ALLEGATO B

UNIVERSITÀ DEGLI STUDI DI MILANO
selezione pubblica per n. 1 posto di Ricercatore a tempo determinato ai sensi dell'art.24, comma 3, lettera b) della Legge 240/2010 per il settore concorsuale 01/B1 - Informatica , settore scientifico-disciplinare INF/01 - Informatica presso il Dipartimento di INFORMATICA "GIOVANNI DEGLI ANTONI" (avviso bando pubblicato sulla G.U. n. 7 del 25/01/2019 Codice concorso 3964

Antonino Rullo
CURRICULUM VITAE

INFORMAZIONI PERSONALI (NON INSERIRE INDIRIZZO PRIVATO E TELEFONO FISSO O CELLULARE)

COGNOME	**RULLO**
NOME	**ANTONINO**
DATA DI NASCITA	25,12,1983

1 Note Biografiche e Posizioni Ricoperte

1.1 Attività di studio

Nel luglio 2011 ho conseguito la Laurea Specialistica in Ingegneria Informatica presso l'Università della Calabria con voti 108/110 discutendo la tesi dal titolo "Optimizing OXPath" (i risultati del lavoro di tesi sono descritti nell'articolo [C9]), relatori: Prof. Domenico Saccà, Prof. Giovanni Grasso, Prof. Tim Furche. Il lavoro di tesi esplora metodi di ottimizzazione per il linguaggio di interrogazione per il Web OXPath, una estensione di XPath progettata nel laboratorio stesso.
Nell'aprile 2015 ho conseguito il titolo di Dottore di Ricerca in Ingegneria dei Sistemi e Informatica presso l'Università della Calabria discutendo la tesi dal titolo "Cyber Defense of Enterprise Information Systems: Advanced Issues and Techniques" (i risultati ottenuti sono descritti negli articoli [J2, J3, J4, C6, C7, C8]), relatori: Prof. Domenico Saccà, Prof. Andrea Pugliese. La tesi esplora metodi per la prevenzione e l'intercettazione di attacchi rivolti ai sistemi informatici.

1.2 Posizione attuale

Da febbraio 2019 ricopro la posizione di ricercatore post-doc con un assegno di ricerca nell'ambito del progetto EMPHASIS, all'interno del Dipartimento di Ingegneria Informatica, Modellistica, Elettronica e Sistemistica (DIMES) dell'Università della Calabria (UniCal).

1.3 Posizioni precedenti

Da settembre 2011 a maggio 2012 ho lavorato presso la società EXEURA S.r.L., nell'ambito del progetto di ricerca industriale "IDEAS - Un ambiente integrato per lo sviluppo di applicazioni e soluzioni".
Da luglio 2012 a giugno 2014 ho lavorato come assegnista di ricerca presso il DIMES, UniCal, nell'ambito del progetto di ricerca "TETRis - Servizi Innovativi Open Source su TETRA".
Da luglio 2014 a dicembre 2017 ho lavorato come assegnista di ricerca presso il DIMES, UniCal, nell'ambito del progetto di ricerca "Cyber Security - Servizi e Processi di Pagamento Elettronici".
Da febbraio 2018 a febbraio 2019 ho lavorato come assegnista di ricerca presso il DIMES, UniCal, con un assegno di ricerca di ateneo.
Da agosto 2015 a maggio 2016 sono stato Visiting Scholar presso il Lawson Computer Science Department, Purdue University, Lafayette, Indiana, USA.

2 Attività Didattica

Svolgo regolarmente attività didattica come esercitatore a partire dall'anno accademico 2012/13, ad eccezione dell'anno 2015/16 che ho trascorso presso la Purdue University, USA, come Visiting Scholar. Di seguito, la lista dei corsi.

- Sistemi Formali, Prof. Domenico Saccà, Corso di Laurea Magistrale in Ingegneria Informatica, Anno Accademico 2012/13, 2013/14, 2014/15, 2016/17, 2017/18, 2018/19. Argo menti trattati: Prolog, Datalog, JSon, automi riconoscitori, compilatori, linguaggi formali, grammatiche.

- Fondamenti di Informatica, Prof. Andrea Pugliese, Corso di Laurea Triennale In Scienze Politiche, Anno Accademico 2012/13. Argomenti trattati: Microsoft Word, Microsoft Excel.

- Informatica, Prof. Andrea Pugliese, Corso di Laurea Magistrale In Scienze Politiche, Anno Accademico 2014/15. Argomenti trattati: Microsoft Access.

- Fondamenti di Informatica, Prof.ssa Antonella Guzzo, Corso di Laurea Triennale in Ingegneria Gestionale, Anno Accademico 2016/17. Argomenti trattati: fondamenti di programmazione in Python.

3 Attività di Ricerca

La mia attività di ricerca si colloca principalmente nell'ambito della sicurezza informatica (cyber security). In particolare essa è incentrata su due linee principali:

- intercettazione di attacchi (intrusion/anomaly detection);
- prevenzione di attacchi (attack prevention).

toccando trasversalmente la teoria dei giochi (game theory), la programmazione lineare (linear programming), e gli algoritmi evoluzionari (evolutionary algorithms).

Altre linee di ricerca riguardano il tema dell' Inverse Frequent Itemset Mining (IFM), e del Process Mining (vedi Sezione 3.3).

3.1 Intrusion/Anomaly Detection

Identificazione di attività note e attività non spiegate. Il problema di identificare occorrenze di attività note all'interno di dati temporali è stato largamente studiato e numerose tecniche sono state proposte per questo scopo.
In ambito cyber security l'identificazione di attività note si è spesso tradotta nella progettazione di algoritmi per la detection di attacchi informatici in corso (malware o attacchi multi-steps). In questo contesto è molto importante che gli algoritmi abbiano un tempo di risposta molto breve e che il numero dei falsi positivi non renda il risultato della detection inutilizzabile per gli amministratori della sicurezza.
Un problema in un certo senso “complementare", di notevole importanza pratica, ma che ha ricevuto tuttavia poca attenzione, è il seguente: dato un insieme di modelli di attività note e dato un dataset di eventi, quali sono le porzioni del dataset dove accadono eventi che non sono catturati sufficientemente bene dai modelli noti? Per esemplificare questo problema, si consideri un'applicazione di videosorveglianza e si supponga di avere un video registrato in un aeroporto. Si supponga anche di avere un insieme di modelli di attività note, che permettono di identificare all'interno del video degli eventi che si è in grado di spiegare perchè si ha un modello. Il problema diventa quindi quello di identificare porzioni di video dove occorrono eventi che non è possibile spiegare sufficientemente bene con i modelli a disposizione (gli eventi che occorrono in queste parti di video potrebbero essere, ad esempio, nuove modalità con cui vengono eseguiti atti terroristici, e per i quali non si ha ancora un modello).

Un algoritmo e un indice per l'identificazione di attacchi noti sono stati proposti in [C7], dove gli attacchi vengono formalizzati secondo una struttura dati basata su grafi. In [J2, C8, C9], invece, viene proposto un modello basato su ipergrafi per la descrizione di attacchi in cui l'ordine dei passi che un attaccante deve seguire non è noto, o non è sempre uguale. Un algoritmo e un indice risolvono il problema della detection. Un'architettura parallela per l'identificazione di attività non spiegate è stata proposta in [J4]. Gli approcci proposti si basano su nozioni di teoria dei giochi, e si sono dimostrati efficienti ed efficaci nelle prove sperimentali.

Intrusion Detection Systems per IoT. Gli Intrusion Detection Systems (IDS) sono strumenti di sicurezza che utilizzano metodi come quelli descritti nel paragrafo precedente per intercettare gli attacchi in corso rivolti al sistema monitorato. La ricerca svolta in questo ambito è stata rivolta al campo dell'internet delle cose (Internet of Things - IoT). Oggi le applicazioni IoT sono sempre più numerose e trovano spazio nei più svariati ambiti: controllo del traffico, sistemi di illuminazione intelligenti, reti veicolari (vehicular networks), industria 4.0, domotica, etc. per citarne alcuni. La gestione della sicurezza per l'IoT è più complicata rispetto al domimio delle tradizionali reti di calcolatori, che sono caratterizzate dall'omogeneità e l'interoperabilità. Al contrario, l'eterogeneità dell'IoT espande la superfice d'attacco e i diversi scenari di sicurezza. Sulla base di queste considerazioni, ho concentrato la mia ricerca sulla progettazione di IDS per l'IoT in grado di auto-adattarsi alle caratteristiche dell'ambiente monitorato, e quindi scegliere le tecniche di detection più adatte al contesto [C1, C4, C11].

3.2 Attack prevention

Allocazione ottima delle risorse di sicurezza. In diversi scenari si presenta il problema di dover allocare delle risorse di sicurezza per impedire che utenti malevoli possano utilizzare un sistema in modo improrpio. L'ordine in cui vengono allocate le risorse disponibili implica un costo e un certo livello di sicurezza. Per trovare un buon compromesso tra il livello di sicurezza e il costo dell'infrastruttura può essere necessario l'utilizzo di un framework che permetta di formalizzare il sistema che si intende difendere, e che fornisca tutte le possibili soluzioni di interesse. Nell'ambito della cyber security il sistema in questione è spesso formalizzato secondo una struttura a grafo, in cui i nodi possono rappresentare dei computer, delle vulnerabilità software, dei dispositivi mobili, etc, e gli archi i collegamenti fisici e/o logici tra i nodi. In questo contesto una risorsa di sicurezza può essere un firewall, un Intrusion Detection System (IDS), un Intrusion Prevention System (IPS), un antivirus, sistemi di crittografia, etc. Per calcolare tutti i piani di allocazione delle risorse occorre un algoritmo che si basi sul principio di Pareto-ottimalità, cioè un algoritmo di ottimizzazione che soddisfi più obbiettivi allo stesso tempo.
In [J3] è stato proposto un framework per la formalizzazione delle vulnerabilità software e le loro dipendenze reciproche, e un algoritmo per il calcolo dei piani ottimi di allocazione delle patch, ognuno dei quali fornisce diversi valori di sicurezza in relazione a diversi valori di costo dell'infrastrittura, e di produttività del sistema che si intendende difendere. In [J1, C3, C6] un framework simile è stato proposto per reti IoT statiche, nelle quali i device che compongono la rete non cambiano posizione nel tempo. In questo contesto, la programmazione lineare è stata adottata come strumento principale per risolvere il problema della Pareto-ottimalità.

Nel contesto delle reti mobili, invece, in cui l'incertezza sulla dimensione e sulla forma del sistema monitorato è altamente caratterizzante, per il calcolo del piano di allocazione delle risorse sono stati utilizzati algoritmi evoluzionari, i quali assicurano una buona approssimazione della soluzione ottima [C1, C5]. In [B1], le tecniche di allocazione sopraccitate vengono presenate insieme e messe a confronto.

Fault tolerance e distributed ledgers. Da settembre 2018, insieme al Prof. Jeorge Lobo (Università Pompeu Fabra, Barcellona, Spagna), ho iniziato una ricerca nell'ambito della fault tolerance per sistemi IoT. Come primo risultato abbiamo prodotto una survey [B2] in cui vengono discussi i principali lavori sulla fault tolerance nell'ambito delle sensor networks, protocolli di routing, e sistemi di controllo. Attualmente è in corso la progettazione di un algoritmo per il consenso distribuito per

sistemi IoT, in cui interviene l'uso di una distributed ledger come struttura dati sulla quale basare il funzionamento dell'algoritmo.

3.3 Altre linee di ricerca

A partire dai primi mesi del 2018 ho iniziato ad interessarmi ad altre linee di ricerca diverse dalla sicurezza informatica. In particolare, in collaborazione con il Prof. Domenico Saccà (DIMES, UniCal), mi sono dedicato allo sviluppo di un algoritmo che risolve varianti del problema dell' Inverse Frequent Itemset Mining (IFM). Il problema dell'IFM consiste nel generare un database transazionale sintetico che soddisfi un insieme di vincoli, estratti da un database reale, espressi in termini di frequent itemsets. Le varianti proposte permettono di generare database sintetici con un livello di accuratezza maggiore rispetto all'IFM tradizionale. In più, è stato implementato un metodo basato sulla programmazione lineare per risolvere IFM e le sue varianti anche per databases no-SQL. In [J5] vengono discusse le varianti dell'IFM e l'algoritmo risolutore.
Dal dicembre 2018 ho iniziato ad interessarmi di Process Mining, in particolare, con la Prof.ssa Antonella Guzzo (DIMES, UniCal), ho iniziato uno studio sull'utilizzo del deep learning come strumento chiave per la detection di attività anomale dei processi [C12].

4 Attività di Revisione

Ho svolto attività di revisione per le seguenti riviste internazionali:

- IEEE Transactions on Services Computing (TSC);
- ACM Transactions on Internet Technology (TOIT);
- Computer Communications - Elsevier (COMCOM);
- IEEE Transaction on Mobile Computing (TMC);
- Computers & Security - Elsevier;
- Recent Advances in Communications and Networking Technology - BenthamScience;
- WIREs Data Mining and Knowledge Discovery (DMKD)

Ho svolto attività di revisione per le seguenti conferenze nazionali ed internazionali:

- 1st International Conference on Process Mining, June 24-26, 2019, Aachen, Germany
- Italian Conference on Cyber Security 2019 (ITASEC);
- 33rd ACM/SIGAPP Symposium On Applied Computing (SAC 2018);
- 13th International Conference on Network and Service Management (CNSM 2017);
- 30th International Florida Arti_cial Intelligence Resarch Society Conference (FLAIRS 2017);
- 11th ACM Asia Conference on Computer and Communications Security (ASIA-CCS 2017);
- 37th International Conference on Distributed Computing Systems (ICDCS 2017);
- 13th International Conference on Security and Privacy in Communication Networks (SecureComm 2017);
- 21st Italian Symposium on Advanced Database Systems (SEBD 2013);

5 Partecipazione a Progetti di Ricerca

Ho partecipato attivamente a vari progetti di ricerca, elencati di seguito.

- **IDEAS** Un Ambiente Integrato per lo Sviluppo di Applicazioni e Soluzioni: Fondo per l'Innovazione Tecnologica, PON legge 46/82, DM 24 Settembre 2009, B01/0686/03/X17 - progetto finalizzato alla realizzazione di una piattaforma per l'analisi dei dati, sia strutturati che testuali. L'attività lavorativa si è svolta presso la società EXEURA S.r.L., ed ha riguardato lo sviluppo in Java di algoritmi di Data Mining ad alte prestazioni.

- **TETRIS** Servizi innovativi Open Source su TETRA: _nanziato nell'ambito del Programma PON Ricerca e Competitività 2007/2013, Bando di Gennaio 2010, con l'obiettivo di estendere le tecnologie del protocollo di telecomunicazione TETRA e di sviluppare servizi innovativi basati su di esso, soprattutto in ambito smart cities.

- **CYBER SECURITY** Protezione dei servizi digitali e di pagamento elettronico: finanziato nell'ambito del Programma MIUR-PON Ricerca e Competitività 2007/2013. Il progetto ha come obiettivo la protezione dei servizi digitali e di pagamento elettronico, attraverso l'innovazione dei processi e la formulazione degli elementi di sicurezza per garantire i nuovi prodotti/servizi, attraverso l'analisi degli scenari di rischio speci_co e di quello sistemico che possono rappresentare pericoli all'intera operatività del sistema.

- **ID Service** Identità Digitale e service Accountability Metodologie e tecnologie innovative per la progettazione e lo sviluppo di infrastrutture per l'accountability di servizi cooperativi, anche basati su infrastrutture blockchain. Obiettivi della ricerca: Studio di modelli e tecniche per l'utilizzo dell'identità digitale in scenari di servizi cooperativi; Studio di modelli e tecniche per l'utilizzo di infrastrutture blockchain per accountability con identità certa .

- **EMPHAsis** - Effective Malware Prevention through Honeypot Assisted analysis. Emphasis prevede la realizzazione di un sistema innovativo che utilizza gli honeypot come mezzo per la prevenzione, la cattura, l^aanalisi morfologica e comportamentale di entità malevole che attaccano i sistemi informatici connessi in rete.

6 Permanenze all'Estero e Scuole di Formazione

Prima da studente e poi in qualità di assegnista post-doc, ho avuto la possibilità di trascorrere vari periodi presso università estere. In Particolare:

- Da settembre 2004 a luglio 2005 sono stato studente presso l'Universidad Politecnica de Valencia nell'ambito del progetto ERASMUS.

- Da febbraio a giugno 2011 ho condotto la ricerca per la tesi di laurea all'interno del laboratorio DIADEM (Domain Centric Intelligent Automated Data Extraction Methodology) presso il Department of Computer Science, University of Oxford, Oxford, UK, diretto dal Prof. George Gottlob.

- Da agosto 2015 a maggio 2016 sono stato Visiting Scholar presso il Lawson Computer Science Department, Purdue University, Lafayette, Indiana, USA, svolgendo attività di ricerca sulla sicurezza per l'internet delle cose (Internet Of Things), all'interno del gruppo di ricerca diretto dalla prof.ssa Elisa Bertino, con la quale continuo a collaborare.

Grazie alla lunga permanenza sia in Spagna che paesi anglofoni (Inghilterra e Stati Uniti), parlo sia la lingua spagnola che inglese ad un buon livello.
Durante il dottorato di ricerca ho partecipato alle seguenti scuole di formazione:

- 12th Summer School on Distributed Data Acquisition Systems", DIMES, UniCal, 2012.

- 5th Int. Summer School on Information Security and Protection", Dipartimento di Informatica, Università degli Studi di Verona, 2014.

7 Partecipazione a Conferenze Internazionali e Workshops

Al fine di presentare personalmente i risultati della mia ricerca, e di allargare le mie conoscenze in ambito scientifico, ho partecipato a diverse conferenze nazionali ed internazionali.

- 2018 IEEE Conference on Dependable and Secure Computing. Kaohsiung, Taiwan. (DSC 2018).
- 22nd European Symposium on Research in Computer Security. Oslo, Norway. (ESORICS 2017).
- 2nd IEEE International Conference on Internet of Things Design and Implementation. Pittsburg, USA. (IoTDI 2017);
- IEEE International Conference on Distributed Computing Systems. Nara, Japan. (ICDCS 2016);
- 22nd Italian Symposium on Advanced Database Systems. Sorrento, Italy. (SEBD 2014);
- 21st Italian Symposium on Advanced Database Systems. Roccella Jonica, Italy. (SEBD 2013);
- 23rdInternational Joint Conference on Arti_cial Intelligence. Beijing, China. (IJCAI 2013);
- Graph Knowledge Representation @IJCAI. (GKR 2013)
- IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. Istanbul, Turkey. (ASONAM 2012);
- Very Large Data Search @VLDB. Istanbul, Turkey. (VLDS 2012);

8 Elenco delle Pubblicazioni

8.1 Riviste

[J1] Antonino Rullo, Daniele Midi, Edoardo Serra, Elisa Bertino. Pareto Optimal Security Resource Allocation for Internet of Things. ACM Transactions on Privacy and Security (TOPS), 2017, 20.4: 15.

[J2] Antonella Guzzo, Andrea Pugliese, Antonino Rullo, Domenico Saccà, Antonio Piccolo. Malevolent Activity Detection with Hypergraph-Based Models. IEEE Transactions on Knowledge and Data Engineering (TKDE), 2017, 29.5: 1115-1128.

[J3] Edoardo Serra, Sushil Jajodia, Andrea Pugliese, Antonino Rullo, V. S. Subrahmanian. Pareto-Optimal Adversarial Defense of Enterprise Systems. ACM Transactions on Information and System Security (TISSEC), 2015, 17.3: 11.

[J4] Cristian Molinaro, Vincenzo Moscato, Antonio Picariello, Andrea Pugliese, Antonino Rullo, V. S. Subrahmanian. PADUA: Parallel Architecture to Detect Unexplained Activities. ACM Transactions on Internet Technology (TOIT), 2014, 14.1: 3.

8.2 Conferenze

[C1] Antonino Rullo, Elisa Bertino, Domenico Saccà. PAST: Protocol-Adaptable Security Tool for Heterogeneous IoT Ecosystems. 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan. IEEE, 2018. p. 46-53.

[C2] Antonino Rullo, Edoardo Serra, Elisa Bertino, Jorge Lobo. Shortfall-Based Optimal Placement of Security Resources for Mobile IoT Scenarios. European Symposium on Research in Computer Security (ESORICS), Oslo, Norway. Springer, Cham, 2017. p. 419-436.

[C3] Antonino Rullo, Daniele Midi, Edoardo Serra, Elisa Bertino. A Game of Things: Strategic Allocation of Security Resources for IoT. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburg, PA, USA. ACM, 2017. p. 185-190.

[C4] Daniele Midi, Antonino Rullo, Anand Mudgerikar, Elisa Bertino. Kalis - A System for Knowledge-Driven Adaptable Intrusion Detection for the Internet of Things. Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. IEEE, 2017. p. 656-666.

[C5] Antonino Rullo, Edoardo Serra, Elisa Bertino, Jorge Lobo. Shortfall-Based Optimal Security Provisioning for Internet of Things. Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. IEEE, 2017. p. 2585-2586.

[C6] Antonino Rullo, Daniele Midi, Edoardo Serra, Elisa Bertino. Strategic Security Resource Allocation for Internet of Things. IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, Japan, 2016.

[C7] Andrea Pugliese, Antonino Rullo, Antonio Piccolo. The AC-Index Fast Online Detection of Correlated Alerts. Security and Trust Management (STM), 11th Intrernational Workshop, Vienna, Austria - September 21-22, 2015, Volume 9331 of the series Lecture Notes in Computer Science, pp 107-122, Springer International Publishing.

[C8] Antonella Guzzo, Andrea Pugliese, Antonino Rullo, Domenico Saccà. Intrusion Detection with Hypergraph-Based Attack Models. Lecture Notes in Arti_cial Intelligent: Graph Structures for Knowledge Representation and Reasoning, Third International Workshop, GKR 2013, Beijing, China, August 3, 2013. Revised Selected Papers, Springer International Publishing.

[C9] Antonella Guzzo, Andrea Pugliese, Antonino Rullo, Domenico Saccà. Hypergraph-Based Attack Models for Network Intrusion Detection. Italian Symposium on Advanced Database Systems. SEBD. 2014. p. 61-68.

[C10] Tim Furche, Giovanni Grasso, Antonino Rullo, Christian Schallhart, Andrew Sellers. Think Before You Act! Minimizing Action Execution in Wrappers. Very Large Data Search (VLDS), Very Large Data Bases (VLDB), Istanbul, Turkey, 2012.

[C11] Antonino Rullo, Elisa Bertino. PAST: Protocol-Adaptable Security Tool for Heterogeneous IoT Ecosystems. Accettato per la pubblicazione in IEEE Conference on Dependable and Secure Computing 2018.

8.3 Capitoli di libri

[B1] Rullo A., Serra E., Bertino E., Lobo J. (2019) Optimal Placement of Security Resources for the Internet of Things. In: Cicirelli F., Guerrieri A., Mastroianni C., Spezzano G., Vinci A. (eds) The Internet of Things for Smart Urban Ecosystems. Internet of Things (Technology, Communications and Computing). Springer, Cham

8.4 Articoli sottomessi per la pubblicazione

[J5] Antonino Rullo, Domenico Saccà, Edoardo Serra. Extending Inverse Frequent Itemsets Mining to Generate Realistic Datasets: Complexity, Accuracy and Emerging Applications. Submitted for the publication in Data Mining and Knowledge Discovery, Springer.

[B2] Rullo A., Serra E., Lobo J. (2019) Redundancy as a Measure of Fault Tolerance for the Internet of Things. Submitted for the publication in Springer Series LNCS State-of-the-Art Survey.

[C12] Antonella Guzzo, Mikel Joaristiy, Antonino Rullo and Edoardo Serra. A Multi-modal Approach for Detecting Novelty in the Process Behaviour. Submitted for the publication in 1st International Conference on Process Mining, June 24-26, 2019, Aachen, Germany.

Ai sensi della Legge 675/96 \Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", autorizzo al trattamento dei dati personali contenuti nel presente curriculum nel pieno rispetto di tale legge e limitatamente ai _ni connessi alla gestione del curriculum medesimo.

Data 19/02/2019 Luogo Rende