AIEA

ASSOCIAZIONE ITALIANA INFORMATION SYSTEMS AUDITORS

nota anche come

ISACA® Capitolo di Milano

Ordine Ingegneri della Provincia di Siena

ORDINE degli INGEGNERI della PROVINCIA di SIENA

PRESENTANO

con il patrocinio di

CONFASSOCIAZIONI Digital

AIP Associazione Informatici Professionisti

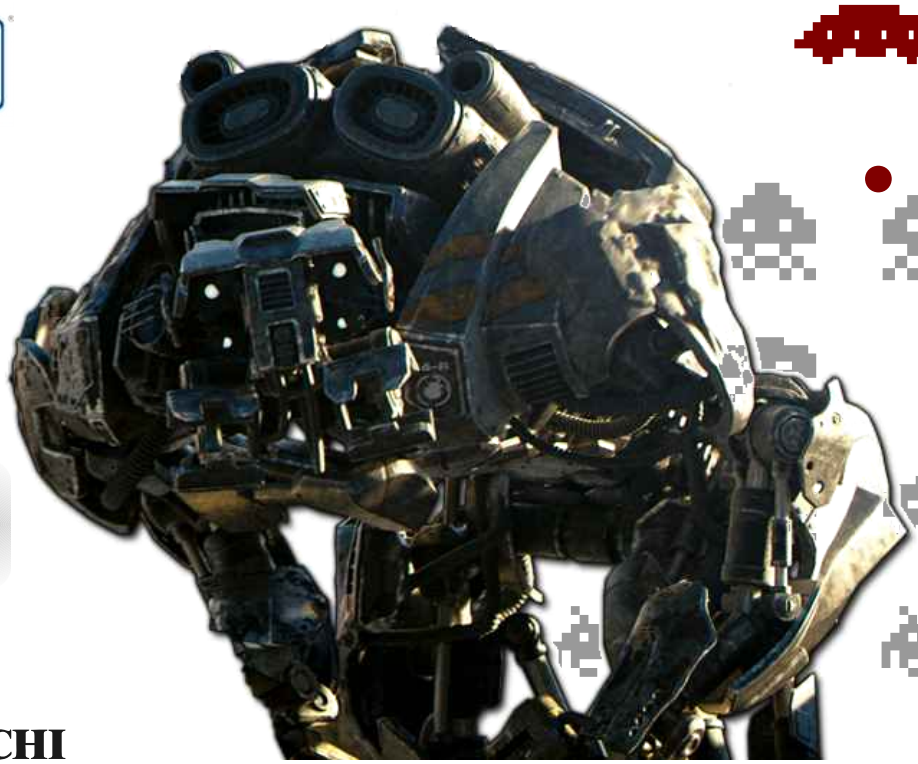
ITCS Italian Computer Society

Clusit

Si ringraziano

DIISM

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472



CYBERSECURITY

VECCHIE E NUOVE MINACCE

Siena, 9 maggio 2019 14.00-18.00

Auditorium
Banca Monte dei Paschi di Siena
Viale Mazzini, 23

PRESENTAZIONI

Luca Bechelli, CLUSIT

Quelli che... "...con la sicurezza sono a posto..."?!?

Mai come oggi lo scenario tecnologico/normativo sta subendo significative rivoluzioni : mobile, cloud, GDPR, AI, blockchain, per citare alcune keywords. I reparti IT, sotto la pressione delle richieste di saving e di erogazione di nuovi servizi alla velocità del cloud, rischiano di sottovalutare i rischi di sicurezza, la cui crescita ed evoluzione sono confermate nell'ultima edizione del Rapporto Clusit.

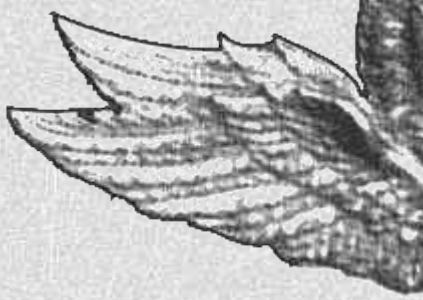
Partendo da una serie di casi reali, non senza un pò di ironia, cercheremo di affrontare i problemi che i CISO e gli IT Manager incontrano tutti i giorni, provando a definire le sfide prossime venture per la cybersecurity!

Gianluca Massettini, Direttore Tecnico Superiore della Polizia di Stato

Cyber Attack alle Infrastrutture critiche e non solo.... Focus della Polizia Postale e delle Comunicazioni sullo stato della Cybersecurity in Italia.

In un mondo, quello virtuale, sempre più lo specchio distorto e a volte più vulnerabile di quello reale, nel quale cittadini, aziende, P.A. ed infrastrutture sensibili per il sistema economico finanziario strutturale del paese sono iperconnessi con macchine e dispositivi di uso quotidiano (IoT) fruendo e offrendo beni servizi e opportunità, emergono con altrettanta forza sul piano globale le minacce del CyberCrime, sempre più organizzato e strutturato, finalizzate, con gli attacchi subdoli e persistenti (APT) o attraverso le più fantasiose tecniche di Social Engeeneering sferrati a diversi target, a monetizzare e a destabilizzare.

In questo quadro, tutte le Istituzioni sono coinvolte ed in particolare la Polizia Postale e delle Comunicazioni con il CNAIPIC - il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - è incessantemente impegnata e specializzata nella prevenzione e nel contrasto dei crimini informatici, con gli operatori della Specialità della Polizia di Stato che utilizzano strumenti e tecniche (come quelle utilizzate nell'Osint) sfruttate dalle stesse organizzazioni criminali nella prepazione e nello sviluppo degli attacchi, con lo scopo di anticiparli e minimizzarli negli effetti, e che sempre più costituisce un tassello fondamentale nel quadro complessivo della Cyber Security in Italia.



PRESENTAZIONI

Sandro Bartolini, Biagio Peccerillo

Università di Siena

Side-channel attacks: quando anche sistemi sicuri non proteggono le informazioni

Tecniche e protocolli crittografici, oltre che sistemi pensati per la sicurezza, sono attualmente impiegati per la gestione sicura di informazioni critiche in molteplici contesti. Proprietà matematiche di tali tecniche e criteri progettuali di tali sistemi riescono a garantire livelli di sicurezza adeguati, almeno in teoria.

Viceversa, in svariati casi, anche sistemi che adottano tecniche crittografiche e protocolli allo stato dell'arte, possono risultare molto meno sicuri di quanto imposto a livello progettuale a causa di possibili "falle" indirette nella gestione della sicurezza, talvolta sorprendenti e molto gravi nella portata dei corrispondenti effetti. Queste falle costituiscono la premessa su cui può essere costruito un side-channel attack, cioè un tipo di attacco che mira a violare la sicurezza di un sistema con un meccanismo tipicamente indiretto e non distruttivo.

In questo intervento si introdurranno i concetti principali che stanno alla base di questa tipologia di attacchi e se ne esemplificheranno alcune fattispecie in modo da delinearne i contorni sia da un punto di vista teorico che pratico. Tra queste, arriveremo ad accennare al princìpi su cui si fonda l'attacco side-channel utilizzato da Meltdown nei moderni processori. Daremo quindi delle indicazioni per la mitigazione di queste tipologie di attacchi in contesti specifici.

AGENDA

14:00 – 14:10

Registrazione partecipanti

14:10 – 14:20

Introduzione

14:20 – 15:10

Luca Bechelli, CLUSIT

Quelli che… “…con la sicurezza sono a posto…”?!?

15:10 – 16:00

Sandro Bartolini, Biagio Peccerillo

Università di Siena

Side-channel attacks: quando anche sistemi sicuri non proteggono le informazioni

16:00 – 16:30

Coffee break

16:30 – 17:20

Gianluca Massettini, Polizia Postale

Cyber Attack alle Infrastrutture critiche e non solo….
Focus della Polizia Postale e delle Comunicazioni sullo stato della Cybersecurity in Italia

17:20 – 18:00

Confronto e dibattito

18:00

Conclusione e ringraziamenti

RELATORI

Luca Bechelli, CLUSIT

Information Security & Cyber Security Advisor, svolge dal 2000 consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione ed al project management per attività di system integration.

Svolge attività di ricerca e sviluppo tramite collaborazioni con enti di ricerca e associazioni, nell'ambito delle quali ha svolto docenze per master post-laurea. Ha collaborato alla realizzazione di numerosi studi e pubblicazioni di riferimento per il settore. Dal 2007 è membro del Consiglio Direttivo e del Comitato Tecnico Scientifico del Clusit, con delega su Tecnologie e Compliance. Dal 2017 partecipa all'Osservatorio Privacy & Security del Politecnico di Milano coordinando la redazione di linee guida su tematiche legate alla data protection.

Ing. Gianluca Massettini, Direttore Tecnico Superiore del Compartimento Polizia Postale delle Comunicazioni di Firenze

Ingegnere Elettronico in forza alla Polizia Postale e delle Comunicazioni per la "Toscana" di Firenze dal 2013. Si occupa di coordinare tutte le le attività e le iniziative di prevenzione e formazione nelle scuole e con i cittadini, promuovendo nei convegni, seminari e incontri l'uso consapevole della rete Internet e dei Social Network.
Responsabile del Settore Analisi Forense e Ricerca Avanzata, nel quale si utilizzano e sperimentano tecniche e software di Digital e Mobile Forensics e di "carving" al fine di recuperare e cristalizzare le "fonti di prova".
Ha avviato e promosso proficue collaborazioni tra le quali con l'Università di Firenze, il Corecom Toscana e Confindustria Firenze.
Responsabile dell'infrastruttura informatica e di rete del Compartimento di Polizia Postale di Firenze,riveste il ruolo di Data Protection Officer e di Ciso ai sensi del GDPR (General Data Protection Regulation).

RELATORI

Sandro Bartolini, Università di Siena

Sandro Bartolini ha ricevuto il Dottorato di ricerca in Architettura dei Calcolatori a Pisa nel 2003 ed è Ricercatore presso il Dipartimento di Ingegneria dell'Informazione e Scienze Matematiche dell'Università di Siena. I suoi principali interessi di ricerca comprendono: calcolatori ad alte prestazioni, sistemi embedded, programmazione parallela ad alte prestazioni e approcci innovativi per la produttività nella programmazione parallela (CPU e GPU), accelerazione hardware e/o software di algoritmi crittografici per la sicurezza informatica, cyber-security e block-chain. Da anni tiene un corso su "Design of Applications Systems and Services" nel corso di laurea magistrale "Computer and Automation Engineering" all'Università di Siena e ha tenuto corsi e seminari in università internazionali. Tiene seminari di programmazione avanzata in C++ per prestazioni e produttività in aziende e ha tenuto corsi di sicurezza informatica e sistemi operativi. Ha partecipato a vari progetti di ricerca internazionali sulle tematiche illustrate ed ha lavorato in progetti di ricerca e sviluppo in collaborazione con aziende italiane e internazionali quali RAI, Siemens, Adnkronos, SpaceDys, UaU Group Limited, STMicroelectronics.

Biagio Peccerillo, Università di Siena

Biagio Peccerillo si laurea in Ingegneria Informatica presso l'Università di Siena nel 2011 con una tesi sulla parallelizzazione di algoritmi finanziari complessi. È attualmente Dottorando presso la stessa facoltà in Computing Systems. I suoi interessi di ricerca comprendono: sviluppo software ad alte prestazioni, programmazione parallela multi-piattaforma con particolare attenzione all'astrazione ad alto livello, architettura dei calcolatori e impatto di questa sulla micro-ottimizzazione del codice, analisi prestazionale e parallelizzazione di algoritmi crittografici, cyber-security. Ha lavorato quattro anni come programmatore in azienda nel campo della produzione di software finanziario ad alte prestazioni, ha tenuto un corso in azienda sulla programmazione Java Enterprise. Attualmente collabora come programmatore con il team di Robotica dell'Università di Siena per lo sviluppo di algoritmi di tracking di dispositivi aptici e realtà virtuale.

ISCRIZIONE

Soci AIEA

L'iscrizione all'evento, gratuita, deve essere completata sul Portale delle Sessioni di Studio AIEA, all'indirizzo ***http://videosessioni.aiea.jed.st/*** *entro e non oltre il 2 maggio 2019. La partecipazione all'evento dà diritto ad acquisire 4 CPE per mantenere le certificazioni CISA, CISM, CGEIT e CRISC.*

Ordine degli Ingegneri

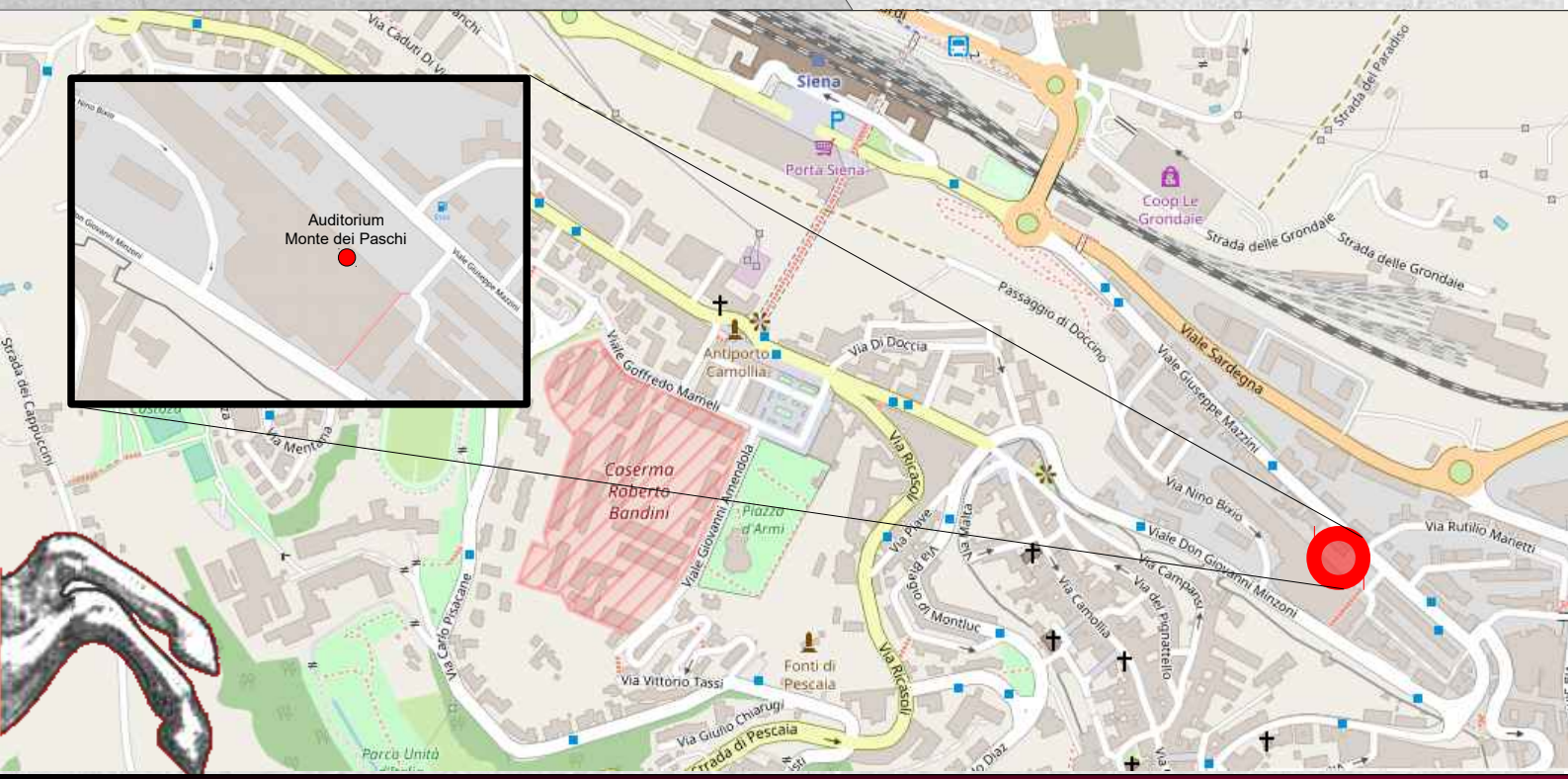
L'iscrizione all'evento deve essere completata sul portale della Formazione Continua dell'Ordine degli Ingegneri della Provincia di Siena ***http://siena.ing4.it/****. L'Ordine può riconoscere 3 CFP a qualunque ingegnere iscritto a qualunque albo Provinciale d'italia purchè l'iscrizione avvenga attraverso il portale della Formazione Continua. La partecipazione all'evento richiede un contributo di 10 Euro.*

Non Soci

La partecipazione all'evento richiede un contributo di 10 Euro. Per iscriversi contattare la Segreteria AIEA all'indirizzo email ***aiea@aiea.it*** *entro e non oltre il 2 maggio 2019.*

L'evento è ***gratuito per gli studenti.***

SEDE DELL'EVENTO



ORDINE degli INGEGNERI della PROVINCIA di SIENA

L'Ordine è un Ente pubblico Non Economico, ausiliario dello Stato, istituito con Legge Ordinaria.

All'Ordine sono attribuite specifiche competenze; è sottoposto al controllo ed alla vigilanza da parte del Ministero di Grazia e Giustizia, presso il quale è stabilita la sede del Consiglio Nazionale CNI

L'Ordine tiene aggiornato l'elenco degli iscritti nell'Albo Professionale.

La professione di Ingegnere, nei sui vari indirizzi, rientra tra le cosiddette professioni protette; ciò significa che per essere legittimati ad esercitare è necessaria l'iscrizione al relativo albo.
L'Ordine professionale da un lato si fa garante dell'accesso all'esercizio della professione di Ingegnere solo da parte di soggetti in possesso dei requisiti richiesti dalla legge, dall'altro lato esercita controllo sui propri iscritti, richiedendo loro che mantengano un comportamento rispondente alla deontologia professionale.

L'Ordine è totalmente sostenuto dai contributi degli iscritti, conferiti provincia per provincia

http://ording.si.it/

Ordine degli Ingegneri della Provincia di Siena
info@ording.si.it

Via Fontebranda 69 - 53100 Siena - E-mail: info@ording.si.it
Sito web: ording.si.it – Tel. +39 0577 4108

Associazione Italiana Information Systems Auditors

L'Associazione Italiana Information Systems Auditors è stata costituita a Milano nel 1979 con lo scopo di promuovere l'approfondimento dei problemi connessi con il controllo del processo di elaborazione automatica dei dati e di favorire lo sviluppo di metodologie e tecniche uniformi per la loro soluzione.

In particolare, gli obiettivi dell'Associazione sono:

- promuovere un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo, di affidabilità dell'organizzazione, Information Systems e di sicurezza dei sistemi;
- ampliare la conoscenza ed esperienza dei suoi oltre 800 membri nel campo dell'IT Governance, IT Security, Information Systems Auditing e Risk Control, favorendo lo scambio di metodologie per lo studio e la soluzione dei problemi inerenti;
- promuovere a livello nazionale la partecipazione alla certificazioni CISA, CISM, CGEIT, CRISC, CobiT e CSX

AIEA è associata da 40 anni ad ISACA, primo Capitolo in Europa, diventando nota internazionalmente come

ISACA®

Capitolo di Milano

ISACA® per i suoi oltre 135,000 soci in 188 paesi e per la comunità dei professionisti IT è fonte affidabile di possibilità di networking, certificazioni professionali, conoscenza e standard negli ambiti IT Governance, Cybersecurity, IT Risk e Assurance

www.aiea.it

Coordinamento AIEA Toscana
granducato@aiea.it