ISACA
Trust in, and value from, information systems
Venice Chapter

Application Security: internet, mobile ed oltre

in collaborazione con

OWASP
The Open Web Application Security Project

Università Ca'Foscari Venezia

Dipartimento di Scienze Ambientali Informatica e Statistica

Venerdì 3 ottobre 2014 - Orario: 9:30 - 17:30
Auditorium Santa Margherita
Campo Santa Margherita
VENEZIA

Alcuni commenti all'edizione 2013

"Una relazione interessante che finalmente presenta un caso concreto di forensic. Ottime le indicazioni pratiche che ho potuto trarre."

"Un buon mix fra nuove idee ed esperienze pratiche. Veramente utile."

"Argomenti di attualità che mi interessano per la mia attività"

"Poca teoria e molte esperienze. E' interessante vedere cosa fanno gli altri concretamente".

CPE

CPE acquisibili: fino a 8 ore

Comitato scientifico e organizzatore

Mauro Bregolin, Roberto D'Orsi, Riccardo Focardi, Orillo Narduzzo.

LA PARTECIPAZIONE E' GRATUITA,

per l'iscrizione compilare la scheda e inviarla a **ISCRIZIONI@ISACAVENICE.ORG**

Per motivi organizzativi i partecipanti saranno avvisati con mail di conferma.

ISACA VENICE Chapter si riserva la facoltà di apportare qualsiasi modifica al programma dell'evento.

L'Auditorium Santa Margherita è un edificio storico del IX secolo, ora adibito a teatro, un tempo chiesa dedicata a Santa Margherita. Degli affreschi che la ornavano, resta il pregiato dipinto del soffitto raffigurante il martirio della santa. Il campo omonimo in cui è collocato è uno dei luoghi più vivi della città, in posizione facilmente e velocemente raggiungibile da Piazzale Roma e dalla stazione ferroviaria.

Application Security: internet, mobile ed oltre

Programma

VENERDI' 3	**ORE 9.30-17.30**
Chairman	Mauro Bregolin, ISACA VENICE Chapter, Resp. programma
Benvenuto	Orillo Narduzzo, Presidente ISACA VENICE Chapter Matteo Meucci, Presidente OWASP Italia Riccardo Focardi, Informatica Università Ca' Foscari di Venezia
Saluto delle Autorità	Michele Bugliesi, Rettore Università Ca' Foscari di Venezia
Stefano Calzavara *Università Ca' Foscari*	Protezione client-side per sessioni web
Key notes Christian Martorella *Skype*	A journey into Application Security *(intervento in lingua inglese senza traduzione)*
Marco Balduzzi *Trend Micro*	(In)security of smart transportation at sea, the Automated Identification System (AIS)
Gianfranco Tonello *TG Soft*	Evoluzione dei malware in ambiente Android: dalle metodologie di infezione alle tecniche di difesa
	CSX - CYBERSECURITY NEXUS - Risorse da ISACA per i professionisti della cybersecurity
Marco Squarcina *Università Ca' Foscari*	Laboratorio On-Line di Ethical Hacking
Lorenzo Nicolodi, Guido Ronchetti *IKS*	La sicurezza delle app mobile in Italia: uno scenario tutt'altro che rassicurante
Key notes Matteo Meucci *OWASP, Minded Security*	Il nuovo standard OWASP per la verifica della sicurezza delle applicazioni web
Gianluca Salvalaggio *Consorzio Triveneto-Bassilichi*	SSL, se non ci fosse bisognerebbe (re)inventarlo

Destinatari Professionisti nel settore IT: CIO, CISO, CTO, Responsabili applicazioni mobile, Sviluppatori, Progettisti, Architetti di sistemi, Auditor, Responsabili della sicurezza delle informazioni, Consulenti, IT Risk Manager.

ABSTRACT

Key notes

A journey into Application Security
Christian Martorella - Skype

A Product security team journey facing the challenges of a fast changing environment and market. How application security has transformed during the years, from Waterfall to Agile and the adoption of Cloud services and the "Devops" model.

Il nuovo standard OWASP per la verifica della sicurezza delle applicazioni web
Matteo Meucci: OWASP / Minded Security

L'intervento presenterà per la prima volta la versione 4 dell'OWASP Testing Guide, uno strumento Open Source che rappresenta lo standard de facto per realizzare un'attività di verifica della sicurezza delle applicazioni web.

Relazioni

Protezione client-side per sessioni web
Stefano Calzavara, Università Ca' Foscari

L'autenticazione su web è notoriamente vulnerabile ad un ampio spettro di attacchi differenti ed è sorprendentemente difficile da rendere sicura. Per questi motivi una recente linea di ricerca propone di proteggere le sessioni web a client-side, vale a dire estendendo il browser con dei meccanismi di sicurezza in grado di prevenire il rischio di "session hijacking", anche qualora i web developer non adottino le pratiche di sicurezza normalmente consigliate per l'autenticazione su Web. In questo talk presenterò una panoramica delle principali problematiche di sicurezza delle sessioni web ed alcune recenti proposte per prevenirle a client-side. In particolare, discuterò il design e la valutazione sperimentale di CookiExt, un'estensione di Google Chrome atta a migliorare in modo automatico la sicurezza delle sessioni web basate su cookie. Concluderò il mio intervento con alcune brevi considerazioni sulla scalabilità delle tecniche di protezione client-side rispetto ad una più vasta gamma di attacchi.

(In)security of smart transportation at sea, the Automated Identification System (AIS)
Marco Balduzzi, Trend Micro

L'"automated identification system" (AIS) è stato introdotto in anni recenti, in aggiunta alle convenzionali installazioni radar, per migliorare la localizzazione del traffico marittimo ed incrementarne la sicurezza.
L'AIS, che è obbligatorio per le navi passeggeri e le navi oltre le 300 tonnellate, opera acquisendo le coordinate via GPS e scambiando informazioni di posizione e rotta con navi limitrofe, installazioni offshore, porti e sistemi di controllo del traffico, nonché provider di tracciamento e visualizzazione su Internet.
Con un numero stimato di 400.000 installazioni, l'AIS è attualmente il miglior sistema di ausilio alla navigazione, sicurezza marittima anti collisione e di investigazione di incidenti.
Nella nostra ricerca su AIS abbiamo identificato numerose vulnerabilità sia nel protocollo usato nelle comunicazioni in radiofrequenza che nell'implementazione dei servizi AIS, che interessano tutti i transponder installati a livello mondiale. In questa presentazione condivideremo i nostri risultati, ossia come siamo stati in grado di dirottare ed eseguire attacchi man-in-the-middle di navi, controllare comunicazioni AIS, manipolare comunicazioni con i principali tracking provider, fino a impersonare un nostro yacht fittizio!

Evoluzione dei malware in ambiente Android: dalle metodologie di infezione alle tecniche di difesa
Gianfranco Tonello, TG Soft

L'intervento ha come obiettivo quello di presentare al pubblico lo stato dell'arte dei malware che colpiscono il sistema operativo Android, e di suggerire comportamenti base quotidiani che permettono di evitare di cadere vittime di tali malware. Verrà inizialmente introdotta l'architettura del sistema operativo Android (in modo semplificato) e le principali tipologie di malware Android. Successivamente, verranno introdotte le principali metodologie di infezione utilizzate, con esempi reali e, per ognuna di queste metodologie, verranno presentati comportamenti adatti ad evitare l'infezione e/o a contrastarla efficacemente.

Laboratorio On-Line di Ethical Hacking
Marco Squarcina, Università Ca' Foscari, Venezia

L'effettiva protezione dei sistemi informatici richiede un'adeguata conoscenza delle tecniche e dei metodi utilizzati dagli attaccanti. Le competizioni di sicurezza informatica di tipo "Capture the Flag" (CTF) si inseriscono in tale contesto, rappresentando l'occasione per i partecipanti di fare esperienze "hands-on" nella difesa e nell'attacco di servizi informatici realistici in un ambiente protetto e legale. In questo intervento viene presentata una piattaforma per la realizzazione di CTF interamente on-line e il suo impiego nel laboratorio del corso magistrale di Security of Computer Systems dell'Università Ca' Foscari di Venezia.

La sicurezza delle *app mobile* in Italia: uno scenario tutt'altro che rassicurante
Lorenzo Nicolodi e Guido Ronchetti, IKS

L'intervento partirà da alcuni esempi per descrivere uno scenario preoccupante: le applicazioni mobile italiane sono tutt'altro che sicure. Il report annuale sulla sicurezza delle app mobile curato da IKS e giunto alla edizione 2014, permetterà di presentare, rispetto ad alcuni indicatori critici, su di un campione rappresentativo, debolezze diffuse e pratiche consolidate. Verranno affrontate le soluzioni tecnologiche possibili e come prevenire la distribuzione di app vulnerabili tramite analisi e linee guida di sviluppo sicuro.

SSL, se non ci fosse bisognerebbe (re)inventarlo
Gianluca Salvalaggio, Consorzio Triveneto Bassilichi

Il protocollo SSL/TLS garantisce la sicurezza e la privacy delle principali comunicazioni su Internet: siti di e-commerce, servizi di webmail, home banking, etc etc. Dopo una breve descrizione dei principi di funzionamento, vengono presentati gli attacchi che in questi ultimi anni hanno sfruttato vulnerabilità architetturali o implementative del protocollo.

BREVI NOTE PERSONALI SUI RELATORI

Christian Martorella, Skype

Christian Martorella has been working in the field of Information Security for the last 14 years, currently working in the Product Security team at Skype, Microsoft. Before he was the Practice Lead of Threat and Vulnerability, for Verizon Business, where he led a team of consultants delivering Security testing services in EMEA for a wide range of industries including Financial services, Telecommunications, Utilities and Government. He is cofounder and an active member of Edge-Security team, where security tools and research is released. He presented at Blackhat Arsenal USA, Hack.Lu, What The Hack!, NoConName, FIST Conferences, OWASP Summits and OWASP meetings. Christian has contributed with open source assessment tools like OWASP WebSlayer, Wfuzz, theHarvester and Metagoofil. He likes all that is related to Information Gathering and offensive security.

Matteo Meucci, OWASP / Minded Security

Matteo Meucci è CEO di Minded Security, la Software Security Company dove è responsabile della direzione strategica e di sviluppo del business. Prima di fondare Minded Security, Matteo ha avuto diverse
esperienze lavorative in BT Global Services, INS, Business-e e CryptoNet. Matteo ha più di 13 anni di esperienza in sicurezza appplicativa e collabora da diversi anni al progetto OWASP. Ha fondato OWASP-Italy nel 2005 ed è responsabile del progetto OWASP Testing Guide dal 2006. Matteo viene invitato come relatore a numerosi eventi in tutto il mondo parlando di Web Application Security. Matteo è laureato in Ingegneria Informatica presso l'Università di Bologna.

Stefano Calzavara, Università Ca' Foscari

Stefano Calzavara ha conseguito la laurea magistrale ed il dottorato di ricerca in Informatica presso l'Università Ca' Foscari di Venezia. Il suo principale ambito di ricerca sono i metodi formali per la definizione e la verifica di proprietà di sicurezza di sistemi software. Stefano è autore di varie pubblicazioni su atti di importanti conferenze internazionali; il suo articolo "Logical foundations of secure resource management in protocol implementations" ha vinto il best paper award per la teoria nell'edizione 2013 di ETAPS.

Marco Balduzzi, Trend Micro

Marco Balduzzi ha conseguito un Ph.D. in sicurezza IT applicata presso Télécom ParisTech ed un M.Sc. in computer engineering all'Università di Bergamo. Si occupa di sicurezza IT da oltre 10 anni, con esperienze internazionali nell'industria e in ambiente accademico. Prima di far parte dell'International Secure Systems Lab e poi come senior research scientist di Trend Micro Research ha svolto lavori di consulenza per varie società a Milano, Monaco e Sophia-Antipolis.
Tra i suoi principali interessi di computer security vi sono browser security, code analysis, botnets detection, cybercrime investigation, privacy and threats in social networks, malware e IDS.

Relatore a conferenze specializzate come Black Hat, Hack In The Box, OWASP AppSec, i lavori delle sue ricerche sono stati pubblicati in conferenze quali NDSS, RAID, DIMVA e diffuse su Forbes, MIT Technology Review, The Register, Slashdot, Info World, Dark Reading, CNN e BBC.

Gianfranco Tonello, TG Soft

Gianfranco Tonello è IT Security Researcher & Software Developer Manager e Direttore del C.R.A.M. Centro Ricerche Anti-Malware di TG Soft. Ha iniziato a studiare virus/malware informatici in ambiente Ms-Dos, da autodidatta, nel 1989 riuscendo a comprenderne il funzionamente e mettere a punto codici per la loro univoca identificazione e corretta rimozione. Dal 1992 è consulente di alcuni dei maggiori gruppi bancari italiani per la gestione/soluzione delle più complesse problematiche derivanti da virus/malware di nuova generazione. Ha collaborato con il prof. Klaus Brunnestein dell'Università di Amburgo nell'ambito di ricerche e analisi sui virus/malware di nuova geneazione. Dirige i gruppi di lavoro che si occupano di sviluppare il software AntiVirus-AntiSpyware-AntiMalware per Windows Vir.IT eXplorer e le App per Android CRAM App Analyser applicazione diagnostica che permette di individuare App potenzialmente malevole ed inviarle al C.R.A.M. per l'analisi e VirIT Mobile Security –AntiMalware per Android- applicazioni liberamente prelevabili da Google Play Store. Gianfranco Tonello è autore di numerose analisi su virus/malware informatici sia in ambiente Windows sia in ambiente Android di nuova generazione pubblicate su alcune della più note riviste del settore, su blog e newsletter.

Marco Squarcina, Università Ca' Foscari, Venezia

Marco Squarcina è Dottore Magistrale in informatica e membro del gruppo di ricerca in "information security" presso l'Università Ca' Foscari di Venezia. È assistente alla didattica per il corso di "security of computer systems" e team leader dei c00kies@venice, squadra con la quale partecipa a competizioni internazionali di "ethical hacking". Svolge saltuariamente l'attività di consulente su tematiche di sicurezza informatica.

Lorenzo Nicolodi, IKS

Ha conseguito la Laurea in Informatica Applicata presso la Libera Università di Bolzano nel 2006, maturando parallelamente fin da subito esperienza lavorativa, presso importanti aziende del nord Italia e, in seguito, come freelancer, supportando forze dell'ordine, private, aziende ed istituti di ricerca negli ambiti della sicurezza e delle investigazioni digitali. Attualmente impegnato nel Team di sviluppo applicativo IKS nelle valutazioni di sicurezza di applicazioni mobile Android e nella ricerca e sviluppo associata, si interessa anche di protocolli di sicurezza, malware e l'ecosistema ad essi connesso.

Guido Ronchetti, IKS

Laureato in Informatica presso l'Università degli Studi di Milano. Sviluppatore specializzato su piattaforme Apple iOS e Mac OSX: dal 2009 segue per Dysto Productions lo sviluppo di alcuni prodotti, per il mercato consumer, specializzandosi sulle capacità di sicurezza dei frameworks Apple. Con IKS dal 2012 segue le attività di assessment mobile e i progetti di sviluppo iOS in ambito security; tra i quali SMASH OTP e SMASH Mobile.

Gianluca Salvalaggio, Consorzio Triveneto Bassilichi

CISSP. Laureato in Ingegneria e in Informatica. Lavora da più di dieci anni nel campo dell'Information Security e attualmente ricopre il ruolo di Responsabile della Sicurezza delle Informazioni presso Triveneto Bassilichi. È docente in corsi specialistici di networking e di Sicurezza Informatica.

SPONSOR E SOSTENITORI DI ISACA VENICE CHAPTER

SECSERVIZI

Sostenitore Platinum

KPMG cutting through complexity

Sponsor Platinum

TVB Triveneto Bassilichi

Sostenitore Platinum

con il patrocinio di

AICA Associazione Italiana per l'Informatica ed il Calcolo Automatico

aicq Associazione Italiana Cultura Qualità triveneta

CLUB TI CLUB PER LE TECNOLOGIE DELL'INFORMAZIONE TRIVENETO

FONDAZIONE INGEGNERI PADOVA

Scheda di Iscrizione
Application Security: internet, mobile ed oltre

La partecipazione all'evento è libera e gratuita ma dovrà essere prenotata con cortese anticipo, inviando la scheda di iscrizione entro Martedì 24 settembre 2014 all'indirizzo e-mail ISCRIZIONI@ISACAVENICE.ORG
Le adesioni saranno accettate fino ad esaurimento dei posti disponibili e saranno confermate con apposita mail.

DATI PERSONALI:

Cognome:

Nome:

Indirizzo:

Cap: Città Prov.

Telefono: Cell:

E-mail:

Consenso ai sensi del D. LGS. 196/2003
Ai sensi degli artt. 13 e 23 del D.lgs. 30 giugno 2003 n. 196, autorizzo ISACA Venice chapter, le organizzazioni patrocinanti e le aziende Sponsor a trattare i dati sopra riportati per la realizzazione delle proprie iniziative, quali l'invio di informazioni ed altre comunicazioni. In qualsiasi momento potrò modificare i miei dati o richiederne la cancellazione scrivendo ad ISACA Venice Chapter una e-mail a info@isacavenice.org.

Data Firma

ISACA – Information Systems Audit & Control Association E' una associazione internazionale, indipendente e senza scopo di lucro. Con oltre 100.000 associati in più di 160 Paesi, ISACA (www.isaca.org) è leader mondiale nello sviluppo delle competenze certificate, nella promozione di community professionali e nella formazione nei settori dell'assurance e sicurezza, del governo dell'impresa, della gestione dell'IT e dei rischi e della compliance in ambito IT. Fondata nel 1969, ISACA organizza conferenze internazionali, pubblica l'*ISACA Control Journal*, sviluppa standard internazionali di audit e per il controllo dei sistemi IT, che contribuiscono a facilitare il perseguimento dell'affidabilità e a trarre valore dai sistemi informativi. ISACA attesta l'acquisizione delle competenze e delle conoscenze IT mediante certificazioni riconosciute a livello internazionale quali: CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT) e CRISC (Certified in Risk and Information Systems Control). ISACA aggiorna continuamente il frame work COBIT che assiste i professionisti dell'IT e i manager delle imprese nel far fronte alle proprie responsabilità per quanto attiene l'IT governance e la gestione manageriale, in particolare nell'ambito di assurance, sicurezza, rischio e controllo e a fornire valore al business.

ISACA Venice Chapter E' un'associazione non profit costituita in Venezia nel novembre 2011 da un gruppo di professionisti del Triveneto che operano nel settore della Gestione e del Controllo dei Sistemi Informativi: è il terzo capitolo italiano di ISACA. Riunisce coloro che nell'Italia del Nord Est svolgono attività di Governance, Auditing e Controllo dei Sistemi Informativi promuovendo le competenze e le certificazioni professionali sviluppate da ISACA. L'associazione favorisce lo scambio di esperienze, promuove un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo sia di affidabilità dell'organizzazione sia di sicurezza dei sistemi.

OWASP (www.owasp.org) è un'organizzazione no profit presente a livello internazionale, focalizzata sul miglioramento della sicurezza del software. La partecipazione ai progetti OWASP è libera, come lo è l'accesso ai materiali prodotti dai progetti di OWASP, che sono rilasciati sotto una licenza open.
Tra le iniziative più conosciute di OWASP si segnalano la OWASP Top Ten, l'OWASP Testing Project (che ha reso disponibile una Testing Guide per la valutazione della sicurezza di applicazioni web), nonchè il rilascio di tool specifici per il testing.

Il Dipartimento svolge attività di ricerca in informatica nell'ambito di progetti di rilevanza nazionale ed internazionale i cui risultati permettono la predisposizione di un'offerta didattica che include l'intera filiera della formazione, dalla Laurea Triennale (in lingua italiana) alla Laurea Magistrale e al Dottorato (in lingua inglese).
Le attività nell'ambito della computer and information security sono svolte dal personale docente e dai ricercatori afferenti ai laboratori e gruppi di ricerca del Centro ACADIA *AdvanCes in Autonomous Distributed and Pervasive Systems*, in collaborazione con i principali istituti di ricerca italiani ed europei, tra i quali l'INRIA a Parigi, la Univ. of Saarland, con il *Center on Information Security, Privacy, and Accountability* (CISPA) di Saarbrücken, la Univ. of Southampton con il *Cyber Security Center*, l'Imperial College di Londra.
