cybersecurity is of capital importance to the development of a sustainable, resilient, and prosperous cyber world. This includes protecting crucial assets ranging from critical infrastructures\(^1\) 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,

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 Synchronphasor-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 Adepu 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
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 models 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.

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 multiagent social reputation models 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.

In this 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 multiagent social reputation models 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.

In this 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 multiagent social reputation models 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.

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. 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 behaviors and representing the coordination between teams of defenders or attackers. In addition, other similar games have been proposed to represent specific features of the cybersecurity domain in which a system administrator wants to reduce the risk or exposure to cyberattacks.

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 dynamics of complex systems with emergent behaviors (human or otherwise). 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.

Automated Negotiation

In automated negotiation, 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. 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 users or a mediator 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. Just to name one emerging domain in which self-organization and self-adaptation play a very important role, the field of moving-target defenses 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 been coined as human-agent collectives (HACs). 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. A key challenge for HACs, which becomes of utmost 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 we need to be answered.

References


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