Visualising the Impact of Network Attacks on Business Processes using the DEViSE Framework

Huw Read[1,2,4], Konstantinos Xynos[1], Iain Sutherland[2,3], Mikhaila Burgess[2]
[1]University of South Wales, Pontypridd, CF37 1DL, UK
[2]Noroff University College, 4068 Kristiansand S, Vest-Agder, Norway
[3]Security Research Institute, Edith Cowan University, Perth, Australia
[4]Norwich University, Northfield, Vermont, USA

Abstract

Organisations rely on business processes to define their day-to-day commercial activities. Any disruption of these business processes will have a direct impact on the organisation's ability to perform its functions. In this paper we review the DEViSE Workbench, developed for network security visualisation, and demonstrate how business processes can be augmented with network security audit information to provide a precise understanding of how attacks impact the higher-level business roles. The paper outlines a prototype tool called BPEvents that can be used to highlight the severity of computer network attacks (CNA) in terms of the impact on business functions using the standard XPDL notation.

Introduction

Visualisation has become more important in the field of information security in recent years; techniques demonstrating interactive discovery and presentation [16] of problems and dedicated conferences such as VizSec [17] remain important resources whether analysing static data files [13] or process propagation [14]. As demonstrated by Fischer, Monsmann, Kein, Pietzko & Waldvogel [15] the ability to visualise both complex network connections and the information transmitted across a network can support the management of the network during a sustained cyber attack. There have been a number of highly publicized targeted attacks on Sony, PayPal, Visa, Mastercard and other private firms by so called "hacktivists" such as Anonymous and LulzSec [5]. Whilst these types of attacks are certainly not lacking in severity, they are still stereotypical of the "opportunistic" hacking style, i.e. perform reconnaissance of the target network and focus all effort on an insecure / vulnerable system. Such attacks have risen to prominence at the government level. In the UK for example, network security has featured quite prominently in a recent strategic defence and security review [1]. This document particularly emphasises the severity of attacks on networks ("...one of the four Tier One risks to national security..." [1]) and "...demonstrates the need for a flexible cyber security response" [1].

We have traditionally considered network attacks in very technical terms, i.e. as affecting computer servers (physical or virtual) on the network. There is a need for tools to start considering such events in terms of what is important to the business, i.e. in terms of business functions. One factor causing concern is the degree to which commercial, government and military organisations now rely upon digital systems to perform tasks that support their day-to-day operations or business functions [6].

Commercial organisations are not only increasingly finding it difficult to address the increasing variety of network attacks but also to understand the degree to which they can impact their core business processes [7]. When attacks start to have an effect on the production line, organisations take notice "...and integrate information protection practices into business processes" [7].

Read H., Xynos K., Sutherland I., and Burgess M., (2015), "Visualising the Impact of Network Attacks on Business Processes using the DEViSE Framework" Norsk Informasjonssikkerhetskonferanse 2015, 23-25 Nov 2015.

Military organisations echo similar problems. An attack on the UK Ministry of Defence supply chain, reportedly at “critical risk of failure” [18], could see overseas efforts severely disrupted. The network defence systems of the Norwegian Military, received in response to Norway’s involvement in the NATO led force in Libya [8], were described as being “...attacked daily, but it's not often we see such a comprehensive attempt at infiltration as this was. The trend is increasing, though, and the attackers are more goal-oriented” [8].

The term “goal-oriented” certainly indicates something more targeted than the opportunistic “hacktivist” approach. Goals for disrupting military may be to affect the delivery of aircraft fuel, resulting in a loss of aerial military capability. For industry, perhaps altering an order of components leading to an underproduction of products and competitors increasing their market share. As thoroughly critiqued by Goel & Chen [9] “... it is imperative to use cognitive aids while analyzing security risks.”

What any organisation, whether commercial, government or military, wants is to remain in continual operation such that its own business goals can be realised. If (or more accurately when) attacks occur, the business will ideally seek resilient methods of operation such that it can continue to function.

The rest of this paper is arranged as follows. Contribution discusses the focus of the paper, literature review provides an overview of business processes and their relation to security visualisation, business process visualisation describes how business processes are being visualised, core functionality of BPEvents highlights the main areas of the prototype application relevant to business process and cyber security, case study demonstrates usage of BPEvents within the DEViSE framework, integration with the DEViSE framework highlights how BPEvents data can be used with other visualisation tools and conclusions discusses what has been learnt in pairing the business process and cyber security fields.

Contribution

An issue when addressing the impact of a computer network attack on an organisation is to try and link the high-level conceptual business process activities and the low-level tangible technical computing systems together. Although the process activities still tend to be initiated, created and updated by people, more of these functions now occur on electronic systems of some description (desktop computer, tablet, smartphone, etc).

Mapping each business process activity directly onto its corresponding digital device, when some malicious activity takes place it is then possible to look at the consequences and disruption to business activities.

The prototype tool presented in this paper will visualise the impact of a selected event observed at the technical level, onto the business process tier, noting not only which activities are directly affected but also how subsequent activities are also under threat. Therefore this should address the following points: how business processes are vulnerable to cyber attack, is it possible to identify critical systems, understanding the implications in terms of lost capability and understanding the knock-on effect to additional business activities.

Literature Review

There are a number of difficulties an organisation can face as a result of a network intrusion. In terms of business process, availability and integrity are usually considered to be more important that confidentiality. The process has to be available and operating

for the business process to function. Work presented by Goudalo & Seret [10] demonstrate how the engineering of security information systems can be formalised into business processes by going through a step-by-step approach with UML modelling. The authors used UML2 activity diagrams so those needing to implement other methods such as the business process model and notation (BPMN) [20] would only need a translation layer for converting between standards.

For organisations with rapidly changing business processes, particularly those that have grown 'organically' over a longer period of time, the way in which the physical network supports business functions may not be immediately apparent until problems arise. This could lead to operational delays when handling an incident; if the IT infrastructure is not well defined in terms of how it supports the specific functions of the business, mitigation strategies cannot be immediately deployed.

Previous work has examined how security goals may be expressed at the business process level. The work by Wolter, Menzel, Schaad, Miseldine & Meinel [11] looks at annotating business processes with high-level security goals and then how they may be transformed into real access control and security policies, which may be deployed on a network. However, addressing the impact of attacks on a business process is outside the scope of their work. Wolter et al. [11] do mention that business process experts need to collaborate with security experts in such a way that new augmented views of the business processes are demonstrated to decision-makers such that mission-critical functions can be dealt with in a prioritised fashion.

Similar work has been presented by D'Amico & Salas [12] whereby mission critical tasks are mapped out in different views. Operational missions are tied into the mission critical tasks, which can then be attached to different types of assets. These different views allow for the mapping of assets to alerts and vulnerabilities which provide situational awareness to the user. The mission critical example presented by D'Amico & Salas [12] is of particular note and would complement the approach taken in this paper.

On the technical side of security visualisation, cyber security protection mechanisms such as anti-virus, intrusion detection systems and firewalls produce logs which typically retain metadata of events they have observed. Such audit data can grow rapidly on busy corporate networks and can be difficult to read individually given the quantity of information. Colour can be added to log files to help make certain events stand out to the analyst (Fig. 1.).

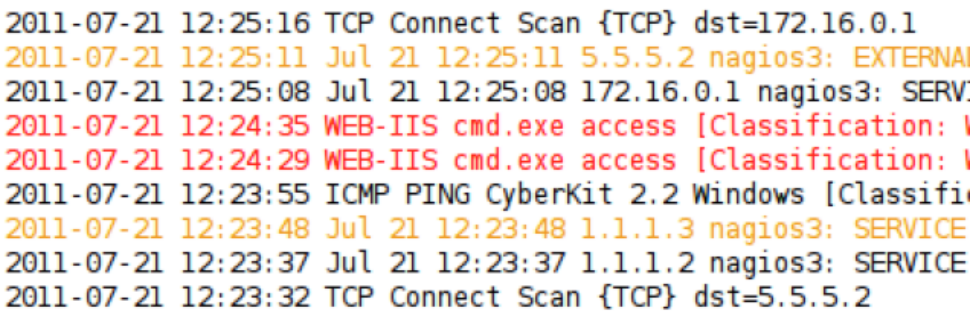

Figure 1: Colours representing severity, logs truncated for brevity

The specialist field of security visualisation has developed considerably further than the use of colour coded log files. There are several dedicated books on the subject and a number of different visualisation techniques have emerged over the years [3-4].

Fig. 2 shows security tools demonstrating geographical, temporal and logical data types. Visualisation tools are typically categorised as either monitoring, analytical, or

informational. Monitoring tools are designed to continually refresh and show new patterns as they occur, analytical tools encourage correlation and data fusion whilst informational tools describe very few, if not a single, attack in verbose detail [15].

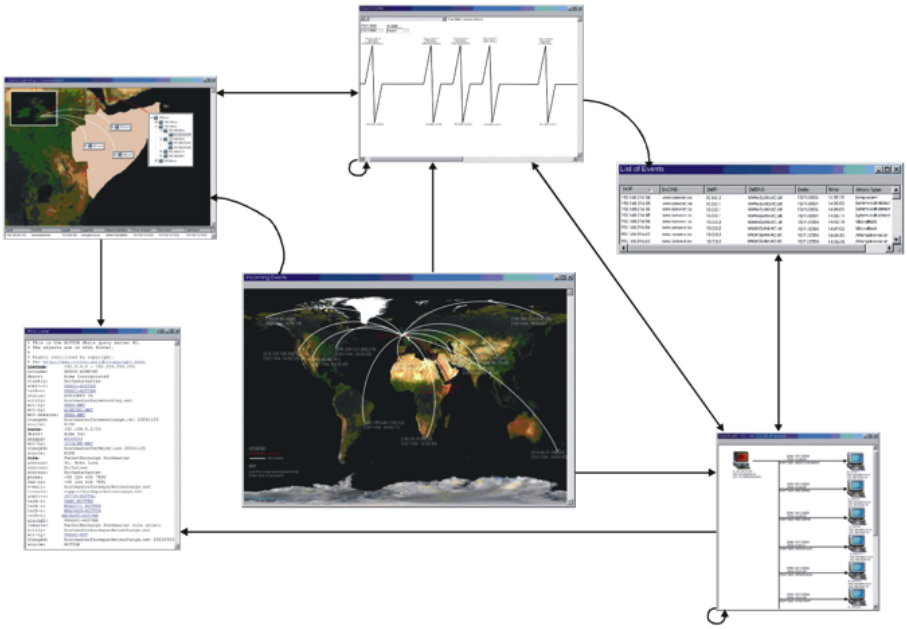

Figure 2: Different security visualisation paradigms

These different classifications may appear in the same security visualisation application. Tools such as TNV and Sawmill provide different views in the one application allowing a user to visually data-mine through logs of events. The difficulty with this approach is that the applications do not readily exchange information for further visualising; interesting patterns in one application cannot readily be passed into another tool.

Architectures such as the DEViSE framework by Read, Xynos & Blyth [2] offer greater interactivity between security visualisations. By incorporating to the principles of the UNIX Philosophy [19] individual applications exhibit specific visualisation types (scatter graphs, bar charts, geographic maps, etc). Hotspots [2] highlight collections of data in a visualisation which can be manipulated and passed as input to other visualisations to allow rapid analysis and understanding of network events.

Overall, looking at the areas of business processes and cyber security demonstrate a need for providing different visualisations for different users and being mindful of their respective needs. For example, a network defender needs to understand to what degree their network has been compromised and would benefit from a suite of tools to enable comprehension of IP / MAC addresses, user names and other technical details identified by security hardware and software. Managers, on the other hand, have a different, but complementary role, needing the ability to understand the impact of the attacks on business functions, and then making decisions as to how the organisation can best respond, adapt and continue to operate.

Business Process Visualisation

Businesses and organisations have a certain way of operating. This operation can be captured and streamlined through the modeling of business logic.

When modelling business logic, a domain expert will document the activities in an abstract model such as a business process. A number of detailed levels will be considered which can help depict an organisation's operations with the use of models or through visual cues. Domain experts also rely highly on IT experts within the organisation to bridge the gap between models and actual implementations, current and projected.

Fundamentally, a business process is an activity diagram showing how a business function is executed from initiation to conclusion. The capture of such information is quite a manual and time consuming task and will be more complex in large organisations. A number of business process modeling languages exist to help with the task of capture, processing and distribution of such information. The current standard is the Business Process Model and Notation (BPMN) system [20], maintained by the OMG consortium. BPMN can be expressed in a visual manner in the form of a Business Process Diagram (BPD).

As can be seen in Fig. 3, a number of standard elements are used; flows, connectors and artifacts all come together to describe a business process. In this particular example, the diagram represents the procurement process for obtaining new goods / services. It should be emphasised that BPMN supports process management to technical and non-technical users. However, BPMN is not a way of storing or transmitting such information electronically. Serialisation of BPMN comes in the form of the "XML Process Definition Language" (XPDL) [21].

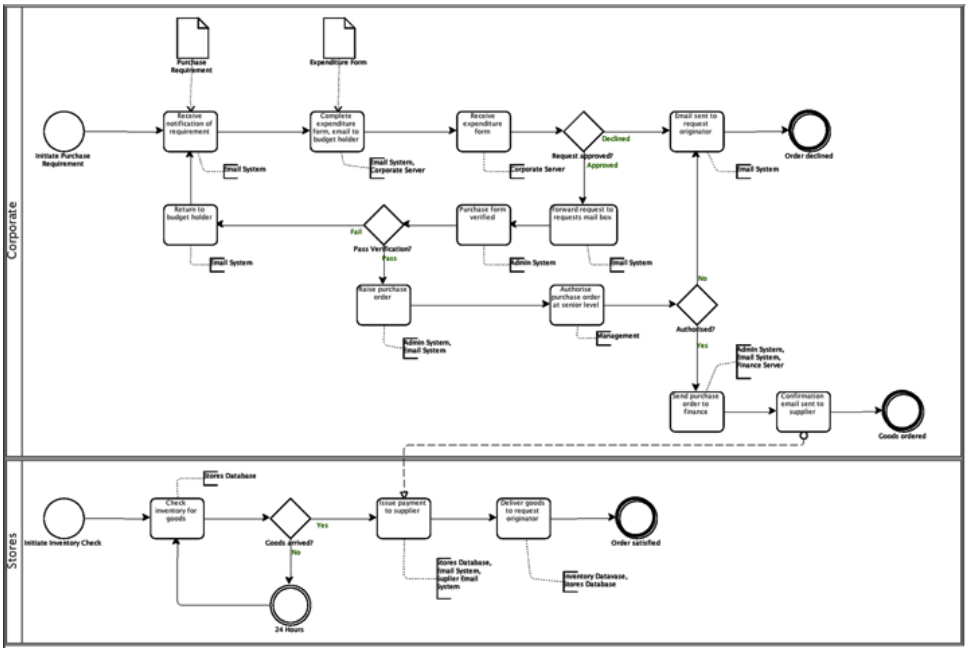

Figure 3: A procurement business process diagram (BPD)

Core Functionality of BPEvents

The tool presented in this paper is an interactive application with two methods of use; a high-level overview of CNA impact on a business process and a deep-dive detailed mode allowing an analyst the opportunity to further their investigations. The functionality of this tool, named BPEvents, is outlined in Figures 4 and 5.

At its core, BPEvents imports standard XPDL files which are then parsed and visualised, creating a blueprint of the business process. An associated network data file

is imported and the two are cross-referenced to identify IP addresses in use by the business process.

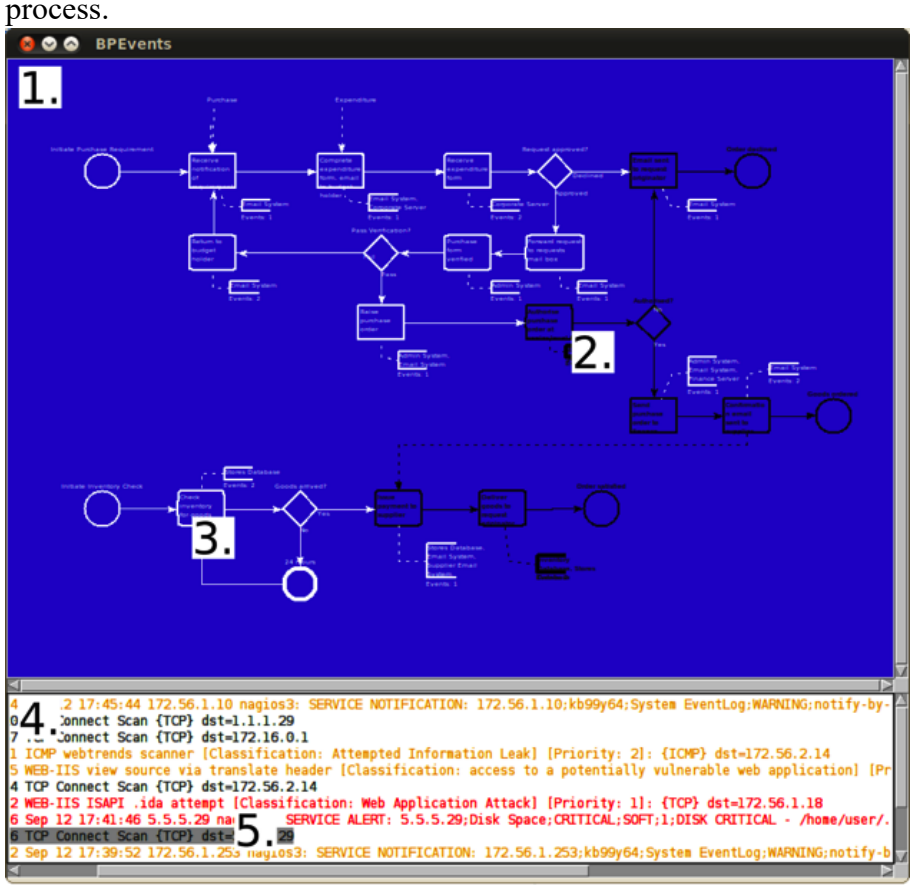

Figure 4: An overview of BPEvents

The main components of the tool in the overview mode (Fig. 4) are as follows. 1. The overall, at-a-glance view permits an analyst to see what areas of the overall business process are affected by the attack. 2. Colour is used to denote the seriousness of the attack as defined by the intrusion detection system feed. 3. White is the default color, indicating these activities/systems are unaffected by the visualised network attack and can continue as normal. 4. The pane has a running feed from the intrusion detection sensors, providing further deep-dive capabilities for an analyst. 5. Selecting an attack (highlighted in grey) locks the event on the overview pane (1.) disabling the live updates, allowing an analyst further opportunity to examine the impact of the attack.

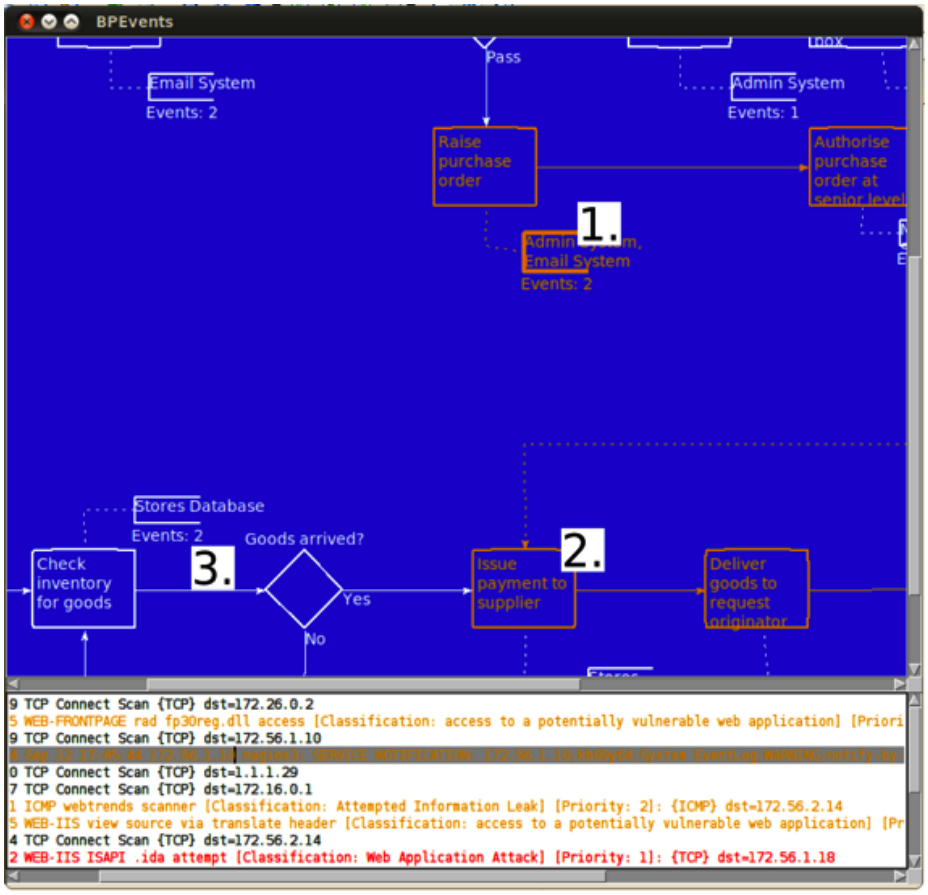

Figure 5: BPEvents - "deep-dive" view

The main components of BPEvents in the deep-dive view (Fig. 5) are as follows. 1. The system or systems that are the recipient of the attack (one computing device may be responsible for several activities) are emboldened, effectively visualising the activity originally affected by the attack. 2. Further business activities that are affected are coloured the same as the attacked system (1.) but are not emboldened. This demonstrates that, although the attack did not directly harm the underlying computing device in this activity, it is affected by proximity in the business process workflow. 3. Event counters will increment alongside each activity as attacks occur.

Case Study: Determining the Greater Impact

Security visualisation assists the analyst by taking log files, alerts and other data sources and correlating them into fewer sources to provide, overall, aggregated information. Unfortunately, one of the shortfalls of this traditional approach is that analysts are disconnected from the business processes that would be affected as a consequence of the attacks they are analysing.

```
2011-07-21 12:56:43 SQL generic sql update injection attempt:
[Classification: Web Application Attack] [Priority: 1]: {TCP}
dst=5.5.5.1
2011-07-21 12:56:34 SQL generic sql update injection attempt:
[Classification: Web Application Attack] [Priority: 1]: {TCP}
dst=5.5.5.2
```

Figure 6: Two SQL injection attacks with different IP addresses

Consider the two almost indistinct log entries in Fig. 6. A SQL injection attack has taken place on two web servers with IP addresses 5.5.5.1 and 5.5.5.2. Apart from the IP, the attack is identical, and the intrusion detection system has logged it as a critical priority 1. We need to determine which is more critical and requires immediate attention.

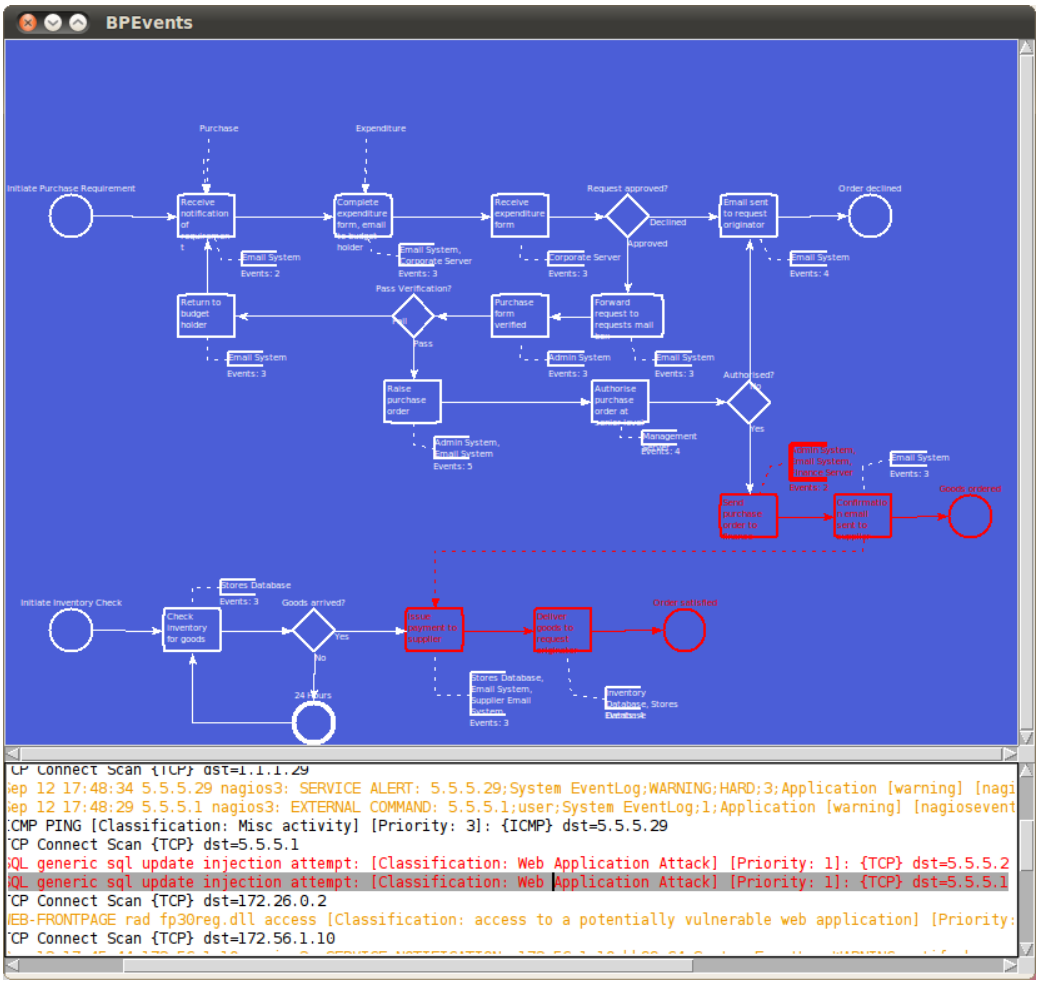

Figure 7: Attack impact on a business process model - attack 1

The impact of this SQL injection attempt cannot be displayed with conventional network analysis visualisations; the two attacks are just too similar. If the business process tier is added to the decision making process, tying the business activities and IT infrastructure together, a different result is seen.

By examining the differences between the two attacks on BPEvents, the resultant visuals, depicted in Figures 7 and 8, help identify, in terms of this particular business process, which attack has the greater impact. It appears the second attack, shown in Fig. 8, affects a greater percentage of the business process, and, therefore, should be

addressed first. By visualising CNA data in this fashion, an organisation is better equipped for business continuity.

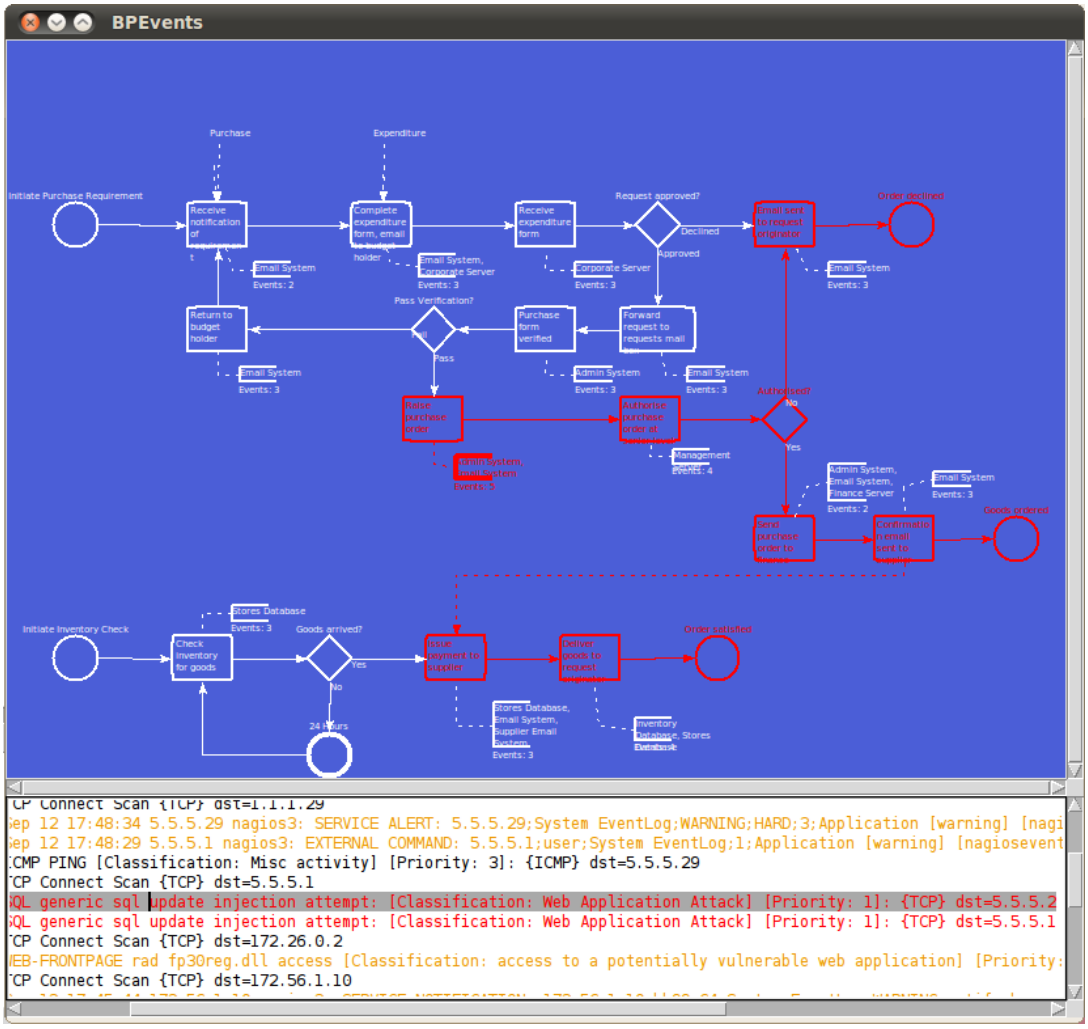

Figure 8: Attack impact on a business process model - attack 2

Integration with the DEViSE Framework

By integrating BPEvents within the existing DEViSE framework, other visualisation tools can be used recursively to explore the data. Analysts can use the information presented from this business process level and further visualise the CNA events in other tools at a logical / network level. Interacting with the hotspots in this tool [2] will provide a list of compatible applications which can receive data directly from BPEvents.

The analyst's use of visualisation tools is tracked by the system using the 'History Manager' [2], which enables the operator to trace back through their analysis to review the investigation. The analyst's view may look similar to Fig. 9, multiple visualisation tools, each pictorially different but all working and interacting with the same data source.

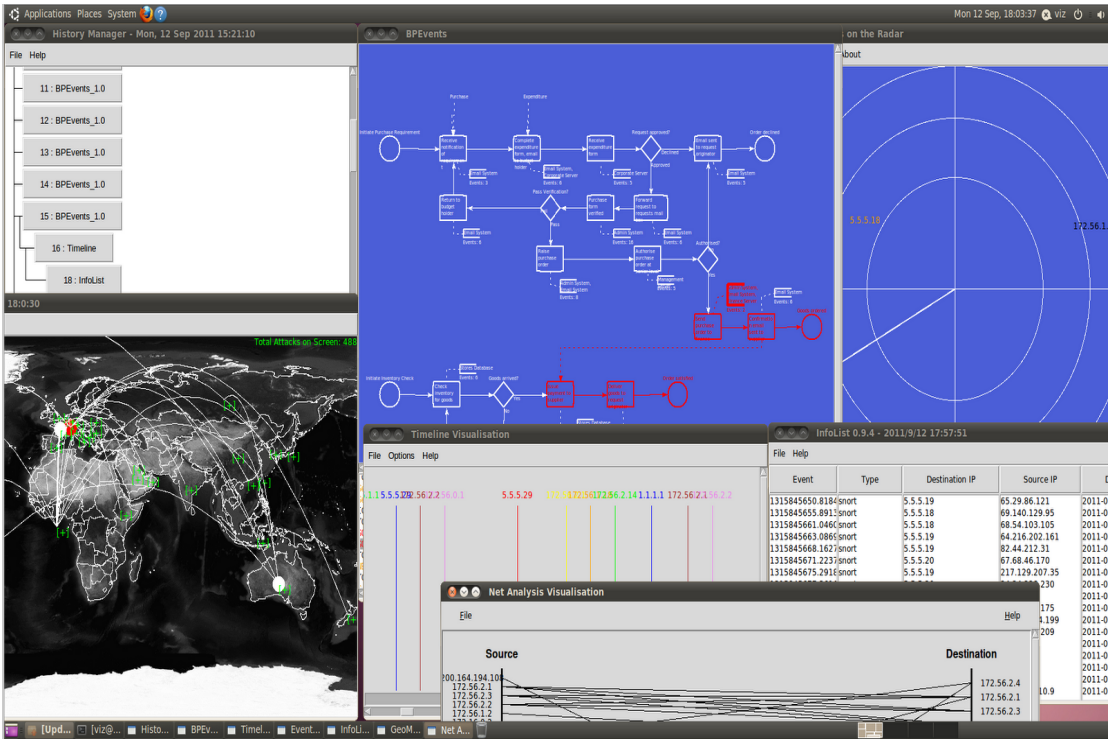

Figure 9: The DEViSE analyst's workbench

Conclusions

This paper has highlighted a prototype suite of tools, which bridge the gap between the technical complexities and impact of events against an organisation's modeled business processes. Future work will investigate the ability to automatically enumerate a network to capture information on the systems present, as well as the way in which the business processes are supported by the underlying IT infrastructure. This would enable those organisations that have rapidly changing infrastructure to observe the changes in their business processes, in addition to any attempted attacks or successful intrusions on their systems.

Automatic response to support the restoration of business processes is another area worth examining in the future. It may be that an organisation has multiple physical sites and redundant/backup infrastructure, which could be better utilised. This future system could present the user with options to move vital business process activities between systems if parts of the underlying IT infrastructure have been compromised.

Overall, the use of the BPMN standard has been incorporated with technical network data demonstrating the mapping between the logical and the managerial layers in an organisation. By visualising technical computer network attack data across business processes, it has been successfully shown that further information can be obtained from CNA impact, leading to greater understanding, situational awareness and more appropriate mitigation.

References

[1]Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, HM Government, Oct 2010.

[2]Read H., Xynos K., Blyth A., Presenting DEViSE: Data Exchange for Visualizing Security Events, IEEE Computer Graphics and Applications, vol. 29, no. 3, pp. 6-11, May/June 2009

[3]G. Conti, Security Data Visualization, No Starch Press; September 2007

[4]R. Marty, Applied Security Visualisation, Addison Wesley Professional; August 2008.

[5]BBC Technology, Q&A Lulz Security, Accessed 26th July 2011, http://www.bbc.co.uk/news/technology-13671195

[6]Judd, T., 9th August 2011, "MOD Supply Chain at Risk of Collapse", Politics Section, Independent Newspaper, Accessed 7th September 2011, http://www.independent.co.uk/news/uk/politics/mod-supply-chain-at-risk-of-collapse-2340150.html

[7]Barwick, H., Sony must learn from PlayStation Network attacks: Sophos, Norton, Accessed 1st August 2011, http://www.computerworld.com.au/article/388162/sony_must_learn_from_playstation_network_attacks_sophos_norton/

[8]Dunn, J., Norweigan Military Admits to March Cyberattack, Accessed 1st August 2011 http://www.csoonline.com/article/682785/norwegian-military-admits-to-march-cyberattack.

[9]Sanjay Goel, Vicki Chen, Can business process reengineering lead to security vulnerabilities: Analyzing the reengineered process, International Journal of Production Economics, Volume 115, Issue 1, September 2008, Pages 104-112.

[10] Goudalo, W.; Seret, D., The Process of Engineering of Security of Information Systems (ESIS): The Formalism of Business Processes, Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on Emerging Security Information, Systems and Technologies, June 2009.

[11] Christian Wolter, Michael Menzel, Andreas Schaad, Philip Miseldine, Christoph Meinel, Model-driven business process security requirement specification, Journal of Systems Architecture, Volume 55, Issue 4, Secure Service-Oriented Architectures (Special Issue on Secure SOA), April 2009, Pages 211-223.

[12] D'Amico, A.; Salas, S.; , Visualization as an aid for assessing the mission impact of information security breaches, DARPA Information Survivability Conference and Exposition, 2003. Proceedings , vol.2, no., pp. 18- 20 vol.2, 22-24 April 2003.

[13] G. Conti, E Dean, M. Sinda and B. Sangster, Visual Reverse Engineering of Binary and Data Files, Proceedings of the Workshop on Visual Computer Security, Spinger, 2007

[14] Y. Xia, K Fairlands and H Owen, Visual Analysis of Programs Flow Data with Data Propagation., Proceedings of the Workshop on Visual Computer Security, Spinger, 2007.

[15] F Fischer, F Monsmann, D A Kein, S Pietzko and M Waldvogel, Large-Scale Network Monitoring for Visual Analysis of Attacks, Proceedings of the Workshop on Visual Computer Security, Spinger, 2007

[16] 1. Garfinkel S.L. Forensics Visualizations with Open Source Tools, 2013. http://simson.net/ref/2013/2013-11-05_VizSec.pdf

[17] IEEE VizSec 2015, 2015. Accessed 1st October 2015, http://vizsec.org/

[18] Curtis, P. Defence supply chain could fail British forces, say MPs. The Guardian. 2011. Accessed 1st October 2015, http://www.theguardian.com/uk/2011/aug/19/military-supply-chain-risks-failure

[19] Kernighan, Brian W. Pike, Rob. *The UNIX Programming Environment.* 1984. viii

[20] Business Process Model and Notation, Object Management Group, 2015. Accessed 1st October 2015, http://www.bpmn.org
[21] XML Process Definition Language, Workflow Management Coalition, 2015. Accessed 1st October 2015, http://www.xpdl.org/