Le problematiche di Web Application Security: la visione di ABI Lab

Matteo Lucchetti

Senior Research Analyst
ABI Lab

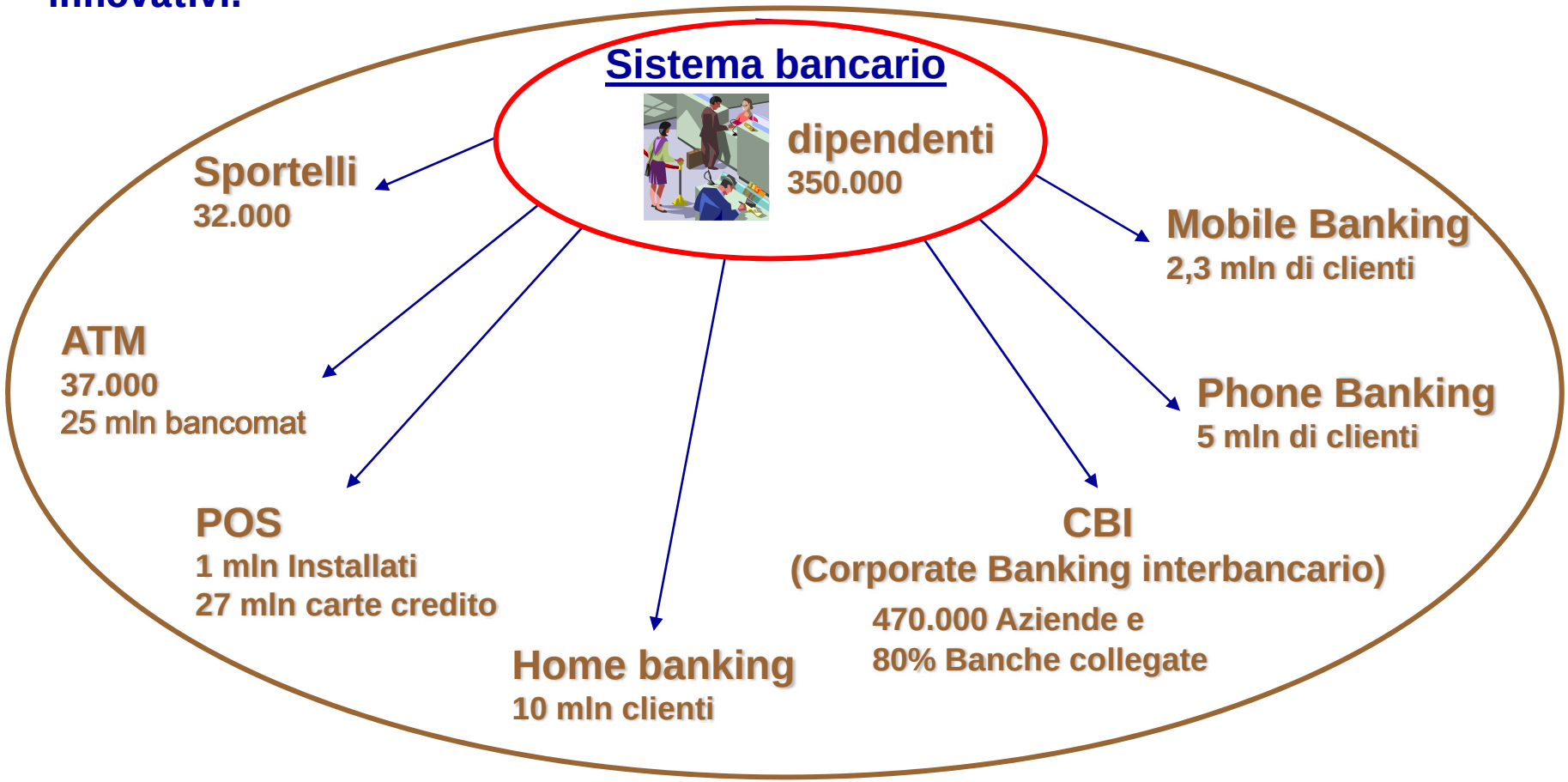
OWASP-Day II
Università “La Sapienza”, Roma
31st, March 2008

Agenda

- **Il sistema bancario e gli attacchi alle informazioni**
- Attacchi e vulnerabilità delle applicazioni
- Azioni di risposta delle banche
- La sicurezza applicativa: da best practice a norma

Banca e clienti: la tecnologia per rafforzare la relazione con la clientela

L'evoluzione delle modalità di comunicazione tra banca e cliente ha consolidato negli ultimi anni lo sviluppo di canali diversificati per l'offerta di servizi innovativi.



I canali e le tecnologie di gestione degli accessi

L'aumento dei canali per l'erogazione dei servizi richiede una particolare attenzione all'individuazione delle **soluzioni tecnologiche e organizzative per la gestione degli accessi e la tutela dell'identità dell'utente**. I sistemi di identificazione, autenticazione e autorizzazione **differiscono in funzione del canale utilizzato**.

CANALI

- Filiale / Dipend.
- Web
- Mobile
- Intranet
- Phone
- ATM
- POS

IDENTIFICAZIONE

Insieme di dati attribuiti in modo esclusivo e univoco ad un soggetto che ne distinguono l'identità.

- User ID e password
- Smart Card
- SIM card
- Token
- Sistemi biometrici
- Badge
- Sensori di prossimità
- Documento d'identità

AUTENTICAZIONE

Validazione dell'identificazione effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso.

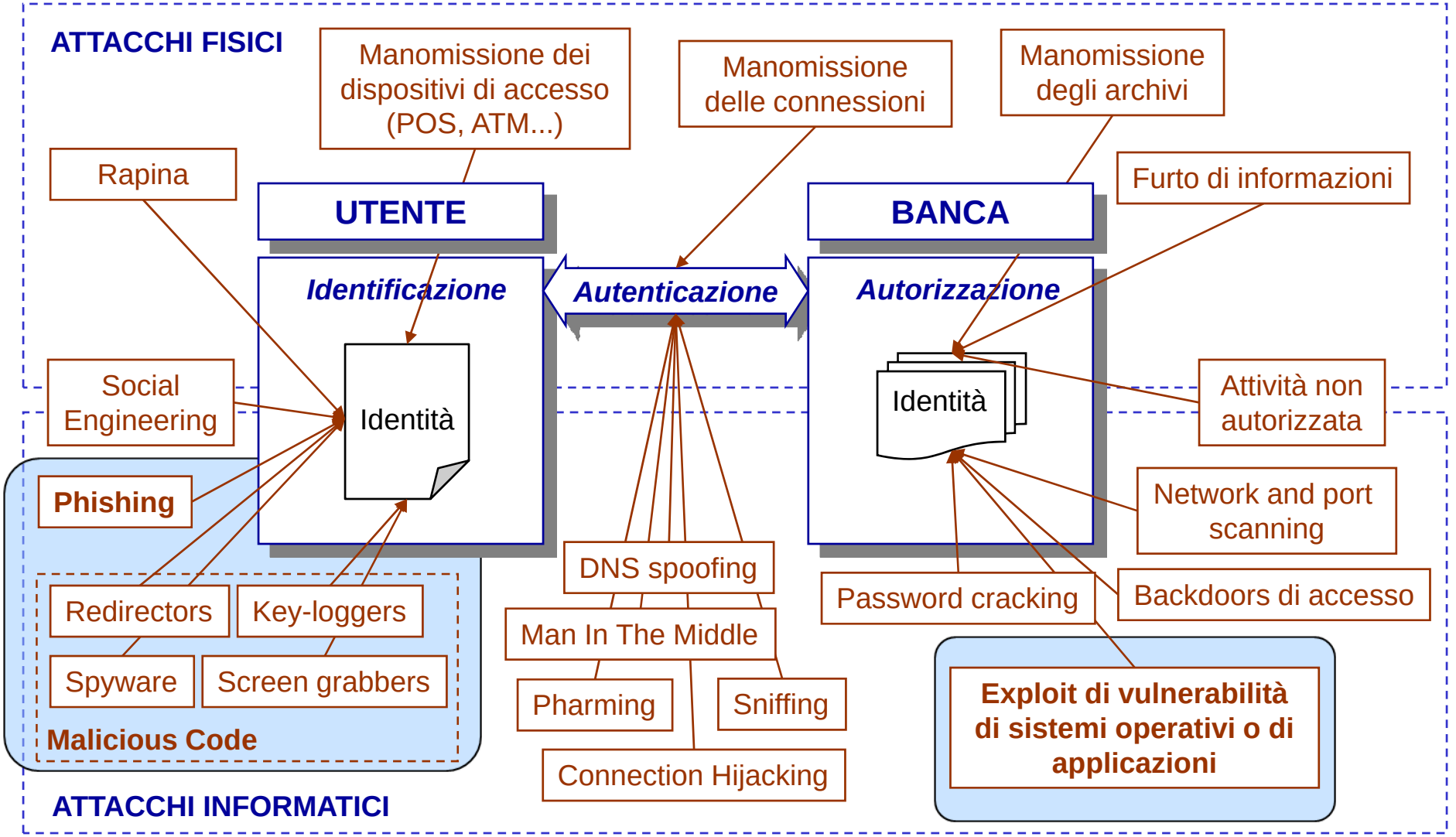
- Log On
- Single Sign On
- One-time Password
- Autenticazione multipla
- Mutua autenticazione
- Certificato elettronico
- Caller Line Identifier
- Firma autografa
- Protocolli di autenticazione
- Autenticazione biometrica

AUTORIZZAZIONE

Verifica della corrispondenza tra le abilitazioni esistenti in capo al soggetto richiedente e il tipo di operazione che il soggetto intende eseguire.

- Access Control List
- DB utenti

Attacchi alle informazioni sui canali di accesso



Agenda

- Il sistema bancario e gli attacchi alle informazioni
- **Attacchi e vulnerabilità delle applicazioni**
- Azioni di risposta delle banche
- La sicurezza applicativa: da best practice a norma

Attacchi e vulnerabilità applicative

- **Phishing**
  - Cross site scripting o controlli non efficaci in fase di autenticazione e/o autorizzazione
- **Violazioni della privacy**
  - Accesso non autorizzato a informazioni riservate
- **Furto di identità**
  - Carenza di controllo sui dati crittografati, compromissione mediante codice malevolo di applicazioni web, controlli non efficaci in fase di autenticazione e/o autorizzazione
- **Compromissione dei sistemi, alterazione dei dati, distruzione dei dati**
  - Vulnerabilità rispetto all'iniezione di codice malevolo
- **Danni economici**
  - Transazioni non autorizzate
- **Danni reputazionali e di immagine**
  - Attraverso lo sfruttamento di una qualsiasi vulnerabilità applicativa

OWASP TOP 10 – 2007 (1-5)

1. Cross Site Scripting (XSS)
   - Esecuzione di script nel browser della vittima (v. es.)
2. Injection Flaws
   - Esecuzioni non volute di codice iniettato o alterazioni dei dati
3. Malicious File Execution
   - Inclusione di codice ostile → anche compromissione totale del server
4. Insecure Direct Object Reference
   - Accesso non autorizzato ad oggetti (file, directory, database..)
5. Cross Site Request Forgery
   - Il browser viene forzato ad eseguire azioni per conto della vittima che è loggata in quel momento

OWASP TOP 10 – 2007 (6-10)

6. Information Leakage and Improper Error Handling
   - Raccolta di informazioni sulla configurazione, il codice e lo stato interno delle applicazioni, da riutilizzare a supporto di altre modalità di attacco

7. Broken Authentication and Session Management
   - Reperimento credenziali utente o amministratore e violazione privacy

8. Insecure Cryptographic Storage
   - Perdita di dati riservati e violazione privacy

9. Insecure Communications
   - Comunicazioni non criptate

10. Failure to Restrict URL Access
    - Accesso non autorizzato ad URL non protetti, ma riservati

Phishing e vulnerabilità applicative

- Le vulnerabilità applicative possono essere sfruttate oltre che per attacchi verso i sistemi centrali, anche per rendere più efficaci attacchi verso l'esterno

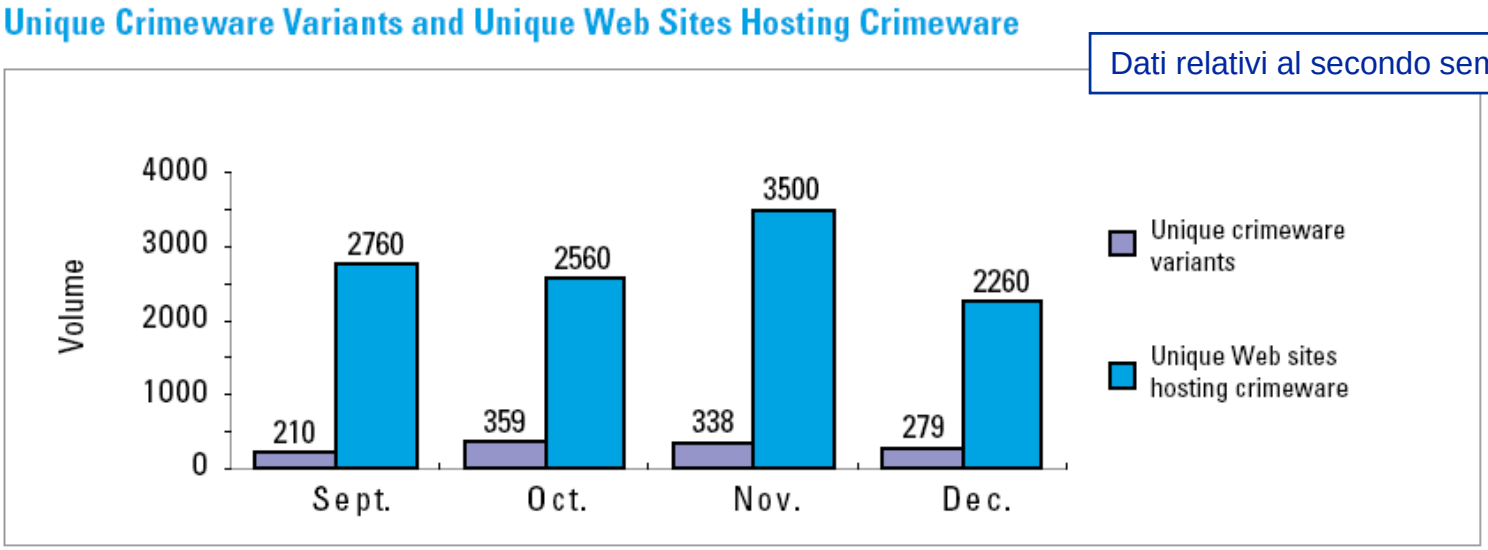
  - CASO DI UNA BANCA ITALIANA
    - **XSS** → modulo utilizzato per visualizzare messaggi di allerta all'utente
    - l'input non era stato propriamente controllato rispetto all'iniezione di codice malevolo
    - il frodatore è riuscito ad immettere un iframe che puntava ad un falso form di log-in localizzato su un server compromesso
      - i--FRAME SRC=" http://www.hijacked-site.com/path/to/fake/login.php " width=800 height=800 scrolling="no" frameborder="0"/i—FRAME
  - CRITICITÀ DELL'ATTACCO
    - Il dominio che viene visualizzato è ancora quello della banca
    - Il browser visualizza l'indirizzo corretto, comprensivo di "https"
  - CONTROMISURE
    - Penetration test applicativo e scansioni automatiche delle applicazioni
    - L'attacco viene portato a seguito dell'invio di una quantità massiva di codice malevolo verso il sito target ➔ Monitoraggio real time dei sistemi mission critical, come i server utilizzati per l'internet banking

Fonte: Symantec, Gennaio 2008

Crimeware - Siti malevoli e diffusione

- **Il 51% dei siti con codice malevolo** fanno riferimento a **siti reali che sono stati violati** mediante lo sfruttamento di qualche vulnerabilità dei sistemi che li ospitano, contro un **49% di siti creati appositamente da hacker per diffondere i propri malware**.
  - Miglior reputazione, Platea più ampia e già costituita di visitatori abituali
  - Non c'è la necessità di creare modalità di reindirizzamento del traffico verso il sito malevolo

- Il 18% dei siti malevoli sono stati creati utilizzando **toolkit** già pronti e **disponibili sul web**.



Fonte: Websense, 2008

Agenda

- Il sistema bancario e gli attacchi alle informazioni
- Attacchi e vulnerabilità delle applicazioni
- **Azioni di risposta delle banche**
- La sicurezza applicativa: da best practice a norma

Cosa fanno le banche

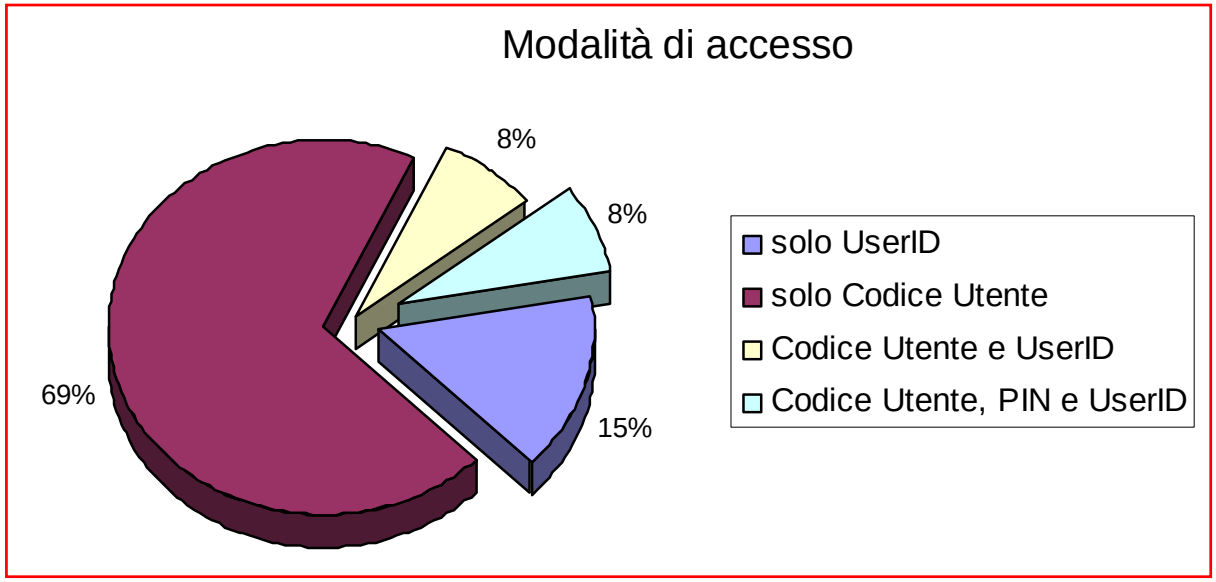
L'azione di risposta delle banche rispetto agli attacchi evidenziati si sono concretizzate lungo una duplice direzione

- **Contromisure tecnologiche**
  - Verso l'esterno
    - Protezione del canale di accesso alle applicazioni web
  - Interne
    - Monitoraggio strutturato degli attacchi
    - Focalizzazione sulle vulnerabilità applicative
      - » PCI DSS e OWASP

- **Formazione interna dei dipendenti e sensibilizzazione dei clienti**
  - Iniziative dei singoli istituti
  - Iniziative di formazione dei dipendenti
  - Iniziative cooperative rivolte ai clienti per sviluppare una cultura diffusa sulla sicurezza
    - Opuscolo ABI Lab
    - Area web dedicata alla sicurezza del cittadino - Corso on-line

Protezione dell'accesso al servizio di home-banking

- Ogni banca prevede una modalità di accesso con un codice identificativo dell'utente o con uno userID (nickname)

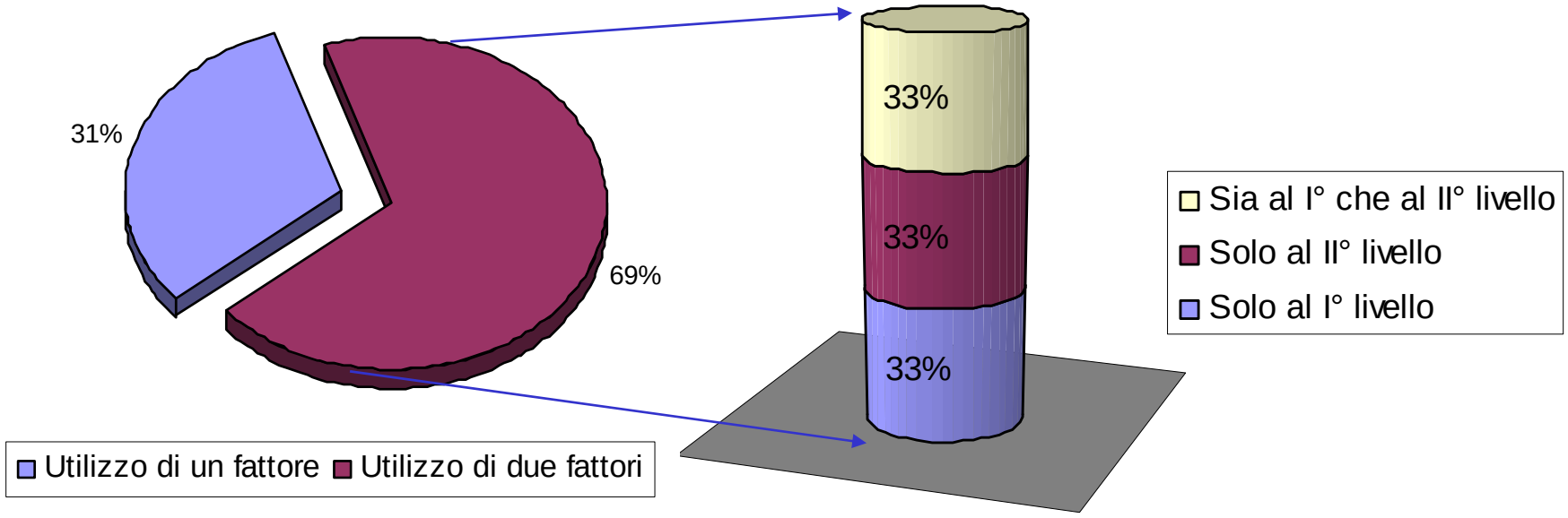


- **Ogni banca prevede l'utilizzo di una prima password statica**, che nel 92% dei casi è modificabile anche dal cliente
- **L'utilizzo di due livelli di autenticazione** è previsto dall'**85% delle banche**
- **L'utilizzo di una password dinamica o di una strong authentication implica l'utilizzo di un secondo fattore**, atto a generare tale password (Carta ad incroci, OTP cartacea, Token...)

Fonte: ABI Lab, Centrale d'Allarme per attacchi informatici, 2007, 13 banche

Doppio livello e doppio fattore

- Il **69% delle banche** già prevede l'autenticazione dei propri clienti mediante **due fattori**.
- Un terzo di esse utilizza il secondo fattore per la sola autenticazione di primo livello, un terzo per la sola autenticazione di secondo livello e un terzo per entrambi i livelli
- È utile sottolineare che nel rimanente 31% sono presenti **istituti che già hanno avviato progetti di adozione del secondo fattore** che si concluderanno entro l'anno



Fonte: ABI Lab, Centrale d'Allarme per attacchi informatici, 2007, 13 banche

Lo standard PCI DSS

- Requisiti di sicurezza definiti dal Payment Card Industry – Security Standards Council (Visa/Mastercard) per la PROTEZIONE DELL'UTILIZZATORE DI CARTE DI PAGAMENTO, rivolti a
  1. Protezione dei dati personali
  2. Controllo dei dati delle transazioni di pagamento
  3. Sicurezza dei dati di autenticazione della carta
  4. Riduzione del rischio complessivo di compromissione dei dati dell'utilizzatore
- Obbligatoria per tutte le aziende che gestiscono dati relativi a
  - Personal Account Number (PAN) – 1.
  - Data di validità – 1.
  - Banda magnetica – 2.
  - CVV2 / CVC2 – 3.
- Non necessariamente coinvolge tutte le banche (outsourcing) e fa riferimento principalmente agli acquirer, più che agli issuer

La sicurezza applicativa in PCI DSS

- **Costruire e mantenere una rete protetta**
  - Installare e mantenere una configurazione con firewall per proteggere i dati dei titolari delle carte
  - Non utilizzare password di sistema predefinite o altri parametri di sicurezza impostati dai fornitori
- **Proteggere i dati dei titolari delle carte**
  - Proteggere i dati dei titolari delle carte memorizzati
  - Cifrare i dati dei titolari delle carte quando vengono trasmessi attraverso reti pubbliche aperte
- **Rispettare un programma per la gestione delle vulnerabilità**
  - Utilizzare e aggiornare con regolarità il software antivirus
  - **Sviluppare e mantenere applicazioni e sistemi protetti**
- **Implementare misure forti per il controllo dell'accesso**
  - Limitare l'accesso ai dati dei titolari delle carte solo se indispensabili per lo svolgimento dell'attività commerciale
  - Assegnare un ID univoco a ogni utente che ha accesso ai computer
  - Limitare la possibilità di accesso fisico ai dati dei titolari delle carte
- **Monitorare e testare le reti con regolarità**
  - Monitorare e tenere traccia di tutti gli accessi effettuati alle risorse della rete e ai dati dei titolari delle carte
  - **Eseguire test periodici dei processi e dei sistemi di protezione**
- **Adottare una politica di sicurezza**

6. Sviluppo e manutenzione applicazioni e sistemi protetti

6.5 Sviluppare tutte le applicazioni per il Web attenendosi a **linee guida di programmazione sicura**, ad esempio le linee guida Open Web Application Security Project. Esaminare il codice delle applicazioni personalizzate per identificare eventuali vulnerabilità. Per prevenire eventuali vulnerabilità nella programmazione, durante i processi di sviluppo del software verificare i seguenti punti:

... OWASP TOP TEN ...

6.6 Assicurarsi che tutte le **applicazioni per il Web siano al riparo dagli attacchi più comuni** adottando uno dei seguenti metodi:

- Incaricando un'organizzazione specializzata in sicurezza delle applicazioni di esaminare tutto il codice delle applicazioni personalizzate alla ricerca delle vulnerabilità più comuni.
- Installando un firewall a livello di applicazione davanti a ogni applicazione Web.

Nota: questo metodo è da considerarsi migliore pratica fino al 30 giugno 2008, dopodiché da tale data diventerà un requisito.

11. Test periodico dei processi e dei sistemi di protezione

11.2 Eseguire scansioni interne ed esterne delle vulnerabilità almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete, ad esempio: l'installazione di un nuovo componente nel sistema, un cambiamento della topologia della rete, una modifica delle regole del firewall o l'aggiornamento di un prodotto.

Nota: le scansioni esterne delle vulnerabilità devono essere eseguite trimestralmente da un ASV approvato dalla PCI. Le scansioni dopo le modifiche della rete possono essere eseguite dal personale interno dell'azienda.

11.3 Eseguire i test di penetrazione almeno una volta all'anno e dopo ogni aggiornamento o modifica significativi apportati all'infrastruttura o a un'applicazione, ad esempio: un aggiornamento del sistema operativo o l'aggiunta di una subnet o di un server Web all'ambiente. I test di penetrazione devono includere:

- **11.3.1** Test di penetrazione al livello di rete
- **11.3.2** Test di penetrazione al livello di applicazioni.

Agenda

- Il sistema bancario e gli attacchi alle informazioni
- Attacchi e vulnerabilità delle applicazioni
- Azioni di risposta delle banche
- **La sicurezza applicativa: da best practice a norma**

La sicurezza applicativa: da best practice a norma

- La costante evoluzione dello **scenario della sicurezza delle applicazioni web** focalizza da sempre l'attenzione delle banche, anche in virtù del crescente numero di applicazioni e servizi che vengono resi disponibili attraverso il web.
- La realizzazione di **attacchi sempre più strutturati**, rivolti soprattutto alla propria clientela, evidenzia la necessità da parte delle banche di fornire una **risposta di contrasto efficace**, sia in termini di prevenzione che di reazione.
- L'azione di **monitoraggio** e **verifica dello stato di protezione** delle proprie applicazioni web si accompagna ad una altrettanto necessaria **attività di formazione** e **sensibilizzazione** sia del proprio personale che dei clienti.
- **PCI DSS**, standard de facto per la sicurezza dei dati utilizzati dalle carte di pagamento, può aiutare per fornire la **spinta a programmare in sicurezza** anche sulla base di una normativa cui attenersi.
- Il **quadro degli standard e delle normative** cui le banche devono essere compliant, però, è attualmente complesso e molto diversificato sulla base sia dei canali che dei processi che si considerano.
- Iniziative come **OWASP** possono fornire il **contesto ideale per unificare tutti gli aspetti relativi alla sicurezza applicativa in un unico framework**, da considerare come **punto di riferimento** per la **gestione di tutte le normative e gli standard presenti in materia**.