Workshop on Multimedia Privacy and Security*

Roger Hallman
US Navy SPAWAR Systems Center Pacific
San Diego, California
roger.hallman@navy.mil

Kurt Rohloff
New Jersey Institute of Technology
Newark, New Jersey
rohloff@njit.edu

Victor Chang
Xian Jiaotong Liverpool University
Suzhou, China
ic.victor.chang@gmail.com

CCS CONCEPTS

• **Security and privacy** → *Information accountability and usage control*; *Software security engineering*;

KEYWORDS

Security,Privacy,Multimedia

This workshop addresses the technical challenges arising from our current interconnected society. Multitudes of devices and people can be connected to each other by intelligent algorithms, apps, social networks, and the infrastructure set by Internet of Things (IoT). As more people and their devices are connected without much restriction, the issues of security, privacy, and trust remain a challenge. Multimedia in IoT services should provide a robust and resilient security platforms and solutions against any unauthorized access. Recent literature shows increased concerns about hacking, security breaches, data manipulation, social engineering, and new attack methods. Malware can be hidden within multimedia files and visiting infected websites can trigger its download to victims machines. There are a multitude of techniques to steal personal information and other sensitive media for unauthorized dissemination; imposters/identity thefts are common in social networks. In order to demonstrate the effectiveness of resilient security and privacy solutions, methods such as new standards, advance cryptography, improved algorithms for intrusion detection, personalized privacy, and isolation of questionable or malicious files can be used independently or all together to minimize the threats.

Multimedia has expanded beyond the scope its original definition. With the rise of social media, large quantities of multimedia (e.g., pictures, videos, data, analytics and personal information) can be created in a short period of time. When all these data are stored in a cloud environment, many people can connect to these services for viewing, sharing, commenting, and storing information. IoT represents a collection of devices, platforms, and software that allow people to store and share data in the cloud and also connects different types of clouds altogether. Hence, multimedia in the IoT serves a significant purpose as many peoples updates, status, locations, and live actions can be seen, disseminated, tracked, commented on, and monitored in near real time. IoT opens up many possibilities since more people can broadcast themselves and allow their networks to view and share in their lives. There are also increased fraudulent activities, cybercrimes, unauthorized access, malicious attacks, phishing, and impersonating/stealing identities. This presents challenges for existing areas such as access control, authentication, data leakage, permission, social engineering, denial of service, and identity management for the attackers to impose identity, steal information, and manipulate data in the IoT environment. Challenges also include new problems such as large scale attacks and prevention, the strength of security protection (e.g., common encryption algorithms), hiding malware with multimedia, location-based privacy with high accuracy and anonymity, underground criminal networks, and hidden security breaches.

Our workshopl, The 1st International Workshop on Multimedia Privacy and Security (MPS), as part of CCS 2017, focuses on these concerns, specific to the IoT ecosystem. We solicited submissions on new and innovative methods, techniques, and proofsofconcepts supported by strong theory/algorithms and simulation/experiments to submit papers for this workshop. We accepted 5 submissions, and organized the workshop around talks for these publications with a keynote from Dr. Jeremy Epstein of the NSF and a panel discussion. Accepted papers include:

(1) "Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks" by Angeliki Aktypi, Jason Nurse, and Michael Goldsmith (University of Oxford, UK)
(2) "A Study on Autoencoder-based Reconstruction Method for Wi-Fi Location Data with Erasures" by Tetsushi Ohki (Shizuoka University, Japan) and Akira Otsuka (Institute of Information Technology, Japan)
(3) "Attacking Automatic Video Analysis Algorithms: A Case Study of Google Cloud Video Intelligence API" by Hossein Hosseini, Baicen Xiao, and Radha Poovendran (University of Washington, USA), Andrew Clark (Worcester Polytechnic Institute, USA)
(4) "Approximate Thumbnail Preserving Encryption" by Byron Marohn (Intel; Portland State University, USA), Charles Wright and Wu-Chi Feng (Portland State University, USA), Mike Rosulek and Rakesh B. Bobba (Oregon State University, USA)

*Co-Located Workshops Chairs Summary Abstract

CCS'17, Oct. 30–Nov. 3, 2017, Dallas, TX, USA.

ACM ISBN 978-1-4503-4946-8/17/10.
https://doi.org/10.1145/3133956.3137043

(5) "Detecting Spying and Fraud Browser Extensions" by Gaurav Varshney and Manoj Misra (Indian Institute of Technology, Roorkee, India), and Pradeep K. Atrey (State University of New York at Albany, USA)

The Keynote is entitled "An NSF View of Multimedia Privacy and Security", and the panel is entitled "Multimedia Security and Privacy with IoT and Social Networks".