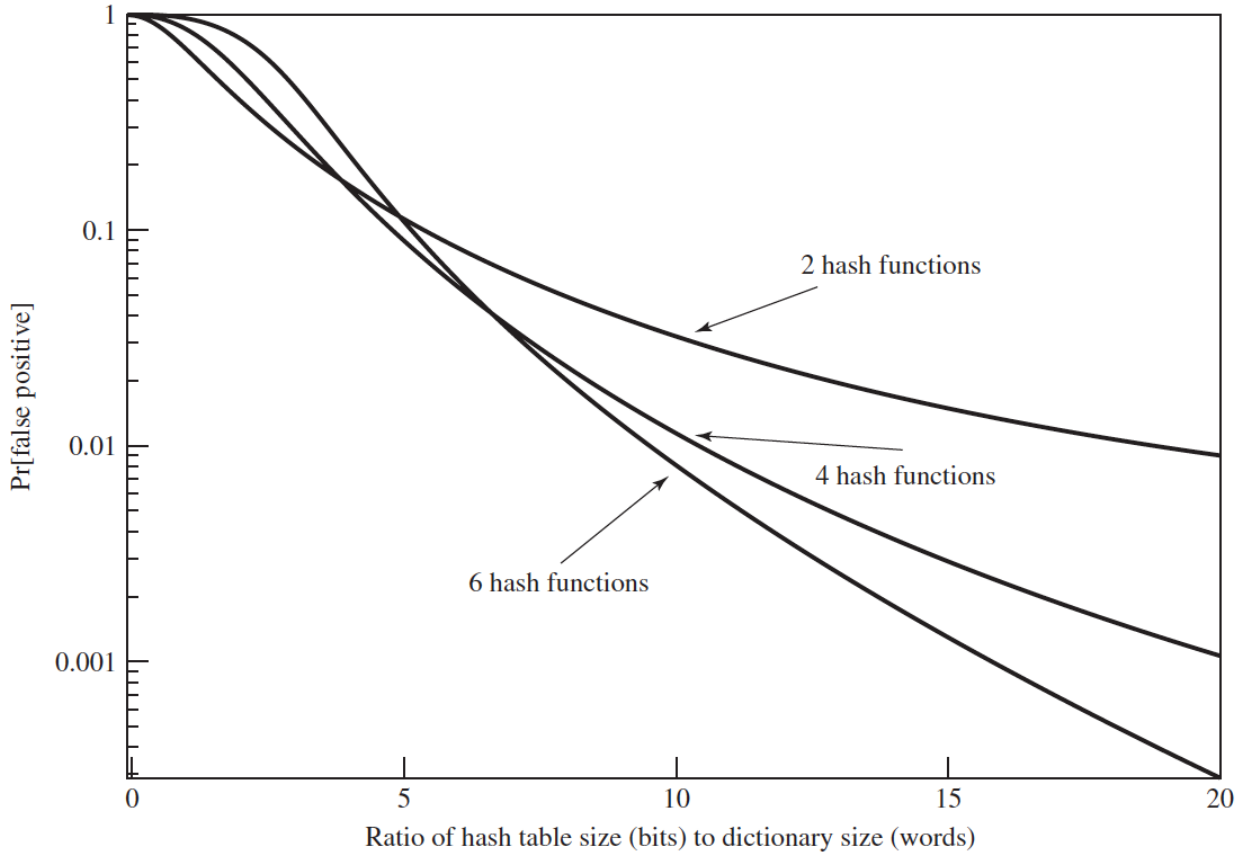

Figure 3.2 **Performance of Bloom Filter**

- L'ascissa è N/D il rapporto tra la dimensione della tabella e quella del dizionario (di passwd inadatte).

Schede Memory Cards

- Una memory card possiede una unità di memoria di sola lettura. Tipicamente un cip o una banda magnetica o entrambe.

Schede Memory Cards

- Una memory card possiede una unità di memoria di sola lettura. Tipicamente un cip o una banda magnetica o entrambe.
- Le più comuni sono i bancomat e le carte di credito.

Schede Memory Cards

- Una memory card possiede una unità di memoria di sola lettura. Tipicamente un cip o una banda magnetica o entrambe.
- Le più comuni sono i bancomat e le carte di credito.
- Anche al tessera sanitaria è una memory card.

Caratteristiche delle Schede

- Alle schede sono associati i PIN. Per leggerle occorrono delle macchine apposite dette ATM (Automatic Teller Machine).

Caratteristiche delle Schede

- Alle schede sono associati i PIN. Per leggerle occorrono delle macchine apposite dette ATM (Automatic Teller Machine).
- In caso di perdita si crea un periodo in cui non si può utilizzare il sistemae vi è un costo non banale per la sostituzione.

Caratteristiche delle Schede

- Alle schede sono associati i PIN. Per leggerle occorrono delle macchine apposite dette ATM (Automatic Teller Machine).
- In caso di perdita si crea un periodo in cui non si può utilizzare il sistemae vi è un costo non banale per la sostituzione.
- Non sembra essere gradito agli utenti dei computer.

Smart Cards

- Sono dispositivi miniaturizzati dotati di (modeste) capacità di elaborazione. Hanno forme variabili come carte o chiavette.

Smart Cards

- Sono dispositivi miniaturizzati dotati di (modeste) capacità di elaborazione. Hanno forme variabili come carte o chiavette.
- Sono dotati di uno schermo (display) e dispositivi per l'interazione umana (tastiere) dette HI (Human Interface).

Smart Cards

- Sono dispositivi miniaturizzati dotati di (modeste) capacità di elaborazione. Hanno forme variabili come carte o chiavette.
- Sono dotati di uno schermo (display) e dispositivi per l'interazione umana (tastiere) dette HI (Human Interface).
- L'autenticazione avviene in cascata con tre modalità diverse

Smart Cards

- Sono dispositivi miniaturizzati dotati di (modeste) capacità di elaborazione. Hanno forme variabili come carte o chiavette.
- Sono dotati di uno schermo (display) e dispositivi per l'interazione umana (tastiere) dette HI (Human Interface).
- L'autenticazione avviene in cascata con tre modalità diverse
  - : Statica: l'essere umano interagisce in modo appropriato e il dispositivo dialoga col soggetto autenticante.

Smart Cards

- Sono dispositivi miniaturizzati dotati di (modeste) capacità di elaborazione. Hanno forme variabili come carte o chiavette.
- Sono dotati di uno schermo (display) e dispositivi per l'interazione umana (tastiere) dette HI (Human Interface).
- L'autenticazione avviene in cascata con tre modalità diverse
  - : Statica: l'essere umano interagisce in modo appropriato e il dispositivo dialoga col soggetto autenticante.
  - : Generazione dinamica di password: il dispositivo genera una passwd che l'essere umano passa al soggetto autenticante.

Smart Cards

- Sono dispositivi miniaturizzati dotati di (modeste) capacità di elaborazione. Hanno forme variabili come carte o chiavette.
- Sono dotati di uno schermo (display) e dispositivi per l'interazione umana (tastiere) dette HI (Human Interface).
- L'autenticazione avviene in cascata con tre modalità diverse
  - : Statica: l'essere umano interagisce in modo appropriato e il dispositivo dialoga col soggetto autenticante.
  - : Generazione dinamica di password: il dispositivo genera una passwd che l'essere umano passa al soggetto autenticante.
  - : Domanda risposta: il soggetto autenticante pone una questione (una stringa) ed il dispositivo risponde (fornisce un'altra stringa).

Specificità dei token

- Le smart card si usano spesso per evitare l'uso da parte di molti utenti di una risorsa autorizzata per uno solo. Ad esempio l'accesso ad un'area o la possibilità di eseguire un codice su una piattaforma.

Specificità dei token

- Le smart card si usano spesso per evitare l'uso da parte di molti utenti di una risorsa autorizzata per uno solo. Ad esempio l'accesso ad un'area o la possibilità di eseguire un codice su una piattaforma.
- Quando un dispositivo di identificazione fisico viene duplicato integralmente si parla di clonazione.

Specificità dei token

- Le smart card si usano spesso per evitare l'uso da parte di molti utenti di una risorsa autorizzata per uno solo. Ad esempio l'accesso ad un'area o la possibilità di eseguire un codice su una piattaforma.
- Quando un dispositivo di identificazione fisico viene duplicato integralmente si parla di clonazione.
- La clonazione può servire ad impersonare un'altra persona ed usarne i privilegi (e.g. transazioni bancarie) o aumentare l'uso delle risorse oltre i limiti autorizzati (autoclonazione).

Specificità dei token

- Le smart card si usano spesso per evitare l'uso da parte di molti utenti di una risorsa autorizzata per uno solo. Ad esempio l'accesso ad un'area o la possibilità di eseguire un codice su una piattaforma.
- Quando un dispositivo di identificazione fisico viene duplicato integralmente si parla di clonazione.
- La clonazione può servire ad impersonare un'altra persona ed usarne i privilegi (e.g. transazioni bancarie) o aumentare l'uso delle risorse oltre i limiti autorizzati (autoclonazione).
- Da quest'anno molte banche stanno ritirando i vecchi token per sostituirli con app che girano sui sistemi operativi dei telefoni cellulari come Android o Iphone.

Tipi di attacchi

- Tabella dei principali attacchi (immagine presa dal William Stalling)

Table 3.4 Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

Attacks	Authenticators	Examples	Typical Defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts, theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication

Tipi di attacchi -cont

- Tabella dei principali attacchi (immagine presa dal William Stalling)

Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of service	Password, token, biometric	Lockout by multiple failed authentications	Multifactor with token

Umano o non umano? Test di Touring.

- Uno degli strumenti utili per evitare le attività moleste dei BOT (programmi che simulano comportamenti umani) è presentare dei test che presumibilmente solo gli esseri umani sono in grado di risolvere.

Umano o non umano? Test di Touring.

- Uno degli strumenti utili per evitare le attività moleste dei BOT (programmi che simulano comportamenti umani) è presentare dei test che presumibilmente solo gli esseri umani sono in grado di risolvere.
- L'esempio classico è la ricognizione di una sequenza di lettere e/o numeri in un riquadro posto in locazione remota e con una immagine molto rumorosa, oppure un personaggio famoso.

Umano o non umano? Test di Touring.

- Uno degli strumenti utili per evitare le attività moleste dei BOT (programmi che simulano comportamenti umani) è presentare dei test che presumibilmente solo gli esseri umani sono in grado di risolvere.
- L'esempio classico è la ricognizione di una sequenza di lettere e/o numeri in un riquadro posto in locazione remota e con una immagine molto rumorosa, oppure un personaggio famoso.
- I test CAPTCHA ("completely automated public Turing test to tell computers and humans apart"), consentono di impedire accessi automatizzati e sistematici ai siti ed anche a contrastare gli attacchi DDOS selezionando richieste genuine ai server.

Umano o non umano? Test di Touring.

- Uno degli strumenti utili per evitare le attività moleste dei BOT (programmi che simulano comportamenti umani) è presentare dei test che presumibilmente solo gli esseri umani sono in grado di risolvere.
- L'esempio classico è la ricognizione di una sequenza di lettere e/o numeri in un riquadro posto in locazione remota e con una immagine molto rumorosa, oppure un personaggio famoso.
- I test CAPTCHA ("completely automated public Turing test to tell computers and humans apart"), consentono di impedire accessi automatizzati e sistematici ai siti ed anche a contrastare gli attacchi DDOS selezionando richieste genuine ai server.
- Un modo astuto per superare i test CAPTCHA consiste nel riproporli in rete ad un utente umano, allettato opportunamente promettendogli qualcosa se supera il test (es strip poker): l'azione dell'utente umano viene replicata identicamente dal bot sul sito cui intende accedere.

Autenticazione Multipla

- Il Furto delle credenziali è divenuto uno di reati informatici più diffusi. Per renderlo più difficile si in molte occasione si ricorre ad autenticazione multipla: i metodi di autenticazione vengono combinati per aumentare la sicurezza (ma diminuire la facilità di accesso).

Autenticazione Multipla

- Il Furto delle credenziali è divenuto uno di reati informatici più diffusi. Per renderlo più difficile si in molte occasione si ricorre ad autenticazione multipla: i metodi di autenticazione vengono combinati per aumentare la sicurezza (ma diminuire la facilità di accesso).
- Ad esempio nel portale della sanità laziale si chiede prima una autenticazione tramite credenziali (username e password, cioè nome di battaglia e parola d'ordine) e pi si richiede un codice di controllo che viene inviato al telefono cellulare.

Autenticazione Multipla

- Il Furto delle credenziali è divenuto uno di reati informatici più diffusi. Per renderlo più difficile si in molte occasione si ricorre ad autenticazione multipla: i metodi di autenticazione vengono combinati per aumentare la sicurezza (ma diminuire la facilità di accesso).
- Ad esempio nel portale della sanità laziale si chiede prima una autenticazione tramite credenziali (username e password, cioè nome di battaglia e parola d'ordine) e pi si richiede un codice di controllo che viene inviato al telefono cellulare.
- L'accesso è reso più difficile perché richiede il funzionamento sia della rete che della telefonia mobile e la disponibilità di un dispositivo di accesso in rete e del telefono cellulare.

Strong Autentication

- Nel linguaggio bancario la strong customer autentication (SCA) è semplicemente una autenticazione doppia tramite una password statica (o un pin) ed una OTP (One Time Password che vedremo) generata da un dispositivo dell'utente.

Strong Autentication

- Nel linguaggio bancario la strong customer autentication (SCA) è semplicemente una autenticazione doppia tramite una password statica (o un pin) ed una OTP (One Time Password che vedremo) generata da un dispositivo dell'utente.
- Recentemente le banche hanno sostituito al dispositivo autonomo per la generazione delle OTP, specifiche app: piccoli software aggiuntivi per i telefoni mobili.

Strong Autentication

- Nel linguaggio bancario la strong customer autentication (SCA) è semplicemente una autenticazione doppia tramite una password statica (o un pin) ed una OTP (One Time Password che vedremo) generata da un dispositivo dell'utente.
- Recentemente le banche hanno sostituito al dispositivo autonomo per la generazione delle OTP, specifiche app: piccoli software aggiuntivi per i telefoni mobili.
- Il riferimento legale per le regole di pagamenteo in europa è la PSD2 (Payment Service Directive 2) DIRETTIVA (UE) 2015/2366 del 25 nov 2015 ha disciplinato l'autenticazione degli utenti per le transazioni bancarie, introducendo l'autenticazione doppia.

Strong Autentication

- Nel linguaggio bancario la strong customer autentication (SCA) è semplicemente una autenticazione doppia tramite una password statica (o un pin) ed una OTP (One Time Password che vedremo) generata da un dispositivo dell'utente.
- Recentemente le banche hanno sostituito al dispositivo autonomo per la generazione delle OTP, specifiche app: piccoli software aggiuntivi per i telefoni mobili.
- Il riferimento legale per le regole di pagamenteo in europa è la PSD2 (Payment Service Directive 2) DIRETTIVA (UE) 2015/2366 del 25 nov 2015 ha disciplinato l'autenticazione degli utenti per le transazioni bancarie, introducendo l'autenticazione doppia.
- La legge italiana, che ha recepito la direttiva e dal primo gennaio 2021 e l'autenticazione SCA è divenuta obbligatoria, ma potrà ancora essere realizzata senza il telefono mobile.

Dispositivo autonomo vs APP

- Le banche preferiscono dissuadere i clienti ad utilizzare il vecchi dispositivi a favore del cellulare imponendo un canone aggiuntivo. Si pensa che la consapevolezza dell'eventuale smarrimento del cellulare avvenga più facilmente e prontamente di quella del dispositivo autonomo

Dispositivo autonomo vs APP

- Le banche preferiscono dissuadere i clienti ad utilizzare il vecchi dispositivi a favore del cellulare imponendo un canone aggiuntivo. Si pensa che la consapevolezza dell'eventuale smarrimento del cellulare avvenga più facilmente e prontamente di quella del dispositivo autonomo
- L'uso obbligatorio del cellulare crea comunque una vulnerabilità aggiuntiva perché sullo stesso dispositivo sono contenute entrambe le informazioni per l'accesso. Infatti le banche forniscono anche un'altra app che consente l'accesso e contiene il pin in memoria.

Messaggio

- l'accesso alle risorse o ai dati dei sistemi informatici, sia in modalità remota che locale è spesso vincolato a procedure di autenticazione.

Messaggio

- l'accesso alle risorse o ai dati dei sistemi informatici, sia in modalità remota che locale è spesso vincolato a procedure di autenticazione.
- L'autenticazione mira ad identificare un utente per consentigli l'accesso alle risorse specifiche cui è autorizzato.

Messaggio

- l'accesso alle risorse o ai dati dei sistemi informatici, sia in modalità remota che locale è spesso vincolato a procedure di autenticazione.
- L'autenticazione mira ad identificare un utente per consentigli l'accesso alle risorse specifiche cui è autorizzato.
- Il processo di autenticazione si basa su requisiti di tipo antropologico, possesso di dispositivi esclusivi o conoscenza di informazioni riservate individuali (credenziali). Ognuno di questi requisiti è oggetto di specifici attacchi a cui corrispondono contromisure adeguate.

Messaggio

- l'accesso alle risorse o ai dati dei sistemi informatici, sia in modalità remota che locale è spesso vincolato a procedure di autenticazione.
- L'autenticazione mira ad identificare un utente per consentigli l'accesso alle risorse specifiche cui è autorizzato.
- Il processo di autenticazione si basa su requisiti di tipo antropologico, possesso di dispositivi esclusivi o conoscenza di informazioni riservate individuali (credenziali). Ognuno di questi requisiti è oggetto di specifici attacchi a cui corrispondono contromisure adeguate.
- Quando si aumenta la robustezza delle credenziali si diminuisce la facilità di accesso.