

# The Science of Security

**S**cience's core goal is to develop fundamental laws that let us make accurate predictions. In computer security, the only prediction we can usually make confidently is that a system will eventually fail when faced with sufficiently motivated attackers. Computer security is



DAVID EVANS  
*University  
of Virginia*

SAL STOLFO  
*Columbia  
University*

too entwined with human behavior and engineered systems to have universal laws at the physics level. However, the need—and opportunity—exists to develop foundational science to guide system design and understand the safety, security, and robustness of the complex systems on which we depend. A fundamental part of this goal is measuring system security in a meaningful way. Suitable metrics would let designers evaluate two alternative designs and determine which is more secure for a given deployment. Designers would also be able to reason about the minimum capabilities and effort an attacker needs to violate the security properties.

This special issue presents three articles illustrating and reflecting on aspects of foundational science for computer security. A big challenge is considering a creative adversary—systems typically break when adversaries find ways to violate a system designer's assumptions. Reasoning about security requires going beyond typical functional correctness reasoning by carefully considering all the

assumptions necessary to map the real implementation and deployment to a formal reasoning model.

This special issue grew out of the November 2008 Science of Security workshop in Berkeley, California, cosponsored by the US National Science Foundation, Intelligence Advanced Research Projects Activity, and National Security Agency. This meeting brought together leading researchers in computer security and other fields such as economics, biology, and control theory to examine the state of security research science and identify important challenges in designing, implementing, and reasoning about secure systems. The call for papers for this special issue yielded 31 abstract submissions spanning a wide range of areas, from which we selected the three articles for publication after a rigorous review.

The first two articles illustrate the power of formal techniques to enable precise reasoning about system security. In "Security Modeling and Analysis," Jason Bau and John C. Mitchell describe a method for evaluating a system's securi-

ty by developing both system and adversary models and using them to determine whether the system satisfies security properties. They illustrate their approach with examples from network, hardware, and Web security, showing in each case how formal modeling helps illuminate unexpected security vulnerabilities. In "On Adversary Models and Compositional Security," Anupam Datta and his colleagues focus on reasoning about security properties of systems built from components. Even when isolated components satisfy the desired security property, establishing composed-system properties requires specialized reasoning.

Finally, "Provable Security in the Real World," by Jean Paul Degabriele, Kenneth G. Paterson,

and Gaven J. Watson, reminds us of what can go wrong when systems that have been proven secure in theory are implemented and deployed in real environments. The authors provide insights on the disconnect between science and engineering. Even though the science of security can formalize systems' and adversaries' properties, creating practical implementations faithful to those formalisms remains an engineering challenge.

This issue also features an On the Horizon department entry, "Measuring Security," which outlines a research agenda for security metrics. A concerted research program in this area has a significant chance of advancing the state of the art and moving security research toward a scientific discipline that will ultimately make the systems and networks we depend on measurably safer and more secure.

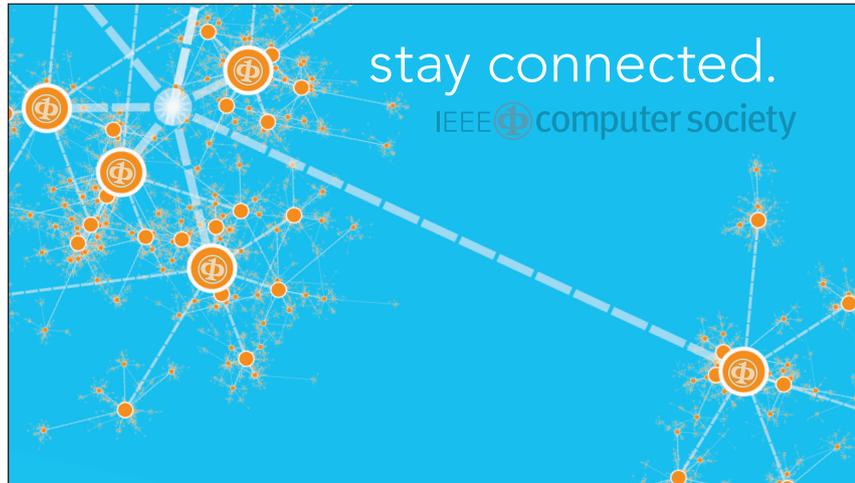
**W**e're a long way from establishing a science of security comparable to the traditional physical sciences, and even from knowing whether such a goal is even achievable. Nevertheless, the articles in this special issue hint at the possibility and promise of foundational approaches to security. □

*David Evans is an associate professor of computer science at the University of Virginia. Contact him via [www.cs.virginia.edu/evans](http://www.cs.virginia.edu/evans).*

*Sal Stolfo is professor of computer science at Columbia University. Contact him at [sal@cs.columbia.edu](mailto:sal@cs.columbia.edu).*

**Interested in writing a letter to the editor?**

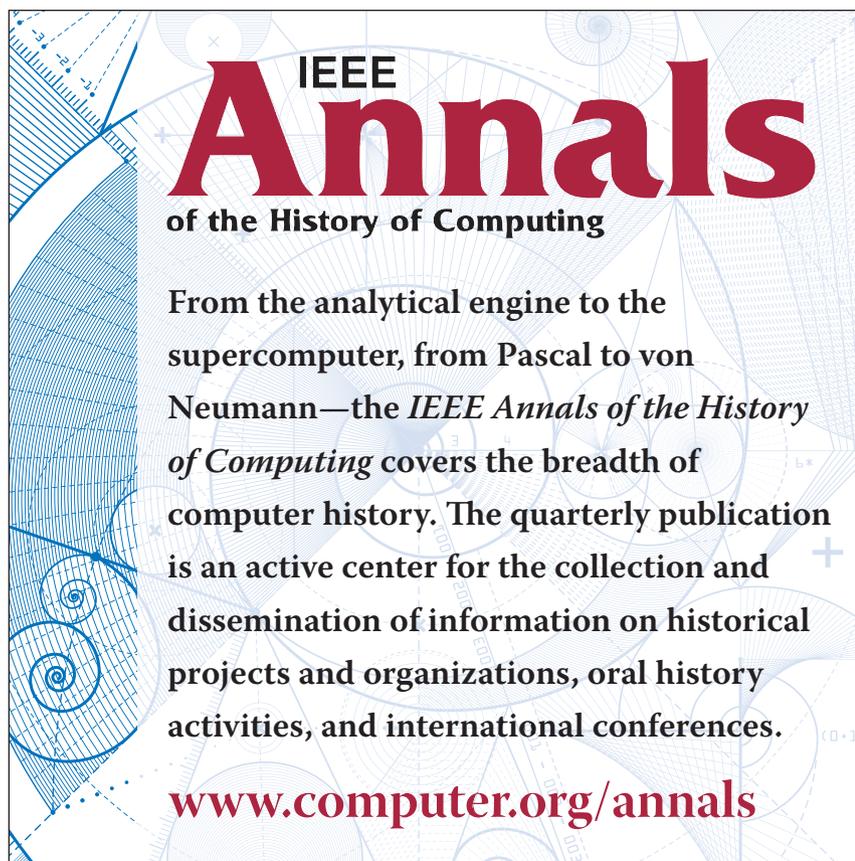
Please contact lead editor Kathy Clark-Fisher ([kclark-fisher@computer.org](mailto:kclark-fisher@computer.org)). Letters will be edited for content.



stay connected.  
IEEE  computer society

Keep up with the latest IEEE Computer Society publications and activities wherever you are.

	@ComputerSociety   @ComputingNow
	facebook.com/IEEEComputerSociety   facebook.com/ComputingNow
	IEEE Computer Society   Computing Now



IEEE  
**Annals**  
of the History of Computing

From the analytical engine to the supercomputer, from Pascal to von Neumann—the *IEEE Annals of the History of Computing* covers the breadth of computer history. The quarterly publication is an active center for the collection and dissemination of information on historical projects and organizations, oral history activities, and international conferences.

[www.computer.org/annals](http://www.computer.org/annals)