Use of Organisational Topologies for Forensic Investigations

George Grispos
Lero – The Irish Software
Research Centre
Ireland
george.grispos@lero.ie

Sorren Hanvey
Lero – The Irish Software
Research Centre
Ireland
sorren.hanvey@lero.ie

Bashar Nuseibeh
Lero – The Irish Software
Research Centre & Open University
Ireland and UK
bashar.nuseibeh@lero.ie

ABSTRACT

In today's highly regulated business environment, it is becoming increasingly important that organisations implement forensic-ready systems and architectures to aid the investigation of security incidents and data breaches. Previously, different solutions have been proposed for implementing forensic readiness within organisations. One of these solutions is that organisations implement an *organisational structure* that takes into consideration digital forensics by establishing roles and responsibilities to assist with investigations. However, no previous research has defined how this can actually be accomplished within an organisation. In this paper, we put forth the idea of using the *topology* of an organisation's structure to define the roles and responsibilities to assist with handling a forensic investigation. In the past, the role of topology has been examined from various perspectives, including software engineering. We draw on this previous research and use the topological properties of *containment*, *proximity* and *reachability* in order to define a representation of the organisational structure that takes into consideration digital forensics. For example, topology can be used to express and provide a context regarding the location of assets that need to be investigated, as well as the individuals, whose assistance is required to investigate such assets. Furthermore, knowing the topology of an organisation's structure can also assist investigators identify stakeholders that could be of interest to an investigation, based on their relationship to the asset(s) under investigation.

CCS CONCEPTS

• **Applied computing** → **Computer forensics**; • **Social and professional topics** → *Computer crime*;

KEYWORDS

Topology, Forensic Readiness, Organisational Structures

ACM Reference Format:
George Grispos, Sorren Hanvey, and Bashar Nuseibeh. 2017. Use of Organisational Topologies for Forensic Investigations. In *Proceedings of 1st International Workshop on Software Engineering and Digital Forensics, Paderborn, Germany, September 4, 2017 (SERF '17),* 4 pages.
https://doi.org/10.1145/3121252.3121253

SERF '17, September 4, 2017, Paderborn, Germany
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5156-0/17/09…$15.00
https://doi.org/10.1145/3121252.3121253

1 INTRODUCTION

In today's highly regulated business environment, it is becoming increasingly important that organisations have digital forensics capabilities to investigate security incidents and data breaches. When incidents and breaches do occur, organisations usually respond by conducting a forensic investigation to establish the root cause of the incident and how it could be prevented in the future [9]. In order to undertake an investigation, forensic investigators rely on the availability of residual data from systems, affected by the incident, as well as any supporting systems [7, 14, 15, 20].

However, such data might not always be available for a variety of reasons including limited data retention times, a lack of extraction capabilities and the costs associated with conducting such investigations [11, 25]. Hence, there have been an increasing number of calls from industry [22, 26] and academia [23, 27] for organisations to implement forensic-ready systems and infrastructure, with the aim of maximising their use of digital evidence, whilst minimising the cost of any such investigation. In the past, researchers have explored numerous solutions for implementing forensic readiness within organisations. These include implementing policies and processes [10, 23], aligning systems with forensics objectives [21] and ensuring that the human resources of an organisation contribute towards investigations [27, 29].

One of the forensic readiness solutions proposed in the literature is establishing and implementing an organisational structure that takes into consideration digital forensics [12]. The idea behind this approach is that organisations establish roles and responsibilities to assist with handling forensic investigations within their organisations [5, 12, 13]. However, no previous research has defined how this can actually be accomplished within an organisation.

In this paper, we propose the idea of using *organisational topology* to assist with the handling of a forensic investigation. In the past, the role of topology has been examined from various perspectives, including software engineering [17], network connections [1] and cyber-physical systems [18]. We also use previous research and concepts [3, 24] to inspire our approach and propose that organisational topologies are a richer representation of an organisational structure, i.e. the relationships between stakeholders and assets. From a forensic readiness perspective, topology can be used to express and provide a context regarding the location of assets that need to be investigated, as well the individuals, whose assistance is required to investigate such assets. Furthermore, knowing the topology of an organisation's structure can also assist investigators identify stakeholders that could be of interest to an investigation, based on their relationship to the asset(s) under investigation.

The rest of this paper is structured as follows. Section 2 introduces topology and explains how it can assist with the identification of relevant assets and stakeholders in an organisational structure. Section 3 presents the use of topology awareness when addressing different forensic challenges faced by organisations. Section 4 concludes the work and presents directions for future research.

2 PROPOSED CONCEPT

This Section introduces topology and organisational structures and explains how topology can be used within organisational structures.

2.1 Topology

Pasquale, et al. cite Euler's [6] definition of topology as "the study of shapes and spaces, including properties such as connectedness and boundary" [17]. Topology has been examined from various perspectives and in different research domains. Mylopoulos and Pavlidis [16] use topology to define spaces and discuss the notions of dimension, connectivity and order of connectivity. Similarly, Castro, et al. [1] constructed a representation of topological network connections in order to manage large-scale distributed systems. The role of topology has also been investigated in the software engineering community. For example, Pasquale, et al. [17] argue that a key characteristic for engineering adaptive security is the topology of the operational environment. These researchers define the structure of space in terms of a *physical topology* (location of physical objects) and a *digital topology* (location and configuration of digital objects), as well as the relationships among the elements they represent including containment, proximity and reachability [17]. In later work, Pasquale, et al. [18] propose representing the topology of digital and physical spaces in smart buildings as an approach for supporting the identification of adaptive security requirements. However, while previous research has examined the use of topology in these various domains, no previous work has examined it from an organisational structure perspective.

2.2 Organisational Structures

Organisational structures are concerned with the relationships between the various members of an organisation [4]. These structures can tell us within an organisation, "who has the resources, who talks to whom, who is accountable for what, what you can do on your own and what you must do with others" [4, 30].

From a digital forensics perspective, researchers have discussed how organisations can establish and prepare an organisational structure that will support digital forensics efforts [5, 12]. Grobler and Louwrens [12] argue that an organisational structure should define the roles that will handle forensic investigations in an organisation and include a clear segregation of duties between the team conducting a forensics investigation and the team responsible for security. Elyas, et al. [5] add that an organisational structure that takes digital forensics into consideration is likely to encourage forensic readiness within organisations. Similarly, Reddy and Venter [21] state that a forensic-driven organisational structure is needed in order to define roles and coordination between various investigation functions within an organisation. While these researchers have proposed establishing a forensics-enabled organisational structure, no solution has been proposed on how this can actually be achieved.

2.3 Organisational Topology

Taking into account organisational topology, could provide a richer representation of the structure within an organisation. This could then allow forensic investigators to conduct enhanced investigations and also aid the engineering of forensic-ready systems [8]. In the context of this paper, we extend the definition of topology presented in Section 2.1 to not only the study of shape and spaces, but also the structure in which these shapes and spaces reside. We propose three types of organisational topology that are relevant to digital forensics: *stakeholder topology*, *cyber topology* and *workflow topology*. We use Figures 1a and 1b to discuss these in more detail.

Stakeholder Topology. Figure 1a presents a topological representation of the stakeholder structure for a segment of an organisation. The organisational structure consists of different stakeholders in the organisation. The stakeholder topology represents the stakeholder's role and relationships within the organisation, as well as their lines of accountability. In this example, a *containment* relationship exists if the stakeholder, S_1, has a direct relationship to another hierarchically lower stakeholder, S_2, (e.g. the Head of Security (HOS) has a direct relationship to the Security Manager (IS) and can authorise them to perform a task). A *proximity* relationship, $ST_{\mathrm{p}}(S_1, S_3)$, identifies that a stakeholder, S_1, has a relationship to a hierarchically lower stakeholder, S_3, through one of their subordinates, S_2, i.e., $ST_{\mathrm{c}}(S_1, S_2)$ & $ST_{\mathrm{c}}(S_2, S_3)$. For example, the Chief Technology Officer (CTO) can instruct the Security Incident Response Team (SIRT) to investigate an incident through the Head of Security. A *reachability* relationship, $ST_{\mathrm{r}}(S_1, S_4)$, expresses if a stakeholder, S_1, has a relationship to a hierarchically lower stakeholder, S_4, that is not a direct subordinate, but through external intervention. For example, the Head of Information Technology (HoIT) can request, through the Head of Security (HoS), that the Security Incident Response Team (SIRT) undertake an investigation. While the HoIT can initiate this request, the SIRT cannot request the HoIT as it does not have a reachability relationship.

Cyber Topology. Figure 1b, shows a representation of the *cyber topology* for a segment of the infrastructure of an organisation. Objects (Assets) within a cyber topology can include terminals, servers (File Server 1 (FS_1) and File Server 2 (FS_2)), virtual machines, data (Credit Card Information (CC) and Customer Data (CD)), applications (App) and processes that reside within physical machines. The cyber topology can be used to represent the relationships among these objects and how they are connected, from the perspective of a forensic investigation. For example, a *containment* relationship defines the files, data or applications stored within a physical machine. In Figure 1b, containment relationships exists between FS_1 and Credit Card (CC) information. This is because CC information is stored within FS_1. Similarly, a containment relationship exists between FS_2 and Customer Data (CD) stored on this physical machine. In terms of Figure 1b, a *proximity* relationship represents the fact that the application (App) and Credit Card Information (CC) are both stored within FS_1. In this sense, *proximity* represents the relationship between objects co-located on the same physical machine. A *reachability* relationship expresses if two or more objects are virtually connected, either through a local or a remote connection between physical machines. For example, debt collectors in the Sales unit can access the Credit Card information (CC) stored in FS_1 because FS_1 accepts incoming local network connections

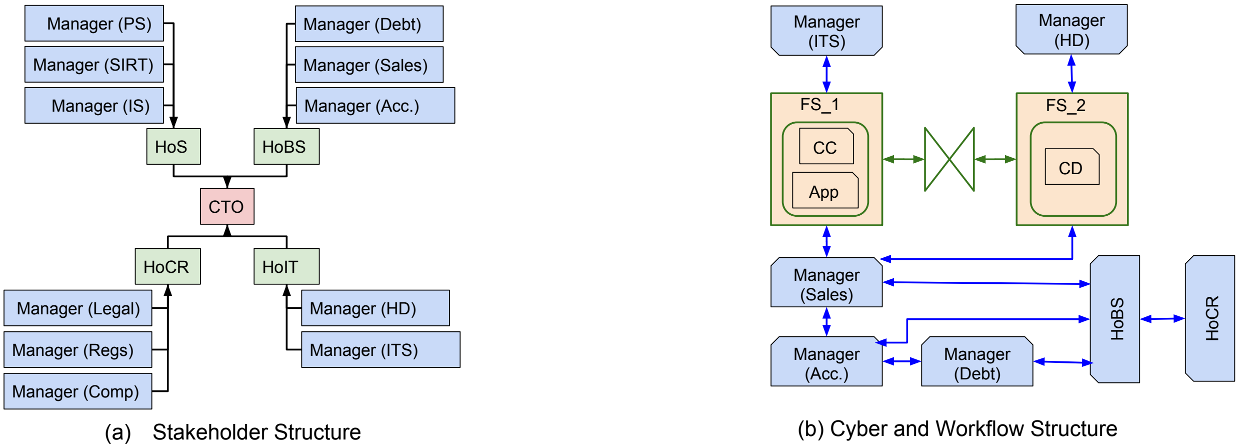

Figure 1: Type of Topology

from this group of users. Likewise, users in the Sales unit can only access the application (App) running on FS_1 if there exists the relevant permissions to execute this application.

Workflow Topology. Figure 1b also shows a representation of the *workflow topology*, within a segment of an organisation. The workflow topology is a topological representation of the structure of workflow within an organisation. It consists of the different stakeholders, assets and the access privileges the stakeholders have over the assets. An analysis of an organisation's workflow topology can allows us to identify how different data collection tasks can be performed based on who can access what data. Given a stakeholder S_1 and an asset A_1, a *containment* relationship, $WT_c(S_1, A_1)$, exists between the stakeholder and the asset, if the stakeholder has direct access privileges over the asset. For example, the manager of IT services (Manager(ITS)) has direct access to the application data (App) stored on File Server 1 (FS_1) in order to perform their tasks. A *proximity* relationship, $WT_p(S_1, A_1)$, exists if a stakeholder shares a proximity relationship, $ST_C(S_1, S_2)$, with another stakeholder, S_2, that has a containment relationship, $WT_C(S_2, A_1)$, to the asset. For example, the Head of Business Services (HoBS) requesting customer data from the Manager(Sales). A *reachability* relationship, $WT_r(S_1, A_1)$, expresses whether the stakeholder has a reachability relationship, $ST_r(S_1, S_2)$ with a stakeholder S_2, that has a containment relationship, $WT_C(S_2, A_1)$, to the asset. In Figure 1b, the Head of Compliance and Regulation (HoCR) can request customer data from the Manager(Sales) by sending a request through the Head of Business Services (HoBS).

3 TOPOLOGY AWARENESS

Topology awareness refers to the insights derived from the analysis of different topological representations of organisational structures. The awareness of the different topologies defined in Section 2.3, could assist in addressing both digital forensics and organisational structure challenges.

3.1 Enhance Organisational Forensic Readiness

Researchers have previously identified the need for organisations to establish and implement an organisational structure that takes into consideration digital forensics [12]. Making use of the different organisational topologies described in Section 2.3, it is possible to represent and analyse the different organisational structures. Stakeholder topology can be used to describe the relationship between different roles within the organisation. It can also be used to describe the chain of accountability within an organisation, allowing an investigator to identify the boundaries of an incident. The boundaries of an incident would then define the set of stakeholders, that are affected by, or accountable for an incident.

The workflow topology describes the relationship between different stakeholders and the assets within the organisation. It can be used to define the different paths an instruction can take before execution. This could be used to identify where an incident-causing instruction has originated and what is the best source of data for an investigation to examine that incident. For example, instructions that perform a task over the credit card data (CC) stored on FS_1, can either come directly from the Sales team or from another team, through a request submitted to the Sales team. In case of an investigation, data can be requested from these teams and analysed in order to identify if the team is involved in the incident.

Cyber topology can be used to describe how different assets communicate with each other. The use of cyber topology to identify the path of an attack has been highlighted in previous research [19]. Therefore, information enriched from a cyber topology could be paramount to identify how an incident propagated through a particular system or an organisation.

3.2 Supporting Forensic-Enabled Structures

While previous research has identified the need for organisational structures to take into consideration digital forensics, this is likely to require a significant reconfiguration of an organisation's existing structure. Previous research has shown that organisations rarely succeed in making changes in their structure [2]. Furthermore, the theories and approaches to manage such changes are often contradictory [28], therefore making the adoption of the approach more challenging. We envision that the same challenges would apply when enforcing a forensics-enabled organisational structure. The use of topology could be used to mitigate the above concerns, while also achieving this goal. Awareness of organisational topology can allow for the assignment of roles and responsibilities for investigations without drastically changing the existing organisational structure. The role and responsibility of investigating an incident related to an asset will likely fall to the stakeholder who has the appropriate relationship(s) to the particular asset. Using cyber topology, we can identify the assets that need to be investigated if a related asset is compromised. Furthermore, workflow topology relationships associated with these assets can allows us to identify the stakeholders with access to the required data that can enhance an investigation. Stakeholder topology allows an investigator to identify the stakeholder with the appropriate hierarchical level to conduct an investigation. The efficiency of a stakeholder to conduct an investigation is based on the cost incurred by them to gain access to relevant data. We can assign a cost to each relationship exploited in order to access the data, increasing from containment through proximity to reachability based on the number of intermediary stakeholders involved. We then assign responsibility to the stakeholder with the lowest cost to investigate an asset.

3.3 Changes in Organisational Structures

Organisations are often in a state of change, adapting to various triggers. For example, as an organisation grows, the definition of stakeholder roles will also likely change. Roles are also likely to be consolidated and separated regularly. This could limit the effectiveness of an established forensics-enabled organisational structure. The use of topology could allow an organisation to automate the allocation of roles and responsibilities. Automating the analysis of a changing topology and then reconfiguring security policy has been previously discussed in smart buildings [18]. Additionally, topology awareness can inform and drive structural change. It would allow an organisation to identify if an existing asset cannot be investigated. In other words, if an asset does not share a reachability relationship with a stakeholder, then this asset cannot be investigated. In this scenario, the topology could be used to inform the allocation of access privileges to an appropriate stakeholder, who can then drive the investigation.

4 CONCLUSIONS AND FUTURE WORK

In this paper, we have proposed the idea for using topology to express an organisational structure that takes into account digital forensics. We propose the use of topological properties such as containment, proximity and reachability to define a representation of such an organisational structure. From a forensic readiness perspective, topology can be used to provider a richer context regarding the location of assets that need to be investigated, as well as the individuals whose assistance is required to investigate such assets. Furthermore, knowing the topology of an organisation’s structure could also also assist investigators identify stakeholders that may be of interest to an investigation, based on their relationship to the asset(s) under investigation. We anticipate that our approach will be of interest to the software engineering community, when attempting to engineer forensic-ready software systems, as well as the digital forensic community. Future work will further investigate the use of topology to express forensic-enabled organisational structures and their role in engineering forensic-ready systems.

ACKNOWLEDGMENTS

This research is partially supported by SFI Grant No. 13/RC/2094 and ERC Advanced Grant. No. 291652 (ASAP),

REFERENCES

[1] Miguel Castro, Peter Druschel, Y Charlie Hu, and Antony Rowstron. 2003. Topology-aware routing in structured peer-to-peer overlay networks. In *Future directions in distributed computing*. Springer, 103–107.

[2] Massimo G. Colombo and Marco Delmastro. 2002. The Determinants of Organizational Change and Structural Inertia: Technological and Organizational Factors. *Journal of Economics & Management Strategy* 11, 4 (2002), 595–635.

[3] Robert Crook, Darrel Ince, and Bashar Nuseibeh. 2005. On modelling access policies: Relating roles to their organisational context. In *Requirements Engineering, 2005. Proceedings. 13th IEEE International Conference on.* IEEE, 157–166.

[4] Lex Donaldson. 1999. The normal science of structural contingency theory. *Studying Organizations: Theory and Method* (1999), 51–70.

[5] Mohamed Elyas, Atif Ahmad, Sean B Maynard, and Andrew Lonie. 2015. Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security* 52 (2015), 70–89.

[6] Leonhard Euler. 1741. Solutio problematis ad geometriam situs pertinentis. *Commentarii academiae scientiarum Petropolitanae* 8 (1741), 128–140.

[7] George Grispos. 2016. *On the enhancement of data quality in security incident response investigations.* Ph.D. Dissertation. University of Glasgow.

[8] George Grispos, Jesús Garcıa-Galán, Liliana Pasquale, and Bashar Nuseibeh. 2017. Are You Ready? Towards the Engineering of Forensic-Ready Systems. In *11th International Conference on Research Challenges in Information Science (RCIS).*

[9] George Grispos, William Glisson, and Tim Storer. 2014. Rethinking Security Incident Response: The Integration of Agile Principles. In *AMCIS 2014.*

[10] George Grispos, William B Glisson, and Tim Storer. 2013. Cloud Security Challenges: Investigating Policies, Standards, And Guidelines In A Fortune 500 Organization. In *ECIS 2013.*

[11] George Grispos, William Bradley Glisson, and Tim Storer. 2015. Security Incident Response Criteria: A Practitioner’s Perspective. In *AMCIS 2015.*

[12] C Grobler and C Louwrens. 2007. Digital forensic readiness as a component of information security best practice. *New approaches for security, privacy and trust in complex environments* (2007), 13–24.

[13] CP Grobler, CP Louwrens, and Sebastiaan H von Solms. 2010. A framework to guide the implementation of proactive digital forensics in organisations. In *ARES 2010.* IEEE, 677–682.

[14] Özgür Kafali, Munindar P Singh, and Laurie Williams. 2016. NANE: Identifying Misuse Cases Using Temporal Norm Enactments. In *RE 2016.* IEEE.

[15] Jason Tyler King et al. 2015. *Measuring the Forensic-ability of User Activity Logs.* Ph.D. Dissertation. North Carolina State University.

[16] John P Mylopoulos and Theodosios Pavlidis. 1971. On the topological properties of quantized spaces, I. the notion of dimension. *Journal of the ACM (JACM)* 18, 2 (1971), 239–246.

[17] Liliana Pasquale, Carlo Ghezzi, Claudio Menghi, Christos Tsigkanos, and Bashar Nuseibeh. 2014. Topology aware adaptive security. In *SEAMS 2014.* ACM, 43–48.

[18] Liliana Pasquale, Carlo Ghezzi, Christos Tsigkanos, Menouer Boubekeur, Blanca Florentino, Tarik Hadzic, and Bashar Nuseibeh. 2017. Topology Aware Access Control of Cyber-Physical Spaces. *IEEE Computer* In Press (2017).

[19] Liliana Pasquale, Sorren Hanvey, Mark Mcgloin, and Bashar Nuseibeh. 2016. Adaptive Evidence Collection in the Cloud Using Attack Scenarios. *Computers & Security* 59 (2016), 236–254.

[20] Sean Philip Peisert. 2007. *A model of forensic analysis using goal-oriented logging.* University of California, San Diego.

[21] Kamil Reddy and Hein S Venter. 2013. The architecture of a digital forensic readiness management system. *Computers & Security* 32 (2013), 73–89.

[22] David Rimmer. 2014. Forensic readiness - the new ’business continuity’. Online at: www.scmagazineuk.com/forensic-readiness–the-new-business-continuity/article/540961/. (2014).

[23] Robert Rowlingson. 2004. A ten step process for forensic readiness. *International Journal of Digital Evidence* 2, 3 (2004), 1–28.

[24] Ravi S Sandhu, Edward J Coyne, Hal L Feinstein, and Charles E Youman. 1996. Role-based access control models. *Computer* 29, 2 (1996), 38–47.

[25] P. Stephenson. 2003. Conducting incident post mortems. *Computer Fraud and Security* 2003, 4 (2003), 16–19.

[26] Dauda Sule. 2014. Importance of Forensic Readiness. Online at: www.isaca.org/Journal/archives/2014/Volume-1/Pages/JOnline-Importance-of-Forensic-Readiness.aspx. (2014).

[27] John Tan. 2001. Forensic readiness. *Cambridge, MA:@ Stake* (2001), 1–23.

[28] Rune Todnem By. 2005. Organisational change management: A critical review. *Journal of change management* 5, 4 (2005), 369–380.

[29] Sebastiaan von Solms, Cecil Louwrens, Colette Reekie, and Talania Grobler. 2006. A control framework for digital forensics. *Adv. in Dig. Forensics II* (2006).

[30] Richard Whittington. 2006. *Organizational Structure.* Oxford Handbooks.