Furto Identità Digitale

Alcune tecniche di attacco

Giuseppe Augiero

Agenda

- Identità digitale
- Tecniche di furto

25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

Digital Identity

- “Identità” è definita come l’insieme dei caratteri peculiari, il complesso delle generalità, l’insieme delle caratteristiche fisiche e dati anagrafici che contraddistinguono un individuo.
- Un’identità digitale contiene dati che descrivono in modo univoco una persona o una cosa (soggetto o entità), ma anche informazioni sulle relazioni esistenti tra il soggetto ed altre entità.

Attributi

- Una identità digitale e' articolata in due parti:
  - Chi uno è (identità).
  - Le credenziali che ognuno possiede (attributi).
- Le credenziali possono essere molto variegate sia dal punto di vista numerico che qualitativo.

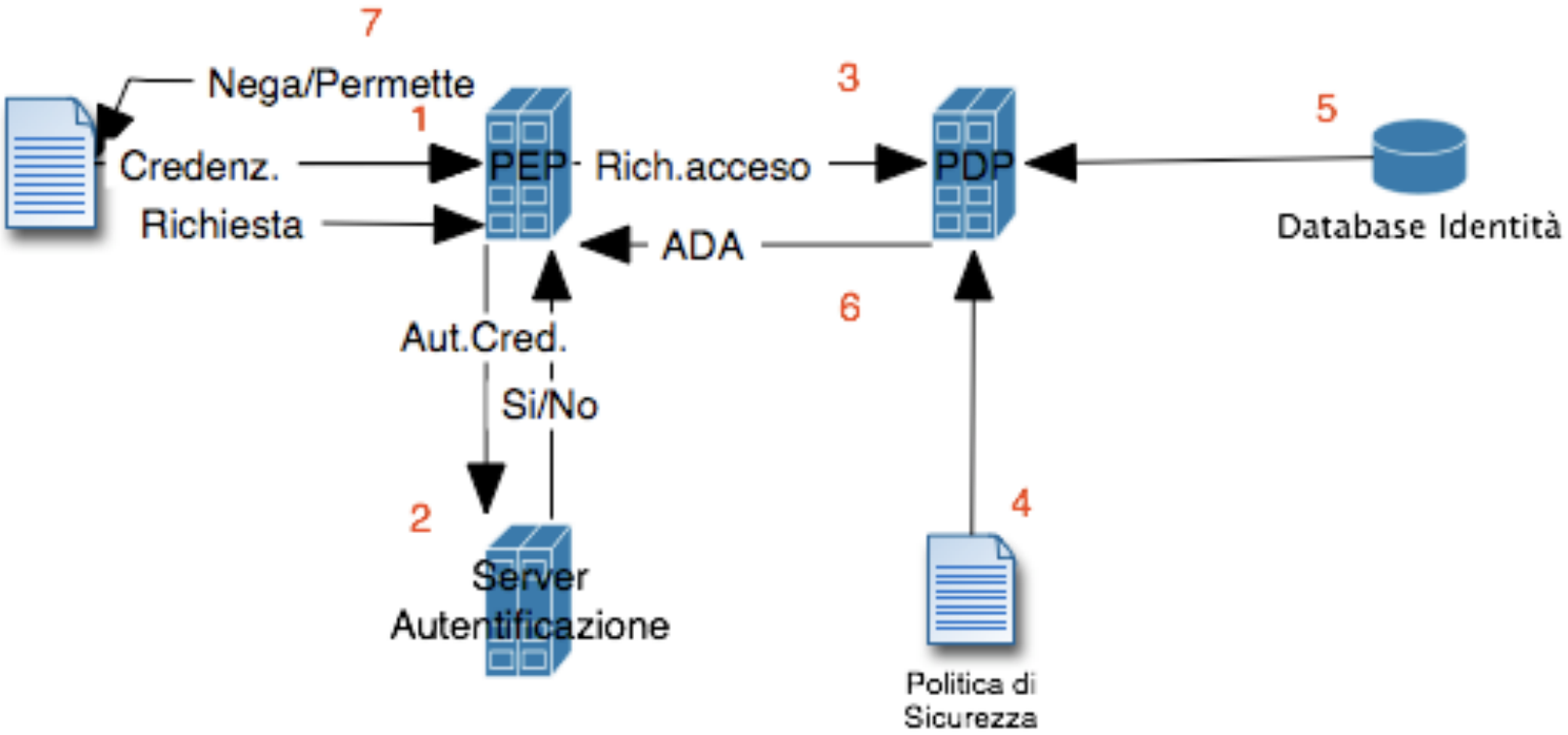
Identità semplice

- L'identità digitale più semplice consiste in uno **username** e una **password** (segreta).
- Lo username è l'identità mentre la password è chiamata credenziale di autenticazione.
- L'identità può essere più complessa come una vera e propria identità umana.

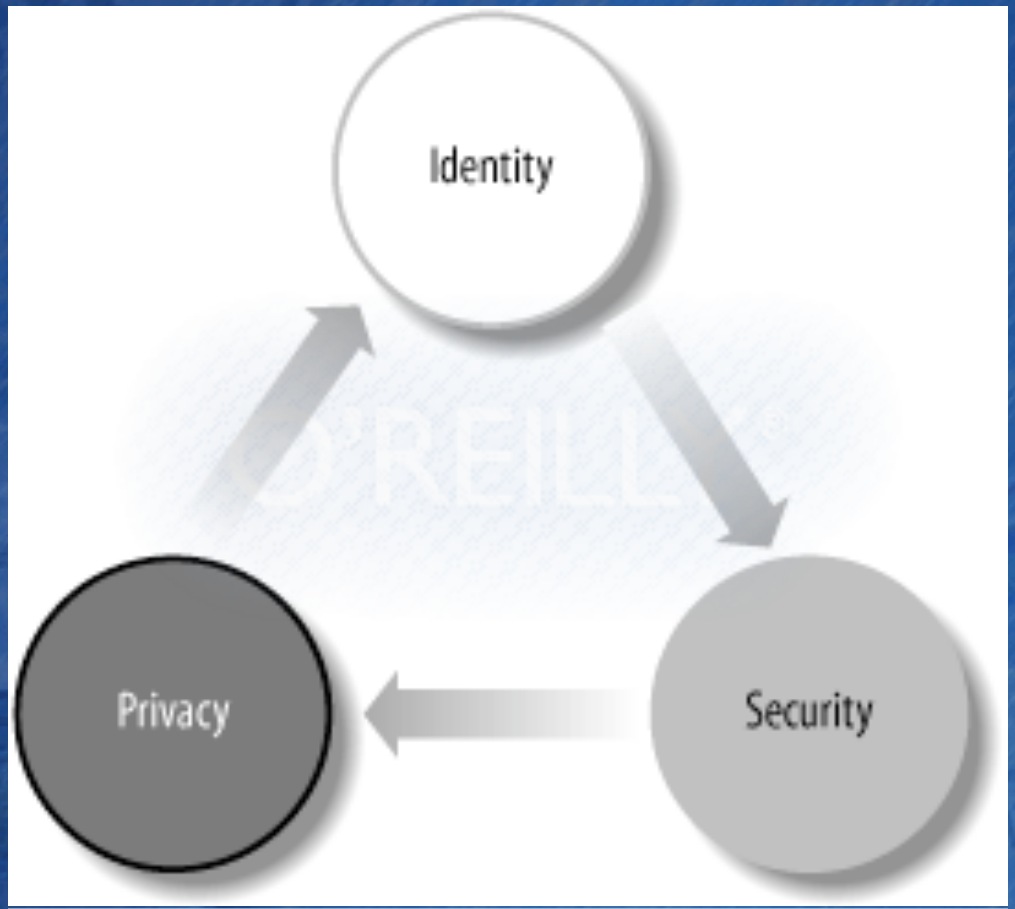
Il linguaggio

- Il mondo dell'identità digitale utilizza un proprio gergo:
  - **Soggetto o entità:** persona, organizzazione o software che vuole richiedere accesso a una risorsa:
  - **Risorsa:** e' rappresentata da una pagina web, una informazione, una transazione bancaria.
  - **Identità:** collezione di dati su un soggetto, rappresenta attributi,preferenze o tratti.
  - **Attributi:** rappresentano le informazioni su un soggetto.

Interazione Pep e Pdp



Identità, sicurezza e privacy



25 ottobre - Linux Day 2008 – Giuseppe Augiero – giuseppe@augiero.it

Insicurezza...

Social Engineering

- Con il termine social enginering si intende una particolare tecnica psicologica che sfrutta l'inesperienza e la buona fede degli utenti per carpire informazioni utili a portare a termine successivi attacchi tecnologi ai sistemi.
- E' una delle tecniche di attacco potenzialmente più dannose per la vittima.
- L'attacco e' di solito condotto mediante una impersonificazione.

Phishing

- E’ una forma particolare di social engineering.
- Consiste nella creazione e nell’uso di email e siti web ideati per apparire come email e siti web istituzionali, con lo scopo di raggirare gli utenti Internet di tali enti e carpire loro informazioni personali riguardanti il proprio account (password, numero di carta di credito).
- I phishers utilizzeranno successivamente tali informazioni per scopi criminali (frodi o furti d’identità).

Malicious code

- Questo termine indica la famiglia di software che ha come obiettivo il danneggiamento, totale o parziale, o l'alterazione del funzionamento di un sistema informatico.
- Alcune forme di codice malevolo sono in grado di esportare i dati o di prendere il controllo del sistema.
- Esistono 4 classi di codice malevolo: Spyware, Keylogging, Redirector, Screen Grabbing.

Spoofing

- Lo spoofing non rappresenta un attacco nel senso stretto del termine, ma una tecnica complementare a vari tipi di attacco.
- Consiste nel falsificare l'origine della connessione in modo tale da far credere di essere un soggetto o sistema diverso da quello reale.
- User Account spoofing, Dns Spoofing, Ip address Spoofing.

Man in the middle

- E’ un attacco che consiste nel dirottare il traffico generato durante la comunicazione tra due host connessi alla stessa rete verso un terzo host.
- Durante l’attacco il terzo host si frappone alla comunicazione tra i due end-point e intercetta il flusso di dati che si scambiano riuscendo a far credere loro di essere il rispettivo legittimo interlocutore.

Sniffing

- Consiste in un'operazione di intercettazione passiva delle comunicazioni per la cattura dei dati.
- E' possibile intercettare informazioni di varia natura (password, messaggi, transazioni).
- Spesso questa attività è realizzata attraverso l'utilizzo di strumenti informatici denominati sniffer.

Password Cracking

- Il password cracking viene realizzato attraverso software che effettuano a ripetizione tentativi di accesso ad aree riservate, provando ad accedere con password generate secondo algoritmi interni predefiniti.
- Utilizzo di Dizionari.

Domande?

Risposte!

- Giuseppe Augiero giuseppe@augiero.it

Grazie per l'attenzione

- Queste trasparenze *(slide)* sono protette dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo e il copyright delle *slide* (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica, testo, tabella, disegno) sono di proprietà dell'autore.
- Le *slide* possono essere riprodotte e utilizzate liberamente dagli istituti di ricerca, scolastici e universitari italiani afferenti al Ministero dell'Istruzione, dell'Università e della Ricerca per scopi istituzionali e comunque non a fini di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altro utilizzo o riproduzione, completa o parziale (ivi incluse, ma non limitatamente, le riproduzioni su supporti ottici e magnetici, su reti di calcolatori e a stampa), sono vietati se non preventivamente autorizzati per iscritto dall'autore.
- L'informazione contenuta in queste *slide* è ritenuta essere accurata alla data riportata nel frontespizio. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, etc. In ogni caso essa è soggetta a cambiamenti senza preavviso. L'autore non assume alcuna responsabilità per il contenuto delle *slide* (ivi incluse, ma non limitatamente, la correttezza, la completezza, l'applicabilità, l'adeguatezza per uno scopo specifico e l'aggiornamento dell'informazione).
- In nessun caso possono essere rilasciate dichiarazioni di conformità all'informazione contenuta in queste *slide*.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata fedelmente e integralmente anche per utilizzi parziali.