



Sharing and Automation for
Privacy Preserving Attack Neutralization

(H2020 833418)

D7.8 Report on Information and Presentation Materials (M24)

Published by the SAPPAN Consortium

Dissemination Level: Public



H2020-SU-ICT-2018-2020 – Cybersecurity

Document control page

Document file: D7.8 Report on Information and Presentation Materials – M24
Document version: 1.0
Document owner: Mehdi Akbari Gurabi (FIT)

Work package: WP7
Task: T7.3
Deliverable type: Report
Delivery month: M24
Document status: ☒ approved by the document owner for internal review
☒ approved for submission to the EC

Document History:

Version	Author(s)	Date	Summary of changes made
0.1	Mehdi Akbari Gurabi (FIT)	2021-04-09	Preliminary document outline
0.2	Mehdi Akbari Gurabi (FIT)	2021-04-27	Initial draft with partners' input
0.3	Mehdi Akbari Gurabi (FIT)	2021-04-29	Applying FIT internal feedback, the first complete version to collect feedback from partners
1.0	Mehdi Akbari Gurabi (FIT)	2021-04-30	Applying reviewers' feedback, ready for submission

Internal review history:

Reviewed by	Date	Summary of comments
Robert Rapp(USTUTT)	2021-04-29	check-reading content, grammar corrections, table layouting

Executive Summary

The purpose of the report on information and presentation materials is to present the project's results to all interested target groups. This is the follow-up iteration of the deliverable D7.7 which was submitted at M12. This deliverable includes presentation materials that have been created and used in the second year of the project. Also, the last iteration will be delivered at M36.

This deliverable lists all the SAPPAN presentation materials and activities in the second 12-month cycle of the project such as the presentation template, website updates and social media presence, as well as any project related motivational, promotional or technical presentations. The last part of the deliverable describes planned information and presentation materials for the next year of the SAPPAN project and beyond the project life cycle.

Table of Contents

EXECUTIVE SUMMARY	3
1 INTRODUCTION.....	5
2 CREATED INFORMATION AND PRESENTATION MATERIALS M13 - M24	5
2.1 SAPPAN PRESENTATION TEMPLATE	5
2.2 UPDATES ON PROJECT WEBSITE	6
2.3 TWITTER ACCOUNT	6
2.4 YOUTUBE CHANNEL.....	7
2.5 PROJECT OF THE WEEK ON CYBERWATCHING PROJECT HUB	7
2.6 SAPPAN ADVISORY BOARD	7
2.7 RELATED BLOG POSTS AND NEWS.....	8
2.8 ORGANIZATION OF NG-SOC 2020 WORKSHOP.....	8
3 SHORT SUMMARY OF SAPPAN PRESENTATIONS IN THE EVENTS	12
3.1 CYBERWATCHING NETWORKING EVENT	12
3.2 JOINT STANDARDISATION WORKSHOP OF DYNAMIC COUNTERING OF CYBER-ATTACKS PROJECTS	12
3.3 SWISS CYBER SECURITY DAYS.....	13
3.4 (ISC) ² CHAPTER SWITZERLAND	14
3.5 LEUVEN AI LAW AND ETHICS CONFERENCE	14
3.6 GIRLS DAY 2021	15
4 PLANNED INFORMATION AND PRESENTATION MATERIALS	17
5 CONCLUSION	19

1 Introduction

This report aims to summarize the current information and presentation materials of SAPPAN. It lists general presentations of the consortium and individual presentations of the partners in events to disseminate SAPPAN goals and results.

The information and presentation materials are and will be used to bring the project's vision, components, results, and experiences obtained throughout the project to the public in scientific and non-scientific events. These activities are focused on raising awareness, showing and explaining SAPPAN result to reach experts and other target audience, and increasing the synergy in the cybersecurity research area with other parties, especially other EU funded projects.

The rest of this document is organized as follows. Section 2 describes the general created information and presentation materials. Section 3 includes short summaries of presentations in events. Lastly, Section 4 lists the plan of information and presentation materials for the next year.

This is the second iteration of the report on information and presentation materials after D7.7. Also, the last iteration of the report will be delivered at the end of the project.

2 Created Information and Presentation Materials M13 - M24

In this section, we briefly report the information and presentation materials that are generated or updated in the second year of the project lifetime.

2.1 SAPPAN Presentation Template

To have a consistent format in our presentations, a PowerPoint template was created. This template utilized for M18 review materials for the first time. It is available internally in the online collaboration workspace of the consortium. Each SAPPAN presentations from M18 onward used and will use the mentioned template. The following figures show the presentation template title slide as well as content layout.



2.2 Updates on Project Website

During the second year of the project (M13 – M24), the project website received a visual upgrade. This upgrade presents important information more appealing and concise. Thus, new visitors are more likely to learn more about the project and already interested people are more likely to revisit the website to view the continuously updated contents. The project website is the key dissemination and communication channel. We have been continuously adding important news, which is related to the SAPPAN project on the website and has been uploading any dissemination material arising in a timely manner. These materials include the public deliverables as soon as we receive EU confirmation, the project's scientific publications, and other dissemination materials such as blog posts and presentations. Furthermore, the project website now includes a short description of all the partners, a map of the location of organizations, and a list of the advisory board members. Finally, we added social media links such that our Twitter and YouTube presences grow.

To collect the traffic and visits statistics of the project to address EU mid-term review feedback and provide the website statistics using the Matomo tracking tool is under consideration. However, there is no meaningful statistics collected to share in this report. The following figure shows the current home page of the project website at <https://sappan-project.eu/>



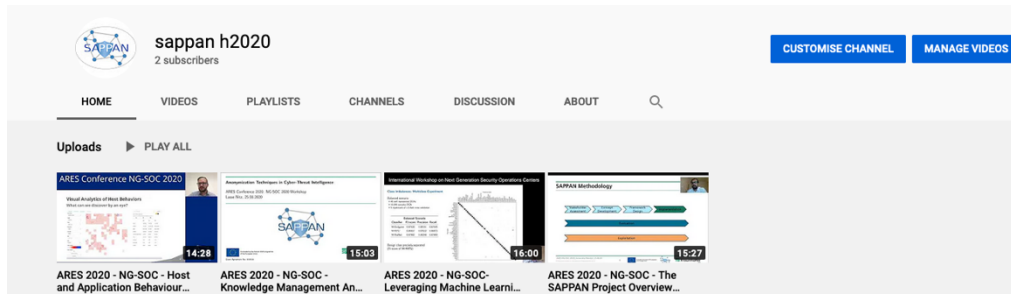
2.3 Twitter Account

We actively present in social media by our Twitter account to enable communication with other cybersecurity projects and increase the visibility of SAPPAN to the domain experts, potential stakeholders, and other target groups. We continuously report our progress, results and events in our account. So far, we have more than 125 followers, and we plan to reach more than 500 audiences on Twitter. The following figure shows the Twitter profile of the project.



2.4 YouTube Channel

SAPPAN YouTube channel has been created in January 2020. Currently, four presentation videos of the NG-SOC 2020 workshop are uploaded to the channel. We will upload at least four more videos into our channel until the end of the project. The following pictures show the current uploaded videos in the channel.



2.5 Project of the Week on Cyberwatching Project Hub

Cyberwatching.eu is the European observatory of research and innovation in the field of cybersecurity and privacy and same as SAPPAN it is funded under the EU H2020 program. Cyberwatching.eu aims to contribute to a safer digital marketplace by promoting and understanding European cutting-edge cybersecurity and privacy services that emerge from research and innovation initiatives. SAPPAN was selected by cyberwatching.eu as the project of the week (17-21 August 2020). Regarding that SAPPAN gained exposure on the Cyberwatching starting page, plus a promotional post was generated regarding SAPPAN main ideas and objectives to increase the visibility of our project. Also, this was promoted via social media channels of Cyberwatching.

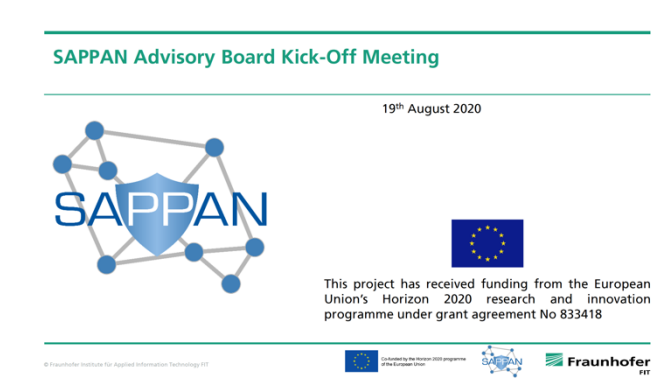


2.6 SAPPAN Advisory Board

During the second year of the project, we have appointed four expert individuals from industry, university, a federal agency, and a research institute in our Advisory Board. A list of Advisory Board members is available on the SAPPAN website.

Board Member	Affiliation
Arthur Schmidt	Federal Office for Information Security (BSI), Germany
Jörn Kohlhammer	Fraunhofer IGD, TU Darmstadt, Germany
Thorsten Holz	Ruhr-University Bochum, Germany
Yoan Miche	Nokia Bell Labs, Finland

Moreover, a kick-off Advisory board meeting was held in Aug 2020. The advisory board members provide feedback and expert advice, as well as input and guidance in the project progression and activity towards the objective. They also consult on technical work packages to meet End-User needs, and continuously inform their networks regarding the project activities and outcomes to maximize SAPPAN dissemination and exploitation effort.



2.7 Related Blog Posts and News

The following table lists the blog posts and news related to SAPPAN on our partners' websites.

Beneficiary	Type	Title	Link of SAPPAN-related blog posts and news
F-Secure	Blog post	Phishing is here to stay	https://blog.f-secure.com/phishing-is-here-to-stay/
Masaryk University	Interview	Interview with Ili Ko for International Women's day	https://www.ics.muni.cz/en/news/women-in-it-ili-ko
DreamLab	News	Dreamlab's participation at ARES: International Conference on Availability, Reliability and Security	https://dreamlab.net/en/news/article/dreamlabs-participation-at-ares-international-conference-on-availability-reliability-and-security/

2.8 Organization of NG-SOC 2020 Workshop

Together with the consortium of the EU project SOCCRATES, SAPPAN organized the NG-SOC 2020 workshop alongside with ARES 2020. The NG-SOC 2020 workshop aimed to create a forum for researchers and experts to discuss the challenges associated with SOC operations and focused on research contributions to address these challenges. Selected members of the projects' consortia presented their research activities. The workshop includes a panel session to foster discussion on the major operational challenges that enterprises and SOC operators face and provide insights into promising research-based solutions.


Agenda:

Session (Moderator)	Talks
Session 1 (<i>Ewa Piatkowska</i>)	<ul style="list-style-type: none"> • Welcome - <i>Ewa Piatkowska (AIT)</i> • The SOCCRATES Project: Overview and Objectives - <i>Frank Fransen (TNO)</i> • The SAPPAN Project: Overview and Objectives - <i>Avikarsha Mandal (Fraunhofer FIT)</i> • Keynote: Semi-Automated Cyber Threat Intelligence (ACT) - <i>Martin Eian (Mnemonic)</i>
Session 2 (<i>Tomas Jirsik</i>)	<ul style="list-style-type: none"> • Monitoring Malicious Infrastructures to Produce Threat Intelligence - <i>Piotr Kijewski (Shadowserver)</i> • Pipeline development for Automatically Generated Domain detection - <i>Irina Chiscop (TNO)</i> • Leveraging Machine Learning for DGA Detection - <i>Arthur Drichel (RWTH Aachen University)</i> • Knowledge Management and Anonymization Techniques in Cyber-Threat Intelligence - <i>Lasse Nitz and Mehdi Akbari Gurabi (Fraunhofer FIT)</i> • Reputation Management Techniques for IP addresses, domains, and mail - <i>Mischa Obrecht (DreamLab)</i>
Session 3 (<i>Avikarsha Mandal</i>)	<ul style="list-style-type: none"> • Host and Application Behaviour Modelling - <i>Tomas Jirsik (Masaryk University)</i> and <i>Sebastian Schaefer (RWTH Aachen University)</i> • L-ADS: Live Anomaly Detection System - <i>Alejandro Garcia Bedoya (ATOS)</i> • Adversarial Examples against Intrusion Detection Systems - <i>Ewa Piatkowska (AIT)</i> • Fast and Scalable Cybersecurity Data Processing - <i>Gabriela Aumayr (HPE)</i>
Session 4 (<i>Irina Chiscop</i>)	<ul style="list-style-type: none"> • Attack Analysis with Attack Defence Graphs - <i>Erik Ringdahl (Foreseeti)</i> • Attack Graph-based Courses of Action for Defense - <i>Wojciech Widel (KTH)</i> • Visual Analytics for Cyber Security Data - <i>Christoph Müller and Franziska Becker (University of Stuttgart)</i> • Process Launch Distribution Model - <i>Dmitry Komashinskiy, David Karpuk, Samuel Marshal and Alexey Kirichenko (Fsecure)</i>
Panel Session	<p>Discussion on Future Challenges for SOC Speakers: <i>Pavel Kacha (CESNET)</i>, <i>Sarka Pekarova (DreamLab)</i> and <i>Paul Smith (AIT)</i></p> <p>Panel chair: <i>Tomas Jirsik (Masaryk University)</i></p>
Wrap up - <i>Ewa Piatkowska (AIT)</i>	

For this workshop, video presentations had been produced and streamed during the live event. SAPPAN organized 2 sessions, chaired and participated in a panel discussion, presented the SAPPAN introduction, and produced 8 technical presentations of the results in 7 timeslots. NG-SOC workshops were attended by approximately 35 participants excluding SAPPAN and SOCCRATES members.

For those authors who gave their consent, the videos had been made publicly accessible on the Vimeo video platform by the ARES team. These videos are available for one year after the event and are linked on the ARES website (<https://2020.ares-conference.eu/conference-2020/accepted-workshop-papers/index.html>). Additionally, 4 of these presentations have been uploaded to the SAPPAN YouTube channel and are publicly accessible. The following figures show some sample screenshots of the public SAPPAN presentation videos.

The SAPPAN Project: Overview and Objectives



ARES NG-SOC 2020 Workshop
Avikarsha Mandal (Fraunhofer FIT, Germany)
25th August 2020


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

ARES Conference
International Conference on Availability, Reliability and Security

ARES NG-SOC 2020 | Avikarsha Mandal | 25.08.20

General Aim

- General Aim:
 - develop a platform for sharing and automation to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and machine learning.
 - develop ML and visualization methods and a platform for sharing data, threat intelligence and ML models to enable privacy preserving and efficient attack detection and response



ARES NG-SOC 2020 | Avikarsha Mandal | 25.08.20

International Workshop on Next Generation Security Operations Centers



Leveraging Machine Learning for DGA Detection

Arthur Driemel
RWTH Aachen University
Research Group IT-Security

International Workshop on Next Generation Security Operations Centers

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418.

SAPPAN SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION

Cofunded by the Horizon 2020 programme of the European Union

IT-SEC RWTH AACHEN UNIVERSITY

International Workshop on Next Generation Security Operations Centers

Explainability I

Analyzing falsely attributed domains from multiclass experiment

- Based towards well-represented classes (→ Ramnit)
- Bedep → Ramnit: no "z" or [0-9]
- Feodo → Blackhole: no domains of length 18
- Odeoor → Vidro: no ".cc" or ".tv" TLD

DGA	# Training Samples	DGA Regex
bedep	5966	[a-z0-9]{12,18}.com
decrypt	552	[a-z]{8,20}.com
gostym	291	[a-z]{5,12}.com
heperkot	142	[a-z]{8,24}.com
ramnit	8000	[a-z]{8,19}(.bdclick.com)w
feodo	153	([a-z]{16})[a-z]{18}.w
blackhole	585	[a-z]{16}.w
odeoor	8000	[a-z]{7,12}(.cc com dyndns.org net w)
vidro	8000	[a-z]{7,12}(.com dyndns.org net)

Simple features

- Included Characters
- Domain length
- TLD (suffix)

ARES NG-SOC 2020 | Avikarsha Mandal | 25.08.20

ARES Conference NG-SOC 2020

Host and Application Behaviour Modelling

NG-SOC 2020
August 25th, 2020

Sebastian Schaefer (RWTH Aachen University)
Tomas Jirsik (Masaryk University)

Cofunded by the Horizon 2020 programme of the European Union

PP

ARES Conference NG-SOC 2020

Future Works Aka Challenging Issues

How to get more detailed profile?

- Endpoint data
- Logs
- OSINT

How to correlate data sources?

What is the added value of the enriched data?

- Except for the improved context

What typical behaviour can we identify across different organizations/datasets/networks?

- What do they represent/mean?

ARES NG-SOC 2020 | Avikarsha Mandal | 25.08.20

ARES Conference NG-SOC 2020

Application Profiling

Approaches

Statistical or rule-based

- manual or automated generation of rules reflecting the application behaviour
- e.g. set or sequence of queried domains, used protocols or ports


Deep learning

- domains and/or flows as input
- multi-class or binary classifiers

Process mining

- automatic extraction of repeating processes in network events
- outputs petri nets that can be used as reference for classification or for extraction of rules

Architecture	F1-Score	Precision	Recall
CNN	88.54	92.39	84.07
LSTM	98.15	98.39	93.47
LSTM-Attention	97.80	98.01	93.82
Transformer	97.18	98.49	92.29




Knowledge Management and Anonymization Techniques in Cyber-Threat Intelligence

ARES Conference 2020: NG-SOC 2020 Workshop


Mehdi Akbari Gurabi, Lasse Nitz

Fraunhofer Institute for Applied Information Technology FIT

25.08.2020

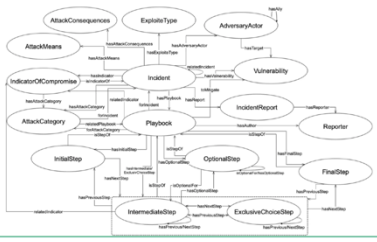


Co-funded by the Horizon 2020 programme of the European Union



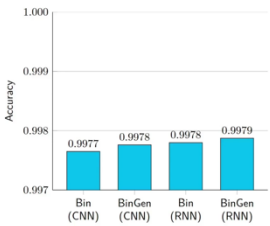
Grant Agreement No. 833418

Preliminary class relationship diagram



Knowledge Management in Cyber-Threat Intelligence | Mehdi Akbari Gurabi | 25.08.2020 | 9
© Fraunhofer Institute for Applied Information Technology FIT

Binary DGA Classifier: Test Set Evaluation - Only Domains



Anonymization Techniques in Cyber-Threat Intelligence | Lasse Nitz | 25.08.2020 | 11
© Fraunhofer Institute for Applied Information Technology FIT

For the second year, the NG-SOC workshop will be co-organized with SOCCRATES in conjunction with ARES 2021 conference in August 2021. In contrast to the previous year, we have a Call for Papers for the workshop and request contributions for peer review. The call for peer-reviewed publications is a step towards establishing the workshop as a respected forum for research contributions on SOC operations and will help to gain visibility within the community. The following figure shows the first page of CfP for the workshop. The workshop details and current CfP are available at: <https://www.ares-conference.eu/workshops-eu-symposium/ng-soc-2021/>



Call for Papers

3rd International Workshop on Next Generation Security Operations Centers (NG-SOC 2021)

to be held in conjunction with the 16th International Conference on Availability, Reliability and Security (ARES 2021 – <http://www.ares-conference.eu>)

August 17 – August 20, 2021
All-digital Conference

Workshop Description

Organisations in Europe face the difficult task of detecting and responding to increasing numbers of cyber-attacks and threats, given that their own ICT infrastructures are complex, constantly changing (e.g. by the introduction of new technologies) and there is a shortage of qualified cybersecurity experts. There is a great need to drastically reduce the time to detect and respond to cyber-attacks. A key means for organizations to stay ahead of the threat is through the establishment of a Security Operations Center (SOC). The primary purpose of a SOC is to monitor, assess and defend the information assets of an enterprise, both on a technical and organizational level.

The aim of this workshop is to create a forum for researchers and practitioners to discuss the challenges associated with SOC operations and focus on research contributions that can be applied to address these challenges. Through cooperation among H2020 European projects, the workshop intends to provide a more comprehensive overview of the promising research-based solutions that enable timely response to emerging threats and support different aspects of the security analysis and recovery process.

The workshop is jointly organized by two H2020 projects: SOCCRATES (<https://www.soccrates.eu/>) and SAPPAN (<https://sappan-project.eu/>).

3 Short Summary of SAPPAN Presentations in the Events

3.1 Cyberwatching Networking Event

Short description of the event:

A networking event held online by Cyberwatching.eu project hub on July 9th 2020. This event includes virtual meeting and introduction of participated EU projects, discussions on the improvement of dissemination and communication activities, the introduction of Cyberwatching Project Radar, Cyberwatching marketplace, and Horizon Results Booster, and discussion on other cooperation opportunities such as a joint webinar. Seven EU projects participated in this workshop: DEFEND, FENITEC, GUARD, PAN-ACEA, PAPAYA, SAPPAN, and SealedGRID.

cyberwatching.eu
The European Union's leading project hub on cybersecurity & privacy

Summary of identified commonalities

7 projects:

Number	Project	Start	End	Radar Quadrant
148	FENITEC	01/01/2018	01/12/2020	Operational Risk
160	SealedGRID	01/01/2018	01/12/2021	Secure Systems
164	PAPAYA	01/05/2018	01/04/2021	Identity & Privacy
168	DEFEND	01/06/2018	01/05/2021	Cybersecurity Governance
185	PANACEA	01/01/2019	01/12/2021	Operational Risk
238	GUARD	01/05/2019	01/04/2022	Secure Systems
261	SAPPAN	01/05/2019	30/04/2022	Secure Systems

Open Discussion:

Dr. Avikarsha Mandal was presenting the SAPPAN at the event and participated in the open discussion to identify synergies between the projects. The workshop had 13 participants.

3.2 Joint Standardisation Workshop of Dynamic Countering of Cyber-Attacks Projects

Short description of the event:

On January 22nd 2021, a joint virtual workshop entitled Joint Standardisation Workshop of Dynamic Countering of Cyber-Attacks Projects was organised by CyberSANE H2020 project.

The workshop aimed to unite all projects funded under the *SU-ICT-01-2018 H2020* call. The objective of this event is to permit the exchange of knowledge and the elaboration of future collaborative standardisation and dissemination activities. Seven EU projects participated in this workshop: C4IIoT, CARMEL, CYBERSANE, GUARD, SAPPAN, SIMARGL, and SOCCRATES.



Presentation:

Each participating EU project had a 30 minutes time slot for an introduction:

- GUARD - A cybersecurity framework to GUArantee Reliability and trust for Digital service chains
- CyberSANE – Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures
- C4IoT - Cyber security 4.0: protecting the Industrial Internet Of Things
- SAPPAN – Sharing and Automation for Privacy Preserving Attack Neutralization
- SIMARGL - Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware
- nIoVe - A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles
- SOCCRATES – SOC & CSIRT Response to Attacks & Threats based on attack defense graphs Evaluation Systems

Dr. Benjamin Heitmann presented the SAPPAN overview and objectives in this workshop. The workshop had 30 participants.

Afterwards, potential cooperation on dissemination results of the projects into standardization bodies was discussed. It was a productive event identifying the potentials of close collaboration with these H2020 projects.

3.3 Swiss Cyber Security Days

Short description of the event:

Switzerland's leading cybersecurity event, Swiss Cyber Security Days (SCSD), brought together key decision-makers and experts on domestic and international cybersecurity for two days on Wednesday 10 and Thursday 11 March 2021. The first day focused on core issues of overall security for Switzerland, while the second explored specific and innovative preventive solutions for businesses, particularly SMEs. The program comprised more than 60 lectures, keynote speeches, panel discussions, best practice presentations and round tables. The full program can be viewed here: <https://swisscybersecuritydays.ch/agenda/>

The third edition of the SCSD closed on a highly encouraging note, having brought more than 1,800 people together live online and created thousands of interactions between experts or service providers and participants. The main elements of the program

were translated with simultaneous interpretation into French, English and/or German – a digital undertaking that was in itself a major event!

Presentation:

Given the packed schedule and since SAPPAN is still a work in progress there was no presentation held about SAPPAN as a project. However, SAPPAN was the topic of about 8 to 10 direct interactions with cybersecurity experts and policy makers from all over the world, the names of which must remain kept private.

3.4 (ISC)² Chapter Switzerland

Short description of the event:

The (ISC)² Chapter Switzerland promotes the community and networks specialists for information security who are resident or working in Switzerland or who have close ties to Switzerland. The mission is to advance information security in a local community by providing our members and other security professionals with the opportunity to share knowledge, grow professionally, educate others, and collaborate on projects.

Presentation:

Dreamlab presented SAPPAN to an audience of about 40 information security professionals and managers in an online session of the Swiss chapter of ISC2 on the 16th of March 2021. The topics were:

- General overview of the SAPPAN project and its goals
- Deep dive into DGA detection and results
- Deep dive into similarity preserving anonymization and results
- Pitch for participation in SAPPANs End User Committee



Dreamlab Technologies
SAPPAN



2021 | Bern

3.5 Leuven AI Law and Ethics Conference

Short description of the event:

Leuven AI Law and Ethics Conference (LAILEC 2021) has been held on 25-26 March 2021. Alexey Kirichenko from F-Secure was invited as a panelist to LAILEC 2021. More information regarding this event can be found via <https://www.law.ku-leuven.be/citip/en/citip-conferences/lailec/lailec-2021>

In this year's (online) edition of the conference, the focus was on how AI and (cyber)security interplay, where they go hand in hand and where they collide. The conference aimed to discuss the role of transparency, information sharing and resilience in the data and machine learning supply chains. In particular, it explored to what extent companies would be willing to devise collaborative mitigation strategies against competing interests over valuable data assets.

The conference attracted over 350 attendees.

Presentation:

In the "AI for resilience and collaborative mitigation strategies for AI-driven response to cyber threats" session (attended by around 80 persons), Alexey talked about the benefits and challenges of intelligence sharing in cybersecurity and how privacy-preserving Machine Learning could alleviate some of the concerns. The SAPPAN work on data and model sharing was used as a key example of sharing approaches in the context of dynamic attack detection and response.

The talk started with historical notes on "sharing among cyber defenders", including the issues of trust, motivation and technical means, and such challenges as sharing information about "governmental malware" and disclosing sensitive information of organizations targeted by attacks. Then the focus moved to one of the key questions in SAPPAN: since advanced attacks are often detected as anomalies via ML-based engines, how sharing can support such engines? Several forms of sharing were briefly discussed: training data, statistics, models (in particular, distributed and federated learning and ensembling approaches), sharing model predictions in the teacher-student setting. Also, options for the statistics and models sharing scope were considered, from the individual machines level to groups of machines, individual organizations, and across multiple organizations.

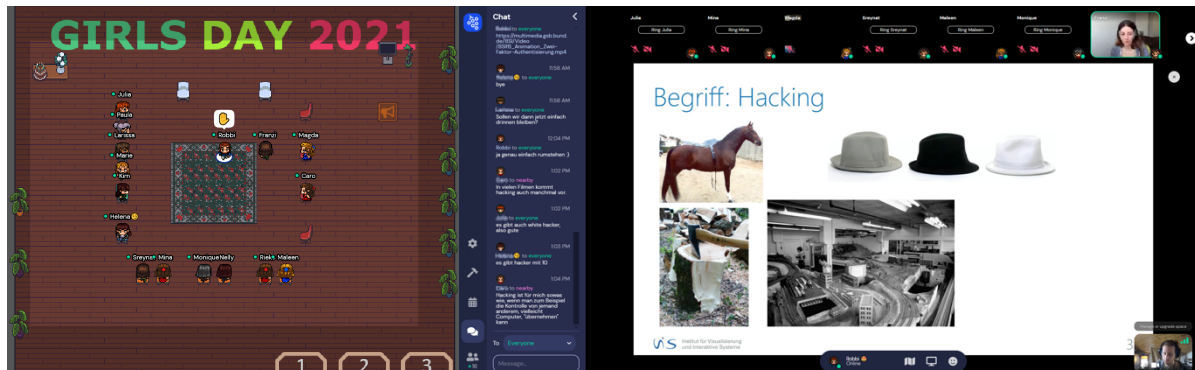
3.6 Girls Day 2021

Short description of the event:

Girls' Day 2021 took place in Germany on April 22nd 2021 and USTUTT was there with a workshop offered to encourage female students to look at information technology courses of study and professions. Franziska Becker and Robert Rapp from the SAPPAN project, therefore, wanted to convey the important content on data protection and encryption. The event "Hacked? Learn about password and secret languages!" was offered by the two. 13 schoolgirls from all over Germany took part in this online event. The online event had an interactive structure and offered the schoolgirls a varied mix of information, discussions and games. After a short introduction, the participants were allowed to take part in a small warm-up game. As an introduction to the topic, the first mini-challenge "Who Am I" was to be carried out in three small working groups. Each team was asked to compile the information they could find about Robert on the Internet. Afterwards, Robert started with the first informal part, why data is collected on the Internet in the first place and what information can be compiled from the collected data. Afterwards, the students were shown how to find hidden trackers in their smartphone apps. With the explanation of "cookies" and the "cookie notification", there was also a small insight into the German Data Protection Regulation (DSGVO). The next topic area also started with a small mini-challenge called "Password please". The

students tried to create the most secure password possible from the given one. In the resolution of the challenge, Robert showed an online tool for password verification. To wrap up the topic, the girls learned more about strong passwords, password managers, and two-factor authentication and were able to ask questions about them. After the lunch break, the session continued with a discussion session about "hacking". For the students, hacking was no longer a new term and they already knew hackers from movies or even had an idea what the goal of a hack attack is. Franziska then explained the origin of the word hacking and the various forms of hackers. To ensure that the participants are better protected against hackers of all kinds in the future, Franziska showed them a quiz that can be used to raise awareness of a widespread hacking attack called "phishing". She also presented an online tool that can be used to check files and URLs for viruses and Trojans. In the mini-challenge "A Different Kind of Secret Language", the schoolgirls were able to playfully encrypt their own text. Working in small groups, the girls created their own encryption method and used it to encrypt the message. Afterwards, the encrypted message was passed on to another group and they tried to decode it. This revealed some really clever ideas for encrypting content, and individual words were also converted back into legible text during decryption. Afterwards, the students mentioned that this challenge in particular had been a lot of fun for them.

After the practical exercise, the students were very curious about the presentation of different encryption methods. The principle of "end-to-end encryption" (E2EE) was explained in a small messenger comparison. After the content part, the students still had enough time to ask all kinds of questions. As a conclusion, the students received a two-part handout.



Verschlüsselung

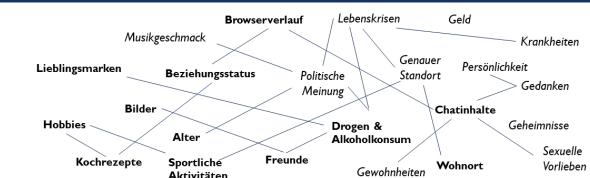
Kryptographie = Geheimschrift



UfS Institut für Medienbildung und Informationskompetenz

6

DEINE INFORMATIONEN IM INTERNET



Öffentliche Informationen

Eine Information ist harmlos, aber ist ein Netzwerk aus Informationen immer noch harmlos?

Private Informationen

Presentation:

The slides we used had only German content because we prepared the content for German schoolgirls with the age of 10 to 15 for the event. We prepared two presentations and a handout for the schoolgirls. We chose an informal way of presentation because the target group was quite young. For that reason, the full slides are not published. In the following, there are some figures from the presented slides at the workshop.

Universität Stuttgart

Hacking & Verschlüsselung

Franziska Becker

Girl's Day 2021 | 22.04.2021

VIS Institut für Visualisierung und Interaktive Systeme

DEINE DATEN IM INTERNET

DU BIST WERTVOLL, DEIN DIGITALES ICH ABER AUCH

```

graph LR
    A[Apps] --> B[Informationen]
    B --> C[Tracking]
    C --> D[Berechtigungen am Smartphone]
    D --> E[Datenschutz?]
  
```



4 Planned Information and Presentation Materials

In this section, the planned activities for the last year of the project lifetime and beyond it are summarized in a table.

Type of presentation activities	Planned Activities
Organization of a Conference or Workshop	<ul style="list-style-type: none"> International Workshop on Next Generation Security Operations Centers (NG-SOC 2021): Joint workshop with the SOCCRATES project. It will be held in conjunction with the 16th International Conference on Availability, Reliability and Security (ARES 2021 – http://www.ares-conference.eu) August 17 – August 20, 2021, University College Dublin, Dublin, Ireland, NG-SOC 2021 will include a peer review proceeding paper submission process Workshop Link: https://www.ares-conference.eu/workshops-eu-symposium/ng-soc-2021/
Participation in activities organized	<ul style="list-style-type: none"> International Workshop on Next Generation Security Operations Centers (NG-SOC 2021) (details mentioned in the above row)

jointly with other EU projects	<ul style="list-style-type: none"> • Co-organizing Cyber Security webinar series • A joint webinar with Soccrates project on DGA topic
Non-scientific and non-peer-reviewed publication (popularised publication)	<ul style="list-style-type: none"> • A series of technical blog posts based on project initiatives and results
Training	<ul style="list-style-type: none"> • Training activities as part of the dissemination plan of several academic partners of the project • Use of project knowledge and experiences in security and privacy courses and proposing bachelor and master theses related to project topics
Social Media	<ul style="list-style-type: none"> • Continuous updates on Twitter and LinkedIn • Upload more videos on YouTube Channel
Website	<ul style="list-style-type: none"> • Continuous updates on the project progress, events, and materials • Revisiting the website design to utilize remote events and restructure for blog post series
Participation to conferences and workshop	<ul style="list-style-type: none"> • Participation in more conferences and workshops is a SAPPAN dissemination KPI and has been promised and planed by most of the consortium members • Presenting the progress and results of the project, spreading the knowledge about SAPPAN, and receiving feedback supposed to be done in each event
Participation to an Event other than a Conference or a Workshop	<ul style="list-style-type: none"> • Participating in ICT exhibitions and trade fairs such as Hannover Messe • Co-organizing webinars and (virtual) visits to provide an environment for girls to engage with IT female professionals • HPE: Participating as an industry partner in a national project called 'Code-Plus' in 2021 and 2022. This project is addressed to secondary-level school girls with the aim of encouraging girls to pursue a technical higher education. • SAPPAN-related presentations in third party meetings and events
Video/Film	<ul style="list-style-type: none"> • Providing at least 4 additional videos for our YouTube Channel
Flyers	<ul style="list-style-type: none"> • General project flyers will be prepared and available for the next events such as NG-SOC 2021 workshop
Pitch Event	<ul style="list-style-type: none"> • Presenting the progress of the project and its advantages and features in the next events including workshops, conferences, and talks in exhibitions • Finding potential stakeholders for the project
Other	<ul style="list-style-type: none"> • Providing a poster of the architecture design

5 Conclusion

Provided information and presentation materials in the second year of the project are the template for SAPPAN presentations, updates on the project website and its contents, social media activities, and activation of the advisory board. Further, SAPPAN is listed in the hub of the research-based European cutting-edge cybersecurity and privacy services and selected as the project of the week in that platform. SAPPAN-related content is mentioned on partners' websites and other dissemination channels to increase the visibility of the project. SAPPAN co-organized NG-SOC workshop in conjunction with ARES 2020 with another H2020 project and will organize it for the second consecutive year.

SAPPAN objectives, initiatives, and results were presented in several networking events and conferences that are described in this report. Also, a workshop for Girls Day 2021 in Germany was held by SAPPAN members at the University of Stuttgart to motivate and encourage young females for more involvement in STEM subjects.

In the last part of the document, planned activities regarding information and presentation are listed in a table to meet the projects dissemination and communication goals.