Research Statement of Florian Skopik on

Collaborative Cyber Security and Defence

The Internet threat landscape is fundamentally changing. A major shift away from hobby hacking towards well-organized cyber crime can be observed. These attacks are typically carried out for commercial reasons in a sophisticated and targeted manner, and specifically in a way to circumvent common security measures. Additionally, networks have grown to a scale and complexity, and have reached a degree of interconnectedness, that their protection can often only be guaranteed and financed as shared efforts. Consequently, new paradigms are required for detecting contemporary attacks and mitigating their effects.

My research regarding collaborative cyber security and defence is centred on three key questions:

- *Topic-1:* How can traces of new forms of attacks, especially Advanced Persistent Threats, be effectively spotted in ICT infrastructures?
- *Topic-2:* How can actionable information be shared across organizations, even on a national level?
- *Topic-3:* How can cyber situational awareness be established and contribute to incident response on a large scale?

Topic-1: Spotting APTs and new attack vectors using anomaly detection

An advanced persistent threat (also known as APT) is a deliberately slow-moving cyberattack that is applied to quietly compromise interconnected information systems without revealing itself. APTs often use a variety of attack methods to get unauthorized system access initially and then gradually spread throughout the network. In contrast to traditional attacks, they are not used to interrupt services but primarily to steal intellectual property, sensitive internal business and legal documents and other data. If an attack on a system is successful, timely detection is of paramount importance to mitigate its impact and prohibit APTs from further spreading. However, recent security incidents, such as Operation Shady Rat, Operation Red October or the discovery of MiniDuke - just to name a few - have impressively demonstrated that current security mechanisms are mostly insufficient to prohibit targeted and customized attacks.

Research Focus. Research is centred on a novel anomaly detection approach, called AECID[1], which applies different machine learning techniques to learn a model of the system (usage) behaviour. The AECID approach digests system log data to keep track of system events, their dependencies and occurrences, and thus learns the normal system behaviour over time and points out actions that differ from the learned system model.

Research Methodology. New algorithms are designed and subsequently tested on data obtained from real or simulated attack cases to rate their feasibility. Empirical studies carried out in testbeds support the evaluation process.

Contributions. Numerous machine learning algorithms have been proposed, implemented and published – most of them also patented[2]. Compared to the state of the art, these algorithms are designed to digest log data (in contrast to network packets or numerical data), thus they are able to handle sequentially produced text lines of unknown form and structure, preferably in real-time and a single-pass manner.

Top-5 Publications.

[1] https://aecid.ait.ac.at/

[2] https://www.skopik.at/#Patents

- Wurzenberger M., Höld G., Landauer M., **Skopik F.**, Kastner W. (2020): Creating Character-based Templates for Log Data to Enable Security Event Classification. *15th ACM ASIA Conference on Computer and Communications Security (ACM Asia CCS)*, October 05-09, 2020, Taipei, Taiwan. ACM.
- Landauer M., **Skopik F.**, Wurzenberger M., Rauber A. (2020): System Log Clustering Approaches for Cyber Security Applications: A Survey. [pdf] *Elsevier Computers & Security Journal*, Volume 92. May 2020, pp. 1-17. Elsevier.
- Landauer M., Wurzenberger M., **Skopik F.**, Settanni G., Filzmoser P. (2018): Dynamic Log File Analysis: An Unsupervised Cluster Evolution Approach for Anomaly Detection. [pdf] *Elsevier Computers & Security Journal*, Volume 79. November 2018, pp. 94-116. Elsevier.
- Friedberg I., **Skopik F.**, Settanni G., Fiedler R. (2015): Combating Advanced Persistent Threats: From Network Event Correlation to Incident Detection [pdf]. *Elsevier Computers & Security Journal*, Volume 48, pp. 35-57. Elsevier.
- **Skopik F.**, Friedberg I., Fiedler R. (2014): Dealing with Advanced Persistent Threats in Smart Grid ICT Networks. *5th IEEE Innovative Smart Grid Technologies Conference*, February 19-22, 2014, Washington DC, USA. IEEE.

Topic-2: Information sharing & threat intelligence exchange

Today, many attack detection tasks are performed within individual organizations, and there is little cross-organizational information sharing. However, the timely exchange of information on new threats and vulnerabilities is a cornerstone of effective cyber defence. Especially national authorities are taking a vital role as information brokers through national cyber security centres and distribute warnings on new attack vectors and vital recommendations on how to mitigate them. information sharing is a crucial step to acquiring a thorough understanding of large-scale cyber-attack situations and is therefore seen as one of the key concepts to protect future networks. Discovering covert cyber attacks and new malware, issuing early warnings, advice about how to secure networks, and selectively distribute threat intelligence data are just some of the many use cases. Although many of these initiatives are effective to some degree, they also suffer from severe limitations. Many steps in the exchange process require extensive human involvement to manually review, vet, enrich, analyse and distribute security information. Some countries have therefore started to adopt distributed cyber security sensor networks to enable the automatic collection, analysis and preparation of security data and thus effectively overcome limiting scalability factors. The basic idea of IoC-centric cyber security sensor networks is that national authorities distribute Indicators of Compromise (IoCs) to organizations and receive sightings in return. This effectively helps them to estimate the spreading of malware, anticipate further trends of spreading and derive vital findings for decision makers.

Research Focus. My research is centred on how to make information sharing more efficient, by creating an appropriate mindset of involved stakeholders, establishing effective procedures and employing feasible technology.

Research Methodology. In this topic I apply a mix of methods, including desk research, structured interviews with experts from national authorities and CERTs, as well as empirical studies, and proof-of-concept-driven evaluations.

Contributions. A number of information sharing protocols (in accordance with the State-of-the-Art, such as STIX), collaboration models, and platforms, as well as strategies and processes to perform information exchange have been proposed. Newer work includes the design of cyber security sensors to make the creation of threat intelligence more applicable.

Top-5 Publications.

- **Skopik F.**, Filip S. (2019): A blueprint and proof-of-concept for a national cyber security sensor network. *International Journal on Cyber Situational Awareness (IJCSA)*, Vol. 4, No. 1, pp. 155-184. C-MRIC.
- **Skopik F.** (2019): National Cyber Security Sensor Networks and the Human in the Loop. [pdf] *Journal of Information Warfare*, Vol. 18, Issue 2, pp. 01-14. Peregrine.

- **Skopik F.** (2017): Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level. 416p., 1st edition, ISBN-10: 1138031828, ISBN-13: 978-1138031821, Taylor & Francis, CRC Press.
- Settanni G., **Skopik F.** et al. (2017): A collaborative cyber incident management system for European interconnected critical infrastructures. [pdf] *Elsevier Journal of Information Security and Applications (JISA)*, Volume 34 Part 2, June 2017, pp. 166-182. Elsevier.
- **Skopik F.**, Settanni G., Fiedler R. (2016): A Problem Shared is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense through Security Information Sharing. [pdf] *Elsevier Computers & Security Journal*, Volume 60. July 2016, pp. 154-176. Elsevier.

Topic-3: Cyber situational awareness, incident handling and attack attribution

National cyber security centres (NCSCs) are gaining more and more importance to ensure the security and proper operations of critical infrastructures. As a prerequisite, NCSCs need to collect, analyse, process, assess and share security-relevant information from infrastructure operators. A vital capability of mentioned NCSCs is to establish Cyber Situational Awareness (CSA) as a precondition for understanding the security situation of critical infrastructures. Knowing which products possess vulnerabilities, what services are affected, which tools and techniques are applied and what threat actors are out there is important for proper risk assessment and subsequent reduction of potential attack surfaces at national level. Moreover, the attribution of cyber attacks is often neglected. The consensus still is that little can be done to prosecute the perpetrators (and unfortunately, this might be right in many cases). What is however only of limited interest for the private industry is in the centre of interest for nation states. Investigating if an attack was carried out in the name of a nation state is a crucial task for secret services. Many methods, tools and processes exist for network- and computer forensics that allow the collection of traces and evidences. They are the basis to associate adversarial actions with threat actors. However, a serious problem which has not got the appropriate attention from research yet, are false ag campaigns, cyber attacks which apply covert tactics to deceive or misguide attribution attempts (either to hide traces or to blame others).

Research Focus. My research focuses on novel models for establishing cyber situational awareness, in particular, what information is required by national authorities to carry out their tasks and how can this information be efficiently collected. It is crucial to present relevant information and analysis findings to decision makers without influencing their decision.

Research Methodology. Most of my research involves user studies, structured interviews and applied tests with user groups in course of cyber security games. These are appropriate means to evaluate which methods, e.g. to aggregate information or visualize a cyber security situation, are received best and appropriately support security processes.

Contributions. Numerous approaches to create context-specific common operational pictures have been proposed and evaluated with Proof-of-Concept implementations. Furthermore, analytical concepts to create higher-level information from low-level data (such as log data and anomaly detection output) have been proposed.

Top-5 Publications.

- **Skopik F.**, Pahi T. (2020): Under false flag: Using technical artifacts for cyber attack attribution. [pdf] *Springer Cybersecurity Journal*, Vol.3, Article 8. Springer.
- Landauer M., **Skopik F.**, Wurzenberger M., Hotwagner W., Rauber A. (2019): A Framework for Cyber Threat Intelligence Extraction from Raw Log Data. IEEE International Conference on Big Data 2019, December 9-12, 2019, Los Angeles, CA, USA. IEEE.
- **Skopik F.**, Pahi T., Leitner M. (2018): Cyber Situational Awareness in Public-Private-Partnerships: Organisationsübergreifende Cyber-Sicherheitsvorfälle effektiv bewältigen. 347p., 1st edition, ISBN-10: 3662560836, ISBN-13: 978-3-662-56083-9, Springer Vieweg.

- Pahi T., Leitner M., **Skopik F.** (2017): Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers. *3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, February 19-21, 2017, Porto, Portugal. INSTICC
- Settanni G., **Skopik F.**, Shovgenya Y., Fiedler R.(2016): A Collaborative Analysis System for Cross-Organization Cyber Incident Handling. *2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, February 19-21, 2016, Rome, Italy. INSTICC.

Funding projects and Grants:

Please refer to my homepage to see a list of national and international projects that fund my research: https://www.skopik.at/#CurrentActivities

Future Perspective

Cyber Security is and will remain a challenging area for the next years, even decades to come. Attacker tools, techniques and procedures continue to evolve together with technological advancements. There is the strong need to integrate the often still isolated areas of intrusion detection, information sharing, and situational awareness. Questions centred on how to interpret low level operational data (such as log data or events from intrusion detection) and create higher-level information on which can be directly acted accordingly, are the main motivation of my current and future research.

/EoF.