Panel

Research Agenda for Data and Application Security

Organizer and Chair
X. Sean Wang
National Science Foundation & University of Vermont
Arlington, Virginia
+1-703-292-5311
xwang@nsf.gov

PANEL SUMMARY

Data and application security is traditionally viewed as a subfield of cybersecurity. The goal is still the same, namely to provide trustworthy computing infrastructure. However, in data and application security, we are dealing with the infrastructural aspects that are closer to humans, their interactions with the system, their perceptions, and their values. Data should not be treated as just bits, but as semantically rich content. Hence, securing data may be different from securing bits. Application software is much more diverse than system software, often directly responding to particular end-user needs. Hence, usability of security may be of more importance.

The above may be just a small sample of the uniqueness of data and application security. What else? What particular research agenda does this uniqueness call for? What about research methodologies?

With the above questions in mind, this panel will bring 4-5 panelists to discuss their experiences and their views of future research directions in data and application security.

Categories & Subject Descriptors:. J.0 [Computer Applications] General, E.0 [Data] General, I.m [Computing Methodologies] Miscellaneous

General Terms: Algorithms, Design, Documentation, Economics, Experimentation, Human Factors, Languages, Legal Aspects, Management, Measurement, Performance, Reliability, Security, Standardization, Theory, Verification.

Keywords: Application security, Data security, Research directions, Research methodologies.

Background Information

Critical infrastructures of modern societies rely heavily on computing; data become critical assets of governments, businesses and even individuals; applications have become more complex and closer to "common" users (a cursory look at the huge availability of "apps" on smartphones may make people concerned about the security of the users and their data). Security research has come a long way to defend users and systems, but attackers seem to have an upper hand in the race of attack and defense. A general question is: can we have a "science of security" so that a set of fundamental principles may be used to guide the design and implementation of data and application security [1]?

Recently, National Coordination Office (NCO)'s Networking and Information Technology Research and Development (NITRD) program presented new Federal cybersecurity game-change R&D themes [2]. The idea is to reverse the trend of defense lagging behind attacks, calling for methods to increase attacker cost, enable tailored security environments, and incentivize security deployment, socially responsible behavior, and deter cyber crimes. These are all very relevant to data and application security. A general question is: is there a specific research agenda suitable to advance the NITRD R&D themes?

Questions for the Panel

To start off the panel discussion, the panelists will be asked to respond to the following questions:

1. What are some general research directions in data and application security? What are the hardest problems in this area?
2. How does data and application security interface with system and network security? What are the critical issues in dealing with this interface?
3. Is there a "science of data and application security"? If yes, how is it defined?
4. How are the NITRD themes relevant to the data and application security? What specific research directions can be spurned by these themes?
5. What are the most important research questions regarding human factors and usability in data and application security?
6. How to evaluate research results in this area?

The panel is promised to be an interactive one, involving the panelists and audience.

References

[1] JASON, MITRE, "Science of Cyber-Security", Report number JSR-10-102, November 19, 2010

[2] http://cybersecurity.nitrd.gov/

CODASPY'11, February 21–23, 2011, San Antonio, Texas, USA.
ACM 978-1-4503-0465-8/11/02.