An Architecture for Privacy-preserving Sharing of CTI with 3rd party Analysis Services

Fabio Giubilo, Ali Sajjad, Mark Shackleton
Security Futures Practice
British Telecommunications plc (BT)
Adastral Park, United Kingdom
{fabio.giubilo,ali.sajjad,mark.shackleton}@bt.com

David W. Chadwick, Wenjun Fan, Rogério de Lemos,
University of Kent
Canterbury, United Kingdom
{w.fan, r.delemos, d.w.chadwick}@kent.ac.uk

Abstract—**Increasing numbers of Small and Medium Enterprises (SME) are outsourcing or hosting their services on different Cloud Service Providers (CSP). They are also using different security services from these CSPs such as firewalls, intrusion detection/prevention systems and anti-malware. Although for the SMEs the main purpose of using these security services is to protect their cyber assets, either physical or virtual, from security threats and compromises, a very useful and valuable by-product of these security services is the wealth of Cyber Threat Information (CTI) that is collected over time. However, a common problem faced by SMEs is that they lack the resources and expertise for monitoring, analysing and reacting to any security notifications, alerts or events generated by the security services they have subscribed to. An obvious solution to this problem is that the SMEs outsource this problem to a cloud based service as well, by sharing their CTI with this service and allowing it to analyse the information and generate actionable reports or patches. The more CTI obtained from different SMEs, the better the analysis result. In this paper, we try to address some of the privacy and confidentiality issues that arise as a result of different SMEs sharing their CTI with such a third party analysis service for the aggregate analysis scenario we just described. We present the design and architecture of our solution that aims to allow SMEs to perform policy-based sharing of CTI, while also offering them flexible privacy and confidentiality controls.**

Keywords: data privacy and confidentiality, cyber threat information, analysis services, infrastructure architecture, policy based sharing

I. INTRODUCTION

According to a recent survey commissioned by the UK Cabinet Office [6], the annual expense in the UK for cyber-crime is £27 billion (1.8% of GDP). This also states an estimate for UK cybercrime losses: £3 billion for citizens and the government, up to £21 billion for companies. Another report by the European Union Agency for Network and Information Security (ENISA) [3] states: "three-quarters of the businesses have seen cyber security as a concern for some time. The majority of respondents believed that their organisation has been the victim of a targeted attack. And almost a third of them reported a significant business impact."

Information security is also becoming a serious matter to consider for Small and Medium Enterprises (SME). They often wish to host their services on different Cloud Service Providers (CSP), increasingly deciding to provide their services over the Internet, exposing the services themselves to potential malicious users who attempt to disrupt those services. For this reason SMEs need security services at several layers, such as application (e.g., login portal of their service), network and infrastructure layers (e.g., the servers proving the service, the enterprise network and so on). Thus, for SMEs security is a complex issue to deal with, which often requires cyber security professionals, more expensive facilities and additional costs.

For enterprise customers there are a range of security services available from 3rd parties, typically referred to as Managed Security Services (MSS). Depending on the MSS provider (MSSP), the MSS can offer several security capabilities. Examples of MSSPs include BT Assure Threat Monitoring [19], SAP Enterprise Threat Detection [20], HPE SIEM Solutions [21], McAfee Enterprise Security Manager [22] and AlienVault Unified Security Management [23].

The Intelligent Protection Service [1] is an MSS developed by British Telecom which is aimed more towards SME customers. It provides services, such as firewalls, intrusion detection/prevention systems, anti-malware analysis, web reputation protection, log inspection and integrity monitoring. This solution can be managed by the SME itself, if they have sufficient capability and skills, or could in principle be outsourced to a 3rd party.

A very useful and valuable by-product of these security services is the wealth of Cyber Threat Information (CTI) collected over time by the MSS. CTI is defined by the National Institute of Standard and Technology (NIST) as any valuable information that can be used to identify, assess, monitor and respond to cyber threats [15]. As cyber threats are increasing considerably, SMEs have to be aware of potential risks, to deal with them in a timely and appropriate manner. This often represents a difficult challenge, due to SMEs' lack of resources, knowledge and expertise, firstly for handling the large amount of CTI data gathered by an MSS without being overwhelmed by it and secondly for monitoring, analysing and responding to any security notifications, alerts or events generated by the MSS.

An obvious solution for this concern might consist of outsourcing the analysis process to a cloud-based service by sharing the CTI data itself with the service, allowing it to generate actionable reports and/or patches. It is clear that in order to achieve a better, effective and timely analysis outcome the analysis service requires as much CTI data as possible, ideally from different SMEs. In this paper, we aim to introduce a capability for SMEs to be able to allow policy controlled sharing of CTI gathered from an MSS, while preserving privacy and confidentiality of that information. This aggregated CTI from different SMEs will be analysed by a cloud-based third party analysis service and the results will be shared among the SMEs. In our scenario, the above mentioned third party analysis service will be C3ISP [24], which is a flexible framework for carrying out secure data analytics being developed as part of a Horizon 2020 collaborative R&D project.

In the remainder of this paper we discuss related work in section II, the motivation for SME information sharing in section III, and the system architecture in section IV, followed by an analysis of the architecture in section V. Our conclusions are then presented in section VI.

II. Related work

Although we are presenting an original proposal for managing collaborative collection, sharing and analysis of CTI, several cyber security solutions exist that are related to our effort. As noted earlier, existing MSS are aimed towards larger enterprises, rather than SMEs. An example is BT Assure Threat Monitoring (ATM), which is a BT security solution oriented to enterprise customers. It is a security event monitoring service running 24x7x365. It operates by re-directing enterprise device data to a central BT Repository, where analysts examine and filter millions of messages from many devices, to discern the irrelevant ones from the suspicious and critical ones, and eventually notify the enterprise of any security concerns. Currently it is not possible to derive additional intelligence and more accurate analysis by sharing/combining the data belonging to different enterprises, since this data is stored in a strictly isolated manner (as it contains sensitive and confidential information).

Coco Cloud [13, 14] was a project that enabled cloud users to securely and privately share their information in the cloud environment. It provided mechanisms to raise trust in cloud services and therefore raise their widespread adoption with consequent benefits for users and for the digital economy in general. The main objectives consisted of:

- facilitating the writing, understanding, analysis, management, enforcement and dissolution of data sharing agreements (DSAs);
- considering the most appropriate enforcement mechanisms depending on the underlying infrastructure and context for enforcing data usage policies;
- addressing key challenges for legally compliant data sharing in the cloud.

By taking a "compliance by design" approach, the project placed an early emphasis on understanding and incorporating legal and regulatory requirements into the DSAs. We are using DSA mechanisms such as these within our framework [5].

III. Motivation

We allow SMEs to set up federations of information providers/consumers (called prosumers) in order both to obtain the information from other SMEs and to exploit the capacity of analysis of an amount of data such as might be available to a larger enterprise today. The overarching goal is that SMEs should be able to benefit from the MSS, in much the same way that a larger enterprise does. The barrier of the small size of an SME is overcome by allowing SMEs to share and combine security and threat information, so that its value will approximate to that available to a larger enterprise.

The need to share information between SMEs of course brings its own challenges [2-4]. In particular, the information might be considered to contain commercially sensitive or confidential data. Therefore our framework protects the information shared by the SMEs by using a DSA that can be attached to the information and will be enforced to protect such information. Options are provided to pre-process information in order to allow some analytics and, at the same time, to preserve the privacy and confidentiality of the data.

Some other features of our solution include:

- SMEs are able to choose the type of privacy and confidentiality controls that are appropriate for safeguarding their CTI data on the cloud-based analysis service, e.g. to select open access, or to apply data anonymisation techniques or even to use homomorphic encryption based techniques for very sensitive data.
- Through the availability of different data confidentiality and access options, SMEs can confidently share specific types of their CTI data via a gateway platform, even with non-trusted third parties.
- The framework can incorporate diverse techniques for supporting the protection of CTI data, as SMEs do not have to be aware of the inner workings of these techniques.
- The framework can also incorporate diverse techniques for analysing the shared CTI without the SMEs worrying about issues like information leakage, as this process is transparent for the SMEs.

IV. System Architecture

The scenario consists of extending the use of a multi-tenant and cloud-based MSS that can be deployed and configured for either public or private cloud environments. SMEs can subscribe to this MSS to enable it to protect their cloud-hosted assets. As SMEs may host their data and applications on cloud platforms different from the one operating the MSS, the MSS can be configured and allowed to acquire the relevant CTI directly from the applications, services, or virtual machines that are being protected by it.

Figure 1 shows a high level view of the system architecture. The SMEs communicate with the MSS to manage the security of the applications and services running on their VMs deployed on different cloud platforms. The MSS enforces the security policies set by SMEs directly on the VMs, which is usually done via a security agent deployed in the VMs. The SMEs delegate the C3ISP framework to collect and process the CTI to a middleware called the C3ISP Gateway, which has the capability of collecting, processing and sending the CTI in a standardised format to the cloud-based C3ISP Service. The SME also delegates the enforcing of the DSA to the C3ISP Gateway, which will process the CTI according to the DSA, before sending it to the C3ISP Service.

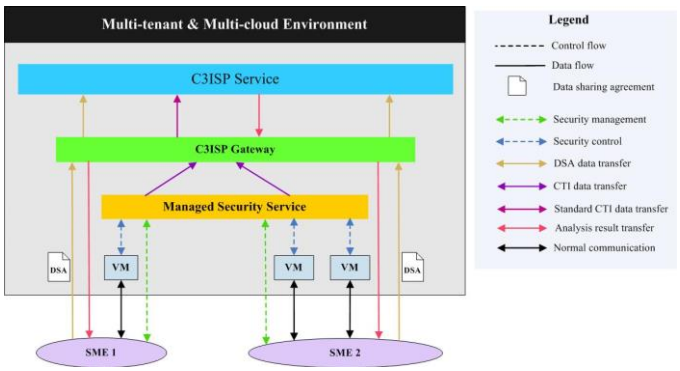

Figure 1. High level view of the system architecture

In the following sections, we discuss the detailed design of the main components of the system architecture using the FMC notation [7], which is a semi-formal but customised framework for describing the concepts and structures of complex informational systems.

A. Managed Security Service

SMEs subscribe to the MSS in order to configure, deploy and protect their assets. The process is illustrated below in Figure 2. The SME, by means of a browser, establishes a secure connection with the management portal of the MSS. Thereafter, the SME can subscribe to the MSS, register and customize VM protection and configure the MSS itself according to its requirements. Once the subscription is completed, credentials are issued to the SME to login to the Security Portal, enabling it to configure and activate/enable individual security services (anti-malware, IDS/IPS, firewalls, etc.) on its virtual machines.

The MSS deploys and enforces the security services and their policies by controlling an MSS Agent installed in the SME VMs. The MSS stores the CTI gathered by the agents on each virtual machine into a CTI database, accessible only from the C3ISP Gateway.

B. C3ISP Gateway

The C3ISP Gateway is the core component of the system architecture, which collects, processes and shares the CTI with the external C3ISP Service. It is illustrated in detail in Figure 3.

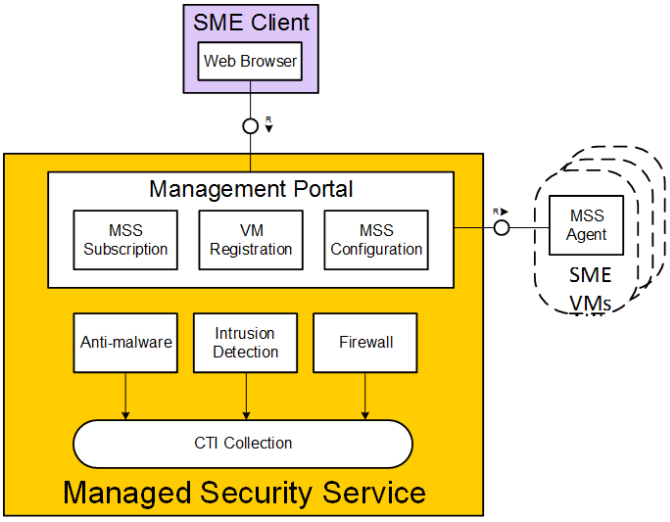

Figure 2. Managed Security Service architecture

The C3ISP Gateway retrieves the raw CTI from the MSS using the Tenant Manager. Once received, the raw CTI has to be formatted and processed by the C3ISP Gateway in accordance with the DSA [8-10] set by the SME. This is where the DSA Manager comes in, by letting the SMEs select DSAs by either configuring a set of pre-formulated policy templates [11,12], or even creating a completely new DSA. The DSA includes details regarding how the data can and cannot be used by the C3ISP Gateway and the C3ISP Service. For example, according to confidentiality levels specified in the DSA, the C3ISP Gateway is able to transform the CTI from raw format into plaintext STIX [15] format, and apply anonymisation [18] or homomorphic encryption techniques [17] on some of the raw CTI before its transformation. Once the DSA has been enforced, the C3ISP Gateway sends the CTI to the C3ISP Service.

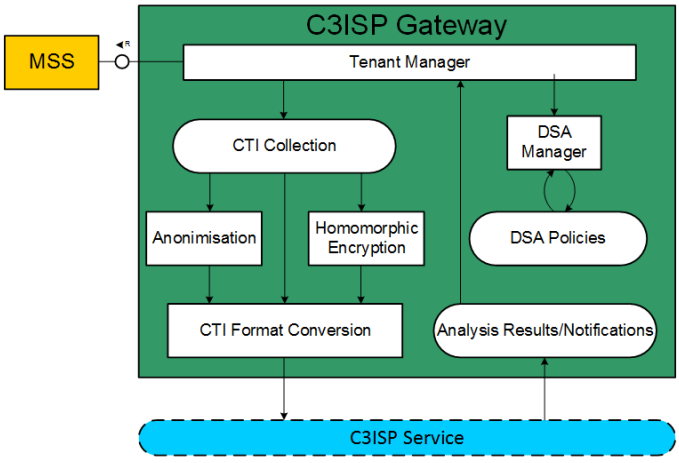

Figure 3. Information Processing Middleware architecture

Once the analysis is completed by the C3ISP Service, SMEs can retrieve the analysis results and outcomes, via the C3ISP Gateway.

V. Architecture Analysis

The C3ISP Gateway acts on behalf of the SMEs and essentially takes care of all the security C3ISP Services for collecting, converting and submitting the CTI to the C3ISP Service. It also provides SMEs with capabilities for defining and customising DSA policies in a user-friendly manner, via a web interface, and provides a front-end for retrieving the analysis outcomes. The C3ISP Service communicates strictly only with the C3ISP Gateway, to make it more difficult for attackers to compromise it.

The MSS also takes care of SME needs, not only for deploying new services and applications but also, and more importantly for security matters. According to our architecture, only the MSS is allowed to handle the security services installed and configured in the VMs, thus avoiding misconfigurations. It also provides CTI to the C3ISP Gateway in a secure way which is transparent to the SMEs.

These platforms are designed according to a modular idea/concept, bringing many advantages. From a security point of view, if the C3ISP Gateway were compromised by attackers, the anonymised and encrypted CTI would not be compromised and the overall damage would be mitigated. Having a modular architecture is also more suitable if the technology regarding specific modules changes in the future, for example regarding how CTI is stored and converted. If the encryption or the anonymisation technique changes, there is no need to change the entire architecture and platform, but only the modules involved.

VI. Conclusion

We have presented an original architectural model aiming to address the current limits of cyber security solutions. The proposal lets SMEs benefit from the same level of security that enterprises do today, via a Managed Security Services (MSS) solution. Our solution for SMEs employs three different platforms, the Gateway, the MSS and the Analytics service. There are several benefits in information sharing for cyber security (including incident notification) as well as several barriers to be removed. The benefits include, earlier detection of attacks, and that the analysis becomes collaborative, which should lead to more precise and informative outcomes. The information of one party can be of benefit to many others (thus leading to an increase of public good). Organisations fear the risk related to business reputation loss if the shared information reveals cyber security incidents which will be reported on public platforms. There are also other concerns related to the compliance with legislation (e.g., sharing of data involving personal information). Barriers of information sharing therefore include lack of trust in sharing data and lack of control over the data which has been shared, so it is important to provide privacy-preserving mechanisms of the type that we have proposed.

Acknowledgment

We acknowledge financial support for this work provided by the European Commission's Horizon 2020 research and innovation programme under the grant agreement No. 675320 (NeCS) and 700294 (C3ISP).

References

[1] Daniel, Joshua and El-Moussa, Fadi and Ducatel, Gery and Pawar, Pramod and Sajjad, Ali and Rowlingson, Robert and Dimitrakos, Theo Integrating Security Services in Cloud ServiceStores. In: Trust Management IX. IFIP Advances in Information and Communication Technology, 454. Springer International Publishing, pp. 226-239 (2015)

[2] Yu, H., Powell, N., Stembridge, D., Yuan, X.: Cloud computing and security challenges. In: ACM-SE 2012 Proceedings of the 50th Annual Southeast Regional Conference, pp 298–302 (2012)

[3] Catteddu, D., Hogben, G.: Cloud Computing Risk Assessment. European Network and Information Security Agency (ENISA) (2009)

[4] Dimitrakos, T.: Cloud Security Challenges and Guidelines. EIT ICT Labs Symposium on Trusted Cloud and Future Enterprises, Oulu, Finland. http://www.eitictlabs.eu/news-events/events/article/eit-ict-labs-symposium-on-trusted-Cloud-and-future-enterprises/ (August 2014)

[5] European Commission on "C3ISP project". Available at: http://cordis.europa.eu/project/rcn/202687_en.html

[6] Anderson,R., Barton, C., Bohme, R, Clayton,R, Eeten, M.J.G, Levi, M., Moore, T., Savage,S, Measuring the Cost of Cybercrime, WEIS 2012, available at http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf (2012)

[7] Knöpfel A, Gröne B, Tabeling P. Fundamental modelling concepts. Effective Communication of IT Systems, England. (2005)

[8] Marco Casassa Mont, Ilaria Matteucci, Marinella Petrocchi, Marco Luca Sbodio: Towards safer information sharing in the cloud. Int. J. Inf. Sec. 14(4): 319-334 (2015)

[9] C. Brodie et al. The Coalition Policy Management Portal for Policy Authoring, Verification, and Deployment. In POLICY, pages 247–249 (2008)

[10] C. Caimi, C. Gambardella, M. Manea, M. Petrocchi, D. Stella. Technical and legal perspectives in Data Sharing Agreements definition. Annual Privacy Forum (2015)

[11] Matteucci, Ilaria, Marinella Petrocchi, and Marco Luca Sbodio. "CNL4DSA: a controlled natural language for data sharing agreements." Proceedings of the 2010 ACM Symposium on Applied Computing. ACM (2010)

[12] Martinelli, Fabio, et al. "A formal support for collaborative data sharing." Multidisciplinary Research and Practice for Information Systems: 547-561 (2012)

[13] Deliverable D4.1: DSA Specifications, Methodologies, and Techniques, Coco Cloud EU FP7 Project, GA #610853

[14] Deliverable D5.1: Enforcement Architecture and Communication Protocol. Coco Cloud EU FP7 Project, GA #610853

[15] Barnum, Sean. "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)." MITRE Corporation 11: 1-22 (2012)

[16] NISP WG2 Plenary Report Information Sharing and Incident Notification available at: https://resilience.enisa.europa.eu/nis-platform/shared-documents/3rd-plenary-meeting-april-2014/ (2014)

[17] Carpov, Sergiu, Paul Dubrulle, and Renaud Sirdey. "Armadillo: a compilation chain for privacy preserving applications." Proceedings of the 3rd International Workshop on Security in Cloud Computing. ACM, (2015)

[18] Chen, K., Liu, L., Privacy-preserving Multiparty Collaborative Mining with Geometric Data Perturbation, IEEE Transactions on Parallel and Distributed Computing, Vol XX, (2009)

[19] BT Assure Threat Monitoring. https://www.globalServices.bt.com/uk/en/products/assure_threat_monitoring/BT_Assure_Threat_Monitoring.pdf

[20] SAP Enterprise Threat Detection. https://wiki.scn.sap.com/wiki/display/Security/SAP+Enterprise+Threat+Detection+-+Security+Monitoring+-+Data+Breach+Protection

[21] HPE SIEM. https://saas.hpe.com/en-us/software/siem-security-information-event-management

[22] McAfee Enterprise Security Manager. https://www.mcafee.com/us/products/enterprise-security-manager.aspx

[23] AlienVault Unified Security Management. https://www.alienvault.com/

[24] Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (C3ISP). http://c3isp.eu/