WISCS'16: The 3rd ACM Workshop on Information Sharing and Collaborative Security

Florian Kerschbaum
SAP
Karlsruhe, Germany
florian.kerschbaum@sap.com

Erik-Oliver Blass
Airbus Group Innovations
DE-81663 Munich
erik-oliver.blass@airbus.com

Tomas Sander
Hewlett Packard Labs
Princeton, NJ 08540, USA
tomas.sander@hpe.com

ABSTRACT

The objective of the 3rd ACM Workshop on Information Sharing and Collaborative Security is to advance the scientific foundations for sharing security-related data. Improving information sharing remains an important theme in the computer security community.

A number of new sharing communities have been formed. Also, so called "threat intelligence" originating from open, commercial or governmental sources has by now become an important, commonly used tool for detecting and mitigating attacks in organizations. Security vendors are offering novel technologies for sharing, managing and consuming such data. The OASIS Technical Committee for Cyber Threat Intelligence (CTI) is creating a standard for structured sharing of information. This is the largest TC within OASIS attesting to the broad interest in the topic.

As progress in real-life deployment of information sharing makes clear, the creation, analysis, sharing, and effective use of security data continues to raise intriguing technical problems. Addressing these problems will be critical for the ultimate success of sharing efforts and will benefit greatly from the diverse knowledge and techniques the scientific community brings.

The 3rd ACM Workshop on Information Sharing and Collaborative Security (WISCS'16) brings together experts and practitioners from academia, industry, and government to present innovative research, case studies, and legal and policy issues. WISCS'16 is held in Vienna, Austria on October 24, 2016 in conjunction with the 23rd ACM Conference on Computer and Communications Security (ACM CCS 2016).

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General – *Security and protection (e.g., firewalls)*; K.6.**5 [Management of Computing and Information Systems]**: Security and Protection; K.4.1 **[Computers and Society]**: Public Policy Issues – *Privacy*.

Keywords

Security, Information Sharing, Collaborative Security, Privacy.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author. Copyright is held by the owner/author(s).
CCS'16, October 24-28, 2016, Vienna, Austria
ACM 978-1-4503-4139-4/16/10.
http://dx.doi.org/10.1145/2976749.2990490

1. INTRODUCTION

Security technologists have asked for a number of years to increase sharing of security and threat related data, yet the perceived risks and implications to reputation have been a major hurdle for organizations. The last few years saw major progress in overcoming these obstacles. As a recent example from December 2015, the Cybersecurity Act in the US and the NIS (Network and Information Security) Directive in the EU now provide better legal foundations for information sharing. Highly publicized, sophisticated attacks have also driven the point home to many organizations that they need to share more effectively in order to stand a chance against their adversaries. A number of new sharing groups, e.g., by retailers or the healthcare industry, have been formed as a result. Existing sharing communities such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the IT ISAC have started to routinely use new technologies for automated sharing of security indicators and other information with and between their members. Some of the technologies this workshop aims to advance have applications beyond traditional cyber-security, e.g., for sharing information about cyber-physical systems and incidents (such as SCADA systems) or secure sharing of information on suspects (as the EU is trying to establish after the recent terror attacks).

The practical benefits of information sharing are by now undisputed. Yet, the scientific basis of information sharing is less clear. The fundamental problems of information sharing arise in a number of different scientific contexts and require an interdisciplinary approach. Some scientific fields that contribute to a science of information sharing are:

- economics of security (why share information?)
- intrusion detection (what information to share and what to do with it?)
- privacy (how can we protect intangible assets such as privacy or reputation?)

The increased adoption of information sharing also shows that important challenges remain. For example, just sharing low level indicators without any clear contextual information is increasingly viewed as offering little value. We need better ways to add context to indicators. Quality control and false positives rates are another common concern for practitioners. Another observation is that in many sharing communities sharing behavior is heavily skewed: a small number of participants contributes the vast majority of the data. This potentially limits their effectiveness.

We are hopeful that the science of information sharing as advanced in the WISCS workshop series will address these (and other) challenges, so that sharing broadly improves the level of protection from cyber intrusions.

2. TOPICS OF INTEREST

Topics of interest for the workshop include, but are not limited to

- Collaborative intrusion detection
- Machine learning on shared information
- Big data for cyber-security
- Case studies of information sharing
- Domain name and IP address blacklists
- Collaborative approaches to spear-phishing, DDoS and other attacks
- Privacy and confidentiality
- Data sanitization
- Cryptographic protocols for collaborative security
- Access control for shared information
- Scalable security analysis on shared data
- Ontologies and standards for sharing security data
- UX and behavioral aspects of collaboration
- Policy and legal issues
- Surveillance issues
- Trust models
- Attacks on information sharing
- Economics of security collaboration

3. PROGRAM FORMAT

WISCS'16 is a one-day workshop held in Vienna, Austria on October 24, 2015. It is pre-conference workshop to the 23rd ACM Conference on Computer and Communications Security (ACM CCS 2016). The workshop opens with a one hour keynote. The keynote is followed by paper presentations.

All submissions were peer-reviewed by at least 3 PC members. The workshop received 26 submissions of which we expect to accept around 9 papers as full papers. The number of submissions increased by more than 50% from WISCS'15.

4. CONCLUSION

WISCS is the first workshop devoted solely to the scientific aspects of sharing threat and security related data. The practical benefits of information sharing are undisputed, and a wide variety of national and international industry initiatives are on-going. Yet, the scientific basis of information sharing is less clear. We expect a number of new insights and impulses towards a scientific basis and new technologies for information sharing to emerge from the WISCS workshop series.

5. WORKSHOP ORGANIZERS

Dr. Florian Kerschbaum (Program Co-Chair) is chief research expert at SAP in Karlsruhe, Germany. In the academic year 2011/12 he was on leave as the deputy professor for the chair of privacy and data security at Dresden University of Technology. His research interests are applied cryptography, security and privacy in cloud computing, big data and cyber-physical systems. He is author of 100 papers and inventor of 50 patents. He was program chair of ACM SACMAT 2015, 2016 and ACM CCSW 2015 and serves as associate editor of ACM TISSEC and IEEE TDSC. He participated in several EU projects including as coordinator of SecureSCM and technical lead of PRACTICE. He holds a Ph.D. in computer science from the Karlsruhe Institute of Technology, a master's degree from Purdue University, and a bachelor's degree from Berufsakademie Mannheim.

Dr. Erik-Oliver Blass (Program Co-Chair) is a senior researcher at Airbus Group Innovations in Munich. Before joining Airbus, he held appointments as research professor at Northeastern University and as a senior researcher at EURECOM, France. His current research focus is on applied cryptography and the design of new cryptographic protocols. His work has been distinguished with best paper awards from the Network & Distributed System Security Symposium (NDSS'14), Annual Computer Security Applications Conference (ACSAC'13), and a runner-up best paper awa rd from ACM's Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'13). His research has been funded by NSF and Visa Inc. Dr. Blass holds a MS and a PhD (with highest honors) in computer science from Universität Karlsruhe in Germany. His thesis was awarded with the prize for the best thesis on security research by Germany's "data security organization (GDD)". He holds an appointment as visiting research assistant professor at Northeastern University, Boston.

Dr. Tomas Sander (Steering Committee) is a senior researcher at Hewlett-Packard Labs in Princeton, New Jersey. He is a member of the Security and Cloud Lab at HP which conducts research in security, privacy and cloud technologies. Before joining HP, he worked for STAR Lab, the research lab of InterTrust Technologies in Santa Clara, California on a broad range of topics relevant to advanced digital rights management (DRM). Tomas Sander received a doctoral degree in Mathematics from the University of Dortmund, Germany in 1996. From September 1996 to September 1999 he was a postdoctoral researcher at the International Computer Science Institute (ICSI) in Berkeley, California. His research interests include computer security, privacy and cryptography. In the last few years he has been researching and developing technology that assists implementing good privacy practices in large organizations. In addition he is conducting research on how to enable effective security information sharing. Tomas is the lead scientist for HP's Threat Central technology, a platform developed for automated and manual security information sharing.

6. ACKNOWLEDGMENTS

We would like to thank Freddy Dezeure, (CERT-EU), Richard Struse (DHS) and Moti Yung (Columbia University and Snapchat) for their work on the steering committee that was invaluable for realizing this workshop. We'd like to thank the authors for providing the workshop's program. We are grateful to the program committee for its excellent job in selecting a high-quality and diverse program. Stefan Katzenbeisser (TU Darmstadt and CASED) and Edgar Weippl (SBA Research) are the General Chairs for CCS and WISCS and have been tremendously helpful in making it all work. Mathias Payer (Purdue University) and Stefan Mangard (TU Graz,) are the CCS Workshop Co-Chairs. We'd like to thank them for their support and guidance. Finally, we'd like to thank ACM SIGSAC for sponsoring this workshop and Hewlett Packard Enterprise for providing some financial support.