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

Sicurezza e governance nell'era dell'Internet of Things

IV 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 23 Settembre 2016

Campus scientifico dell'Università Ca' Foscari

Venezia

Obiettivi

Le applicazioni vivono ed operano in un mondo sempre più interconnesso e tecnologicamente differenziato. Attraverso i contributi di relatori provenienti da settori ed esperienze diverse, cercheremo di gettare un colpo d'occhio sullo stato dell'arte. I punti di vista sono diversi e richiedono specializzazioni crescenti; abbiamo cercato di coprire i più significativi:

- Governance: cosa significa la cybersecurity nel contesto Europeo e in particolare in quello Italiano del del Framework Nazionale di Cyber Security
- Risk Management: minacce malware su dispositivi mobili e gestione frodi nell'online banking
- Internet of Things: minacce di sicurezza e privacy ad utenti di dispositivi mobili; i problemi di privacy nei dispositivi in ambito sanitario
- Defensive and Offensive Computing: la sfida di sviluppare applicazioni in modo sicuro, e la prospettiva da un evento di Capture the Flag hacking-style
- Applied Cryptography: sfide e promesse della crittografia osservando applicazioni pratiche quali Bitcoin ed attacchi a dispositivi crittografici

Programma

8.30 – 9.30 Registrazione	
Chairman	Mauro Bregolin, *ISACA VENICE Chapter*
Common Track Benvenuto	Marco Salvato, *Presidente ISACA VENICE* Matteo Meucci, *Presidente OWASP Italia*
Common Track Saluto delle Autorità	Michele Bugliesi, *Rettore Università Ca' Foscari Venezia* Daniele De Martino, *Dirigente Polizia Postale e delle Comunicazioni – Veneto*
Common Track Can't You Hear Me Knocking: Novel Security and Privacy Threats to Mobile Users	Mauro Conti *Università di Padova*
Common Track Enhancing infrastructure cybersecurity in Europe	Rossella Mattioli *ENISA*
Coffe break offerto dagli Sponsor e dai Sostenitori di ISACA VENICE	
Common Track CopperDroid: Automatic Android Malware Analysis and Classification	**Intervento in lingua inglese** Lorenzo Cavallaro *Royal Holloway, University of London*
Track 1 Put yourself in the appsec pipe	Paolo Perego *codiceinsicuro.it*
Track 2 BankSealer: A Decision Support System for Online Banking Fraud Analysis and Investigation	Michele Carminati *Politecnico di Milano*
Pranzo offerto dagli Sponsor e dai Sostenitori di ISACA VENICE	

Sessione Pomeridiana	
Track 1 Attacchi a livello APDU su dispositivi crittografici	Francesco Palmarini *Università Ca' Foscari Venezia*
Track 2 A governance model for ubiquitous medical devices accessing eHealth data: the need for standards	Massimiliano Masi *Tiani "Spirit", Wien*
Track 1 Un'introduzione pratica al Bitcoin	Federico Pintore *Università di Trento*
Track 2 Sopravvivere a un CTF attacco e difesa	Marco Squarcina *Università Ca' Foscari Venezia*
Coffe break offerto dagli Sponsor e dai Sostenitori di ISACA VENICE	
Common Track Cyber Risk Management e Sicurezza Applicativa nel contesto del Framework Nazionale di Cyber Security	Andrea Zapparoli Manzoni, *KPMG*
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.

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

Data: venerdì 23 Settembre 2016

Orario: 9:30 – 17.30

Partecipazione **gratuita** previa iscrizione soggetta a conferma.
Inviare la scheda di adesione a iscrizioni@isacavenice.org entro **il 12 settembre 2016**.

CPE

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

ABSTRACT

Enhancing infrastructure cybersecurity in Europe

Rossella Mattioli

ENISA, the European Union Agency for Network & Information Security, is working together with stakeholders to identify pragmatic solutions to cybersecurity challenges for Critical Information Infrastructures, Internet infrastructure, ICS SCADA and transport infrastructure in Europe. The agency has undertaken several activities to support relevant stakeholders by helping them to improve their security practices and by raising awareness to both industry and the public sector. This talk with provide an overview on the latest efforts and future steps.

Cyber Risk Management e Sicurezza Applicativa nel contesto del Framework Nazionale di Cyber Security

Andrea Zapparoli Manzoni

L'aumento esponenziale delle minacce cibernetiche richiede oggi un profondo ripensamento delle strategie di mitigazione dei rischi cyber, le quali devono includere allo stesso tempo contromisure tecnologiche, organizzative e culturali. L'area della sicurezza applicativa risulta fortemente coinvolta da questa evoluzione, anche alla luce del recente Framework Nazionale di Cyber Security.

CopperDroid: Automatic Android Malware Analysis and Classification

Lorenzo Cavallaro

Rapid advent of Android platforms has dawned an era of sophisticated malware that attack these systems. Static approaches developed to detect malware are often left wanting as malware writers take to increasingly obfuscated code that bypass static detection. This has triggered research into Android sandboxes that derive meaningful semantic information about malware by running them.

To better understand this slew of threats, in this talk I will first introduce CopperDroid, an automatic VMI-based dynamic analysis system to reconstruct the behaviors of Android malware, developed within the Systems Security Research Lab at Royal Holloway, University of London. The novelty of CopperDroid lies in its agnostic approach to identify interesting OS- and high-level Android-specific behaviors. It reconstructs these behaviors by observing and dissecting system calls and, therefore, is resistant to the multitude of alterations the Android runtime is subjected to over its life-cycle. CopperDroid automatically and accurately reconstructs events of interest that describe not only well-known process-OS interactions (e.g., file and process creations), but also complex intra- and inter-process communications (e.g., sending and receiving text messages, accessing GPS coordinates, camera, and contacts list), whose semantics are typically contextualized through complex Android objects. Because CopperDroid's reconstruction mechanisms are agnostic to the underlying action invocation methods, it is able to capture actions initiated both from Java and native code execution. CopperDroid's analysis generates detailed behavioral profiles that abstract a large stream of low-level---often uninteresting---events into concise, high-

level semantics, which are well-suited to provide insightful behavioral traits and open the possibility to further research directions. To this end, I will then show our current research efforts to investigate the efficacy of behavioral profiles of different abstractions to differentiate between families of malware. Our experiments report an accuracy, precision and recall of 94.5%, 99.2% and 97.8%, respectively, in a multi-class Android malware family classification setting. In addition, in a significant departure from traditional classification techniques, we further apply a statistical classification approach to include samples showing poor behavior counts and depict a means to achieve near-perfect accuracy by considering a prediction set of top few matches than a singular choice.

BankSealer: A Decision Support System for Online Banking Fraud Analysis and Investigation

Michele Carminati

Risk Management

The significant growth of online banking frauds, fueled by the underground economy of malware, raised the need for effective fraud analysis systems. Unfortunately, almost all of the existing approaches adopt black box models and mechanisms that do not give any justifications to analysts. Also, the development of such methods is stifled by limited Internet banking data availability for the scientific community. In this paper we describe BankSealer, a decision support system for online banking fraud analysis and investigation. During a training phase, BankSealer builds easy-to-understand models for each customer's spending habits, based on past transactions. First, it quantifies the anomaly of each transaction with respect to the customer historical profile. Second, it finds global clusters of customers with similar spending habits. Third, it uses a temporal threshold system that measures the anomaly of the current spending pattern of each customer, with respect to his or her past spending behavior. With this threefold profiling approach, it mitigates the under-training due to the lack of historical data for building well-trained profiles, and the evolution of users' spending habits over time. At runtime, BankSealer supports analysts by ranking new transactions that deviate from the learned profiles, with an output that has an easily understandable, immediate statistical meaning. Our evaluation on real data, based on fraud scenarios built in collaboration with domain experts that replicate typical, real-world attacks (e.g., credential stealing, banking trojan activity, and frauds repeated over time), shows that our approach correctly ranks complex frauds. In particular, we measure the effectiveness, the computational resource requirements and the capabilities of BankSealer to mitigate the problem of users that performed a low number of transactions. Our system ranks frauds and anomalies with up to 98% detection rate and with a maximum daily computation time of 4 minutes. Given the good results, a leading Italian bank deployed a version of BankSealer in their environment to analyze frauds.

Can't You Hear Me Knocking: Novel Security and Privacy Threats to Mobile Users

Mauro Conti

IoT & Privacy

While Smartphone and IoT devices usage become more and more pervasive, people start also asking to which extent such devices can be maliciously exploited as "tracking devices". The concern is not only related to an adversary taking physical or remote control of the device, but also to what a passive adversary without the above capabilities can observe from the device communications. Work in this latter direction

aimed, for example, at inferring the apps a user has installed on his device, or identifying the presence of a specific user within a network.

In this talk, we discuss threats coming from contextual information and to which extent it is feasible, for example, to identify the specific actions that a user is doing on mobile apps, by eavesdropping their encrypted network traffic.

A governance model for ubiquitous medical devices accessing eHealth data: the need for standards

Massimilano Masi

IoT & Privacy

The Electronic Health Record (EHR) is a reality in almost all the EU and USA regions. The introduction of EHR dramatically reduced the need for paper-based records, thus resulting in an improvement of patient care, including the “freedom of movement” principle across countries. EHRs contain very sensitive information (Private Healthcare Information, PHI) and they are ruled by several acts and international regulations, defined by each country. Key principles for this sector are interoperability, and security. There are two overarching standards for such security, FHIR and IHE. This short presentation aims at providing an overall status across eHealth Security and Interoperability, common pitfalls, and a description of common architectures, when connecting medical devices to patient’s EHR.

Put yourself in the appsec pipe

Paolo Perego

Defensive computing

Building an effective application security pipeline is the necessary step for each company to establish a meticulous appsec program. Create secure software is more than run a penetration test or a code review, just before the deploy and having some automatism can help you in have a low error rate process.

In this talk we will go through the pipeline building process, explaining how to automate some boring tasks dedicating ourselves to having fun, playing tricks like pros. At the end of our journey both tech people than security managers, will have the feeling that using the pipeline approach, they can lower vulnerabilities, with an affordable time to market so to make the bosses happy.

Sopravvivere a un CTF attacco e difesa

Marco Squarcina

Offensive computing

Le competizioni di sicurezza informatica di tipo Capture the Flag (CTF) rappresentano una preziosa risorsa per svolgere esperienze hands-on nella difesa e nell'attacco di servizi informatici realistici e consentono ai partecipanti di misurarsi rispetto ai migliori team internazionali. In questo intervento viene riportata la partecipazione della squadra c00kies@venice dell'Università Ca' Foscari alle finali del RuCTF 2016 a Ekaterinburg (Russia), una delle principali competizioni di ethical hacking a livello mondiale. Nel talk viene descritto il funzionamento di un CTF utilizzando

il contest russo come caso di studio. Vengono inoltre presentati i tool sviluppati dal team veneziano e le metodologie adottate per fronteggiare queste sfide.

Un'introduzione pratica al Bitcoin

Federico Pintore

Le parole Bitcoin e Blockchain stanno diventando sempre più ricorrenti nell'ambito dei pagamenti elettronici. L'intento del mio intervento è quello di presentare le caratteristiche della crittovaluta Bitcoin e della tecnologia ad essa sottostante, la Blockchain. In particolare verranno introdotti, con una breve panoramica sul coinvolgimento della crittografia, i concetti di conto Bitcoin, di transazione Bitcoin (lo strumento col quale i bitcoin vengono scambiati), e di mining (il processo tramite il quale le transazioni vengono validate ed inserite all'interno del libro mastro di tutte le transazioni avvenute: la Blockchain). In conclusione, verranno presentate alcuni esempi di utilizzo innovativo della Blockchain.

Attacchi a livello APDU su dispositivi crittografici

Francesco Palmarini

In questa presentazione illustreremo nuovi attacchi su dispositivi crittografici che si basano sull'interazione con il protocollo "APDU" di basso livello, utilizzato per comunicare con il dispositivo. Gli attacchi si basano su debolezze delle implementazioni proprietarie che permettono a un attaccante di evitare le protezioni fornite dalle API standard. Alcuni degli attacchi permettono di ottenere il valore di chiavi crittografiche su dispositivi ritenuti sicuri. Introdurremo un nuovo modello dell'attaccante per questo tipo di dispositivi e analizzeremo gli attacchi rispetto a vari attaccanti e configurazioni. Gli attacchi sono stati tutti comunicati ai produttori di hardware seguendo un protocollo di "responsible disclosure". Questa ricerca verrà presentata a settembre 2016 al 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2016, http://www.raid2016.org/)

BREVI NOTE PERSONALI SUI RELATORI

Michele Carminati – Politecnico di Milano

Michele Carminati received his B.Sc. in Computer Engineering (2010) and his M.Sc. in Computer Engineering (2013, cum laude) both from Politecnico di Milano. He discussed his M.Sc. thesis about fraud and anomaly detection in the Online banking scenario entitled “BANKSEALER: A TRANSACTION MONITORING SYSTEM FOR INTERNET BANKING FRAUD DETECTION” supervised by prof. Stefano Zanero and prof. Federico Maggi.

Since November 2013 he is a PhD student in Computer Engineering at Politecnico di Milano. His research interests are mainly focused on computer security and in particular on financial malware analysis and Internet banking fraud detection.

Lorenzo Cavallaro – Royal Holloway, University of London

Lorenzo “Gigi Sullivan” Cavallaro was raised in a fantastic epoch where information and knowledge was meant for those who were just curious enough. He grew up on pizza, spaghetti, Phrack (do “smashing the stack for fun and profit” and “IP spoofing demystified” ring a bell to you?), and W. Richard Stevens' TCP/IP illustrated masterpieces. Underground and academic research interests followed shortly thereafter and he has never stopped wondering and having fun ever since.

Lorenzo is currently a Reader (Associate Professor) of Information Security in the Information Security Group (ISG) at Royal Holloway, University of London. Prior joining the ISG, Lorenzo proudly spent time at Stony Brook University (Prof. R. Sekar), as a visiting PhD scholar from University of Milan, and UC Santa Barbara (Profs Giovanni Vigna and Christopher Kruegel) and Vrije Universiteit Amsterdam (Prof. Andrew S. Tanenbaum) as a PostDoc Researcher---amazing and intense years he still remembers vividly. Lorenzo's research focuses largely on systems security. To this end, he has founded and is leading the recently-established Systems Security Research Lab (S2Lab) within the ISG, which focuses on devising novel techniques to protect systems from a broad range of threats, including those perpetrated by malicious software. In particular, Lorenzo's lab aims ultimately at building practical tools and providing security services to the community at large. He is Principal Investigator and co-Investigator on a number of UK EPSRC- and EU-funded research projects, sits in technical program committee of top and well-established information security academic conferences and workshops, and has published in top and well-known venues. Lorenzo's Coursera MOOC on “Malicious Software and its Underground Economy:Two Sides to Every Story” attracted more than 100,000 students since its pilot in 2013, which makes him shamelessly bragging on his pizza, spaghetti, and Phrack heritage furthermore.

Mauro Conti – Università di Padova

Mauro Conti is an Associate Professor at the University of Padua, Italy. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009.

After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011 he joined as Assistant Professor the University of Padua, where he became Associate Professor in 2015. He has been Visiting Researcher at GMU (2008), UCLA (2010), UCI (2012, 2013, and 2014), and TU Darmstadt (2013). He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His main research interest is in the area of security and privacy. In this area, he published more than 130 papers in topmost international peer-reviewed journals and conference. He is Associate

Editor for several journals, including IEEE Communications Surveys & Tutorials and IEEE Transactions on Information Forensics and Security. He was Program Chair for TRUST 2015 and ICISS 2016, and General Chair for SecureComm 2012 and ACM SACMAT 2013. He is Senior Member of the IEEE.

Massimilano Masi – Tiani "Spirit"

Massimiliano Masi received his Ph.D. in theoretical computer science from the University of Florence. He has more than 13 years of experience in IT security. Relevant experience includes specification of IT security measures of the eGP-EGOR and BeS Projects in Austria, and South African eHR.ZA (governmental eHealth initiatives), lead role of epSOS.eu Common Components Development (CCD) and leader of the Core team of the epSOS Security Experts Group, design security aspects of the LHC computing GRID. He has been a member of the OASIS Trust Elevation Committee.

Masi is also the editor of the IHE ITI profile Cross Community Fetch (XCF), and participated in the evaluation of the IHE profiles related to security (e.g., XUA, XUA++, SeR, Access Control White Paper, and ATNA). Massimiliano Masi has strong experience in both leading and contributing to working groups and teams in international projects (results are part of commission decision 2015/1032). He is actually leading various task forces in the e-SENS project. Selected Expert from the Austrian Ministry of Health, and consultant for various European Commission bodies (DG DIGIT and SANTE, eHealth Network). ITIL and ISO 27000 certified.

As developer, Dr. Masi main focus is on high performant Java Backends. Several nationwide projects depend upon security-related services that have been implemented.

Rossella Mattioli – ENISA

Rossella Mattioli works at ENISA, the European Union Agency for Network and Information Security. Her work focuses on enhancing the security of Critical Information Infrastructures, Internet infrastructure, ICS SCADA and transport infrastructure in Europe. She holds a MSc in Engineering with main specialization in Cybersecurity at Tallinn University of Technology and a BA in Communication Sciences. Prior to focus on infrastructure security and resilience, she was the intranet manager of a major financial group in Italy for 9 years coordinating an internal network of over 6,000 employees.

Paolo Perego – codiceinsicuro.it

It was 1994 and Paolo discovered that filling a buffer with 0x41 and 0x90 was really fun moreover it was funny having system applications to spawn shells for him. He started fighting against insecure software with the motto "defensive programming will save us" writing some application security tools he currently uses for his own job.

Back in 2012, Paolo launched http://armoredcode.com, a technical blog about application security as seen either from the developer point of view.

In 2014 Paolo launched Codice Insicuro (https://codiceinsicuro.it), an application security focused blog in Italian language only.

Paolo wrote wordstress (https://wordstress.org), a Wordpress PHP plugin and a whitebox ruby scanner for wordpress related vulnerabilities.

Paolo also wrote dawnscanner (https://rubygems.org/gems/dawnscanner), the real opensource alternative to Brakeman for Ruby powered web application security static analysis. It supports Sinatra, Padrino and Rails out of the box.

In his spare time Paolo is an husband, a proud father, a Taekwon-do ITF martial artists and instructor.

Francesco Palmarini – Università Ca' Foscari Venezia

Francesco Palmarini è uno studente al primo anno di dottorato in sicurezza informatica presso l'Università Ca' Foscari Venezia sotto la supervisione del professor Riccardo Focardi. Durante questo periodo è stato co-autore di un paper accettato alla conferenza RAID 2016.

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.

Federico Pintore – Università di Trento

Giovane ricercatore presso il Laboratorio di Crittografia e Matematica Industriale dell'Università degli Studi di Trento. È supervisore di un progetto, in collaborazione con l'azienda trentina Argentea, per l'estensione al Bitcoin di un servizio di pagamento mediante cartà fedeltà. Dopo aver conseguito la laurea triennale e magistrale a Cagliari, nel 2011 inizia il Dottorato di Ricerca presso il Dipartimento di Matematica di Trento, conseguendo il titolo a Marzo 2015 con una tesi sulla teoria dei numeri e sulle curve ellittiche, quest'ultime diffusamente impiegate nell'ambito della sicurezza informatica ed in particolare nella crittografia.

Marco Squarcina – Università Ca' Foscari Venezia

Marco Squarcina è dottorando 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 magistrale in System and Network Security e team leader dei c00kies@venice, squadra con la quale partecipa a competizioni internazionali di ethical hacking. I suoi principali interessi di ricerca riguardano hardening dei sistemi, sicurezza web e security API. Svolge attività di consulenza aziendale in ambito di vulnerability assessment e penetration test e attualmente collabora con Cryptosense, spin-off accademica dell'INRIA e dell'Università Ca' Foscari.

Andrea Zapparoli Manzoni – KPMG

Andrea Zapparoli Manzoni si occupa con passione di ICT Security dal 1997. Fa parte dei Consigli Direttivi di Assintel e di Clusit, è stato membro dell'OSN (Osservatorio per la Sicurezza Nazionale), ed è Board Advisor del Center for Strategic Cyberspace + Security Science di Londra. Dal 2014 è Senior Manager della divisione Information Risk Management di KPMG Advisory, con la responsabilità dell'area Cyber Security. E' co-autore del "Framework Nazionale di Cyber

Security". Per il "Rapporto Clusit sulla Sicurezza ICT in Italia" da cinque edizioni cura la sezione relativa all'analisi dei principali attacchi di dominio pubblico a livello globale ed alle tendenze per il futuro.

Iniziativa realizzata grazie a:

Sostenitore Platinum

Sponsor Platinum

Sostenitore Platinum

Sponsor Platinum

con il patrocinio di:

LA PARTECIPAZIONE È 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.

ISACA – Information Systems Audit & Control Association

E' 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.**

Scheda di Iscrizione da inviare a iscrizioni@isacavenice.org entro 12.9.2016

Sicurezza e governance nell'era dell'Internet of Things

DATI PERSONALI:

Cognome:					
Nome:					
Indirizzo:					
Cap:		Città:		Prov.:	
Telefono:		Cell:			
E-mail:		ID Associato:			

GARANZIE E DIRITTI DELL'INTERESSATO in ottemperanza al D. Lgs. 196/03 "Codice in materia di protezione dei dati personali". I dati personali in possesso dell'Associazione sono direttamente da Lei forniti ovvero acquisiti altrimenti nel rispetto delle disposizioni legislative vigenti e potranno formare oggetto di trattamento per gli scopi amministrativi del presente corso. Titolare del trattamento è ISACA VENICE CHAPTER che è a disposizione per l'eventuale aggiornamento, rettifica, integrazione o cancellazione.

Data _____ **Firma** _____

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

Sede della conferenza

Campus scientifico dell'Università Ca' Foscari Venezia,

Auditorium edificio Alfa,

Via Torino 155,

Venezia Mestre