



OWASP - Italy Day III

Web Application Security: research meets industry

23 Feb 2009



Organizzato da
OWASP-Italy e Daisy-Net nodo
pugliese del Centro di Competenza ICT Sud

Ospitato da
Dipartimento di Informatica
Università degli Studi di Bari

Per ulteriori informazioni e registrazione **gratuita** visitare:
www.owasp.org/index.php/Italy_OWASP_Day_3



8:30h	Registrazione
9.00h	"Accoglienza e apertura dei lavori" Prof. Giuseppe Visaggio - Università di Bari - Presidente del Centro di Competenza ICT-Puglia
9.20h	"Introduzione all'OWASP-Day III" Matteo Meucci - OWASP-Italy Chair, CEO Minded Security
09.45h	"Trusted Computing: tecnologia ed applicazione alla protezione del web" Prof. Antonio Lioy - Politecnico di Torino
10.30h	Coffee Break
11.00h	"L'implementazione di un modello di sicurezza in ambito bancario: l'esperienza di ABN AMRO" Manuele Cavallari - Responsabile IT Security Office Consorzio Operativo Gruppo MPS
11.30h	"Analisi forense dopo un cyber attack" Ass. Davide Gabrini - Analista forense presso il Compartimento Polizia Postale e delle Comunicazioni di Milano
12.15h	"A Software Security Maturity Model" Brian Chess - Chief Scientist at Fortify Software
13.00h	Business Lunch
14.00h	"Http Parameter Injection" Stefano Di Paola - CTO Minded Security
14.30h	"SHIELDS: metrics, tools and Internet services to improve security in application developments" Domenico Rotondi, Alessandra Bagnato, Eva Coscia, Cinzia Rubattino - TXT
15.00h	"Secure Code Review: dalla teoria alla pratica" Antonio Parata - Security Consultant Emaze
15.30h	Coffee Break
16.00h	"Automatic Generation of Test Cases for Web Application Security: a Software Engineering Perspective" Prof. Corrado Aaron Visaggio - Università del Sannio
16.30h	"Harden your Java Components!" Pierre Parrend - SE FZI Karlsruhe
17.00h	Tavola rotonda: "La ricerca nella Web Application Security, qual è lo stato dell'arte?" Quali progetti/iniziativa per aiutare le aziende a creare applicazioni più sicure e a difendersi da nuove forme di attacchi? Cosa sta facendo l'Università in tal senso? Quanto sono vicini il mondo aziendale al mondo accademico?"
Partecipanti: Danilo Calvano - Università di Bari - SER&P Practices srl, Corrado Aaron Visaggio - Università del Sannio, Giorgio Fedon - COO Minded Security, Mauro Bregolin - Kima Moderatore: Matteo Meucci	

Dopo il successo dell'**OWASP-Italy Day II** tenutosi a ROMA nel 2008, il 23 Febbraio 2009 si terrà a Bari l'**OWASP-Italy Day III**.

Obiettivi:
OWASP (The Open Web Application Security Project) è una comunità mondiale che si pone l'obiettivo di accrescere la sicurezza delle applicazioni software. La strategia OWASP è rendere "visibile" la sicurezza delle applicazioni, consentendo a utenti e imprese di assumere decisioni ponderandone i rischi. La partecipazione alla community OWASP è aperta a tutti e i suoi prodotti sono disponibili con licenza gratuita. Gli OWASP Days rappresentano, a livello mondiale, un momento di confronto sul Web Application Security. L'**OWASP-Italy Day III**, in particolare, si focalizzerà sul tema: "Web Application Security: research meets industry".

Temi di interesse:
I Temi dell'**OWASP-Italy Day III** includono, ma non sono limitati a:

- * L'evoluzione di attacchi e contromisure per la sicurezza nelle Applicazioni Web.
- * Casi di studio ed esperienze sull'adozione delle linee guida OWASP.
- * Modelli per la verifica e certificazione della sicurezza delle applicazioni software.

Programma:

OWASP-Italy Day III avrà durata di un giorno. Durante la conferenza si presenteranno contributi ed esperienze in tema di sicurezza delle applicazioni web con l'obiettivo di stimolare la discussione, il confronto e lo scambio di opinioni tra i partecipanti.

La giornata prevede:

- * 3 interventi su invito da parte di esperti del settore.
- * Presentazioni di contributi ed esperienze seguite da momenti di dibattito.
- * Una tavola rotonda al termine della giornata, che vedrà il coinvolgimento di ospiti internazionali, e riprenderà approfondendo gli argomenti più significativi emersi nel corso dell'evento.
- * due coffee break (alle ore 10:30 e alle ore 15:30) e un business lunch (ore 13:00).

Il programma dettagliato della conferenza è disponibile sul sito www.owasp.org.

INTERVENTI SU INVITO:

INTERVENTO 1

TITOLO : Trusted Computing: tecnologia ed applicazione alla protezione del web.

Relatore

Prof. Antonio Lioy (Politecnico di Torino)

Abstract

Il modello del Trusted Computing (TC) si basa sulla disponibilità di un componente hardware a basso costo (il TPM, Trusted Platform Module) in grado di garantire un elevato grado di fiducia circa le applicazioni attivate su un computer. Basandosi su questo elemento - già disponibile su moltissimi PC ed anche su alcuni server - il progetto Open-TC ha sviluppato una piattaforma open-source in grado di migliorare la protezione delle più comuni applicazioni. Dopo una rapida panoramica sulle principali caratteristiche del TC, verrà presentata una sua possibile applicazione ad un sistema di Internet banking basato su web.

Curriculum

Antonio Lioy è Professore Ordinario di Sistemi di Elaborazione presso il Dipartimento di Automatica e Informatica del Politecnico di Torino, ove guida il gruppo di ricerca TORSEC attivo nella protezione delle reti e dei sistemi informatici. A partire dal 1996 questo gruppo ha preso parte ad innumerevoli progetti di sicurezza a livello italiano e soprattutto europeo. Tra i più importanti e recenti si citano i seguenti:
OpenTC per lo sviluppo di un sistema di Trusted Computing su piattaforma "open" basata su Linux. **Desiree** per l'adozione di metodologie e strumenti volti ad incrementare la dependability di un sistema ICT, in un'ottica di Critical Infrastructure Protection; **Stork** (2008-2010, EC) per l'interoperabilità dei sistemi di identificazione elettronica (e-ID) in Europa e lo sviluppo di servizi elettronici trans-frontalieri basati su di essi.

Il Prof. Lioy è autore di circa 100 articoli scientifici e tecnici, è iscritto all'Ordine degli Ingegneri di Torino ed è un membro della IEEE e della IEEE Computer Society. Dal giugno 1999 è revisore della Commissione Europea per i progetti di ricerca e sviluppo nel settore della sicurezza informatica, sia per la valutazione delle proposte sottoposte alla Commissione sia per il controllo dell'esecuzione dei progetti finanziati. Dal settembre 2002 è Presidente di AssoSecurity, un'organizzazione senza fini di lucro per la diffusione della sicurezza informatica in ogni aspetto del settore ICT. Dal settembre 2007 il Prof. Lioy è un membro del PSG (Permanent Stakeholders' Group) di ENISA (la European Network and Information Security Agency della UE).

INTERVENTO 2

TITOLO: Il modello della sicurezza di ABN AMRO, caratteristiche ed esperienze d'uso.

Relatore

Dott. Manuele Cavallari - Consorzio Operativo Gruppo Montepaschi

Abstract

Il modello della sicurezza di ABN AMRO è un modello particolarmente maturo e la sua implementazione in Banca Antonveneta è stata molto importante. Ovviamente il percorso è

stato irto di difficoltà ed ostacoli, ma ha portato benefici notevoli. Si illustrerà, nel corso di questo intervento, sia il modello -orale di ABN AMRO, sia le problematiche affrontate sul campo per la sua implementazione presso Banca Antonveneta. Sinteticamente, i punti salienti dell'intervento saranno:
- Le componenti del modello di sicurezza ABN AMRO
- Risk Management come fulcro della sicurezza
- Implementazione del processo di Risk Management in Banca Antonveneta

Curriculum

Nato a Roma nel 1965, e laureato in Economia e Commercio, ha focalizzato la sua attività lavorativa sull'Information Security, ottenendo, tra l'altro le certificazioni CISA e CISM di ISACA, nonché recentemente LoCSI di AIPSI. Dal 1990 al 2000 circa ha lavorato presso la Guardia di Finanza, collaborando, tra l'altro, con il Servizio Centrale Ispettori Tributarie del Ministero delle Finanze nell'ambito delle prime iniziative tese a conoscere e regolamentare il commercio elettronico. Nel periodo 2000-2007 è passato alla libera professione, formando consulenza in materia di sicurezza IT a diverse realtà aziendali (a titolo di esempio: BPM Gestioni Sgr, Datasiel, Banca di Roma e Capitalia, BNL, Procura presso il Tribunale di Alessandria). In questo periodo ha collaborato con l'Università Cattolica del Sacro Cuore di Milano, insegnando presso la Facoltà di Scienze Bancarie e di Economia, le materie Informatica Generale e Informatica 2. Altre iniziative di docenza lo hanno visto impegnato con Banca Intesa, BPM Gestioni Sgr, Fondo Sociale Europeo. Verso la metà del 2007, è stato assunto presso Banca Antonveneta in qualità di Responsabile dell'IT Security Office con il compito di implementare il modello di sicurezza della capogruppo ABN AMRO. Da settembre 2008, a seguito della fusione di Banca Antonveneta con MPS, fa parte del Consorzio Operativo del gruppo MPS, con mansioni varie nell'ambito del Servizio Sicurezza.

INTERVENTO 3

TITOLO: Analisi Forense dei Sistemi Compromessi.

Relatore

Ass. Davide Gabrini - Analista forense presso il Compartimento Polizia Postale e delle Comunicazioni di Milano

Abstract

L'intervento punta ad illustrare i concetti chiave della computer forensics come attività complementare all'incident response nei casi di sistemi violati. Dopo aver introdotto i principi fondamentali della materia, sarà illustrato il come individuare e preservare le "evidenze" in maniera idonea alla loro presentazione in sede processuale; infine verranno messe a confronto alcune statistiche in materia di sicurezza ed evidenziate alcune problematiche investigative che caratterizzano l'attuale scenario.

Curriculum

Davide Gabrini nell'ultimo decennio si è occupato di reati informatici e, in particolare del contrasto ai crimini informatici in senso proprio, alla pedopornografia (anche tramite operazioni sotto copertura) e al terrorismo, prendendo parte ad importanti indagini di rilievo nazionale. Attualmente lavora per la Polizia Postale di Milano e si occupa prevalentemente di ricerca e sviluppo, computer forensics e formazione del personale.

