King's Research Portal

DOI:

[10.1109/MIS.2016.79](https://doi.org/10.1109/MIS.2016.79)

Document Version

Publisher's PDF, also known as Version of record

[Link to publication record in King's Research Portal](#)

Citation for published version (APA):

Such, J. M., Criado, N., Vercouter, L., & Rehak, M. (2016). Intelligent Cybersecurity Agents. *Intelligent Systems, IEEE*, 31(5), 3-7. <https://doi.org/10.1109/MIS.2016.79>

Citing this paper

Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

General rights

Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Research Portal

Take down policy

If you believe that this document breaches copyright please contact librarypure@kcl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Intelligent Cybersecurity Agents

Jose M. Such, *Lancaster University*

Natalia Criado, *King's College London*

Laurent Vercouter, *INSA Rouen*

Martin Rehak, *Cisco Systems and CTU in Prague*

Cybersecurity is of capital importance to the development of a sustainable, resilient, and prosperous cyber world. This includes protecting crucial assets ranging from critical infrastructures¹ to individuals' personal information,² and it spans domains like cloud computing, cyber-physical systems, social

computing, e-commerce, and other emerging computing paradigms, such as the Internet of Things and software-defined networks. For instance, the first manifestations of the Internet of Things are rapidly emerging in supply chains, logistics, transportation, and home automation, and their distributed nature and inherently bounded connectivity and computational resources will have profound implications on their security models.

In parallel with the emergence of new computing paradigms, cybersecurity has undergone a major disruptive transformation in the past few years. Attackers now regularly target companies, governments, and individuals with varying degrees of sophistication and have devised very professional approaches to monetizing their exploits, ranging from political and industrial espionage to highly efficient networks of criminals using compromised resources and

Joint Special Issue with *IEEE Internet Computing*

This issue is part of a joint special issue with *IEEE Internet Computing*. The theme of the September/October 2016 issue of *IEEE Internet Computing* is "Cyber-Physical Security and Privacy." As Alvaro Cardenas and Bruno Crispo note in their guest editors' introduction for *IC*,¹

Cyber-physical systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world. These systems are usually composed of a set of networked agents, including sensors, actuators, control processing units, and communication devices. The widespread growth of wireless embedded sensors and actuators is creating several new applications—in areas such as medical devices, automotive, and smart infrastructure—and increasing the role that the information infrastructures play in existing control systems—such as in the process control industry or the power grid.

Many CPS applications are safety-critical: their failure can cause irreparable harm to the physical system under control and to the people who depend on it. In particular, the protection of our critical infrastructures that rely on CPS (such as electric power transmission and distribution; industrial control systems; oil and natural gas systems; water and waste-water treatment plants; healthcare devices; and transportation networks) play a fundamental and large-scale role in our society. Their disruption can have a significant impact to individuals—and nations—at large.

Yet security tools designed for traditional information systems generally aren't a good fit for CPS systems. To prevent and mitigate the effect of attacks on CPS, we must go beyond general information technology security solutions to address the unique challenges and opportunities that CPS provide.

IC's special issue investigates these challenges in four articles:

- "Rethinking the Honeypot for Cyber-Physical Systems" by Samuel Litchfield and colleagues;
- "Micro Synchrophasor-Based Intrusion Detection in Automated Distribution Systems: Toward Critical Infrastructure Security" by Mahdi Jamei and colleagues;
- "Next-Generation Access Control for Distributed Control Systems" by Jun Ho Huh and colleagues; and
- "Argus: An Orthogonal Defense Framework to Protect Public Infrastructure against Cyber-Physical Attacks" by Sridhar Adepudi and colleagues.

This is an exciting opportunity to consider research on cybersecurity for intelligent systems and agents from more than one angle, and we hope that you enjoy the results of this collaboration.

Reference

1. A. Cardenas and B. Crispo, "Cyber-Physical Security and Privacy," *IEEE Internet Computing*, vol. 20, no. 5, 2016, pp. 6–8.

information to launch denial-of-service attacks, perform credit card fraud, or engage in illicit money transfers. Of particular concern are the highly sophisticated and targeted attacks arising from insider and advanced persistent threats as well as social engineering attacks such as spear phishing.

We need approaches that are intelligent and self-adaptable to deal with the complexities of effective cybersecurity. This is where research from the agent community can make a real difference. Applications of agent techniques and approaches throughout the cybersecurity industry are growing very quickly, motivated by advances in attack techniques. Agent techniques are not, however, capable of providing a drop-in replacement for current cybersecurity methods; they need to be carefully crafted to work with existing systems. Also,

the security of a security mechanism itself is an important issue to study. Not only do such mechanisms need to be secure on their own, but collaboration protocols and any information transfers need to be secure as well, on top of respecting the privacy of individual users.

We can offer several examples of agent technologies and how they can be useful for (or are already being applied to) the cybersecurity domain; we highlight the related articles appearing in this special issue where appropriate.

Norms

Cybersecurity shouldn't only be addressed from a technical viewpoint—we also need to look at it from a social viewpoint as well. In this sense, cybersecurity is about regulating the actions of the different stakeholders interacting within a sociotechnical

system,³ as these actions can have an enormous impact on the whole system's security. Research on normative multiagent systems,⁴ which combine models for normative systems with models for multiagent systems, offers an ideal paradigm for addressing sociotechnical challenges in cyber-physical systems. For example, normative multiagent systems have been applied to model the social dimension of cyber-physical systems³ and to represent and reason about both top-down explicit and bottom-up implicit information-sharing norms.^{5,6}

In this issue, we have a further example of the application of normative multiagent systems to model, represent, and reason about information-sharing norms in sociotechnical systems. In particular, "Revani: Revising and Verifying Normative Specifications for Privacy" presents a formal representa-

**IEEE Computer Society
Publications Office**

10662 Los Vaqueros Circle, PO Box 3014
Los Alamitos, CA 90720-1314

Lead Editor
Bonnie Wylie
b.wylie@computer.org

Editorial Management
Jenny Stout

Publications Coordinator
isystems@computer.org

Director, Products & Services
Evan Butterfield

Senior Manager, Editorial Services
Robin Baldwin

Digital Library Marketing Manager
Georgann Carter

Senior Business Development Manager
Sandra Brown

Senior Advertising Coordinator
Marian Anderson
manderson@computer.org

Submissions: For detailed instructions and formatting, see the author guidelines at www.computer.org/intelligent/author.htm or log onto *IEEE Intelligent Systems'* author center at Manuscript Central (www.computer.org/mc/intelligent/author.htm). Visit www.computer.org/intelligent for editorial guidelines.

Editorial: Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion in *IEEE Intelligent Systems* does not necessarily constitute endorsement by the IEEE or the IEEE Computer Society. All submissions are subject to editing for style, clarity, and length.

tion of norms as well as model-checking techniques to validate and modify these norms in accordance with a given set of requirements.

Trust and Reputation

Trust and reputation are utterly essential for both human and software entities to select the most suitable interaction partners, especially when previously unknown parties interact through the Internet. For instance, if a buyer agent enters an e-marketplace for the first time, she'll need to choose among all the available seller agents, so each seller agent's reputation plays a crucial role in the buyer's choice. Thankfully, the agent community has developed a vast number of trust and reputation models⁷ that aim to precisely reason about agent trustworthiness and reputation. Examples of the application of trust and reputation in cybersecurity include distributed intrusion detection systems, where trust has been used as the foundation for enabling collaboration between individual intrusion detection sensors.⁸

In this special issue, the article entitled "Using Behavioral Similarity for Botnet Command-and-Control Discovery" augments a generic threat propagation model with novel social similarity metrics grounded in multi-agent social reputation models to identify actors, their collaboration patterns, and their operational assets (such as command-and-control servers).

Security Games

Security games are a subset usually consisting of a Stackelberg model in which a defender allocates security resources to targets while an attacker tries to attack unprotected resources after observing the defender's strategy.⁹ Security games have been mostly applied to protect physical assets from malicious adversaries by determining patrolling schedules. These schedules have been

used with excellent results in many real-world traditional security scenarios, from antiterrorist checkpoints to wildlife protection. Recent research in this area focuses on developing learning mechanisms for modeling attacker and defender behaviors¹⁰ and representing the coordination between teams of defenders or attackers.¹¹ In addition, other similar games have been proposed to represent specific features of the cybersecurity domain in which a system ad-

Trust and reputation are utterly essential for both human and software entities to select the most suitable interaction partners, especially when previously unknown parties interact through the Internet.

ministrator wants to reduce the risk or exposure to cyberattacks.¹²

In this issue, "Case Studies of Network Defense with Attack Graph Games" explores the application of game theory to network security. In particular, the authors propose the use of attack graphs and games to improve network security decisions such as the location of honeypots within a computer network.

Agent-Based Modeling and Simulation

Agent-based modeling and simulation (ABMS) is an approach to modeling

THE AUTHORS

Jose M. Such is a lecturer at Lancaster University. His research interests include multiagent systems, cybersecurity, and privacy. Such received a PhD in computer science from the Technical University of Valencia. Contact him at j.such@lancaster.ac.uk.

Natalia Criado is a lecturer at King's College London. Her research interests include multiagent systems, normative systems, and their application to cybersecurity. Criado received a PhD in computer science from the Technical University of Valencia. Contact her at natalia.criado@kcl.ac.uk.

Laurent Vercouter is a full professor in computer science at INSA Rouen. His research interests include multiagent systems, trust management, and adaptive systems. Vercouter received a PhD in computer science from MINES Saint-Etienne. Contact him at [laurent.vercouter@insa-rouen.fr](mailto:vercouter@insa-rouen.fr).

Martin Rehak is a principal engineer at Cisco and lecturer at CTU in Prague. His research interests include network security, anomaly detection, and multiagent systems. Rehak received a PhD in artificial intelligence from the Czech Technical University in Prague. Contact him at marrehak@cisco.com.

the dynamics of complex systems with emergent behaviors (human or otherwise).¹³ Agents have individual behaviors that might be simple rules or more sophisticated behaviors based on desires and intentions; they interact with and influence other agents, who also have their own behaviors. This approach, therefore, models systems from the “ground up,” so that patterns, structures, and behaviors aren't explicitly programmed or “hard-coded” but emerge from agent interactions. In addition to emerging properties due to agent interactions, one of the key advantages of ABMS with respect to other approaches to modeling and simulation is the heterogeneity of system elements, as individual agents can be endowed with different behaviors. An example of emerging applications of ABMS to cybersecurity includes modeling and accounting for user circumvention of security.¹⁴

Automated Negotiation

In automated negotiation,¹⁵ a negotiation mechanism is composed of a negotiation protocol, which is a means of standardizing the communication between participants in the negotiation process by defining how actors can interact with each other; and strategies that agents can play over the course of a negotiation protocol. Agents can negotiate directly with each other, with a human, or via a mediator.¹⁶ An example of automated negotiation is to protect co-owned data in social media. Take a simple but illustrative scenario: Alice and Bob are in a photo together, and Alice shares it on Facebook with her friends. What if Bob's privacy preferences about photos conflict with Alice's, such as if Bob doesn't want to share photos with some of Alice's friends? In this scenario, being able to negotiate an optimal sharing decision for a co-owned data item is crucial to

respect all users' privacy preferences. Automated negotiation has already been applied to this problem, with software agents working on behalf of users¹⁷ or a mediator¹⁸ helping to successfully negotiate and recommend an optimal sharing decision.

Self-Organization and Self-Adaptation

Other key characteristics that agent technologies can contribute to cybersecurity are self-organization and self-adaptation.¹⁹ Just to name one emerging domain in which self-organization and self-adaptation play a very important role, the field of moving-target defenses²⁰ is becoming a new way to overcome the limitations of traditional cybersecurity approaches, which are very often criticized on the grounds that they present a static target for attackers. In the moving-target defense field, some aspect of a machine or a network of machines dynamically changes as a function of time, with the idea of making a target harder to compromise.

Human-Agent Collectives

Finally, there's much ongoing research focusing on the interplay between agent technologies and humans. In particular, the idea is how agents and

humans can be part of a team and collaborate to achieve particular goals, an area that's being coined as human-agent collectives (HACs).²¹ We're beginning to see some of the potential applications of HACs to cybersecurity, such as joint sense-making and decision-making activities undertaken by security analysts and software agents in cyber operations.²² A key challenge for HACs, which becomes of outmost importance when it comes to cybersecurity, is how to ensure a positive sense of control from the point of view of the humans within HACs. That is, questions like how we humans would feel about collaborating with computational elements that can have as much control over the environment as us need to be answered.²¹ ■

References

1. S.M. Rinaldi, “Modeling and Simulating Critical Infrastructures and Their Interdependencies,” *Proc. 37th Annual Hawaii Int'l Conf. System Sciences*, 2004, pp. 1–8.
2. J.M. Such, A. Espinosa, and A. Garcia-Fornes, “A Survey of Privacy in Multi-Agent Systems,” *Knowledge Eng. Rev.*, vol. 29, no. 3, 2014, pp. 314–344.
3. M.P. Singh, “Norms as a Basis for Governing Sociotechnical Systems,” *ACM*

- Trans. Intelligent Systems and Technology*, vol. 5, no. 1, 2013, p. 21.
4. N. Criado, A. Estefania, and V. Botti, "Open Issues for Normative Multi-Agent Systems," *AI Comm.*, vol. 24, no. 3, 2011, pp. 233–264.
 5. Y. Krupa and L. Vercouter, "Handling Privacy as Contextual Integrity in Decentralized Virtual Communities: The PrivaCIAS Framework," *Web Intelligence and Agent Systems*, vol. 10, no. 1, 2012, pp. 105–116.
 6. N. Criado and J.M. Such, "Implicit Contextual Integrity in Online Social Networks," *Information Sciences*, vol. 325, 2015, pp. 48–69.
 7. J. Sabater and C. Sierra, "Review on Computational Trust and Reputation Models," *Artificial Intelligence Rev.*, vol. 24, no. 1, 2005, pp. 33–60.
 8. K. Bartos and M. Rehak, "Trust-based Solution for Robust Self-Configuration of Distributed Intrusion Detection Systems," *Proc. European Conf. Artificial Intelligence*, 2012, pp. 121–126.
 9. P. Paruchuri et al., "Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games," *Proc. 7th Int'l Joint Conf. Autonomous Agents and Multiagent Systems*, 2008, pp. 895–902.
 10. A. Sinha, D. Kar, and M. Tambe, "Learning Adversary Behavior in Security Games: A PAC Model Perspective," *Proc. 15th Int'l Conf. Autonomous Agents and Multiagent Systems*, 2016, pp. 214–222.
 11. Q. Guo et al., "Coalitional Security Games," *Proc. 15th Int'l Conf. Autonomous Agents and Multiagent Systems*, 2016, pp. 159–167.
 12. M. Chapman et al., "Playing Hide-and-Seek: An Abstract Game for Cyber Security," *Proc. 1st Int'l Workshop Agents and Cybersecurity*, 2014, p. 3.
 13. C.M. Macal and M.J. North, "Tutorial on Agent-Based Modelling and Simulation," *J. Simulation*, vol. 4, no. 3, 2010, pp. 151–162.
 14. V. Kothari et al., "Agent-based Modeling of User Circumvention of Security," *Proc. 1st Int'l Workshop Agents and Cybersecurity*, 2014, p. 5.
 15. N.R. Jennings et al., "Automated Negotiation: Prospects, Methods and Challenges," *Group Decision and Negotiation*, vol. 10, no. 2, 2001, pp. 199–215.
 16. M. Chalamish and S. Kraus, "AutoMed: An Automated Mediator for Multi-Issue Bilateral Negotiations," *J. Autonomous Agents and Multiagent Systems*, vol. 24, no. 3, 2012, pp. 536–564.
 17. J.M. Such and M. Rovatsos, "Privacy Policy Negotiation in Social Media," *ACM Trans. Autonomous and Adaptive Systems*, vol. 11, no. 1, 2016, p. 4.
 18. J.M. Such and N. Criado, "Resolving Multi-Party Privacy Conflicts in Social Media," *IEEE Trans. Knowledge and Data Eng.*, vol. 28, no. 7, 2016, pp. 1851–1863.
 19. M. Luck et al., "Agent Technology: Computing as Interaction (A Roadmap for Agent-Based Computing)," *AgentLink III*, 2005.
 20. M. Carvalho and R. Ford, "Moving-Target Defenses for Computer Networks," *IEEE Security & Privacy*, vol. 12, no. 2, 2014, pp. 73–76.
 21. N.R. Jennings et al., "Human-Agent Collectives," *Comm. ACM*, vol. 57, no. 12, 2014, pp. 80–88.
 22. L. Bunch et al., "Human-Agent Teamwork in Cyber Operations: Supporting Co-Evolution of Tasks and Artifacts with Luna," *Multiagent System Technologies*, Springer, 2012, pp. 53–67.

IEEE Internet Computing

For some insight into the Internet and cyber-physical security and privacy, view our companion issue, *IEEE Internet Computing*, vol. 20, no. 5, 2016.

www.computer.org/csdl/mags/ic/2016/05/index.html