Colloquia

LA SICUREZZA DEI SISTEMI DI CONTROLLO INDUSTRIALE NELLE INFRASTRUTTURE CRITICHE: ASPETTI PECULIARI, INNOVAZIONI ED ESPERIENZE

Roma, 24 maggio 2017
ore 15.00

presso

Università Roma Tre

Sala Conferenze - Dipartimento di Ingegneria – via Vito Volterra, 62

Gentili Associati,

Il Consiglio Direttivo è lieto di informarVi che, proseguendo nell'attuazione delle iniziative promosse dall'Associazione Italiana Esperti in Infrastrutture Critiche volte al processo di miglioramento, di formazione e informazione dei propri associati, ha organizzato un incontro che avrà luogo presso il ***Dipartimento di Ingegneria dell'Università Roma Tre****, come da agenda allegata.*

La sessione, come sempre, è gratuita per gli associati; la partecipazione è estensibile, inoltre, ai non Soci e a tutti gli interessati.

Chi vorrà, potrà avere l'occasione di associarsi ad AIIC per ***l'anno 2017****, sottoscrivendo contestualmente la relativa quota.*

Per aderire all'iniziativa è richiesta una conferma da inviare via email a: segreteria@infrastrutturecritiche.it

entro e non oltre il **22 maggio p.v.**

Ricordiamo che la partecipazione all'evento dà diritto a ricevere un attestato di partecipazione.

Vi Aspettiamo!

Il Presidente
(L. Franchina)

11maggio 2017

Il Vicepresidente
(S. Bari)

LA SICUREZZA DEI SISTEMI DI CONTROLLO INDUSTRIALE NELLE INFRASTRUTTURE CRITICHE: ASPETTI PECULIARI, INNOVAZIONI ED ESPERIENZE

programma

14.45	Registrazione dei partecipanti
15.00	Apertura dei lavori e saluto **Silvano Bari** (vicepresidente AIIC), **Stefano Panzieri** (Università Roma Tre)
15.10	**Sessione 1 - il punto di vista degli esperti (**moderatore **Silvano Bari)** **Claudio Pantaleo (**Ass.Pri.Com. - Presidente) *Introduzione ai sistemi SCADA* **Enzo Maria Tieghi** (ServiTecno s.r.l. – Amministratore Delegato) *Industrial Internet, IIoT, Cybersecurity, Cloud e dispositivi mobili per sistemi di controllo e telecontrollo* **Torsten Noack** (Fox-IT – Central Europe & Eastern Europe, High Assurance Products) *Scada Cyber Security: the mammoth cost of not being prepared*
16.30	**Sessione 2 - il punto di vista accademico e aziendale (**moderatore **Stefano Panzieri)** **Federica Pascucci** (Università Roma Tre – Dipartimento di Ingegneria) *La contropartita fisica negli attacchi cyber alle Infrastrutture Critiche: il punto di vista dei controlli* **Andrea Guarino (**ACEA s.p.a. - Responsabile Security, Privacy & Compliance) *Outsmarting cyber attackers: ACEA and the PANOPTESEC experience* **Luigi Morabito (**Vitrociset s.p.a. - Business Unit Transport & Infrastructures) *ICS Cyber-Phisical Protection*
18.00	**Chiusura**

Associazione Italiana Esperti in Infrastrutture Critiche
00198 Roma, Via Spalato, 11 c/o Nitel - Tel. +39/06/64003640 e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Abstract delle relazioni

Claudio Pantaleo (Ass.Pri.Com.)

Introduzione al mondo SCADA

Il mondo delle connessioni ed elaborazioni informatiche non si limita a quello comunemente chiamato Internet o Office Network che più tecnicamente viene identificato con la sigla IT (Information Technology) ma è completato da una seconda parte chiamata Operational Technology (OT), che riguarda i sistemi di computer impiegati nello svolgimento, gestione e controllo di processi produttivi industriali.

Enzo Maria Tieghi (ServiTecno s.r.l.)

Industrial Internet, IIoT, Cyber Security, Cloud e dispositivi mobili per sistemi di controllo e telecontrollo

Il tema della OT Cyber Security (*OT sta per Operational Technology, l'altro lato della IT Information Technology*) che riguarda sistemi utilizzati per la gestione di impianti, sensori e macchinari nell'industria, nelle utility e nelle infrastrutture distribuite sul territorio, è oggi sempre più importante in quanto i sistemi sono connessi ed accessibili da remoto. Si parla di Industrial Internet, Internet of Things, Cloud, Industria4.0 ma anche di Utility4.0: la protezione di sistemi OT comporta approcci, metodologie, architetture e tecnologie differenti da quelli utilizzati per la difesa dei tradizionali sistemi ICT. In questa relazione si approfondisce il tema e si indicano alcuni aspetti peculiari da valutare nelle Infrastrutture Critiche, anche in vista dell'utilizzo di architetture e dispositivi innovativi, mutuati dal mondo industriale.

Torsten Noack (FOX-IT)

Scada Cyber Security: the mammoth cost of not being prepared (intervento in lingua inglese)

Cybersecurity view on the ICS/Scada market. What are the challenges, possible solutions and how do we think is the market going to develop.

Federica Pascucci (Università Roma Tre – Dipartimento di Ingegneria)

La contropartita fisica negli attacchi cyber alle infrastrutture critiche: il punto di vista dei controlli

Le infrastrutture critiche sono sistemi cyber-fisici in cui una parte informatica interagisce con una fisica: per questa particolare caratteristica, gli attacchi informatici possono avere impatti disastrosi a livello fisico. La sola rilevazione di attacchi informatici non cattura la complessità degli effetti che questi potrebbero avere sul sistema. D'altro canto, mentre esistono metodologie, tecniche e procedure per la rilevazione dei guasti fisici, più complessa è l'identificazione della causa del guasto quando essa proviene dal mondo cyber. In questa relazione si approfondisce il tema dell'identificazione delle anomalie fisiche dovute ad attacchi cyber, proponendo architetture di protezione innovative che considerino entrambi gli aspetti.

Andrea Guarino (ACEA s.p.a.)

Outsmarting cyber attackers: ACEA and the PANOPTESEC experience

L'argomento della presentazione consiste nell'analisi delle principali minacce volte al danneggiamento delle infrastrutture critiche informatizzate in genere, con esempi contestualizzati presi dai risultati raggiunti nell'ambito del progetto europeo FP7 "PANOPTESEC" (applicato ad Areti, già Acea Distribuzione) e delle principali e più efficaci strategie, tattiche e contromisure utilizzabili per gestire (e ridurre) i Cyber Risk.

Luigi Morabito (Vitrociset s.p.a.)

ICS Cyber-Phisical Protection

Oggi sempre più cresce la necessità di proteggere i cosiddetti Industrial Control Systems, che includono o sono basati su tecnologie SCADA, DCS e PLC. La situazione sempre più critica, aggravata dal fatto che questo tipo di sistemi è spesso presente in quelle che sono ad oggi identificate come infrastrutture critiche di un paese, ha spinto Vitrociset, che da sempre lavora in contesti critici, a far suo il concetto di "ICS cyber-phisical protection", studiando metodi, in ambito ICS, efficaci ed efficienti per assicurare elevati livelli di protezione.

Moderatori

Silvano Bari, Professore a contratto di "Valutazione del rischio" presso l'Università Campus Bio-medico di Roma e presso il Master in "Homeland Security", è certificato CISM (Certified Information Security Manager) e CEPAS (ISMS Senior Manager). E' stato Responsabile Sicurezza Informatica e Privacy di Alitalia. Ha svolto docenze presso le Università di Milano Politecnico, Padova, Roma Sapienza e Roma Tre. E' consulente aziendale sui temi della governance, della cybersecurity, della protezione dei dati personali. Ha partecipato a vari gruppi di ricerca istituiti da ACCREDIA, dall'Istituto Superiore delle Comunicazioni, dall'Associazione Italiana Information Systems Auditors (AIEA), dal Forum delle Competenze Digitali di INFORAV. E' vicepresidente di AIIC (Associazione Italiana Esperti in Infrastrutture Critiche) e socio di ISACA (Information Systems Audit and Control Association) e di ANDIG (Associazione Nazionale Docenti di Informatica Giuridica).

Stefano Panzieri, Professore Associato di Automatica presso Roma TRE. Vicepresidente del Comitato Unico di Garanzia dell'Ateneo Roma TRE. Responsabile del Laboratorio di Modellistica e Simulazione nel settore della Protezione delle Infrastrutture Critiche (MCIP Lab). Coordinatore di Ateneo del progetto per la Regione Lazio Smart Environments. Responsabile di ricerche sul tema della diagnostica energetica nell'ambito Smart Buildings. Coordinatore di alcuni progetti Europei sulle Infrastrutture Critiche. Coordinatore del Dottorato di Ricerca in Ingegneria Informatica e dell'Automazione. Dottore di Ricerca in Ingegneria dei Sistemi nel 1993 alla Sapienza. La sua attività di insegnamento si svolge nel settore dei Controlli Automatici, nei Sistemi di Controllo di Processo e nella gestione della sicurezza di grandi infrastrutture. Autore di più di 150 pubblicazioni in ambito internazionale sulle tematiche già citate e nel settore della Robotica.

Relatori

Enzo Maria Tieghi (ServiTecno s.r.l.), imprenditore, informatico, milanese, da oltre 30 anni si occupa di software per automazione e controllo di impianti, di security e compliance a standard e normative dei diversi settori industriali e delle infrastrutture in cui opera. E' Amministratore Delegato di ServiTecno srl di Milano, azienda che dal 1985 distribuisce e supporta software di GE Digital per sistemi OT industriale, SCADA, Industrial Internet, IIoT, Plant Intelligence, Analytics e tool per protezione di reti e sistemi nell'industria ed utility. Attivo in Associazioni di settore (AIIC, Clusit, CSA Cloud Security Alliance, ISPE, Anipla, ISA, AFI, Assintel, ecc.) ove coordina vari Gruppi di Lavoro, tiene lezioni e partecipa come speaker ad eventi specialistici sia in Italia che all'estero, oltre a contribuire con articoli e memorie a riviste specializzate e conferenze internazionali. Autore del Quaderno Clusit "Introduzione alla protezione di reti e sistemi di controllo ed automazione", ha curato l'edizione italiana del volume "SCADA Good Security Practices" per il settore delle acque potabili ed ha partecipato alla stesura del Rapporto Clusit 2012 sulla Sicurezza ICT in Italia e del ROSIv2.

Andrea Guarino (ACEA s.p.a.) è il responsabile per la Security, Privacy & Compliance presso la Funzione ICT di Acea SpA, una delle principali utility italiane, attiva nella gestione e nello sviluppo di reti e servizi nei business dell'acqua, dell'energia e dell'ambiente. E' un esperto di sicurezza informatica con oltre 30 anni di esperienza e attualmente segue con particolare interesse l'evoluzione delle minacce APT nelle Infrastrutture Critiche e nel mondo ICS-SCADA in generale. Partecipa spesso, anche come speaker, a tavoli istituzionali ed eventi nazionali e internazionali relativi alla sicurezza cibernetica. E' il team leader del progetto europeo FP7 "PANOPTESEC" per Acea SpA (www.panoptesec.eu).

Federica Pascucci (Università Roma Tre, Dip.to di Ingegneria) è ricercatore universitario presso l'Università degli Studi "Roma Tre" ed ha conseguito il Dottorato in Ingegneria dei Sistemi all'Università degli Studi di Roma "La Sapienza". I suoi interessi di ricerca includono le reti di sensori, la localizzazione in ambienti chiusi, i sistemi cyber-fisici. Si occupa da diversi anni di protezione delle infrastrutture critiche con riferimento a sistemi di diagnosi dei guasti in grado e di intrusioni informatiche. Ha pubblicato più di 70 contributi scientifici, ricevendo diversi premi. E' socia della AIIC dalla sua fondazione ed ha fatto parte del consiglio direttivo ricoprendo il ruolo di segretario.

Torsten Noack (FOX-IT) works in the IT Security for more than ten years. He is from Germany, but worked in the whole of Europe of the years. He always worked in Sales positions , was employed by the Deutsche Telekom, Wick Hill (a Security Distributor) as a Product Manager for WatchGuard and started working for WatchGuard Directly. Since then he worked for Palo Alto Networks as a Business Development Manager and since 2015 he works for Fox-IT being responsible for Central Europe & Eastern Europe for the High Assurance products of Fox-IT.

Claudio Pantaleo (Ass.Pri.Com.), ha ricoperto il ruolo di Direttore Sistemi e Tecnologie a Protezione del Patrimonio, in azienda leader, in Italia e all'estero, nel Trasporto Pubblico Locale (ATM Milano); precedentemente è stato il Direttore Sicurezza Aziendale per l'Italia e il Sud Europa, in primaria azienda multinazionale nel mondo del tabacco (BAT - British American Tobacco); la sua prima esperienza lavorativa di durata trentennale è stata in una multinazionale leader mondiale nel settore informativo (IBM), dove ha ricoperto ruoli tecnici sulle nuove tecnologie e ruoli commerciali, terminando come Direttore Sicurezza Aziendale. Durante la sua, oltre quarantennale, esperienze lavorativa, ha avuto l'opportunità di lavorare e vivere per lunghi periodi in molte geografie europee ed extra europee, dove ha completato la sua preparazione. Attualmente effettua consulenze direzionali ed attività di docenza universitarie o personalizzate alle necessità del Cliente.

Luigi Morabito (Vitrociset s.p.a.) è nato a Reggio Calabria, dove ha studiato presso la facoltà di ingegneria elettronica dell'Università Mediterranea degli Studi di Reggio Calabria, conseguendo la laurea nel Novembre del 2004. A Maggio del 2005 inizia la sua esperienza lavorativa in Vitrociset S.p.A. come analista software, ricoprendo poi negli anni numerosi ruoli, fino all'attuale posizione di system engineer con la responsabilità tecnica del competence center di monitoraggio e controllo. Completa la sua formazione professionale nel 2013-2014 frequentando il Master in Sicurezza delle Informazioni e Informazione Strategica presso l'Università di Roma La Sapienza. E' ad oggi responsabile tecnico di numerosi progetti legati a ICS e sistemi di monitoraggio e controllo per infrastrutture critiche.

Università Roma Tre – Dipartimento di Ingegneria – Sala Conferenze
Via Vito Volterra, 62

Come arrivarci:

Mezzi pubblici (raccomandato)

- *Tutti i Bus ATAC (128 – 170 – 761 – 766 791) con fermata a Viale Marconi/incrocio Largo Enea Bortolotti*
- *Metropolitana B, fermata Marconi, poi breve passeggiata a piedi*

Auto

- *Parcheggio lungo via Vito Volterra*

o lungo via della Vasca Navale (ingresso dal retro)