GDPR HUD: A Better Security Policy Visualizer

Andrew Nicolalde - Supervised by: Konstantinos Markantonakis and Raja Naeem Akram
Information Security Group, Smart Card and IoT Security Centre

The Smart Card and Internet of Things Security Centre

Objectives

We want to create a visualization tool that allows us to see the real-time flow of personal and private information through a network and detect policy violations as they occur.

Any visualization we create must be:

- Simple enough to be worth using
- Powerful enough to merit using it instead of looking at raw logs
- Multi-layered, to show convey specific meanings and concepts at each level of a network (networks, subnets, hosts, ports, services)

Introduction

Visualization of information security information is a highly researched topic. Today, the set of tools available to analysts is vast and fragmented, with no common interface or visualization style having been widely adopted by the industry at large.

With public concern and awareness of the way personally identifying and private information is handled mounting, we believe it is more important now than ever to equip analysts with tools which will allow them to ensure that the organisations they serve are fully in compliance with ever stricter data protection regulations and policies including GDPR.

We will expand on the works such as those by Arendt et al. to create a visualization for real-time compliance auditing.

Materials

The following materials are required to complete the research:

- Large datasets of logs & simulated network traffic such as those listed in the viszec.
- Data visualization libraries such as:
  - edgebundleR
  - Mingle JS

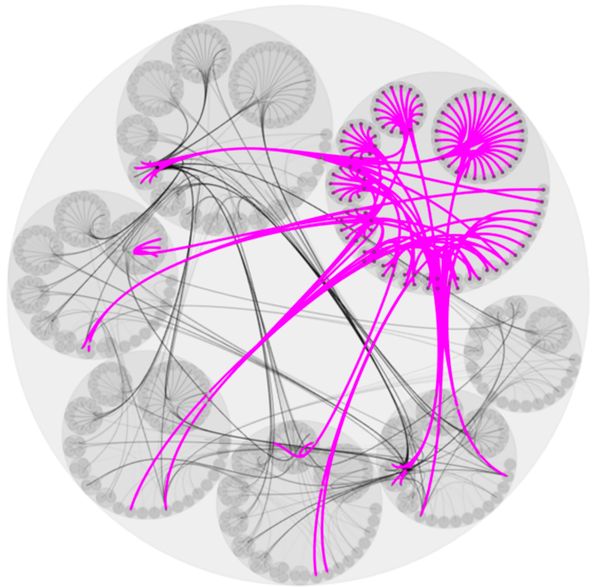

Figure 1: Possible option for showing which nodes in a network communicate with one another in a 'data-flow' view. Smallest circles represent ports, medium sized nodes represent hosts, large nodes represent subnets. Full credit to [1].

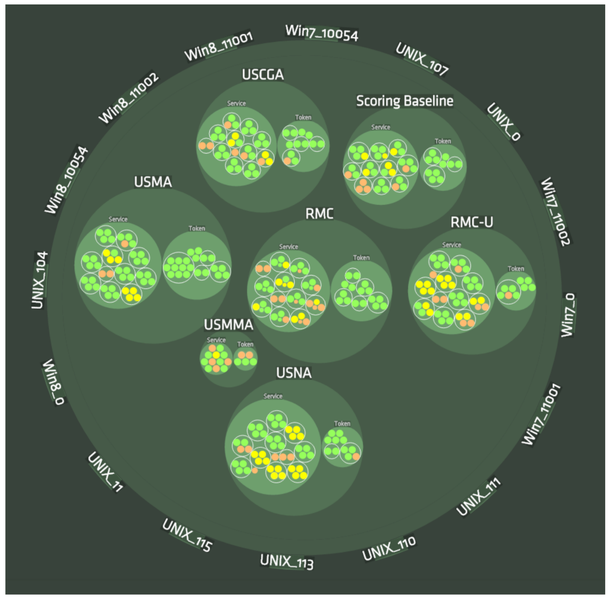

Figure 2: Potential option for displaying real-time status of anomalous services and hosts on a network in a 'system status' view, allowing for a quicker and more informed response to attacks on systems. Full credit to [2].

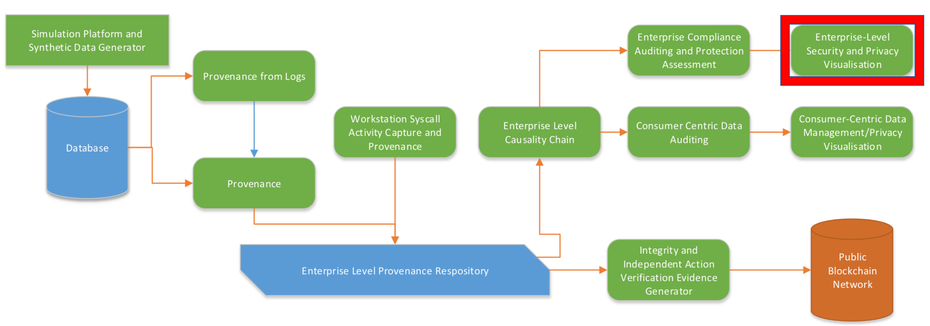

Figure 3: Full Project View with Visualisation Aspects

References

- Visually Guided Flow Tracking in Software-Defined Networking by Tobias Post, Thomas Wischgoll, Adam R. Bryant, Bernd Hamann, Paul Müller and Hans Hagen [1]
- CyberPetri at CDX 2016: Real-time Network Situation Awareness by Dustin Arendt, Dan Best, Russ Burtner and Celeste Lyn Paul [2]

Conclusion

We strive to create a tool which allows the analyst to monitor the adherence of a system to a security policy which meets statuatory requirements and organisation-specific needs. We seek to achieve this by exploring different visualization technologies & techniques to create the most intuitive and complete tool yet made for real-time enterprise-level compliance auditing.

Additional Information

This project is related to the EPSRC funded project "Data to Improve Customer Experience (DICE)". The project is particularly interested in personal data, and is using rail passengers as a specific focus of interest. The overall aims of the project are:

- Understand the role that personal data plays in enhancing the user experience of rail passengers
- To develop technical solutions to data privacy
- To develop an evaluation framework that can be implemented so passengers can understand how their data is used and how they can control and verify its use.

The project started in October 2016, and runs for three years to September 2019. For more information about the project, please visit http://www.dice-project.org.

Acknowledgements

We acknowledge the support of the ISG-SCC for the summer internship program and EPSRC funded project. The views and opinions expressed in this poster are those of the authors and do not necessarily reflect the position of DICE project or any of partners associated with this project.

Contact Information

- Web: https://scc.rhul.ac.uk/
- Email: ZDAC007@live.rhul.ac.uk