SCIENCE AND TECHNOLOGY ORGANIZATION

APPLIED VEHICLE TECHNOLOGY PANEL

Science & Technology Organization
Collaboration Support Office
Applied Vehicle Technology Panel

AVT-337 Research Workshop on

Anti-tamper protective systems for NATO operations

Online

08 - 10 November 2021

This Workshop is open to NATO Nations, Australia, Finland, Japan and Sweden.

Theme and Topics

Anti-tamper technologies provide the means to protect an electronic device against compromise of sensitive and proprietary data/technology through physical attacks, as well as techniques to mitigate the damages caused by such attacks from an adversary. The AVT-337 Technical Team has arranged a Research Workshop (RWS) to gather researchers in the area of anti-tamper protective technologies to exchange ideas and explore solutions related to emerging technologies and corresponding security standards to protect sensitive military systems from being compromised. An example of an emerging technology, where it is not clear to what extent current established security standards cover the secure design, implementation and testing, is an anti-tamper system based on Physical Unclonable Functions (PUFs). Therefore, in addition to contribute to explore existing and new anti-tamper technologies, a new point of view on security tests could emerge from this RWS. This activity will also encourage collaboration within NATO to develop hardware demonstrators. This RWS furthermore aims at increasing the awareness in the NATO S&T community of the needs and necessities for incorporating anti-tamper protective solutions in military electronic equipment to prevent compromising sensitive information and reverse engineering of military technology.

Background

The mission of the Science & Technology Organization is to conduct and promote co-operative research and information exchange. STO consists of a three level organization: the Science and Technology Board, the Panels and the Technical Teams. The Applied Vehicle Technology (AVT) Panel, comprising more than 1000 scientists and engineers, strives to improve the performance, reliability, affordability, and safety of vehicles through advancement of appropriate technologies. The Panel addresses platform technologies for vehicles operating in all domains (land, sea, air, and space), for both new and ageing systems.

Registration

Online registration for this event AVT-337 is mandatory for all delegates, Programme Committee members, authors, presenters and external guests. Participation is free of charge. Due to security restrictions only duly registered and re-confirmed participants will receive invitation to virtual meeting a week prior to the event. Registration will close 2 weeks before the event. For online registration, please go to STO Events website.

AVT Executive Office, Collaboration Support Office (CSO), Paris – Points of Contact:

Mr David KLASSEN
AVT Executive Officer
Tel: +33 (0)1 55 61 22 85
David.Klassen@cso.nato.int

Ms Aurelie BETRAND
AVT Panel Assistant
Tel: +33 (0)1 55 61 22 87
Aurelie.Bertrand@cso.nato.int

AVT-337 Research Workshop on Anti-tamper protective systems for NATO operations

Programme Committee

CO-CHAIRS

Mr Vincent IMMLER (DEU)
Central Office for Information Technology in the Security Sector (ZITiS)
Email: vincent+nato@immler.us

Mr Christophe MARRON (FRA)
Thales Communications & Security
Email: christophe.marron@thalesgroup.com

Mr Tomas SOLLUND (NOR)
Norwegian Defence Research Establishment (FFI)
Email: tomas.sollund@ffi.no

MEMBERS

FRANCE
Mr Philippe BRIAND
Direction générale de l'armement - Ministère des Armées (DGA) / Information Superiority
Email : philippe-c.briand@intradef.gouv.fr

UNITED KINGDOM
Mr Peter BERRYMAN
Defence Science and Technology Laboratory (DSTL)
Email: ptberryman@dstl.gov.uk

NORWAY
Mr Lars Jørgen Johnsen AAMODT
Kongsberg Defence and Aerospace (KDA)
Email: lars.jorgen.johnsen.aamodt@kongsberg.com

Mr Hans-Are ELLINGSRUD
Kongsberg Defence and Aerospace (KDA)
Email: hans.are.ellingsrud@kongsberg.com

Mr Håvard FILTVEDT
Thales Norway
Email: havard.filtvedt@thales.no

Dr Jakob GAKKESTAD
Norwegian Defence Research Establishment (FFI)
Email: jakob.gakkestad@ffi.no

PANEL MENTOR

Dr Tom THORVALDSEN
Norwegian Defence Research Establishment (FFI)
Email: tom.thorvaldsen@ffi.no

TECHNICAL EVALUATOR

Dr Anne Marie HEGLAND
Kongsberg Defence and Aerospace (KDA)
Email: anne.m.hegland@kongsberg.com

Programme

DAY 1

Monday, 08 November 2021, 15:55 - 18:45 (CET) // 09:55-12:45 (EST)

15 :55		Opening and introduction of the research workshop AVT-337 Co-Chairs: Vincent IMMLER, Christophe MARRON, Tomas SOLLUND

Session 1 – Theory meets Practice/AT is not just Cryptography

Session Chair: Tomas SOLLUND

16:00	KN 1	**KEYONTE:** Anti Tamper Protective Systems Olivier Mangeot, Direction générale de l'armement - Ministère des Armées (DGA), France
16:30	1	Security of autonomous and unmanned devices: Cryptography and its limits Martin STRAND, Jan Henrik WIIK, Norwegian Defence Research Establishment (FFI), Norway
17:00		BREAK

Session 2 – Lessons learned in AT

Session Chair: Vincent IMMLER

17:15	2	Lessons identified from 15 years of embedding anti-tamper into defence systems Peter BERRYMAN, Defence Science and Technology Laboratory (DSTL), United Kingdom
17:45	3	Anti-tamper and cryptography in Pay-TV - lessons learned Anders PAULSHUS, Thales Norway, Norway
18:15	4	Thinking outside the tamper-box Bjørn GREVE, Federico MANCINI, and Solveig BRUVOLL, Norwegian Defence Research Establishment (FFI), Norway
18:45		END OF DAY 1

DAY 2

Tuesday, 09 November 2021, 16:00– 19:15 (CET) // 10:00– 13:15 (EST)

Session 3 – Quo Vadis Physical Unclonable Functions?

Session Chair: Christophe MARRON

16:00	5	Physically unclonable functions: Design principles, applications and outstanding challenges Basel HALAK, University of Southampton, United Kingdom
16:45	6	Towards designing machine-learning attack resistant PUFs Elena DUBROVA, Royal Institute of Technology (KTH), Sweden
17:30		BREAK

Session 4 - Tamper-Evident Physical Unclonable Functions

Session Chairs: Jakob GAKKESTAD & Håvard FILTVEDT

17:45	7	Future-proof access denial systems Vincent IMMLER, Central Office for Information Technology in the Security Sector (ZITiS), Germany
18:45	8	A novel physically unclonable function for cryptographic purposes Dan Credgington, Awerian Ltd., United Kingdom
19:15		END OF DAY 2

DAY 3

Wednesday, 10 November 2021, 16:00– 19:15 (CET) // 10:00– 13:15 (EST)

Session 5 – Hardware Security Attacks and Countermeasures

Session Chairs: Peter BERRYMAN & Philippe BRIAND

16:00	KN 2	**KEYNOTE**: Embedded security: attacks, countermeasures and testing Benedikt GIERLICHS, KU Leuven, COSIC, Belgium
17:00	9	Overview of hardware attacks on security boxes Joan MAZENC, Thales IT Security Evaluation Facility (ITSEF), Thales, France
17:30		BREAK

Session 6 - Discussion and Evaluation

Session Chair: Hans-Are ELLINGSRUD

17:45		Discussion/panel debate
18:45		Technical Evaluation Summary Anne Marie HEGLAND, Kongsberg Defence and Aerospace (KDA), Norway
19:15		END OF WORKSHOP

Science and Technology Organization in NATO

In NATO, Science & Technology (S&T) is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models:

- The Collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange.
- The In-House delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The Science and Technology Organization - STO

The mission of the NATO STO is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by:

- Conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives;
- Contributing to NATO's ability to enable and influence security - and defence-related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies;
- Supporting decision-making in the NATO Nations and NATO.

S&T organization CSO

AVT-337 Research Workshop