



# TEACH

APPROFONDIMENTI TECNOLOGICI

## **Vulnerabilità dei sistemi e tecniche di difesa: NAC, IDS e Trusted computing**

Chairman  
Antonio LIOY, Politecnico di Torino

**Milano, 1 dicembre 2006**

I nostri sistemi informatici continuano ad essere sotto attacco, nonostante i grossi sforzi fatti in anni recenti per migliorarne la sicurezza.



## Presentazione

In questa giornata si esaminano alcune aree che meritano maggiore attenzione al fine di raggiungere un ancor più elevato grado di protezione.

In primo luogo le applicazioni web, per le quali non basta la creazione di canali sicuri SSL ma occorre anche adottare tecniche di programmazione sicure. L'uso di piattaforme trusted e compartimentate come quelle rese oggi possibili dall'architettura Trusted Computing, possono contribuire a innalzare notevolmente la difesa sia di un singolo server, sia dei canali di comunicazione.

Nell'ambito delle reti aziendali si discuterà di come limitare l'accesso alla rete solo agli utenti autorizzati e con protezioni sulle postazioni di lavoro correttamente configurate, e come controllare che i comportamenti degli utenti ed il traffico di rete rispettino le politiche di sicurezza aziendali. Inoltre – poiché è impossibile raggiungere un grado di protezione assoluto – bisogna organizzare un gruppo aziendale di risposta agli incidenti di sicurezza, in grado di operare 24x7 (perché gli attacchi si concentrano soprattutto nei periodi notturni e festivi) e di coordinarsi con gruppi analoghi nazionali ed internazionali, nonché di cooperare con le forze dell'ordine. Queste attività includono sempre più spesso operazioni di "Computer forensics" per identificare le debolezze sfruttate dagli attaccanti e cercare prove informatiche da utilizzarsi in un'eventuale procedura giudiziaria.

La giornata si concluderà coi risultati di un interessante esperimento condotto in sala relativo alla sicurezza dei dispositivi Bluetooth (telefoni cellulari, PDA e notebook).

## Destinatari

Responsabili della sicurezza, responsabili EDP, IT, dell'organizzazione, business development manager, ICT auditors, system and network manager, system engineer, sviluppatori e tutti coloro che sono interessati ad approfondire gli aspetti attinenti la vulnerabilità dei sistemi e alcune tecniche di difesa.



## Agenda della giornata

9.00 Registrazione dei partecipanti, benvenuto e introduzione del chairman

9.30 ***Gli attacchi informatici: sempre meno tecnologici, sempre più web***

**Antonio Lioy, Politecnico di Torino**

Nel campo della sicurezza informatica la tendenza in atto vede gli attacchi spostarsi dai livelli bassi a quello applicativo, con particolare predilezione per le applicazioni web. Che cosa si può fare per contrastare questa tendenza? quali sono le tipologie di attacco più frequenti? quali strumenti automatici esistono per effettuare un'auto-analisi di sicurezza delle applicazioni web? quali suggerimenti dare agli sviluppatori per rendere più robuste le loro applicazioni?

11.00 Coffee break

11.20 ***Prevenzione e monitoraggio degli incidenti di sicurezza, il ruolo di un CERT/CSIRT***

Relatore TBD

11.50 ***Gestione degli incidenti: come il SOC reagisce agli attacchi e ripristina tempestivamente***

***l'operatività dei sistemi. Il caso Bancalntesa – Manuela Burzoni, Direzione Sicurezza, Prevenzione Frodi e Crisi Informatiche***

L'intervento illustrerà come Banca Intesa fronteggia gli incidenti di sicurezza informatica, coordinando le diverse entità della coinvolte, secondo il modello organizzativo in essere e pianificando gli interventi necessari per ripristinare al più presto la normale operatività.

12.20 ***Lo stato dell'arte dell'Incident Response e della digital Investigation, Dario Forte, Università di Milano - DTI Crema***

L'intervento è suddiviso in due parti. La prima presenta lo stato dell'arte della gestione degli incidenti informatici: partendo da alcune statistiche, passerà alla overview dei modelli organizzativi e terminerà presentando gli standard tecnici per lo scambio delle informazioni. La seconda parte affronta gli aspetti più importanti della digital investigation: le manovre elusive, le best practices e le tecnologie di risposta.

12.50 Dibattito

13.00 Pranzo



14.00 ***NAC – Network Admission Control: di cosa stiamo parlando?*** Stefano Zanero, Politecnico di Milano

Esiste una certa confusione nel campo del NAC: ogni vendor ha la sua soluzione e la sua definizione di cosa significhi fare il controllo dei dispositivi che accedono alla rete, e nessuna di queste soluzioni (o molto poche) sono davvero interoperabili. Quali sono le vulnerabilità e i rischi che derivano agli utenti da questa situazione? Quali sono le falle che un aggressore potrebbe sfruttare? Quali sono gli standard emergenti e le possibili soluzioni?

14.50 ***Trusted Computing: non solo DRM ma anche fiducia e sicurezza*** – Antonio Lioy, Politecnico di Torino

Un numero crescente di produttori hardware stanno offrendo sistemi dotati di un chip di sicurezza aderente agli standard definiti dal TCG (Trusted Computing Group): il TPM (Trusted Protection Module). Spesso accompagnato dalla cattiva fama di "grande fratello" per il suo possibile uso come strumento di controllo dei copyright digitali (DRM, Digital Rights Management) il TPM può però essere anche usato per creare sistemi sicuri e fidati, con la possibilità di estendere queste proprietà anche ad applicazioni di rete quali le transazioni di commercio elettronico.

15.40 ***IDS Intrusion Detection System: nuove frontiere*** – Stefano Zanero, Politecnico di Milano

Perché i sistemi di intrusion detection di oggi non funzionano?

Si ragionerà a voce alta, in modo estremamente pragmatico, su quali siano i limiti delle tecnologie di oggi, e quali invece possano essere le promettenti evoluzioni nel campo della ricerca. Dovendo affrontare oggi il tema, come valutare un sistema di IDS adeguato alla nostra realtà, che possa evolversi senza tramutarsi in un fallimento?

16.30 Presentazione dei risultati dell'esperimento ***"Il tuo cellulare, proprio il tuo...e' al sicuro ?"*** condotto durante la giornata da **Luca Caretoni e Claudio Merloni, Secure Network**

Dopo essere andati a spasso per Milano con un trolley blu modificato e trasformato in un laboratorio mobile per lo studio della sicurezza Bluetooth (interessante esperimento che ha incuriosito e appassionato la stampa di mezzo mondo), i due ricercatori mostreranno dal vivo cosa significa subire un attacco a un dispositivo mobile scelto a caso tra quelli in platea.

17.00 Dibattito

17.30 Fine dei lavori



### Data, Sede e Orari

**Milano, 1 dicembre 2006**  
**AC Hotel - Via Tazzoli, 2 - Tel. 02/20424211 - Orari: 9.00 – 17.30**

L'hotel è raggiungibile dalla Stazione Centrale con il **tram 33** - direzione Cacciatori delle Alpi per 9 fermate, scendendo alla fermata Ferrari-Farini. L'hotel è a 100 metri a piedi. Davanti l'ingresso dell'hotel c'è la fermata del Passante Ferroviario che collega la città e l'hinterland Milanese. Dallo stesso Passante si può raggiungere la fermata della metropolitana Garibaldi.

La tariffa convenzionata con Teach per il pernottamento presso AC Hotel è di **130 Euro** camera doppia uso singola che prevede prima colazione, mini bar e centro fitness inclusi nel prezzo.

### Quota di iscrizione

**Euro 490 + iva 20%**  
**PER LE ISCRIZIONI CHE PERVERRANNO ENTRO IL 16 NOVEMBRE LA QUOTA DI ISCRIZIONE SARA' DI 390 EURO + IVA**

La quota comprende gli atti dell'evento, la colazione di lavoro e il coffee break. Nel caso di iscrizioni multiple da parte della stessa Azienda o Ente, verrà praticato lo sconto del 20% a partire dalla terza partecipazione compresa.

### Modalità di iscrizione

Prenotazione telefonica alla quale dovrà seguire via fax o per posta la scheda di iscrizione a seguito della quale verrà spedita via fax o per e-mail conferma dell'avvenuta iscrizione. Il pagamento dovrà avvenire entro l'inizio dell'evento. In caso contrario i partecipanti non saranno accolti in aula.

### Modalità di pagamento

- Assegno bancario o circolare
- Bonifico bancario intestato a Between Spa - CASSA DI RISPARMIO DI PARMA E PIACENZA Agenzia 12 Milano - Codice IBAN IT 54 – CIN J – N. CONTO CORRENTE 000056695695 ABI 06230 –CAB 01600

### Condizioni generali

In caso di rinuncia scritta pervenuta almeno cinque giorni prima dell'inizio dell'evento verrà addebitato il 50% della quota; per quelle pervenute successivamente verrà addebitato il 100%.

Qualora l'evento, per qualsiasi causa, venisse cancellato, la responsabilità di Between si intende limitata al rimborso delle quote di iscrizione già pervenute. In caso di controversie il Foro competente sarà quello di Milano

### Segreteria organizzativa

Fathea El Bendary – Tel. 02.855.00.555 – [fathea.elbendary@between.it](mailto:fathea.elbendary@between.it)  
Via Broletto 37 – 20121 Milano - [www.teach.it](http://www.teach.it)



## Scheda di iscrizione

da fotocopiare e spedire via fax al nr. 02.855.00.558

Cognome ..... Nome .....

Società.....

Posizione ricoperta in Azienda .....

Direzione/Funzione di appartenenza .....

e-mail .....

Telefono ..... Fax .....

Sede di lavoro .....

Via ..... Città ..... CAP .....

### MODALITÀ DI PAGAMENTO

assegno circolare o bancario  bonifico bancario\*

\* Intestare bonifico a: Between Spa - Cassa di Risparmio di Parma e Piacenza, Ag.12 - Milano CODICE IBAN IT 54 CIN J c/c 000056695695 - ABI 06230 CAB 01600 - nella causale si prega di indicare il titolo del corso

### INTESTARE LA FATTURA A

Società .....

Via ..... Città .....CAP .....

C.F. / P.IVA .....

Indicare eventuale riferimento da inserire in fattura .....

In caso di Ente Pubblico **esente IVA** indicare articolo di esenzione .....

### SPEDIRE LA FATTURA A

c.a. ....

Via ..... Città ..... CAP .....

Le iscrizioni verranno accettate secondo l'ordine cronologico di arrivo. Ogni eventuale disdetta deve essere comunicata via fax al n. 02.855.00.558. Nel caso di rinuncia scritta pervenuta fino a 7 giorni lavorativi prima dell'inizio dell'evento, non si dovrà alcun corrispettivo. Nel caso di rinuncia scritta pervenuta dopo il suddetto limite verrà addebitato il 100% della quota. In caso di cancellazione dell'evento, per qualsiasi causa, la responsabilità si intende limitata al rimborso delle quote di iscrizione già pervenute. La documentazione distribuita agli eventi è concessa in utilizzo a BETWEEN Spa dai docenti e pertanto non potrà essere diffusa senza autorizzazione.

data timbro e firma

.....