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

V Conference on Application Security and Modern Technologies

in collaborazione con

OWASP
The Open Web Application Security Project

Università Ca'Foscari Venezia

Dipartimento di Scienze Ambientali Informatica e Statistica

Venerdì 6 Ottobre 2017

Campus scientifico dell'Università Ca' Foscari

Venezia

Obiettivi

Nella tradizione della conferenza tratteremo vari temi di sicurezza inerenti a: Cloud, BYOD, Crittografia, Android, Industry 4.0, Privacy in the Big Data era, Phishing, The Dark Web… Vedremo come queste tematiche siano oramai profondamente interconnesse.

Quest'anno siamo anche particolarmente lieti nel fornire una testimonianza di un Istituto Superiore del territorio riguardo un'esperienza nell'ambito della robotica, che ci auguriamo sia di buon auspicio per diffondere consapevolezza in nuove possibilità e necessità educative, per trovarsi preparati ad affrontare nuove sfide.

Alcuni spunti su come intendiamo intrattenervi, incuriosendovi e – forse – preoccupandovi…

Privacy in the Big Data era
Trattare dati personali sensibili in modo sicuro e conforme alle normative di privacy: dati sanitari, servizi in cloud, big data, GDPR. Mission impossible?

Cloud Security
Ci si sta progressivamente e velocemente spostando verso modelli di esternalizzazione dove infrastruttura, sistemi e possibilmente servizi sono "dematerializzati" altrove, con benefici evidenti in termini di costi di gestione, flessibilità, scalabilità. Non altrettanto evidenti, o analizzate con precisione, sono le implicazioni di sicurezza associate al paradigma cloud. Se vi parlassero di un attacco rivolto al vostro ambiente cloud il cui "goal is to secretly exfiltrate sensitive data from one fully isolated virtual machine to another virtual machine on the same physical host", vi sembrerebbe una minaccia credibile? Please read on...

Internet of Things
Tra gli 8.4 miliardi ($8.4*10^9$) di dispositivi che Gartner prevede siano connessi nel 2017 ci sono apparecchiature industriali coinvolte in processi critici. "Hacking robots" sarà una delle prossime frontiere del hacking?

Android Security
Google riporta oltre due miliardi di device Android in uso in contesti personali, aziendali e (attenzione!) misti. Le implicazioni di sicurezza sono ben comprese? Are the Android app ecosystem and security model hopelessly flawed?

Defensive and Offensive Computing
Un CTF (Capture the Flag) ed un penetration test sono classici esercizi offensivi utilizzati per affinare anche capacità difensive. Vedremo da esperienze reali come difendersi, spesso, sia molto più difficile che attaccare, e come la stessa nozione di perimetro aziendale possa essere poco compatibile con minime aspettative di sicurezza.

Applied Cryptography
Le frontiere della crittografia sono rappresentate dalla crittografia quantistica, che promette di portare innovazioni importanti. Il suo avvento potrebbe "mandare in soffitta" generazioni di algoritmi crittografici correntemente in uso ora considerati, a meno di imperfezioni implementative o di errori riguardanti aspetti di gestione organizzativa, inattaccabili. Per fare un parallelo, dopo un ventennio di onorata carriera il protocollo SSL è ormai considerato deprecato a causa di vulnerabilità di sicurezza; le evidenze riportano un'inerzia enorme riguardo le problematiche del suo aggiornamento a versioni sicure TLS. Se vi sarà una "rivoluzione critto-quantistica", siamo pronti ad affrontarne le conseguenze?

Programma

8.30 – 9.15 Registrazione	
Chairman	Mauro Bregolin, *ISACA VENICE Chapter*
Common Track Benvenuto Saluto delle Autorità	Marco Salvato *Presidente ISACA VENICE Chapter* Daniele De Martino, *Dirigente Polizia Postale e delle Comunicazioni – Veneto*
Common Track OWASP: i nuovi standard per la sicurezza applicativa	Matteo Meucci *OWASP Italia*
Common Track Thwarting Cyber Attacks: Scientific Alignment and the Italian Landscape	Roberto Baldoni *Università di Roma La Sapienza*
Common Track Robotica Educativa	Cristiano Tessarolo e Davide Bassan *ITI Galileo Ferraris*
Coffe break offerto dagli Sponsor e dai Sostenitori di ISACA VENICE	
Track 1 Hello from the Other Side: Reliable Communication over Cache Covert Channels in the Cloud	**Intervento in lingua inglese** Michael Schwarz e Manuel Weber *Graz University of Technology*
Track 2 Post-quantum cryptography, come cifreremo nel (post)futuro?	Gianluca Salvalaggio *Triveneto Bassilichi*
Track 1 Cyber-crime and attacks in the dark side of the web.	Marco Balduzzi *Trend Micro*
Track 2 Gestione della privacy e della protezione dei dati: Case Study in ambito sanitario	Andrea Praitano *Business-e*
Pranzo offerto dagli Sponsor e dai Sostenitori di ISACA VENICE	

Sessione Pomeridiana	
Common Track Saluto del Magnifico Rettore	Michele Bugliesi *Rettore Università Ca' Foscari Venezia*
Track 1 Da APK al Golden Ticket	Andrea Pierini
Track 2 Sicurezza dei Keystore	Mauro Tempesta *Università Ca' Foscari Venezia*
Track 1 Cloak & Dagger: From Two Permissions to Complete Control of the UI Feedback Loop	**Intervento in lingua inglese** Yanick Fratantonio *University of California, Santa Barbara*
Track 2 RuCTF Debriefing	Francesco Palmarini *Università Ca' Foscari Venezia*
Coffe break offerto dagli Sponsor e dai Sostenitori di ISACA VENICE	
Common Track Hi robot, can I hack you? A journey into industrial robots security vulnerabilities, risks, and solutions	Federico Maggi *Trend Micro*
17.15 Conclusione	

Destinatari

Professionisti nel settore IT, Auditor, IS Auditor, Addetti ai Sistemi Informativi, Addetti alla Sicurezza delle informazioni, Responsabile della sicurezza delle informazioni, Consulenti, IT Risk Manager, Responsabile Qualità dei Dati, Responsabile Rischi Operativi, Studenti universitari o Neolaureati.

Logistica

Sede: Campus scientifico dell'Università Ca' Foscari Venezia - Auditorium ed. Alfa, Via Torino 155, **Venezia Mestre**

Alcune presentazioni sono organizzate su due tracce distinte (specificate come *Track 1* e *Track 2* nella programmazione), in due sale attigue del Campus.
La partecipazione alle tracce è libera, ad esaurimento posti disponibili.
La sala *Common Track* coincide con la sala *Track 1*.

Le presentazioni, salvo dove indicato, saranno in lingua italiana.

Data: venerdì 6 Ottobre 2017

Orario: 9:15 – 17.15

Iscrizioni

La partecipazione è **gratuita**, previa iscrizione soggetta a conferma.

Per registrarsi all'evento utilizzare la mail di invito ricevuta entro il 26/9/2016.

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.

CPE

L'evento permette di acquisire 7 ore CPE per le certificazioni CISA, CISM, CGEIT, CRISC, ISO27000LA, CSSP.

ABSTRACT

Cyber-crime and attacks in the dark side of the web

Marco Balduzzi

The dark-web including TOR, FreeNet and I2P, is that part of the Internet that is not indexed by traditional search engines and where anonymity and confidentiality is enforced at the root. For these characteristics, cyber-criminals started abusing the dark-web to conduct illicit or malicious activities like illegal trading, malware hosting, and more recently targeted attacks. In this talk, we explore the cyber-criminal ecosystem in the dark-web and provides insights on its activities against hidden services and other users.

Robotica Educativa

Davide Bassan e Cristiano Tessarolo

La diffusione e lo studio delle scienze informatiche tra i più giovani è ad oggi una sfida per i docenti che cercano di coltivare fantasia e creatività, fornendo al tempo stesso basi scientifiche e metodi di ricerca. Un aiuto concreto tra le varie attività formative è la robotica educativa che grazie all'applicazione dei fondamenti della materia, dà la possibilità di affrontare in prima persona problemi reali.

Nel nostro caso, l'attivazione di un corso pomeridiano di robotica ha permesso agli studenti di realizzare un robot con l'ipotetico obbiettivo di seguire un percorso prestabilito in caso di calamità in grado di portare in salvo eventuali superstiti, denominato RescueLine. I ragazzi che hanno partecipato al progetto provenivano da classi diverse: ciò si è rivelato un ulteriore punto di forza del corso, permettendo a studenti di età diverse di collaborare tra di loro e imparare a vicenda, sotto l'ottica di uno sviluppo collettivo. Sviluppando in questo modo l'attitudine al team building e al problem solving.

Divisi in due squadre, hanno partecipato alla gara territoriale di robotica, riuscendo a classificarsi per la fase nazionale a Foligno di Robocup Junior. Dopo questo risultato gli studenti si sono sentiti particolarmente motivati evidenziando un notevole miglioramento dal punto di vista dell'apprendimento, riuscendo ad assimilare concetti e conoscenze avanzati.

Hi robot, can I hack you? A journey into industrial robots security vulnerabilities, risks, and solutions

Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Stefano Zanero

Industrial robots are complex systems used in various applications, from food packaging to critical system manufacturing. These robots aren't just "machines" but include complex embedded controllers, often connected with other computers, and to the Internet. In simple words, industrial robots are an essential component in the Industry 4.0 ecosystem. Industry-grade networking devices also play a key role, because they directly expose the robots' controller. Therefore, a simple vulnerability can have great impact, granting attackers an easy entry point. In this talk, we show how remote attackers can violate the fundamental laws that "regulate" a robot's correct operations, up to altering manufactured products, physically damage the robot, steal industry secrets, or injure humans. After covering in-depth technical aspects of our research, we will follow up with a broader discussion on the security posture of industrial routers and robots: Why these devices are attractive for attackers? What could they achieve? Are they hard to compromise? How can their security be improved?

OWASP: i nuovi standard per la sicurezza applicativa

Matteo Meucci

Il talk introdurrà il progetto OWASP e gli ultimi standard rilasciati nel corso degli ultimi mesi per quanto riguarda il mondo della sicurezza mobile, DevSecOps e ambienti di sviluppo.

Da APK al Golden Ticket

Andrea Pierini, Giuseppe Trotta

Tratto da una storia vera: BYOD, questa buzzword ormai quasi dimenticata è stata la parola chiave di un nostro penetration test.

Partendo da una campagna di phishing, dopo aver effettuato spear phishing sulla segretaria e sul suo smartphone, ci siamo intrufolati nella rete aziendale fino a diventare amministratori del dominio e sottrarre file sensibili. In questo talk spiegheremo alcuni passaggi chiave e alcune tecniche stealth utilizzate rigorosamente basate sulla nostra filosofia KISS: Keep It Simple.

Gestione della privacy e della protezione dei dati: Case Study in ambito sanitario

Andrea Praitano

L'erogazione delle prestazioni mediche, storicamente connessa alla presenza fisica del paziente presso gli ospedali, sta evolvendo verso servizi sanitari digitali, comunemente denominati *eHealth's services*. Le nuove tecnologie rappresentano un'importante opportunità per ottimizzare i costi, oggi ancora elevati, delle prestazioni sanitarie; al contempo presentano diverse criticità, a partire dalla tipologia dei dati scambiati (dati sanitari). Quando si parla di servizi sanitari digitali si ha sempre il coinvolgimento di dati sensibili di cui deve essere garantito un alto livello di tutti gli aspetti di sicurezza (RID) in un contesto, spesso, di diffidenza e di ridotta fiducia da parte del cittadino/paziente.

In questo quadro complesso nel 2015 è iniziato il progetto VisiOn (finanziato con fondi H2020) che ha definito e predisposto una piattaforma in grado restituire ai cittadini una visibilità ed un controllo sui propri dati che sono gestiti dalle organizzazioni. La piattaforma consente di ottenere il livello desiderato di controllo sui propri dati permettendo prima di andare a creare e poi monitorare e modificare un vero e proprio PLA (Privacy Level Agreement) personale fra lui e l'organizzazione. L'amministrazione o l'ospedale che usufruisce di questa funzionalità e modalità operativa potrà quindi migliorare gli aspetti di trasparenza arrivando quasi ad avere un consenso ed informativa elettronica completa e modulare (anche se non in sostituzione del consenso informato che deve seguire le modalità di legge).

Quello che si andrà a trattare nell'intervento spazierà dalla problematica della trasparenza delle informazioni fra le organizzazioni e gli interessati/pazienti; la definizione in un modo semplice di un Privacy Level Agreement fra i cittadini e le organizzazioni; il *case study* di VisiOn Privacy Platform nell'ambito del servizio di telemedicina; il PLA come *e-consent*; esperienza sull'applicazione pratica dei principi del Privacy by Design e del Privacy by Default.

Post-quantum cryptography, come cifreremo nel (post)futuro?

Gianluca Salvalaggio

I social network, le comunicazioni mobili, il cloud computing sono tutti servizi digitali che vengono messi in sicurezza adottando tecniche crittografiche ritenute mature e affidabili. Tra gli algoritmi più utilizzati citiamo RSA, Diffie-Hellman, ECC:

essi fondano la propria robustezza sulla difficoltà di risolvere determinati problemi matematici. All'orizzonte però si profila una seria minaccia per tali algoritmi: i *quantum computers*. Un quantum computer sufficientemente potente, infatti, potrebbe risolvere tali problemi in tempi relativamente brevi, rendendo così inefficaci tutti gli attuali sistemi crittografici. È necessario quindi, individuare nuovi algoritmi che possano rimanere sicuri anche in presenza di quantum computers.

Thwarting Cyber Attacks: Scientific Alignment and the Italian Landscape

Roberto Baldoni

Governance

After analyzing the relationship among domestic economy, the globalization factor and national cyberspace, the talk will address both the scientific challenges for the next 10 years to come in the multidisciplinary arena of cybersecurity and how to make a national cyberspace a safe place to install digital businesses. The talk will consider recent attack campaigns and it will discuss lessons learned. The talk finally will introduce the National Architecture for Cybersecurity including lessons learned, recent revisions and it will discuss the role of national cybersecurity research in this context. The talk contains some computer science material but it is has been conceived for a wider audience including economic, legal and geo-political aspects.

Hello from the Other Side: Reliable Communication over Cache Covert Channels in the Cloud

Michael Schwarz, Manuel Weber

Cloud Security

In this talk, we present the first practical cache covert channel in the cloud. The goal is to secretly exfiltrate sensitive data from one fully isolated virtual machine to another virtual machine on the same physical host. Both communication endpoints require no privileges and run as regular user programs.

Our attack exploits the CPU cache that is present in all modern processors. These caches are crucial to performance; they are shared across virtual machine boundaries and thus violate isolation guarantees. Cache covert channels have been discussed in many academic works; however, a practical application has not been demonstrated so far. One reason is that especially hypervisor activity and external events disrupt communication.

Our covert channel is resilient against noise as we adapt established techniques from wireless transmission protocols. Even with extraordinarily high system activity, our covert channel stays entirely error free while maintaining high throughput and low latency. We sustain transmission rates of more than 45 KB/s on the Amazon EC2 cloud, exceeding state of the art by 3 orders of magnitude. Our protocol allows us to build an SSH connection between two virtual machines, where all existing covert channels fail.

We demonstrate our covert channel attacks on the Amazon cloud by streaming a video from one virtual machine to another without producing any traffic. Finally, we present an open-source tool that helps security researchers in investigating the underlying hardware problem and assessing the risk for their infrastructure.

RuCTF Debriefing

Francesco Palmarini

Offensive computing

Le simulazioni di cyberwar in stile Capture the Flag (CTF) rappresentano ormai una consolidata realtà per testare a livello internazionale tecniche di difesa e attacco su sistemi informatici realistici. Il team di ethical hacking c00kies@venice analizza in questo talk la recente partecipazione al RuCTF 2017, uno dei contest di riferimento nel settore, evidenziando le

challenge tecniche che la squadra di Ca' Foscari ha dovuto affrontare. Vengono inoltre presentati i tool sviluppati per l'ottimizzazione del firewalling, l'analisi del traffico, monitoring dell'integrità dei servizi ed esecuzione parallela degli exploit.

Cloak & Dagger: From Two Permissions to Complete Control of the UI Feedback Loop

Yanick Fratantonio

While both the SYSTEM_ALERT_WINDOW and the BIND_ACCESSIBILITY_SERVICE Android permissions have been abused individually (e.g., in UI redressing attacks, accessibility attacks), previous attacks based on these permissions failed to completely control the UI feedback loop and thus either rely on vanishing side-channels to time the appearance of overlay UI, cannot respond properly to user input, or make the attacks literally visible. In this work, we demonstrate how combining the capabilities of these permissions leads to complete control of the UI feedback loop and creates devastating and stealthy attacks. In particular, we demonstrate how such an app can launch a variety of stealthy, powerful attacks, ranging from stealing user's login credentials and security PIN, to the silent installation of a God-like app with all permissions enabled. To make things even worse, we note that when installing an app targeting a recent Android SDK, the list of its required permissions is not shown to the user and that these attacks can be carried out without needing to lure the user to knowingly enable any permission, thus leaving him completely unsuspecting. In fact, we found that the SYSTEM_ALERT_WINDOW permission is automatically granted for apps installed from the Play Store and, even though the BIND_ACCESSIBILITY_SERVICE is not automatically granted, our experiment shows that it is very easy to lure users to unknowingly grant that permission by abusing capabilities from the SYSTEM_ALERT_WINDOW permission. We also found that it is straightforward to get a proof-of-concept app requiring both permissions accepted on the official store. We evaluated the practicality of these attacks by performing a user study: none of the 20 human subjects that took part of the experiment even suspected they had been attacked. We conclude with a number of observations and best-practices that Google and developers can adopt to secure the Android GUI.

Sicurezza dei Keystore

Mauro Tempesta

I keystore vengono utilizzati dalle applicazioni per memorizzare, in modo sicuro, le chiavi crittografiche. I keystore sono protetti da password che ne garantiscono confidenzialità e integrità, ma nella maggior parte dei casi i dettagli su come tali password siano utilizzate all'interno dei keystore non sono resi pubblici. In questa presentazione illustreremo i risultati di un'analisi effettuata su keystore reali allo scopo di valutarne il livello di sicurezza. Mostreremo come la scelta dei meccanismi interni di protezione possa fornire livelli di sicurezza molto diversi e, in particolare, come una scelta errata di tali meccanismi possa portare ad attacchi sulle chiavi crittografiche. Durante la presentazione mostreremo esempi pratici basati su keystore esistenti.

BREVI NOTE PERSONALI SUI RELATORI

Roberto Baldoni – Università di Roma La Sapienza

Roberto Baldoni is Director of the Sapienza Research Center for Cyber Intelligence and Information Security (CIS) and Director of the Cyber Security National Laboratory at Consorzio Interuniversitario Nazionale Informatica. Roberto is also the Coordinator of the National Committee for Cybersecurity Research born on February 2017 as an agreement between CNR and CINI.

At the international level he is Italian Chair of the Cyber Security Working Group of the IT-US Bilateral Science & Technology Cooperation.

Roberto is the Project Coordinator of FILIERASICURA (Securing the Supply Chain of Domestic Critical Infrastructures from Cyber Attacks). FILIERASICURA is a Research Project funded by Cisco Research and Leonardo SpA whose consortium has a critical mass of academic scientists from 8 among the most prestigious Italian Universities. He recently led the public-private working groups developing the "Cybersecurity National Framework" and the "National Cybersecurity Essentials". He also has been the founder with Camil Demetrescu of Cyberchallenge.IT. Roberto Baldoni also co-edited the Italian White Book on Cybersecurity.

Marco Balduzzi – Trend Micro

Dr. Marco Balduzzi holds a Ph.D. in applied security from Télécom ParisTech and a M.Sc. in computer engineering from University of Bergamo. His interests concern all aspect of computer security, with particular emphasis on real problems that affect systems and networks. Some topics of interest are web and browser security, code analysis, malware detection, cyber-crime, privacy, and threats in the IoT space.

With 15 years of experience in IT security, he's now with Trend Micro as senior research scientist. His work has been published in top peer-reviewed conferences like NDSS, RAID and ACSAC, and featured by distinguished media like Forbes, The Register, InfoWorld, DarkReading, BBC and CNN. He's a regular speaker at conferences like BlackHat, HITB, OWASP AppSec, and now sits in the review board of IEEE journals and venues like HITB, AppSec, eCrime and DIMVA.

Davide Bassan e Cristiano Tessarolo – ITI Galileo Ferraris

L'Istituto Tecnico Industriale Galileo Ferraris è presente da oltre 30 anni nel territorio e forma giovani allievi all'eccellenza nel campo dell'informatica, utilizzando strumenti innovativi e stimolando l'apprendimento con casi di studio pratici e moderni. L'ITI Galileo Ferraris Legalmente Riconosciuto nel 1988 per il corso Diurno e nel 1993 per il Corso Serale, nel segmento delle Scuole Superiori appartiene agli Istituti Tecnici Industriali con il Biennio Comune e il triennio di specializzazione di Informatica.

Yanick Fratantonio – University of California, Santa Barbara

Yanick Fratantonio is a Ph.D. candidate in Computer Science at the University of California, Santa Barbara, and he is soon going to join EURECOM as an Assistant Professor. His research focuses on mobile systems security and privacy. In particular, his work aims at keeping users of mobile devices safe, and it spans different areas of mobile security, such as malware detection, vulnerability analysis, characterization of emerging threats, and the development of novel practical protection mechanisms. In his free time, he enjoys playing and organizing Capture The Flag competitions with the Shellphish hacking team.

Federico Maggi – Trend Micro

Federico Maggi is a Senior Threat Researcher with Trend Micro's Forward-Looking Threat Research (FTR) team, an elite team of researchers whose mission is to fighting against cyber criminals and scouting the future of emerging technologies, striving to predict and prevent emerging security risks and threats. His research interests, mainly developed during his MSc and PhD, revolve around various topics under the "cyber security" and "cyber crime" umbrella terms, including threat analysis, malware analysis, mobile security, financial fraud analysis and detection, web- and social-network security and data analysis. Before joining Trend Micro, Federico was an Assistant Professor at Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano in Italy, where he co-directed the system-security group at the NECST Laboratory. In his career, he collaborate(d) with several research groups (e.g., UCSB, FORTH, NEU, Stony Brook, KU Leven, and RHUL), and has given several lectures and talks as an invited speaker at international venues and research schools. He also serves in the review or organizing committees of well-known conferences.

Matteo Meucci – OWASP

Matteo Meucci ha più di 16 anni di specializzazione in Application Security e collabora dal 2002 con il progetto OWASP.

Ha fondato il Capitolo OWASP-Italia nel 2005 e conduce la OWASP Testing Guide dal 2006 che è diventata lo standard de facto per realizzare un'attività di verifica della sicurezza di una applicazione, ovvero un Web Application Penetration Testing.

Matteo ha conseguito la laurea in Ingegneria Informatica presso l'Università di Bologna, Italia, è il CEO e cofondatore di Minded Security dal 2007, dove è responsabile della direzione strategica e dello sviluppo delle attività aziendali.

Francesco Palmarini – Università Ca' Foscari Venezia

Francesco Palmarini è uno studente al secondo anno di dottorato in sicurezza informatica presso l'Università Ca' Foscari Venezia sotto la supervisione del professor Riccardo Focardi. Il percorso di studi universitario è stato completato in Ca' Foscari nel 2015 con la laurea magistrale conseguita con lode, in cui ha presentato il proprio lavoro di ricerca nella tesi "On Reverse Engineering of Embedded Architectures". E' un componente senior del team di ethical hacking c00kies@venice e partecipa attivamente a numerose competizioni di sicurezza internazionali. Da tre anni ha assunto il ruolo di manager dell'infrastruttura di rete e virtualizzazione in uso nel laboratorio del corso di sicurezza della laurea magistrale. Negli ultimi anni si è concentrato sulla ricerca nell'ambito del reverse engineering di architetture embedded ed analisi di sicurezza in sistemi di autenticazione e crittografia basati su hardware. Ad oggi ha svolto molteplici collaborazioni e consulenze con aziende specializzate, in particolare nel settore automotive.

Andrea Pierini – IT Architect & security manager & penetration tester

Attualmente ricopre il ruolo di "IT Architecture & Security Manager – Group Wide" in un'importante multinazionale industriale italiana. Laureato, certificato in passato Cisco e Microsoft ed attualmente ECPPT ed EWPT, ha maturato una lunga esperienza nel mondo dell'ICT, dallo sviluppo Software alla gestione sistemistica, dal networking fino alla sicurezza. Ha guidato importanti progetti sia applicativi che infrastrutturali con ruolo di Project Manager. Docente di corsi su temi specifici riguardanti la gestione dei sistemi Windows, Linux e Networking, con particolare attenzione alla sicurezza ICT, orientati anche ad una vista Executive. Si definisce un "IT Security enthusiast" interessato a tutte le tecnologie emergenti ed alle ultime frontiere della sicurezza, sia "offensive" che "defensive". Animato da un forte spirito divulgativo, ha presenziato diversi interventi in sedi anche accademiche, e pubblicato diversi articoli su magazine di settore. Ha iniziato recentemente un suo blog (*https://decoder.cloud*).

Andrea Praitano – Business-e

Andrea Praitano lavora per Business-e che è il coordinatore del progetto VisiOn. È laureato in Ingegneria e lavora nel settore dell'ICT e della Sicurezza delle Informazioni da oltre quindici anni maturando una considerevole esperienza nell'ambito dell'IT Governance, IT Audit & Compliance, dell'Information Security Governance, Data Protection/Privacy, IT Service Management nonché il Project Management. L'esperienza è stata maturata su una pluralità di contesti di clienti diversi (sanitario, manifatturiero, bancario, industriale, telecomunicazioni, gioco, PA, ecc.) e attraverso molteplici tipologie di attività quali: audit, consulenza e servizi stabili presso clienti.

È in possesso di certificazione professionali quali ambiti (CISA, Lead Auditor ISO/IEC 27001 e 22301, PRINCE2, ITIL Expert, CRISC, COBIT 5, ISO/IEC 20000 Auditor e Manager, MoR, Programme Management, Green IT, ecc.). Ha conseguito, in ultimo, un MBA presso il MIP-Polimi. È accreditato come trainer per diversi enti internazionali (EXIN, APMG International e PeopleCert) ed ha tenuto diversi interventi a seminari e conferenze.

Gianluca Salvalaggio – Triveneto Bassilichi

Gianluca Salvalaggio ha conseguito la Laurea in Ingegneria Elettronica presso l'Università degli Studi di Padova e la Laurea in Informatica presso L'Università Ca' Foscari di Venezia. Lavora da più di dieci anni nel campo dell'Information Security e attualmente ricopre il ruolo di Responsabile della funzione Architetture e Sicurezza ICT del Gruppo Bassilichi. Si interessa di application security, crittografia e protocolli di sicurezza. È docente in corsi specialistici di Networking e di Sicurezza Informatica.

Michael Schwarz – Graz University of Technology

Michael Schwarz is an Infosec PhD student at Graz University of Technology with a focus on microarchitectural side-channel attacks and system security. He holds two master's degrees, one in computer science and one in software development with a strong focus on security. He frequently participates in CTFs and has also been a finalist in the European Cyber Security Challenge. He was a speaker at Black Hat Europe 2016 and Black Hat Asia 2017 where he presented his research on microarchitectural side-channel attacks. He co-authored several papers published at international academic conferences and journals, including USENIX Security 2016 and NDSS 2017.

Mauro Tempesta – Università Ca' Foscari Venezia

Mauro Tempesta è uno studente iscritto al secondo anno di dottorato in sicurezza informatica presso l'Università Ca' Foscari sotto la supervisione del professor Riccardo Focardi. Ha conseguito la laurea magistrale con lode a Ca' Foscari nel 2015 con la tesi di ricerca intitolata "Enforcing Session Integrity in the World "Wild" Web". Negli ultimi anni l'attività di ricerca si è concentrata sulla sicurezza web e sistemi di firewalling. Dal 2011 fa parte del team di hacking etico c00kies@venice con cui partecipa attivamente a competizioni internazionali di sicurezza informatica. Ha inoltre svolto attività di penetration test in collaborazione con varie aziende specializzate nel settore.

Giuseppe Trotta – Penetration tester

È un penetration tester e security researcher "wannabe". Ottimo creatore di guai e drogato di qualsiasi cosa richieda un intenso uso del cervello (rompicapo, indovinelli, CTF e così via). Giuseppe è stato lo sviluppatore di *hack.me* e anche autore di diverse challenge pubbliche e private, autore del corso WAPTX (eLearnSecurity) e anche creatore ed ex-ingegnere dei potenti Hera Labs.

Manuel Weber – Graz University of Technology

Manuel Weber is a PhD student in the field of Security in the Internet of Things and Industry 4.0 at Graz University of Technology. He did his master in computer science, focusing on IT-security and the Internet of Things. His research interests lie within security issues of IoT devices and its communication protocols, lifecycle management systems for such devices and the effectiveness of new security mechanisms. In the field of IoT, he co-authored a paper accepted at EWSN 2017. In the field of security, he co-authored a paper accepted at NDSS 2017 and spoke at BlackHat Asia 2017.

Iniziativa realizzata grazie a:

SECSERVIZI

Sostenitore Platinum

EY Building a better working world

Sponsor Platinum

Triveneto Bassilichi

Sostenitore Platinum

KPMG cutting through complexity

Sponsor Platinum

con il patrocinio di:

AICA Associazione Italiana per l'Informatica ed il Calcolo Automatico

FONDAZIONE INGEGNERI PADOVA

aicq Associazione Italiana Cultura Qualità triveneta

Trust in, and value from, information systems

Venice Chapter

ISACA – Information Systems Audit & Control Association

È una associazione internazionale, indipendente e senza scopo di lucro. Con oltre 140.000 associati in più di 180 Paesi, ISACA© (www.isaca.org) aiuta i leader delle imprese e dell'IT a massimizzare il valore ottenibile dalle informazioni e dalla tecnologia e a gestirne i relativi rischi.

Fondata nel 1969, ISACA è una fonte affidabile di conoscenze, standard, opportunità di relazioni e sviluppo di carriera per professional che si occupano di audit, assurance, sicurezza, rischi, privacy e governance dai sistemi informativi.

ISACA mette a disposizione Cybersecurity Nexus™, un completo insieme di risorse per i professional della cyber security, e COBIT©, un framework per le aziende che aiuta le imprese nel gestire e governare il loro sistema informativo e le tecnologie informatiche.

ISACA sviluppa e attesta le conoscenze e le competenze critiche per le imprese attraverso le seguenti certificazioni affermate in tutto il mondo: 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).

Nel mondo sono associati ad ISACA più di 200 capitoli.

ISACA VENICE Chapter

ISACA VENICE Chapter è 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.

Riunisce coloro che nell'Italia del Nord Est svolgono attività di Governance, Auditing, Controllo e Security 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.

Maggiori informazioni su www.isacavenice.org

ISACA VENICE PER L'ATTIVITA' SVOLTA NEL 2015 HA RICEVUTO I SEGUENTI RICONOSCIMENTI:

- ✓ **honorable mention per il K. Wayne Snipes Best Chapter Award 2015**
- ✓ **Communications Commendation.**

Sede della conferenza

Campus scientifico dell'Università Ca' Foscari Venezia,

Auditorium edificio Alfa,

Via Torino 155,

Venezia Mestre