New Frontiers: Assessing and Managing Security Risks

Rolf Oppliger, eSECURITY Technologies
Günter Pernul, University of Regensburg
Sokratis Katsikas, Norwegian University of Science and Technology

Like the Wild West, cyberspace respects few laws and resists order. As essential, life-sustaining systems increasingly connect in this space, how will we go about identifying, assessing, anticipating, and managing risk?
Recently, it was argued that quantitative risk analysis— as required for risk assessment in risk management— works better in theory than in practice, and that some alternative approaches are needed. This challenge was the inspiration for this special issue of Computer. In our call for papers, we asked for new approaches or work that would point to appropriate directions for further research. Unfortunately, we did not receive many submissions from the open call, thus we sought and invited submissions from professionals working in the field. This yielded an interesting set of articles.

Preparing this special issue allowed us to have many interesting and stimulating discussions about risk management in general, as well as the intrinsic value of risk assessment. Surprisingly, most of our colleagues agreed with our starting hypothesis— currently deployed approaches for risk assessment do not work in practice and are difficult or impossible to apply in the field. There are a number of reasons for this, as discussed in an article in *IEEE Security & Privacy*. In short, the use of probability theory and statistics in a constantly changing field like cybersecurity is pointless.

To illustrate, we compare the value of statistics in assessing risk for physical versus cybercrime. In physical crime prevention, statistics about burglaries and murders in a given region are used to define crime rates and the likelihood that someone in a particular region will be victimized. The use of statistics here makes sense and can influence people’s behavior in that region—they might behave more vigilantly in a city with a high crime rate than they do in a city with a low crime rate. Now consider the same situation in the digital world. Statistics offer less utility because although we can use them to predict with near certainty that an e-commerce site will be attacked when a business logic flaw is exploited, we cannot say when. And it is not clear how the website owner’s behavior might change with this information. If he knows about a bug in a software module he is using, what would he or could he do differently? If the answer is “nothing, just wait for the vendor patch,” then the behavior is essentially to add a statement to the site’s policy on proper patch management. The statistical prediction does not meaningfully change behavior, which means that the statistics are essentially useless.

Taking the argument a step further—this is a discussion brought to us by cybersecurity pioneer Marcus J. Ranum—security risk assessment tries to predict the future based on past outcomes, whereas these outcomes and the lessons learned from them should be used to plan for the future in some meaningful way, without predictions and projections. Rather than trying to guess probabilities and likelihoods that refer to moving targets, we refine architectures based on lessons learned, and design better products and services that are inherently more secure and resilient.

Another point of view we encountered in our discussions was that risk assessment is so inherently flawed that it is not even scientifically worth arguing about. Although this is an understandable position, we do not agree with it. If we as a research community recognize that an approach is flawed, then we must determine the reasons why. Otherwise, bad actors and snake oil salespersons might take advantage of our ignorance.

Instead, we believe that security risk assessment—and, more generally, security risk management—can be studied in a scientific, educated, and enlightened way. We can explore its value both in theory and in practice, and apply it in use cases that make sense from our own experience. If it helps us make more informed (security) decisions in the future, then it is useful.

**IN THIS ISSUE**

In “Information Security Risk Assessment: A Method Comparison,” Gaute Wangen compares three widely used information security risk-assessment methods, namely, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), ISO/IEC 27005:2011, and a Norwegian method known as NSMROS. The author argues that the choice of one method over another influences the resulting assessment process tremendously. This article provides a nice introduction into the information security risk-assessment field and puts the available methods into perspective.

In “Determining and Sharing Risk Data in Distributed Interdependent Systems,” Pete Burnap, Yulia Cherdantseva, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart address the problem of how to best model complex systems that are supposed to be independent (though in reality they are not), as well as how to then aggregate the respective risk data. Having this kind of holistic view is key for risk assessment, particularly because current systems tend to be increasingly complex and interdependent. What is required to successfully handle such systems from a risk-assessment perspective is presently not well understood.
Finally, in “An Enhanced Risk-Assessment Methodology for Smart Grids,” Judith E.Y. Rossebø, Reinder Wolthuis, Frank Fransen, Gunnar Björkman, and Nuno Medeiros present a risk-management methodology designed for the smart grid that has a much wider applicability and that can motivate further research in this area. By establishing a set of requirements for comparing existing risk-assessment methods for the energy sector, the authors were able to evaluate candidate assessment methods and propose a four-step risk-assessment approach combining aspects of the three highest-scoring methods. This exploration of practical risk assessment led them to identify the need for a fourth method—SEGRID Risk Management Methodology (SRMM)—that could provide a risk-management framework.

These articles provide a useful overview of this topic and point out the research questions worth studying. We hope readers will enjoy these articles and take the challenge to move toward solutions that work both in theory and in practice.

REFERENCE

ABOUT THE AUTHORS

ROLF OPPLIGER is the founder and owner of eSECURITY Technologies and an associate professor at the University of Zurich. His research interests include information security management, cryptography, network security, and privacy. Oppliger received a PhD in computer science from the University of Berne. He is a Security and Privacy area editor for Computer. Contact him at rolf.oppliger@esecurity.ch.

GÜNTER PERNUL is a chaired professor of Information Systems at the University of Regensburg. His research interests include information security, identity and access management, security information and event management, and all aspects of data-centric applications. Pernul received a doctorate degree in information systems from the University of Vienna. He is an IEEE Society Affiliate, and a member of ACM, the German Informatics Society (Gesellschaft für Informatik), and the Austrian Computer Society (OCG). Contact him at guenther.pernul@wiiwi.uni-regensburg.de.

SOKRATIS KATSIKAS is a professor at the Center for Cyber and Information Security at the Norwegian University of Science and Technology, and a professor in the Department of Digital Systems at the University of Piraeus. His research interests include information and communication systems security, critical infrastructure security and resilience, privacy, and related policy matters. Katsikas received a PhD in computer engineering and informatics from the University of Patras. He is a member of the Greek Computer Society and of the Technical Chamber of Greece. Contact him at sokratis.katsikas@ntnu.no.