Why all the fuss about process control system (PCS) security these days? Control systems, PCSs, industrial control systems, distributed control systems, and other similarly named systems control the processes that manage the components of our critical infrastructures, such as the electric power grid, factories and refineries, oil and gas pipelines, and water infrastructures. Operated and maintained by process control engineers, these traditionally dedicated, stand-alone control systems might only be able to be modernized or replaced every 10 years. The people using these systems, however, want to enjoy increased functionality that recent applications, email, and Web browsing offer—things they can easily get by connecting directly to the Internet. How can these critical real-time control systems continue to work uninterrupted when introduced to the wild and lawless world of the Internet? How are these legacy systems going to keep pace with the rapidly changing environment of modern information technology security? Can the IT security industry evolve its products to be effective on these real-time systems, where the emphasis is often on resiliency and availability first and confidentiality second?

In this special issue, our first article, “Security for Process Control Systems: An Overview,” by Markus Brändle and Martin Naedele of ABB Corporate Research, sets the stage by introducing problems facing control system security today, describing current industry security practices and discussing challenges that remain. (ABB is one of the top international PCS vendors.) Problems include assessing and understanding the risks, integrating enterprise system technology and thinking with control system operations, and the need to develop and enforce a security policy. The authors explain why security isn’t like safety and how control systems differ from the information technology environment of the office. The control system community relies on standards being developed by consensus through several industry groups and associations. The article briefly discusses standards being developed by the ISA SP99 standards committee and touches on the controversial topic of certification.

In “Vulnerability Assessment for Critical Infrastructure Control Systems,” Ray Parks of Sandia National Laboratories and Edmond Rogers of Ameren Services give practical advice on how to perform a security assessment based on the fairly recent North American Electric Reliability Corporation’s (NERC’s) Critical Infrastructure
Protection standards. The authors detail a critical infrastructure protection cybervulnerability assessment process developed from years of experience with the control system community. The development of standards, recommended practices, and regulations is only as good as companies’ ability to measure and document how they’re doing in respect to those standards. Wouldn’t it be nice to have security metrics that would immediately tell you whether you’re secure enough? Through work by groups like NERC, the US National Institute of Standards (NIST), and these authors, progress is being made on defining and measuring security in these environments.

In our final article, Alysson Neves Bessani, Paulo Sousa, Miguel Correia, Nuno Ferreira Neves, and Paulo Veríssimo at the University of Lisbon look to the future by proposing a secure architecture for the next generation of control systems. “The Crucial Way of Critical Infrastructure Protection” describes a sophisticated approach to security using smart devices such as the Crucial Information Switch.

These articles describe only a few of the efforts now under way to improve PCS security. Awareness and education during the past few years has led to an eagerness in the PCS arena to focus on protecting these critical infrastructures from threats of a cyber nature. At the same time, concerns about disruptions to these systems, whether caused by natural disasters or humans, have become acute. We thank the authors of all the articles submitted for their hard work and the external reviewers for their efforts in helping us select and review these articles. Information on other research in the PCS security area can be found at www.energetics.com/csroadmap/.

Ron Trellue is a consultant to the Institute for Information Infrastructure Protection (I3P), where he has been supporting its PCS security projects since August 2006. Prior to his retirement in 2006, he was the senior manager of the Information Assurance and Survivability Group and deputy director of the Information Systems Analysis Center at Sandia National Laboratories. Trellue has an MS in computer science and a BS in physics from New Mexico State University. Contact him at trellue@swcp.com.

Charles C. Palmer is CTO of security and privacy at IBM Research and the chair and director of research for the Institute for Information Infrastructure Protection (www.thei3p.org). His technical interests vary widely, including cybersecurity, security engineering and usable security, and privacy. Palmer has a PhD in computer science from Polytechnic University, New York. He is an ACM Distinguished Engineer and a member of the IEEE. Contact him at ccpalmer@dartmouth.edu.

CALL FOR PAPERS
Securing the Domain Name System
(for the September/October 2009 issue)

Deadline for submissions: 15 January 2009

Guest editors: Daniel Massey (Colorado State University) and Dorothy Denning (Naval Postgraduate School)

Submit a manuscript:
www.computer.org/portal/pages/security/author.xml

The Domain Name System (DNS) is a critical part of the Internet infrastructure and virtually every Internet application depends on some form of DNS data. Security wasn’t a major goal of the original DNS design and basic security issues are well known. Today, both the attacks and defenses are becoming increasingly sophisticated. DNS servers have been used in reflective flood attacks against other services. Motivated by both the importance of DNS and the recent enhancements, this upcoming issue of IEEE Security & Privacy looks at the challenges in securing the DNS.

We seek feature articles with an in-depth coverage of topics relating to all aspects of DNS security. Among potential topics are:

- analysis of DNS vulnerabilities,
- techniques of mitigating the impact of denial of service attacks on the DNS,
- deployment experience with DNS Security,
- techniques for managing DNSSEC public keys and signatures,
- providing DNSSEC benefits to end system resolvers,
- proposals for learning DNSSEC public keys, and
- legal and privacy issues in DNS data

Submissions will be subject to peer-review resulting in refereed scientific papers. Articles should be understandable to a broad audience of people interested in security and privacy and be less than 6,000 words. The writing should be down-to-earth, practical, and original. Authors should not assume that the audience will have specialized experience in a particular subfield. All accepted articles will be professionally copyedited according to the IEEE Computer Society style guide.