IEEE Symposium on Privacy and Security

Poster: "Assumption Busters" – A Public-Private Discussion on Critical Cyber Security Strategies

Brad Martin ODNI/NSA

During 2011, the U.S. Federal Cyber Research Community conducted a series of four workshops designed to examine key assumptions that underlie current security architectures in cyberspace. Described as "Assumption Busters" meetings, these sessions were designed to create an open forum for select participants from academia, industry, and government to discuss the strengths and weaknesses of different aspects of cyberspace security, as well as discuss the development of novel solutions that are based on a fundamentally different understanding of the problem. These sessions also created a stronger basis for moving U.S. cyberspace security forward on better-founded or well-founded assumptions.

Assumption Busters meetings were sponsored by different Federal Agencies, who also contributed to the tailoring of discussions around the specific themes. During 2011, Assumption Busters workshops were held to discuss the following assumptions (as well as the sponsoring agency):

--Defense in depth is a smart investment (Office of the Director of National Intelligence)
--Trust anchors are invulnerable (NSA)
--Abnormal behavior finds malicious actors (Treasury)
--Current implementation of cloud computing indicate a new approach to security (NIST)

The meetings were announced in the Federal Register, and non-U.S. government participants were required to submit a short paper describing qualifications, subject matter expertise, novel approaches, or other relevance to the discussion. Government participants were chosen by virtue of the same criteria or by roles within the sponsoring agency.

Participants were led through a day-long session involving short presentations and facilitated discussions. Attention was paid to ideas that support the assumption, ideas that challenge the assumption, and areas for further research and exploration. The Assumption Buster Workshop concept recognizes the importance of a multidisciplinary approach to thinking about cyber security, including the development of wholly new paradigms and novel solutions to improving it. Similarly, the concept allows for the prospect of cyber security solutions to emerge in the creative space across and between government, industry, and academia, beyond those that will emerge in the individual sectors.

Even in light of the diverse range of topics considered, a number of themes emerged throughout the four Assumption Buster workshops that merit additional attention:

--the need for more rigorous definitions: terms like cyber security, information security, network security, and others lack sufficient definition across government, academia, and industry, as are concepts like reliability, resiliency, robustness, survivability, and even security

--more diverse thinking about adversarial behavior: our adversaries in cyberspace are diverse and creative, ranging from highly capable individuals to advanced persistent threats. We need better thinking about their motives and methods to anticipate and counter them. What are the behavioral, economic, and game theoretic aspects of understanding and predicting their behavior?

--the need for new analytic approaches to understanding the threat: at the most basic level, we need improved classification and modeling of factors that relate to malicious behavior – and potentially other problems – in cyberspace. Our lack of understanding of "normal" and "abnormal" behavior (including the ability to discriminate between benign, malicious, and meaningless anomalies in cyberspace), the big data challenges and the extreme temporal challenges of threat identification and response demand a new analytic construct, including methods and tools and an ability to leverage machine and human response in the appropriate context. This analytic construct should also include approaches taken in other disciplines, including astronomy, behavioral sciences, biomedical informatics, epidemiological investigation, financial risk management, and others where relevant. The large data presence may actually be an advantage, given the ability to map historical trends and provide warning and anticipatory information.

--the importance of human factors in cyber security: human factors play an ever important role in cyber security: threats no longer target the information technology core of an enterprise, rather they target human behavior as a means of developing the threat. A wide range of capabilities designed to help humans recognize potential sources of threat, understand trust frameworks and trust signals, interact with trust anchors and deliberate action designed to mitigate or eliminate threat is needed.

--the need for an improved understanding of how to layer defense mechanisms such as security architectures and trust anchors: unlike classic defense-in-depth strategies in more traditional areas, further consideration is needed to understand the tradeoffs and consequences of such an approach in cyberspace. What is the relationship between defense mechanisms and trust frameworks? Should we consider 1000-layer mechanisms? With what consequences for trust and efficiency? What are the economics associated with these mechanisms?

Finally, the Assumption Busters workshops highlighted the importance of understanding the relevant short- and long-term research underway across government, industry, and academia in order to create synergies among them, as well as identify important nuances or gaps in research.

Additional Assumption Busters workshops are envisioned for 2012. These workshops will enable multi-disciplinary discussions on a wide array of topics that are crucial to the cyber security arena, and therefore to our political, social, and economic vitality. In the face of a rapidly changing threat, collaboration between sectors will be increasingly necessary.