HOW TO ENHANCE THE SHARING OF CYBER INCIDENT INFORMATION VIA FINE-GRAINEDACCESS CONTROL

Jarno Salonen[1], Tatu Niskanen[2] and Pia Raitio[3]

[1]VTT Technical Research Centre of Finland, Tampere, Finland
[2]University of Jyväskylä, Jyväskylä, Finland
[3]Finnish Transport Infrastructure Agency, Helsinki, Finland

ABSTRACT

Industry 4.0 and the ongoing digital transformation along with a large number interconnected machines and devices increase the role of cybersecurity, cyber incident handling and incident response in the factories of the future (FoF). Cyber incident information sharing plays a major role when we need to formulate situational pictures about FoF operations and environment, and respond to cybersecurity threats related to e.g. the implementation of novel technologies. Sharing of incident information has a major drawback since it may reveal too much about the attack target, e.g. in the case of legacy systems and therefore restrictions may apply. We have developed a proof-of-concept service that combines access control and encryption of data at high granularity and a mechanism for requesting access to restricted cyber incident information. Theobjective was to demonstrate how access to restricted incident data fields could be managed in a fine-grained manner to enhance information sharing.

KEYWORDS

Incident Management, Visualisation, Cybersecurity, Information Sharing.

1. INTRODUCTION

Industry 4.0 promotes the use of emerging technologies such as Internet of Things (IoT), Big Data, artificial intelligence (AI) and cloud computing, supported by cyber-physical systems, as the design to achieve what they call smart factories or factories of the future (FoF). One common characteristic of Industry 4.0 is to decentralise production systems [1] and allow controlling, monitoring, adaptation, and optimisation to be done in real time, based on the large amounts of data available in the factory environment that feeds the use of machine learning (ML) techniques. This so called fourth technological revolution is expected to bring significant gains in productivity, resource savings and lower maintenance costs, as machines will have all the information necessary to operate more efficiently, adaptable and keep up with any fluctuations in demand. Devezas et al. (2017) summarised Industry 4.0 to comprise strong customisation of products under high flexibility mass production that require the introduction of methods for self-organised systems to establish a suitable link between the real and virtual worlds [2].

The rapid human evolution and the search for strategies that facilitate our daily lives, imply a close synergy with technology that must adapt to the user needs. In this context, HMI (Human Machine Interface) interfaces emerge, responsible for human-machine interconnection. HMI, as the name already indicates, consists of software and hardware that allow an operator (human) interact with a controller (machine) [3]. The term "machine" is defined by Merriam-Webster as "*mechanically,*

David C. Wyld et al. (Eds): DMML, SEAS, ADCO, NLPI, SP, BDBS, CMCA, CSITEC - 2022
pp. 195-208, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.120717

electrically or electronically operated device for performing a task" [4]. In other words, a machine is a device that has the function of transmitting or modifying energy to perform a certain task that assists the human being. Technically, you could apply the acronym HMI to any kind of screen or visual display that someone uses to interact with a device, but in general, we use it to describe screens used in industrial environments. HMIs display real-time data and allow the user to control the equipment using a graphical user interface. In the industrial environment, the HMI can take many forms. It can be a standalone screen, a panel connected to other equipment, or even a tablet computer. Despite of its looks, the primary purpose of HMI is to allow users to view data about the device operations and control it. Operators can use an HMI, for example, to see which conveyor belts are running or adjust the temperature of an industrial water tank.

In terms similar to human-human interaction, humans as rational beings also need to communicate and interact with technological systems, hence the emergence of artificial intelligence (AI). Artificial intelligence, which we consider today as a domain of knowledge, and define as the type of intelligence similar to that of the human but displayed through mechanisms or software. Thus, the "intelligent agent", which is also often called as autonomous agent, is a system that perceives the entire environment (internal and external factors) via sensors and acts rationally (generally makes decisions to maximise its success) upon that environment with its effectors. Weiss et al. (1999) define intelligent agent being capable of flexible autonomous actions in order to meet its design objectives and where flexible means reactivity, pro-activeness and social ability [5]. The goal of an intelligent system is to perform functions, with the ability to establish logical reasoning (by means of established rules), recognising patterns, learning (acquiring future knowledge future knowledge based on mistakes), and inference (apply reasoning to everyday situations). In the caseof a vehicle, the human being adopts the role of driver and performs the interaction with the entiresystem present in the vehicle. Therefore, this system must be prepared to interact with the driver through the most appropriate means of communication (e.g. haptics, images, and/or sound), and must be able to recognise the interactions used by the driver. The previous can be applied to the factory of the future where the human operator is the driver and the industrial system or multiple (interconnected) systems represent the vehicle(s).

All technological development, for example the fourth technological revolution with its decentralisation, breakthrough technologies such as Industrial IoT and AI, and the convergence of human and machine interaction have also weaknesses. In this case, one major weakness is cybersecurity. The digital transformation of the FoF involves a growing number of interconnecteddevices, which we need to protect from hackers and other malicious third parties. Traditionally theoperational technology (OT) systems of factories were isolated from the (public) internet, but thisseparation is no longer valid. This is due to e.g. robots being maintained remotely while membersof the supply network gain access, not only to the factory information technology (IT), but also toOT systems in order to, e.g. collect orders, acquire production specifications or update their own production information to the system. In addition, customers or service providers may access thesesystems directly in order to obtain production schedules or even optimise factory operations via the use of existing production data.

In order to maintain an adequate level of cybersecurity within the FoF during the aforementioned development, we need to update our cybersecurity strategy to meet the requirements of the FoF. The strategy consists of among others the following items:

- FoF cyber risk and threat management
- Development and implementation of cybersecurity policies for access and trust management within the FoF
- Evaluation of new technologies (e.g. 5G and AI) potential cybersecurity vulnerabilities
- FoF monitoring and incident response (intrusion detection/prevention systems, SIEM,

SOC, etc.)
- Organisation of cybersecurity training and awareness activities
- Planning of decision-aided or autonomous remediation and recovery of assets in case of a cyber incident

This article focuses on the topic of FoF monitoring and incident handling and response by introducing a proof-of-concept for a fine-grained cyber incident information sharing which is also the basis of cyber situational awareness for the FoF. Our research questions are the following:

1. How can we enhance incident information sharing between organisations?
2. How should we modify the IODEF data format to enable encryption and decryption?
3. How to request and enable the sharing of sensitive information in the cyber-incident dashboard (service)?

We developed this proof-of-concept as part of an ongoing Horizon 2020 project. Due to the nature of the PoC and the schedule of the project, the concept does not involve end-user-evaluation or the security and vulnerability testing of the service. This is because the objective was to discover new and innovative possibilities for sharing incident information in a fine-grained manner.

The article is structured as follows. We begin by describing the terminology and existing research behind our concept. Then we describe our methodology related to the IODEF data format update, visualisation aspects and the development of the event generator, which we used to generate random IODEF data content. In chapter 4, we describe the developed incident manager dashboardand some of its functionalities. Finally, we discuss about the findings during our research and futureR&D topics before we conclude the article.

2. THEORETICAL PERSPECTIVE

NIST defines cybersecurity as "*the process of protecting information by preventing, detecting and responding to attacks*" [6]. The prevention, detection and response to cyber-attacks has been studied quite extensively during the two decades. For example, Lee (2015) has studied the prevention of cyber-attacks and their response and listed both technical (firewalls, routers, filtering, etc.) and non-technical (training, information sharing, awareness-raising, etc.) means for different kind of cyber-attacks ranging from Distributed Denial of Service (DDoS) attacks to phishing and data breaches [7]. Indre and Lemnaru (2016) propose a solution against malware and intrusion attacks that is based on intrusion detection and prevention systems [8]. Kholidy has studied autonomous mitigation of cyber risks in cyber-physical systems (CPS) [9] and Zhou et al. have studied a multi-agent-based hierarchical detection and mitigation of cyber-attacks in smart grids [10]. In addition to the scientific contribution, the U.S. National Institute of Standards and Technology (NIST) has introduced its own cybersecurity framework to create a baseline and a toolbox to protect the government, critical infrastructure and individual companies against cyber-attacks, which includes among others learning material, implementation guidance and even models for evaluating the security maturity of the organisation [11].

Two key measures for improving the cybersecurity of the FoF or any other organisation is situational awareness and information sharing. According to Gilson (1995) the term "situational awareness" was first identified by Oswald Boelke during World War I who described it as "*the importance of gaining an awareness of the enemy before the enemy gained a similar awareness, and devised methods for accomplishing this*" [12]. The CNSS Glossary defines situational awareness as "*the perception of an enterprise's security posture and its threat environment*" [13]. Information sharing has been studied by, e.g. Harrison and White (2012), and Steenbruggen and Nijkamp (2012) both highlighting the importance of information sharing and proposing methods

for enabling communities to detect cyber incidents via the use of shared security information [14] and stating that public organisations often have information that is valuable to each other's operations [15]. In general, legislation such as the General Data Protection Regulation in Europe requires cyber incident reporting in the case of a breach of personal data, but it does not cover reporting of other incidents [16]. The same applies to the U.S. and China where the respective privacy acts have been enforced to protect the personal data of citizens, but other incident reporting is often voluntary though strongly recommended. There are some exceptions though. For example, national legislation often forces critical infrastructure providers to report any kind of incidents that influence their operations to the supervising authority.

In cybersecurity, situational awareness and information sharing often conflict with each other. Even though sharing cyber incident information may help others prevent the same kind of cyber-attack, it may reveal other vulnerabilities that may cause new and even larger attacks against the party sharing the incident information. For example, the description of the attack or its countermeasures may reveal that the target was a specific legacy system, which makes it possible for the malicious third party to focus on its known vulnerabilities. This makes the supervising authorities' role as the middle-man quite difficult. After all, they receive the information from all (cyber) incidents, but they necessarily cannot share the information to other relevant parties even within the same sector. The risks of sharing cyber incident information have been studied by Mallinder and Drabwell (2014) [17] and Albakri et al. (2018) [18] while Lawton and Parker (2002) focused on barriers in incident reporting of a healthcare system more than a decade earlier [19]. This information sharing issue has been partially solved by establishing sector-based Information Sharing and Analysis Centers (ISACs). According to the definition by ENISA (2018) ISACs are "*trusted entities to foster information sharing and good practices about physical and cyber threats and mitigation*" [20]. Most countries have their own ISAC networks focused especially in critical infrastructure sectors. In Finland, there are eleven different ISAC groups ranging from food production and distribution to water management and hosted by the National Cyber Security Centre [21].

3. DESIGN AND PLANNING

In this section, we describe the methodology related to the IODEF data format update. Then we will describe the development of the event generator, which we used to generate random IODEF data content so that we can test the incident dashboard with data that resembles actual incident reports and encrypt some of the field contents. Finally we will focus on the main topic, i.e. the incident manager dashboard and its visualisation.

3.1. Applying fine-grained access control to the IODEF data format

In order to demonstrate and visualise fine-grained access control (FGAC) in action, we created an applicable use case. The selected demonstrative use case is the visualisation of fine-grained access control in cybersecurity incident documents, also known as reports, and more specifically, incident documents in the incident object description exchange format (IODEF). IODEF is a data format used to describe cybersecurity incident information for exchange between computer security incident response teams (CSIRTs). IODEF was first defined in RFC5070 [22] and it was later updated to version 2 in RFC7970 [23]. The format is used in multiple software and other real-world applications, such as in the security information and event management system SIEM.

According to the RFC7970, IODEF has the following main information fields that are shown in table 1.

Table 1. IODEF file fields [23]

Field	Multiplicity	Description
IncidentID	One	An incident identification number assigned to this incidentby the CSIRT who creates the IODEF document.
AlternativeID	Zero or one	The incident ID numbers used by other CSIRTs to refer tothe incident described in the document.
RelatedActivity	Zero or one	The ID numbers of the incidents linked to the onedescribed in this document.
DetectTime	Zero or one	Time at which the incident was detected for the first time.
StartTime	Zero or one	Time at which the incident started.
EndTime	Zero or one	Time at which the incident ended.
ReportTime	One	Time at which the incident was reported.
Description	Zero or more	Non-formatted textual description of the event.
Assessment	One or more	A characterisation of the incident impact.
Method	Zero or more	Techniques used by the intruder during the incident.
Contact	One or more	Contact information for the groups involved in theincident.
EventData	Zero or more	Description of the events involving the incident.
History	Zero or more	A log, of the events or the notable actions which tookplace during the incident management.
AdditionalData	Zero or more	Mechanism which extends the data model.

In addition to these main fields, IODEF contains multiple other less used and optional fields. For the scope of this demo, we deal only with the main fields. We can apply fine-grained access control to the IODEF documents when incident information needs to be shared with parties in an organised manner, but the parties have different privileges to the incident information. Fine-grained access control allows the encrypted documents to be uploaded to a central location so the information can be shared as fast as possible. This way the party in charge of distributing the incident information does not need to alter the information in the document for every receiver. Fine-grained access control can also be used to dynamically encrypt individual tags in an IODEF document, based on the privileges of the reader.

To demonstrate the possibilities of fine-grained access control in IODEF documents, a dashboard was created. The dashboard is a demo of a cybersecurity incident management cloud service, where the incident information can be uploaded in the IODEF format. The users of the service can then view these documents and only access the information they are authorised to. The dashboard is developed with Angular 12 typescript framework. It has simple demonstrative login and logout functionalities and allows you to login as four different users in order to demonstrate the fine-grained access control with IODEF documents. You can then view two different documents as each individual user to see the varying access rights in action.

3.2. Event generator and API

For simulation purposes we developed an event generator to allow gathering information about the functionalities and response of the system. By firing stochastic incident events that simulate the incidents happening within a real productive scenario, the event generator works as the base engine of the simulation environment, producing plausible incident data that can visualised across all the dashboards of different actors and locations.

Each of the fired incident events follows the Incident Object Description Exchange Format (IODEF) RFC5070 Standard, which is XML-based data with a human readable structure. Each file contains at least one incident entity, with each entity being comprised by the fields listed in table 1.

The fine-grained access control functionality manages the ability of certain actors to visualise these fields in a different way, and acts in conjunction with the cryptographic keys. The event generator randomly selects a subset of tags within the IODEF document, and encrypts them with a randomly generated key and a certified and secure cryptographic algorithm. The individual teams or users can then request this key, by providing the necessary data such as the unique user identification (UID) and the incident identifier. These encrypted tags contain the FGAC keyword as an XML attribute with the team/user identification numbers, which can access and decrypt them. This way, when the document is shared, the sensitive tags are shared encrypted and, unless using a key, cannot be viewed in plain text.

The event generator system was designed to be object-oriented with a strict segregation of responsibilities between different components. It contains a central component, IODEF generator, responsible for generating the documents and assign them to different products. It also contains an XML processor component, responsible for building valid XML documents from the generated incidents, sharing them with the team. The event generator overall architecture is displayed in figure 1 below.

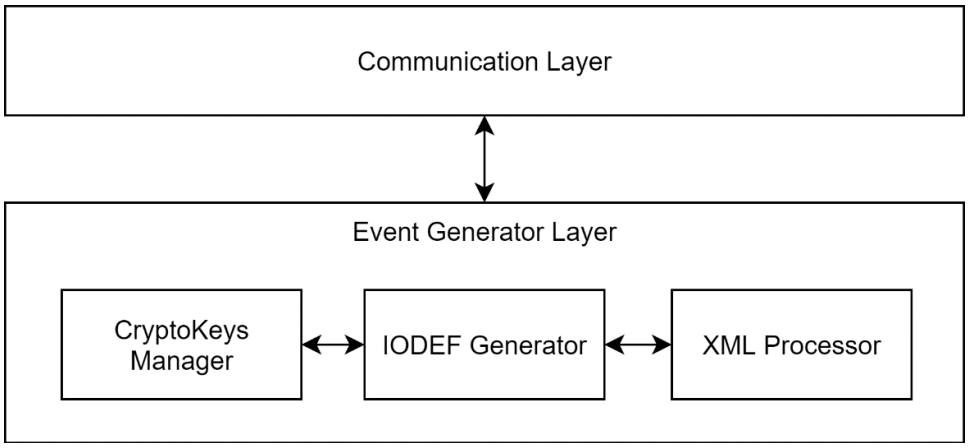

Figure 1. Event generator architecture

Since the dashboards are to be web-based, the event generator has a communications layer using HTTPS protocol, in order to quickly and effectively exchange data with the different dashboards.

The communication methods of the event generator are displayed in table 2 below.

Table 2. Event generator communication methods

Method	**Description**	**Parameters**
/InitSimulation	Initializes/resets the simulation.	None
/GetSimulationData	Returns all the generated IODEF documentsand organizations in both JSON and XML format	None

/GetKey	Returns the key used to decrypt elements thatare encrypted within an FGAC tag	Owner, IncidentID and TagName

The InitSimulation method allows the user to reset the simulation, creating new organisations and IODEF documents. GetSimulationData returns both the list of generated organisations and IODEF, together with the assignments between both entities, in JSON and XML (IODEF standard) format. Lastly, GetKey is used for requesting a cryptographic key that can decrypt a set of sensitive information of an IODEF document. This key is only returned if both the tag and the organisation that is requesting the key match, avoiding giving keys to unwanted entities.

Since this article focuses on the incident dashboard and the visualisation of incident data, we will consider the event generator as a black box with the desired output that the incident manager receives and processes from this point forward and therefore we will not describe the event generator any more.

3.3. Visualisation of incidents in a fine-grained manner

One task of our project, the collaborative monitoring and response task aims to design and implement a collaborative security operations center (SOC) for distributed operations. It collects all relevant information, then orchestrates, analyses it, and finally responds to security incidents in a timely manner. The objective is to enable collaborative incident response on distributed manufacturing environments, shorten the decision making, response and recovery time, and optimise attack and response resources (costs). Information sharing is seen as a key element to support vulnerability, threat and incident management, and thus helping organisations to prepare and prevent cyberattacks. However, it is primarily based on trust, which is also seen as the most significant barrier to organisational information sharing as e.g. Albakri et al. (2018) state in their research [18].

In this work we have focused on boosting the trust in incident information sharing by using fine-grained access control. The aim is to reveal only pre-allowed pieces of incident data to different users or groups. For example, an automotive factory that has been attacked may allow that all incident information may be shared with their named SOC operator who works in close collaboration with them, but other SOC operators do not see the target IP address which was under attack at the factory. The factory may also allow sharing of the incident details to other automotive factories in Europe, which might be targets to a similar attack as it seemed to be targeted to the automotive sector. However the factory allows sharing of only the very basic details to other European factory operators, not revealing, e.g. what was the targeted factory and when did the attack happen. By revealing too much information, it might be possible to count one plus one and figure out what was the targeted organisation or/and system. By sharing too much information about the incident, the information might end up into the hands of a malicious third party who may get insights of how successful their attack was. Thus, using fine-grained access control we try to create a PoC of a system that would boost organisations into sharing incident information in a trustable manner.

In order to visualise the incidents in a fine-grained manner, the IODEF documents are enhanced with fine-grained access control tags. These tags act as attributes to the fields containing the incident information. The users are then granted access to the encrypted information based on these tags. The users can be saved in a database and given two corresponding tag-attributes. One specifies the clearance group the user belongs to and the other is a specific tag belonging to the user. The responsible SOC can then distribute IODEF information based on the clearance groups or by the specific user. The SOC can achieve this by populating the IODEF document with the corresponding tag-attributes within the information fields. The Angular front-end then compares these tags within the IODEF document to the ones held by the logged in user. When the tags match, the information in the IODEF-document is displayed to the user. Otherwise a placeholder text "You are not authorised for this information" is shown. In the demo, the information is encrypted if the user has not authorisation to view it. In case the user has no authorisation, the system consist of a functionality for requesting permission (namely a decryption key) to the data from the data owner, which can then be used to decrypt the information.

There is already some research conducted on fine-grained access control systems for XML-documents. For example, Luo et al (2004) have presented the QFilter method for fine-grained run-time access control for XML-documents. In the research it is stated that it is crucial to tailor information in XML-documents for various user and application requirements, preserving confidentiality and efficiency at the same time. Thus, it is critical to enforce access control over XML data to ensure that the users only have access to the portion of the data they are allowed to. The research currently presents different access control methods for XML-documents, but only little to no research has been done on visualisation of fine-grained access control. [24]

When choosing how to visualise encrypted data in a fine-grained manner, it is also important to decide on how to convey the data that is not visible to the viewer. In some contexts, the best approach is not to show the data at all. In other contexts, a better approach is to convey that the data exists but hide it from the unauthorised viewer in other ways. Possible approaches to visualising the hidden data include:

- Blurring, overlining and other visual hiding methods
- Placeholder text, such as "You are not authorised to view this information"
- Not showing the hidden information at all

In this case, our chosen approach was a placeholder text. This is because the document does not contain fields whose existence in itself is classified. In some other fine-grained access control situations, the existence of the hidden items may be information that should not be shared with all parties. The existence of the hidden information may be enough for the intruder or other malicious party to get interested and therefore figure out where to intrude.

In order to be able to visualise data in a fine-grained manner with many different users having access to the same document, it is important to structure the document in a way that supports implementing fine-grained access control. This is where structures such as IODEF are helpful. When the structure of the document is predefined, the programming logic behind the fine-grained access control is easier to implement and maintain. If fine-grained access control is to be implemented in a cloud environment, for example for viewing documents, it should be considered to come up with a predefined and commonly agreed structure for the shared documents. Formats such as IODEF can be adapted to other contexts. For example in the automotive industry, predefined formats such as IODEF can be applied to the manufacturing manuals shared in the cloud. The predefined individual tags or fields allow for easy distribution of access control.

4. IMPLEMENTATION OF THE INCIDENT MANAGER

This section describes the implementation of the incident manager dashboard (service) as well as its functionalities. The incident manager dashboard is a service (frontend application) for viewing incident information that is stored in an external (cloud) repository. The service requirements towards the repository in addition to being the source of incident information (IODEF) data are the implementation of fine-grained access control (FGAC) tags along with the encryption mechanism of any desired individual incident information field. In addition, the repository should offer the possibility to provide the decryption key to the incident manager dashboard based on a request from the manager.

After launching the service from the browser, the user is shown an empty dashboard with instructions to perform user login. After the user has logged into the service, the user clicks the "Fetch Incidents" button to download incident data from the (cloud) repository, which in this case is represented by the event generator. The figure below (Figure 2) displays the incident manager dashboard after the user has logged in and fetched the incident data. As you can see from the figure, the dashboard screen is divided into two sections. The left half of the dashboard shows a list of incidents and when the user clicks on a specific incident, the detailed incident information is displayed on the right hand side. In this case the user can see six incidents. Please also note that the user has full privileges, i.e. he can see all fields in incident number six.

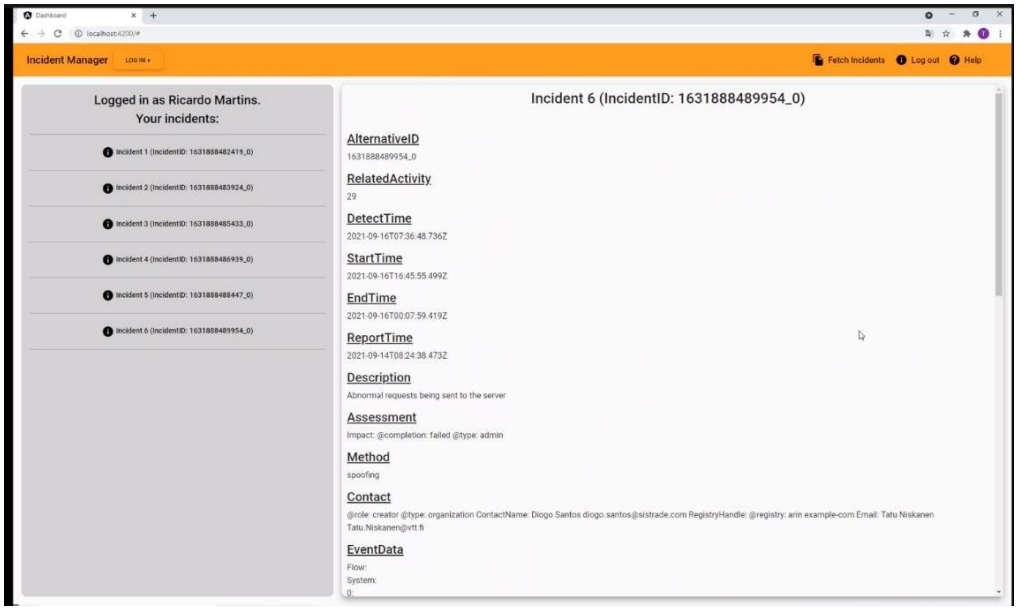

Figure 2. Incident view by user with "all" privileges

The figure (Figure 3) shows the same incident six as before, but with a different user who has a restricted view. Instead of showing the field content, the user sees a placeholder text with "You are not authorized for this information" along with a "Request key" button, which is used for requesting access to that specific field content.

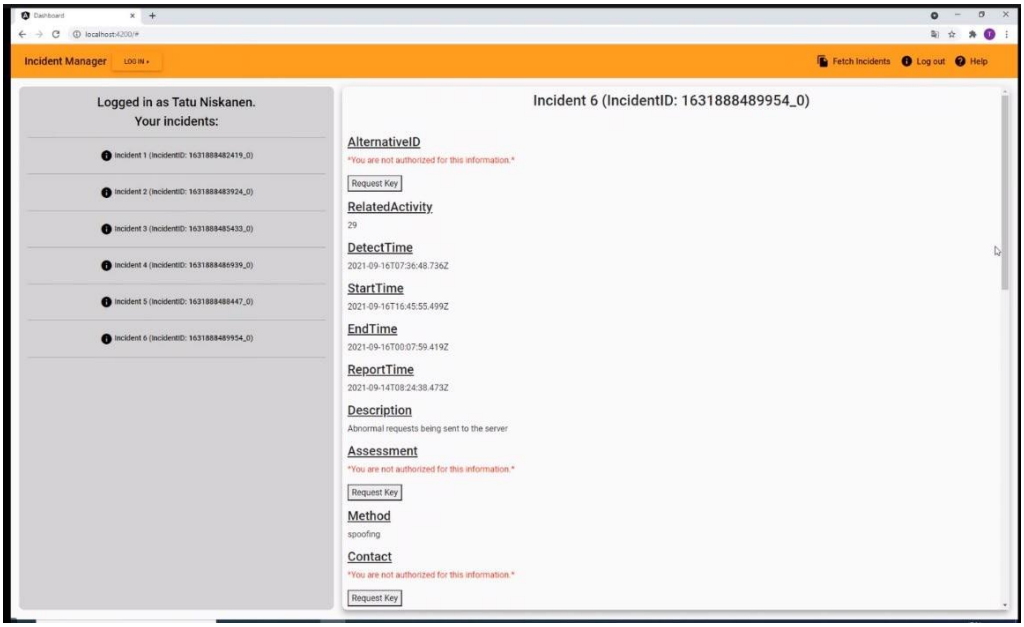

Figure 3. Incident view with restricted access showing both visible and encrypted fields

This functionality highlights the high granularity of the service, i.e. each field has been encrypted with its own key and therefore access is requested for each field separately.

The next figure (Figure 4) shows the incident manager dashboard after the user has clicked the "Request key" button in order to gain access to the encrypted data content.

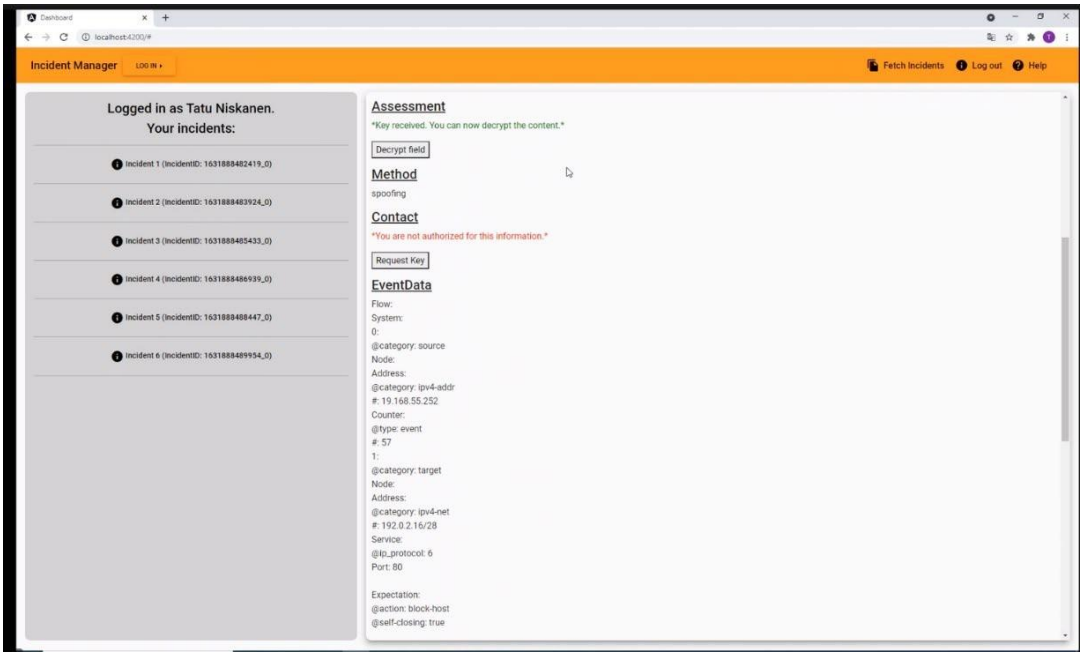

Figure 4. Incident view with decryption key received from the data owner

Clicking the button sends the user and field identifiers to the data owner (which in this case is represented by the event generator) who grants access to the data and therefore sends the decryption

key to the incident manager dashboard. In this case, the user sees a message that the access to the field content has been received and he can then click on the “Decrypt field” button to display the content.

The last figure (Figure 5) displays the incident view with the restricted content now visible to the user. Please note that only the requested field information is shown to the user, i.e. if the user wishes to see the content of other restricted fields, then he should click on the respective “Request key” buttons to request access to them. In other words each incident information field has been encrypted with a unique key and therefore the received decryption key works only for that one specific field. You may also note that the structure of the field content visible in Figure 5 is slightly different from the content in figure 2, i.e. the decrypted data has line spaces between the different words while the user with “all privileges” did not have them (i.e. all field data was in one row). This is mainly due to the technical encryption and decryption process which will be taken care of in the next version of the service.

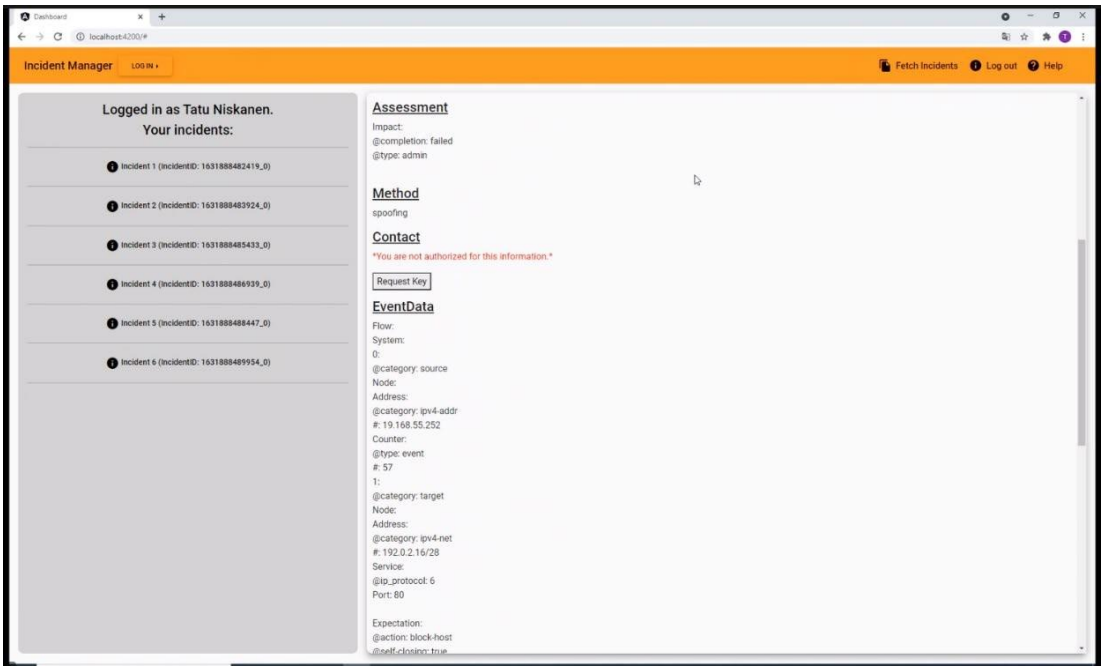

Figure 5. Incident view with decrypted field information visible to the user

5. DISCUSSION AND FUTURE WORK

This section describes the major observations that we discovered during the development of the incident manager dashboard. This list of observations is not an exhaustive one, but rather a review of what kind of functionalities we considered to be useful in future work, i.e. the next version of the service.

The PoC offers only username and password as the only available authentication mechanism, but it would be possible and also highly recommended to use two-factor authentication (2FA) or a similar strong authentication mechanism to identify and authorise the user properly. Since our objective was to demonstrate the incident information sharing functionalities of the dashboard, as well as the visualisation, we decided not to waste time on implementing strong authentication into the service.

The PoC includes only one repository for downloading incident information, but it would be possible to fetch incident information from any available repository included in the list of sources. The "Request key" functionality resulted in automatic granting of access rights from the event generator, i.e. it sends the decryption key to the service immediately. It would be possible to demonstrate an open text for justifying the access request to the incident information owner, but since we had only one repository at use and the user interface of the data owner nor the manual access-granting mechanism was not included in our objectives, they were not implemented. In any case the user interface for the data owner could be implemented either directly to the incident manager dashboard or it could be done e.g. via email. In the latter case the justification message would be sent via email to the owner (using the email listed in the incident contact information) and the message could also include links to approve or reject the request), which might provide added usability to the system.

During the PoC development, we also discussed about the access right (key) validity period. The access right to an individual field could be given for a certain time period, it could be based on the number of times that the user reads the restricted content, or it could also be valid indefinitely. Since this wasn't the objective of this PoC, we decided to grant only one time access rights, i.e. the key was valid only for that specific login session, which was enough for our demonstration. The decision is often dependent on the data owner and therefore we should perhaps offer multiple options for choosing the validity period in the next version of the incident manager.

Like we described in the introduction section, we did not consider an end-user piloting nor evaluation to the PoC. Neither did we consider conducting security testing to the system or cryptographic analysis to the encryption/decryption functionality. These decisions were made intentionally since the objective of the PoC was to test the possibility of sharing incident information in a novel way.

The future research and development activities would consist of a thorough evaluation of the proposed service. It would consist among others an analysis of the service efficiency and applicability, collection and statistical analysis of the views from end-user evaluations, and a comparative analysis covering the advantages and disadvantages of the service compared to other (existing) incident reporting management tools and services. The evaluation would include an implementation of the service to a real incident management reporting use case with actual incident data. In addition we could test the security of the service and the developed encryption mechanism, and try to find a similar tool or service from another sector/topic in order to compare the evaluation results with each other.

Since the project is very close to its end, we do not have plans to develop the incident manager dashboard further at this stage. However in case we find another suitable project, then we might reconsider creating the next iteration of the service. Due to the current trend of cybersecurity information sharing and this topic being in the focus of the current Horizon Europe Cybersecurity topic calls, future development might be highly possible.

6. CONCLUSIONS

This article describes the research and development of a proof-of-concept incident manager dashboard (service) that combines access control and encryption of data at high granularity, and a mechanism for requesting access to restricted cyber incident information. We claim that the PoC will enhance incident information sharing between organisations since it allows the sharing of incident (IODEF) data while applying access control and encryption in a fine-grained manner to individual fields containing sensitive information in the perspective of the information owner. The access rights are implemented into the IODEF in the form of FGAC tags that are defined separately

for each field, enabling the fine-grained access control and encryption functionality. The service also demonstrates a way to request access to one or more restricted (encrypted) IODEF fields within the incident information, while maintaining the full control of data within its owner. The article also discusses about the observations regarding some missing but perhaps useful functions that could be implemented in next iterations of the PoC.

ACKNOWLEDGEMENTS

This article is based on research and development work conducted together with the Portuguese partner Sistrade in the Secure Collaborative Intelligent Industrial Assets (SeCoIIA) project. SeCoIIA aims at securing the digital transition of manufacturing industry towards more connected, collaborative, flexible and automated production techniques. The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871967.

REFERENCES

[1] Meissner, H., Ilsen, R., Aurich, J. (2017). Analysis of Control Architectures in the Context ofIndustry 4.0. Procedia CIRP. 62. 165-169. 10.1016/j.procir.2016.06.113.
[2] Devezas, T., Sarygulov, A. (2017). Industry 4.0. Basel: Springer. 10.1007/978-3-319-49604-7
[3] NIST, S. (2015). 800-82 Rev 2. Guide to industrial control systems (ICS) security. 10.6028/NIST.SP.800-82r2.
[4] Definition of Machine. Available from: https://www.merriam-webster.com/dictionary/machine (Accessed 15.2.2022)
[5] Weiss, G. (Ed.). (1999). Multiagent systems: a modern approach to distributed artificial intelligence. MIT press.
[6] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). Developing cyber resilient systems: a systems security engineering approach (No. NIST Special Publication (SP) 800-160 Vol. 2 (Draft)). National Institute of Standards and Technology. 10.6028/NIST.SP.800-160v2r1.
[7] Lee, N. (2015). Cyber attacks, prevention, and countermeasures. In Counterterrorism and Cybersecurity (pp. 249-286). Springer, Cham. 10.1007/978-3-319-17244-6.
[8] Indre, I., Lemnaru, C. (2016). "Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things," 2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP), pp. 175-182, 10.1109/ICCP.2016.7737142.
[9] Kholidy, H. A. (2021). Autonomous mitigation of cyber risks in the Cyber–Physical Systems. Future Generation Computer Systems, 115, 171-187. 10.1016/j.future.2020.09.002.
[10] Zhou, T. L., Xiahou, K. S., Zhang, L. L., & Wu, Q. H. (2021). Multi-agent-based hierarchical detection and mitigation of cyber attacks in power systems. International Journal of Electrical Power & Energy Systems, 125, 106516. 10.1016/j.ijepes.2020.106516.
[11] NIST. 2021. Cybersecurity framework. https://www.nist.gov/cyberframework (Accessed:15.2.2022)
[12] Gilson, R. (1995). Situation awareness — special issue preface. Hum. Factors 37 (1), 3–4.
[13] Dukes, C. W. (2015). Committee on national security systems (CNSS) glossary. CNSSI, Fort 1322 Meade, MD, USA, Tech. Rep, 1323, 1324-1325. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf (Accessed: 15.2.2022)
[14] Harrison, K., White, G. (2012). Information sharing requirements and framework needed for community cyber incident detection and response. IEEE Conference on Technologies for Homeland Security (HST) (pp. 463-469). IEEE. 10.1109/THS.2012.6459893.
[15] Steenbruggen, J., Nijkamp, P., Smits, J. M., Mohabir, G. (2012). Traffic incident and disaster management in the Netherlands. Challenges and obstacles in information sharing. Netcom. Réseaux, communication et territoires, (26-3/4), 169-200. 10.4000/netcom.975.
[16] European Commission. (2018) Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01). European Commission / Data protection Newsroom. https://ec.europa.eu/newsroom/article29/items/612052 (Accessed 16.2.2022)
[17] Mallinder, J., & Drabwell, P. (2014). Cyber security: A critical examination of information sharing

versus data sensitivity issues for organisations at risk of cyber attack. Journal of business continuity & emergency planning, 7(2), 103-111.
[18] Albakri, A., Boiten, E., De Lemos, R. (2018). Risks of Sharing Cyber Incident Information. In Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018). Association for Computing Machinery, New York, NY, USA, Article 58, 1–10. 10.1145/3230833.3233284
[19] Lawton, R., & Parker, D. (2002). Barriers to incident reporting in a healthcare system. BMJQuality & Safety, 11(1), 15-18. 10.1136/qhc.11.1.15
[20] ENISA. (2018). Information Sharing and Analysis Centers (ISACs) - Cooperative models. European Union Agency For Network and Information Security. 10.2824/549292
[21] National Cyber Security Centre. (2022). ISAC information sharing groups. Finnish Transport and Communications Agency. https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups (Accessed 16.2.2022)
[22] Danyliw, R., Meijer, J., Demchenko, Y. (2007). RFC5070 - The Incident Object Description Exchange Format. Internet Engineering Task Force (IETF), Network Working Group. December 2007. https://datatracker.ietf.org/doc/html/rfc5070 (Accessed 10.2.2022)
[23] Danyliw, R. (2016). RFC7970 - The Incident Object Description Exchange Format Version 2. Internet Engineering Task Force (IETF). November 2016. https://datatracker.ietf.org/doc/html/rfc7970 (Accessed 10.2.2022)
[24] Luo, B., Lee, D., Lee, W. C., Liu, P. (2004). QFilter: fine-grained run-time XML access control via NFA-based query rewriting. In Proceedings of the thirteenth ACM international conference on Information and knowledge management (pp. 543-552). 10.1145/1031171.1031273.

AUTHORS

Jarno Salonen is working as a Senior Scientist in the applied cybersecurity team at VTT Technical Research Centre of Finland. He has a professional background of over 20 years in making the digital world a better place for ordinary users especially in the areas of cybersecurity, privacy, resilience and the development of electronic services.

Tatu Niskanen is a cybersecurity oriented graduate student from University of Jyväskylä, Finland. He is currently finishing up his master's studies from Hanyang University, South Korea, where he is staying as an exchange student in the school of engineering. He has worked for VTT Technical Research Centre of Finland in multiple research projects during 2021.

Pia Raitio is currently working as a Senior Officer, Cybersecurity Specialist at Fin- nish Transport Infrastructure Agency, where she recently started after a long career as a cybersecurity researcher and project manager at VTT. Her focus is on ensuring the cybersecurity of critical infrastructures and other ICS/OT-systems, covering both cybersecurity governance of the whole infrastructure as well as the very detailed technical aspects - and everything in between.