Privacy and Security in a Networked World

Steven Fraser
Independent Consultant
Research Relations & Tech Transfer
sdfraser@acm.org

Djenana Campara
CEO and Co-Founder
KDM Analytics
djenana@kdmanalytics.com

Michael C. Fanning
Principal Security Development Lead
Microsoft
Michael.Fanning@microsoft.com

Gary McGraw
CTO
Cigital
gem@cigital.com

Kevin Sullivan
Associate Professor
University of Virginia
sullivan.kevinj@gmail.com

Abstract
As news stories continue to demonstrate, ensuring adequate security and privacy in a networked "always on" world is a challenge; and while open source software can mitigate problems, it is not a panacea. This panel will bring together experts from industry and academia to debate, discuss, and offer opinions – questions might include:

- What are the "costs" of "good enough" security and privacy on developers and customers?
- What is the appropriate trade-off between the price to provide security and the cost of poor security?
- How can the consequences of poor design and implementation be managed?
- Can systems be enabled to fail "security-safe"?
- What are the trade-offs for increased adoption of privacy and security best practices?
- How can the "costs" of privacy and security – both tangible and intangible – be reduced?

Categories and Subject Descriptors
K.4.1 Public Policy Issues
K.5 Legal Aspects of Computing
K.6.5 Security and Protection

General Terms Policy, Privacy, Security.

Keywords *Privacy, security, cost, design, soft issues*

1. Steven Fraser
In Portland 2014, we return to a theme first discussed as a panel at OOPSLA 2008 in Nashville TN. At that time, we explored whether openness (many eyes) and transparency contribute to improved security and discussed the benefits of achieving privacy "and" security – rather than simply privacy "or" security. Has the state of the art changed for the better or is the combination of increasing system states and complexity leading to lose-lose trade-offs?

STEVEN FRASER is an independent consultant on innovation and technology transfer. From 2007 to 2013, Steven was the Director of the Cisco Research Center. His achievements included: increasing the visibility and leverage of Cisco-university research collaborations, fostering technology transfer from university research projects through the recruitment of PhD/Post-Docs, and accelerating internal technology transfer through the establishment of the Cisco Research Commons and the CTech Forum – a proprietary conference for Cisco Staff. Prior to joining Cisco, Steven was a Senior Staff member of Qualcomm's Learning Center in San Diego, leading software learning programs and creating the corporation's internal technical conference (the QTech Forum). Late in the last century, Steven held a variety of technology strategy roles at BNR/ Nortel including: Senior Manager (Disruptive Technology and Global External Research) and Advisor (Design Process Engineering). In 1994 he spent a year as a Visiting Scientist at the Software Engineering Institute (SEI) collaborating with the "Application of Software Models" project on the development of team-based domain analysis (software reuse) techniques. Steven is a Senior Member of the ACM and the IEEE.

2. Djenana Campara
In the context of cyber systems, both attackers and defenders favor automated code analysis tools (dynamic and/or static) for detecting vulnerabilities. However, while attackers are satisfied with an *ad-hoc*, hit-and-miss vulnerability detection strategy, such an approach is not well suited for defenders,

SPLASH '14 Companion, Oct 20-24 2014, Portland, OR, USA
ACM 978-1-4503-3208-8/14/10.
http://dx.doi.org/10.1145/2660252.2661294

who need to be meticulously systematic in understanding the risks and designing security mechanisms.

A systematic cyber defense approach must go well beyond the knowledge of vulnerabilities. It needs to include a knowledge of the system, threats and risks to the system, safeguards and their effectiveness, and knowledge of the system's security assurance goals. Only when armed with this knowledge, can defenders assess and address the security posture of the system. While it is easy to claim that a system is *not* secure when at least one potential vulnerability is detected – to support a claim that the system *is* adequately secure for its operational intent requires a convincing argument and evidence. To provide the requisite evidence, vulnerability testing must be driven by a threat model that anticipates attacks and evaluates vulnerabilities.

Unfortunately, many of today's approaches to threat risk assessment rely on informal artifacts such as documentation and personnel interviews – making for a too subjective, non-comprehensive, non-repeatable approach that is prone to inaccuracies and assumptions about the true nature of the system risks and vulnerabilities. To create a systematic, formal, comprehensive and automated security assurance approach to validate that a system meets its security objectives requires the collaboration of multiple automated solutions from different vendors. My position is that the "magic glue" is a set of standards! Let's discuss approaches and results.

DJENANA CAMPARA has over 25 years progressive experience and leadership in Software and Security Engineering. Campara is the CEO and co-founder of KDM Analytics Inc. with expertise in the areas of: formal methods; formalization and information/data modeling; system and enterprise architecture; reverse engineering (binary and source); software and system security design and assessments; security assurance; network analysis; and developing technology strategies. Campara's expertise in design process automation led to the development of an innovative and time-saving security assurance and threat risk assessment tools used in industry today. Campara serves as a board member on the Object Management Group (OMG), an international standard body and co-chairs the OMG System Assurance Task Force. She also has served on the SAS Technical Advisory Panel of National Institute for Standards and Technology (NIST) and previously served as a Board Member of the Canadian Consortium of Software Engineering Research (CSER), an industry directed research program that creates a collaborative environment for industry, researchers, and students to stay competitive in the broader IT marketplace. In December 2010 Campara co-authored the book titled *System Assurance: Beyond Detecting Vulnerabilities*, which is used as a text by Master of Software Assurance course syllabus at Carnegie Mellon University.

3. Michael C. Fanning

Security is a quality measure of software often regarded as a necessary but secondary concern relative to the matter of extending program functionality in a useful way. The non-negotiable center of secure development (including effective security response) is a willing, informed and disciplined engineering process. The necessarily inconsistent realization of this goal can be offset by security-focused evolution of operating systems, runtimes, application frameworks, development tools and mechanisms for providing information to programmers. Inevitably, other critical properties (backwards compatibility, performance, interoperability, language expressiveness and engineer productivity) limit or actively work against security as a value. The answer to the question of what we should do is simple enough, 'that depends.' In an increasingly diverse, connected and decentralized software landscape, it's hard to imagine there will be a diminishing need for discernment.

MICHAEL C. FANNING is a Principal Security Development Lead on the Trustworthy Computing team at Microsoft. The bulk of his 20+ year career has been dedicated to development tools, with a particular focus on static analysis checkers. He was an original developer on Microsoft's .NET MSIL scanner (FxCop) and was development lead for the first release of this functionality (as well as C++ static analysis) in Visual Studio. Recently, Michael has focused on producing security-focused static and dynamic verification tools for web applications. He is a frequent collaborator in the tooling space across Microsoft and is listed on many related published or pending Microsoft patents.

4. Gary McGraw

Only ten years ago, the idea of building security in was brand new. Back then, if system architects and developers thought about security at all, they usually concentrated on the liberal application of magic crypto fairy dust. We have come a long way since then. Perhaps no segment of the security industry has evolved more in the last decade than the discipline of software security. Several things happened in the early part of the decade that set in motion a major shift in the way people build software: the release of my book *Building Secure Software*, the publication of Bill Gates's *Trustworthy Computing* memo, the publication of Lipner and Howard's *Writing Secure Code*, and a wave of high-profile attacks such as Code Red and Nimda that forced Microsoft, and ultimately other large software companies, to get religion about software security. Now, ten years later, Microsoft has made great strides in software security and building security in – and they're publishing their ideas in the form of the SDL. Right about in the middle of the last ten years (five years in) we all collectively realized that the way to approach software security was to integrate security practices that I term the "Touchpoints" into the software development

lifecycle. Now, at the end of a decade of great progress in software security, we have a way of measuring software security initiatives called the BSIMM (http://bsimm.com).

As a discipline, software security has made great progress over the last decade. Of the many large-scale software security initiatives we are aware of, sixty-seven – all household names – are currently included in the BSIMM study. Those companies among the sixty-seven who graciously agreed to be identified include: Adobe, Aetna, Bank of America, Box, Capital One, Comerica Bank, EMC, Epsilon, F-Secure, Fannie Mae, Fidelity, Goldman Sachs, HSBC, Intel, Intuit, JPMorgan Chase & Co., Lender Processing Services Inc., Marks and Spencer, Mashery, McAfee, McKesson, Microsoft, NetSuite, Neustar, Nokia, Nokia Siemens Networks, PayPal, Pearson Learning Technologies, QUALCOMM, Rackspace, Salesforce, Sallie Mae, SAP, Sony Mobile, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, TomTom, Vanguard, Visa, VMware, Wells Fargo, and Zynga. The BSIMM was created by observing and analyzing real-world data from leading software security initiatives. The BSIMM can help you determine how your organization compares to other real software security initiatives and what steps can be taken to make your approach more effective. BSIMM is helping transform the field from an art into a measurable science.

GARY MCGRAW is the CTO of Cigital, Inc., a software security consulting firm with headquarters in the Washington, D.C. area and offices throughout the world. He is a globally recognized authority on software security and the author of eight bestselling books on this topic. His titles include *Software Security*, *Exploiting Software*, *Building Secure Software*, *Java Security*, *Exploiting Online Games*, and 6 other books; and he is editor of the Addison-Wesley Software Security series. McGraw has also written over 100 peer-reviewed scientific publications, authors a monthly security column for SearchSecurity and Information Security Magazine, and is frequently quoted in the press. Besides serving as a strategic counsellor for top business and IT executives, Gary is on the Advisory Boards of Dasient (acquired by Twitter), Fortify Software (acquired by HP), Raven White, Max Financial, and Wall+Main. His dual PhD is in Cognitive Science and Computer Science from Indiana University where he serves on the Dean's Advisory Council for the School of Informatics. Gary served on the IEEE Computer Society Board of Governors and produces the monthly Silver Bullet Security Podcast for IEEE Security & Privacy magazine (syndicated by SearchSecurity).

5. Kevin Sullivan

Security means sustained, justifiable confidence in one's safety from unacceptable harm or loss (physical, economic, social, environmental). Such security is an emergent and evolving property of a complex, socio-technical system within a complex and evolving socio-technical environment. While faults in software are a crucial proximate cause of many security failures (and potential causes of even more frightening future failures), the deeper causes are often rooted in larger failures at the overall systems level to manage possibilities for unacceptable loss. Traditional systems engineers have the system-wide perspectives needed to address security as an emergent property, but they all too often lack the software expertise needed to manage threats posed by software. Software engineers have traditionally acted as systems engineers for mostly-software systems, but they are often focused at the code level, and lack the broader perspective needed to deal with phenomena ranging from software to regulatory, operational, human, and social phenomena. The cyber-security research community has traditionally focused on the mathematics of information and on reactive response to specific threats and vulnerabilities, but not so much on software engineering, human, or systems-level aspects of security. No established discipline is configured to address the problem we face now, as we enter an era of organically complex cyber-physical-social systems. Moreover, the extant research and practitioner communities exhibit "architectural mismatches" that can make it hard for them to work together. If we wish to be secure, then we need to rethink and significantly restructure our approaches to systems-level engineering of the complex systems of the future.

KEVIN SULLIVAN received his Ph.D. in Computer Science from the University of Washington in Seattle, Washington in 1994. He joined the University of Virginia as Assistant Professor of Computer Science. He received an NSF Career Award in 1995, the (first) ACM Computer Science Professor of the Year Award from undergraduate students in 1998, a University Teaching Fellowship in 1999, the Harold Morton Jr. Teaching Prize in 2000, and a Virginia Engineering Foundation Endowed Faculty Fellowship in 2003. Kevin's research addresses systems-level, value-driven software and systems engineering with a focus on non-functional system properties, trade-offs, and the satisfaction of diverse stakeholder value propositions. His current research is funded by the National Science Foundation, the Systems Engineering Research Center, and a U.S. Department of Defense Science of Security Lablet. He has also served as a visiting scientist, consultant, and member of the external technical advisory group for the Carnegie Mellon Software Engineering Institute. His current service activities include serving as Steering Committee Chair of Onward!, on the steering committees of SPLASH and AOSD, and as a co-organizer of several research agenda-settings and community-building meetings in the area of national-scale health information systems. In the fall of 2014, he will teach an advanced undergraduate course on functional programming and constructive logic.