

# Barriers to achieving a science of cybersecurity |

Tom Longstaff

Several recent reports, such as the JASON “Science of cyber-security” report [1], point to examples and approaches for achieving success in applying science to cybersecurity. Audiences everywhere enthusiastically agree and thrash themselves for bypassing science all along, bemoaning the fact that we could be “so much further along” if we only did science. Of course, after the presentation is over, everyone goes back to the methods that have been used throughout our generation to create prototypes and tools with no regard for the scientific principles involved. Why?

**D**uring the winter of 2009, an informal group of three cybersecurity researchers—Roy Maxion from Carnegie Mellon University, Tom Longstaff from Johns Hopkins Applied Physics Laboratory, and John McHugh from the University of North Carolina—pondered this question based on

their collective experience. The results of their discussion generated a presentation at the 2010 Annual Computer Security Applications Conference and a National Science Foundation (NSF) Washington Area Trustworthy Computing Hour (WATCH) lecture on March 15, 2012. (A transcript of the lecture can be

found here, [http://www.nsf.gov/events/event\\_summ.jsp?cntn\\_id=123376&org=NSF](http://www.nsf.gov/events/event_summ.jsp?cntn_id=123376&org=NSF).)

At the NSF WATCH lecture, Tom Longstaff discussed some barriers to achieving a science of cybersecurity within the cybersecurity culture—barriers that seem to prevent well-meaning researchers from taking a more scientific approach to cybersecurity projects. Three of these barriers are described below.

## 1 Research begins after a conference is announced.

The informal group recognized that the publication cycle for cybersecurity papers is very short in comparison to other scientific fields, such as physics, chemistry, or psychology. The group noted that in other fields research is completed far in advance of a call for papers. In cybersecurity, however, common practice is to begin the research after a particular conference or venue is identified, often within six months of the submission deadline.

## 2 Program committees lack scientists.

The members of the informal group had been on many program committees before. They recognized that such committees were often made up of nonscientists who did not recognize or value the material in a scientific cybersecurity paper. Thus, papers accepted by these committees often did not include a methodology section, nor were authors encouraged to provide enough information to make their results repeatable or reproducible.

## 3 Publications favor articles about novelties in the field.

Finally, cybersecurity publications typically prefer articles or papers that indicate entirely new directions in cybersecurity, rather than incremental approaches that better describe the causal relationships found in cybersecurity. Being aware of this preference, authors do not spend time executing careful scientific experiments that lead to incremental approaches, but instead speculate or quickly produce a novel prototype.

While there are many incentives that could be added to address these three barriers, several were called out specifically in the WATCH lecture as likely to have

a good long-term impact on the field of cybersecurity. They are to:

- ▶ Encourage the publication of longer-duration research in cybersecurity through preferential acceptance of such research in conferences and journals,
- ▶ Leverage the knowledge of traditional physical scientists in structuring scientific publications by encouraging coauthorship and collaboration with cybersecurity researchers,
- ▶ Train computer science students to use the scientific method through the development of new courses in experimental research and publication,
- ▶ Sponsor conferences and journals that promote the scientific method as a main acceptance criterion,
- ▶ Require authors of papers to use scientific rigor in their construction for sponsored conferences and journals,
- ▶ Create a publicly available body of knowledge consisting of a scientific publication in cybersecurity, and
- ▶ Create an explicit separation between scientific contributions and technological contributions (and reward scientific contributions).

Cybersecurity culture is rooted in performing rapid prototyping and programming ad hoc solutions to engineering problems. Changing this culture and overcoming the barriers described above will be difficult, but the benefits of encouraging science in cybersecurity will be well worth the effort. 📌

## About the author

**Tom Longstaff** is the technical director for the System Behavior Office within the NSA Research Directorate. He has spent the last 25 years leading research in Internet security, incident detection and response, and cyber resilience.

## Reference

[1] JASON Program Office. "Science of cyber-security." 2010. McLean (VA): The Mitre Corporation. Report No.: JSR-10-102. Available at: <http://www.fas.org/irp/agency/dod/jason/cyber.pdf>