AFCEA Europe Cryptography workshop

in partnership with secunet secusmart BlackBerry Subsidiary

13 September 2018, Pullman Brussels Centre Midi, Belgium

Framework for New Cryptographic Capabilities in Defence and Security

Dr. John Zangardi

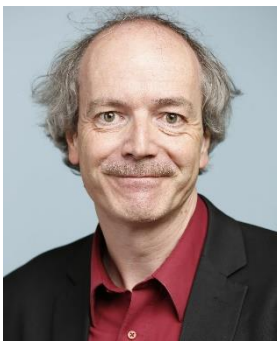
Chief Information Officer,
Department of Homeland Security, USA

Opening Keynote from 09:00 – 09:15

Biography

Perspective on Challenges for Trusted Data

Dr. John Zangardi, Chief Information Officer of the U.S. Department of Homeland Security, will discuss the landscape for trusted data at DHS, including the organization and its Components, and the complex DHS data environment. He will discuss the future for trusted data that the Department faces, like quantum computing, which presents a host of challenges in a new environment. He will then present a future data trust chain model for DHS, which is a framework that will help improve trust for the consumers and producers of the Department's rich and complex data environment. He will close with future considerations for trusted data, such as securing the supply chain through hardware, integrators, and products.



Dr. Bart Preneel

Head, Computer Security and Industrial Cryptography (COSIC) research group
KU Leuven, Belgium

Keynote Speech from 09:15 – 09:30

Biography

Actual Status on Research for Cryptography

This presentation will give an overview of the key research challenges that are being tackled in industry and academia in the area of cryptography.

Gen. José L. Triguero de la Torre

Director
NATO HQ C3 Staff

Keynote Speech from 09:30 – 09:45

Biography

NATO Perspective: Cryptographic Interoperability to Ensure Secure Communications

Challenges with the Operational Use of Encryption Today

Panel Session 1 – Technological Challenges Today: Benefits and Disadvantages of Classical Crypto Technologies

Dr. Kai Martius
Chief Technical Officer
Secunet Security Networks AG

Moderator of the Panel Session 1 from 10:15 – 11:15

Biography

Technological Challenges Today: Benefits and Disadvantages of Classical Crypto Technologies

Crypto has come a long way: secret science, cumbersome use, proved to be insecure over time, but nevertheless required in MIL / GOV since ever. Its usefulness was also proven, otherwise all electronic communication is "open", big, a worldwide open “stage” where everybody can listen to everybody. Nowadays it’s integrated everywhere, transparently... but does it help to be transparent (i.e. invisible)? For some use cases, yes (primarily confidentiality). As soon as you want to *enforce* a policy, it becomes visible (maybe, not as crypto, but as a user interaction, a management effort etc.) Technology can do a lot to hide the complex mechanisms under the hood, but there WILL be efforts. Not to mention the right / correct way of integration into a product and a solution (evaluation / certification, key management...).

BGen. Vasil Sabinski
Director EUMS/Communication and Information Systems
European External Action Service

Panelist during the Panel Session 1 from 10:15 – 11:15

Biography

Crypto usage in CSDP missions and operations

EU procedures, guidelines and used crypto in EU led military CSDP missions and operations including shortfalls and an actual use case.

Mr. Stefano Piermarocchi

NATO - Allied Command Operation
Cyberspace Cryptographic Modernization and Transformation

Panelist during the Panel Session 1 from 10:15 – 11:15

Biography

Modernizing and Transforming cryptographic capabilities: challenges and opportunities

Dr. Stavros Kousidis

Consultant
Requirements for and Development of Cryptographic Mechanisms Section
Federal Office for Security in Information Technology BSI

Panelist during the Panel Session 1 from 10:15 – 11:15

Biography

Challenges and Solutions for Modern Cryptography

Major challenges for modern cryptography are technological improvements, algorithmic innovations and implementation security. Further great demands on the security of cryptographic technologies are imposed by the lifetime of information in our Digital Age and the span of product lifecycles. The Federal Office for Information Security (BSI) meets those challenges and demands by aiming at high flexibility through hybrid, agile and parametrizable designs.

Mr. Gerard Elzinga

Head of Branch
NATO C3 Staff Spectrum and Infrastructure Branch

Panelist during the Panel Session 1 from 10:15 – 11:15

Biography

Secure Interoperability Challenge

A major concern in Operations nowadays is Interoperability especially secure Interoperability. Although this may not only be a technical issue, non-interoperable technical equipment will limit secure interoperability. This can currently be solved by deploying the same (cryptographic) equipment but this will also limit competition. Consequently work is ongoing to define interoperability specifications to which manufacturers can build. Within a NATO context, this is considered a positive development and it will also need to take into account that NATO operates with many partner nations. To allow for this, new cryptographic equipment will need to be flexible and adaptable to many situations and scenarios.

Panel Session 2 – Procedural Challenges Today: Do we have the Right Policies for Implementation?

Dr. Christoph Erdmann
Managing Director
Secusmart

Moderator of Panel Session 2 from 11:15 – 12:15

Biography

Procedural Challenges Today: Do we have the Right Policies for Implementation?

- There have been huge advances in cryptography during the past years
- Cryptography has made its way into many industrial (COTS) products and…
- Industry has established and implemented common standards
- We are already on the verge of completely new technologies such as quantum computing and blockchain becoming available in commercial products

Hence, using state-of-the-art cryptography is almost seamlessly integrated in our workflows and processes. So, everything is secure?

Well, not really…particularly in Government and other organisations with high security requirements, crypto products are not as widely deployed as they should be. Neither have large multinational organisations been able to agree on common standards and policies amongst their member states. In many cases, solutions evaluated and approved for classified are not accepted by the users.
The experts in this panel are policy makers and security experts from national and international information security authorities. We will discuss what exactly keeps us from using advances crypto products where it really matters. Do we have the right policies to keep up with the pace of today's development cycles?

Mr. Jan Fanekrog

Cyber Security Planning Engineer
NATO Communications and Information Agency

Panelist during Panel Session 2 from 11:15 – 12:15

Biography

COMSEC Community too slow?

Is the COMSEC community to slow in adapting new technologies?

Mr. Bas Dunnebier

Manager
National Communication and Security Agency, The Netherlands

Panelist during Panel Session 2 from 11:15 – 12:15

Biography

The Dutch perspective on current challenges

The threat landscape is changing at a rapid pace, heavily influencing the need for proper information security products. At the same time, societal and technological developments ask for new kinds of products and ways of looking at product development. In this short introduction we will present the Dutch vision and strategy to deal with these challenges to ensure protection of our confidential information.

Mr. Salvador Llopis

Project Officer Cyber Defence Technology
European Defence Agency

Panelist during Panel Session 2 from 11:15 – 12:15

Biography

Challenges of technological advances in cyber

In 2016, EDA participating member states established a Cyber Research and Technology Working Group within the EDA R&T framework, focused on developing and keeping a

Cyber Defence Strategic Research Agenda (SRA) up to date. The Cyber SRA calls for research in emerging technologies such as artificial intelligence, or cyber resilience to name just a few.

Mr. Nicolas Dubois

Head of Sector, Information and EUCI
European Commission, DG Human Resources and Security

Panelist during Panel Session 2 from 11:15 – 12:15

Biography

Title of presentation

Abstract

New Encryption Technologies – Are New Policies Required?

Mr. Michael Brown

Chief Technology Officer
ISARA

13:45 – 14:00

Biography

A quantum of Safety – Preparing for the Quantum World

The coming Quantum Threat brings a sea-change to the cryptography we rely upon throughout our IT systems. Secure Voice and Video conversations are one area which has grown from only specialty government security to everyday communications with services such as Signal, WhatsApp and others. We will discuss the threat to secure communications from quantum computers, review the current state of new standards and a case study on what a quantum safe secure voice system could look like.

Dr. Andreas Wespi

IBM Researcher, Specialist for Cyber Security
IBM Research Center Zurich

14:00 – 14:15

Biography

Quantum Computing: A View on Already Existing Possibilities

Building a fully functional quantum computer is one of today's most exciting scientific and engineering challenges. As the IBM Q Experience platform demonstrates, quantum computers are becoming real. Besides the quantum computing technology also the quantum algorithms are evolving. Algorithms that can be used to break current cryptographic primitives are of particular interest. Over the past few years, an increasing number of cryptographic primitives has been proposed that are safe against such quantum attacks. While the standardization of quantum-safe cryptographic primitives has been initiated, it will take years until there is an agreed standard. This is becoming a challenge for forward-looking organizations that want to be protected today against the attacks of tomorrow.

Workshop Part 1 – Myth and Reality of New Technologies; Recommendations for Further Proceedings

Dr. Christoph Erdmann
Managing Director
Secusmart

Moderator of Workshop Part 1 from 14:15 – 15:00

Biography

Myth and Reality of New Technologies; Recommendations for Further Proceedings

In this Workshop we are going to explore the current state and latest development of those new and upcoming technologies everybody is talking about. What is the reality behind blockchain, quantum, AI, etc, what state are they actually in? When are we going to see first real world applications and what are the scenarios that will be impacted most likely?

Upon discussing those questions with our experts, we will demystify these technologies to a certain extend on order to get a better view about their true capabilities. We will also ask about the missing pieces, i.e., what other rising technologies (such as 5G wireless broadband with ultra-low latency) need to be put in place to make technologies based on Quantum, Blockchain and AI become part of real solutions that arrive in relevant applications.

To get a historical perspective, we will also ask about the technologies that we hyped in the previous decade. How did we implement those previous technology superstars of the younger past like PKI, Elliptic Curve, Identity Based Encryption etc? Did they really make the impact they were promised to have?

Workshop Part 2 – Are New Policy Approaches Needed for New Technologies? Recommendations for Cultural Changes

Dr. Kai Martius
Chief Technology Officer
Secunet Security Networks AG

Moderator of Workshop Part 2 from 15:00 – 15:45

Biography

Are New Policy Approaches Needed for New Technologies? Recommendations for Cultural Changes

Policy rules Cryptography, which rules practical use cases. So, initially: Do we have problems at all? Generally, yes, I think so. Maybe not so much with crypto itself - as said in the morning: Crypto has come a long way: from secret science and cumbersome use to - at least in commercial products - seamlessly integrated in many ways. So why not "just use that"? There is obviously a gap between availability of crypto-enabled products and solutions, and making them (quickly) available to MIL / GOV end users. But who is to blame?

One part of the answer: complexity and trustworthiness. Crypto is only as good as it is integrated into products, as good as the key management and the control over keys by the end user. Commercial grade products often do not perform well in this regard (blame the vendor). Evaluation, certification is another part of the answer (who is to blame here?). And how to deal with this ever-increasing speed of innovation - Cloud, 5G, mobile devices, Quantum Computer...? It doesn't make it better.

Yet Another Crypto Challenge… Perspective Beyond Existing Networks

Mr. Terry Halvorsen
Executive Vice President
Samsung

Closing Keynote from 15:45 – 16:15

Biography

Industry Perspective on the upcoming 5G/6G Technology