

# Intel Dialogue at the Munich Security Conference: *“Emerging Cybersecurity Trends and Technology Directions” (Munich, Feb 17, 2020)*

## 1 Scouting Trends and Emerging Responses:

Co-located with the Munich Security Conference, we invite leading cybersecurity experts from academia, industry, and government in Germany to discuss emerging cybersecurity trends and responses to create awareness and guide stakeholders' priorities. The workshop will discuss high level trends and associated recommendations including policy, technology, standards, and societal impact.

## 2 Leaders from Academia, Industry, Government, and Standards

The workshop is invitation-only. Participation is limited to ten leading representatives each from academia, industry, and governments/standardization. Confirmed keynote speakers are:

1. Prof. Dr. Ahmad Sadeghi, Systems Security Lab, TU Darmstadt
2. Prof. Dr. Georg Siegl, IT Security, Fraunhofer AISEC and TU Munich
3. Dr. Udo Helmbrecht, former Executive Director of ENISA
4. Dr. Claire Vishik, Intel Fellow, Security and Privacy Policy

## 3 Discussion Themes

Our goal is to collect perspectives and foster discussion. The structure for each session is: 20min Invited keynote, 5min statement by each panel participant; 40min discussion, 10min summary/wrapup.

### 3.1 Emerging Technologies and Emerging Risks – What new security challenges will arise?

While protecting security, privacy, and safety of today's complex and heterogeneous critical infrastructures and systems is a hard challenge, emerging technologies and emerging threats create a moving target for security researchers and practitioners.

In this session, we will discuss security, privacy, and safety challenges of new technologies such as Artificial Intelligence, Autonomous Driving, Blockchain, or the Internet-of-Things and the impact of emerging risks on today's and future systems.

### 3.2 Establishing and Sustaining Trustworthiness of Complex Systems – Can we create maintain trust despite continued attacks?

Trusted computing and related areas focused on provable system integrity. The latest requirements, e.g., for cyber-physical systems, require models with integrated support for privacy, safety and security and identify and help identify use cases where these characteristics drive conflicting requirements. The first part of the discussion will focus on the concept of trustworthiness and its use in research, standardization, and industry. The second part of the discussion will explore challenges with regard to sustaining trustworthy operations, including for technologies with diverse lifecycle. We will discuss how to foster trust for the whole extended life-cycle of products. This includes design, composition, deployment, operation and sustained maintenance over long periods of time.

### 3.3 Security Ecosystem – How to organize and encourage coordinated vulnerability disclosure?

Today, improving security depends on manufacturers continuously mitigating newly identified vulnerabilities. Coordinating disclosure among bounty hunters, academia, governments and industry

remains unsolved due to the wildly diverging interests that range from creation of cyber-arms by maximum delay up to immediate publication. As input to this workshop, Intel has drafted a suggested policy to foster collaboration on vulnerability disclosure.

In this session, we will present, discuss, and solicit feedback on the proposed policy.

## 4 Organization

Registration is mandatory before Feb 10, 2020 to Paul Schelin [paul.d.schelin@intel.com](mailto:paul.d.schelin@intel.com). Also email him to offer participation in a panel.

### 4.1 Workshop Summary

We plan to publish a written summary of the findings of this workshop, without attribution. Participants will be listed in the Summary unless otherwise requested.

### 4.2 Venue and Logistics, and Registration

The workshop takes place 09:00-17.00h on Feb 17, 2020 in Fürstensalon room on the second floor of the Palais Montgelas at the Bayerischer Hof in Munich (address: Promenadeplatz 2-6, 80333 Munich). Intel will sponsor room and catering.

## 5 Agenda

Start	Session	Speaker
09:00	Registration/Coffee	
09:30	<b>Start of Main Workshop</b>	
09:30	Kickoff/Intro/Goals	Claire Vishik, Intel Fellow
09:40	Security Risks and Protection in Germany/EU	tbc
10:00	<b>Coffee</b>	
10:30	Session 1: Emerging Technologies and Risks Moderator: Astrid Elbe (Intel)	Keynote: Prof. Ahmad Sadeghi
12:00	<b>Lunch</b>	
13:15	Session 2: Designing and Sustaining Trustworthiness of Complex System Moderator: Claire Vishik (Intel)	Keynote: Prof. Georg Sigl
14:45	<b>Coffee</b>	
15:15	Session 3: Fair Play in the Security Ecosystem Moderator: Astrid Elbe (Intel)	Keynote: Dr. Claire Vishik
16:15	Summary / Next Steps / Conclusions	
17:00	<b>End of Workshop</b>	