Cari colleghi,

Focalizzeremo questo numero della newsletter principalmente sulle proposte progettuali presentate nella 5°call che hanno avuto una valutazione positiva e che saranno, molto probabilmente, finanziate per portare avanti le attività di ricerca.
Queste idee progettuali sono nate dall'aggregazione delle competenze dei diversi membri di SERIT e hanno contributo a rafforzare la presenza italiana in ambito di ricerca per la sicurezza a livello europeo, secondo quanto ci eravamo proposti di raggiungere come obiettivo lo scorso anno.
L'ottimo risultato conseguito sarà un nuovo punto di partenza e un ulteriore stimolo per portare avanti ed ampliare le attività della piattaforma.

Buona navigazione!
Cristina Leone e Fabio Martinelli

In questo numero

Security research in Italy

I progetti premiati nella V Call Security FP7

Sono tre i progetti che hanno ottenuto le migliori valutazioni nella V call Security che si è conclusa il 23 novembre. All' iniziativa promossa da SERIT lo scorso anno, nata con lo scopo di rafforzare lapartecipazione italiana nel contesto europeo, hanno partecipato 8 progetti, frutto dell'unione delle diverse expertise dei partner SERIT. I progetti premiati sono stati: il progetto EDEN, il progetto SAWSOC e il progetto TAWARA RTM.

Il progetto EDEN (End-user driven DEmo for cbrNe) punta a valorizzare strumenti e metodi provenienti da precedenti attività di Ricerca e Sviluppo con la finalità di accrescere la capacità di risposta ad eventi CBRNE attraverso la loro integrazione a livello multi nazionale. Una parte corposa del progetto prevede la validazione sul campo delle soluzioni proposte. Coordinato da BAE Systems (UK) e accompagnato dal prestigioso rank di Collaborative Project, il progetto ha 39 partners di cui ben 7 sono italiani con l' ENEA capofila nelle attività di ricerca. **Selex Galileo**, **Selex SI** e **Tecnoalimenti** rivestiranno un ruolo di primo piano nell'ambito dello sviluppo industriale.
Infine l'attività dell'**Istituto Affari Internazionali**, l'**Università cattolica del Sacro Cuore** e il **Centro per la Scienza la Società e la Cittadinanza** sarà finalizzato ad indirizzare il progetto secondo le reali necessità dei vari end-users.

SAWSOC (Situation AWare Security Operations Center) è una proposta di Capability Project sulla convergenza tra sicurezza fisica e logica, una tematica di grande interesse, sia per le importanti sfide in termini di tematiche di ricerca che per le enormi potenzialità commerciali. Il progetto si concentra su tre casi di studio: la protezione di un'infrastruttura critica per la gestione del traffico aereo; la protezione di un'infrastruttura critica per la produzione e la distribuzione di energia elettrica e la protezione di un luogo pubblico, in questo caso uno stadio, nel corso di un evento. Coordinatore del progetto é **Selex Elsag Spa**. Il coordinamento tecnico é del **Consorzio Interuniversitario Nazionale per l'Informatica** (CINI).

Il progetto TAWARA_RTM (TAp WAter RAdioactivity Real Time Monitor) ha come obiettivo lo sviluppo di una piattaforma completa per il controllo on-line della radioattività dell'acqua erogata dagli acquedotti. La piattaforma misurerà l' attività alfa e beta per verificare se si è nei limiti stabiliti dalla legislazione europea o se si raggiungono limiti che richiedono rapide azioni. In questo caso il management dell' acquedotto verrà allertato e si attiverà una seconda parte del sistema per definire il tipo di contaminazione. Il prototipo del sistema verrà installato nella North Waterworks Plant dell' acquedotto di Varsavia (MPWIK). Il coordinamento del progetto sarà dell' **Università di Padova** con partecipazione italiana dell' **Università di Pisa**, dell' **ENEA** e della **CAEN SpA**.

FOCUS On

Il gruppo di Telecomunicazioni Multimediali Satellitari dell'università di Roma "Tor Vergata", unità di ricerca del consorzio NITEL ha presentato al "2nd International Security Symposium", organizzato dall'ESA presso ESRIN, una relazione sulla rilevanza dell'infrastruttura e delle architetture protocollari nell'approccio alla protezione dei dati, sviluppando un emulatore di rete satellitare in grado di riprodurre il funzionamento di una rete che può essere configurata per attività di dimostrazione di casi di studio di attacchi e di attuazione di contromisure. Durante il simposio, sono state presentate in particolare due sessioni demo mirate a riprodurre attacchi IP che sfruttano le vulnerabilità delle reti satellitari con relative proposte di contromisure. Il primo attacco fa leva sulla presenza di acceleratori PEP nei due estremi di un collegamento satellitare. La presenza di PEP è fondamentale per il conseguimento di prestazioni accettabili, ma allo stesso tempo introduce specifiche vulnerabilità legate alla violazione della semantica "end-to-end" del protocollo TCP. Nella dimostrazione è stato proposto come possibile contromisura un Intrusion Dection System (IDS) che monitorizza possibili asimmetrie di traffico ai due estremi di un collegamento satellitare oltre all'evoluzione di connessioni TCP aperte. Il secondo ha riguardato l'analisi dell'effetto di una botnet istallata in una LAN interfacciata ad un terminale satellitare. La finalità di quest'ultima dimostrazione è quella di valutare l'impatto dell'introduzione di traffico indesiderato sulle dinamiche di assegnazione di banda su domanda nel canale di ritorno satellitare.

Eventi SERIT

• **La scadenza per la partecipazione al SERIT Award è stata posticipata al prossimo 30 Aprile.** Il SERIT AWARD è un riconoscimento per il laboratorio pubblico che si è distinto per la ricerca e l'innovazione in ambito Security. Un comitato di valutazione, analizzerà i diversi requisiti dei laboratori candidati, sulla base dei criteri di Eccellenza Tecnologica & Innovazione, Eccellenza Gestionale, Ambiente di lavoro. Potete trovare regolamento e scheda di candidatura sul sito:
http://www.piattaformaserit.it/?p=1239, compilare e inviare ad info@piattaformaserit.it.
La premiazione avverrà durante la prossima riunione plenaria SERIT .

• **Il 22-23 Maggio si terranno a Bruxelles gli SMI2G days** (Security Mission Information & Innovation Group), un Open Forum organizzato da industrie ed enti di ricerca europei, al fine di stabilire network, cooperazione e partnership a livello europeo.
Gli SMIG2G days saranno l'occasione avere informazioni sulla prossima call; attivare partnership attorno ad idee progettuali; scambiare informazioni su specifici contributi e fornire opportunità di networking per trovare partner per le proposte che si vogliono presentare.

Nuovi partners

- Maglan Europe Srl
- CNR IEIIT
- Università degli Studi di Parma, Dipartimento di Scienze Ambientali
- C.R.A.M. Centro Ricerche Anti Malware di TG Soft
- Istituto Italiano di Studi Strategici Niccolò Machiavelli
- SASD - Studio Analisi Sicurezza e Difesa

Ultima Ora

• **E' on line il documento di lavoro (non ancora ufficiale) relativo alla prossima 6° Call Security – FP7.**
Per visionarlo, accedere al sito : https://ec.europa.eu/research/participants/portal/ShowDoc/Extensions+Repository/General+Documentation/Orientation+papers+2013/Cooperation/fp7-sec-2013-orientation-paper-working-doc_en.pdf.

Comitato curatore della Newsletter
Michela Alunno Corbucci, Stefania Fabbri, Gian Mario Scanu, Cristina Leone, Fabio Martinelli, Luca Papi, Daniele Sgandurra, Anna Vaccarelli;
Grafica: Francesco Gianetti **Hanno contribuito a questo numero**: Prof. Michele Luglio, Antonio Palucci, Giuseppe Viesti, Luigi Romano.

SERIT Security research in Italy