Relazioni triennali - Terza sessione 2014
Data Chiusura 23/01/2015

Cognome	FOCARDI
Nome	Riccardo
Qualifica	Professori Associati
Dipartimento	Dipartimento di Scienze Ambientali, Informatica e Statistica
Ha usufruito di un periodo di congedo per motivi di studio nel triennio	No

Descrizione attività di ricerca

In questi tre anni l'attività di ricerca di Riccardo Focardi si è focalizzata su: analisi di Security API, Sicurezza delle reti e del Web e sicurezza dei sistemi.

- Analisi di Security APIs

Le Security APIs (Application Programming Interfaces) sono interfacce di programmazione perdispositivi sicuri, quali smartcard e token di autenticazione, in grado disvolgere operazioni crittografiche su dati sensibili. A settembre 2013, Riccardo Focardi ha fondato, assieme a colleghi di INRIA, Francia, lo spin-off Cryptosense, che si occupa dello sviluppo di software per l'analisi della sicurezza di sistemi crittografici, con particolare attenzione a sistemi bancari e sistemi ad alto rischio di frode informatica. Cryptosense trasferisce nel mondo industriale la ricerca accademica sulle Secuirty APIs svolta da Riccardo Focardi negli ultimi anni. Per maggiori informazioni: http://cryptosense.com/

- Sicurezza delle reti

Mignis è un software per la configurazione di firewall basato su una semantica formale. Permette di specificare regole di firewall in modo estremamente leggibile e intuitivo. Le specifiche dichiarative vengono compilate in regole Netfilter (iptables) che possono essere eseguite su un qualsiasi sistema Linux. Un teorema garantisce che la traduzione preserva la semantica della specifica. Mignis è stato presentato al IEEE Computer Security Foundation Symposium 2014 ed è disponibile su github: https://github.com/secgroup/Mignis

- Sicurezza del Web

Il Web è estremamente flessibile e complesso e, di conseguenza, molto difficile da proteggere. CookieExt and SessInt sono estensioni del browser Chrome basate su uno studio formale della sicurezza Web. Implementano meccanismi lato client che permettono di migliorare la sicurezza del Web per l'utente finale. La sicurezza dei meccanismi implementati è stata dimostrata formalmente su un modello matematico, e i risultati sono stati pubblicati nel 2014 al International Symposium on Engineering Secure Software and Systems e al IEEE Computer Security Foundation Symposium.

- Sicurezza dei sistemi

Gran è uno strumento software per l'analisi di politiche di controllo degli accessi in sistemi grsecurity, una versione "hardened" di Linux che permette un sofisticato controllo degli accessi basato sui ruoli degli utenti e delle applicazioni. Gran è basato su un modello matematico di grsecurity e su una astrazione la cui correttezza è stata dimostrata formalmente. Lo strumento di analisi verrà incorporato nelle prossime versioni di grsecurity. Gran è stato presentato al IEEE Computer Security Foundation Symposium nel 2012 ed è disponibile su github. Per maggiori informazioni: http://secgroup.dais.unive.it/projects/grsecurity/

Elenco delle pubblicazioni degli

2014

Michele Bugliesi, Stefano Calzavara, Riccardo Focardi, Wilayat Khan, Mauro Tempesta.

ultimi 3 anni solari

Provably Sound Browser-Based Enforcement of Web Session Integrity
In: Proceedings of the 27th Computer Security Foundations Symposium. IEEE, ISBN: 9781479942909
Contributo in volume

M. Bugliesi, S. Calzavara, R. Focardi, W. Khan.
Automatic and robust client-side protection for cookie-based sessions
In: 6th International Symposium, ESSoS 2014., Springer, ISBN: 9783319048963
Contributo in Atti di convegno

Pedro Adão, Claudio Bozzato, Gian-Luca Dei Rossi, Riccardo Focardi, Flaminia Luccio.
A semantic based tool for firewall configuration
In: 2nd Workshop on Hot Issues in Security Principles and Trust (HotSpot 2014). Grenoble, France, 5th April 2014, no formal editor
Abstract in Atti di convegno

P. Adão, Claudio Bozzato, Gian-Luca Dei Rossi, R. Focardi, F.L. Luccio.
Mignis: A semantic based tool for firewall configuration
In: CSF 2014. pp. 15, IEEE, ISBN: 9781479942909
Contributo in volume

2013

Matteo Centenaro, Riccardo Focardi, Flaminia L. Luccio.
Type-based Analysis of Key Management in PKCS#11 cryptographic devices
JOURNAL OF COMPUTER SECURITY, 21;
Articolo in rivista

Pedro Adão, Riccardo Focardi, Flaminia L. Luccio.
Type-Based Analysis of Generic Key Management APIs
In: IEEE CSF. IEEE Computer Society, ISBN: 9780769550312
Contributo in volume

2012

R. Focardi, F. Luccio.
Towards a type-based analysis of real PKCS#11 devices
In: Proceedings of the 6th International Workshop on Analysis of Security APIs (ASA 2012). Cambridge MA, USA,, June 28 2012, non definito
Abstract in Atti di convegno

M. Centenaro, R. Focardi, Flaminia Luccio.
Type-Based Analysis of PKCS#11 Key Management
In: Principles of Security and Trust. 7215, Springer Berlin Heidelberg, ISBN: 9783642286407
Contributo in volume

R. Focardi, Flaminia Luccio.
Guessing Bank PINs by Winning a Mastermind Game
THEORY OF COMPUTING SYSTEMS, 50 (1);
Articolo in rivista

R. Focardi, F. Luccio.
Secure recharge of disposable RFID tickets
In: FAST 2011. Leuven; Belgium, Germany: Springer Verlag Germany, 7140, ISBN: 9783642294198
Contributo in Atti di convegno

R. Focardi, F. Luccio, M. Squarcina.
Fast SQL Blind Injections in High Latency Networks.
In: Security and Privacy Special Track, IEEE-AESS Conference in Europe about Space and Satellite Communications (ESTEL'12). Roma, 2-5/10/2012, IEEE COMPUTER SOCIETY, ISBN: 9781467346870
Contributo in Atti di convegno

BUGLIESI M.; CALZAVARA S.; FOCARDI R.; SQUARCINA M;.
Gran: model checking grsecurity RBAC policies
In: CSF 2012. Cambridge, Massachusetts, USA, 25-27 June 2012, IEEE Computer Society, ISBN: 9780769547183
Contributo in Atti di convegno

R. Bardou, R. Focardi, Y. Kawamoto, L. Simionato, G. Steel, J. Tsay.
Efficient Padding Oracle Attacks on Cryptographic Hardware
In: CRYPTO 2012. Santa Barbara, CA, USA, August 19-23, 2012, Germany: Springer Verlag Germany, ISBN: 9783642320088
Contributo in Atti di convegno

Riccardo Focardi.
Practical Padding Oracle Attacks on RSA
In: Defend Yourself! Hands-on Cryptography. Hackin9, IT Security Magazine
Contributo in volume

Elenco delle pubblicazioni in corso di stampa	Nessun documento
Altri prodotti scientifici	Dato non presente
Partecipazione a comitati editoriali di riviste/collane scientifiche	Journal of Computer Security (JCS) - IOS Press - member of the Editorial Board
Partecipazione come referee di progetti di ricerca nazionali ed internazionali	È stato revisore di progetti finanziati dalla Comunità Europea e progetti FIRB nazionali
Menzioni e premi ricevuti	Dato non presente
Relazioni invitate presso convegni o workshops	"Analisi automatica di sistemi crittografici". Convegno Soluzioni e sicurezza per applicazioni mobile e payments. ISACA. Venezia 27 settembre 2013. "Sicurezza e riservatezza dei dati clinici: minaccia o opportunita?". Convegno Navigando verso il Fascicolo La prossima sfida. Arsenal.IT, Treviso. 15 ottobre 2014. "Cryptosense: Analisi automatica di dispositivi crittografici". Convegno Nazionale Cyber Security. Centro Studi Difesa e Sicurezza (CESTUDIS) e Dipartimento informazione e sicurezza della Presidenza del Consiglio dei Ministri. Roma, 1 Dicembre 2014.
Seminari su invito tenuti presso altre Università, Centri di Ricerca, Aziende,...	"An Introduction to Computer Security". Generali Group Innovation Academy, Mogliano Veneto. 25 settembre 2012. "Role-based Access Control in Real Systems". Generali Group Innovation Academy, Mogliano Veneto. 26 settembre 2012. Ciclo di seminari su "Scripting, programmazione a Oggetti e crittografia". Presso l'azienda Yarix S.r.l., Montebelluna. Giugno/Luglio 2013. "A semantic based tool for firewall configuration". Laboratory for Foundations of Computer Science (LFCS), University of Edinburgh. 24 Gennaio 2014. "Semantic based tools for practical security". Security & Trust Research Unit, Fondazione Bruno Kessler, Trento. 21 Ottobre 2014.
Altre attività scientifiche: partecipazione a comitato scientifico di conferenze, peer-review di articoli sottomessi a riviste o convegni, etc.	Partecipazione a comitati scientifici di conferenze: IEEE CSF'14 (PC member) IEEE Computer Security Foundations Symposium. Vienna, as part of the Vienna Summer of Logic, July 19-22, 2014. ESORICS'13 (PC member) European Symposium on Research in Computer Security. Egham U.K. at Royal Holloway, University of London on 9th – 11th September 2013. IEEE CSF'13 (PC member) IEEE Computer Security Foundations Symposium. Tulane University, New Orleans, LA, June 26-28, 2013. ACM CCS'12 (PC member) ACM Computer and Communications Security Conference. Oct. 16-18, 2012, Sheraton Raleigh Hotel, Raleigh, NC, USA. ESORICS'12 (PC member) European Symposium on Research in Computer Security. September 2012 in Pisa, Italy. IEEE CSF'12 (PC member) IEEE Computer Security Foundations Symposium. Harvard University, Cambridge, MA, USA, June 25-27, 2012.

CISIM'13 (PC member) International Conference on Information Systems and Industrial Management. Krakow 2013, September 25-27.

CISIM'12 (PC member) International Conference on Information Systems and Industrial Management. Venice, Italy, September 26-28, 2012.

Contratti di Ricerca e Finanziamenti esterni del triennio

Security Horizons

Attività Didattica: insegnamenti negli ultimi tre anni accademici

Anno accademico	Nome corso	Codice corso	Voto medio	Voto medio ponderato di facoltà
2014	SISTEMI OPERATIVI	CT0125		
2014	SECURITY OF COMPUTER SYSTEMS	CM0228		
2013	SECURITY OF COMPUTER SYSTEMS	CM0228	2,94/4	3,05/4
2013	SISTEMI OPERATIVI	CT0125	3,29/4	3,05/4
2012	SISTEMI OPERATIVI	CT0125	3,7/4	3,2/4
2012	SECURITY OF COMPUTER SYSTEMS	CM0228	3,8/4	3,2/4
2011	SECURITY OF COMPUTER SYSTEMS	CM0228	3,7/4	3,1/4
2011	SISTEMI OPERATIVI	CT0125	3,3/4	3,1/4
2010	SISTEMI OPERATIVI	CT0125		
2010	SECURITY OF COMPUTER SYSTEMS	CM0228		
2010	SICUREZZA	CM0089		

Altra attività didattica (attività integrativa, insegnamenti di master o dottorato, etc.)

Anno accad.	Titolo del corso	Sede	Note
2012-13	Sicurezza delle applicazioni web	Ca' Foscari	Laboratorio Ca' Foscari Summer School, in collaborazione con Kima Projects & Services e ISACA Venice
2013-14	Rischi e minacce nel mondo digitale	Digital Academia	Intervento all'interno del Master MADEE IV
2013-14	Insicurezza nel mondo digital	Digital Academia	Intervento all'interno del Master MADEE V
2014-15	Cyber security and insecurity	Digital Academia	Intervento all'interno del Master MADEE VI
2012-2013-2014	Orientamento studenti scuole superiori: Sicurezza e Crittografia	Ca' Foscari	Laboratori di orientamento per gli studenti delle scuole superiori

Tesi di laurea seguite come relatore

Anno solare	n. Tesi triennali	n. Tesi magistrali	n. Tesi dottorato
2014	3	4	1
2013	1	1	0
2012	6	1	0
2011	2	1	1

Incarichi accademici e attività organizzative

Incarichi accademici/attività organizzative/partecipazione commissioni giudicatrici	Ateneo/Facoltà/Dipartimento/altri organi collegiali	Compiti istituzionali/cariche elettive/nomine dirette
Dato non presente	Dipartimento di Scienze Ambientali, Informatica e Statistica, Ca' Foscari	Coordinatore Dottorato di Ricerca in Informatica
Commissione per la procedura valutativa per la copertura di n. 1 posto di Professore associato (II fascia)	Università di Verona	Dato non presente
Commissione di ammissione dottorato trentesimo ciclo	Università Ca' Foscari, Venezia	Dato non presente
Presidente commissione esame finale ventiseiesimo ciclo di dottorato	Università Ca' Foscari, Venezia	Dato non presente
Commissione valutazione assegno di ricerca	Dipartimento di Scienze Ambientali Informatica e Statistica	Dato non presente
Comitato organizzatore convegno "Application Security: internet, mobile ed oltre"	Ca' Foscari in collaborazione con ISACA Venice	Dato non presente

Attività Professionali esterne

Incarichi esterni non accademici -partecipazione a collegi/comitati/commissioni –consulenze-associazioni professionali-attività editoriali	Ente o istituzione	Compiti istituzionali/cariche elettive/nomine dirette	periodo
Dato non presente	Cryptosense	Chief Scientist	da Settembre 2013

Altre informazioni

Oggetto	Periodo	Note
Abilitazione Scientifica Nazionale come Professore Ordinario	29/01/2014	Abilitazione Settore Concorsuale 01/B1 - I Fascia
Supervisore assegno di ricerca FSE per l'anno 2013	2013	"Sicurezza delle informazioni nel territorio veneto", in collaborazione con l'azienda Yarix