ISBN: 978-989-8533-67-8 © 2017

THE SOCIAL IN TECHNICAL ATTACKS – QUESTIONING THE BIFURCATION IN THE FIELD OF INFORMATION SECURITY

Jukka Vuorinen[1] and Pekka Tetri[2]
[1]Economic Sociology, Department of Social Research, University of Turku, Finland
[2]Oulu University Secure Programming Group, University of Oulu, Finland

ABSTRACT

This paper examines the social in information security. We argue that there is always a social aspect in technical information security attacks. By using Erving Goffman's sociological concept of "frame", we analyse the social in different illustrative contexts, in which technical attacks are compared with social engineering attacks. Through examining the concept of normality, we found that social engineering attacks and technical attacks can resemble each other. In both attack forms, the intruders can hide their actions in the flow of normality. Thus, we question the fertility of information security's bifurcation into the two separate branches (technical/social). Instead of thinking the technical as separated and free of the social, we argue that the social is present everywhere in the field of security, including the technical side as well. All security is social in the first place.

KEYWORDS

Keywords: social engineering, frame, normality, fabrication

1. INTRODUCTION

In this paper, we examine the social as part of technical attacks and argue that the social element can work similarly in technical and social engineering attacks. The main body of research in the field of information and cyber security asserts a fundamental bifurcation between technical (or technological) and social security. The bifurcation concerns as much the guidance of "making" security – how practitioners are guided by standards and frameworks – as well as academic research on information security. Firstly, there is the technological side of security, which refers to hardware and its counterpart software. Secondly, there is the social side of security, in the form of human behaviour, which also covers a vast array of activities and roles from human as end-users and administrators to humans as the creators and designers of technology and code (Gupta and Sharman 2009).

However, in terms of information security research and its emphasis, the two branches of bifurcation are not treated equally. Since the emergence of computers, computer security has been considered mainly as a technical issue (Baskerville 1993) as if technology driven systems call for security that is based on technology. The emphasis on the technological branch of security is affirmed by security frameworks and standards such as PCI DSS (Payment Card Industry Data Security Standard) that consists of 12 requirements, of which 11 are technology-driven and only one requirement is about people which thus refers to the social element.

Recently, softer approaches to information security have emerged. These approaches are based on the inclusion of social aspects (see Loch, Carr and Warkentin, 1992; Adams and Sasse, 1999; Siponen, Baskerville and Heikka, 2006; Gupta and Sharman, 2009). Thus, the social layer is certainly acknowledged in the field. Moreover, the social pertains to a variety of specific issues. For example, security policy compliance issues (Bulgurcu, Cavusoglu and Benbasat, 2010; Siponen and Vance, 2010), insider threat (Colwill, 2009), or computer abuse (Willison and Warkentin, 2013), all include a significant social aspect. The currently fashionable notion of the human element as the weakest link of security (Nohlberg, 2009; cf. Adams and Sasse, 1999) affirms and re-establishes the bifurcation as well. The social level – the human factor – opens a road for accidents and security incidents which then take place at the technical level. In social engineering, vulnerability comes with the social element that affects the technical side of security (Mitnick and Simon, 2011; Tetri and Vuorinen, 2013). In other words, a human element is used as an attack vector in order to make the attack on a technological system possible.

In this paper, we argue that there are similarities between social engineering and technical attacks. Technical attacks and defence for technical attacks contain a social aspect. More precisely, the social and technology are not merely intertwined (see Carter and Grover, 2015) but are inseparable. The layers of security (social, physical, technical) are anything but isolated. Rather, they form a machinery in which the levels are mixed (Vuorinen and Tetri, 2012). We argue that technical attacks include a significant social aspect as well. In order to make sense of the overarching social side in security, we use the sociological concepts of the frame, fabrication, and normality. Through these concepts, we can examine the social and the social construction of reality. Then, we are able to analyse social engineering that is the most obvious actualisation of the social in the field of information security and compare social and technical attacks through examples of phishing, Stuxnet worm, Heartbleed bug, honey pots and log manipulation. Finally, we question whether it is fertile to make a division between social and technical attacks in the first place.

2. THE FRAME, FABRICATION, AND NORMALITY

Sociologist Erving Goffman (1986) argues that everyone applies a “frame” – a set of thoughts – that answers the question of “what is going on here?” So, “I am typing” or “I am reading” are frames that describe the activity of the self. However, the frames are not solely limited to the activities of self but there are frames that relate to other actors, including both material and human actors. For example, “she sent a message”, “a security patch is installed”, or “it is raining”, are frames – descriptions and accounts – of what is going on. Goffman’s ideas pertain to the tradition of social constructionism which means that reality is always (partly) intersubjectively constructed (e.g. Blumer, 1986; Berger and Luckmann, 1990). For example, it is normal to scream and shout in a rock concert but it is not normal to act in such a way in a formal meeting with a client. Normality is, thus, a social construct. There is no “normal” without the social.

In this sense, the Goffman’s frames can be considered as ontological work in which reality – in the sense of “what is going on” – is constituted. Here, the term “ontology” refers to the field of philosophy instead of the field of information system science in which ontology is understood, not as a process, but as a static map (e.g. Vuorinen, 2014, p. 24). Goffman’s frames are not static but a product of constant ontological work that can change. The interpretation of a situation can alter quickly. For example, in context of traffic, a normally driving car that accelerates quickly can turn from a non-dangerous car to a serious threat from a pedestrian point of view. In such a case, the ontological status of a car changes (Woolgar and Neyland, 2013).

Goffman examined mainly face-to-face interaction. In this microsociological approach, face-to-face communication and binary relations reside in the focus. Nonetheless, the concept of frame can be applied to a broader context as well. In terms of groups and organisations, frames function in the intersubjective manner: frames can be commonly shared but they are also open to dispute. Whereas in quickly changing situations the frame (what is going on) can be in dispute, the suggested course of action – “what should be done” – is even more prone to disagreement. In the ideal case of consensus, everyone answers the questions of “what is going on here” and “what should be done next” in a similar way.

In terms of frames, intersubjectivity works on different levels. In addition to sharing the same frame between different subjects, we constitute frames on information that is communicated intersubjectively. Slightly differently put, frames are shaped in interaction with others. Importantly, it is not merely human subjects that provide information for frames. For example, a firewall log can offer information that provides material for the constitution of frame. In fact, a log is a frame in itself as it tells what has happened. In case of rain, the raindrops bring or “express” information of “raining”. Therefore, different actors, humans and non-humans take part in the process of frame creating. In simple terms, there are different actors that carry out *ontological work*. By including material actors to the process of constitution of reality, we approach the viewpoint of sociomaterialism (in philosophy of science see Serres (2007); in sociology see Latour (1999, 2005), Suchman (2005); in information system science Scott and Orlikowski (2014) and Introna (2013, 2015)).

However, while some frames can be accurate and valid, other frames can fail to tell correctly what is going on. For example, it can simply be that there is not enough information to build an overarching accurate frame. When a computer is used, the frame is likely to be reduced at the level of "use of computer" instead of thinking of all the processes that take place using the computer. In other words, the frame is a simplified, incomplete version of what is happening. The frame fails to be accurate in terms of details. Alternatively, some information can be overlooked and interpreted wrongly. This means that the construction of the correct frame fails. Nonetheless, in such case, there is a frame constructed and applied but the frame is flawed.

In addition to mistakes and the lack of information, there is another source of false frames, namely, fabrication (Goffman 1986). In terms of security research – compared to overlooked information or improperly interpreted data – fabrication provides a more interesting case of frame. The frames that pertain to security become intriguing especially in cases in which information for the construction of frames is manipulated in a deceptive way (see Tetri and Vuorinen, 2013; Vuorinen, 2014). In other words, deceptive information is fed in order to tamper the thought of what is going on here.

In terms of communication, fabrication is misleading information. Interaction is used as the channel of communication through which the frame is fabricated – polluted by false information – into a form that benefits the attacker. This kind of an attack materializes in the form of phishing emails that seek to create a false frame. For example, such an email can say that your email account has exceeded a critical limit and suggest that you should log on immediately using a provided link that in fact directs you to a phishing site. Of course, the sender of this mail is only interested in your username and password – perhaps in hijacking your email account. Another popular scheme include providing false URLs for the victim to click, and instead of doing what the message says, it actually fetches malware, installs it on the victim's computer undetected by modern anti-virus software and becomes part of a botnet – to be used in further attacks, for example distributed denial of service attacks, or ddos attacks. In fabrication, attacker's frame is sought to be kept in the dark and the false interpretation of situation is imposed on the dupe. In such case, in Goffman's (1986) terms, the frame is fabricated. In other words, the cues offered to interpret and construct a frame are intentionally made different from what is really going on. Phishing, which is considered a social engineering technique, is not only technique which is based on fabrication. In fact, many of SE-cases include some fabricating elements, pretexting for example. (Tetri and Vuorinen, 2013.)

Nevertheless, how convincing phishing emails are depend on how the false narrative – the fabricated frame – is constructed. Fabrication seeks to propose a frame that can be true; the point is that the proposed frame is treated as a true one. We argue that the more normal the fabricated frame seems, the more likely it works. There is power in familiarity and normality. For example, this is the case in the modern CEO frauds[1], phishing e-mails. These types of frauds rely on the fact that people trust other people they know in real life (in this example, your colleague). Spoofing mimics the email address of someone the dupe knows, someone from the organisation. attacked@mycompany.com sends an email to the dupe, also working for mycompany.com, seems reliable. Co-workers communicate via email, ask for favours and transfer files. In fact, it would be odd to suspect if the email was spoofed, unless the message itself was very off. In this example, the attacker creates the frame using technology, yet the attack is based on trust between people, and people trusting technology. Technology can be hijacked, controlled, but also used as a fake narrative, in which the outside attacker only seems to be inside, even when they are not.

In terms of information security, the power of the normal should be noted. Normality is based on the social, in the sense that different social systems consider different things and customs normal. A visit to a strange culture can make you see your own normalities. The normal is powerful and possibly deceitful as it does not trigger any alarms. Normal things are approached with natural attitude (Berger and Luckmann, 1990). In a sense, the normal in its mundanity and continuously repeated refrain makes everything invisible, imperceptible. Normality can hide things because there is nothing alarming about normality. In security, normality is something that lays a pavement for threats. The threats do not come in isolated packages but are constituted through relations. Figure 1 summarises the construction of frame and the effect of normality.

[1] see https://krebsonsecurity.com/2017/02/irs-scam-blends-ceo-fraud-w-2-phishing/#more-37923

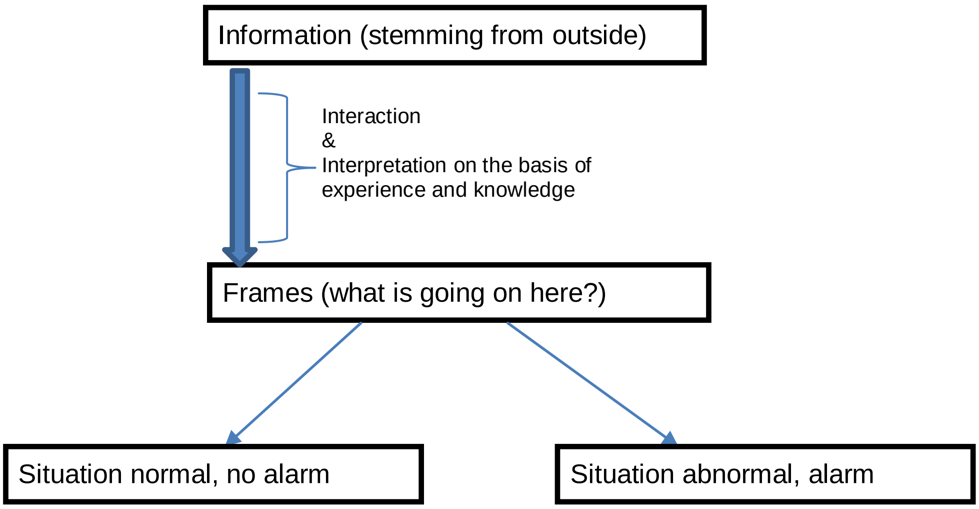
Information (stemming from outside)
Interaction
&
Interpretation on the basis of experience and knowledge
Frames (what is going on here?)
Situation normal, no alarm
Situation abnormal, alarm

Figure 1. The construction of frame and alarm

However, normality does not concern merely the human side of information and cybersecurity. We argue that normality – what is treated as normal (partly a social construction) – extends to technical attacks as well. In the following section we deal with this subject.

3. THE SOCIAL IN TECHNICAL ATTACKS

As shown above, in SE, false trust between people is created through different frames. A false narrative is fed for the dupe to believe in. Similarly, technology can facilitate a false frame – carry out ontological work – or be the canvas for a false narrative. For example, in the network environment, trust is mediated with certificates, authentication, and tokens. In other words, a certificate carries out ontological work of "what is going on here?" It is a system of trust mediated by IT artefacts. Generally, in "man in the middle attacks", a trusted position – the channel in the middle – is occupied by a third party (e.g. Callegati, Cerroni and Ramilli, 2009). Differently phrased, attacker can use the systems of trust in order to achieve the goals of an attack. For example, the notorious Stuxnet virus used a stolen certificate, so that it would be considered legitimate code.[2] Here, a piece of technology, a malicious code, fools a technological system by pretending to be something else – pretending to be a normal, non-alarming case. Stuxnet, which was targeted to destroy Iranian centrifuges, acted as a normal code but made slight changes, powerful enough, to break the centrifuges. It can be then argued that Stuxnet attack was as social as it was technical. It used familiarity and normality to hide its true targets.

In the practical field of cybersecurity, the defenders can also play the same game of creating false frames that seem legit for the attacker. A honey client crawls through malicious websites pretending to be a normal browser, while it collects information about malicious websites (Wang, 2009). Another example is implanting faked credentials, that are flagged as stolen, and then tracked. These fake and tracked credentials are examples of honey tokens. An analogy of the previous could be tracking money, or marked notes. Once the money is used, the trackers can then pinpoint where the money went, and possibly track down who took it and used it. The idea is not to block it from happening per se, but to follow the trail. The attacker does not realise that they are using marked goods which make their own actions trackable. Again, normality is used. In above, the entire term "honey" refers to something that is made look tempting but is actually something else, a precious looking object that is used to allure and capture intruders without losing anything valuable. The ontological work takes place as the frame of honey is fabricated. In other words, how the temping features of a honey object are constituted.

Yet another defender technique using frames would be to deploy a honey net in the actual network. It is isolated from the actual goods and assets of the defender, so the attacker can roam freely, thinking they have

[2] see https://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history/

successfully intruded the target while being trapped, monitored, and analysed. The gist of the matter is that for both sides create the frame seems valid. The key in fabrication is not technology, or devices that monitor, isolate, and analyse but the idea of the frame, which is based on the social. The narrative is built using technology. However, in the narrative technology and the frame (the social) are inseparable, neither will exist without the other. The technical and the social are entangled.

Trust is also created between technological devices. A company laptop is trusted to its user, and the laptop itself is trusted in the network. It is an entity that is allowed to enter the perimeter and use the services which it has been assigned privileges. The laptop itself might have security controls, such as antivirus, or other software. From a server, new updates are propagated into the laptops that are trusted. For example, group policies can be enforced to all of the machines. While this is all daily administration, it is another example of frame, where technology trusts technology.

The relations of trust can be as complex as the number of nodes in the network, people, services, and every single entity that functions in it. People trust people and machines, machines trusts other machines and people (after they log on with proper credentials). With thousands, or tens, or even hundreds of thousands of entities, endless amounts of traffic (both machine logs and network traffic logs), as well as endless frames, it only takes one frame that works for the attacker to get in.

Sometimes, the entire foundation of a trust system can fail. This was the case with the Heartbleed vulnerability. The discovery of Heartbleed vulnerability– or the Heartbleed Bug – in 2014 disclosed severe and critical problems and flaws in OpenSSL library. The problem in the vulnerability is in the very core of the information security procedures –the *trusted* library was vulnerable, which has (without repair) tremendous consequences. “This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).” (Heartbleed.com). Furthermore, attacks can be carried out “without leaving a trace”. OpenSSL library was vulnerable to begin with, however, it was trusted, as it was an unknown vulnerability (until it became known). As long as people are not aware of vulnerabilities, they do not exist, and therefore, they can be trusted. It is especially dangerous, when they regard security controls that function on the basis of trust. Ontologically, there are some things we need to know and trust. Otherwise we can never trust anything, especially security controls. Good programming is difficult in the sense that programs are supposed to do what they are supposed to do meaning that secure programming includes that they do not do anything else, except what they’re supposed to do. Applications calling other libraries might assume that those libraries are safe. In the case of OpenSSL it was not the case.

At the moment when *unknown* vulnerability became known vulnerability, trust was shattered in terms of frames. The library was trusted and the frame was “we are safe if we use these services” although the great potential to be abused was there all the time. Furthermore, exploiting the vulnerability, left no traces. This means that there were no material, hints or log files left in order to fix the assumption of what is going on here. Yet, this was not a fabrication but simply overlooking risks because this vulnerability was unknown.

Logs are also known to be targets of forgery and being tampered with. The security people rely on logs to find out “what really happened” or is happening. Therefore, the logs must be relied on to tell the truth. However, attackers can target the logs themselves, injecting malicious code in a browser (should the server itself still remain tamper-proof). An example of log injection, in which a new log entry is injected (https://capec.mitre.org/data/definitions/93.html):
“%0D%0A[Thu%20Nov%2012%2011:22]:Info:%20User%20admin%20logged%20in”
may appear as:"[Thu Nov 12 12:11:22]:Info: User admin logged in”

Logging can be also evaded, leaving no clear trace of the attacker. Such a problem existed in Microsoft’s IIS servers. The below example illustrates how, technically, attackers bypass controls and become invisible for the included transactions (http://www.webappsec.org/projects/articles/082905.shtml):

```
Attack Request
GET /?id=<insert 4095 A's>
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: TestServer

Logged Response (IIS 5.0 with default logging)
```

```
2005-08-10 17:21:29 172.16.10.3 - 172.16.10.111 80 GET /Default.asp ... 200
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
```

Logged Response (IIS 6.0 with default logging)

```
2005-08-10 17:09:54 172.16.10.116 GET /Default.asp ... 80 - 172.16.10.3
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0) 200 0 0
```

The point of logging examples is to illustrate that the systems provides insights to a human, answering “what is really going on?”, while the attacker can dupe the victim by crafting requests that alternate the logs into something different or evade logging altogether. The dupe has to be aware of this problem of not knowing when evidence can be trusted. Narratives are created between humans, between human-machine, machine-machine interaction. This is one of the biggest challenges for security; how can one really trust anything, or in other words, how can one evaluate the frame and how is it done reliably? Even security controls play a part of storytelling and are used against the dupe.

All in all, ontological work – the construction of frames – is carried out socially and technically. However, the two levels are mixed and blended into each other in ways that makes it impossible to isolate them. What is the technical and the social in logs? What is the technical and the social in Stuxnet? What is the technical and the social in Heartbleed vulnerability? It is difficult to point solely to the technical. The technical comes with the social. Technologies can run own their own – yet, they are initiated socially. Moreover, the attack techniques – both social and technical – resemble each other. Both can seek to hide themselves in normality (as is the case with Stuxnet and log tampering).

4. CONCLUSIONS

The social extends much deeper into the “technical” level than it is assumed by the bifurcation statement in the field of information security. Both levels address the problem of normality in very similar manner. Whether the case was about a successful social engineering attack or an act of breaking into an information system, both cases are enormously difficult to detect because the marks they leave on the surface of the normal flow are imperceptible or very subtle. Of course, there are unsuccessful cases, in which the attackers are not able to mix in the stream of normal; they act visibly strange and are noisy. The hiding game into the veil of normality is on as much at the technical level as it is in the sophisticated social engineering attacks. In other words, the fabrication of the frame (the thought of what is going on here) is entirely possible at both levels. As the hiding game is played, the defenders have to constantly struggle with different techniques to check the validity of their frame. However, they have a chance to take the initiative as in all “honey” cases.

In this light, it should be clear that the division between the technical and the social is not fertile in terms of understanding information security and how it works, and how it is made. Rather, the two are intertwined and blended together in several different ways in the field of information security. Fundamentally, security is social and discursive; it seeks to find normality in order to spot abnormal activity. The key in becoming imperceptible is to appear normal – to impose a fabricated frame, to hide in normality. This concept aligns the social and technical. Security is social and discursive. The technical side – which for so long time has been treated separately from the social and is seen as the pinnacle of security – is always merged with the social.

REFERENCES

Adams, A. and Sasse, M. A. (1999) ‘Users are not the enemy’, *Communications of the ACM*, 42(12), pp. 40–46.

Berger, P. L. and Luckmann, T. (1990) *The social construction of reality: a treatise in the sociology of knowledge*. Anchor Books, New York, USA

Blumer, H. (1986) *Symbolic interactionism: Perspective and method*. University of California Press, Oakland, California, USA.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) ‘Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.’, *MIS Quarterly*, 34(3), pp. 523-548.

Callegati, F., Cerroni, W. and Ramilli, M. (2009) ‘Man-in-the-Middle Attack to the HTTPS Protocol’, *IEEE Security & Privacy*, 7(1), pp. 78–81.

Colwill, C. (2009) ‘Human factors in information security: The insider threat - Who can you trust these days?’, *Information Security Technical Report*, 14(4), pp. 186–196.

Goffman, E. (1986) *Frame analysis: an essay on the organization of experience*. Northeastern University Press, Boston.

Gupta, M. and Sharman, R. (eds) (2009) *Social and human elements of information security: emerging trends and countermeasures*. Information Science Reference, Hershey, PA, USA.

Introna, L. (2013) ‘Epilogue: Performativity and the becoming of sociomaterial assemblages’, in Vaujany, F.-X. de and Mitev, N. (eds) *Materiality and space: organizations, artefacts and practices*. Palgrave Macmillan, Houndmills, Basingstoke, Hampshire, UK, pp. 330–342.

Introna, L. (2015) ‘Algorithms, Governance, and Governmentality: On Governing Academic Writing’, *Science, Technology & Human Values*, 41(1), pp.17-49.

Latour, B. (1999) *Pandora’s hope: essays on the reality of science studies*. Harvard University Press, Cambridge, MA, USA.

Latour, B. (2005) *Reassembling the social: an introduction to actor-network-theory*. Oxford University Press, Oxford, UK.

Loch, K. D., Carr, H. H. and Warkentin, M. E. (1992) ‘Threats to Information Systems: Today’s Reality, Yesterday’s Understanding.’, *MIS Quarterly*, 16(2), pp. 173–186.

Mitnick, K. D. and Simon, W. L. (2011) *The art of deception: Controlling the human element of security*. John Wiley & Sons, Hoboken, New Jersey, USA.

Nohlberg, M. (2009) ‘Why Humans are the Weakest Link’, in *Social and Human Elements of Information Security. Emerging Trends and Countermeasures*. Information Science Reference, New York, USA.

Scott, S. V. and Orlikowski, W. J. (2014) ‘Entanglements in practice: Performing anonymity through social media’, *MIS Quarterly*, 38(3), pp. 863–893.

Serres, M. (2007) *The Parasite*. University of Minnesota Press, Minneapolis, MN, USA.

Siponen, M., Baskerville, R. and Heikka, J. (2006) ‘A Design Theory for Secure Information Systems Design Methods.’, *Journal of the Association for Information Systems*, 7(11), pp. 725–770.

Siponen, M. and Vance, A. (2010) ‘Neutralization: New Insights Into The Problem Of Employee Information Systems Security Policy Violations.’, *MIS Quarterly*, 34(3), pp. 487-A12.

Suchman, L. (2005) ‘Agencies in technology design: Feminist reconfigurations’, available at: <www.lancs.ac.uk/fass/sociology/papers/suchman-agenciestechnodesign.pdf>.

Tetri, P. and Vuorinen, J. (2013) ‘Dissecting social engineering’, *Behaviour & Information Technology*, 32(10), pp. 1014–1023.

Vuorinen, J. (2014) *Parasitic Order Machine. A Sociology and Ontology of Information Securing*. Annales Universitatis Turkuensis. Available at: <http://urn.fi/URN:ISBN:978-951-29-5868-9>.

Vuorinen, J. and Tetri, P. (2012) ‘The Order Machine - The Ontology of Information Security’, *Journal of the Association for Information Systems*, 13(9), pp. 695–713.

Wang, K. (2009) ‘Open Source Honeyclient: Proactive Detection of Client-Side Exploits’, in Oram, A. and Viega, John (eds) *Beautiful Security*. O’Reilly Media, Sebastopol, CA, USA, pp. 131–146.

Willison, R. and Warkentin, M. (2013) ‘Beyond Deterrence: An Expanded View Of Employee Computer Abuse.’, *MIS Quarterly*, 37(1), pp. 1–20.

Woolgar, S. and Neyland, D. (2013) *Mundane governance: ontology and accountability*. Oxford University Press, Oxford, UK.