Statement of Research

Carlos E. Rubio-Medrano, Ph.D.

Motivation. Computing has had a major impact in modern societies, which has ultimately resulted in extended convenience, efficiency, and an steady reduction in costs and prices. However, cyber-infrastructures now face a plethora of attacks and threats, e.g., privacy violations [1], data leaks [2], and even recent state-sponsored attacks to mission-critical *energy delivery systems* (EDS) such as the power grid, gas, and oil industries [3]. Besides having disastrous economical consequences, successful cyber-attacks also severely undermine the public's confidence in cyber-infrastructures and emerging technologies.

My Approach. As a response to this challenge, I am developing solutions that not only target the roots and causes of cyber-attacks and incidents, but can be also easily understood, used, and customized by both developers and end-users. To achieve such a goal, the following thrusts are needed:

(I) We need to **analyze, understand, and assess the attacks, threats, and risks** targeting cyber-infrastructures, as well as their existing counteracting techniques.

(II) Based on observed strengths, shortcomings, and deficiencies of existing cyber-protections, we need to **introduce new theoretical models and techniques** providing a novel, innovative, and efficient take on fundamental cybersecurity principles and techniques, e.g., authorization and access control.

(III) We also need to **correctly implement these novel models and techniques**, e.g., by constructing software following a *security-by-design* principle, and by leveraging existing and newer techniques for effective software *verification* and *validation* (V&V), such that bugs and vulnerabilities an be removed.

In the rest of this document, I elaborate on my future research plans as well as the experience I have accumulated as a result of previous work on each of these thrusts.

Thrust I: Proactive Understanding and Assessment of Cybersecurity Risks

Main Idea. I am working on approaches for the automated and proactive monitoring and risk assessment of mission-critical cyber-infrastructures, such that a meaningful, well-defined, and *up-to-date* representation of risk can be retrieved directly from data obtained from such cyber-infrastructures, ultimately supporting further decision-making and convenience.

Previous Work. I led the development of *OntoEDS* [4], an ontology engine featuring a series of recommendations and best practices for implementing cyber-protections in the context of EDS, as featured by a series of documents issued by well-reputed organizations in such a domain, e.g., IEEE, NERC and NIST, among others. Later, using *OntoEDS* as a back-end engine, I developed *ExSol* [5], a framework that intelligently calculates risk scores by leveraging a set of metrics as well as information on attacks, threats, and their corresponding security requirements, Using ontology projections, *ExSol* calculates both an *exploitation* and a *solution* scores, which are obtained by mathematically combining metric scores for each of the attacks and threats (exploitations), as well as the security requirements and techniques (solutions) for EDS assets. Also, I developed *EDS-SAT* [6], a consolidated and highly-customizable framework in the context of EDS, which leverages *ExSol* to automatically calculate risks from EDS devices. Finally, I assessed the current cybersecurity state of a series of open-source *medical cyber-physical systems* (MCPS) [7], which resulted in most of them failing to implement essential cyber-protections as mandated by existing regulations, making them vulnerable to several attacks and threats.

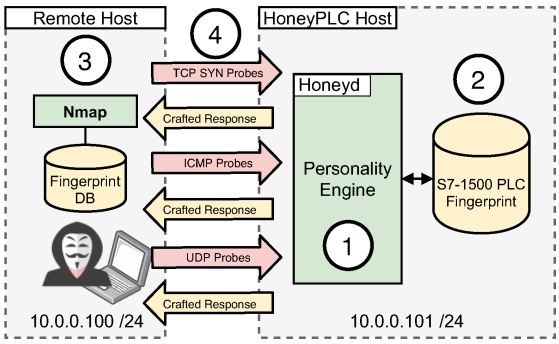

Figure 1: The HoneyPLC Personality Engine.

Current and Future Work. Continuing with this line of work, I recently led the development of *HoneyPLC* [8], a high-interaction, extensible, and malware-collecting honeypot for *programmable logic controllers* (PLCs), which play a key role as a bridge between the cyber and the physical worlds in EDS, e.g., controlling centrifuge machines in nuclear power plants. Experimental results showed that UCM exhibits a high level of camouflaging due to its *personality engine* featured in Fig. 1: it was identified as real devices by multiple widely used reconnaissance tools, and it was also able to record a large amount of interesting interactions over the Internet. Following with this line of work, I am currently leading a project intended to collect and analyze recent attacks and defenses for PLCs, in an effort to better assess the current security state of such devices, including pressing concerns and potential research gaps.

Thrust II: Effective and Convenient Enforcement of Cybersecurity Principles

Main Idea. Based on the idea that emerging technologies must be paired with equally innovative security solutions, I am working on solutions that not only address pressing concerns, but also allow for end-users tocwrite and enforce security policies without the need of extensive training and/or complex management interfaces, in an effort to encourage the adoption of cyber-protections in practice.

Previous Work. I recently led the development of *SpaceProtector* [9], a framework that leverages a distributed architecture and a novel attribute-based theoretical model for writing, storing, and enforcing authorization policies for *mobile augmented reality* (MAR) [10] applications, a.k.a., MAR-Apps, allowing them to restrict their functionality, e.g., display of digital objects on top of a video stream, in *sensitive* physical spaces such as hospitals, memorials, schools, etc. Additionally, I developed *DyPolDroid* [11], a similar security framework which automatically calculates, deploys, and enforces security policies for Android devices by leveraging recent innovations introduced by the Android Enterprise Management System, ultimately protecting end-users from costly *permission-abusing* attacks [12] carried out by malicious applications.

Current and Future Work. I am currently leading the development of *No-Fly-Zone* [13], featured in Fig. 2, an open-source framework to regulate commercial and recreational fly-overs made by *unmanned aerial vehicles* (UAVs), a.k.a., drones. by: identifying and delimiting sensitive physical spaces, specifying and enforcing restrictions on drone flights, calculating flight plans for drones passing over sensitive spaces, and limiting airspace drone occupancy by orchestrating flight plans. In addition, I am also leading the development of *ScienceAccess* [14], which leverages previous experiences implementing *federated access management* (FAM) [15] in the context of independently-run organizations interested in sharing resources between them, e.g., computational time and remote storage, in a secure way. Using *ScienceAccess*, participant organizations mediate access to resources by means of a set of *federated* authorization policies, which leverage security-relevant, runtime-collected pieces of information known as *attributes* [16]. Ultimately, *ScienceAccess* will provide a flexible approach that will allow for organizations to leverage their existing cyber-protection mechanisms, and will also provide automated, seamless, and efficient authorization enforcement making it convenient for administrators and scientists.

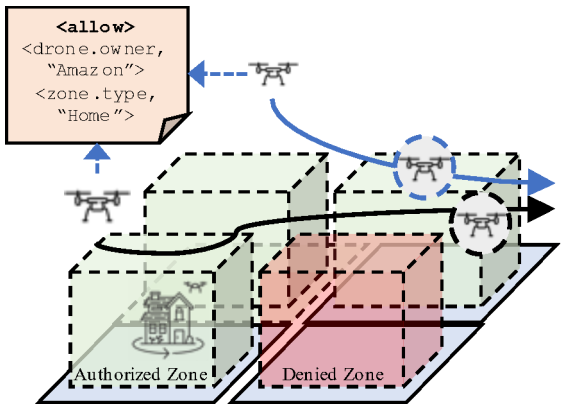

Figure 2: The No-Fly-Zone UAV Framework.

Thrust III: Cybersecurity Assurance with Assertion-based Software Construction

Main Idea. I am working on providing formal specifications of cybersecurity methodologies, such that their components, interactions, assumptions, and potential runtime exceptions are well-defined and documented. Based on those specs, I am leading the development of frameworks and tools that can effectively expose and remove security vulnerabilities, and can also be customized by developers/testers as needed.

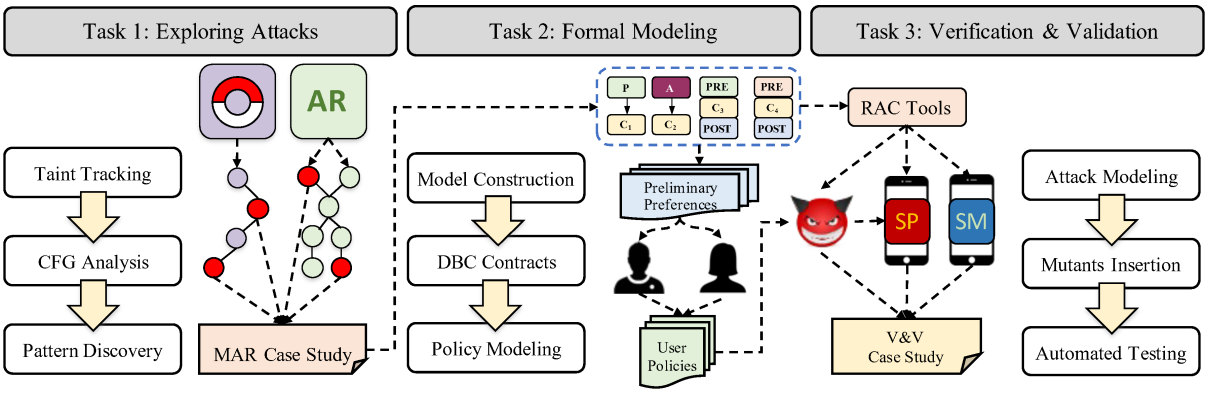

Figure 3: The Tasks and the Research Products devised for the Initial Steps of *SafeMAR*.

Previous Work. I have recently leveraged well-established techniques for behavioral specification and V&V of software modules such as *software assertions* [17] and *design by contract* (DBC) [18]. As an example, I have developed DBC-like specifications for cybersecurity methodologies and techniques such as the Java Security Package [19] and *role-based access control* (RBAC) [20]. In addition, I have also worked on the development of tools for effective software V&V at the source code level featuring *runtime assertion code* (RAC) [21] and automated testing [22]. Also, I recently collaborated in an approach [23] to provide formal specifications of access control models and using them to verify the correct implementation of cybersecurity properties in a series of software systems used in practice, which resulted in the discovery of a series of vulnerabilities that may have allowed for attackers to completely bypass existing cyber-protections.

Current and Future Work. I am currently leading the development of *SafeMAR*: a Secure and Safe Software Construction Framework, which will allow for MAR-Apps to correctly follow the users' preferences when distributing digital content. As shown in Fig. 3, I will first explore how the functionality offered to users by MAR-Apps, as well as their internal code constructs for content distribution facilitate and make the aforementioned attacks possible. To achieve this, we will conduct a case study on a series of MAR-Apps that are currently available in the market, leveraging techniques such as *Taint Tracking* [24] and *Control Flow Analysis* [25]. Next, I will formally describe how content is distributed on MAR-Apps, such that not only future implementations can use such description as a well-defined reference, but it can also be used as an effective aid for producing better MAR-Apps via supporting APIs and V&V tools. To this end, we will develop a *Content Mediation* (CM) model, which will in turn leverage *First Order Logic* [26], *Software Assertions* [27], and *Design by Contract* (DBC) [28]. Next, I will conduct a user study to determine a representative set of preferences for content distribution using a subset of the MAR-Apps along with a variety of case scenarios. Our results will be incorporated into a series of *User Policies* that will leverage the CM model, along with *Attributes* [29], to allow for non-expert users to define their preferences for content distribution. Finally, there is a need to detect and remove erroneous implementations in the enforcement of user preferences regulating the distribution of content. As an initial step towards this goal, we will leverage the CM model and the User Policies produced in as well as well-established techniques such as *Runtime Assertion Checking* (RAC) [30], and *Automated Specification-based Testing* [31]. In this project, I am leveraging the aforementioned *SpaceProtector* as well as *SpaceMediator* [32], two gaming MAR-Apps we have developed from scratch in previous work.

References

[1] Time, "Pokemon Go Players Anger 9/11 Memorial Visitors." `http://time.com/4403516/pokemon-go-911-memorial-holocaust-museum/`, 2017. [Online; accessed June-5-2017].

[2] Wired, "Everything We Know About Facebook's Massive Security Breach." `https://www.wired.com/story/facebook-security-breach-50-million-accounts/`, 2019. [Online; accessed September-27-2019].

[3] Dragos Inc., "CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations." https://dragos.com/blog/crashoverride/CrashOverride-01.pdf, 2017. [Online; accessed September-27-2019].

[4] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G.-J. Ahn, "Ontoeds: Protecting energy delivery systems by collaboratively analyzing security requirements," in *Collaboration and Internet Computing, 3rd IEEE International Conference on*, pp. 1–10, IEEE, October 2017.

[5] J. Lamp, C. E. Rubio-Medrano, , Z. Zhao, and G.-J. Ahn, "Exsol: Collaboratively assessing cybersecurity risks for protecting energy delivery systems," in *Modeling and Simulation of Cyber-Physical Energy Systems, 2019 Workshop on*, pp. 1–6, IEEE, April 2019.

[6] J. Lamp, C. E. Rubio-Medrano, , Z. Zhao, A. Doupe, and G.-J. Ahn, "Towards adaptive and proactive security assessment for energy delivery systems," in *Modeling and Simulation of Cyber-Physical Energy Systems, 2017 Workshop on*, pp. 1–6, IEEE, April 2017.

[7] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G.-J. Ahn, "The danger of missing instructions: A systematic analysis of security requirements for mcps," in *Connected Health: Applications, Systems and Engineering Technologies: CHASE-MedSPT2018, the IEEE/ACM 3rd International Conference on*, pp. 94–99, ACM/IEEE, September 2018.

[8] E. López-Morales, C. Rubio-Medrano, A. Doupé, Y. Shoshitaishvili, R. Wang, T. Bao, and G.-J. Ahn, "Honeyplc: A next-generation honeypot for industrial control systems," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, (New York, NY, USA), p. 279–291, Association for Computing Machinery, 2020.

[9] C. E. Rubio-Medrano, S. Jogani, M. Leitner, Z. Zhao, and G.-J. Ahn, "Effectively enforcing authorization constraints for emerging space-sensitive technologies," in *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, SACMAT '19, (New York, NY, USA), pp. 195–206, ACM, 2019.

[10] J. Carmigniani, B. Furht, M. Anisetti, P. Ceravolo, E. Damiani, and M. Ivkovic, "Augmented reality technologies, systems and applications," *Multimedia Tools Appl.*, vol. 51, pp. 341–377, Jan. 2011.

[11] C. Rubio-Medrano, M. Hill, L. Claramunt, J. Baek, and G. Ahn, "Dypoldroid: Protecting users and organizations from permission-abuse attacks in android," in *Secure Knowledge Management In The Artificial Intelligence Era - 9th International Conference, SKM 2021, Proceedings*, Communications in Computer and Information Science, pp. 23–36, Springer Science and Business Media Deutschland GmbH, 2022.

[12] X. Wei, L. Gomez, I. Neamtiu, and M. Faloutsos, "Permission evolution in the android ecosystem," in *Proceedings of the 28th Annual Computer Security Applications Conference*, ACSAC '12, (New York, NY, USA), pp. 31–40, ACM, 2012.

[13] C. Rubio-Medrano, T. Chu, P. Rangel, and J. Baca, "CISE-MSI: DP: SaTC: Dynamically Enforcing User-Oriented Geospatial Restrictions for Drone Fly-Overs." https://www.nsf.gov/awardsearch/showAward?AWD_ID=2131263, 2021. [Online; accessed November-1-2022].

[14] G.-J. Ahn, C. Rubio-Medrano, and J. Baek, "CICI: UCSS: ScienceAccess: Enabling Zero-Trust Resource Access Management for Scientific Collaborations." https://www.nsf.gov/awardsearch/showAward?AWD_ID=2232911, 2022. [Online; accessed November-1-2022].

[15] C. E. Rubio-Medrano, Z. Zhao, A. Doupe, and G.-J. Ahn, "Federated access management for collaborative network environments: Framework and case study," in *Proceedings of the 20th ACM Symposium on Access Control Models and Technologies*, SACMAT '15, (New York, NY, USA), pp. 125–134, ACM, 2015.

[16] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, pp. 85–88, Feb 2015.

[17] L. A. Clarke and D. S. Rosenblum, "A historical perspective on runtime assertion checking in software development," *SIGSOFT Softw. Eng. Notes*, vol. 31, pp. 25–37, May 2006.

[18] B. Meyer, "Applying 'design by contract'," *Computer*, vol. 25, pp. 40–51, Oct 1992.

[19] P. Agarwal, C. E. Rubio-Medrano, Y. Cheon, and P. J. Teller, "A formal specification in jml of java security package," in *Advances and Innovations in Systems, Computing Sciences and Software Engineering* (K. Elleithy, ed.), (Dordrecht), pp. 363–368, Springer Netherlands, 2007.

[20] C. E. Rubio-Medrano, G.-J. Ahn, and K. Sohr, "Achieving security assurance with assertion-based application construction," *EAI Endorsed Transactions on Collaborative Computing*, vol. 1, 12 2015.

[21] C. E. Rubio-Medrano and Y. Cheon, "Access control contracts for java program modules," in *International Workshop on Security, Trust, and Privacy for Software Applications (STPSA)*, IEEE, 2010.

[22] C. Rubio-Medrano, G.-J. Ahn, and K. Sohr, "Verifying access control properties with design by contract: Framework and lessons learned," in *Computer Software and Applications Conference (COMPSAC), 2013 IEEE 37th Annual*, pp. 21–26, July 2013.

[23] B. J. Berger, C. Maeder, R. Wete Nguempnang, K. Sohr, and C. Rubio-Medrano, "Towards effective verification of multi-model access control properties," in *Proc. of the 24th ACM Symposium on Access Control Models and Technologies*, SACMAT '19, (New York, NY, USA), pp. 149–160, ACM, 2019.

[24] S. Arzt, *Static Data Flow Analysis for Android Applications*. PhD thesis, Technische Universität, Darmstadt, 2017.

[25] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. Le Traon, D. Octeau, and P. McDaniel, "Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps," in *Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI '14, (New York, NY, USA), p. 259–269, ACM, 2014.

[26] J. Y. Halpern and V. Weissman, "Using first-order logic to reason about policies," *ACM Trans. Inf. Syst. Secur.*, vol. 11, July 2008.

[27] D. S. Rosenblum, "A practical approach to programming with assertions," *IEEE Transactions on Software Engineering*, vol. 21, no. 1, pp. 19–31, 1995.

[28] B. Meyer, "Applying "design by contract"," *Computer*, vol. 25, p. 40–51, Oct. 1992.

[29] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to attribute based access control (abac) definition and considerations," *NIST Special Publication*, vol. 800, p. 162, 2014.

[30] Y. Cheon, "Automated random testing to detect specification-code inconsistencies," in *Proceedings of the 2007 International Conference on Software Engineering Theory and Practice*, 2007.

[31] C. E. Rubio-Medrano and Y. Cheon, "Access control contracts for java program modules," in *International Workshop on Security, Trust, and Privacy for Software Applications (STPSA)*, IEEE, 2010.

[32] C. E. Rubio-Medrano, L. Claramunt, J. Bael, and G.-J. Ahn, "SpaceMediator-App." `https://github.com/sefcom/SpaceProtector-GameEngine`, 2021. [Online; accessed June-19-2021].