Sharing Cyber Intelligence in Trusted Environments – A Literature Review

Thomas D. Wagner
School of Computing, Telecommunications and Networks
Faculty of Computing, Engineering and the Built Environment,
Birmingham City University
E-mail: thomas.wagner@bcu.ac.uk

Abstract: *Cyber threats are increasing on a daily basis and protection measures such as firewalls and anti-virus software have proven insufficient in today's threat landscape. Much money is invested into protection measures but this has not eradicated the root cause. Cyber-attacks occur every second around the world and many attacks use the same patterns to exploit systems. Hence attacks could be thwarted by sharing threat information with trusted peers. Therefore, elaborate models for sharing cyber intelligence are needed which include models for trust, sanitation, crowd sourcing and automated threat sharing. This article depicts and compares resources about existing models and ideas about threat sharing.*

Keywords: information security, cyber intelligence sharing, threats, risks, mitigation.

Introduction

The virtual world has gained many followers in recent decades which opened up a whole new world of possibilities to render our lives more pleasant through easy access to information and services. The dark side of this convenience is that miscreants are trying to exploit systems with elaborate attacks on a daily basis. Such attacks are possible because cybercriminals often share or sell information about exploitable systems, and attack different systems with the same method. Today's organizations invest in protection measures but not in eliminating the root cause for attacks.

Many organizations would like to share cyber intelligence but do not know how to do so (Vasquez *et al*., 2012). This is because threat sharing models do not exist or are in an embryonic stage. To attain an acceptable level of security, cyber intelligence has to be shared between trusted peers. The intelligence has to be complete and actionable, so that peers are immediately able to remediate vulnerabilities.

This literature review depicts and compares different resources about threat sharing. Threat sharing not only has positive attributes, but it also brings issues that have to be thoroughly scrutinised before threat intelligence can be shared. Legal issues are one of the major concerns for researchers, not only because threat intelligence could contain personal information about the organization or clients, but also because every country has different privacy laws. This could lead to privacy infringements if certain metadata

is not sanitised before sharing. It could also damage the reputation if an organization was under attack and, for example, credit card details were stolen, hence anonymity is a sharing requisite.

Trust has to be established between peers wanting to share cyber intelligence. Trust is a research topic itself but can be, on the surface, established with is a mixture of technicality of the Public Key Infrastructure (PKI) and personalized trust tables.

Literature review

Daily repeated and successful cyber-attacks visualise the urgent remediation of cyber defences (Trope & Humes, 2013). To counter such attacks, one of the methods to mitigate threat impact is to share cyber threat intelligence within a trusted community. Several studies, (such as Vasquez *et al*., 2012; Gardin, 2014; Curran, 2013) have shown that sharing cyber intelligence is the way forward and a necessity if increasing attacks are to be survived. Trust has to be established between sharing peers or sharing communities, and cyber intelligence has to be classified as relating to low and high risk data. Vasquez *et al*. (2012) emphasise that data has to be classified before it can be shared, but fail to propose a model that effectively enables threat sharing. A low risk environment is suggested which does not allow the sharing of high risk cyber intelligence that could act as an incentive for sharing peers. It could start a sharing community with low risk information, which could lead to sharing high risk information at a later stage.

The reason why companies, governments, academia and other bodies are not yet sharing information, or only sharing between industry sectors, is due to missing threat sharing models, reputational and legal issues (Curran, 2014). Curran (2013) stated that the government is able to share information with companies but not vice versa, since companies would face legal issues if they share information about their clients. Companies could remove critical information that would identify a person. Information could be reduced to a bare minimum just to identify the threat and not the detailed information behind it. Hofmann (2012), on the other hand, argues that governments might find it challenging to share classified information with the community, especially sharing threat intelligence with enemy countries. Sander (2012) presented an application which has the capability to provide anonymity for participating threat sharers. A thorough scrutiny has to be conducted to analyse whether the application really eliminates all metadata from a threat indicator or if there are some leftover traces. The legal issue contributes to unwillingness to share cyber intelligence, because companies can be held responsible if they received threat indicators and did not react (Trope & Hume, 2013). Customers are likely to sue the company for not responding to known threats. So it seems that some companies prefer to stay in the dark, feeling that they cannot be held responsible if they did not know about the threat. Cultural and language barriers can block the process of exchanging threat intelligence between different countries (Vasquez *et al*. 2012).

Imura *et al*. (2014) developed an application called NECOMAtter which disseminates new threats via a Twitter-like scheme. The application filters relevant threat information and tweets it to the peers. The problem with this application is that it does not read all file formats, which limits its compatibility with existing file formats. It is not stated who can join the

sharing community, hence it is assumed that anyone can create an account and share cyber intelligence. This would be a detriment to establishing trust because the sharing peers have not been vetted. Furthermore, the authors do not specify how the threats are collected, how they are rendered relevant to the peer and how they classify the threat information. A threat sharing model from a 2004 patent suggests anonymous threat sharing but fails to automate the process, therefore all incident information has to be entered manually (Bhimani et al. 2004). When these two approaches to threat sharing are compared neither then we can see that none possesses the capability of automatically analysing and sharing threats. Human intervention is mandatory with both models, rendering them inappropriate for current threat sharing needs.

Another trend for the future might be that all security related issues are dealt with by a managed service (Ring, 2014). Hence companies would not have to grapple with security issues at all. Then again, this would raise further security issues about Trusted Third Parties (TTP).

Moriarty (2013) argues that information shared equally results in information shared with no one since it would be an information overflow of useless data. This is particularly true, since irrelevant information will distract peers from the real information, and most existing threat sharing processes suffer from too much information. Factors such as legal issues and distrust could deter participants from sharing threat intelligence, but as Curran (2013) and Constantine (2012) describe it, cyber threat intelligence sharing has to be reciprocal and cannot be approached as a one-way information flow. It also has to be shared with the right peers at machine-readable speed to reduce threat impact of vulnerable systems (Lee & Rotoloni, 2014)

According to West (2014) the attacker only has to be successful one time out of a million to infiltrate the system, on the other hand, the defender has to be successful all the time.

The importance for threat sharing is that companies alone will not stand a chance if they decide not to share or the information is not shared at appropriate speed. Hofmann gave an example of how an attack could not only affect the monetary system, but could also be life threatening.

> “Think about a massive cyber-attack on the power grid for a moment. We saw what happened in the aftermath of Hurricane Katrina when the power went off for quite a while in New Orleans, surrounding areas and neighbouring states. It wasn't pretty.
>
> Now, imagine the same thing happening today, but blacking out the entire East Coast for weeks. It would be "Road Warrior" time” (Hofmann, 2012).

According to Barford *et al*. (2010), an ideal state would be if a system could automatically learn from the attack and respond to it without human interference. This self-learning system could, after identifying the threat, disseminate the information automatically to trusted peers. According to Kampanakis (2014), companies might be sceptical if their information is shared automatically without having the content reviewed previously. A phishing e-mail attack could not be shared without revealing company

sensitive data and is, therefore, unsuitable for threat sharing at machine speed. Hence legal issues could be faced by participating threat sharing peers if the shared cyber intelligence contains sensitive metadata. Few businesses expose attacks they have suffered (2013), because companies fear for their reputation and the consequent business loss if they disclose information about attacks.

Cyber defence teams currently refer to manually added and shared threat intelligence, but automated defence mechanisms are preferred to actionable intelligence, especially for smaller companies that lack efficient security mechanisms (Moriarity, 2013). Constantine (2012) describes the current problem with threat sharing that companies are willing to share the data of others, but not their own. Constantine does not see any technological problem or legal issues that could be solved easily, rather a problem with the human mind of not wanting to share information for free and that it might be used against them. I agree that the technological part can be easily solved, but not the legal part. Constantine did not describe how he would solve the legal issues.

Some industry sectors are manually sharing information (Clancy, 2012), such as the retail sector and the financial sector (Curran, 2014). The financial sector has been compromised countless times and most of these attacks could have been prevented if cyber intelligence had been automatically shared. Clancy writes about the financial sector sharing information inside the community and how it produces more actionable information. The problem is that the community only disseminates information but does not really share in a reciprocal way. Sharing or disseminating information manually is inappropriate, because the threat landscape changes daily and actionable cyber intelligence has to be shared automatically to be effective.

Treglia and Park (2009) have identified the following key influences of threat sharing in their paper: technical (interoperability, availability and control), social (trust, shadow network and critically) and legal (policy conflict and governance). The responsible person for sharing intelligence might be influenced by his or her personal opinions which can affect the information shared. If the intelligence was analysed by a machine and disseminated without human interference, then we have achieved an unbiased intelligence sharing mechanism. On the other hand, the programmer of the sharing platform could have included his or her own opinion on how and what is shared and could, therefore, influence the action.

Interoperability is an issue that existing threat sharing platforms face. Shared intelligence is manually disseminated via a platform but the receiving peer may be unable to use the information since the data extension is not supported by the used application (Vasquez *et al*. 2012). To tackle the problem with interoperability, the MITRE group has developed the following technical specifications: TAXII (Trusted Automated Exchange of Indicator Information), STIX (Structured Threat Information Expression) and CYBOX (Cyber Observable Expression) (Mitre Corporation, 2014; Connelly *et al.*, 2014; Barnum, 2012). The interoperability issue could be solved if these specifications are adopted as a standard for threat sharing formats. Other specifications are available such as CDXI (Cyber Defence Data Exchange and Collaboration Infrastructure) for exchanging cyber intelligence and SCAP (Security Content Automation Protocol) for data

standardization. If no data standard can be established between peers, then data transformation has to be applied to ensure compatibility.

Dumitras and Shou (2011) propose a Worldwide Intelligence Network Environment (WINE) to fill in metadata that is missing from zero-day attacks. The collected data about zero-day attacks reveal critical information about how these attacks occurred and how to prevent them. It is suggested that threat intelligence is mostly forgotten after publication, and no threat has been accompanied for its complete life cycle. I agree that no threat has been accompanied completely, because a threat can only be followed once it has attacked an entity. The creation stage of the threat is only known to the miscreant who developed it. The proposed life cycle depicts certain threats and how to analyse them throughout their lifespan, but only after the attack occurred. This approach can give an insight of how zero-day attacks happen and eventually contribute to preventing future attacks.

Hutchins (2011) and Barnum (2012) describe the cyber kill chain, which refers to a military approach to identify the threat and break it at a certain point. The cyber kill chain is also used in the virtual world and can be broken at any time to terminate the attack. It consists of the following stages: reconnaissance, weaponize, deliver, exploit, control, execute and maintain. The attack can already be spotted when surveillance of the system is conducted by a hacker. The attack can also be terminated when the system has already been compromised, but the preferred stage is to stop the attack before the exploitation. The cyber kill chain is an efficient approach to depict different stages that an attacker goes through before compromising the system. The kill chain alone cannot prevent an attack but can show where an attack can be stopped and the consequences if the attack was detected too late.

Trust is a challenge in sharing cyber intelligence because the shared information is of high value and can decide over an organization's fate. Peers are heterogeneous and we have to assume that some peers are of good nature and some peers have malicious intentions and are unable to provide the promised cyber intelligence (Wang & Vassileva, 2003). To keep malicious activities out of the trusted threat sharing circle, members have to be vetted by a trusted authority. Abouzahra and Tan (2014) argue that peers expect repayment for shared information and thus could be encouraged to share their knowledge . Trust has many incentives and can be achieved in different ways, but trust will always be a personal choice and can be affected by several causes.

There are many incentives for sharing cyber intelligence. One is the financial incentive (Vasquez *et al*., 2012). Financial incentives include the need for fewer security analysts to analyse threats because trusted peers have already analysed and shared it, and a reduction in time and monetary investment for remediating vulnerabilities. Therefore the financial benefit will encourage organizations to participate in sharing cyber intelligence.

Conclusion

Sharing cyber intelligence is still at an embryonic state and needs development to fully reach its potential. Different models and applications have been developed but are insufficient for today's threat landscape. Incentives are available, such as financial incentives that render threat sharing attractive. Negative sides were looked at too in this literature review that depicted the detriments of sharing, such as privacy issues. Threat sharing will enable organizations to ameliorate security defences.

References

Abouzahra, M. and Tan, J. (2014) "The effect of community type on knowledge sharing incentives in online communities: A meta-analysis," *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 1765–1773.

Barnum, S. (2012) "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)," *MITRE Corporation*, p. 11.

Bhimani, A., Marlow, W., Weiss, E. and Schugar, F. (2004) "Trusted and anonymous system and method for sharing threat data to industry assets," US6807569 B1, 19-Oct-2004.

Clancy, M. (2012) "Information sharing," *SC Magazine*, vol. 23, no. 2, p. 18.

Connolly, J., Davidson, M. and Schmidt, C. (2014) "The Trusted Automated eXchange of Indicator Information (TAXII ™)."

Constantine, C. (2012) "Threat intelligence: what to share?," *Database and Network Journal*, vol. 41, no. 1, p. 23.

Curran, J. (2013) "DHS Official: Private sector interest in threat-sharing program growing.," *Cybersecurity Policy Report*. [Online]. Available: http://ezproxy.bcu.ac.uk:2073/docview/1426059409?pq-origsite=summon. [Accessed: 24-Oct-2014].

Curran, J. (2014) "Cyber threat data-sharing venture formed by financial sector groups," *Cybersecurity Policy Report* [Online]. Available: http://ezproxy.bcu.ac.uk:2073/docview/1568138165?pq-origsite=summon. [Accessed: 29-Oct-2014].

Curran, J. (2013) "Security firms looking forward to more cyber threat data-sharing," *Cybersecurity Policy Report* [Online]. Available: http://ezproxy.bcu.ac.uk:2073/docview/1370934780?pq-origsite=summon. [Accessed: 31-Oct-2014].

Dumitras, T. and Shou, D. (2011) "Toward a standard benchmark for computer security research: the worldwide intelligence network environment (WINE)," *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security - BADGERS '11*, pp. 89–96, Gardin, D. (2012) "Threat Intelligence," *Leadership Excellence*, 2012. [Online]. Available: http://ezproxy.bcu.ac.uk:2073/docview/1151716690?pq-origsite=summon.

Guthrie, J. (2013) "Data sharing would help to neutralise the cyber threat," *FT.com*, 2013. [Online]. Available: http://ezproxy.bcu.ac.uk:2073/docview/1412190616?pq-origsite=summon. [Accessed: 04-Dec-2014].

Hofmann, M. (2012)"Fight rising cyber threats by sharing," *Business Insurance*, 2012. [Online]. Available: http://ezproxy.bcu.ac.uk:2073/docview/1023448994?pq-origsite=summon. [Accessed: 23-Oct-2014].

Hutchins, E. (2011) "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research 1*, vol. 1, p. 80.

IID (2014) "White Paper : Clearing the red tape ensnaring cybersecurity collaboration," 2014. [Online]. Available: http://internetidentity.com/wp-

content/uploads/2014/07/IID-Clearing-the-Red-Tape-white-paper.pdf. [Accessed: 09-Dec-2014].

Iimura, T., Miyamoto, D., Tazaki, H. and Kadaobayashi,Y. (2014) "NECOMAtter: curating approach for sharing cyber threat information," *Proceedings of The Ninth International Conference on Future Internet Technologies*, vol. 19.

Jajodia, S., Peng, L., Vipin, S. and Cliff, W. (2010) *Cyber situational awareness: Issues and research*, vol. 46. Boston, MA: Springer US, 2010.

Kampanakis, P. (2014) "Security Automation and Threat Information-Sharing Options," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 42 – 51.

Lee, W. and Rotoloni, B. (2014) "Cyber threats emerging report 2014,"
Mitre Corporation, "Cyber Observable eXpression A Structured Language for Cyber Observables," 2014. [Online]. Available: http://cybox.mitre.org/. [Accessed: 13-Dec-2014].

Moriarty, K. (2013) "Transforming expectations for threat-intelligence sharing," [Online]. Available: https://www.emc.com/collateral/emc-perspective/h12175-transf-expect-for-threat-intell-sharing.pdf. [Accessed: 25-Nov-2014].

Ring, T. (2014) "Threat intelligence: why people don't share," *Computer Fraud & Security*, vol. 2014, no. 3, pp. 5–9.

Sander, T. (2014) "HP Discover 2014: Fighting next-gen adversaries and automatically sharing threat intelligence [video online]," 2014. [Online]. Available: https://www.youtube.com/watch?v=wnoYbyLIu0c. [Accessed: 05-Nov-2014].

Sprenger, S. (2013) "NSA Chief Urges 'Real-Time' Threat Sharing Between ISPs, Agencies.," *Inside the Pentagon's Inside the Air Force*. [Online]. Available: http://ezproxy.bcu.ac.uk:2073/docview/1441247181?pq-origsite=summon. [Accessed: 23-Oct-2014].

Treglia, J. and Park, J. (2009) "Towards trusted intelligence information sharing," *Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics - CSI-KDD '09*, pp. 45–52.

Trope, R. and Humes, S. (2013) "By Executive Order: Delivery of Cyber Intelligence Imparts Cyber Responsibilities.," *IEEE Security & Privacy*, vol. 11, no. 2, pp. 63–67.

Vázquez, D., Acosta, O., Spirito, C., Brown, S. and Reid, E. (2012) "Conceptual framework for cyber defense information sharing within trust relationships," *(CYCON), 2012 4th*.

Wang, Y. and Vassileva, J. (2003) "Trust and reputation model in peer-to-peer networks," *Peer-to-Peer Computing.(P2P 2003). Proceedings. Third International Conference on*, pp. 150–157.

West, J. (2014) "Keynote - Fighting Next-Generation Adversaries with Shared Threat Intelligence. [video online]," 2014. [Online]. Available: https://www.youtube.com/watch?v=HXUyeUn-r_Q. [Accessed: 06-Nov-2014].