Curriculum Vitae

Roberto Carbone

January, 2021

Personal Information

Name: Roberto Carbone
Date of Birth:

Birthplace:

Citizenship:

Languages: Italian, English

Address

Office:
Security and Trust Research Unit, Fondazione Bruno Kessler - Irst
Via Sommarive 18, Povo, 38123 – Trento, Italy
Phone: +39 0461.314.185
Mobile: +39 3666381005
Email: carbone@fbk.eu
WWW: http://st.fbk.eu/RobertoCarbone

Current Position

- Head of the *Security and Trust Research Unit* at the Cybersecurity Research Center of Bruno Kessler Foundation in Trento, since January, 2021.

Academic and Research Appointments

Since November, 2010: Researcher of the *Security and Trust Research Unit* at Bruno Kessler Foundation.

2017: Visiting Scholar in the Department of Computer Science at the University of Pittsburgh (Pennsylvania, US). My proposal for a period of research in a partner institution has been selected in the context of the FBK mobility program 2017: from September 2017, I spent three months as a Visiting Scholar in the Department of Computer Science at the University of Pittsburgh (Pennsylvania, US), where a collaborated with Professor Adam J. Lee. The main research topic concerned the domain of cryptographically enforcing dynamic access control policies in the Cloud.

2009 - 2010: Research Associate at "Dipartimento di Informatica, Sistemistica e Telematica" (DIST) at the Faculty of Engineering of the University of Genova.

Degrees

- Ph.D. in Electronic and Computer Engineering and Telecommunications (Dottore di Ricerca in "Ingegneria Elettronica, Informatica e delle Telecomunicazioni"), University of Genova, April, 2009.
- Professional qualification in Engineering (2006). (Esame di stato per l'abilitazione alla professione di Ingegnere.)
- MSc in Computer Engineering, University of Genova, Faculty of Engineering (2005). Score: 110/110 with honour (Lode).

Research Projects

I am currently involved in the following research projects, funded by the European Commission under the H2020 project:

- *SPARTA:* Strategic programs for advanced research and technology in Europe.
- *5G CARMEN:* 5G for Connected and Automated Road Mobility in the European UnioN.
- *FINSEC:* Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures.

I have been involved in the following research projects:

- *Teichos:* Technical Environment for Intelligent Cyber Operational Security (in the context of the EIT Digital activities 2019). I contributed by developing security analyses tools for the pentesting of web applications.
- *API Assistant 2:* (in the context of the EIT Digital activities 2019). This is a follow-up of API Assistant, and I contributed with Amir Sharif by extending the Android Studio plugin for SSO solutions, and providing a tool to detect logical vulnerabilities in OAuth/OpenID Connect-based mobile native applications.
- *API Assistant:* Automated Security Assessment of 3rd party apps for the API economy (in the context of the EIT Digital activities 2018). This activity created an assistant for mobile app developers capable of rising Cyber Security awareness and mitigating threats in API-based mobile apps by offering a toolkit for code hardening against known security problems and a managed security service for testing, analysis, and compliance.
  Role: leader of the "Digital health Business case" task.
- *SECENTIS:* a European Industrial Doctorate on Security and Trust of Next Generation Enterprise Information Systems. `http://www.secentis.eu/`
  Role: Academic supervisor of Avinash Sudhodanan.
- The activity *Federated Identity Management System (FIDES 2016)* in the context of the EIT Digital activities 2016 (Innovation Area: Privacy, Security & Trust in Information Society).
  Role: responsible for FBK.
  Duration: 1 year from January 1, 2016.

  Building on results achieved in its first year, in 2016 FIDES has been extended to become a EU-wide platform for federated identity management, by providing concrete business cases demonstrated in partnering countries (IT, NL and ES).
- The activity *Federated Identity Management System (FIDES 2015)* in the context of the EIT Digital activities 2015 (Innovation Area: Privacy, Security & Trust in Information Society). The outcome was a technical blueprint for a federated and interoperable identity management platform, compliant with the current regulations, such as eIDAS, Data Protection and the most relevant national legislations, such as SPID in Italy.
  Duration: 1 year from January 1, 2015.

- The activity *Security Threat Identification and Testing (STIATE)* was in the context of the EIT ICT Labs activities 2014 (Innovation Area: Privacy, Security & Trust in Information Society). The outcome was a technology supporting threat analysis and security testing of collaborative business applications. I was the leader of the task about the "Threat Modeling and Automated Testcase Generation and Execution".

- The activity *SecSES - Secure Energy Systems* in the context of the EIT ICT Labs activities 2013 (Innovation Area: Smart Energy Systems). Our contribution was the formal modeling and the mechanical analysis of security protocols and policies used in the complex scenario of the Secure Smart Home Energy Gateway for Smart Buildings.

- *SmartCampus*. Our contribution was the analysis of the security aspects of the SmartCampus platform. `http://www.smartcampuslab.it/`

- *Automated Security Analysis of Identity and Access Management Systems (SIAM)*, funded by Provincia Autonoma di Trento in the context of the "team 2009 - Incoming COFUND action" of the European Commission (FP7).

- The activity *SESSec-EU - Networked Smart Energy Systems Security in Europe* in the context of the EIT ICT Labs activities 2012. Our contribution was to apply our techniques for formal modeling and mechanical analysis of security protocols and policies used in Smart Energy Systems.

- I collaborated to the *Secure Provision and Consumption in the Internet of Services (SPaCIoS)*, Project no. 257876, FP7-ICT-2009-5, ICT-2009.1.4: Trustworthy ICT 01/10/2010 - 30/09/2013 being the main developer of the tool SATMC used in the project.

- *Cartella Clinica del Cittadino (TreC)*, funded by Provincia Autonoma di Trento: `www.trec.trentinosalute.net`. Our goal was the Design, development, and validation of the authorization policies of the TreC platform handling Personal Health Records.

- *Automated Validation of Trust and Security of Service-oriented Architectures (AVANTSSAR)*, STREP project number 216471, funded by the EU in the context of the 7th Framework Programme, THEME ICT-1-1.4 Secure, dependable and trusted Infrastructures.
  Partner Institutions: U. of Verona (coordinator), U. of Genova, ETHZ, SAP Research, Siemens AG, INRIA-Lorraine, IRIT, OpenTrust, Institute e-Austria Timisoara.
  Duration: 36 months from January 1, 2008.
  The goal of the AVANTSSAR Project was to extend the AVISPA technology so to support the automatic analysis of service-oriented architectures.

- *Verifica automatica dei protocolli di sicurezza* (RBAU01P5SS), funded by the Italian Ministry of Scientific and Technological Research in the context of the FIRB 2001 Programme.
  Partner Institutions: DIST, University di Genova (Prof. A. Armando, coordinator); University of Trento (Prof. F. Massacci); University of Napoli (Prof. M. Benerecetti).
  Duration: 36 months starting from July 1, 2003.

I was involved in activities in the context of the Joint Labs with FBK of:

- Istituto Poligrafico e Zecca dello Stato: I contributed to the design of an authentication solution for mobile applications based on the CIEs. Our solution has been notified to the European Commission, according to the "electronic IDentification Authentication and Signature" (eIDAS) regulation.

- Poste Italiane (2017): I supervised a master student in the topic "Security Test Plan for SAML SSO 2.0 Implementations: The SPID Use Case".

Teaching and Supervision

- Academic Year 2020 - 2021: member of the board of the PhD program on Security, Risk and Vulnerability (Curriculum: Cybersecurity and Reliable Artificial Intelligence), University of Genova.
- Academic Years 2015 - 2020: Lecturer for the "Master Universitario di II livello" in Cyber Security and Data Protection / Critical Infrastructure Protection of the University of Genova `https://mastercybersecurity.it/`.
- In 2017, I have been appointed as member of the Examination Committee for the final examination of the doctoral candidate Mojtaba Eskandari at DEPARTMENT OF INFORMATION ENGINEERING AND COMPUTER SCIENCE, ICT International Doctoral School, University of Trento. Title: "Smartphone Data Transfer Protection According to Jurisdiction Regulations". Supervisors: Bruno Crispo and Anderson Santana De Oliveira.
- In 2017, I was a member of the selection committee of the doctoral course in "COMPUTER SCIENCE AND SYSTEMS ENGINEERING - Curriculum: SECURE AND RELIABLE SYSTEMS (CODICE 6879)" at the University of Genova, for 2 grants funded by the Bruno Kessler Foundation (winner: Amir Sharif).
- I have been appointed by the Steering Committee of the FBK PhD Program as member of the Quality Assessment Committee of several PhD students in FBK.
- In 2020, I was one of the reviewers of the PhD thesis of the doctoral candidate Andrea Valenza, doctoral course in "Computer Science and Systems Engineering", Computer Science Curriculum, at DIBRIS, University of Genova. Title: "<script>alert('Expect the Unexpected')</script> Raising Cybersecurity Awareness by Hook or by Crook". Supervisors: Alessandro Armando and Gabriele Costa.
- In 2019, I was one of the reviewers of the PhD thesis of the doctoral candidate Giuseppina Mùrino, doctoral course in "Ingegneria Matematica e Simulazione" at the University of Genova. Title: "Resilienza di sistemi Cyber-fisici: valutazione sperimentale di misure quantitative nel contesto della sicurezza informatica". Supervisors: Armando Tacchella, Alessandro Armando, and Francesco Vestito.
- Academic Year 2014: Lecturer for the Doctoral Course on Security Threat Identification and Testing, in the context of the Doctoral School in Information and Communication Technology of the University of Trento, organized in collaboration with the Center for Information Technology of the Bruno Kessler Foundation (FBK) and EIT ICT Labs.
- Academic Years 2005/2006, 2006/2007, 2007/2008, and 2008/2009: Teaching Assistant for the Computer Security course taught by Prof. A. Armando at the CS Engineering Faculty of the University of Genova.
- Academic Year 2009/2010: Teaching Assistant for the Operating Systems and Computer Security course taught by Prof. A. Armando at the CS Engineering Faculty of the University of Genova.
- 2008: Teaching Assistant for the module "Sicurezza delle reti" of the Master Universitario Integrato di II livello *Tecnologie Avanzate per Sistemi Intelligenti Integrati*.
- I am currently supervising the following PhD students:
  - Amir Sharif (University of Genova, XXXIII Cycle).
  - Stefano Berlato (University of Genova, together with Silvio Ranise).
  - Andrea Bisegna (University of Genova, together with Silvio Ranise).
- I have co-supervised the following PhD students:

  - Avinash Sudhodanan (University of Trento, together with Luca Compagna, SAP). "Black-Box Security Testing of Browser-Based Security Protocols". PhD Thesis in the International Doctorate School in Information and Communication Technologies, DISI (2017).
  - Giada Sciarretta (University of Trento, together with Alessandro Armando and Silvio Ranise). "A Methodology for the Design and Security Assessment of Mobile Identity Management: Applications to real-world scenarios". PhD Thesis in the International Doctorate School in Information and Communication Technologies, DISI (2018).
  - Federico Sinigaglia (University of Genova, together with Gabriele Costa). "Security Analysis of Multi-Factor Authentication Security Protocols". Ph.D. Thesis in Computer Science and Systems Engineering, Computer Science Curriculum, DIBRIS (2020).

- I was co-supervisor for the master Thesis of:
  - Mercy Viola Akuleut. "Security Test Plan for SAML SSO 2.0 Implementations: The SPID Use Case" (University Supervisor: prof. Fabio Massacci). Laurea Thesis in Computer Science, University of Trento (2017).
  - Marco Pernpruner. "A passwordless out-of-band authentication protocol based on eID cards and push notifications. Design and formal security analysis" (University Supervisor: prof. Massimo Merro, Co-supervisor: Dr. Giada Sciarretta). Laurea Thesis in Computer Science and Engineering, University of Verona (2019).
  - Stefano Berlato. "A Pragmatic Approach to "Handle Honest but Curious" Cloud Service Providers: Cryptographic Enforcement of Dynamic Access Control Policies" (University Supervisor: prof. Silvio Ranise). Laurea Thesis in Computer Science, University of Trento (2019).
  - Giulio Pellizzari. "Micro-Id-Gym: a Tool to Support Sandboxing and Automated Pentesting of Identity Management Protocols" (University Supervisor: prof. Silvio Ranise, Co-supervisor: Andrea Bisegna). Laurea Thesis in Computer Science, University of Trento (2020).
  - $\sim$10 Bachelor Theses (University of Trento).
  - 1 Internship from the University of Verona.

- I have co-supervised (supervisor Alessandro Armando) the following people in their Thesis (University of Genova):
  - Serena Elisa Ponta. "Modeling, Formalisation and Automatic Analysis of Security-sensitive Banking Workflows: the Loan Origination Process as a Case Study". Laurea Thesis in Computer Engineering (2007).
  - Alessandro Cappai. "Progetto e sviluppo di un'architettura orientata ai servizi per uno strumento di analisi automatica di protocolli di sicurezza" (in Italian). Bachelor Thesis in Computer Engineering (2008).
  - Andrea Rosina. "Automatic Analysis of Adminstrative Role-Based Access Control Policies". Laurea Thesis in Computer Engineering (2008).
  - Roberto Basile. "Specifica ed analisi della sicurezza del servizio di Single Sign-On di Google" (in Italian). Laurea Thesis in Computer Engineering (2008).
  - Simone Larosa. "Specifica ed analisi formali di un protocollo di sicurezza per l'autorizzazione di applicazioni web" (in Italian). Laurea Thesis in Computer Engineering (2009).
  - Matteo Grasso. "Scoperta ed analisi di un attacco di Cross-Site Scripting al SAML-based Single Sign-On per le Google Applications" (in Italian). Bachelor Thesis in Computer Engineering (2010).
  - Andrea Piccaluga. "Analisi Comparativa di Strumenti per il Test di Penetrazione delle Applicazioni Web" (in Italian). Bachelor Thesis in Computer Engineering (2010).
  - Fabio Carraro. "Modellazione ed analisi della sicurezza di una soluzione per il Single Sign-on di complessità industriale" (in Italian). Laurea Thesis in Computer Engineering (2011).

- Matteo Grasso. “Design and Development of a Formal Specification Language for Security Protocols”. Laurea Thesis in Computer Engineering (2012).
- Federico Sinigaglia. “Formal Modeling and Security Analysis of Strong Authentication Protocols” (in Italian). Laurea Thesis in Computer Engineering (2015).

Service

Program Committee Member

- Local organization chair of the 30th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2016).
- Co-Chair of the third OAuth Security Workshop 2018.
- Member of the Demos track committee of the Italian Conference on Cybersecurity (ITASEC17, ITASEC18, ITASEC19).
- Member of the Editorial Board in “Frontiers in Computer Science” as a review editor.(2014-2020) and as Associate Editor in Computer and Network Security (2020).
- Member of the Technical Program committees of SECURWARE 2018-2021, SHPCS 2018, SHPCS 2019, SACMAT 2019, SACMAT 2020, SACMAT 2021.

Reviewer

- Several International Journals and Conferences: e.g., JCS, IEEE Access, JISA, IET Information Security, ITASEC, IJAHUC, SECURWARE, SACMAT, SECRYPT.

Invited Talk

Invited talk on “SATMC”, 13th International School on Foundations of Security Analysis and Design (FOSAD’13), September 4, 2013, Bertinoro, Italy.

Research Activity

My research mainly focuses on identity and access management systems. One of the main research interests is on the (formal) analysis of security protocols. Since these protocols are at the core of security-sensitive applications in a variety of domains (e.g., health-care, e-commerce, and e-government), their proper functioning is crucial as a failure may undermine the customer and, more in general, the public trust in these applications.

To provide an excerpt of my activity, I report below some of the results concerning the automatic analysis of security protocols and black-box security testing of browser-based security protocol implementations.

Automatic Analysis of Security Protocols. Even under the assumption of perfect cryptography, the design of security protocols is notoriously error-prone. I have extended a bounded model-checking procedure for the analysis of security protocols based on the reduction to propositional logic so to support the specification of security properties and assumptions on the communication channels in a temporal logic (LTL) [ACC07; ACC09; ACC14]. I have implemented this procedure extending the tool SATMC. By using SATMC I have contributed to the detection of a number of flaws (including unknown ones) in commonly used protocols:

- **Contract Signing Protocols:** we have been able to formalise all the assumptions required by the protocol for optimistic fair exchange proposed by Asokan, Shoup and Waidner, and some of its key security properties. Besides the previously reported attacks on the protocol, I have contributed to the discovery of a new attack on a patched version of the protocol [ACC07; ACC09].

- **Single Sign-On Protocols:** I have contributed to the detection of a serious vulnerability in the SAML Single Sign-On (SSO) Service for Google Apps. We have promptly informed both Google and the Computer Emergency Response Team (CERT) of the problem. Google has initially instructed their customers to implement measures to mitigate potential exploits and has later offered a new version of their SSO service which is free of the problem. (See `http://www.google.com/corporate/security.html`.) The US-CERT has released a vulnerability report on the issue which is available at `http://www.kb.cert.org/vuls/id/612636`. A detailed description of the vulnerability is given in [Arm+08].

  By using the same approach, we have also shown that the main emerging SSO protocols, namely SAML SSO and OpenID, suffer from an authentication flaw that allows a malicious service provider to hijack a client authentication attempt or force the latter to access a resource without its consent or intention [Arm+11]. This may have serious consequences, as evidenced by a Cross-Site Scripting attack that we have identified in the SAML-based SSO for Google Apps and in the SSO available in Novell Access Manager v.3.1. Both vendors have been informed of the vulnerabilities in their products and both have promptly patched their implementations. The findings have also been discussed with members of the OASIS Security Services Technical Committee and a SAML V2.0 Errata has been redacted and approved (`http://www.oasis-open.org/committees/download.php/45096/sstc-saml-approved-errata-2.0-wd55.pdf`).

- **Strong Authentication Protocols:** Strong authentication protocols supplement traditional authentication mechanisms based on user's credentials (namely, username and passwords) with other proofs of identity (e.g., a one-time password generated by a special purpose hardware token). In the past, I have contributed to the detection of serious vulnerabilities in protocols for two-factor and two-channel authentication for web applications. The vulnerabilities allowed an attacker to carry out a security-sensitive operation by using only one of the two authentication factors [ACZ13]. While strong authentication protocols are nowadays widely used, both the regulation regarding data protection and the research work are not keeping the same pace. We performed a latitudinary study on the adoption of multi-factor authentication (MFA) and the design choices made by banks operating in different countries [Sin+20], and we developed a methodology and an automatic tool for the security analysis of strong authentication protocols [Sin+19; Sci+20; Per+20].

Black-Box Security Testing of Browser-Based Security Protocol Implementations. Browser-based security protocols are protocols that run over the HTTP protocol and are executable by web-browsers. They ensure that the right people (or applications) access the right resources, thereby greatly simplifying the design and implementation of complex, online applications. The implementation of browser-based security protocols is usually so complex that severe vulnerabilities are often present even after intensive use of traditional verification techniques (e.g., manual inspection, penetration testing etc.). This is witnessed, for example, by vulnerabilities found in the integration of various Single Sign-On (SSO) and Cashier as-a-Service (CaaS) protocols by service provider web applications. This happens mainly due to the fact that commercial penetration testing tools have limited support for certain types of vulnerabilities (e.g., logical vulnerabilities and Cross-Site Request Forgery-CSRF).

This research has been mainly conducted by the PhD student Avinash Sudhodanan, under my co-supervision activity in the context of the European Industrial Doctorate on Security and Trust of Next Generation Enterprise Information Systems (SECENTIS). In this research, we focused on automatic detection of replay attacks (caused by logical vulnerabilities) and CSRF attacks on browser-based security protocols. The research challenge was to come up with a security testing approach more general than the currently available security testing techniques. The main results were as follows:

- **Multi-Party Web Applications:** We targeted logical vulnerabilities affecting the browser-based security protocols underlying Multi-Party Web Applications (MPWAs). In particular, we proposed an automatic technique based on attack patterns for black-box security testing of MPWAs. In collaboration with SAP, we implemented our ideas on top of OWASP ZAP (a popular, open-source penetration testing tool) and a US patent has been filed. We discovered twenty one previously unknown vulnerabilities in prominent MPWAs (e.g., twitter.com, developer.linkedin.com, pinterest.com) [Sud+16].

- **Auth-CSRF Attacks:** We focused on Auth-CSRF attacks, i.e. CSRF attacks on web sites' authentication and identity management functionalities. We collected several Auth-CSRF attacks reported in literature, analyzed the strategies underlying them and identified some testing strategies that can help a manual tester uncover a large majority of Auth-CSRF attacks. We run a large-scale experimental analysis in Alexa global top web sites and we further generalized our testing strategies, enhanced them with the knowledge we acquired during our experiments and implemented them as an extension (namely CSRF-checker) to OWASP ZAP. Our findings include serious vulnerabilities in prominent web sites such as Microsoft, Google, eBay, etc. [Sud+17].

Awards

My PhD Thesis, titled "LTL Model-Checking for Security Protocols", has been awarded the CLUSIT prize 2010 by the Italian Association for Information Security.

Software Tools

- **SATMC** (SAT-based Model Checker) [ACC14; ACC16] is a bounded model checker for security protocols. SATMC reduces the problem of checking whether a protocol is vulnerable to attacks of bounded length to the satisfiability of a propositional formula which is then solved by a state-of-the-art SAT solver taken off-the-shelf. SATMC has been developed and used as back-end in a number of EU projects: AVISS (01-02), AVISPA (03-05), AVANTSSAR (08-10), SPaCIoS (11-13), STIATE (14). Moreover, SATMC in the past has been used as an automated testcase generator in Tookan, a tool for analysing PKCS#11 security tokens, and it lied at the core of industrial strength tools (e.g., the Security Validator plugin for SAP NetWeaver BPM, developed by the Product Security Research unit at SAP).

  The core of SATMC has been developed by Alessandro Armando and Luca Compagna. I developed some key extensions of SATMC and I am currently the main developer of the tool. On September, 2013 I gave an invited talk about SATMC in the context of the "Tool Session" of the 13th International School on Foundations of Security Analysis and Design (FOSAD 2013).

- **Blast** (BLAck-box Security Testing) [Sud+16] is a tool for discovering security vulnerabilities in the protocols underling security-critical Multi-Party Web Applications (MPWAs). MPWAs rely on core trusted third-party systems—e.g., payment servers, identity providers—and protocols—e.g., Cashier-as-a-Service, Single Sign-On—to deliver business services to users. Blast leverages 6 attack patterns (generalizations of 11 prominent attacks from the literature) to generate attack test cases against the MPWAs under test. Blast has been used to discover 21 previously-unknown security vulnerabilities in prominent MPWAs (e.g. `twitter.com`, OpenCart v2.1.0.1). The implementation of Blast is based on OWASP ZAP, a widely-used, open-source penetration testing tool.

  The first version of Blast has been developed by the PhD student Avinash Sudhodanan, under my co-supervision, together with SAP, in the context of the SECENTIS project. Blast is currently being experimented at SAP and other industrial players are considering its adoption.

- **MuFASA** (`https://stfbk.github.io/tools/MuFASA`) is a tool for high-level specification and analysis of Multi-factor Authentication (MFA) protocols, which aims at supporting normal users and security experts (in the design phase of an MFA protocol), providing a high level report regarding possible risks associated to the specified MFA protocol, its resistance to a set of attacker models (defined by NIST), its ease-of-use and its compliance with a set of security requirements derived from European laws.

  MuFASA has been developed by the PhD student Federico Sinigaglia, under my co-supervision, together with Gabriele Costa and Silvio Ranise.

- **mIDAssistant** (`https://github.com/stfbk/mIDAssistant`) is an Android Studio plugin that guides native mobile app developers with secure integration of Single Sign-On and Access Delegation solutions within their apps.

  mIDAssistant has been developed by the PhD student Amir Sharif, under my co-supervision, together with Silvio Ranise and Giada Sciarretta.

- **Micro-Id-Gym** (`https://stfbk.github.io/tools/Micro-Id-Gym`) offers Identity Management Workouts with Container-Based Microservices: users can develop hands-on experiences on how IdM solutions work and increase their awareness related to the underlying security issues.

  Micro-Id-Gym has been developed by Andrea Bisegna (with the contributions of students involved in internships and theses in FBK), under my co-supervision, together with Silvio Ranise.

- **CryptoAC** (`https://stfbk.github.io/tools/CryptoAC`) is a tool for Flexible and Automated Role-based Cryptographic Access Control Enforcement in the Cloud.

  CryptoAC has been developed by Stefano Berlato, under my co-supervision, together with Silvio Ranise.

Patent

US Patent Filed
- Invention Status Filed
- Invention Title: Dynamic Analysis Security Testing of Multi-Party Web Applications via Attack Patterns
- Inventors: Alessandro Armando, Roberto Carbone, Luca Compagna, Avinash Sudhodanan
Filing Information:
Country: United States of America, Application No: 16 Oct 2015, Patent ID: 14/885,001, Reference No: 83111010, Status: 150880US01

List of Publications

International Journals

[Sci+20] G. Sciarretta, R. Carbone, S. Ranise, and L. Viganò. "Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Login". In: *ACM Trans. Priv. Secur.* 23.3 (2020), 13:1–13:37. DOI: `10.1145/3386685`. URL: `https://doi.org/10.1145/3386685`.

[Sin+20] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone. "A survey on multi-factor authentication for online banking in the wild". In: *Comput. Secur.* 95 (2020), p. 101745. DOI: `10.1016/j.cose.2020.101745`. URL: `https://doi.org/10.1016/j.cose.2020.101745`.

[Bis+19] A. Bisegna, R. Carbone, I. Martini, V. Odorizzi, G. Pellizzari, and S. Ranise. "Micro-Id-Gym: Identity Management Workouts with Container-Based Microservices". In: *International Journal of Information Security and Cybercrime* 8 (2019), pp. 45–50. DOI: `10.19107/IJISC.2019.01.06`. URL: `http://doi.org/10.19107/IJISC.2019.01.06`.

[Sci+17] G. Sciarretta, R. Carbone, S. Ranise, and A. Armando. "Anatomy of the Facebook solution for mobile single sign-on: Security assessment and improvements". In: *Comput. Secur.* 71 (2017), pp. 71–86. DOI: `10.1016/j.cose.2017.04.011`. URL: `https://doi.org/10.1016/j.cose.2017.04.011`.

[ACC16] A. Armando, R. Carbone, and L. Compagna. "SATMC: a SAT-based model checker for security protocols, business processes, and security APIs". In: *Int. J. Softw. Tools Technol. Transf.* 18.2 (2016), pp. 187–204. DOI: `10.1007/s10009-015-0385-y`. URL: `https://doi.org/10.1007/s10009-015-0385-y`.

[Arm+13] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino, and A. Sorniotti. "An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations". In: *Comput. Secur.* 33 (2013), pp. 41–58. DOI: 10.1016/j.cose.2012.08.007. URL: https://doi.org/10.1016/j.cose.2012.08.007.

[Car11] R. Carbone. "LTL model-checking for security protocols". In: *AI Commun.* 24.3 (2011), pp. 281–283. DOI: 10.3233/AIC-2010-0489. URL: https://doi.org/10.3233/AIC-2010-0489.

[ACC09] A. Armando, R. Carbone, and L. Compagna. "LTL model checking for security protocols". In: *J. Appl. Non Class. Logics* 19.4 (2009), pp. 403–429. DOI: 10.3166/jancl.19.403-429. URL: https://doi.org/10.3166/jancl.19.403-429.

Book Chapters

[Bis+20a] A. Bisegna, R. Carbone, M. Ceccato, S. Manfredi, S. Ranise, G. Sciarretta, A. Tomasi, and E. Viglianisi. "Automated Assistance to the Security Assessment of API for Financial Services". In: *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Ed. by J. Soldatos, J. Philpot, and G. Giunta. Boston-Delft: now publishers, 2020, pp. 94–103. DOI: 10.1561/9781680836875.ch6. URL: http://dx.doi.org/10.1561/9781680836875.ch6.

[Arm+12b] A. Armando, R. Carbone, L. Compagna, and G. Pellegrino. "Automatic Security Analysis of SAML-Based Single Sign-On Protocols". In: *Digital Identity and Access Management: Technologies and Frameworks*. Ed. by R. Sharman, S. D. Smith, and M. Gupta. IGI Global, 2012, pp. 168–187. DOI: 10.4018/978-1-61350-498-7.ch010. URL: http://doi.org/10.4018/978-1-61350-498-7.ch010.

[Car+11] R. Carbone, M. Minea, S. Mödersheim, S. E. Ponta, M. Turuani, and L. Viganò. "Towards Formal Validation of Trust and Security in the Internet of Services". In: *The Future Internet - Future Internet Assembly 2011: Achievements and Technological Promises*. Ed. by J. Domingue, A. Galis, A. Gavras, T. B. Zahariadis, D. Lambert, F. Cleary, P. Daras, S. Krco, H. Müller, M. Li, H. Schaffers, V. Lotz, F. Alvarez, B. Stiller, S. Karnouskos, S. Avessta, and M. Nilsson. Vol. 6656. Lecture Notes in Computer Science. Springer, 2011, pp. 193–208. DOI: 10.1007/978-3-642-20898-0_14. URL: https://doi.org/10.1007/978-3-642-20898-0_14.

[Rud+09] C. Rudolph, L. Compagna, R. Carbone, A. Muñoz, and J. Repp. "Verification of S&D Solutions for Network Communications and Devices". In: *Security and Dependability for Ambient Intelligence*. Ed. by S. Kokolakis, A. M. Gómez, and G. Spanoudakis. Vol. 45. Advances in Information Security. Springer, 2009, pp. 143–163. DOI: 10.1007/978-0-387-88775-3_9. URL: https://doi.org/10.1007/978-0-387-88775-3_9.

International Conferences

[Ber+20] S. Berlato, R. Carbone, A. J. Lee, and S. Ranise. "Exploring Architectures for Cryptographic Access Control Enforcement in the Cloud for Fun and Optimization". In: *ASIA CCS '20: The 15th ACM Asia Conference on Computer and Communications Security, Taipei, Taiwan, October 5-9, 2020*. Ed. by H. Sun, S. Shieh, G. Gu, and G. Ateniese. ACM, 2020, pp. 208–221. DOI: 10.1145/3320269.3384767. URL: https://doi.org/10.1145/3320269.3384767.

[Bis+20b] A. Bisegna, R. Carbone, G. Pellizzari, and S. Ranise. “Micro-Id-Gym: A Flexible Tool for Pentesting Identity Management Protocols in the Wild and in the Laboratory”. In: *Emerging Technologies for Authorization and Authentication - Third International Workshop, ETAA 2020, Guildford, UK, September 18, 2020, Proceedings*. Ed. by A. Saracino and P. Mori. Vol. 12515. Lecture Notes in Computer Science. Springer, 2020, pp. 71–89. DOI: 10.1007/978-3-030-64455-0_5. URL: https://doi.org/10.1007/978-3-030-64455-0_5.

[Cen+20] M. Centenaro, S. Berlato, R. Carbone, G. Burzio, G. F. Cordella, S. Ranise, and R. Riggio. “Security Considerations on 5G-Enabled Back-Situation Awareness for CCAM”. In: *3rd IEEE 5G World Forum, 5GWF 2020, Bangalore, India, September 10-12, 2020*. IEEE, 2020, pp. 245–250. DOI: 10.1109/5GWF49715.2020.9221064. URL: https://doi.org/10.1109/5GWF49715.2020.9221064.

[Per+20] M. Pernpruner, R. Carbone, S. Ranise, and G. Sciarretta. “The Good, the Bad and the (Not So) Ugly of Out-of-Band Authentication with eID Cards and Push Notifications: Design, Formal and Risk Analysis”. In: *CODASPY ’20: Tenth ACM Conference on Data and Application Security and Privacy, New Orleans, LA, USA, March 16-18, 2020*. Ed. by V. Roussev, B. M. Thuraisingham, B. Carminati, and M. Kantarcioglu. ACM, 2020, pp. 223–234. DOI: 10.1145/3374664.3375727. URL: https://doi.org/10.1145/3374664.3375727.

[Sha+20] A. Sharif, R. Carbone, G. Sciarretta, and S. Ranise. “Automated and Secure Integration of the OpenID Connect iGov Profile in Mobile Native Applications”. In: *Emerging Technologies for Authorization and Authentication - Third International Workshop, ETAA 2020, Guildford, UK, September 18, 2020, Proceedings*. Ed. by A. Saracino and P. Mori. Vol. 12515. Lecture Notes in Computer Science. Springer, 2020, pp. 50–70. DOI: 10.1007/978-3-030-64455-0_4. URL: https://doi.org/10.1007/978-3-030-64455-0_4.

[Sha+19] A. Sharif, R. Carbone, S. Ranise, and G. Sciarretta. “A Wizard-based Approach for Secure Code Generation of Single Sign-On and Access Delegation Solutions for Mobile Native Apps”. In: *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2: SECRYPT, Prague, Czech Republic, July 26-28, 2019*. Ed. by M. S. Obaidat and P. Samarati. SciTePress, 2019, pp. 268–275. DOI: 10.5220/0007930502680275. URL: https://doi.org/10.5220/0007930502680275.

[Sin+19] F. Sinigaglia, R. Carbone, G. Costa, and S. Ranise. “MuFASA: A Tool for High-level Specification and Analysis of Multi-factor Authentication Protocols”. In: *Emerging Technologies for Authorization and Authentication - Second International Workshop, ETAA 2019, Luxembourg City, Luxembourg, September 27, 2019, Proceedings*. Ed. by A. Saracino and P. Mori. Vol. 11967. Lecture Notes in Computer Science. Springer, 2019, pp. 138–155. DOI: 10.1007/978-3-030-39749-4_9. URL: https://doi.org/10.1007/978-3-030-39749-4_9.

[CRS18] R. Carbone, S. Ranise, and G. Sciarretta. “Design and Security Assessment of Usable Multi-factor Authentication and Single Sign-On Solutions for Mobile Applications - A Workshop Experience Report”. In: *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data - 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers*. Ed. by E. Kosta, J. Pierson, D. Slamanig, S. Fischer-Hübner, and S. Krenn. Vol. 547. IFIP Advances in Information and Communication Technology. Springer, 2018, pp. 51–66. DOI: 10.1007/978-3-030-16744-8_4. URL: https://doi.org/10.1007/978-3-030-16744-8_4.

[Sci+18] G. Sciarretta, R. Carbone, S. Ranise, and L. Viganò. “Design, Formal Specification and Analysis of Multi-Factor Authentication Solutions with a Single Sign-On Experience”. In: *Principles of Security and Trust - 7th International Conference, POST 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings*. Ed. by L. Bauer and R. Küsters. Vol. 10804. Lecture

Notes in Computer Science. Springer, 2018, pp. 188–213. DOI: 10.1007/978-3-319-89722-6_8. URL: https://doi.org/10.1007/978-3-319-89722-6_8.

[CSC17] G. Costa, F. Sinigaglia, and R. Carbone. "PolEnA: Enforcing Fine-grained Permission Policies in Android". In: *Computer Safety, Reliability, and Security - SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017, Proceedings*. Ed. by S. Tonetta, E. Schoitsch, and F. Bitsch. Vol. 10489. Lecture Notes in Computer Science. Springer, 2017, pp. 407–414. DOI: 10.1007/978-3-319-66284-8_34. URL: https://doi.org/10.1007/978-3-319-66284-8_34.

[SCC17] F. Sinigaglia, R. Carbone, and G. Costa. "Strong Authentication for e-Banking: A Survey on European Regulations and Implementations". In: *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT, Madrid, Spain, July 24-26, 2017*. Ed. by P. Samarati, M. S. Obaidat, and E. Cabello. SciTePress, 2017, pp. 480–485. DOI: 10.5220/0006438504800485. URL: https://doi.org/10.5220/0006438504800485.

[Sud+17] A. Sudhodanan, R. Carbone, L. Compagna, N. Dolgin, A. Armando, and U. Morelli. "Large-Scale Analysis & Detection of Authentication Cross-Site Request Forgeries". In: *2017 IEEE European Symposium on Security and Privacy, EuroS&P 2017, Paris, France, April 26-28, 2017*. IEEE, 2017, pp. 350–365. DOI: 10.1109/EuroSP.2017.45. URL: https://doi.org/10.1109/EuroSP.2017.45.

[Sci+16] G. Sciarretta, A. Armando, R. Carbone, and S. Ranise. "Security of Mobile Single Sign-On: A Rational Reconstruction of Facebook Login Solution". In: *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4: SECRYPT, Lisbon, Portugal, July 26-28, 2016*. Ed. by C. Callegari, M. van Sinderen, P. G. Sarigiannidis, P. Samarati, E. Cabello, P. Lorenz, and M. S. Obaidat. SciTePress, 2016, pp. 147–158. DOI: 10.5220/0005969001470158. URL: https://doi.org/10.5220/0005969001470158.

[SCR16] G. Sciarretta, R. Carbone, and S. Ranise. "A delegated authorization solution for smart-city mobile applications". In: *2nd IEEE International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow, RTSI 2016, Bologna, Italy, September 7-9, 2016*. IEEE, 2016, pp. 1–6. DOI: 10.1109/RTSI.2016.7740623. URL: https://doi.org/10.1109/RTSI.2016.7740623.

[Sud+16] A. Sudhodanan, A. Armando, R. Carbone, and L. Compagna. "Attack Patterns for Black-Box Security Testing of Multi-Party Web Applications". In: *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*. The Internet Society, 2016. URL: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/attack-patterns-black-box-security-testing-multi-party-web-applications.pdf.

[Arm+15] A. Armando, R. Carbone, G. Costa, and A. Merlo. "Android Permissions Unleashed". In: *IEEE 28th Computer Security Foundations Symposium, CSF 2015, Verona, Italy, 13-17 July, 2015*. Ed. by C. Fournet, M. W. Hicks, and L. Viganò. IEEE Computer Society, 2015, pp. 320–333. DOI: 10.1109/CSF.2015.29. URL: https://doi.org/10.1109/CSF.2015.29.

[Car+15] R. Carbone, L. Compagna, A. Panichella, and S. E. Ponta. "Security Threat Identification and Testing". In: *8th IEEE International Conference on Software Testing, Verification and Validation, ICST 2015, Graz, Austria, April 13-17, 2015*. IEEE Computer Society, 2015, pp. 1–8. DOI: 10.1109/ICST.2015.7102630. URL: https://doi.org/10.1109/ICST.2015.7102630.

[Arm+14a] A. Armando, R. Carbone, E. G. Chekole, C. Petrazzuolo, A. Ranalli, and S. Ranise. “Selective Release of Smart Metering Data in Multi-domain Smart Grids”. In: *Smart Grid Security - Second International Workshop, SmartGridSec 2014, Munich, Germany, February 26, 2014, Revised Selected Papers*. Ed. by J. Cuéllar. Vol. 8448. Lecture Notes in Computer Science. Springer, 2014, pp. 48–62. DOI: `10.1007/978-3-319-10329-7\_4`. URL: `https://doi.org/10.1007/978-3-319-10329-7\_4`.

[Arm+14b] A. Armando, R. Carbone, E. G. Chekole, and S. Ranise. “Attribute based access control for APIs in spring security”. In: *19th ACM Symposium on Access Control Models and Technologies, SACMAT ’14, London, ON, Canada - June 25 - 27, 2014*. Ed. by S. L. Osborn, M. V. Tripunitara, and I. Molloy. ACM, 2014, pp. 85–88. DOI: `10.1145/2613087.2613109`. URL: `https://doi.org/10.1145/2613087.2613109`.

[ACC14] A. Armando, R. Carbone, and L. Compagna. “SATMC: A SAT-Based Model Checker for Security-Critical Systems”. In: *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*. Ed. by E. Ábrahám and K. Havelund. Vol. 8413. Lecture Notes in Computer Science. Springer, 2014, pp. 31–45. DOI: `10.1007/978-3-642-54862-8\_3`. URL: `https://doi.org/10.1007/978-3-642-54862-8\_3`.

[ACZ13] A. Armando, R. Carbone, and L. Zanetti. “Formal Modeling and Automatic Security Analysis of Two-Factor and Two-Channel Authentication Protocols”. In: *Network and System Security - 7th International Conference, NSS 2013, Madrid, Spain, June 3-4, 2013. Proceedings*. Ed. by J. López, X. Huang, and R. Sandhu. Vol. 7873. Lecture Notes in Computer Science. Springer, 2013, pp. 728–734. DOI: `10.1007/978-3-642-38631-2\_63`. URL: `https://doi.org/10.1007/978-3-642-38631-2\_63`.

[Arm+12a] A. Armando, W. Arsac, T. Avanesov, M. Barletta, A. Calvi, A. Cappai, R. Carbone, Y. Chevalier, L. Compagna, J. Cuéllar, G. Erzse, S. Frau, M. Minea, S. Mödersheim, D. von Oheimb, G. Pellegrino, S. E. Ponta, M. Rocchetto, M. Rusinowitch, M. T. Dashti, M. Turuani, and L. Viganò. “The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures”. In: *Tools and Algorithms for the Construction and Analysis of Systems - 18th International Conference, TACAS 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings*. Ed. by C. Flanagan and B. König. Vol. 7214. Lecture Notes in Computer Science. Springer, 2012, pp. 267–282. DOI: `10.1007/978-3-642-28756-5\_19`. URL: `https://doi.org/10.1007/978-3-642-28756-5\_19`.

[ACM12] A. Armando, R. Carbone, and A. Merlo. “Formal Analysis of a Privacy-Preserving Billing Protocol”. In: *Smart Grid Security - First International Workshop, SmartGridSec 2012, Berlin, Germany, December 3, 2012, Revised Selected Papers*. Ed. by J. Cuéllar. Vol. 7823. Lecture Notes in Computer Science. Springer, 2012, pp. 108–119. DOI: `10.1007/978-3-642-38030-3\_8`. URL: `https://doi.org/10.1007/978-3-642-38030-3\_8`.

[Arm+12c] A. Armando, G. Pellegrino, R. Carbone, A. Merlo, and D. Balzarotti. “From Model-Checking to Automated Testing of Security Protocols: Bridging the Gap”. In: *Tests and Proofs - 6th International Conference, TAP@TOOLS 2012, Prague, Czech Republic, May 31 - June 1, 2012. Proceedings*. Ed. by A. D. Brucker and J. Julliand. Vol. 7305. Lecture Notes in Computer Science. Springer, 2012, pp. 3–18. DOI: `10.1007/978-3-642-30473-6\_3`. URL: `https://doi.org/10.1007/978-3-642-30473-6\_3`.

[Arm+11] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino, and A. Sorniotti. “From Multiple Credentials to Browser-Based Single Sign-On: Are We More Secure?” In: *Future Challenges in Security and Privacy for Academia and Industry - 26th IFIP TC 11 International Information Security Conference, SEC 2011, Lucerne, Switzerland, June 7-9, 2011. Proceedings*. Ed. by J. Camenisch, S. Fischer-Hübner, Y. Murayama, A. Portmann, and C. Rieder. Vol. 354. IFIP Advances in Information and Communication Technology. Springer, 2011, pp. 68–79. DOI: 10.1007/978-3-642-21424-0_6. URL: https://doi.org/10.1007/978-3-642-21424-0_6.

[ACR11] A. Armando, R. Carbone, and S. Ranise. "Automated Analysis of Semantic-Aware Access Control Policies: A Logic-Based Approach". In: *Proceedings of the 5th IEEE International Conference on Semantic Computing (ICSC 2011), Palo Alto, CA, USA, September 18-21, 2011*. IEEE Computer Society, 2011, pp. 356–363. DOI: 10.1109/ICSC.2011.74. URL: https://doi.org/10.1109/ICSC.2011.74.

[Ghe+11] G. Gheorghe, B. Crispo, R. Carbone, L. Desmet, and W. Joosen. "Deploy, Adjust and Readjust: Supporting Dynamic Reconfiguration of Policy Enforcement". In: *Middleware 2011 - ACM/IFIP/USENIX 12th International Middleware Conference, Lisbon, Portugal, December 12-16, 2011. Proceedings*. Ed. by F. Kon and A. Kermarrec. Vol. 7049. Lecture Notes in Computer Science. Springer, 2011, pp. 350–369. DOI: 10.1007/978-3-642-25821-3_18. URL: https://doi.org/10.1007/978-3-642-25821-3_18.

[Arm+10] A. Armando, R. Carbone, L. Compagna, K. Li, and G. Pellegrino. "Model-Checking Driven Security Testing of Web-Based Applications". In: *Third International Conference on Software Testing, Verification and Validation, ICST 2010, Paris, France, April 7-9, 2010, Workshops Proceedings*. IEEE Computer Society, 2010, pp. 361–370. DOI: 10.1109/ICSTW.2010.54. URL: https://doi.org/10.1109/ICSTW.2010.54.

[Arm+08] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, and L. Tobarra. "Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps". In: *Proceedings of the 6th ACM Workshop on Formal Methods in Security Engineering, FMSE 2008, Alexandria, VA, USA, October 27, 2008*. Ed. by V. Shmatikov. ACM, 2008, pp. 1–10. DOI: 10.1145/1456396.1456397. URL: https://doi.org/10.1145/1456396.1456397.

[ACC07] A. Armando, R. Carbone, and L. Compagna. "LTL Model Checking for Security Protocols". In: *20th IEEE Computer Security Foundations Symposium, CSF 2007, 6-8 July 2007, Venice, Italy*. IEEE Computer Society, 2007, pp. 385–396. DOI: 10.1109/CSF.2007.24. URL: https://doi.org/10.1109/CSF.2007.24.

Trento, January, 2021

Roberto Carbone