UWE Bristol | University of the West of England

Presentation by

Dr. Phil Legg

Associate Professor in Cyber Security

Security Data Analytics and Visualisation

8: Case Studies

Date: Autumn 2019

UWE Bristol University of the West of England

Research in Security Data Analytics and Visualisation

What's new in this area…?

UWE Bristol University of the West of England

IEEE Visualization for Cyber Security (VizSec)

http://www.vizsec.org

Review of Papers provided via Blackboard

Extra:

A review of 5 papers from the 2015 and 2016 VizSec conference

UWE Bristol | University of the West of England

Understanding the Context of Network Traffic Alerts

Bram C.M. Cappers* Jarke J. van Wijk†

Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands

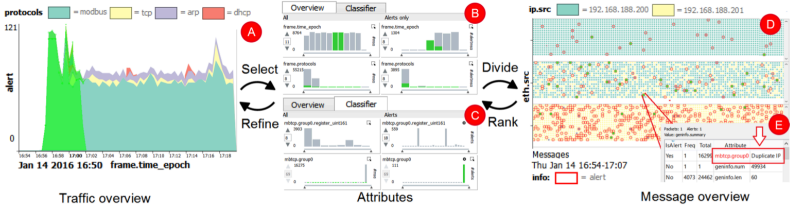


Figure 1: The discovery of Man-in-the-Middle behavior in network traffic meta-data using selection-based attribute ranking.

ABSTRACT

For the protection of critical infrastructures against complex virus attacks, automated network traffic analysis and deep packet inspection are unavoidable. However, even with the use of network intrusion detection systems, the number of alerts is still too large to analyze manually. In addition, the discovery of domain-specific multi stage viruses (e.g., Advanced Persistent Threats) are typically not captured by a single alert. The result is that security experts are overloaded with low-level technical alerts where they must look for the presence of an APT. In this paper we propose an alert-oriented visual analytics approach for the exploration of network traffic content in multiple contexts. In our approach CoNTA (Contextual analysis of Network Traffic Alerts), experts are supported to discover threats in large alert collections through interactive exploration us-

Since manual inspection of network traffic is
size and complexity, forensic experts use netw
tion Systems (IDS) to assist them in finding
though these systems automate the analysis
number of (false) alerts is often too large to
Given that alerts in message content analysis c
nation of hundreds of message attributes, the
greatly varies. In this paper we propose an ex
enables experts to gain insight in traffic conte
ing and correlating network traffic alerts defin

Similar to Livnat et al. [17], we believe th
of a complex attack does not stand on its ov
ity of an alert can not be determined by solely inspecting its structural properties such as what, when, or where that alert has occurred

ABSTRACT

For the protection of critical infrastructures against complex virus attacks, automated network traffic analysis and deep packet inspection are unavoidable. However, even with the use of network intrusion detection systems, the number of alerts is still too large to analyze manually. In addition, the discovery of domain-specific multi stage viruses (e.g., Advanced Persistent Threats) are typically not captured by a single alert. The result is that security experts are overloaded with low-level technical alerts where they must look for the presence of an APT. In this paper we propose an alert-oriented visual analytics approach for the exploration of network traffic content in multiple contexts. In our approach CoNTA (Contextual analysis of Network Traffic Alerts), experts are supported to discover threats in large alert collections through interactive exploration using selections and attributes of interest. Tight integration between machine learning and visualization enables experts to quickly drill down into the alert collection and report false alerts back to the intrusion detection system. Finally, we show the effectiveness of the approach by applying it on real world and artificial data sets.

well-established visualization and machine learning techniques. In summary, our main contributions are:

- a visual analytics approach to network forensics, enabling experts to:
  - explore and analyze network traffic on both attribute and temporal level using alerts as a ground truth, and
  - identify and confirm (visual) correlations between network traffic messages and alerts using selection-based relevance metrics and conversation analysis.
- a data-driven coupling between machine learning and visualization for the detection and refinement of network alerts.

2 case studies:
Water Plant and
University

Understanding the Context of Network Traffic Alerts

Bram C.M. Cappers* Jarke J. van Wijk†

Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands

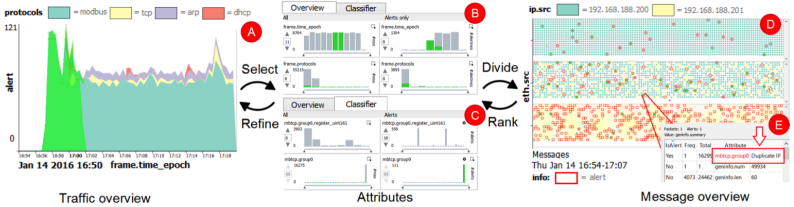


Figure 1: The discovery of Man-in-the-Middle behavior in network traffic meta-data using selection-based attribute ranking.

ABSTRACT

For the protection of critical infrastructures against complex virus attacks, automated network traffic analysis and deep packet inspection are unavoidable. However, even with the use of network intrusion detection systems, the number of alerts is still too large to analyze manually. In addition, the discovery of domain-specific multi stage viruses (e.g., Advanced Persistent Threats) are typically not captured by a single alert. The result is that security experts are overloaded with low-level technical alerts where they must look for the presence of an APT. In this paper we propose an alert-oriented visual analytics approach for the exploration of network traffic content in multiple contexts. In our approach CoNTA (Contextual analysis of Network Traffic Alerts), experts are supported to discover threats in large alert collections through interactive exploration us-

Since manual inspection of network traffic is impossible due to size and complexity, forensic experts use network Intrusion Detection Systems (IDS) to assist them in finding areas of interest. Although these systems automate the analysis of network traffic, the number of (false) alerts is often too large to analyze one by one. Given that alerts in message content analysis can arise at any combination of hundreds of message attributes, the number of alert types greatly varies. In this paper we propose an exploration method that enables experts to gain insight in traffic content by visually exploring and correlating network traffic alerts defined at message-level.

Similar to Livnat et al. [17], we believe that an alert as a result of a complex attack does not stand on its own. The true severity of an alert can not be determined by solely inspecting its structural properties such as what, when, or where that alert has occurred

7 DISCUSSION AND LIMITATIONS

The use cases in Section 6 illustrate that there is a strong interplay between high-level traffic overviews, low-level message views, and attributes. The tight linking between the different views plays a key role in understanding how high-level phenomena such as bursts relate to the presence of low-level alerts in messages. By tagging message collections through (de)selection, network traffic can be incrementally enriched with intuitive domain-specific descriptions.

The definition of an outlier greatly depends on the domain knowledge and the context in which the data is observed. The access of a file X does for instance not have to be malicious in general, but can be dangerous when performed by a certain user. The exploration method should therefore be flexible and expressive enough to create and inspect new selections without much effort. The time table facilitates this by enabling experts to inspect traffic with visualizations they are familiar with. Combined with multi-context functionality, outliers can be inspected in various contexts with a single mouse click. Being able to select and deselect messages based on their attributes, values, and temporal occurrence in conversations, while directly gaining feedback on both message and traffic level provides experts with a powerful exploration mechanism.

Like any methodology, there are limitations. First, the number of small multiples in the time table does not scale well when considering attributes with many different values. Although the expert is enabled to hide values and use scroll bars to limit the number of displayed values, this only solves the problem partly. Furthermore, the node-link diagram in the conversation view does not scale when visualizing large networks. Note however that the analysis of alerts hardly involves the analysis of all the traffic in the network at once. Since the analysis of alerts quickly narrows the area of interest, we decided to choose visualization methods based on their understandability and commonality, rather than their scalabiliy.

Second, the interaction with attributes is limited to the number of visible scented widgets. Showing too many attributes will break the interaction whereas too few attributes will increase the risk of missing potential correlations. Although sorting, filtering, and scrolling helps to find interesting attributes, creating queries involving many attributes can become a burden and a textual interface is preferred.

Third, the proposed classifier refinement approach implicitly assumes that the underlying classification model is suitable for semi-supervised learning. Although the interaction enables experts to train the classifier additionally on specific parts of the traffic, there is no clear boundary between fitting and overfitting the underlying model. The extent to which an expert can detect a false positive can greatly influence the classifier's performance in a good or bad way.

What are the limitations?

UWE Bristol University of the West of England

Abstract

SELinux policies have enormous potential to enforce granular security requirements, but the size and complexity of SELinux security policies make them challenging for security policy administrators to determine whether the implemented policy meets an organization's security requirements. To address the challenges in developing and maintaining SELinux security policies, this paper presents V3SPA (Verification, Validation and Visualization of Security Policy Abstractions). V3SPA is a tool that can import SELinux and Security Enhancements (SE) for Android source or binary policies and visualize them using two views: A policy explorer, and a policy differ. The policy explorer supports users in exploring a policy and understanding the relationships defined by the policy. The diffing view is designed to support differential policy analysis, showing the changes between two versions of a policy.

The main contributions of this paper are 1) the design of the policy explorer, and the design and novel usecase for the policy differ, 2) a report on system design considerations to enable the graph visualizations to scale up to visualizing policies with tens of thousands of nodes and edges, and 3) a survey of five SELinux and SE for Android policy developers and analysts. The results of the survey indicate a need for tools such as V3SPA to help policy workers understand the big picture of large, complex security policies.

Examining access policies using node-link filtering

V3SPA: A Visual Analysis, Exploration, and Diffing Tool for SELinux and SEAndroid Security Policies

Robert Gove*
Invincea Labs

Abstract

SELinux policies have enormous potential to enforce granular security requirements, but the size and complexity of SELinux security policies make them challenging for security policy administrators to determine whether the implemented policy meets an organization's security requirements. To address the challenges in developing and maintaining SELinux security policies, this paper presents V3SPA (Verification, Validation and Visualization of Security Policy Abstractions). V3SPA is a tool that can import SELinux and Security Enhancements (SE) for Android source or binary policies and visualize them using two views: A policy explorer, and a policy differ. The policy explorer supports users in exploring a policy and understanding the relationships defined by the policy. The diffing view is designed to support differential policy analysis, showing the

rules. These rules express the relationships between 3,410 subjects, 4,037 objects, 77 permissions, and 231 object classes.

To address the challenges faced by security engineers and analysts, this paper presents V3SPA[3], an open source interactive visualization tool for analyzing and exploring SELinux and SE for Android security policies. V3SPA is designed to be a scalable system capable of visualizing all the allow rules of a policy simultaneously, while allowing users flexibility to selectively apply filters to see only the relevant components of the policy. V3SPA has two main visualizations: A policy explorer (Figure 1), and a policy differ (Figure 2). These visualizations are designed to explore a policy to better understand the rules and relationships in the policy, and to visually diff two versions of a policy and analyze the differences between them. I discuss V3SPA's design, and I describe several de-

Doing so, we see the `mediaserver` subject node, and several object-class nodes that have either the device object or the `chr_file` class (see Figure 3b). The `mediaserver` subject node is connected to the `video_device.chr_file`, `rpmsg_device.chr_file`, `camera_device.chr_file`, `tee_device.chr_file`, `gpu_device.chr_file`, and `audio_device.chr_file` nodes via the `write` permission.

The user could choose to check if the `mediaserver` has permissions on a particular object-class pair, such as the `sdcard_type.file` node. To do so, users can open the "Always visible" tab, and begin typing "sdcard_type" in the input box. An autocomplete list of suggested node names appears, and the user can select "sdcard_type.file" from the list. This node is then added to the list of nodes that are always visible, and the node appears in the visualization. It is connected to the `mediaserver` subject node, and the user can click on the `sdcard_type.file` node to see all of its allow rules in the "Details" tab (see Figure 3c). There are six allow rules, and we see that one of them gives `mediaserver` write permission on the `sdcard_type` object and `file` class.

If the user decides to add rules to address the AVC denial, the user could modify the policy, build it, re-import it, and then use the policy differ to verify that the changes only affect the desired portions of the policy.

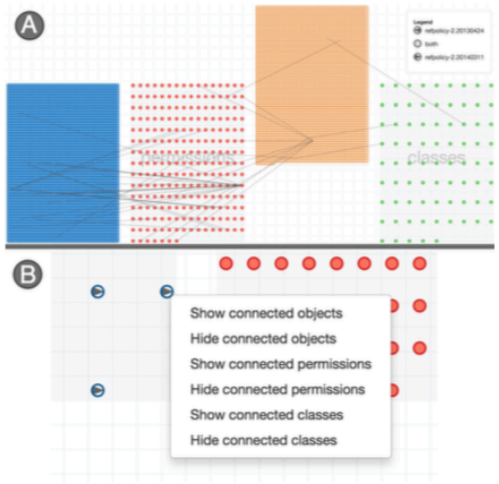


Figure 4: (a) Connections between policy components. These connections were removed after version 20130424. (b) A context menu gives users options for filtering connected nodes.

V3SPA: A Visual Analysis, Exploration, and Diffing Tool for SELinux and SEAndroid Security Policies

Robert Gove*
Invincea Labs

ABSTRACT

SELinux policies have enormous potential to enforce granular security requirements, but the size and complexity of SELinux security policies make them challenging for security policy administrators to determine whether the implemented policy meets an organization's security requirements. To address the challenges in developing and maintaining SELinux security policies, this paper presents V3SPA (Verification, Validation and Visualization of Security Policy Abstractions). V3SPA is a tool that can import SELinux and Security Enhancements (SE) for Android source or binary policies and visualize them using two views: A policy explorer, and a policy differ. The policy explorer supports users in exploring a policy and understanding the relationships defined by the policy. The diffing view is designed to support differential policy analysis, showing the rules. These rules express the relationships between 3,410 subjects, 4,037 objects, 77 permissions, and 231 object classes.

To address the challenges faced by security engineers and analysts, this paper presents V3SPA[3], an open source interactive visualization tool for analyzing and exploring SELinux and SE for Android security policies. V3SPA is designed to be a scalable system capable of visualizing all the allow rules of a policy simultaneously, while allowing users flexibility to selectively apply filters to see only the relevant components of the policy. V3SPA has two main visualizations: A policy explorer (Figure 1), and a policy differ (Figure 2). These visualizations are designed to explore a policy to better understand the rules and relationships in the policy, and to visually diff two versions of a policy and analyze the differences between them. I discuss V3SPA's design, and I describe several de-

Any limitations you can think of?

6.2 Policy Differ

In this example, I load two consecutive versions of the Tresys reference policy. First I load the 20130424 release, and then I load the 20140311 release to compute a diff between them.

When the policy differ initially loads, it defaults to showing only policy components that have been added or removed from one policy to the next. We see two subject nodes with left arrows, indicating that these are subjects from the 20130424 policy that have been removed in the 20140311 policy. Meanwhile, 46 subjects have been added to the 20140311 policy. Similarly, we see 6 objects that were removed in the 20140311 version, and 59 objects that were added. There are no added or removed permissions or classes.

In the "Nodes" tab, we can select to see all of the permissions and classes. By doing so, we can hover over a subject and object node and see the other policy components associated with it. For example, we can hover over the `redis_log_t` subject and see that it has the `associate` permission on itself and the `filesystem` class (see Figure 2). This was policy functionality that was added in the 20140311 version.

One usecase of the policy differ is to verify that policy changes do not accidentally introduce unexpected behavior. For example, we might wonder if the `redis_log_t` has any permissions on other objects. To examine this, we can right click on the `redis_log_t` subject and click the "Show connected objects" menu item (see Figure 4b). T
objects group: the `tmp_t` and `tm`
Both of these objects are in both p
that they are rendered as a solid-c
`redis_log_t` has the behavior t
is nothing out of the ordinary.

Scope to improve the differ to compare timesteps?

Differ compares two timesteps

In this paper we discuss three design methods — qualitative coding, personas, and data sketches — and frame their use specifically for designing visualizations of cyber security data from a user-centered perspective. We ground the discussions of these methods in two different cyber security visualization design projects, and we illustrate how each design method was both efficient and effective for this design space. For each method, we present outcomes from the design projects, as well as practical usage recommendations, which we believe will be useful for future cyber security projects.

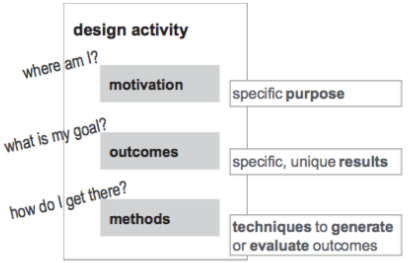


Fig. 1. Overview of the design activity framework [26], showing how each design activity has a motivation, outcomes, and methods.

Unlocking User-Centered Design Methods for Building Cyber Security Visualizations

Sean McKenna* University of Utah
Diane Staheli MIT Lincoln Laboratory
Miriah Meyer University of Utah

Abstract— User-centered design can aid visualization designers to build better, more practical tools that meet the needs of cyber security users. The cyber security visualization research community can adopt a variety of design methods to more efficiently and effectively build tools. We demonstrate how previous cyber visualization research has omitted a discussion of effectiveness and process in the explanation of design methods. In this paper, we discuss three design methods and illustrate how each method informed two real-world cyber security visualization projects which resulted in successful deployments to users.

1 Introduction

The practice of user-centered design incorporates careful consideration of users' needs, wants, and limitations throughout the design process [6], which helps in evaluating both the effectiveness and appropriateness of tools [27]. In a survey of the Visualization for Cyber Security (VizSec) proceedings from the past 5 years, roughly 40% of the 51 papers included evaluation with users, mirroring the findings of a recent survey looking back a full 10 years [33]. Only 7 of these 51 papers discuss iterative evaluation with users to improve the design of a tool, with the more common case being evaluation with users only after the design of a tool is complete. Thus, there is an opportunity within the VizSec community to improve the efficacy of visualization tools by using evaluation and user-centered design methods throughout the *entire* design process, which includes gathering user needs, design opportunities, and ideas before even building a tool; we found only 1 instance of a VizSec paper which did so in the past 5 years [38].

Introducing users into the design process often requires significant time commitments on their part. Cyber security analysts have very limited time due to the fast-paced nature of their jobs, leaving visualization designers with limited access to these domain experts. Si-

efficiently, and with increased satisfaction, thus providing benefits such as increased productivity, better accessibility, reduced stress and risk of harm, and an improved user well-being [6]. Within the cyber security visualization literature, a number of user-centered design methods have been utilized. Komlodi et al. performed iterative usability studies on visualization prototypes to improve upon their glyph design [19], while Hao et al. focus their discussion on justifying a web visualization framework [15]. Furthermore, Paul et al. present a design-first approach for finding innovative visualization solutions that emphasizes visual concepts before user requirements [29]. The limitation of these works is that they do not address the usefulness of design methods early in the design process to obtain requirements from users.

Several cyber security papers have discussed user-centered design methods during the early phases of the visualization design process, but these papers have rarely linked these methods to a final, deployed tool. Goodall et al. interviewed analysts to derive requirements for a network security tool [14], while Stoll et al. explain the personas design method [34]; however, neither of these methods were validated for their efficacy or efficiency. The cyber command gauge cluster by

4.1 Qualitative Coding

When tasked with redesigning a large cyber security tool, our design team had limited access to end users. Despite the fact that a fully deployed tool already existed, we were taking a step back to find users' needs in the first design activity: *understand*. Our motivation in this activity was to better understand the needs and design opportunities for network security analysts to redesign the firm's tool. But how do we identify user needs without direct access to end users? Many researchers have studied users in this domain from a variety of perspectives, particularly with cognitive task analyses. For this project we built off of this rich existing body of knowledge through qualitative coding of three cognitive task analyses.

Design – thinking about *why* we are visualising data?

UWE Bristol | University of the West of England

Persona – thinking about *who* we are designing for?

Paper provides recommendations from each of the three studies

Unlocking User-Centered Design Methods for Building Cyber Security Visualizations

Sean McKenna* University of Utah
Diane Staheli MIT Lincoln Laboratory
Miriah Meyer University of Utah

Abstract— User-centered design can aid visualization designers to build better, more practical tools that meet the needs of cyber security users. The cyber security visualization research community can adopt a variety of design methods to more efficiently and effectively build tools. We demonstrate how previous cyber visualization research has omitted a discussion of effectiveness and process in the explanation of design methods. In this paper, we discuss three design methods and illustrate how each method informed two real-world cyber security visualization projects which resulted in successful deployments to users.

1 Introduction

The practice of user-centered design incorporates careful consideration of users' needs, wants, and limitations throughout the design process [6], which helps in evaluating both the effectiveness and appropriateness of tools [27]. In a survey of the Visualization for Cyber Security (VizSec) proceedings from the past 5 years, roughly 40% of the 51 papers included evaluation with users, mirroring the findings of a recent survey looking back a full 10 years [33]. Only 7 of these 51 papers discuss iterative evaluation with users to improve the design of a tool, with the more common case being evaluation with users only after the design of a tool is complete. Thus, there is an opportunity within the VizSec community to improve the efficacy of visualization tools by using evaluation and user-centered design methods throughout the *entire* design process, which includes gathering user needs, design opportunities, and ideas before even building a tool; we found only 1 instance of a VizSec paper which did so in the past 5 years [38].

Introducing users into the design process often requires significant time commitments on their part. Cyber security analysts have very limited time due to the fast-paced nature of their jobs, leaving visualization designers with limited access to these domain experts. Si-

efficiently, and with increased satisfaction, thus providing benefits such as increased productivity, better accessibility, reduced stress and risk of harm, and an improved user well-being [6]. Within the cyber security visualization literature, a number of user-centered design methods have been utilized. Komlodi et al. performed iterative usability studies on visualization prototypes to improve upon their glyph design [19], while Hao et al. focus their discussion on justifying a web visualization framework [15]. Furthermore, Paul et al. present a design-first approach for finding innovative visualization solutions that emphasizes visual concepts before user requirements [29]. The limitation of these works is that they do not address the usefulness of design methods early in the design process to obtain requirements from users.

Several cyber security papers have discussed user-centered design methods during the early phases of the visualization design process, but these papers have rarely linked these methods to a final, deployed tool. Goodall et al. interviewed analysts to derive requirements for a network security tool [14], while Stoll et al. explain the personas design method [34]; however, neither of these methods were validated for their efficacy or efficiency. The cyber command gauge cluster by

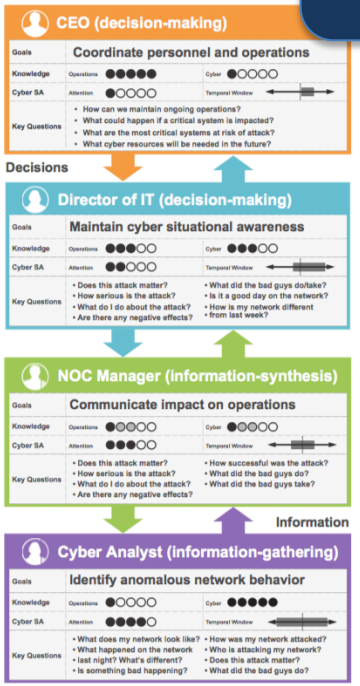


Fig. 5. An overview of the four visual personas we identified, showing the role decisions and information play across all users. The personas method was particularly effective at narrowing our design focus and facilitating consistent communication as a design team.

Results and Implications

We showed each data sketch to our analyst; here we summarize the analyst's feedback for each kind of data sketch.

- *Network Graphs*: The analyst was unconvinced that the graphs could show meaningful insights at scale with each node representing a single IP address. Furthermore, the layout algorithm confused the analyst since it positioned each IP address at a location that was not meaningful to the analyst.
- *Maps*: In contrast to the network graph sketches, the map representations garnered positive feedback from the analyst, in particular the cartograms due to their novelty.
- *Aggregated Charts*: These charts concerned the analyst because the finest level of detail was not available. We also included one data sketch to show a 3D data chart, which seemed to entice the analyst despite our continued warnings about the usability challenges of 3D for cyber security visualization [19]. More unique kinds of visualization, such as parallel coordinates and treemaps, confused the analyst on first glance and required further explanation. After explanation, the analyst commented that parallel coordinates seemed promising for exploring multidimensional data, while the treemaps, which showed the IP address hierarchy, seemed less useful.
- *Time*: These sketches were discussed in less detail; however, the analyst stated that the timestamp was one of the least important data fields to him.

https://www.youtube.com/watch?v=uMpYCJCX95k&feature=youtu.be

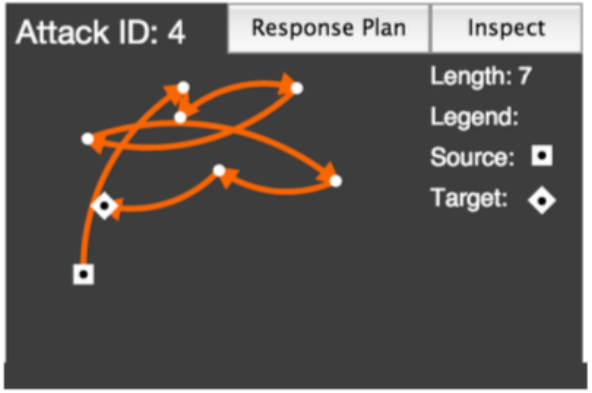


Fig. 5. Detailed view of an attack path; the figure shows the sequence of nodes, the path length, source and target nodes. It also allows for animating the attack steps ("Inspect" button) or to review the linked response plan ("Response Plan" button).

Attack path - Small multiples to show temporal activity on network graph

Overcomes issues of scalability in network graphs

PERCIVAL: Proactive and rEactive attack and Response assessment for Cyber Incidents using Visual AnaLytics

Marco Angelini, Nicolas Prigent, and Giuseppe Santucci

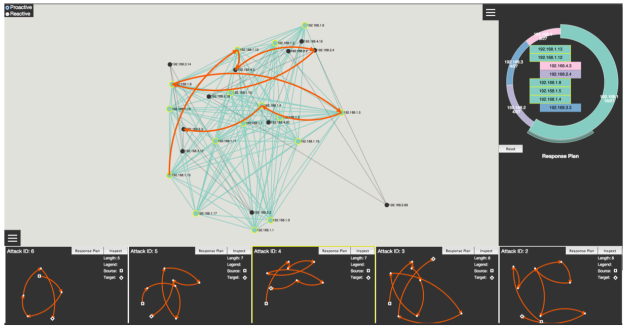


Fig. 1. The PERCIVAL system. In the attack path detailed view, the user selects a subnet (the green one) perceiving the proportion of the nodes of the attack path belonging to that subnet; moreover he can inspect the subnet nodes on the network topology view.

Abstract—Situational awareness is a key concept in cyber-defence. Its goal is to make the user aware of different and complex aspects of the network he or she is monitoring. This paper proposes PERCIVAL, a novel visual analytics environment that contributes to situational awareness by allowing the user to understand the network security status and to monitor security events that are happening on the system. The proposed visualization allows for comparing the proactive security analysis with the actual attack progress, providing insights on the effectiveness of the mitigation actions the system has triggered against the attack and giving an overview of the possible attack's evolution. Moreover, the same visualization can be fruitfully used in the proactive analysis since it allows for getting details on computed attack paths and evaluating the mitigation actions that have been proactively computed by the system. A preliminary user study provided a positive feedback on the prototype implementation of the system. A video of the system is available at: https://youtu.be/uMpYCJCX95k.

Index Terms—Cyber-security, attack paths, incident response assessment, proactive analysis

1 Introduction

Situational awareness plays a central role in cyber-defence. Its objective is to fulfill at least three goals: *understanding the system* (what are

visualization and which is the most effective representation still constitutes a challenging research area.

In this paper, we present PERCIVAL, a situational awareness tool

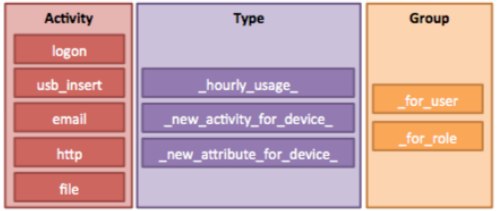


Fig. 2. Components of derived daily features from user profiles. A single feature consists of one activity (logon, usb, email, file, http), one type (hourly usage, new activity, new attribute), and one group (user/role). All feature combinations are computed from the user profile on a daily basis, resulting in 30 features per user per day.

Visualizing the Insider Threat: Challenges and tools for identifying malicious user activity

Philip A. Legg

Abstract—One of the greatest challenges for managing organisational cyber security is the threat that comes from those who operate within the organisation. With entitled access and knowledge of organisational processes, insiders who choose to attack have the potential to cause serious impact, such as financial loss, reputational damage, and in severe cases, could even threaten the existence of the organisation. Security analysts therefore require sophisticated tools that allow them to explore and identify user activity that could be indicative of an imminent threat to the organisation. In this work, we discuss the challenges associated with identifying insider threat activity, along with the tools that can help to combat this problem. We present a visual analytics approach that incorporates multiple views, including a user selection tool that indicates anomalous behaviour, an interactive Principal Component Analysis (iPCA) tool that aids the analyst to assess the reasoning behind the anomaly detection results, and an activity plot that visualizes user and role activity over time. We demonstrate our approach using the Carnegie Mellon University CERT Insider Threat Dataset to show how the visual analytics workflow supports the Information-Seeking mantra.

Index Terms—Insider threat, behavioural analysis, model visualization

1 Introduction

The threat posed by those who operate on the inside is becoming a serious risk for organisational security management. As is often recalled, *"employees are an organisation's greatest asset, and yet also their greatest threat"*. Insiders may not just be employees though - they could well be stakeholders, contractors, former employees, or management - anyone who has privileged access to organisational systems and knowledge of the organisational operations could potentially attack. This could range from financial or intellectual property losses, reputational damage and negative media attention, through to damaging the competitive edge of the organisation and threatening its continued existence. According to the 2015 Insider Threat report by Vormetric [24], 93% of U.S. organisations polled responded as being vulnerable to insider threats, with 59% of U.S. respondents stating that privileged users pose the biggest threat to their organisation. It is clear then, that the threat posed by insiders is real, and that there is a need for sophisticated measures and tools in order to effectively combat this.

What is it then, that has provoked the threat of insiders to become more prevalent? One answer to this would be the increase in opportunity as a result of technology. As technology has advanced, so to have the ways that we are able to conduct our work activities. Remote lo-

behaviour is typically anomalous to the user's normal behaviour. However, anomalous behaviour is certainly not always indicative of malicious behaviour, which results in many false positives being generated, and many frustrated security analysts who have to examine each of these. There is a need then, for effective integration between automated detection routines that can help to reduce the workload of the human analyst, whilst also having powerful exploratory tools that can support the human analyst for conducting insider threat investigations.

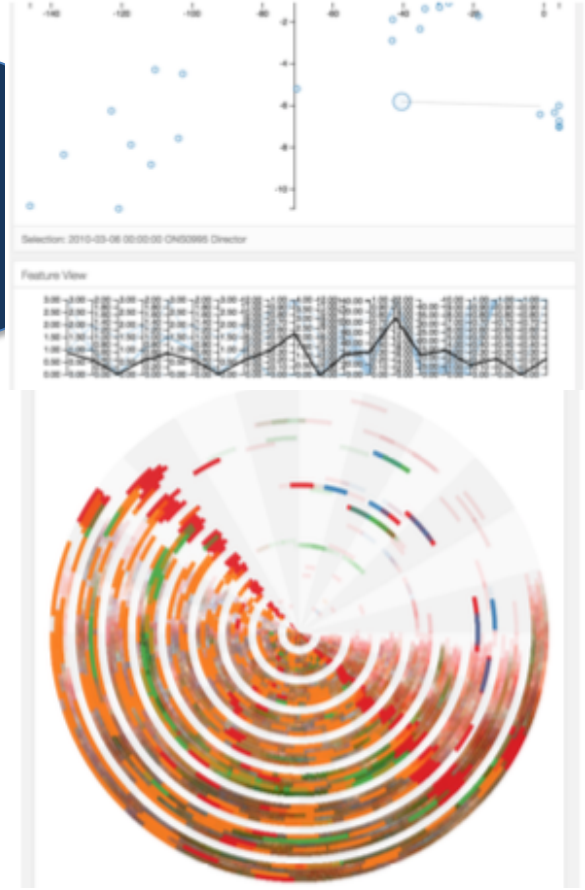
In this paper, we propose a visual analytics approach to insider threat detection. The system incorporates an anomaly detection tool [15], with a visual analytics dashboard that facilitates an integrated exploration of both the detection results and the original activity records. In particular, the system incorporates *model visualization* to better understand the outcome of the detection routine, allowing the analyst to explore the relationship between the detection results and the original profile features that describe the user's behaviour. The analyst can explore how different feature combinations impact on the detection results, and can examine which features provoke the system to identify an anomaly. With a detailed activity visualization, the analyst can also explore the raw activity data to reason as to whether or

available. Detecting the presence of an insider threat can typically be described by three types of anomaly:

- **New observations** - has the user performed a new activity, or performed an activity with new attributes? (e.g., sending an e-mail to a new recipient). If the activity/attribute is new for this user, is it also new for this role (i.e., has anyone else in the same role performed this same activity before?)
- **Time of the observation** - has the user performed an activity/attribute at a different time of day compared to their usual behaviour? (e.g., logging on early). Likewise, how does this compare against other users in the same role?
- **Frequency of the observation** - has the user performed an activity/attribute more frequently compared to their usual behaviour? (e.g., downloading many files from a server). Likewise, how does this compare against other users in the same role?

How can we derive features of 'insider' activity?

How can we visualise the features, and the corresponding ‘actual’ activity?



Visualizing the Insider Threat: Challenges and tools for identifying malicious user activity

Philip A. Legg

Abstract—One of the greatest challenges for managing organisational cyber security is the threat that comes from those who operate within the organisation. With entitled access and knowledge of organisational processes, insiders who choose to attack have the potential to cause serious impact, such as financial loss, reputational damage, and in severe cases, could even threaten the existence of the organisation. Security analysts therefore require sophisticated tools that allow them to explore and identify user activity that could be indicative of an imminent threat to the organisation. In this work, we discuss the challenges associated with identifying insider threat activity, along with the tools that can help to combat this problem. We present a visual analytics approach that incorporates multiple views, including a user selection tool that indicates anomalous behaviour, an interactive Principal Component Analysis (iPCA) tool that aids the analyst to assess the reasoning behind the anomaly detection results, and an activity plot that visualizes user and role activity over time. We demonstrate our approach using the Carnegie Mellon University CERT Insider Threat Dataset to show how the visual analytics workflow supports the Information-Seeking mantra.

Index Terms—Insider threat, behavioural analysis, model visualization

1 Introduction

The threat posed by those who operate on the inside is becoming a serious risk for organisational security management. As is often recalled, *“employees are an organisation’s greatest asset, and yet also their greatest threat”*. Insiders may not just be employees though - they could well be stakeholders, contractors, former employees, or management - anyone who has privileged access to organisational systems and knowledge of the organisational operations could potentially attack. This could range from financial or intellectual property losses, reputational damage and negative media attention, through to damaging the competitive edge of the organisation and threatening its continued existence. According to the 2015 Insider Threat report by Vormetric [24], 93% of U.S. organisations polled responded as being vulnerable to insider threats, with 59% of U.S. respondents stating that privileged users pose the biggest threat to their organisation. It is clear then, that the threat posed by insiders is real, and that there is a need for sophisticated measures and tools in order to effectively combat this.

What is it then, that has provoked the threat of insiders to become more prevalent? One answer to this would be the increase in opportunity as a result of technology. As technology has advanced, so to have the ways that we are able to conduct our work activities. Remote lo-

behaviour is typically anomalous to the user’s normal behaviour. However, anomalous behaviour is certainly not always indicative of malicious behaviour, which results in many false positives being generated, and many frustrated security analysts who have to examine each of these. There is a need then, for effective integration between automated detection routines that can help to reduce the workload of the human analyst, whilst also having powerful exploratory tools that can support the human analyst for conducting insider threat investigations.

In this paper, we propose a visual analytics approach to insider threat detection. The system incorporates an anomaly detection tool [15], with a visual analytics dashboard that facilitates an integrated exploration of both the detection results and the original activity records. In particular, the system incorporates *model visualization* to better understand the outcome of the detection routine, allowing the analyst to explore the relationship between the detection results and the original profile features that describe the user’s behaviour. The analyst can explore how different feature combinations impact on the detection results, and can examine which features provoke the system to identify an anomaly. With a detailed activity visualization, the analyst can also explore the raw activity data to reason as to whether or

UWE Bristol | University of the West of England

UWE Bristol University of the West of England

Much research going on about how ML and VA can better inform Cybersecurity