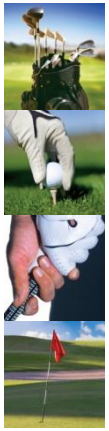
SECSERVIZI

SECurity Online

lo scenario e le evoluzioni di sicurezza per servizi bancari

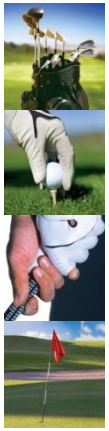
Febbraio 2012

AGENDA



- **Presentazione generale**
  - **La Società**
  - **Numeri chiave e clienti**
  - **Linee guida trasversali**
- La sicurezza in SEC Servizi
- Crittografia e strong authentication nell'online banking
- Lo scenario delle frodi online
- Evoluzioni di sicurezza di SEC Servizi
- Conclusioni

La Società



- SEC SERVIZI è un consorzio bancario operante sul mercato da quasi 40 anni nella gestione di servizi di outsourcing ICT in ambito bancario

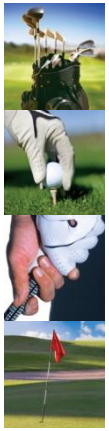
LA VISION DI SEC SERVIZI

"Essere un leader riconosciuto nella erogazione di servizi al settore finanziario e non, che sostiene, sviluppa e promuove la conoscenza tecnologica e finanziaria nell'ambito della comunità economica, scientifica e sociale"

SERVIZI OFFERTI

- Servizi di outsourcing ICT in ambito bancario, in modalità full outsourcing e/o selettivo/verticale
- Servizi a Confidi e SGR/SIM (tramite le partecipate Galileo e AMS)
- Facility management (sistemi mainframe e dipartimentali)
- Servizi ausiliari (es. stampe), supporto, consulenza

Numeri chiave e Clienti



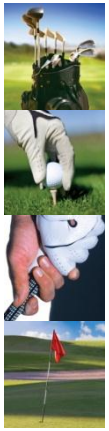
- SEC SERVIZI è un consorzio bancario operante sul mercato da oltre 35 anni nella gestione di servizi di outsourcing ICT in ambito bancario

ALCUNI INDICATORI

- **Capitale sociale** 25.000.000,00 euro
- 17 **soci**
- **Dipendenti** ad agosto 2011: 301
- Oltre 40 **clienti** attivi
- Volume della **produzione** 2010: 117,5 milioni di Euro
- **Operatività** oltre 30 milioni di transazioni medie al giorno
- Circa 1.400 **sportelli** collegati, circa 15.000 **postazioni di lavoro**, oltre 4.500.000 **clienti** finali
- Primo outsourcer in Italia a ottenere la certificazione GSC

I NOSTRI CLIENTI

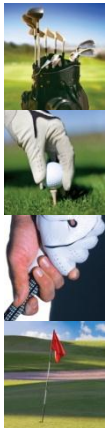
Gruppo Banca Popolare di Vicenza
PrestiNuova
Banca Nuova
VENETO BANCA
CLARIS CINQUE
BANCA ITALO ROMENA
bancApulia
IPIBI
Banca Popolare dell'Alto Adige
CASSA DI RISPARMIO DI FABRIANO E CUPRAMONTANA
Banca di Credito Popolare
Allianz Bank Financial Advisors
CheBanca!
UBAE
BancaITB
FARBANCA SPA
Apulia prontoprestito
BANCA DELLA NUOVA TERRA



Linee guida trasversali di evoluzione

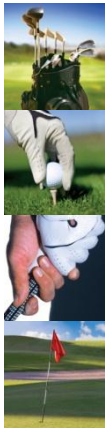
- Approccio di system integrator (ove possibile) con utilizzo pacchetti di mercato
- Logica a processi/servizi con alta riusabilità delle componenti applicative
- Sviluppo nuove applicazioni su framework standard SEC JMC
  - basato su SOA e generazione automatica software da modellazione processi
  - interfaccia web based
- Forte investimento su strumenti di workflow e gestione documentale
- Continua ottimizzazione dei processi di ciclo di vita del software

AGENDA



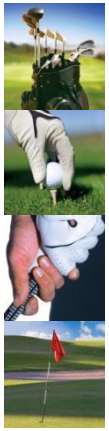
- Presentazione generale
- **La sicurezza in SEC Servizi**
  - **Ambito**
  - **Il Modello organizzativo di Sicurezza**
  - **Il Sistema di gestione di Sicurezza**
- Crittografia e strong authentication nell'online banking
- Lo scenario delle frodi online
- Evoluzioni di sicurezza di SEC Servizi
- Conclusioni

Ambito

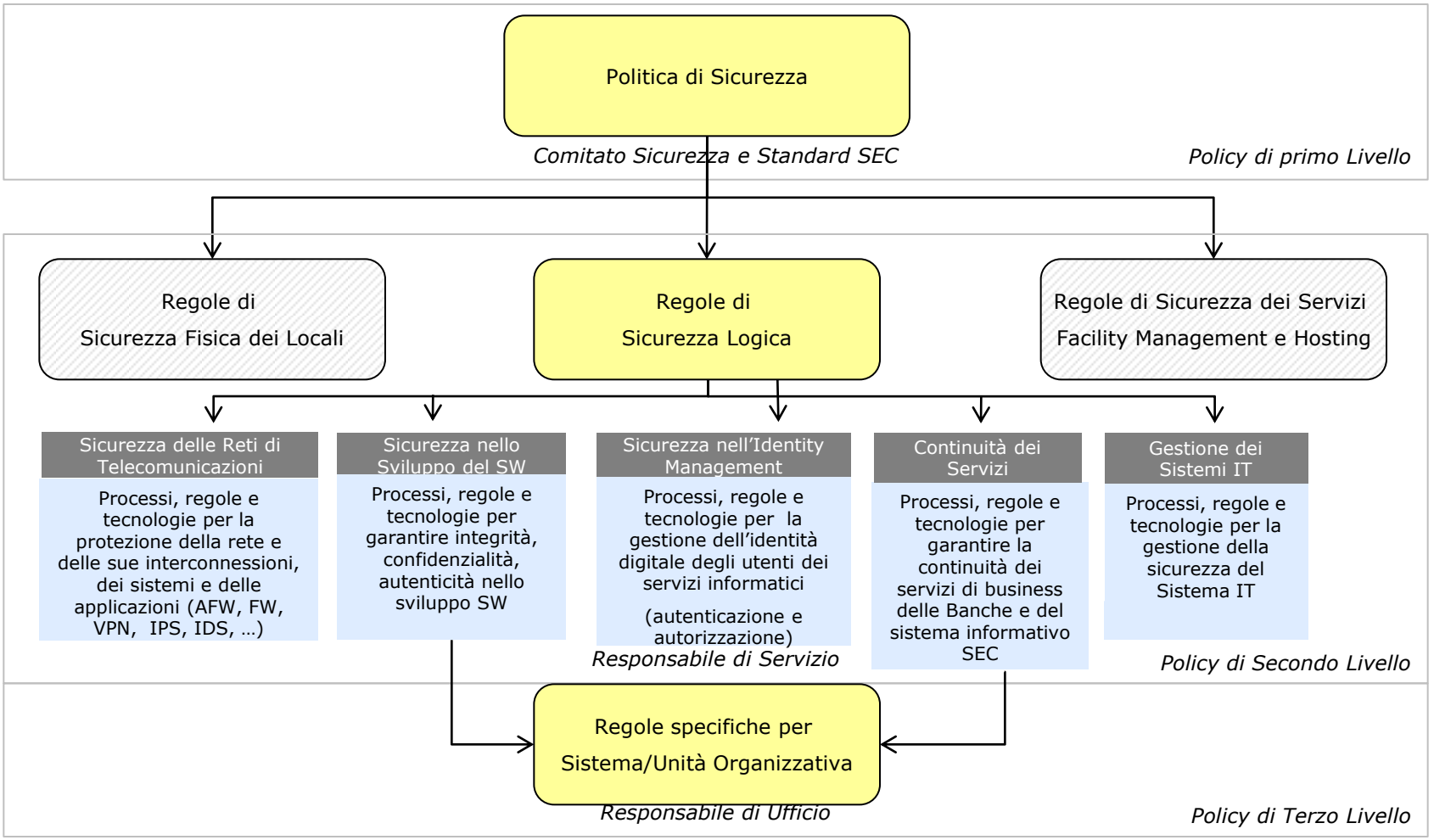


- Il tema della sicurezza è considerato di primaria importanza da parte di SEC Servizi, che si pone quindi l'obiettivo di definire univocamente modelli organizzativi ed operativi volti a:
  - assicurare ai clienti la ***continuità del business***;
  - ***prevenire e gestire incidenti*** informatici che possano portare a perdite finanziarie dirette, riduzione della competitività, sanzioni normative, tramite interventi operativi che contrastino effetti e propagazione dei danni informatici;
  - adempiere agli ***obblighi legislativi*** vigenti ;
  - seguire percorsi di sviluppo che consentano l'ottenimento di ***certificazioni*** di settore;
  - ***proteggere i dati*** garantendone ***riservatezza***, ***integrità***, ***autenticità*** e ***disponibilità***;
  - migliorare i processi di gestione delle ***identità digitali*** e la sicurezza all'interno dei processi aziendali, coinvolgendo tutti i livelli dell'organizzazione;
  - ***standardizzare*** lo sviluppo applicativo in termini di sicurezza, verificandone poi la conformità.

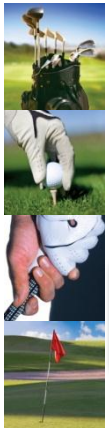
Il Modello organizzativo di Sicurezza



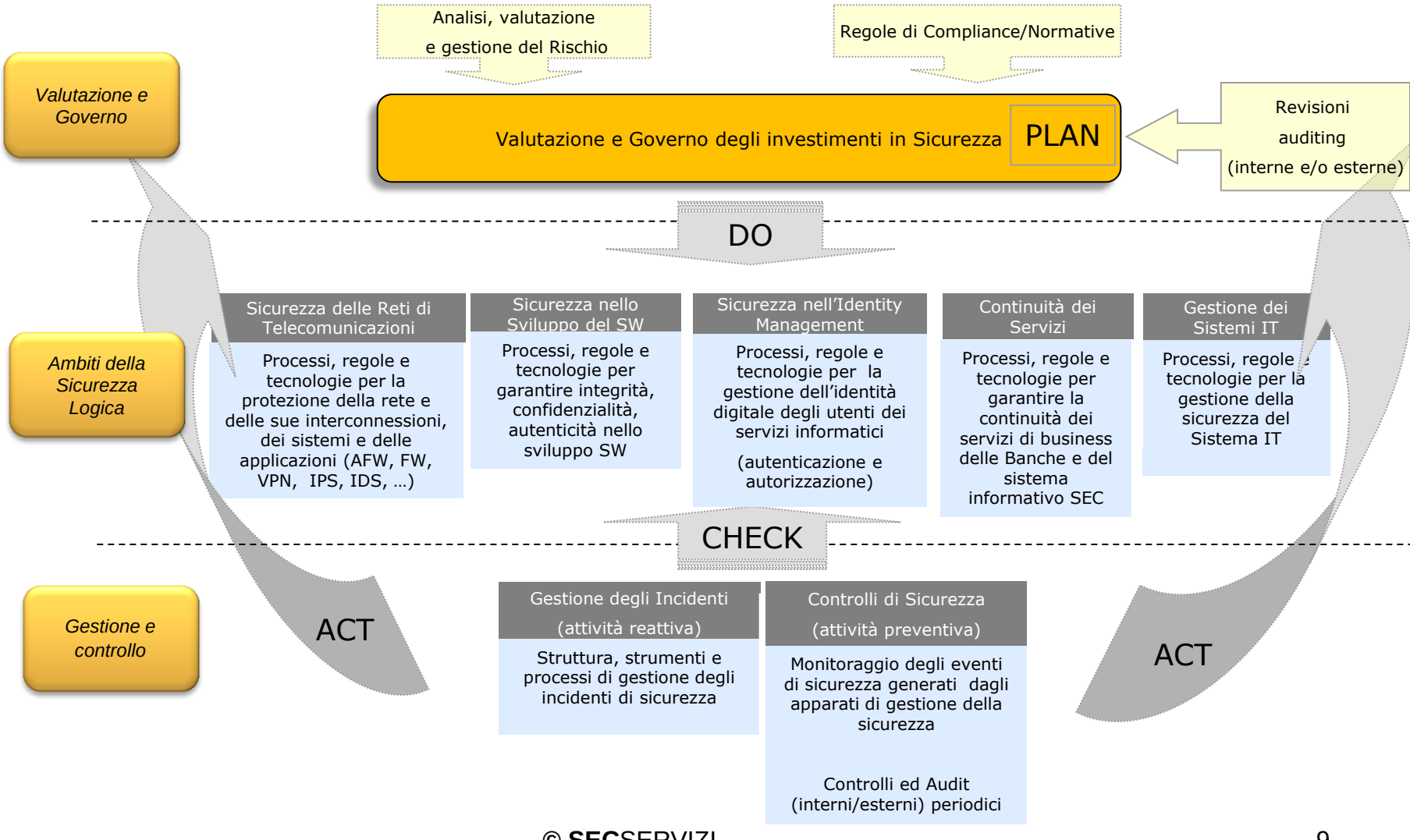
- Il Modello organizzativo di Sicurezza di SEC Servizi è consolidato e dettagliato nelle policy di sicurezza



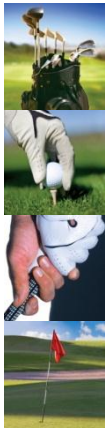
Il Sistema di gestione di Sicurezza



- Il Sistema di gestione di Sicurezza di SEC Servizi ivi rappresentato è in fase di evoluzione e viene progressivamente perfezionato e consolidato in ottica di raggiungimento delle Certificazioni ISO 20K-27K

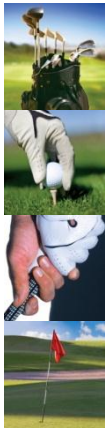


AGENDA



- Presentazione generale
- La sicurezza in SEC Servizi
- **Crittografia e strong authentication nell'online banking**
  - **Crittografia nell'online banking**
  - **Meccanismi di strong authentication**
- Lo scenario delle frodi online
- Evoluzioni di sicurezza di SEC Servizi
- Conclusioni

Crittografia nell'online banking



Client SSL

Società Servizi

WS Security

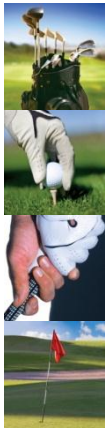
SAML Federation

Firma Digitale Remota

encrypted data

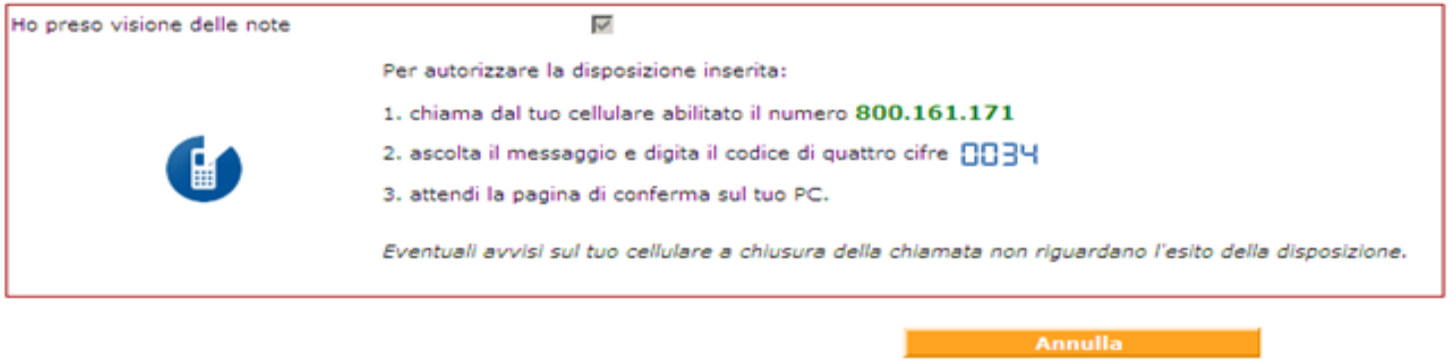
Società Servizi

Meccanismi di strong authentication

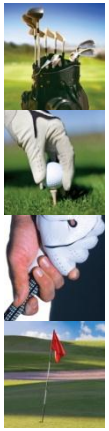


- La sicurezza non è basata solo sulla crittografia del canale, ma anche dai meccanismi di autenticazione;
- Con l'avvento dei primi fenomeni di phishing, key logger e/o mouse logger si sono introdotti meccanismi di strong authentication;
- In particolare SEC ha introdotto 2 tipologie di autenticazione forte basata su One time password (password univoca usa e getta):
  - RSA SecureId : One time password basata sul token

  - Telecom SecureCall, One time password inserita tramite telefono, disaccoppiando il canale di autenticazione da quello di disposizione

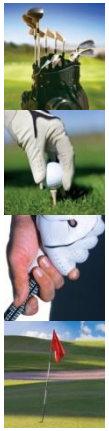


AGENDA

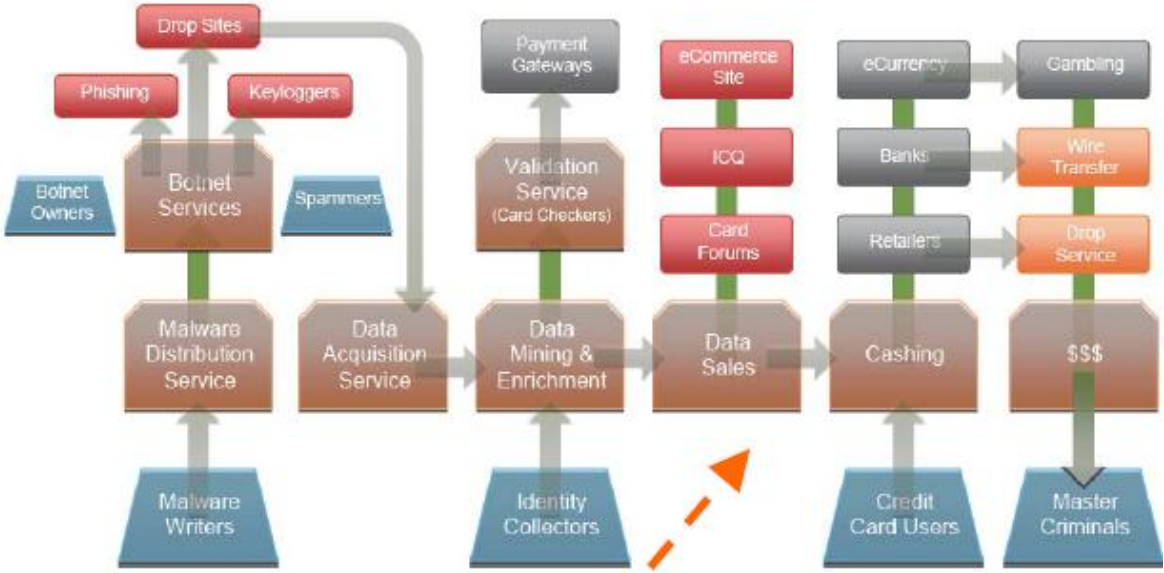


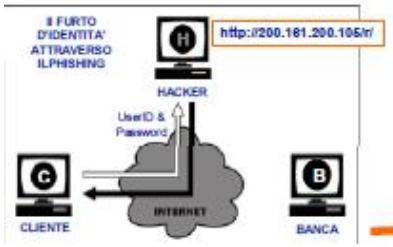
- Presentazione generale
- La sicurezza in SEC Servizi
- Crittografia e strong authentication nell'online banking
- **Lo scenario delle frodi online**
  - **Evoluzione frode informatica**
  - **Modello dell'organizzazione fraudolenta**
  - **BotNet e Command & Control**
  - **Nuove varianti di trojan**
  - **Sei tu Alice?**
- Evoluzioni di sicurezza di SEC Servizi
- Conclusioni

Evoluzione frode informatica (fonte ABILAB)



L'evoluzione del fenomeno delle frodi informatiche cui si è assistito nel corso degli ultimi anni evidenzia un **livello crescente di organizzazione e di strutturazione del percorso della frode**, in relazione ad una capacità crescente da parte dei frodatori di gestire una **numerosità sempre più consistente di attacchi** che sfruttano i differenti canali di comunicazione



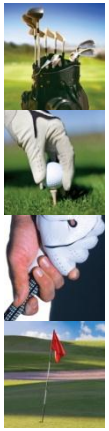


Il flusso delle informazioni è regolato da una **regia internazionale** che fa sì che il denaro alla fine del percorso arrivi alla destinazione fraudolenta

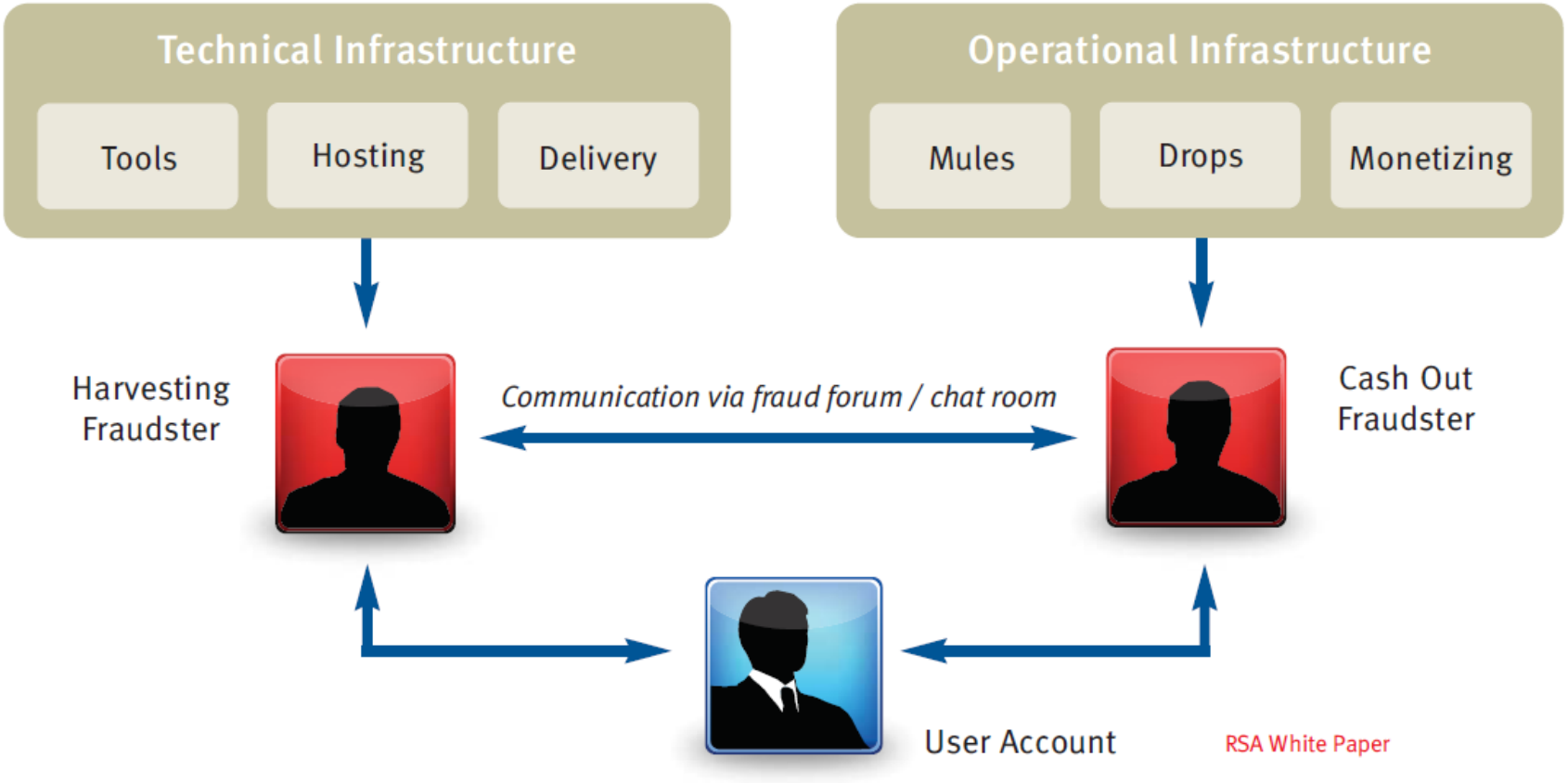
La banca viene quindi ad essere interessata da un **fenomeno trasversale** che richiede una **capacità di monitoraggio e prevenzione non più limitata ad un singolo contesto funzionale**

2005 2007 2010

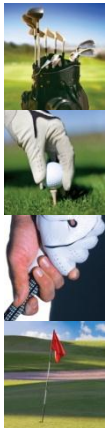
Modello dell'organizzazione fraudolenta

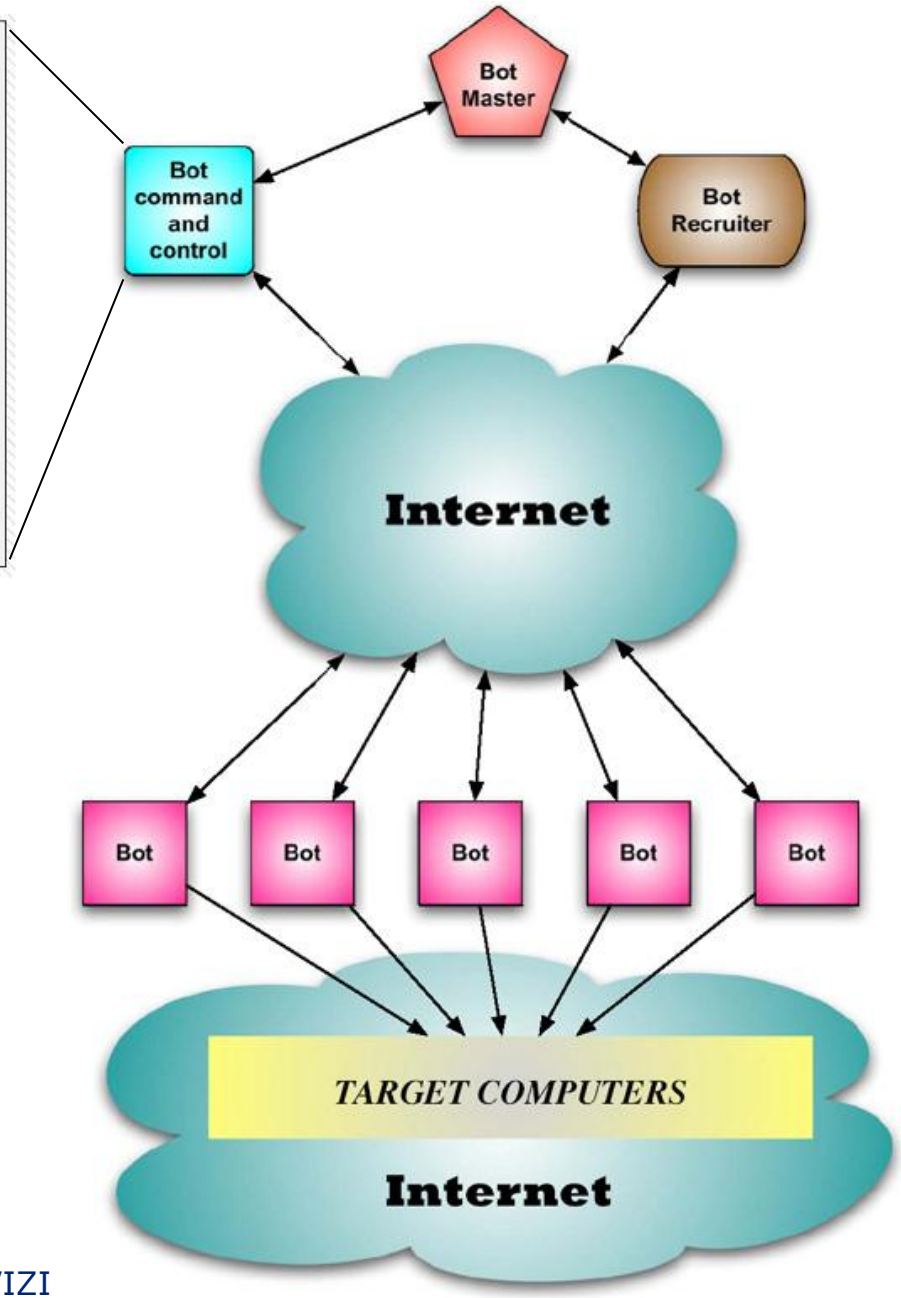


- Parlare di frode informatica e analizzare le sue forme ed entità il più delle volte corrisponde a creare allarmismo. Ma bisogna essere consapevoli che ad oggi dietro ad un crimine informatico, non c'e' più un singolo hacker bensì organizzazioni specializzate.



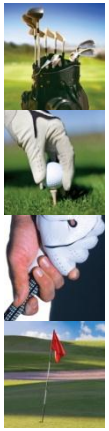
BotNet e Command & Control





- Nel 2009 il crimine online è cresciuto vertiginosamente attorno al 600%.
- I tool per comandare una botnet sono facilmente reperibili e semplici da usare;
- Si usa il phishing per far accedere l'utente a contenuti di siti internet che (drive-by-download) iniettano il trojan sul pc della vittima.

Nuove varianti di trojan



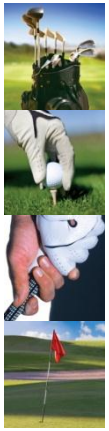
• È stata identificata una nuova famiglia di trojan, evoluzione di ZeuS, cui è stato dato il nome di ZeuS 3.0:

  – Supporto a Firefox
  – Cifratura più efficace del file di configurazione
  – L'eseguibile e le chiavi di registro non hanno nomi fissi ma casuali

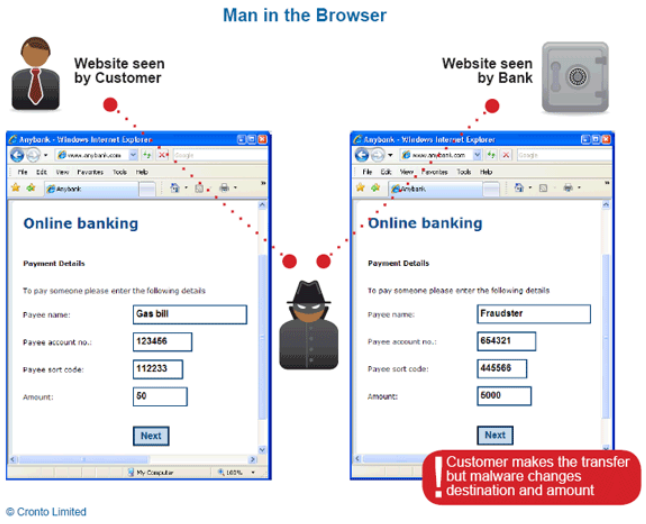
• Funzionalità:

  – Keylogging
  – Genrazione di screenshot
  – Logging delle credenziali
  – HTML injection
  – Furto di credenziali memorizzate
  – Furto di credenziali POP3 e FTP
  – Modulo Back Connect, per consentire upload e download dal PC contagiato
  – Modulo Reverse VNC, per pieno controllo dell'interfaccia grafica
  – Modulo Proxy, per inserire il PC infetto in attacchi di tipo fast-flux
  – **Furto di certificati digitali**

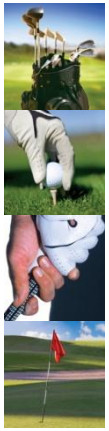
Sei tu Alice?



- La crittografia è implementata dai browser, ma se questi sono infetti da virus c'e' la possibilità di compromettere la comunicazione sicura;
- La sicurezza con meccanismi di strong authentication può fallire in caso di attacchi man in the browser perché il codice OTP non è legato alla transazione;
- Un trojan (programma malevolo) che ha il possesso del browser può modificare il contenuto della pagina sia verso il sistema informativo, modificando i dati dell'utente, sia dopo aver ricevuto la risposta, può rimodificare i dati visti dall'utente finale;

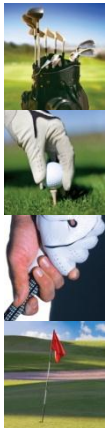


AGENDA



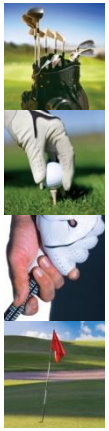
- Presentazione generale
- La sicurezza in SEC Servizi
- Crittografia e strong authentication nell'online banking
- Lo scenario delle frodi online
- **Evoluzioni di sicurezza di SEC Servizi**
  - **La risposta di SEC alle nuove minacce informatiche**
  - **Firma delle transazioni**
  - **Analisi comportamentale – Collaborazione Università**
- Conclusioni

La risposta di SEC alle nuove minacce informatiche

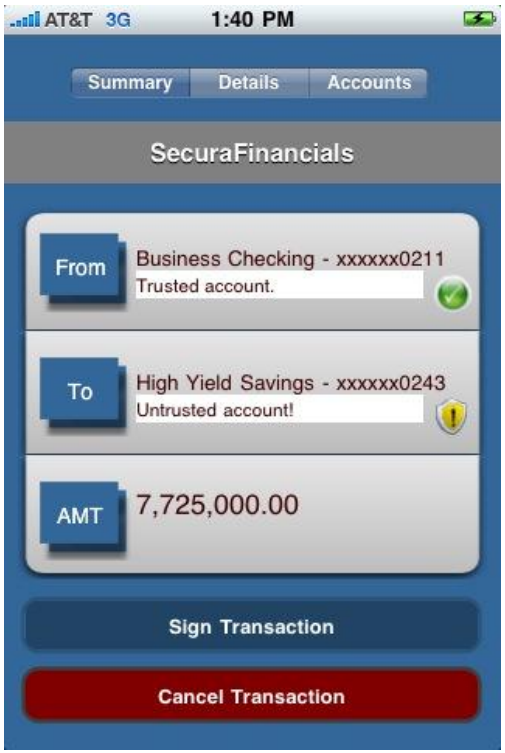


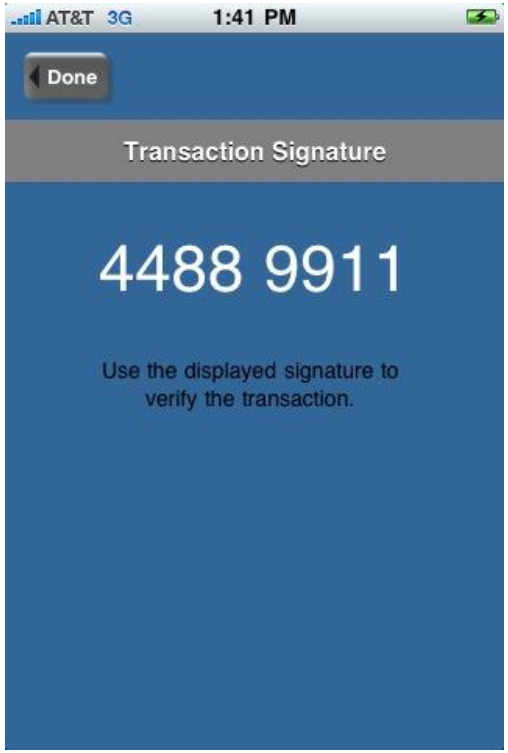
- SEC Servizi continua a seguire con attenzione le evoluzioni tecnologiche e centralizza le esperienze per poter sempre fornire ai propri clienti il supporto per trovare, in questo ambito, soluzioni di contrasto.
- Le principali risposte sono:
  - **Preventive**
    - Notifiche delle operazioni via SMS
    - Introduzione di meccanismi di autenticazione adattativi Out of the box (SMS di verifica in caso di operazione sospetta)
    - Firma delle transazioni
  - **Rilevazione**
    - Utilizzo di servizi di mercato antitrojan e antispam
    - Introduzione di soluzioni di fraud intelligence ed analisi comportamentale

Firma delle transazioni

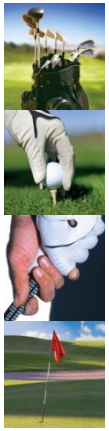


- La firma della transazione può essere realizzata con applicazioni deviceless o con device;
- Firmare significa generare un codice OTP determinato dai dati salienti della transazione;





Analisi comportamentale – Collaborazione Università (3/3)

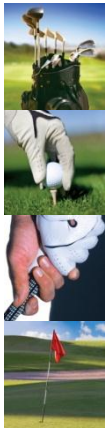


UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

- SEC sta sperimentando una collaborazione con il Dipartimento d'Ingegneria Dell'Informazione dell'Università di Padova, verificando algoritmi di datamining in ambito di fraud detection;
- Partendo da un percorso esplorativo di letteratura, si sono trovate nelle frodi dell'online banking analogie con gli ambiti già esplorati del mondo della telefonica (SIM clonate) e delle carte di Credito;
- Gli algoritmi usati in questi ambiti sono basati su reti neurali/learning machine, ma si è notato fin da subito che le transazioni online non avevano la stessa frequenza delle operazioni su SIM o su carta;
- Si è passati dunque a tecniche di intrusion detection, ma anche queste cercano di risolvere problemi legati principalmente alla morfologia delle richieste, cercando di determinare modifiche di parametri della richiesta;
- Si è dunque giunti al testare l'utilizzo di macchine a stati probabilistiche al fine di ottenere come risultato il discostamento comportamentale delle transazioni online.

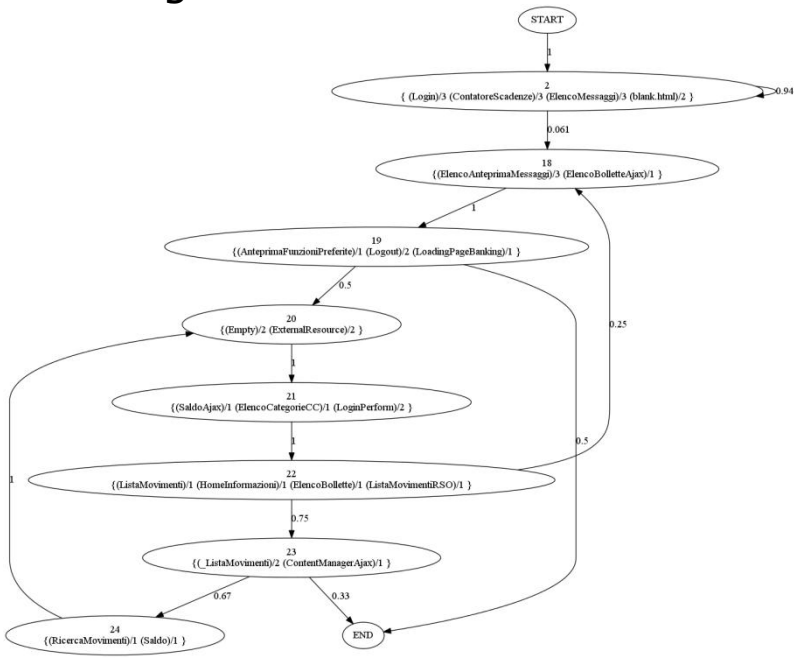
Analisi comportamentale – Collaborazione Università (2/3)



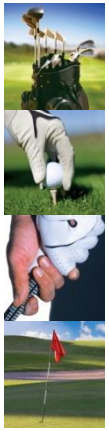
UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

- L'approccio è quello di rappresentare la navigazione degli utenti come un linguaggio accettato da una grammatica probabilistica modellata con l'uso di un Hidden Markov Model. Tale modello viene poi generalizzato tramite una tecnica di fusione degli stati che cerca di ottimizzare la probabilità a posteriori del modello con tecniche di ragionamento Bayesiano. Questo fondamentalmente porta ad una generalizzazione rispetto al modello originale.



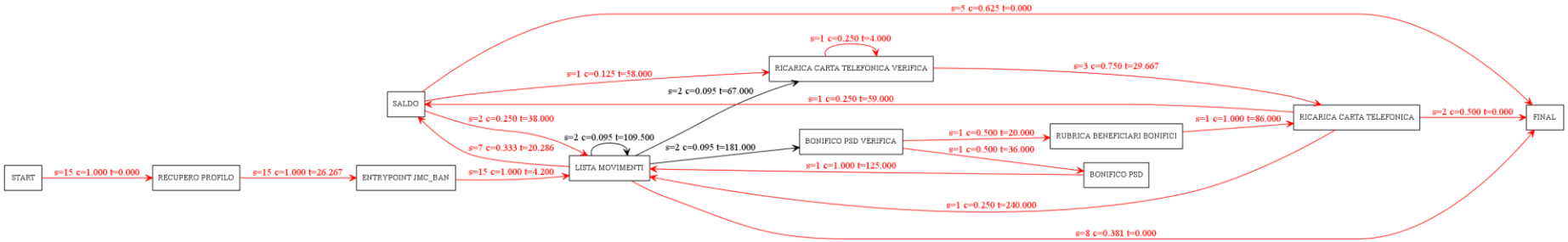
Analisi comportamentale – Collaborazione Università (3/3)



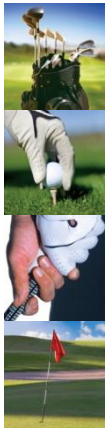
UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

- L'approccio che si vorrebbe usare alla fine è multimodello, utilizzando tutte le informazioni a disposizione sugli utenti, tra cui le tempistiche di navigazione da una pagina all'altra e le caratteristiche delle operazioni dispositive, in particolare i bonifici, al fine di ottenere un'anomalia o un livello di rischio alto nel caso di frode.

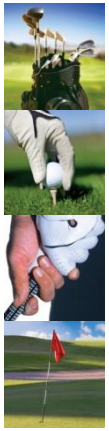


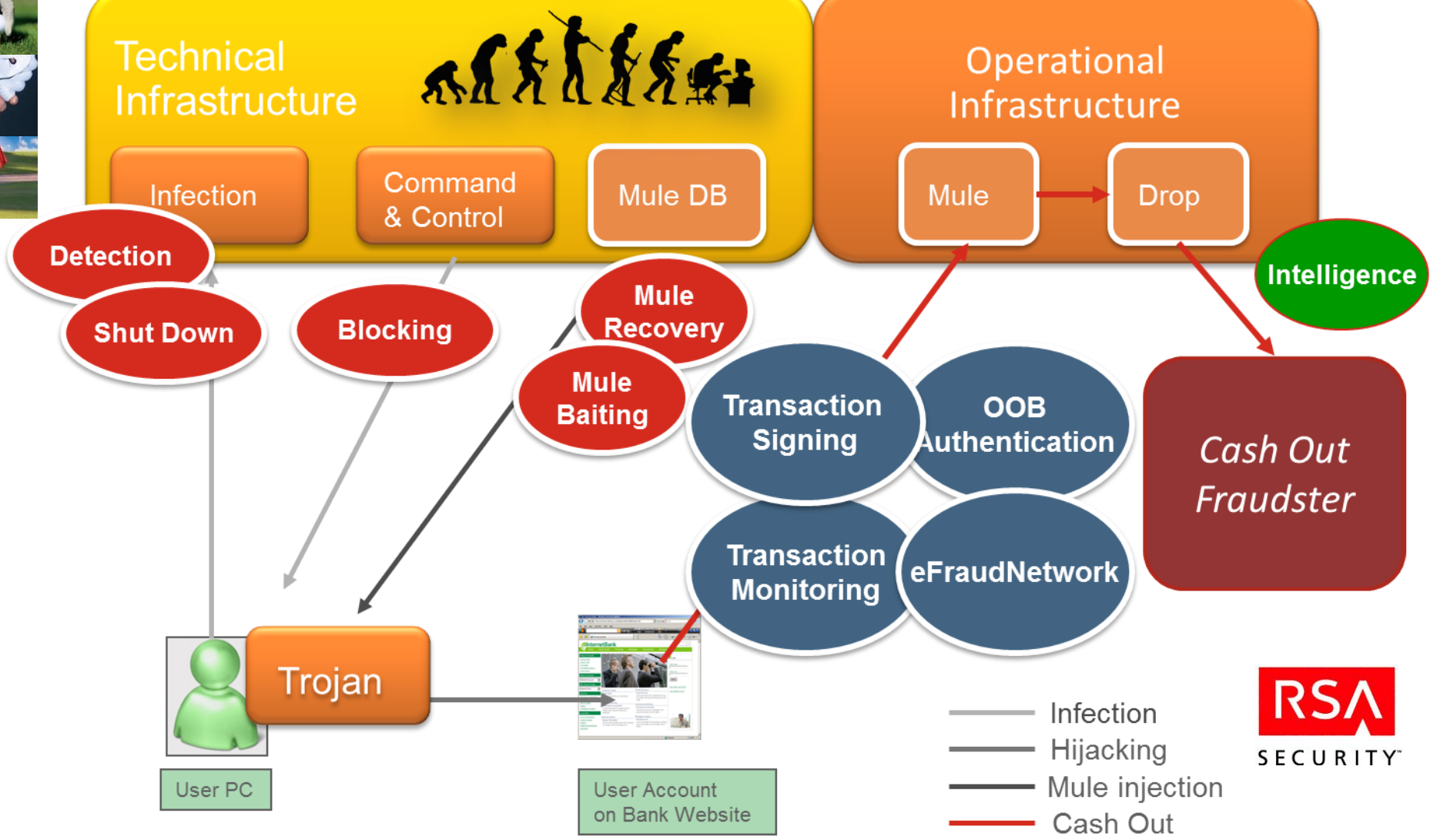
AGENDA



- Presentazione generale
- La sicurezza in SEC Servizi
- Crittografia e strong authentication nell’online banking
- Lo scenario delle frodi online
- Evoluzioni di sicurezza di SEC Servizi
- **Conclusioni**

Conclusioni





SECSERVIZI

GRAZIE PER L'ATTENZIONE

Per info e contatti:
Dario Zandolin
Ufficio Architetture
SEC SERVIZI S.C.p.A.
Via Transalgardo, 1, 35129 – Padova

e-mail: dario_zandolin@secservizi.it
www.secservizi.it

Febbraio 2012