Visualization and Data Provenance Trends in Decision Support for Cybersecurity

Jeffery Garae and Ryan K.L. Ko

Abstract The vast amount of data collected daily from logging mechanisms on web and mobile applications lack effective analytic approaches to provide insights for cybersecurity. Current analytical time taken to identify zero-day attacks and respond with a patch or detection mechanism is unmeasurable. This is a current challenge and struggle for cybersecurity researchers. User- and data provenance-centric approaches are the growing trend in aiding defensive and offensive decisions on cyber-attacks. In this chapter we introduce (1) our Security Visualization Standard (SCeeL-VisT); (2) the Security Visualization Effectiveness Measurement (SvEm) Theory; (3) the concept of Data Provenance as a Security Visualization Service (DPaaSVS); and (4) highlight growing trends of using data provenance methodologies and security visualization methods to aid data analytics and decision support for cyber security. Security visualization showing provenance from a spectrum of data samples on an attack helps researchers to reconstruct the attack from source to destination. This helps identify possible attack patterns and behaviors which results in the creation of effective detection mechanisms and cyber-attacks.

1 Introduction

Data analytics and decision support for cybersecurity through methodologies, techniques, and applications has been the core ingredient to drawing conclusions and making better judgements on cyber-attacks. Network mapping and logging techniques in applications such as Wireshark has always assisted security network analysts to understand malicious IP packets [1, 2]. Other anomaly detection systems and techniques have enabled security experts to understand threats and attacks in a deeper way through identifying attack patterns and behaviors [3, 4]. This in return helps security experts and researchers to draw better cyber security decision support conclusions.

J. Garae (✉) • R.K.L. Ko
Cyber Security Lab, Department of Computer Science, University of Waikato, Hamilton, New Zealand
e-mail: jg147@students.waikato.ac.nz; ryan@waikato.ac.nz

I. Palomares et al. (eds.), *Data Analytics and Decision Support for Cybersecurity*, Data Analytics, DOI 10.1007/978-3-319-59439-2_9

While network logging and analytical methods help data analytics, data collected from modern threats and attacks are growing rapidly and new malicious attacks are more sophisticated. This requires better security approaches, methods and solutions to help understand them. Data provenance and security visualization are the growing trend for cyber security solutions [5–7]. Data captured from desired cyber-attacks creates the ability to reconstruct malicious attack landscapes and attribution to the attack origin. In addition the ability to track files end-to-end, from creation till deletion provides better decision support to cyber security experts and researchers [6, 7]. This helps security experts to identify malicious patterns and behaviors, as a result of which better conclusions are drawn and effective security implementation are taken such as security patches and defensive measures. Unlike the "ILoveYou" worm in 2000, hackers and malware developers are getting smarter by implementing cyber-attacks not only for fame or revenge, but also as targeted attacks in forms of phishing attacks, organized cybercrime attacks and nation state attacks [8]. For example, the STUXNET attack (zero day attack) on the Natanz uranium enrichment plant in Iran was regarded as the first digital weapon [9, 10]. Another example is the Sony Pictures data leak which has believed to be instigated by a nation state [11, 12]. Such cyber-threats require urgent and intelligent security methods to help protect systems and networks. However, if the attacks have penetrated systems and networks, then the need for intelligent data analytics are highly favorable. Security Visualization as a method in data analytics is a go to technique where security experts not only investigate the cyber-attacks using visualization but they also visually interpret how the attacks occur therefore reducing the analysis time spent on analyzing attack datasets [13–16]. This in return provides better decision support for the entire cyber security realm.

1.1 Motivation for This Chapter

Cybercrime has relived in a new sophisticated manner. Modern technologies have revolved around stronger security, and as technologies evolve defensively and securely. As a result, hackers and cybercriminals are stepping up their game by modifying their attack methods using smarter, sophisticated and stealth cyber-threats. Zero-day attacks are stressing the capacity for decision support technology techniques. Current analytical time on identifying zero-day attacks is unmeasurable before a patch and detection mechanism is released [17, 22]. Modern security approach and methods of countering cyber-threats and attacks have fallen short whereby users, businesses and even nations are frequently becoming targets and victims of cyber-attacks. A burgeoning attack type with the use of ransomware such as Locky ransomware is currently a new digital blackmailing attack method [18]. It has proven to be a major cyber-threat to individual users, businesses particularly in health and medical industries [19]. The Sony Pictures data breach cyber-attack has resulted in millions of losses [17, 18, 20, 21]. These form of attacks require knowledgeable security experts and most importantly security techniques, methods

and applications that draw effective conclusions aiding decision support for cyber security. For example, effective security technologies that have tracking, monitoring and reporting capabilities. There is a need to harmonize threat intelligence technologies with time-base provenance technologies to provide effective and precise findings.

The focus of this chapter is on data provenance; security visualization techniques, effective visualization measurement techniques, cyber security standards and application to aid decision support for cyber security. Although data provenance is defined in many ways depending on its niche area of interest, in this chapter, data provenance is defined as series of chronicles and the derivation history of data on meta-data [22, 23]. The ability to track data from the state of creation to deletion and reconstruct its provenance to explore prominent cyber-attack patterns at any given time is the prime approach for this chapter. This is done using data collected from logging applications and security visualization [6, 7, 22].

This chapter elaborates on incorporating security visualization and data provenance mechanisms aiding data analytics and decision support for cybersecurity. The benefits of incorporating security visualization and data provenance mechanisms are as follows:

- It shares precise insights drawn from visually analyzing collected data (systems, networks and web data).
- It also provides a comparison between existing cyber security standards and establishes a new security visualization standard to aid users.

Several use cases from Tableau and Linkurious visualization platforms are used in this chapter in Sect. 4.1. In addition, we will be emphasizing more on the inclusion of security visualization into the law enforcement domain. We provide an overview of our new security visualization standard and further discuss the benefits of threat intelligence tools. And finally security visualization provides a full-proof user-centered reporting methodology for all level of audiences (CEOs, management and ordinary employees).

This chapter is organized as follows: Sect. 2 offers a background knowledge on cyber security technologies; Sect. 3 identifies common areas where cyber security technologies exists; Sect. 4 provides how cybersecurity technologies contribute to 'Decision Support' for Cyber Security; Sect. 5 provides our main contribution of research work which is the establishment of a new 'Security Visualization Standard'; Sect. 6 proposed our 'Security Visualization Effectiveness Measurement (SvEm)' theory; the concept of providing 'Data Provenance as a Security Visualization Service (DPaaSVS)' and User-centric Security Visualization; and Sect. 7 provides the concluding remarks for this chapter.

2 Background

In general, data analytics for cyber security is widely used for exploring and reporting, particularly when analyzing threat landscapes, vulnerabilities, malware and implementing better detection mechanisms. Situation awareness is a prime reporting

feature in data analytics. Knowing the exact types of cyber-threat threatening organizational and banking industries is an important key indicator to implementing better security solutions [24]. Understanding different threat vectors targeting different domains, helps researchers and industries to develop specific defensive solutions.

However, business intelligence, Big data analytics provided in cloud technologies are some of the methods used to provide better understanding of the security processes in organizations. Sections 2.1 and 2.2 will share insights on current uses, trends and challenges for business intelligence in cloud technologies.

2.1 Business Intelligence and Analytics

Data analytics is widely used alongside business intelligence (BI&A) and in big data analytics [24, 25]. It is an important area of study by both researchers and industries with intentions of exploring and reporting data-related problems and to find solutions. As the Internet grows, there is an exponential increase in the type and frequency of cyber-attacks [27]. Sources ranging from data warehouses to video streaming and tweets generate huge amount of complex digital data. Cloud technologies provide scalable solutions for big data analytics with efficient means of information sharing, storage and smart applications for data processing [26, 28]. Gartner estimated that by 2016, more than 50% of large companies data will be stored in the cloud [27, 29]. Big data analytics using data mining algorithms that require powerful processing power and huge storage space are an increasingly common trend. It has reporting mechanism and often visual dashboards. However, because CEOs and upper-level managers are not always tech-savvy, lack of clarity and complexity with information acquired, makes the comprehensive reporting on such analytics a difficult task for cyber security experts. This is a challenge which often raises concerns in decision making situations. For example, data breach magnitude and the assessment process are often under estimated, not not reported clearly. This affects how mitigation processes to resolve the situation. As a result, the organization's reputation can be at stake and such organizations are vulnerable to cyber-attacks.

2.2 Big Data and Cloud Technologies

A major application in big data analytics is parallel and distributed systems. This method coexists as part of the entire cloud infrastructure to sustain exceeding exabytes of data and the rapid increase rate in data size [30]. The need to frequently increase processing power and storage volumes are critical the factor for cloud infrastructures. Adding onto this, security, fault-tolerance and access control are critical for many applications [30]. Continuous security techniques are built to

maintain these systems. This is yet another key decision factor in organizations and industries for cyber security frameworks. Cloud technologies also provide scalable software platforms for the use of smart grid cyber-physical systems [31]. These platforms provide adaptive information assimilation channels for ingesting dynamic data; a secure data repository for industries and researchers [31, 32]. It is a trend for power and energy companies whereby data has become valuable and further investigations into the data for insights are required and relevant for better service delivery. While information sharing and visual data analytics are useful features in these systems, data security is still major concern. With current sophisticated cyber-attacks involving phishing or social engineering elements, customer data and utility data are the main target [33, 34].

3 Cyber Security Technologies

The technological shift and drift from common use of desktop computers to mobile platforms and cloud technologies have expanded the cyber-threat landscapes [45–47]. Newer urgent needs emerged in as the digital economy has matured over the past decade. Businesses and consumers are more dependent than ever on information systems [48]. This has contributed to how cyber security has evolved over the past decade. The cyber security focus in the past decade for researchers and industries can be summed up with the list below [45–48]:

1. *Endpoint Detection and Response:* These technologies includes intrusion detection systems [36], provide the ability to frequently analyze the network and identify systems or applications that might be compromised. With endpoint detection mechanisms, responsive steps can be taken to mitigate cyber-attacks [35].
2. *Network and Sensors for Vulnerabilities:* Such technologies provide flexibilities to both users and network operators. Either wireless or wired, the sensor network has multiple preset funtions such as sensing and processing, to enable multiple application goals [49]. Senor nodes are capable of monitoring the network area with the aim identifying and detecting interested security events and reporting to a base station deployed on the network.
3. *Cloud Security:* The emerging cloud technologies have offered a wide range of services including network, servers, storage, range of applications and services [37]. However, this brought in a new range of security challenges which have contribute to how cloud technologies have transformed from the past 10 years.
4. *Cyber Threat Intelligence:* Cyber threat intelligence technologies profiles a holistic approach for automated sharing, real-time monitoring, intelligence gathering and data analytics [38]. Organizations are emphasizing on cyber threat intelligence capabilities and information sharing infrastructure to enable communications and trading between partners [39].

5. *Hardware & Software Security:* These includes providing security for hardware products and software products. Current trends indicated that hardware and software technologies have added capabilities and functions which require security components to safeguard networks and applications.
6. *Security Tools:* Security tools generally covers applications which are often used for securing systems and networks, e.g. penetration testing tools, vulnerability scanners and antivirus softwares.
7. *Security Tracking and Digital Auditing:* These technologies focus on auditing purposes especially to observe and record changes in the systems and networks. Configuration changes of a computerized device by tracking the processes and system tracks modification are some examples [40]. Other security tracking purposes include geo-location tracking, monitoring operational variables and outputs of specific devices of interest [44].
8. *User and Behavioral Analytics:* These technologies emphasize on understanding user behaviors, behavioral profiles and end users. Security concerns over targeting inappropriate audience are some of the issues encountered with these technologies [41].
9. *Context-aware Behavioral Analytics:* Context-aware technologies provide application mechanisms that are able to adapt to changing contexts and able to modify its behavior to suit the user's needs, e.g. smart homes inbuilt with a context aware application that can alert a hospital if a person urgently requires medical attention [42].
10. *Fraud Detection Services:* As Fraud cases are becoming popular, computer based systems designed to alert financial institutions based on set fraud conditions used to analyze card-holder debits. These systems also identify 'at risk' cards which are possessed by criminals [43].
11. *Cyber Situational Awareness:* Recent research and surveys have shown that the rise of cyber criminal activities have triggered the need to implement situational awareness technologies. These includes the use of surveys, data analytic and visualization technologies.
12. *Risk Management Analytics:* Risk management analytics are methodologies used by organizations as part of their business strategies to measure how well their business can handle risks. These technologies also allows organizations to predict better approach to mitigate risks.

The research and industry interests are targeting mainly end-users, data collected, security tools, threat intelligence and behavioural analytics [46–48, 50]. For example in context-aware behavioral analytics technologies, we can witness techniques such as mobile location tracking, behavioral profiling, third-party Big data, external threat Intelligence and bio-printing technologies. These are founded on the principles of unusual behavior or nefarious events [50]. Overall, popular cyber security technologies are summarized in the following categories as shown in Fig. 1 [50]. Honeypots are examples of active defense measures. Cloud-based applications and BYODs technologies are far beyond the realm of traditional security and firewall. They are well suited for the cloud and Security Assertion Markup Languages (SAML)

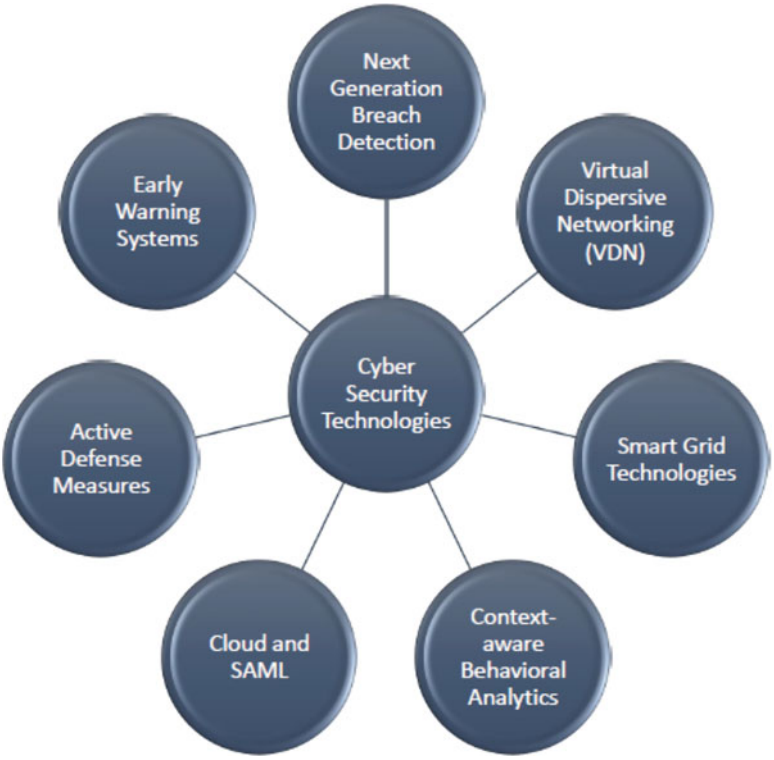

Fig. 1 Cyber security technologies trend overview in 2016

combined with intrusion detection technologies and encryption to maintain control in corporate networks [51, 52]. Early warning systems using smart algorithms are able to determine and alert security professionals on which sites and servers are vulnerable to being hacked [50].

4 Decision Support for Cyber Security

In Cyber Security, the notion of Decision Support or decision support technologies are of prime importance for corporate businesses. Early warning systems, risk management analytics, security tracking and digital auditing systems are giving corporate businesses and researchers the ability to make better decisions. Traditional decision support technologies heavily rely on data analytic algorithms in order to make important security decisions on cyber-attack and data breaches. This is often based on post-data analytics to provide reports on attack patterns and behaviors. Cyber security countermeasures as part of risk planning are effective to ensure

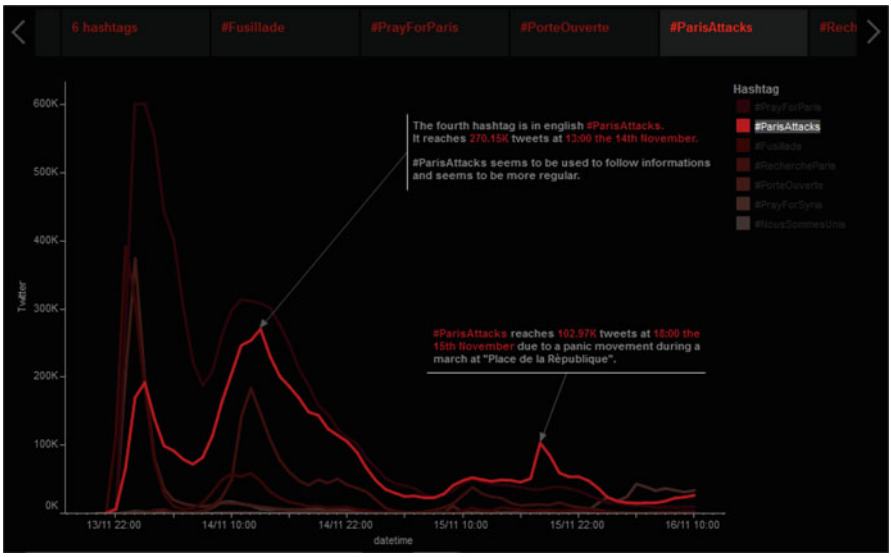

Fig. 2 Tableau visualization—analysis on twitter Hashtags on the Paris attacks

confidentiality, availability and integrity of any information system [53]. Decision support for cyber security is critical for researchers but especially for corporate organizations. It affects the organizations reputation particularly its daily operations. The ability to minimize the uncertainties in cyber-threat rates, countermeasures and impacts on the organization resulting in a low cybersecurity costs [53].

4.1 Visual Analytics for Cyber Security

In this subsection, we assess a number of leading cyber security visualization platforms and discuss the directions targeted by each of these platforms with regards to aiding decision making processes. These assessments are based on existing use cases.

Current data analytics applications have enhanced reporting features by including visualization as part of their reporting templates. For example, the use of visual dashboards is highly popular with impressive statistical analytic benefits. Most business intelligence & analytics (BI&A) systems use visual dashboards to provide statistical reports. They displays a multidimensional information sharing platform with minimal space required to display findings and has changed the way reporting is presented in the twenty-first century. BubbleNet is a visualization dashboard for cybersecurity which aims to show visual patterns [55] and Tableau is a visualization dashboard tool that offers live data visualization by connecting to local or remote data [56]. For example, the Paris attack twitter communication as shown in Fig. 2 was largely spread by social media and Edward Snowden's Twitter analysis as

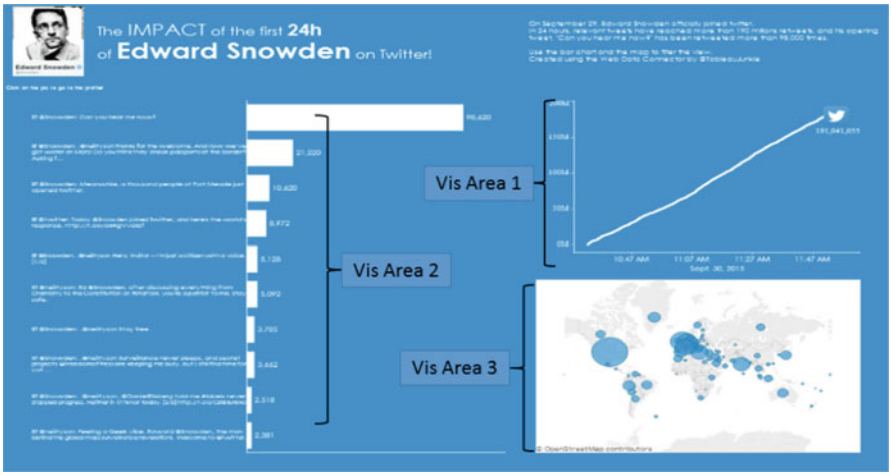

Fig. 3 Tableau visualization dashboard of Edward Snowden's impact on Twitter

shown in Fig. 3. Tableau has capabilities of loading raw data and dashboard display columns that could accommodate different visual reports of a given data collected. This is illustrated with "Vis Area 1, 2, and 3" labels in Fig. 3.

Linkurious, a web-based graph data visualization platform has capabilities to visualize complex data from security logs (network, system, application logs) [56]. It is a graph data visualization for cyber security threat analysis with the aims of (1) aiding decision support and (2) providing intelligence to support the decisions made [63]. Below are several Linkurious threat visualization analysis shown in Figs. 4, 5 and 6.

Figure 4 shows a Linkurious visual analytics of a "normal network behaviour." With such known visual patterns of what a normal network behaviour is, any future changes in the visual pattern will prompt security experts to further investigate it. For example, comparing a visual analytics pattern in Fig. 5 (a UDP Storm Attack) with Fig. 4, Cyber Security experts can effectively spot the difference and conclude that Fig. 5 shows a possibly malicious network traffic. A storm of incoming network packets targeting the IP: 172.16.0.11, as indicated by the direction of the arrows on the visualization clearly indicates that this is a denial of service attack (DoS). Linkurious also has the capabilities of representing data relationships between entities. In Fig. 6, visual representations of IP addresses are shown indicating data packets movement from the source IP address to the destination IP address.

Pentaho, a business analytics visualization platform, visualizes data across multiple dimensions with the aim of minimizing dependence on IT [58]. It has user-centric capabilities of drill through, lasso filtering, zooming and attribute highlighting to enhance user experiences with reporting features. It provides user interactions with the aim of allowing users to explore and analyze the desired dataset.

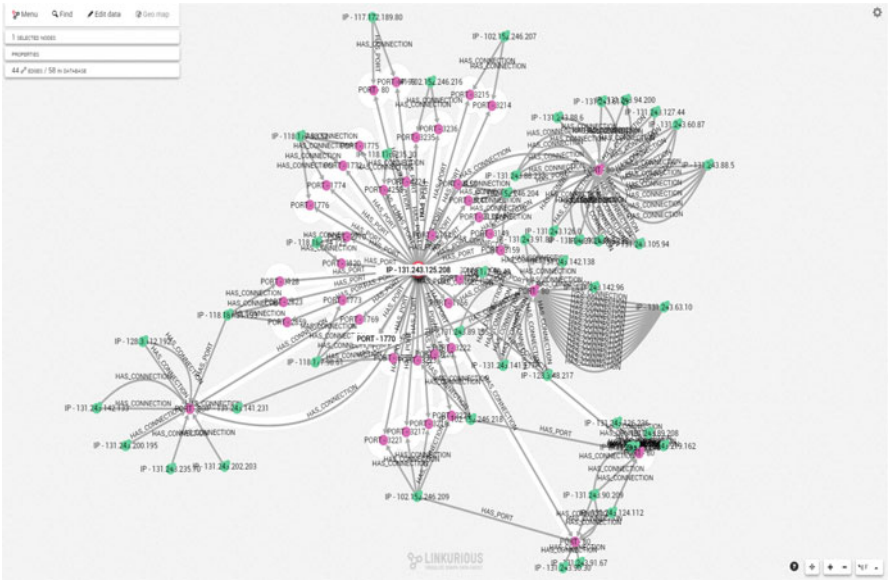

Fig. 4 Linkurious visualization threat analysis—normal network behaviour

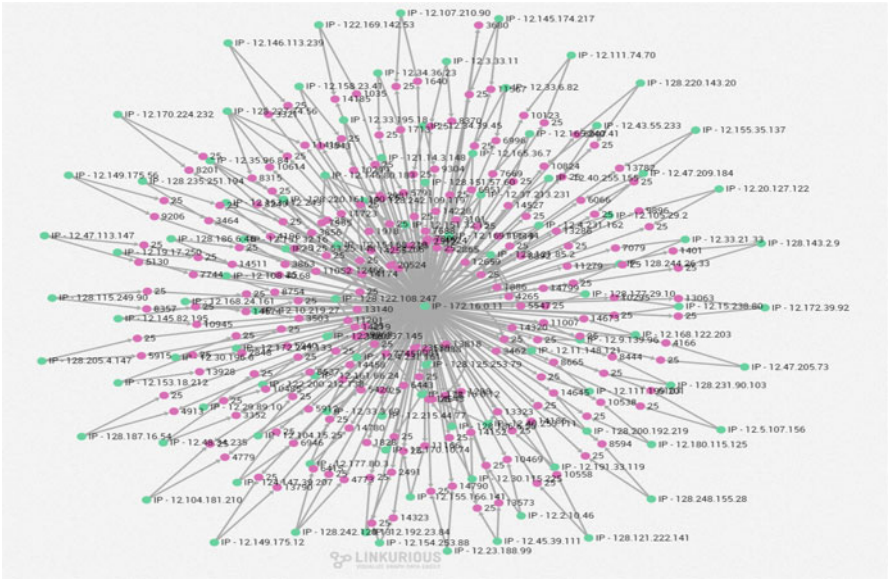

Fig. 5 Linkurious visualization threat analysis—UDP storm on IP

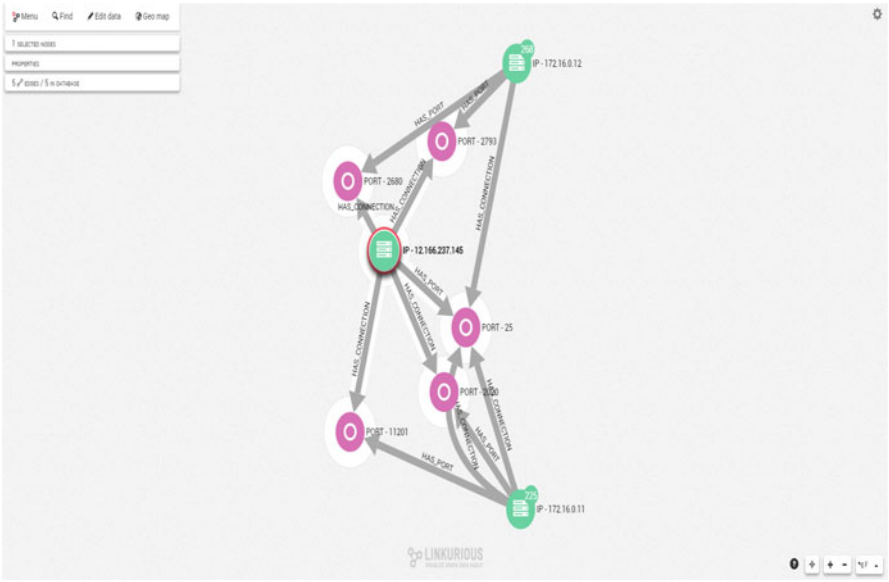

Fig. 6 Linkurious visualization IP relationship threat analysis

The ability to include visualization in these applications provides better reporting capabilities for security experts and researchers. OpenDNS with its OpenGraphiti visualization platform has features pairing up visualization and Big Data to create 3D representations of threats [54]. This enables visual outputs which practically do not require much additional explanation, due to the simplicity and self-explanatory visual outputs. Linkurious provides Intelligence analysis, fraud detection mechanisms and cyber security attack analysis mechanisms [57]. Other security companies such as Kaspersky, Norse, and Fireeye also provide real-time visualization platforms to help security researchers to better understand cyber-attacks and therefore make better decisions [59–62].

5 The Need: Security Visualization Standard

Although there is a vast range of cyber security tools, and software applications publicly available, there is still a need for data analytics and decision support mechanisms targeting specific cyber security landscapes. This is because, users (CEOs, Management and analysts) may belong to different security background and exhibit different levels of knowledge. Specific user-centric cyber security tools and techniques targeting specific audiences requires some specific cyber security standard. Cyber security decision support standards are important to guide and habour all reporting processes. Security researchers and experts leverage on such

Table 1 Standards directly related to cyber security

ISO/IEC 27000 series	
ISO Codes	Description
ISO/IEC 27000	Information Security Management Systems (ISMS)—overview
ISO/IEC 27001	Information Technology: Security Techniques in ISMS
ISO/IEC 27032	Guideline for Cybersecurity

standards in order to be on the same page with how a security event is being presented using visualization. This means creating a security visualization standard would provide a scope and guideline to help reduce the time spent on producing and presenting security visualizations. Therefore, less time will be spent on assessing a given security visualization to gain the most insights on a security visual event. Although current academic research centers and security enterprises have implemented in-house cyber security standards that suit their research aims, projects and enterprise operations, the challenge and complexity in security visualization reports manifests to some difficulties in understanding visualization reports. In the following subsection, we present various cyber security standards and assess them with the purpose of highlighting the importance how cyber security standards help manage and reduce possible cyber-attacks.

5.1 Outline on Cyber Security Standards

As part of the International Organization for Standarization/International Electrotechnical Commission 27000 series, 27001 (ISO/IEC 27001:2013)—Information security management and ISO 27032—Guideline for cybersecurity, has established guidelines and certification standard for Information security and cybersecurity as a whole [68–70]. Table 1 summarizes the cyber security standards. From a practical perspective, ISO 27001 formally provides a guideline of managing information risks through information security controls in an organization. For example, the ISO/IEC 27001:2005 provided the "PDCA (Plan-Do-Check-Act/Adjust) cycle or Deming cycle." ISO 27032 on the other hand is a cybersecurity certification standard on Internet Security [70]. In any security standards, policies and guidelines are implemented to include and maintain all aspects in security events. Alternatively, the use of visualization in cyber security should have a Security Visualization Standard [71, 72].

Table 2 Types of cyber security visualization guidelines

Cyber security visualization guidelines	
Guidelines	Description
Representation guidelines	How information is represented
Selection guidelines	Visualization platforms
Color guidelines	Guidelines on how to select and use colors
Shape guidelines	Guidelines on choices of shapes used
User guidelines	User-interaction guidelines

5.2 SCeeL-VisT: Security Visualization Standard

Although different organizations have in-house visualization standards according to their preferences, interpretation complexities from visualization platforms to users without a solid technical background is a common concern in the cyber security domain. Interpretation accuracy with meaningful and useful insights in a time sensitive manner is a key feature when using security visualization.

In most cyber security research centers, particularly in law enforcement, security use cases are presented with research outputs often with sensitive data that require urgent need to safeguard and preserve them with policies, physical secure storage and guidelines. These policies and guidelines outlines how to handle and use these sensitive data. Security visualization for law enforcement requires a security visualization standard to maintain information security, information sharing and exchanging of insights presented from visualizing of security events. This standard will act as basis to implementing and presenting security visualization with the aim to maintain the confidentiality and integrity of the underlying raw data. We present our Security Visualization Standard (SCeeL-VisT) model with related descriptions. Further detail on SCeeL-VisT standard is given in the following pages. The SCeeL-VisT standard has two major parts:

1. Understanding what is in Hand (Dataset)
2. Security Visualization Process

5.3 Security Visualization Policies and Guidelines

On a broader coverage of the Standard, a way forward for cyber security researchers and industry security experts is to establish security visualization policies and guidelines. These guidelines are shown in Table 2.

The purpose of developing SCeeL-VisT standard is to put emphasis on common grounds with security visualization development, presentation, and understanding security events. Because the use of data visualization has been widely used across many research domains and industries, complying with a security visualization

standard is of vital importance. This is due to the high frequency in which sensitive data must be dealt with. In addition to that, current security visualizations are tailored towards specific audiences making it difficult for other interested users to understand insights presented in a given visualization. Finally, the most crucial purpose of having a standard like SCeeL-VisT is its contribution to making effective decisions in cyber security. Such standards creates a clear and precise scope for both cyber security experts and what security visualizations should show in relations to the raw data used.

5.4 Law Enforcement Visualization Environment

Cyber security for law enforcement organizations especially international law enforcement agencies are seeing new trends emerging in highly complex cybercrime networks. Generally, law enforcement agencies such as Interpol have classified "Cybercrime" in two main types of internet-related crime [64]:

- **Type 1: Advanced cybercrime** (or high-tech crime)—Sophisticated Attacks against computer hardware and software.
- **Type 2: Cyber-enabled crime**—Many 'traditional' crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even terrorism.

For the law enforcement environment, cybersecurity technologies are driven towards aiding investigations, information sharing, securing and preserving data. Examples of this include malware threat intelligence, defensive and mitigation technologies [57, 59–62]. Cyber security today is driven by the way cybercriminals are executing cyber-attacks. Most cyber-attacks are increasingly smart and sophisticated coercively drives law enforcement, researchers and industry experts to match up with both defensive and offensive security applications. Data analytics and threat intelligence are some of some of the examples used for tracking and monitoring interested cyber criminal entities. As the cybercrime nature grows from individual and small group cybercriminals to advance methodologies, we see highly complex cyber criminal networks from both individuals and organized cyber criminal organizations. Current cyber attacks stretch across transnational jurisdictions in real-time to execute cyber-attacks on an unprecedented scale. Interestingly, the flow of digital currencies movement are associated with these cybercrimes, especially organized

cybercrimes. Therefore the cyber security trend for law enforcement can be scaled down to three main technology categories: (1) Attribution tools; (2) Cyber Threat Intelligence and (3) Secure Information Sharing Technologies (SIST). However, the rate at which malwares and ransomwares are created versus the implementation of new cybersecurity tools to combat these cyber-threats is far beyond proportion. This raises a concern for law enforcement and cyber security across international borders.

Existing cybercrime challenges for law enforcement range from malware attacks, ransomwares and terrorism [64]. Security approaches such as data analytics and threat intelligence methodologies are some of the steps taken by law enforcement research domains to help with improving investigation technologies. Due to how cybercrime has been broadening its attack environment from not just the technology domain but broadly penetrating others such as health and financial domain, the fight against cybercrime for law enforcement has taken extensive direction which requires external and international collaborations. This means information sharing legislations have to be re-visited, policies and guidelines have to be implemented.

The rise of dark market trading between cybercriminals on the dark web allows them to produce and escalate cyber-attacks at a rate leaving law enforcement, academia and industry researchers to encounter cyber security challenges. However, associating the use of digital currencies (Bitcoins) by cybercriminals with cybercrimes, triggers the need for new threat intelligence tools, data analytics tools and vulnerability scanners that would allow effective execution of investigations.

Threat Intelligence tools and 24/7 monitoring live-feed applications allow law enforcement agencies to carry out their investigations effectively especially for transnational cybercrimes whereby international collaborations is required. Information sharing between international law enforcement agencies without sharing the underlying raw data capabilities is of high demands.

Bitcoin[1] [65] is a peer-to-peer distributed electronic cash system that utilizes the blockchain[2] protocol [66, 67]. Due to how bitcoin payment transactions operate over the Internet in a decentralized trustless system, law enforcement agencies are seeking ways aid their investigations especially to track and monitor Bitcoins movements that are involved in cybercrime events. The ability to provide visual threat intelligence on Bitcoin transactions using blockchain tools are some of the way forward to fighting cybercrime. Where the money flows to and from known cybercriminals, allows law enforcement and cyber security investigators to track cybercrime events.

[1] Bitcoin is a distributed, decentralized crypto-currency, which implicitly defined and implemented Nakamoto consensus.

[2] Blockchain is a public ledger of all Bitcoin transactions that have executed in a linear and chronological order.

Security Visualization Standard (SCeeL-VisT)

Part 1: Understanding what is in Hand (Dataset)

1. **The Problem**:- Identification of Security Event
   - Identify Security Event (e.g. Malware Attack, SQL Injection, etc.) & Data Type (Raw data: log files, Social media data, etc.)
   - Understand the nature of data (e.g. financial data, Health data. etc.)
2. **The Purpose**: Know the Visualization Type and Technique
   - Understand the intension of security Visualization (e.g. show relationships, etc.)
   - Decision: Exploratory or Reporting Visualization
   - Decision: Security visualization Technique (e.g. Categorizing: time-base, Provenance-base attack-base)
3. **Cyber Attack Landscape**: Know the cyber-attack location (e.g. Network, Systems, Application layer, etc.)
   - Know the point of attack (e.g. network attack, identify source and destination of attack, etc.)
   - Attribution of cyber-attack

Part 2: Security Visualization Process

1. **Visual Presentation Methodologies**: How to present data visually
2. **Color & Shape Standard for Security**: Decision on choice of colors
   - Standardizing Main Color choices
     - Color: Red = High Attack Nature or Violation (e.g. Malware Process)
     - Color: Yellow = Suspicious Process (e.g. IP address)
     - Color: Green = Good or Normal Process (e.g. Network traffic)
     - Color: Blue = Informational Process (IP address)
     - Color: Black = Deleted, Traces: non-existed (e.g. deleted file,)
   - Standardizing Main Shapes choices
     - Shape: Circle = Nodes (e.g. Network Nodes)
     - Shape: Rectangle = Files (e.g. .docs, .jpeg, etc.)
     - Shape: Square = Data Clusters (e.g. IP address—network traffic)
     - Shape: Diamond = Web / Social Media Process (Social media data)

(continued)

- Standardizing Use of Line Types
  - Line: Single Line (—) = Relationships, Connections, Links, Provenance, time-base (e.g. between two Network Nodes)
  - Line: dotted Line (- - -) = Possible Relationships (e.g. .docs, .jpeg)
  - Line: Solid Arrow (→) = Direction of relationship or interaction
  - Line: Dotted Arrow (−− >) = Predicted Relationship or Interaction

3. **Security Visualization Techniques**: Provenance & Attribution-base, User-centered, Real-time base
4. **Security Visualization Type**: Animated, 3D, Static, etc.

6 Effective Visualization Measurement Techniques

Prior to this section, cyber security technology trends and use cases were analyzed and discussed including security visualization. These are part of the growing trend and effective methodologies for addressing cyber security issues (cybercrime). However, to improve security visualization technologies, we have to look into 'how' and 'what' makes security visualization appealing to viewers of the visualization. Measuring how effective, useful and appropriate security visualizations are to users helps provide researchers and developers ways of improving security visualization technologies. Before we discuss our new 'effective visualization measurement technique', a summary of existing effectiveness measurement techniques are outlined in Table 3.

6.1 The Security Visualization Effectiveness Measurement (SvEm) Theory

By analyzing existing techniques and understanding how they function, we introduce our new effective measurement technique which measures the effectiveness in both a given security visualization and the viewer's experiences on security events. It is based on both the visualization approach and user intuition. We refer to this new effective measurement technique as 'Security Visualization Effectiveness Measurement (SvEm) theory and is displayed in Eq. (1). Elaborating on thetheorem,

Table 3 Existing visualization measurement techniques

Summary—visualization effectiveness measurement techniques	
Effective measurement factor	Range of measurement (quantity)
Cognitive load	High (germane/intrinsic/extraneous cognitive load)
Working memory (prior knowledge)	High (effects to cognitive load)
NASA-TLX test (indirect-work load)	Medium (based on work load)
Subjective Workload Assessment Technique (SWAT)	Medium (scale rating factors—mental effort)
Image quality assessment	Medium—high (based on distortion)
Eye tracking (CODE theory-visual attention)	High (eye movement based—information theory)
Brain activity	High
Response time on task (s)	Low (depends on prior knowledge and effort
Effort/difficulty rating	Low (based on insights
User interactions/performance	Low (based on naive physics; body, social, environmental awareness skills)
Visual perception metrics (visualization efficiency)	Low (based on graphical methods e.g. similarities)

the SvEm[3] theory aims to minimize the time (duration) spent on viewing a visualization and making sense out from the intended insights portrayed in a visualization. The components of the SvEm theorem are:

1. *Mobile platform screen surface area (w * h)*: This refers to the surface area used to display a security visualization. Screen sizes have a great impact on how visualizations appear.
2. *Security Visual Nodes (Sv_f)*: These are known security attributes identified in a visualization, e.g. an malicious or infected IP address.
3. *N-dimensions*: N-dimensions refers to how many visual dimensions used to represent the visualization. The higher number of dimensions are used for visualization indicates the depth of data being able to represent visually.
4. *User Cognitive Load (Cl)*: This is based on how much knowledge (Prior knowledge) a user has on the expect visualization. It is a prerequisite security knowledge around expected security events such as a malware cyber-attack.
5. *Memory Efficiency (t_{me})*: This is a time-base attribute which measures how fast one can recall security related attributes.
6. *Number of Clicks (n_{clicks})*: This refers to how many clicks one has to perform on the mobile platform screen in order to view the required visualization.

[3]The Security Visualization effectiveness Measurement theory designed for mobile platforms is measured in percent (%) provides a way to measure clarity and visibility in a given security visualization.

Security Visualization Effectiveness Measurement (SvEm) Theory

$$SvEm = \frac{(w * h)/Sv_f * d_n}{Cl * t_{me} * n_{clicks}} > 50\%(Distortion) \quad (1)$$

Where:
w * h : Mobile Display Area (dimensions)
Sv_f : Security Visual Nodes (e.g. Infected-IP, Timestamp, etc.)
d_n : n-dimensional view of security visualization
Cl : Cognitive Load (Identifiable Attributes (Quantity)—Prior Knowledge)
t_{me} : Memory efficiency (Effort based on Working memory—Time-base)
n_{clicks} : Number of clicks on Visualization

The theoretical concept behind SvEm is based on two main effectiveness measurement factors:

1. **Visualization Distortion**: Effectiveness in Distortion is defined when a visualization has *greater than* 50% visual clarity
   - How clear and readable visualization is presented
   - Features and Attributes presented are visible
   - Visual patterns emerge into reality to observers.
2. **User Response Time**: Duration in milliseconds (ms)
   - Analytical time of processing the visualization
   - Time of user- cognition to recall known memory

Based on this theory, we have observed that the factors highly contributing to a high SvEm value are: (1) *w * h: smartphone dimensions* and (2) d_n*: n-dimensional view of security visualization* i.e. a 3-dimensional representation visualization view has proven less distorted than a single-dimensional visualization view. More data information are visible and shown in higher n-dimensional visualization views. This affects the users (viewer) ability to provide a higher count for Sv_f. The less value of n_{clicks}, indicates that the overall *time* spent on viewing the visualization. This contributes to higher effectiveness measurement outcome. However, the current focus is on the following:

- Mobile platform screen resolution types
- Users cognitive load (CL: prior knowledge)
- Data input size.

Due to these contributing challenge factors, assumptions are established as guides, to give a better effectiveness measurement reading. As a result, errors are minimized to achieve appropriate and reasonable SvEm reading.

- If a user is able to understand a given security visualization within *less than* 5 s, then visualization has effective SvEm output.
- Input data has to be within the capable processing power of mobile platform used.
- User must always have some form of cognitive ability (Prior knowledge) before engaging the given security visualization.
- Number of Clicks (n_{clicks}) refers to number of clicks(navigating) on the mobile platform screen to the point where the first known security attribute has been identified.

6.2 *Data Provenance as a Security Visualization Service (DPaaSVS)*

Many cyber security researchers are investing their efforts into finding technological solutions in understanding cyber-attack events, defending against them and finding ways to mitigate such cyber-attacks. A prominent method in understanding cyber-attack events is related to the concept of 'Data Provenance' which is defined as "a series of chronicles and derivation history of data on meta-data" [7, 22]. Including data provenance into security visualization allows cyber security researchers and experts to be able to analyze cyber-attacks from it's origins through to it's current state i.e. from the instant when the cyberattack was found in the systems to the state of mitigation or even further to the 'post - digital forensic' state of the cyberattack. Having the ability to apply data provenance as a security visualization service (DPaaSVS), cybersecurity experts will better understand cyber-attacks, attack landscapes and the ability to visually observe attack patterns, relationships and behaviors in a nearly real-time fashion [73]. For example, Fig. 7 presents a deep node visualization of network nodes, with patterns highlighted colors, rings-nodes and lines of nodes captured every 5 s [73]. Although provenance has been used as exploratory features in existing visualization platforms, we present the concept of 'Data Provenance as a Security Visualization Service (DPaaSVS) and its features.

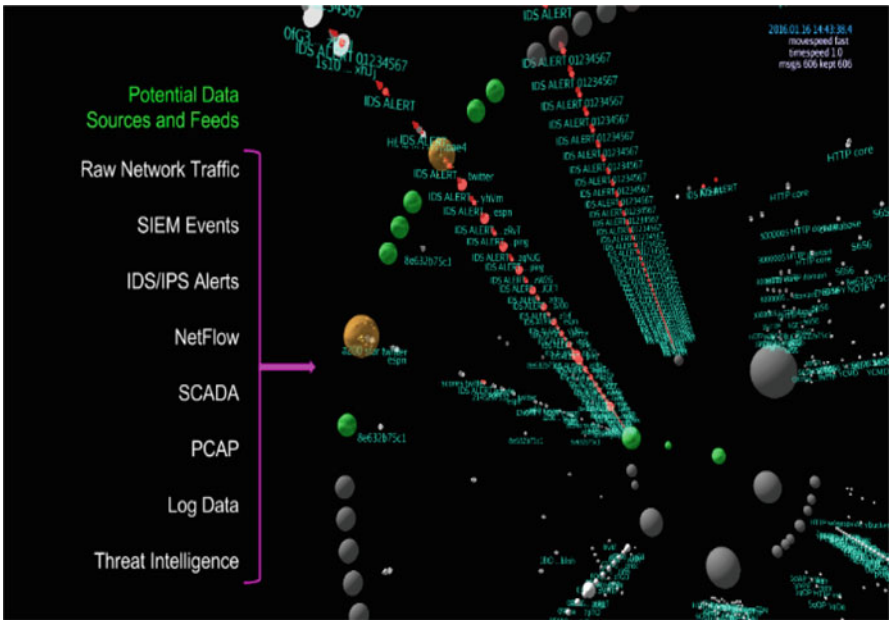

Fig. 7 Security visualization with Deep Node Inc. provenance time-base patterns

Data Provenance as a Security Visualization Service (DPaaSVS) features:

- Tracking and observing cyber-attacks from past to present using historical data.
- Threat Intelligence and monitoring.
- Educating viewers (users) with cyberattack types and attack landscapes.
- Exploring cyber-attacks using visual patterns and behaviors.
- Pinpointing cyber-attacks using timestamps.
- Empowering viewers (users) to interact with cyber security events using data collected.
- Empowering viewers (users) to effectively make decisions on cyberattack issues.

Generally, both offensive and particularly defensive security technologies depend on '*Past Knowledge*.' Security visualization based on past knowledge (Provenance) are able to show matching patterns and behaviours while observing a given visualization therefore gives insights on who such cyber-attacks are penetrating network systems. Based on provenance Cyber defenses including Firewalls, Intrusion Prevention Systems (IPS) and Antivirus are able to implement secure approaches such as:

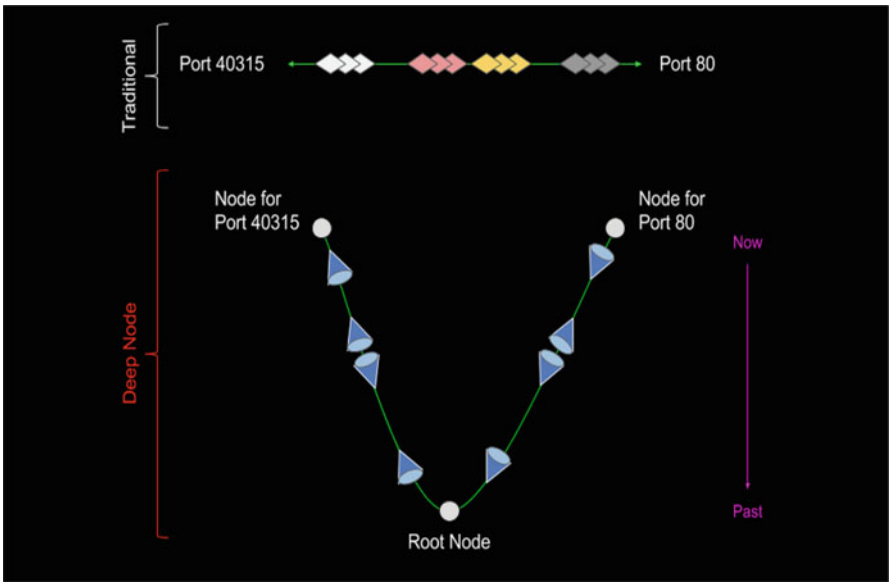

Fig. 8 Deep Node security visualization with provenance base knowledge

- *pre-defined* signature-based rules to block known suspicious traffic.
- capabilites to monitor *signs* of known malicious activities over the network traffic (web).
- capabilities to see *known* attack traffics and protocol violations over the network.

For example, Deep Node security visualization provides it's security analysts with the ability to use Data Provenance as a Security Visualization Service (DPaaSVS) by understanding network traffics based on Nodes in the concept of *Past-Node* and present [73, 74]. Nodes visualized are monitored through network traffics via it's corresponding communication *Port*. See Fig. 8.

6.3 User-Centric Security Visualization

Security visualizations like any other general visualization has a purpose. Data analytics, data exploration and reporting are the most common areas for security visualization. However, the art of presenting the visualization to the viewers (users) defines how useful it is. With targeted audiences, presenting visual insights enables users make smart and effective decisions. While there area lot of aspects

to discuss under user-centric security visualization, this subsection highlights the core importance on what makes security visualization a user-centric approach and highlight important user-centric features in security visualizations. But before we look further into the details of users and their interactions with visualizations, the term 'User-centric Security Visualization' is defined in the context of this chapter. The term 'User-centric Security Visualization' refers to visualizations that empower users to interact with any given visualization in platforms to observe and explore security events. To name a few, such user-interactions features include:

- *Mouse-over click* control, labeling and tagging features.
- *Zoom-in and zoom-out* features.
- *Lasso filtering and Attribute highlighting* features
- *Multi-dimensional* (e.g. 3-Dimension (3D)) visual views.
- *Visual Animation* features.
- *Virtual reality* capabilities.
- *data input* features.
- *Color categorization* features.
- *Time and abstracts insertion* control features.

These user-interactions in visual platforms enables users to have a sense of control and interaction when visually interacting with security events based on data collected or at real-time. Such interactions naturally installs the viewers interests and instincts in motivating them to engage and understand security events in a realistic approach therefore enhances user experience and contributes to making decisions effectively.

7 Concluding Remarks

In summary, cyber security technologies are driven by Internet users and industry demands to meet security requirements to secure their systems and networks. As technologies evolve, existing cyber security technological trends are often dictated by smart sophisticated cyber-attacks causing cyber security experts to step up their game into security researches. This motivates research opportunities for data provenance and security visualization technologies in aid of understanding cyber-attacks and attack landscapes.

Due to the increasing statistics of cyber-attacks penetrating networks, existing cyber security technologies for 'decision support' are directed mainly into data analytics and threat intelligence. Understanding how to prevent, protect and defend systems and networks are the prime reasons for data analytics and threat intelligence technologies. However, Security Visualization in the context of data provenance

and user-centric approaches are increasingly common and driven into the cyber security technologies for smarter and effective decision support reporting. Finally, with specific directed cyber security standards, policies and guidelines for security visualization, effective decisions and conclusions can be reached with minimal time required to react, defend and mitigate cyber-attacks.

Acknowledgements The authors wish to thank the Cyber Security Researchers of Waikato (CROW) and the Department of Computer Science of the University of Waikato. This research is supported by STRATUS (Security Technologies Returning Accountability, Trust and User-Centric Services in the Cloud) (https://stratus.org.nz), a science investment project funded by the New Zealand Ministry of Business, Innovation and Employment (MBIE). The authors would also like to thank the New Zealand and Pacific Foundation Scholarship for the continuous support towards Cyber Security postgraduate studies at the University of Waikato.

References

1. Orebaugh, Angela, Gilbert Ramirez, and Jay Beale. Wireshark & Ethereal network protocol analyzer toolkit. Syngress, 2006.
2. Wang, Shaoqiang, DongSheng Xu, and ShiLiang Yan. “Analysis and application of Wireshark in TCP/IP protocol teaching.” In E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference on, vol. 2, pp. 269–272. IEEE, 2010.
3. Patcha, Animesh, and Jung-Min Park. “An overview of anomaly detection techniques: Existing solutions and latest technological trends.” Computer networks 51, no. 12 (2007): 3448–3470.
4. Yan, Ye, Yi Qian, Hamid Sharif, and David Tipper. “A Survey on Cyber Security for Smart Grid Communications.” IEEE Communications Surveys and tutorials 14, no. 4 (2012): 998–1010.
5. Tan, Yu Shyang, Ryan KL Ko, and Geoff Holmes. “Security and data accountability in distributed systems: A provenance survey.” In High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on, pp. 1571–1578. IEEE, 2013.
6. Suen, Chun Hui, Ryan KL Ko, Yu Shyang Tan, Peter Jagadpramana, and Bu Sung Lee. “S2logger: End-to-end data tracking mechanism for cloud data provenance.” In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 594–602. IEEE, 2013.
7. Ko, Ryan KL, and Mark A. Will. “Progger: an efficient, Tamper-evident Kernel-space logger for cloud data provenance tracking.” In Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on, pp. 881–889. IEEE, 2014.
8. Bishop, Matt. “Analysis of the ILOVEYOU Worm.” Internet: http://nob.cs.ucdavis.edu/classes/ecs155-2005-04/handouts/iloveyou.pdf (2000).
9. D. Kushner, The Real Story of Stuxnet, IEEE Spectrum: Technology, Engineering, and Science News, 26-Feb-2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
10. A. K. Z. K. Z. Security, An Unprecedented Look at Stuxnet, the Worlds First Digital Weapon, WIRED. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
11. Rigby, Darrell, and Barbara Bilodeau. “Management tools & trends 2011.” Bain & Company Inc (2011).
12. Bonner, Lance. “Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches.” Wash. UJL & Pol’y 40 (2012): 257.

13. Siadati, Hossein, Bahador Saket, and Nasir Memon. “Detecting malicious logins in enterprise networks using visualization.” In Visualization for Cyber Security (VizSec), 2016 IEEE Symposium on, pp. 1–8. IEEE, 2016.
14. Gove, Robert. “V3SPA: A visual analysis, exploration, and diffing tool for SELinux and SEAndroid security policies.” In Visualization for Cyber Security (VizSec), 2016 IEEE Symposium on, pp. 1–8. IEEE, 2016.
15. Rees, Loren Paul, Jason K. Deane, Terry R. Rakes, and Wade H. Baker. “Decision support for cybersecurity risk planning.” Decision Support Systems 51, no. 3 (2011): 493–505.
16. Teoh, Soon Tee, Kwan-Liu Ma, and S. Felix Wu. “A visual exploration process for the analysis of internet routing data.” In Proceedings of the 14th IEEE Visualization 2003 (VIS’03), p. 69. IEEE Computer Society, 2003.
17. Wang, Lingyu, Sushil Jajodia, Anoop Singhal, and Steven Noel. “k-zero day safety: Measuring the security risk of networks against unknown attacks.” In European Symposium on Research in Computer Security, pp. 573–587. Springer Berlin Heidelberg, 2010.
18. Mansfield-Devine, Steve. “Ransomware: taking businesses hostage.” Network Security 2016, no. 10 (2016): 8–17.
19. Sgandurra, Daniele, Luis Muñoz-González, Rabih Mohsen, and Emil C. Lupu. “Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection.” arXiv preprint arXiv:1609.03020 (2016).
20. Davis, Thad A., Michael Li-Ming Wong, and Nicola M. Paterson. “The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite.” Colum. Bus. L. Rev. (2015): 613.
21. L. Widmer, The 10 Most Expensive Data Breaches | Charles Leach, 23-Jun-2015. [Online]. Available: http://leachagency.com/the-10-most-expensive-data-breaches/.
22. J. Garae, R. K. L. Ko, and S. Chaisiri, UVisP: User-centric Visualization of Data Provenance with Gestalt Principles, in 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, August 23–26, 2016, 2016, pp. 1923–1930.
23. Zhang, Olive Qing, Markus Kirchberg, Ryan KL Ko, and Bu Sung Lee. “How to track your data: The case for cloud computing provenance.” In Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, pp. 446–453. IEEE, 2011.
24. Microsoft, 2016 Trends in Cybersecurity: A quick Guide to the Most Important Insights in Security, 2016. [Online]. Available: https://info.microsoft.com/rs/157-GQE-382/images/EN-MSFT-SCRTY-CNTNT-eBook-cybersecurity.pdf.
25. Chen, Hsinchun, Roger HL Chiang, and Veda C. Storey. “Business intelligence and analytics: From big data to big impact.” MIS quarterly 36, no. 4 (2012): 1165–1188.
26. Durumeric, Zakir, James Kasten, David Adrian, J. Alex Halderman, Michael Bailey, Frank Li, Nicolas Weaver et al. “The matter of heartbleed.” In Proceedings of the 2014 Conference on Internet Measurement Conference, pp. 475–488. ACM, 2014.
27. Mahmood, Tariq, and Uzma Afzal. “Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools.” In Information assurance (ncia), 2013 2nd national conference on, pp. 129–134. IEEE, 2013.
28. Talia, Domenico. “Toward cloud-based big-data analytics.” IEEE Computer Science (2013): 98–101.
29. C. Pettey and R. Van der Meulen, Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond, 01-Dec-2011. [Online]. Available: http://www.gartner.com/newsroom/id/1862714.[Accessed:01-Feb-2017].
30. Kambatla, Karthik, Giorgos Kollias, Vipin Kumar, and Ananth Grama. “Trends in big data analytics.” Journal of Parallel and Distributed Computing 74, no. 7 (2014): 2561–2573.
31. Simmhan, Yogesh, Saima Aman, Alok Kumbhare, Rongyang Liu, Sam Stevens, Qunzhi Zhou, and Viktor Prasanna. “Cloud-based software platform for big data analytics in smart grids.” Computing in Science & Engineering 15, no. 4 (2013): 38–47.
32. Cuzzocrea, Alfredo, Il-Yeol Song, and Karen C. Davis. “Analytics over large-scale multidimensional data: the big data revolution!.” In Proceedings of the ACM 14th international workshop on Data Warehousing and OLAP, pp. 101–104. ACM, 2011.

33. Ericsson, Gran N. “Cyber security and power system communication essential parts of a smart grid infrastructure.” IEEE Transactions on Power Delivery 25, no. 3 (2010): 1501–1507.
34. Khurana, Himanshu, Mark Hadley, Ning Lu, and Deborah A. Frincke. “Smart-grid security issues.” IEEE Security & Privacy 8, no. 1 (2010).
35. Bejtlich, Richard. The practice of network security monitoring: understanding incident detection and response. No Starch Press, 2013.
36. Desai, Anish, Yuan Jiang, William Tarkington, and Jeff Oliveto. “Multi-level and multi-platform intrusion detection and response system.” U.S. Patent Application 10/106,387, filed March 27, 2002.
37. Mell, Peter, and Tim Grance. “The NIST definition of cloud computing.” (2011).
38. Burger, Eric W., Michael D. Goodman, Panos Kampanakis, and Kevin A. Zhu. “Taxonomy model for cyber threat intelligence information exchange technologies.” In Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, pp. 51–60. ACM, 2014.
39. Barnum, Sean. “Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX).” MITRE Corporation 11 (2012).
40. O’Toole Jr, James W. “Methods and apparatus for auditing and tracking changes to an existing configuration of a computerized device.” U.S. Patent 7,024,548, issued April 4, 2006.
41. Gerace, Thomas A. “Method and apparatus for determining behavioral profile of a computer user.” U.S. Patent 5,848,396, issued December 8, 1998.
42. Gu, Tao, Hung Keng Pung, and Da Qing Zhang. “Toward an OSGi-based infrastructure for context-aware applications.” IEEE Pervasive Computing 3, no. 4 (2004): 66–74.
43. Anderson, Douglas D., Mary E. Anderson, Carol Oman Urban, and Richard H. Urban. “Debit card fraud detection and control system.” U.S. Patent 5,884,289, issued March 16, 1999.
44. Camhi, Elie. “System for the security and auditing of persons and property.” U.S. Patent 5,825,283, issued October 20, 1998.
45. L. Widmer, The 10 Most Expensive Data Breaches | Charles Leach, 23-Jun-2015. [Online]. Available: http://leachagency.com/the-10-most-expensive-data-breaches/.
46. SINET Announces 16 Most Innovative Cybersecurity Technologies of 2016 | Business Wire, 19-Sep-2016. [Online]. Available: http://www.businesswire.com/news/home/20160919006353/en/SINET-Announces-16-Innovative-Cybersecurity-Technologies-2016.
47. C. Pettey and R. Van der Meulen, Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond, 01-Dec-2011. [Online]. Available: http://www.gartner.com/newsroom/id/1862714.
48. C. Heinl and E. EG Tan, Cybersecurity: Emerging Issues, Trends, Technologies and Threats in 2015 and Beyond. [Online]. Available: https://www.rsis.edu.sg/wp-content/uploads/2016/04/RSIS$_$Cybersecurity$_$EITTT2015.pdf.
49. Kavitha, T., and D. Sridharan. “Security vulnerabilities in wireless sensor networks: A survey.” Journal of information Assurance and Security 5, no. 1 (2010): 31–44.
50. B. Donohue, Hot Technologies in Cyber Security, Cyber Degrees, 03-Dec-2014.
51. Jeong, Jongil, Dongkyoo Shin, Dongil Shin, and Kiyoung Moon. “Java-based single sign-on library supporting SAML (Security Assertion Markup Language) for distributed Web services.” In Asia-Pacific Web Conference, pp. 891–894. Springer Berlin Heidelberg, 2004.
52. Gro, Thomas. “Security analysis of the SAML single sign-on browser/artifact profile.” In Computer Security Applications Conference, 2003. Proceedings. 19th Annual, pp. 298–307. IEEE, 2003.
53. Rees, Loren Paul, Jason K. Deane, Terry R. Rakes, and Wade H. Baker. “Decision support for cybersecurity risk planning.” Decision Support Systems 51, no. 3 (2011): 493–505.
54. T. Reuille, OpenGraphiti: Data Visualization Framework, 05-Aug-2014. [Online]. Available: http://www.opengraphiti.com/.
55. McKenna, S., Staheli, D., Fulcher, C. and Meyer, M. (2016), BubbleNet: A Cyber Security Dashboard for Visualizing Patterns. Computer Graphics Forum, 35: 281–290. doi:10.1111/cgf.12904

56. Linkurious, Linkurious - Linkurious - Understand the connections in your data, 2016. [Online]. Available: https://linkurio.us/.
57. T. Software, Business Intelligence and Analytics | Tableau Software, 2017. [Online]. Available: https://www.tableau.com/.
58. P. Corporation, Data Integration, Business Analytics and Big Data | Pentaho, 2017. [Online]. Available: http://www.pentaho.com/.
59. Norse Attack Map, 2017. [Online]. Available: http://map.norsecorp.com/$#$/.
60. Kaspersky Cyberthreat real-time map, 2017. [Online]. Available: https://cybermap.kaspersky.com/.
61. FireEye Cyber Threat Map, 2017. [Online]. Available: https://www.fireeye.com/cyber-map/threat-map.html.
62. Cyber Threat Map, FireEye, 2017. [Online]. Available: https://www.fireeye.com/cyber-map/threat-map.html.
63. L. SAS, data visualization Archives, Linkurious - Understand the connections in your data., 2015.
64. Interpol, Cybercrime / Cybercrime / Crime areas / Internet / Home - INTERPOL, Cybercrime, 2017. [Online]. Available: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
65. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.
66. Barber, Simon, Xavier Boyen, Elaine Shi, and Ersin Uzun. "Bitter to better: how to make bitcoin a better currency." In International Conference on Financial Cryptography and Data Security, pp. 399–414. Springer Berlin Heidelberg, 2012.
67. Swan, Melanie. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.", 2015.
68. IsecT Ltd, ISO/IEC 27001 certification standard, 2016. [Online]. Available: http://www.iso27001security.com/html/27001.html.
69. ISO, ISO/IEC 27001 - Information security management, ISO, 01-Feb-2015. [Online]. Available: http://www.iso.org/iso/iso27001.
70. IsecT Ltd, ISO/IEC 27032 cybersecurity guideline, 2016. [Online]. Available: http://iso27001security.com/html/27032.html.
71. Ware, Colin. Information visualization: perception for design. Elsevier, 2012.
72. Ramanauskait, Simona, Dmitrij Olifer, Nikolaj Goranin, Antanas enys, and Lukas Radvilavius. "Visualization of mapped security standards for analysis and use optimisation." Int. J. Comput. Theor. Eng 6, no. 5 (2014): 372–376.
73. Deep Node, Inc, Why Deep Node?, Deep Node, Inc., 2016. [Online]. Available: http://www.deepnode.com/why-deep-node/.
74. Deep Node, Inc, The Concept Deep Node, Inc., 2016. [Online]. Available: http://www.deepnode.com/the-concept/.

Jeffery Garae is a PhD research student with the Cyber Security Researchers of Waikato (CROW). As a PhD candidate, his research focus is on security visualization for mobile platforms and user-centric visualization techniques and methodologies. He is also interested in data provenance, threat intelligence, attribution, digital forensics, post-data analytics and cyber security situation awareness. He values the importance of security in ICT. He is the first recipient of to the University of Waikato's Master of Cyber Security (MCS) program in 2014. He is currently the Doctoral Assistant for the Cyber Security course at the University of Waikato. In the ICT and Security industry, he has a great number of years experience with Systems and Networks. As part of his voluntary contribution to the Pacific Island countries, he serves as a security advisor and an advocate to Cyber Security Situation Awareness.

Ryan K.L. Ko is Head of the Cyber Security Researchers of Waikato (CROW) and Senior Lecturer with the University of Waikato. With CROW, he established NZ's first cyber security lab and graduate research programme in 2012 and 2013 respectively. He is principal investigator of MBIE-funded (NZ$12.23million) STRATUS project. Ko co-established the NZ Cyber Security Challenge since 2014. His research focuses on returning data control to users, and challenges

in cloud computing security and privacy, data provenance, and homomorphic encryption. He is also interested in attribution and vulnerability detection, focusing on ransomware propagation. With 50 publications including 3 international patents, he serves on 6 journal editorial boards, and as series editor for Elsevier's security books. He also serves as the editor of ISO/IEC 21878 Security guidelines in design and implementation of virtualized servers. A Fellow of Cloud Security Alliance (CSA), he is a co-creator of the (ISC)2 CCSP certification—the gold-standard international cloud security professional certification. Prior to academia, he was a HP Labs lead computer scientist leading innovations in HP global security products. He is technical adviser for the Ministry of Justice's Harmful Digital Communications Act, NZ Minister of Communications Cyber Skills Taskforce, LIC, CSA and Interpol.