

CURRICULUM DELL'ATTIVITÀ SCIENTIFICA,
DIDATTICA E PROFESSIONALE

DICHIARAZIONE SOSTITUTIVA DELL'ATTO DI
NOTORIETÀ

(art. 46 e 47 del DPR 445/2000)

Il sottoscritto Gabriele Costa nato a La Spezia (SP) l'8 novembre 1981, residente a Genova (GE) in via Giovanni Santolini n. 12, codice fiscale CSTGRL81S08E463J, consapevole della responsabilità penale prevista, dall'art. 76 del D.P.R. 445/2000, per le ipotesi di falsità in atti e dichiarazioni mendaci ivi indicate

DICHIARA

che quanto riportato nel seguito del presente documento corrisponde al vero.

Informazioni Personali

Nome: Gabriele Costa

Residenza: via Giovanni Santolini 12, 16132, Genova

Data di nascita: 08 novembre 1981

Mail: gabriele.costa@unige.it

Mobile: +39 347 7368440

• • •

Istruzione e Formazione

Dottorato di ricerca in informatica conseguito il 22 novembre 2011 presso l'Università di Pisa con tesi dal titolo "On the Security of Software Systems and Services" (supervisor Pierpaolo Degano e Fabio Martinelli).

Laurea specialistica in informatica (23/S LM18 SSD INF/01), conseguita il 13 ottobre 2006 presso l'Università di Pisa con tesi dal titolo "Inferenza dei Tipi e degli Effetti in un Linguaggio Orientato alla Sicurezza" (supervisor Pierpaolo Degano e Massimo Bartoletti). Votazione finale 110/110.

• • •

Partecipazione a scuole estive

FOSAD '08 (8th International School on Foundations of Security Analysis and Design), 25-30 agosto 2008, Bertinoro (FC).

GLOBAN '08 (Global Computing Approach to Analysis of Systems), 22-26 settembre 2008, Varsavia, Polonia.

FOSAD '09 (9th International School on Foundations of Security Analysis and Design), 30 agosto - 4 settembre 2009, Bertinoro (FC).

NIS '09 (2nd ENISA-FORTH Summer School on Network & Information Security), 14-18 settembre 2009, Creta, Grecia.

FOSAD '10 (10th International School on Foundations of Security Analysis and Design), 6-11 settembre 2010, Bertinoro (FC).



Attività presso Università e Centri di Ricerca

- 01/09/2014 – oggi
 - Posizione: Ricercatore universitario a tempo determinato
 - Ente: Università degli Studi di Genova
 - Struttura: Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS)
- 02/01/2014 – 31/08/2014
 - Posizione: Assegnista di ricerca
 - Ente: Università degli Studi di Genova
 - Struttura: Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS)
- 02/01/2013 – 01/01/2014
 - Posizione: Assegnista di ricerca
 - Ente: Università degli Studi di Genova
 - Struttura: Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS)
- 02/01/2012 – 01/01/2013
 - Posizione: Assegnista di ricerca
 - Ente: Università degli Studi di Genova
 - Struttura: Dipartimento di Informatica, Sistemistica e Telematica (DIST)
- 16/01/2011 – 01/01/2012
 - Posizione: Assegnista di ricerca
 - Ente: Consiglio Nazionale delle Ricerche

- Struttura: Istituto di Informatica e Telematica (IIT)
- 16/01/2010 – 15/01/2011
 - Posizione: Assegnista di ricerca
 - Ente: Consiglio Nazionale delle Ricerche
 - Struttura: Istituto di Informatica e Telematica (IIT)
- 16/01/2009 – 15/01/2010
 - Posizione: Assegnista di ricerca
 - Ente: Consiglio Nazionale delle Ricerche
 - Struttura: Istituto di Informatica e Telematica (IIT)
- 16/01/2008 – 15/01/2009
 - Posizione: Assegnista di ricerca
 - Ente: Consiglio Nazionale delle Ricerche
 - Struttura: Istituto di Informatica e Telematica (IIT)



Attività di ricerca

Le principali aree tematiche e di interesse includono (ma non sono limitate a) le seguenti categorie.

Language-based security. La maggior parte dei linguaggi di programmazione più comunemente utilizzati nelle comunità di sviluppo e industriali non forniscono operazioni primitive adeguate per la definizione e verifica di proprietà di sicurezza. Questa mancanza non permette di implementare le specifiche di sicurezza, che tipicamente vengono definite in fase di progettazione, insieme al sistema stesso. In questo modo, le proprietà di sicurezza devono essere verificate in un secondo momento e a partire da un sistema già implementato che, se scoperto difettoso, richiederebbe una seconda implementazione. Le tecniche formali possono mitigare queste limitazioni includendo specifici operatori nei linguaggi di programmazione. In fase di sviluppo, sia i requisiti funzionali che le specifiche di sicurezza vengono implementati e verificati per ottenere componenti software che rispettano i requisiti iniziali.

History-based security. L'applicazione di tecniche di analisi formale richiede che i sistemi reali e il loro comportamento vengano opportunamente modellati. Infatti, il processo di astrazione permette sia di ignorare gli aspetti non rilevanti di un sistema, rendendo così i dati trattabili senza perdere informazione, che di utilizzare metodi matematici e rigorosi. Negli ultimi anni è diventato sempre più comune l'approccio basato sulla rappresentazione dei comportamenti rilevanti di un sistema in termini delle sue tracce di esecuzione. Brevemente, una traccia di esecuzione è una sequenza di operazioni attuate da un sistema. Usando appropriate tecniche di modellazione e specifiche di requisiti di sicurezza è possibile rappresentare un sistema tramite le tracce che esso esegue e verificare se, eventualmente, alcune non soddisfano i requisiti prefissati.

Sicurezza del codice mobile. L'uso dei dispositivi mobili, in costante aumento, ha favorito lo sviluppo delle applicazioni mobili. Queste applicazioni viaggiano nella rete, sotto forma di pacchetti di istruzioni, e vengono infine installate ed eseguite sui dispositivi destinatari. Chiaramente, codice mobile parzialmente compromesso può impattare con effetti nefasti sulla sicurezza dei dispositivi. Una tecnica in crescente diffusione consiste nell'associare alle applicazioni mobili un contratto che ne descriva accuratamente le caratteristiche di interesse, soprattutto in termini di sicurezza. Tecniche di analisi formale possono quindi essere applicate a tali contratti per verificarne la correttezza (rispetto al reale comportamento del codice) e la validità (rispetto ai vincoli imposti dal destinatario del codice).

Orchestrazione di servizi. I servizi web sono in continua espansione e, in molti contesti, stanno modificando il modo di progettare (Service Oriented Computing – SOC) e strutturare (Service Oriented Architecture – SOA) le applicazioni. I servizi interagiscono per mezzo di specifiche invocazioni nel rispetto di interfacce simili a contratti. Arricchendo tali contratti con definizioni formali dei comportamenti dei servizi in termini di gestione delle risorse sensibili (per esempio dati e beni virtuali) è possibile verificarne la composizione in fase di progettazione. Questo tipo di analisi previene composizioni e interazioni che potrebbero potenzialmente violare le specifiche di sicurezza dei singoli servizi.

Tecniche di monitoring. In molti casi la garanzia di specifiche proprietà di sicurezza non può prescindere da un controllo dinamico del comportamento del sistema in considerazione. Il monitoring di proprietà di sicurezza comporta costi aggiuntivi in termini di performance e utilizzo delle risorse computazionali. L'uso di strumenti di analisi statica può prevenire controlli non necessari con conseguenti benefici. Inoltre, approcci di tipo probabilistico possono ridurre i campionamenti necessari per controllare che il sistema non incorra in violazioni. È interessante notare che, fissata una soglia di rischio/costo arbitraria, è possibile regolare algebricamente i controlli dinamici affinché le violazioni rispettino la soglia data.



Publicazioni su riviste internazionali

- [J1] Alessandro Armando, Gabriele Costa, Alessio Merlo, Luca Verderame: *Formal modeling and automatic enforcement of Bring Your Own Device policies*. International Journal of Information Security 14(2): 123-140 (2015).
<http://dx.doi.org/10.1007/s10207-014-0252-y>
- [J2] Alessandro Armando, Gabriele Costa, Luca Verderame, Alessio Merlo: *Securing the "Bring Your Own Device" Paradigm*. IEEE Computer 47(6): 48-56 (2014).
<http://dx.doi.org/10.1109/MC.2014.164>
- [J3] Gabriele Costa, Iliaria Matteucci: *Gate automata-driven run-time enforcement*. Computers & Mathematics with Applications 63(2): 518-524 (2012).
<http://dx.doi.org/10.1016/j.camwa.2011.08.046>

- [J4] Gabriele Costa, Pierpaolo Degano, Fabio Martinelli: *Modular plans for secure service composition*. Journal of Computer Security 20(1): 81-117 (2012).
<http://dx.doi.org/10.3233/JCS-2011-0430>
- [J5] Gabriele Costa, Pierpaolo Degano, Fabio Martinelli: *Secure service orchestration in open networks*. Journal of Systems Architecture - Embedded Systems Design 57(3): 231-239 (2011).
<http://dx.doi.org/10.1016/j.sysarc.2010.09.001>
- [J6] Gabriele Costa, Fabio Martinelli, Paolo Mori, Christian Schaefer, Thomas Walter: *Runtime monitoring for next generation Java ME platform*. Computers & Security 29(1): 74-87 (2010).
<http://dx.doi.org/10.1016/j.cose.2009.07.005>
- [J7] Massimo Bartoletti, Gabriele Costa, Roberto Zunino: *Jalapa: Securing Java with Local Policies: Tool Demonstration*. Electr. Notes Theor. Comput. Sci. 253(5): 145-151 (2009).
<http://dx.doi.org/10.1016/j.entcs.2009.11.020>
- [J8] Massimo Bartoletti, Gabriele Costa, Pierpaolo Degano, Fabio Martinelli, Roberto Zunino: *Securing Java with Local Policies*. Journal of Object Technology 8(4): 5-32 (2009).
<http://dx.doi.org/10.5381/jot.2009.8.4.a1>



Publicazioni in atti di convegni

- [C1] Alessandro Armando, Gianluca Bocci, Gabriele Costa, Rocco Mammoliti, Alessio Merlo, Silvio Ranise, Riccardo Traverso, Andrea Valenza: *Mobile App Security Assessment with the MAVeriC Dynamic Analysis Module*. 7th ACM CCS International Workshop on Managing Insider Security Threats (MIST'15), Denver (CO), USA, October 12-16: 41-49
<http://doi.acm.org/10.1145/2808783.2808786>
- [C2] Gabriele Costa: *Securing Android with Local Policies*. Programming Languages with Applications to Biology and Security – Essays Dedicated to Pierpaolo Degano on the Occasion of His 65th Birthday, 2015: 202-218
http://dx.doi.org/10.1007/978-3-319-25527-9_14
- [C3] Alessandro Armando, Roberto Carbone, Gabriele Costa, Alessio Merlo: *Android Permissions Unleashed*. 28th IEEE Computer Security Foundations Symposium (CSF'15), Verona, Italy, July 13-17, 2015: 320-333
<http://dx.doi.org/10.1109/CSF.2015.29>
- [C4] Alessandro Armando, Gianluca Bocci, Gianantonio Chiarelli, Gabriele Costa, Gabriele De Maglie, Rocco Mammoliti, Alessio Merlo: *SAM: The Static Analysis Module of the MAVERIC Mobile App Security Verification Platform*. 21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'15), Held as Part of the European Joint Conferences on

Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015: 225-230.

http://dx.doi.org/10.1007/978-3-662-46681-0_19

- [C5] Alessandro Armando, Gabriele Costa, Alessio Merlo, Luca Verderame: *Enabling BYOD through secure meta-market*. 7th ACM Conference on Security & Privacy in Wireless and Mobile Networks, WiSec'14, Oxford, United Kingdom, July 23-25, 2014: 219-230.

<http://doi.acm.org/10.1145/2627393.2627410>

- [C6] Gabriele Costa, Fabio Martinelli, Artsiom Yautsiukhin: *Multi-dimensional Secure Service Orchestration*. Business Process Management Workshops - BPM 2013 International Workshops, Beijing, China, August 26, 2013: 473-485.

http://dx.doi.org/10.1007/978-3-319-06257-0_37

- [C7] Alessandro Armando, Aniello Castiglione, Gabriele Costa, Ugo Fiore, Alessio Merlo, Luca Verderame, Ilsun You: *Trustworthy Opportunistic Access to the Internet of Services*. Information and Communication Technology - International Conference, ICT-EurAsia 2013, Yogyakarta, Indonesia, March 25-29, 2013: 469-478.

http://dx.doi.org/10.1007/978-3-642-36818-9_52

- [C8] Alessandro Armando, Gabriele Costa, Alessio Merlo: *Bring your own device, securely*. 28th Annual ACM Symposium on Applied Computing, SAC'13, Coimbra, Portugal, March 18-22, 2013: 1852-1858.

<http://doi.acm.org/10.1145/2480362.2480707>

- [C9] Giulio Caravagna, Gabriele Costa, Luca Wiegand, Giovanni Pardini: *Lazy Monitoring for Distributed Computing Environments*. 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012, Palermo, Italy, July 4-6, 2012: 259-265.

<http://doi.ieeecomputersociety.org/10.1109/IMIS.2012.186>

- [C10] Giulio Caravagna, Gabriele Costa, Giovanni Pardini: *Lazy Security Controllers*. Security and Trust Management - 8th International Workshop, STM 2012, Pisa, Italy, September 13-14, 2012: 33-48.

http://dx.doi.org/10.1007/978-3-642-38004-4_3

- [C11] Alessandro Armando, Gabriele Costa, Alessio Merlo: *Formal Modeling and Reasoning about the Android Security Framework*. Trustworthy Global Computing - 7th International Symposium, TGC 2012, Newcastle upon Tyne, UK, September 7-8, 2012: 64-81.

http://dx.doi.org/10.1007/978-3-642-41157-1_5

- [C12] Gabriele Costa, Fabio Martinelli, Artsiom Yautsiukhin: *Metric-Aware Secure Service Orchestration*. Fifth Interaction and Concurrency Experience, ICE 2012, Stockholm, Sweden, 16th June 2012: 32-46.

<http://dx.doi.org/10.4204/EPTCS.104.4>

- [C13] Gabriele Costa, Iliaria Matteucci: *Trust-Driven Policy Enforcement through Gate Automata*. Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2011, Seoul, Korea, June 30-July 02, 2011: 208-215.
<http://dx.doi.org/10.1109/IMIS.2011.88>
- [C14] Gabriele Costa, Iliaria Matteucci: *Elective temporal logic*. 7th International Conference on the Quality of Software Architectures, QoSA 2011 and 2nd International Symposium on Architecting Critical Systems, ISARCS 2011. Boulder, CO, USA, June 20-24, 2011: 143-152.
<http://doi.acm.org/10.1145/2000259.2000283>
- [C15] Gabriele Costa, Valérie Issarny, Fabio Martinelli, Iliaria Matteucci, Rachid Saa-di: *Security and Trust*. Formal Methods for Eternal Networked Software Systems - 11th International School on Formal Methods for the Design of Computer, Communication and Software Systems (Advanced Lectures), SFM 2011, Bertinoro, Italy, June 13-18, 2011: 393-416.
http://dx.doi.org/10.1007/978-3-642-21455-4_12
- [C16] Gabriele Costa, Nicola Dragoni, Aliaksandr Lazouski, Fabio Martinelli, Fabio Massacci, Iliaria Matteucci: *Extending Security-by-Contract with Quantitative Trust on Mobile Devices*. Fourth International Conference on Complex, Intelligent and Software Intensive Systems, Krakow, Poland, 15-18 February, 2010: 872-877.
<http://doi.ieeecomputersociety.org/10.1109/CISIS.2010.33>
- [C17] Gabriele Costa, Pierpaolo Degano, Fabio Martinelli: *Modular Plans for Secure Service Composition*. Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security - Joint Workshop (Revised Selected Papers), ARSPA-WITS 2010, Paphos, Cyprus, March 27-28, 2010: 41-58.
http://dx.doi.org/10.1007/978-3-642-16074-5_4
- [C18] Giuseppe Amato, Paolo Bolettieri, Gabriele Costa, Francesco la Torre, Fabio Martinelli: *Detection of images with adult content for parental control on mobile devices*. 6th International Conference on Mobile Technology, Applications, and Systems, Mobility Conference 2009, Nice, France, September 2-4, 2009.
<http://doi.acm.org/10.1145/1710035.1710070>



Capitoli di libro

- [B1] Gabriele Costa, Roberto Mandati, Fabio Martinelli, Iliaria Matteucci, Artsiom Yautsiukhin: *Mitigating Security Risks in Web Service Invocations: Contract-Based Approaches*. Handbook of Research on Architectural Trends in Service-Driven Computing (2013).
<http://dx.doi.org/10.4018/978-1-4666-6178-3.ch021>



Altre pubblicazioni

- [I1] Gabriele Costa, Alessio Merlo, Luca Verderame: *Market-Based Security for Mobile Devices*. ERCIM News 2013(93) (2013).
<http://ercim-news.ercim.eu/en93/special/market-based-security-for-mobile-devices>
- [I2] Gabriele Costa, Francesco la Torre, Fabio Martinelli, Paolo Mori: *Parental Control for Mobile Devices*. ERCIM News 2010(82): 61-62 (2010).
<http://ercim-news.ercim.eu/en82/rd/parental-control-for-mobile-devices>



Partecipazione a conferenze e attività di revisore

- Session chair**
- 4th International Workshop on Managing Insider Security Threats (MIST), Fukuoka, Japan, 2012.
 - 4th International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing (IMIS), Krakow, Poland, 2010.
- Program committee**
- 11th International Workshop on Security and High Performance Computing Systems (SHPCS), 2016.
 - 6th International Workshop on Security, Privacy and Performance in Cloud Computing (SPCLOUD), 2016.
 - 5th International Workshop on Security, Privacy and Performance in Cloud Computing (SPCLOUD), 2015.



Attività didattica

Corsi universitari

- SpA** Sistemi per l'Automazione, AA 15/16, CFU 11, Corso di Laurea in Ingegneria Meccanica, Università di Genova. Ruolo: Docente.
- LFdI** Laboratorio di Fondamenti di Informatica, AA 14/15, CFU 3, Corso di Laurea in Ingegneria Nautica, Università di Genova. Ruolo: Docente.
- FdIA** Fondamenti di Informatica A, AA 13/14, CFU 6, Corso di Laurea in Ingegneria Nautica, Università di Genova. Ruolo: Docente.
- CS** Computer Security, AA 13/14, CFU 6, Corso di Laurea in Ingegneria Informatica, Università di Genova. Ruolo: Assistente.
- SOSI** Sistemi Operativi e Sicurezza Informatica, AA 12/13, CFU 9, Corso di Laurea in Ingegneria Informatica, Università di Genova. Ruolo: Assistente.
- SOSI** Sistemi Operativi e Sicurezza Informatica, AA 11/12, CFU 9, Corso di Laurea in Ingegneria Informatica, Università di Genova. Ruolo: Assistente.
- EdCC** Elementi di Calcolabilità e Complessità, AA 10/11, CFU 6, Corso di Laurea in Informatica, Università di Pisa. Ruolo: Assistente.

EdCC Elementi di Calcolabilità e Complessità, AA 09/10, CFU 6, Corso di Laurea in Informatica, Università di Pisa. Ruolo: Assistente.

Fdi Fondamenti di Informatica, AA 08/09, CFU 6, Corso di Laurea in Lettere, Università di Pisa. Ruolo: Assistente.



Corsi post lauream

MCS Sicurezza del codice mobile, Dottorato in Informatica e Ingegneria dei Sistemi, Università di Genova, 2015.

MCS Sicurezza del codice mobile, Master di secondo livello in Cyber Security, Università di Genova, 2015.

MCS Sicurezza del codice mobile, Master di primo livello in Cyber Security (moduli AF1, AF2, AF3), Distretto Tecnologico di Cyber Security, Cosenza, 2015.



Attività di Supervisione

Studenti di dottorato

- Federico Sinigaglia, Dottorato in informatica e ingegneria dei sistemi, XXXI ciclo di dottorato, Università degli Studi di Genova (in corso). Ruolo: co-advisor.

Correlatore di tesi magistrali

- Marco Malvasio, Ingegneria Informatica, Università degli Studi di Genova, 2015
- Giulio Puri, Ingegneria Informatica, Università degli Studi di Genova, 2015
- Gabriele De Maglie, Ingegneria Informatica, Università degli Studi di Genova, 2014
- Fabrizio Brizzolara, Ingegneria Informatica, Università degli Studi di Genova, 2014



Partecipazione in progetti di ricerca

Progetti di ricerca europei

SPACIOS Secure Provisioning and Consumption in the Internet of Services (Project no. 257876, FP7-ICT-2009.1.4: Trustworthy ICT). Inizio: 1 ottobre 2010. Fine: 1 gennaio 2014 (concluso).

NESSOS Network of Excellence on Engineering Secure Future Internet Software Services and Systems (Project no. 256980, FP7-ICT-2009.1.4: Trustworthy ICT). Inizio: 1 ottobre 2010. Fine: 31 marzo 2014 (concluso).

ANIKETOS Secure and Trustworthy Composite Services (Project no. 257930, FP7-ICT-2009.1.4: Trustworthy ICT). Inizio: 1 agosto 2010. Fine: 31 gennaio 2014 (concluso).

CONNECT Emergent connectors for eternal software intensive networked systems (Project no. 231167, FP7-ICT-2007.8.6: ICT forever yours). Inizio: 1 febbraio 2009. Fine: 31 luglio 2012 (concluso).



Progetti di ricerca nazionali

SECURITY HORIZONS Progetto di Ricerca di Interesse Nazionale (PRIN 2010-2011). Durata 36 mesi (concluso).



Altri progetti

MAVERIC DYNAMIC ANALYSIS Progetto di collaborazione con Poste Italiane (2015). Prosecuzione del precedente progetto “Maveric Static Analysis”. Durata 9 mesi (in corso).

BYODROID DEMONSTRATOR Progetto selezionato per un finanziamento da parte della NATO Communications and Information Agency (NCIA) nell’ambito programma Cyber Security Incubator 2015. **Il progetto è stato invitato e presentato alla principale Cyber Conference della NATO, NIAS 2015.** Durata 3 mesi (concluso).

MAVERIC STATIC ANALYSIS Progetto di collaborazione con Poste Italiane (2014) selezionato per l’integrazione tecnologica dell’infrastruttura in dotazione al CERT di Poste Italiane. **Maveric è stato presentato durante l’Industry Keynote Speech di ESSOS 2015.** Durata 9 mesi (concluso).



Indicatori di Qualità della Ricerca

Indicatori ANVUR

- Indicatori normalizzati (secondo parametri ASN 2015)
 - # Articoli su rivista normalizzato: 14.29
 - # Citazioni normalizzato: 13.29
 - H-index contemporaneo: 6
- Scostamento percentuale dalle mediane nazionali per professori associati – settore concorsuale 01/B1
 - # Articoli su rivista normalizzato: +42.9%
 - # Citazioni normalizzato: +45,25%
 - H-index contemporaneo: +20%

- Scostamento percentuale dalle mediane nazionali per professori associati – settore concorsuale 09/H1
 - # Articoli su rivista normalizzato: +42.9%
 - # Citazioni normalizzato: +24,55%
 - H-index contemporaneo: ±0%



Altre Attività e Riconoscimenti

SC Primo posto nella selezione Start Cup 2013 dell'Università degli Studi di Genova con il progetto BYODroid.

IC Finalista Idea Challenge 2014 promossa dagli EIC ICT Labs dello European Institute of Innovation and Technology con il progetto BYODroid.

SC Finalista Start Cup 2010 con il progetto ICareMobile, selezionato al terzo posto (**più di 33400 voti degli utenti de Il Sole 24 Ore**).



Altre esperienze lavorative

Capgemini. Periodo: Gennaio-Ottobre 2007. Ruolo: Junior Consultant. Principali mansioni: Sviluppo di software e firmware per sistemi embedded, armamenti terrestri e navali. Implementazione di protocolli per l'interfaccia uomo-macchina.



Partecipazione in progetti di sviluppo

A conseguenza dell'attività di ricerca svolta e descritta precedentemente sono stati sviluppati e rilasciati diversi strumenti software e applicativi.

Jalapa. Jalapa è una estensione del modello di sicurezza di Java che permette di specificare, verificare e garantire politiche di sicurezza sull'uso delle risorse di un programma. Gli sviluppatori possono usare il tool per applicare operatori di sandbox su parti di codice sospette o comunque non verificate. Tali operatori garantiscono che la politica associata sia soddisfatta tramite verifica e, in caso negativo, tramite controllo a runtime.

☞ <http://jalapa.sourceforge.net/>

iCareMobile. iCareMobile è un software per il monitoring di dispositivi mobili. L'applicazione controlla il rispetto di politiche di sicurezza arbitrarie definite sia sul comportamento dei programmi che sull'uso del dispositivo da parte dell'utente. Per esempio, se l'utente è un minore, iCareMobile permette di specificare politiche di parental control.

☞ <http://icaremobile.iit.cnr.it/>

SPaCioS Tool. Lo scopo principale dello SPaCioS Tool consiste nel fornire agli analisti un supporto automatico per la verifica di proprietà di sicurezza. Tale scopo è ottenuto tramite la composizione di diverse tecniche formali che vanno dalla modellazione, alla verifica e al security testing. Dato che la maggior parte di queste tecniche è coinvolta nel processo di design e sviluppo delle applicazioni web, lo SPaCioS Tool è stato realizzato come un'estensione di una delle più diffuse piattaforme di sviluppo, cioè Eclipse.

📄 <http://www.spacios.eu/>

SATMC@NESSoS. Il NESSoS Service Development Environment (SDE) è una piattaforma per la progettazione e implementazione di orchestrazioni di servizi web. Il model checker SATMC (<http://www.ai-lab.it/satmc/>) è stato incorporato nel NESSoS SDE per integrarne le funzionalità. L'estensione permette di includere SATMC in un'orchestrazione passando gli input appropriati e ottenendo in risultato di una verifica formale.

📄 <http://svn.pst.ifi.lmu.de/update/NESSoSools/SATMC/>

BYODroid. BYODroid è l'implementazione di un'estensione del tradizionale sistema di distribuzione delle applicazioni mobili. In particolare, BYODroid consiste di un meta-market che, frapponendosi tra gli utenti registrati a un dominio di sicurezza e i market di applicazioni standard, verifica che il codice richiesto per l'installazione sia sempre compatibile con i requisiti di sicurezza. La verifica viene effettuata tramite model checking di modelli estratti direttamente dal codice mobile. Se la verifica non termina con successo, cioè il codice include comportamenti potenzialmente dannosi, BYODroid instrumeta automaticamente dei controlli di sicurezza per prevenire violazioni a runtime.

📄 <http://www.ai-lab.it/byodroid/index.html>

SCP. Secure Component Provider (SCP) ridefinisce il sistema dei permessi dei dispositivi Android e permette agli sviluppatori di applicare politiche di sicurezza alle proprie app. Le politiche definite in questo modo estendono i controlli nativi di Android e permettono una verifica automatica (effettuata tramite un SAT-solver). Le politiche verificate non possono essere violate e gli utenti non possono mai causare esecuzioni illegali (ne volontariamente ne involontariamente) pur non dovendo mai prendere decisioni sulla sicurezza.

📄 <https://github.com/SCPTeam/Safe-Component-Provider>

Maveric. Maveric è una piattaforma web per la verifica automatica delle applicazioni Android commissionata da Poste Italiane. Gli analisti sottomettono le app da analizzare e ottengono un security profile che ne identifica le caratteristiche verificando automaticamente la presenza di malware ed altre proprietà di sicurezza. Maveric è in fase di interazione con il Mobile Application Security Monitoring (MASM) di Poste Italiane e non è attualmente accessibile al pubblico.

📄 http://www.posteitaliane.it/it/innovazione/campus_tecnologico/certcyb.shtml



Organizzazione e partecipazione a eventi

Eventi e meeting relativi all'attività di ricerca

ESSOS'10 International Symposium on Engineering Secure Software and Systems, 03-04 febbraio, 2010 Pisa. Membro del comitato locale organizzativo.

NESSoS Kick Off First project meeting, settembre 2010, Pisa. Organizzatore.

SPaCioS Meeting Project meeting, 10-11 luglio 2012, Genova. Organizzatore.



Eventi di divulgazione scientifica

CLUSIT Workshop 2015 <http://www.csec.it/pages/events/CLUSIT-2015-WS.html>

CLUSIT Workshop 2014 <http://www.csec.it/pages/events/CLUSIT-2014-WS.html>

Family Festival 2011 <http://fiuggifamilyfestival.org/>

Festival della scienza 2010 <http://festival2010.festivalscienza.it>

Festival della scienza 2009 <http://festival2009.festivalscienza.it>

