Newsletter N. 10

IN EVIDENZA

PER LA PRIMA VOLTA IN ITALIA LA CONFERENZA EUROPEA SULLA SECURITY RESEARCH

Nell'ambito del CPExpo 2014, si terrà il Security Event 2014 della Commissione Europea, evento organizzato dalla Commissione stessa sui temi della sicurezza che si tiene ogni anno dal 2006.
Un'occasione unica per entrare in contatto con lo staff della Commissione Europea e con tutti coloro che in Europa sono i principali attori in ambito ricerca in Security. Ci sarà anche un brokerage event per poter discutere progetti per la prossima call.

IN QUESTO NUMERO

EDITORIALE

Da questo numero attraverso la newsletter vogliamo evidenziare alcune attività svolte dai membri SERIT inerenti ad uno o più dei Settori Guida e delle Aree Tematiche in cui è suddivisa la Piattaforma SERIT.
Iniziamo con Cyber Security, che ha un suo specifico Settore Guida nella piattaforma SERIT, e che ha molti punti di contatto con altri settori ed aree tematiche. Nel farlo, traiamo anche spunto dal fatto che il mese appena passato, Ottobre, è stato il Cyber Security Month con molte iniziative di interesse che si sono tenute in Italia e all'estero.
La Sicurezza nell'ICT ha ormai assunto un ruolo importantissimo nell'ambito della Homeland Security. Secondo il rapporto Clusit 2014, nel 2013 nel mondo si sono verificati 2804 gravi attacchi informatici che hanno colpito enti, aziende e istituzioni di pubblico interesse. Un aumento degli attacchi del 245% rispetto ai dati relativi al 2011. Il Rapporto Clusit ha analizzato tra gli altri 35 gravi attacchi informatici che hanno colpito enti, istituzioni o aziende del nostro Paese. Oltre agli enti governativi, partiti e personalità politiche, nuovi bersagli dei cyber attacchi sono diventati sempre più di frequente anche le aziende

fornitrici di energia e le stesse forze dell'ordine.
Queste minacce stanno aumentando rapidamente e hanno ormai raggiunto livelli di elevata pericolosità e complessità. Un potenziale attacco totale che ormai tocca vari gangli nevralgici della sicurezza nazionale attraverso azioni sofisticate, mirate e coordinate condotte negli ultimi anni contro obiettivi sensibili, a riprova della mutata natura assunta dagli attacchi informatici e della dimensione globale che ormai li caratterizza.
Per combatterle occorre mettere in atto strategie altrettanto efficaci e mirate, anche attraverso progetti di ricerca che coinvolgano partner che provengono da settori differenti, in grado di mettere a sistema tecnologie, sistemi e ambiti di ricerca diversi fra loro. A livello Europeo la Commissione ha proposto la cyber security directive (NIS) (http://ec.europa.eu/digital-agenda/en/cybersecurity) che identifica una serie di misure che gli stati membri devono adottare per garantire un livello minimo di protezione da cyber attacchi. Anche l'Italia ha definito la sua cyber security strategy (http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html) mostrandosi pronta ed attenta a tali tematiche.
In questo numero parleremo di esempi virtuosi, che vedono la partecipazione di diversi partners della nostra piattaforma. Uno è il Distretto Tecnologico della Cyber Security, istituito a Cosenza e che coinvolge grandi imprese come Poste Italiane e NTT DATA Italia SpA, due PMI come Centro di Competenza ICT-SUD Scrl e NOVA Systems Roma srl e tre Organismi di Ricerca come Università della Calabria (Dipartimento DIMES), Università Mediterranea di Reggio Calabria e CNR– DIITET (Istituto ICAR).
Inoltre parleremo di numerosi progetti di cybersecurity che vedono protagonista Selex ES, accanto ad altri organismi di ricerca italiani come Enea, CNIT, CINI, RadioLabs, UniGenova.
La piattaforma SERIT, tramite il CNR, coordina anche il gruppo di lavoro su secure ICT research and innovation WG3 della piattaforma Europea NIS (Network and Information Security). A tal riguardo, l'8 ottobre a Firenze si è tenuto un seminario internazionale sulla tematica della ricerca ed innovazione in cyber security in cooperazione con vari Progetti di ricerca Europei.
Vi invitiamo inoltre a segnalarci altri esempi virtuosi di collaborazione in progetti di ricerca all'interno del Settore Guida 4, che riceveranno adeguato spazio nelle pagine del nostro sito www.piattaformaserit.it.
Chi volesse illustrare un progetto di ricerca in questo settore può inviarci una mail a info@piattaformaserit.it
Buona lettura e vi aspettiamo a CPEXPO 2014!

A COSENZA IL DISTRETTO TECNOLOGICO DELLA CYBER SECURITY

Il Distretto Tecnologico Cyber Security nasce con l'obiettivo di organizzare un centro di competenza nel settore della sicurezza informatica (Cyber Security) da realizzarsi nell'**Area di Cosenza** e rientra nelle iniziative di sviluppo e potenziamento del Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) finalizzate alla creazione di nuovi Distretti e/o nuove Aggregazioni Pubblico/Private" nell'ambito del Programma Operativo Nazionale "Ricerca e Competitività" 2007-2013 (PON R&C) per le Regioni della Convergenza (Calabria, Campania, Puglia, Sicilia).

Il Distretto vanta un'ampia prospettiva di **crescita tecnologica e di mercato**. Attraverso la creazione di una rete di attori pubblici e privati con esperienze, know how e capacità di intervento nei mercati di sbocco finali, vuole contribuire all'aumento della competitività delle imprese del Distretto e del sistema economico calabrese e nazionale.

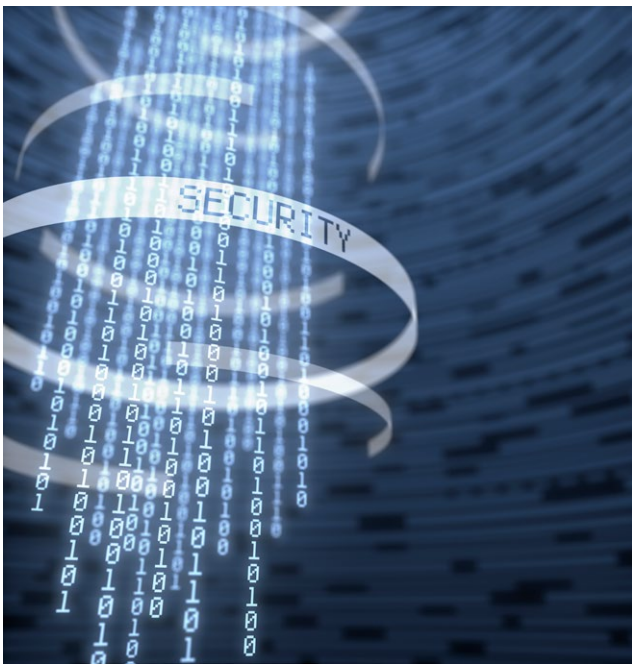
Il Distretto darà lavoro a 54 giovani laureati che saranno destinati ad attività di ricerca industriale e sviluppo sperimentale. La governance è affidata a un'Associazione Temporanea di Scopo (ATS) dei partecipanti, coordinata da Poste Italiane.

Partecipano al Distretto:

- **due Grandi Imprese**: Poste Italiane SpA e NTT DATA Italia SpA;
- **due Piccole e Medie Imprese (PMI)**: Centro di Competenza ICT-SUD Scrl e NOVA Systems Roma srl - ulteriori otto PMI calabresi partecipano alle attività del Distretto attraverso il coordinamento di ICT-SUD;
- **tre Organismi di Ricerca**: Università della Calabria (Dipartimento DIMES), Università Mediterranea di Reggio Calabria e CNR– DIITET (Istituto ICAR).

Il Distretto ha iniziato le sue attività sottoponendo tre proposte di progetti di ricerca industriale, che sono state approvate dal MIUR nel primo semestre del 2014:

- **Protezione dell'Utente Finale.** Con lo scopo di fornire una risposta scientifica e tecnologica alle necessità di sicurezza dell'utente finale nella fruizione di servizi in rete, preservando



riservatezza, integrità e disponibilità delle informazioni trattate.

I principali risultati previsti sono:

  - **Modelli di specifica** delle politiche di sicurezza e interazione degli utenti finali con i servizi internet ;
  - **Strumenti e metodi innovativi** di controllo della sicurezza degli accessi degli utenti finali e dei dispositivi utilizzati.
- **Protezione dei Sistemi di Pagamento Elettronici.** Ha come oggetto i sistemi digitali di pagamento sempre più utilizzati mediante l'ausilio di

tecnologie, dispositivi e architetture di rete evolute (Cloud computing e dispositivi mobili). I principali risultati previsti sono:

- **Modelli di riferimento e di specifica** per ridurre vulnerabilità e rischi nei sistemi di pagamento, sia lato utente, sia da quello dei servizi Web;
- **Tecniche e strumenti di sicurezza** basati su approcci di frontiera nella ricerca scientifica, per la gestione delle credenziali anonime e tecniche di intelligenza artificiale per fraud detection.

- **Dematerializzazione Sicura**. Il patrimonio informativo delle organizzazioni sta migrando dai formati cartacei a quelli digitali (basi di dati,data warehouseed ed event log). Il progetto intende proporre un approccio strutturato e innovativo per la protezione delle informazioni di un documento nel suo intero ciclo di vita (conservazione, utilizzo, copia, condivisione, trasformazione). I principali risultati previsti sono:
  - **Modelli di specifica** per il controllo della sicurezza nelle fasi di vita dei documenti digitali;
  - **Piattaforma end-to-end** di gestione sicura del ciclo di vita di un documento digitale.

DAI LABORATORI SELEX ES CYBER, UNA NUOVA SOLUZIONE INTEGRATA CONTRO I CYBER ATTACCHI

Tutte le infrastrutture vitali del Paese si basano i sull'ICT e sulla rete internet e sono minacciate da una criminalità tecnologica in crescente attività. Una qualsiasi perturbazione del funzionamento delle infrastrutture ICT può determinare gravi ripercussioni sulla crescita economica e su funzioni vitali della società. Esempi di questo tipo di perturbazioni sono i **"cyber-attacchi"** che hanno riguardato le reti Nato e quelle del governo Ucraino, gli attacchi portati verso le banche e le istituzioni Israeliane o gli attacchi verso siti istituzionali italiani e dello Stato Pontificio.

Per combattere questi crimini informatici, Selex ES ha sviluppato una soluzione che supporta la formazione di un quadro globale della **sicurezza delle reti e dei sistemi informativi** e capace di integrare informazioni di differenti tipologie e da fonti diverse.

Questa soluzione fornisce **funzionalità di analisi dinamica del rischio** e di valutazione continuativa dei possibili impatti di un eventuale attacco informatico sui processi e sui servizi operativi di una organizzazione, supportando anche l'individuazione

dei rimedi più opportuni.
Ampi e complessi dataset di informazioni vengono visualizzati tramite modalità grafiche che sintetizzano il risultato di analisi, sia automatiche che supervisionate, consentendo una **rapida comprensione degli eventi**. A completamento dell'approccio di difesa proattiva basata sulla rilevazione rapida degli attacchi e sulla velocizzazione dei processi di reazione, la soluzione realizza un continuo **monitoraggio** di fenomeni legati alle **attività criminali** nello sviluppo ed utilizzo di tecniche e strumenti malevoli. L'acquisizione di fonti a questo riguardo arricchisce le conoscenze e permette l**a formazione di una superiorità informativa** rispetto agli attaccanti, utile ad anticipare il rischio.
In particolare, sono realizzate:

- **le acquisizione di flussi di informazioni commerciali** o di pubblico dominio relative alla descrizione di attacchi già realizzati, degli agenti di attacco, degli indicatori di rischio.
- **la capacità di ricerca** di informazioni provenienti da sistemi esposti liberamente su internet (web 2.0; deep/dark web) e da repository proprietarie.

Selex ES è uno dei principali nodi del tessuto industriale a livello nazionale ed Europeo in grado di realizzare e facilitare la collaborazione con enti di ricerca nazionali sui temi della gestione del rischio, del'intelligence informativo e della protezione delle infrastrutture critiche nazionali, con specifiche esperienza realizzate con Enea, CNIT, CINI, UniRoma1-CIS, RadioLabs, UniGenova. Alla costituzione della soluzione descritta ha contribuito la partecipazione di Selex ES in programmi di ricerca, come ad esempio:
- **SawSoc**: EU-FP7 Security Call 5, svilupperà un "Security Operation Center" in grado di supportare il rilevamento e la diagnosi di attacchi in maniera accurata, tempestiva ed affidabile.
- **Gamma**: EU-FP7 Security Call 5, svilupperà metodi per una valutazione completa delle minacce e vulnerabilità delle strutture di controllo del traffico aereo (ATM), considerandone sia gli aspetti tecnologici che di processo operativo.
- **RoMA**: MIUR Smart Cities & Communities. Nel quadro dello sviluppo di un centro servizi per supportare la resilienza delle aree metropolitane, si vogliono sperimentare tecniche di "Open Source Intelligence" finalizzate alla formazione della conoscenza e supporto alle decisioni nel tema della sicurezza del cittadino e della protezione delle infrastrutture critiche metropolitane.
- **nSHIELD**: ARTEMIS JU, il progetto dimostrerà metodi di composizione dinamica della SPD (Security, Privacy, Dependability) nel contesto delle reti di sistemi embedded e metterà le basi per la definizione di embedded "SPD-ready".
- **MCDC**: NATO "Multinational Capability Development Campaign" 2013-14, autofinanziamento. Ha lo scopo di sviluppare ed introdurre nuove funzionalità per migliorare l'efficacia operativa della forza di coalizione nelle operazioni congiunte (Combined Operational Access), focalizzando lo studio delle capacità necessarie di una azione congiunta in una zona operativa. Selex ES ha contribuito allo studio di un concetto relativo alla costituzione di una conoscenza di scenario sulla sicurezza cyber nell'area di intervento, ottenuta anche tramite capacità di intelligence informativo.

CPEXPO 2014 AND EUROPEAN SECURITY RESEARCH CONFERENCE

In occasione del semestre europeo a Presidenza italiana, la Regione Liguria organizza a Genova, dal 9 all'11 dicembre 2014 il CPExpo 2014, per promuovere le tecnologie e le imprese operanti nel settore della "Secure Society".
CPExpo è una iniziativa annuale, con contenuti misti di natura espositiva e congressuale, dedicata ai temi delle tecnologie per la sicurezza, dalla cyber security alla protezione delle infrastrutture nazionali critiche, dalla protezione delle coste a quella dei confini, dalla salvaguardia e prevenzione dalle calamità naturali, ai provvedimenti per la cosiddetta "business continuity", compresi analisi e studio delle forme più opportune per contenere gli effetti che qualunque evento calamitoso o terroristico lascia sulla popolazione ed in particolare sulle fasce più deboli.
Nell'ambito del CPExpo 2014, si terrà il Security Event 2014 della Commissione Europea, evento organizzato dalla Commissione stessa sui temi della sicurezza che si tiene ogni anno dal 2006.
Il primo venne organizzato a Vienna in occasione della Presidenza austriaca dell'Unione Europea.
Le edizioni successive si sono tenute a Berlino, Parigi,Stoccolma, Ostenda (Belgio) e, più recentemente, a Varsavia e Parigi sempre con l'appoggio delle rispettive presidenze dell'UE.
L'evento, che si terrà negli spazi espositivi dei Magazzini del Cotone presso il Porto Antico di Genova, è stato inserito fra le iniziative della Presidenza del Consiglio nell'ambito del semestre di Presidenza italiana dell'Unione Europea ed è promosso da Regione Liguria in collaborazione con il Ministero della Difesa ed il Ministero dell'Istruzione, dell'Università e della Ricerca, il Ministero degli Interni, il Distretto tecnologico SIIT, l'Università di Genova, il CNR ed il Distretto Tecnologico DLTM.
L'agenda di CPExpo 2014 è consultabile in bozza sul sito dell'evento: www.cpexpo.it.

SEMINAR ON ROAD MAPPING CYBERSECURITY RESEARCH AND INNOVATION

L'8 Ottobre, in concomitanza con gli ICT proposers day, si è tenuto a Firenze il seminario internazionale sulle attività di ricerca ed innovazione sulla cyber security. Durante il seminario, organizzato dalla Comunita' Europea (gruppo di lavoro WG3 della piattaforma NIS guidato da Fabio Martinelli), in cooperazione con i due progetti Europei CAPITAL e SECCORD (CSP Forum) numerosi speakers italiani e più di 150 delegati hanno dibattuto sulle esigenze e sulle sfide che la cyber security pone al complesso industriale Europeo.
Durante la giornata è stata discussa la strategic research agenda della Comunità Europea sulla cyber security che dovrebbe essere presentata nel Marzo 2015.
Il prossimo meeting del WG3 si terrà a Madrid il prossimo febbraio in cooperazione con il progetto Europeo TDL. Maggiori informazioni sul seminario possono essere trovate sulla pagina: http://seminarcybersecurity.eventbrite.com/

COMITATO CURATORE DELLA NEWSLETTER

Michela Alunno Corbucci, Stefania Fabbri, Cristina Leone, Fabio Martinelli, Luca Papi, Gian Mario Scanu, Anna Vaccarelli, Grafica: Francesco Gianetti,
hanno collaborato a questo numero: Leonardo Fiocchetti (Selex ES) Giuseppe Manco (ICAR-CNR)