Anonymizing Cybersecurity Data in Critical Infrastructures: The CIPSEC Approach

Ana Rodríguez-Hoyos
Universitat Politècnica de Catalunya (UPC)
Escuela Politécnica Nacional (EPN)
ana.rodriguez@epn.edu.ec

José Estrada-Jiménez*
Universitat Politècnica de Catalunya (UPC)
Escuela Politécnica Nacional (EPN)
jose.estrada@epn.edu.ec

David Rebollo-Monedero
Universitat Politècnica de Catalunya (UPC)
david.rebollo@entel.upc.edu

Jordi Forné
Universitat Politècnica de Catalunya (UPC)
jforne@entel.upc.edu

Rubén Trapero Burgos
ATOS
ruben.trapero@atos.net

Antonio Álvarez Romero
ATOS
antonio.alvarez@atos.net

Rodrigo Diaz Rodríguez
ATOS
rodrigo.diaz@atos.net

v1.1.1
2019/03/25

ABSTRACT

Cybersecurity logs are permanently generated by network devices to describe security incidents. With modern computing technology, such logs can be exploited to counter threats in real time or before they gain a foothold. To improve these capabilities, logs are usually shared with external entities. However, since cybersecurity logs might contain sensitive data, serious privacy concerns arise, even more when critical infrastructures (CI), handling strategic data, are involved.

We propose a tool to protect privacy by anonymizing sensitive data included in cybersecurity logs. We implement anonymization mechanisms grouped through the definition of a privacy policy. We adapt said approach to the context of the EU project CIPSEC that builds a unified security framework to orchestrate security products, thus offering better protection to a group of CIs. Since this framework collects and processes security-related data from multiple devices of CIs, our work is devoted to protecting privacy by integrating our anonymization approach.

Keywords

privacy, critical infrastructures, data anonymization, CIPSEC, security logs

*corresponding author

INTRODUCTION

Critical infrastructures (CIs) are either physical or virtual systems whose operation directly supports the functioning of a society. In fact, given the wide reach of critical infrastructures, even small problems on their operation could have a massive impact on a vast population (House 2013). Besides their reach, CIs are tightly coupled with sensitive areas such as health, telecommunications or economy, which are strategic for a country, so their interruption might imply severe affectation for citizens (House 2013). We are talking about the infrastructure of hospitals, transportation systems, oil and energy distribution systems, banking, environment monitoring, etc. Since these services are essential to the security, prosperity, and social welfare of the population, their corresponding CIs must not stop working and are usually managed by governments.

Given the importance of CIs, their information systems are usually strongly protected against intrusions, mainly against those coming from the Internet. Currently, the resources available for such protection involve "intelligent" cybersecurity solutions that “learn” how attackers behave and ultimately detect and stop future incidents. To do so, these solutions are fueled with so called logs, i.e., detailed information about past events, which are stored as records describing every security incident. Furthermore, logs from multiple sources are commonly shared among several devices and then aggregated so that more input information can improve the efficiency of protection . Aiming to ensure the continuity of their services, CIs have widely adopted such protection mechanisms that generate very detailed and vast information about the entities and interactions involved in security incidents.

Although more granular logs provide more intelligent security protection in CIs, inappropriate sharing of sensitive data may rise serious privacy concerns. Cybersecurity logs could include identifying attributes (IP addresses, user names, fingerprints, etc.), strategic information of companies (e.g., about vulnerabilities, software versions), and several other indicators (path names, user data) that, when disclosed, could easily be used to violate the privacy of the individuals or companies involved. The risk for privacy in this context is not only exacerbated by the increasing need of security services to aggregate shared cybersecurity data (to get improved protection mechanisms), but also by the large number of data items enclosed in cybersecurity logs.

Beyond the security they require to protect their information systems, CIs are more exposed to external attacks than conventional infrastructures due to a number of factors. First, since CIs commonly serve a large population, they are desired targets of attackers who aim at magnifying the impact of their offensive (Edwards 2018; Moyer 2010). Also, dealing with strategic processes and information, CIs are usually the target of high-level adversaries supported by powerful organizations and even governments (Swinford 2018; Woollaston 2017). These factors aggravate even more the effects of information leakage to the point that, e.g., the mere revealing of internal IP addresses or user names might imply severe risks for the integrity of such infrastructures. Interestingly then, the privacy of companies and individuals whose information is revealed in logs may have a direct impact on the security of CIs.

Our work is aimed at preserving the privacy of individuals and organizations in the context of the CIPSEC framework, and particularly in what involves the sharing of cybersecurity information. The EU project CIPSEC proposes a unified security framework to orchestrate state-of-the-art heterogeneous, diverse, security products aiming to offer high levels of cybersecurity protection. To do so, this framework is able to collect and process security-related data (logs, reports, events) so as to generate security anomaly alerts that can affect a CI health and that can have cascading effects on other CI systems. Our proposal includes a methodology and a tool (data privacy tool, DPT) for obfuscating sensitive data from cybersecurity logs to protect the privacy of the involved entities and individuals.

Namely, our DTP will modify sensitive data with the aim of *sanitizing* or cleaning it from too distinctive attributes. This involves applying several anonymization mechanisms to cybersecurity logs (suppression, generalization, pseudonymization) whose implementation will depend on the specific anonymized attributes.

THE CIPSEC FRAMEWORK

CIPSEC objectives

The main objective of the EU project CIPSEC is to create a unified security framework that orchestrates state-of-the-art heterogeneous, diverse security tools and offers high levels of cybersecurity protection in IT & OT Critical infrastructure environments. The framework is currently built to collect and process security-related data (logs, reports, events) so as to generate alerts for security incidents that can affect the integrity of a CI together with the potential cascading effect affecting other parts of the CI or event other CIs. The framework aims to be very flexible, adaptable and causing minimum interference to the normal operations of the CI, allowing for its easy updating when needed in a secure and easy manner.

The CIPSEC framework is capable of collecting events supported by different tools that monitor different aspects of the CI, such as network traffic, malware threats or wireless spectrum among others. Along with the operations for

collecting events there is also a reasoning capability based on correlation algorithms that generate alerts for the anomalies detected in the events collected. Additionally, the CIPSEC framework provides with additional services, transverse to the CI monitoring activity, which complements the activities carried out:

- vulnerability tests and recommendations, including cascading effect attacks; which allows to have a snapshot of the level of protection against cyber threats exploiting current vulnerabilities of the assets within a CI ;
- security information sharing, leveraging the report of security incidents either across the infrastructure or to the rest of the world, in order to, for instance, prevent incidents propagation;
- training services, assisting on the usage of the framework and on different characteristics of security management aspects, allowing for an easy training of security staff in the context of the CIPSEC framework;
- updating and patching mechanisms, with the purpose of having a unified view of the status of all the monitoring tools deployed in the infrastructure and giving the possibility to automatically update them, guaranteeing the timely protection against the latest security threats.

The CIPSEC framework is being validated in real environments using the infrastructure of three pilots that covers different domains: rail transportation, environmental monitoring and health sector.

CIPSEC architecture

For the sake of flexibility, the CIPSEC framework was designed to be independent from the underlying critical infrastructure (i.e., independent from the resources managed or the security requirements). The reference architecture of CIPSEC was conceived based on the flow of the data managed within a CI, or, said otherwise, was design to be infrastructure-agnostic by design. With this aim, the architecture is defined according to the life cycle of the security data (logs, events, reports) acquired, disseminated and consumed in CIs.

Data Acquisition refers to the process of collecting or storing the information (logs, events) generated by end devices devoted to secure the integrity of CIs. Thus, there are multiple sources of this data, e.g., intrusion detection systems.

Data Dissemination covers the transmission of the acquired security information to the components that will further process it. The dissemination of this data is usually performed in real-time describing the multiple processes carrying out in a CI, so that they can be monitored and controlled. In the context of CIPSEC, the information disseminated encompasses security data related to events, alarms, updates, etc.

Data Consumption concerns the processing of the acquired security information after being disseminated to the relevant consumers (e.g., incident correlators). Such information is processed and interpreted to fuel several assessment tools that enable users to make informed decisions.

Figure 1 depicts the architecture of the CIPSEC framework based on a group of layers that follow the flow of security data described above. This illustration also shows how the security data travels from the CI to a user interface so that the system admin can take appropriate decisions based in the processing activities carried out by the framework, such as enforcing mitigations or applying contingency plans.

The acquisition layer obtains a lot of information directly from the CI components dedicated such as vulnerability assessment, identity access management, integrity management, endpoint detection and response, and cryptography. The information collected is aggregated and processed by a component called anomaly detection reasoner that triggers security alerts depending on the patterns devised in security data.

The *data processing* layer is on top of the acquisition layer and involves two main components: the DPT and the forensics service. While the forensics filters and analyzes indicators potentially useful for forensic analysis, the DPT aims at preserving privacy in the security data coming from the CI and at storing such sanitized data in a different database for sharing purposes. This component is the one whose implementation we present in this paper.

The *presentation layer* aggregates the information produced by the underlying layers through a dashboard that offers a user interface where statistics and evolution indicators are presented to illustrate the security status of the whole CI. Such interface provides with an aggregated and uniform view of this status to the user in order to facilitate decision-making processes.

Finally, other complementary services are also provided by the architecture in order to guarantee the support to end users, the compliance with the CIPSEC framework, and the continuity of the services.

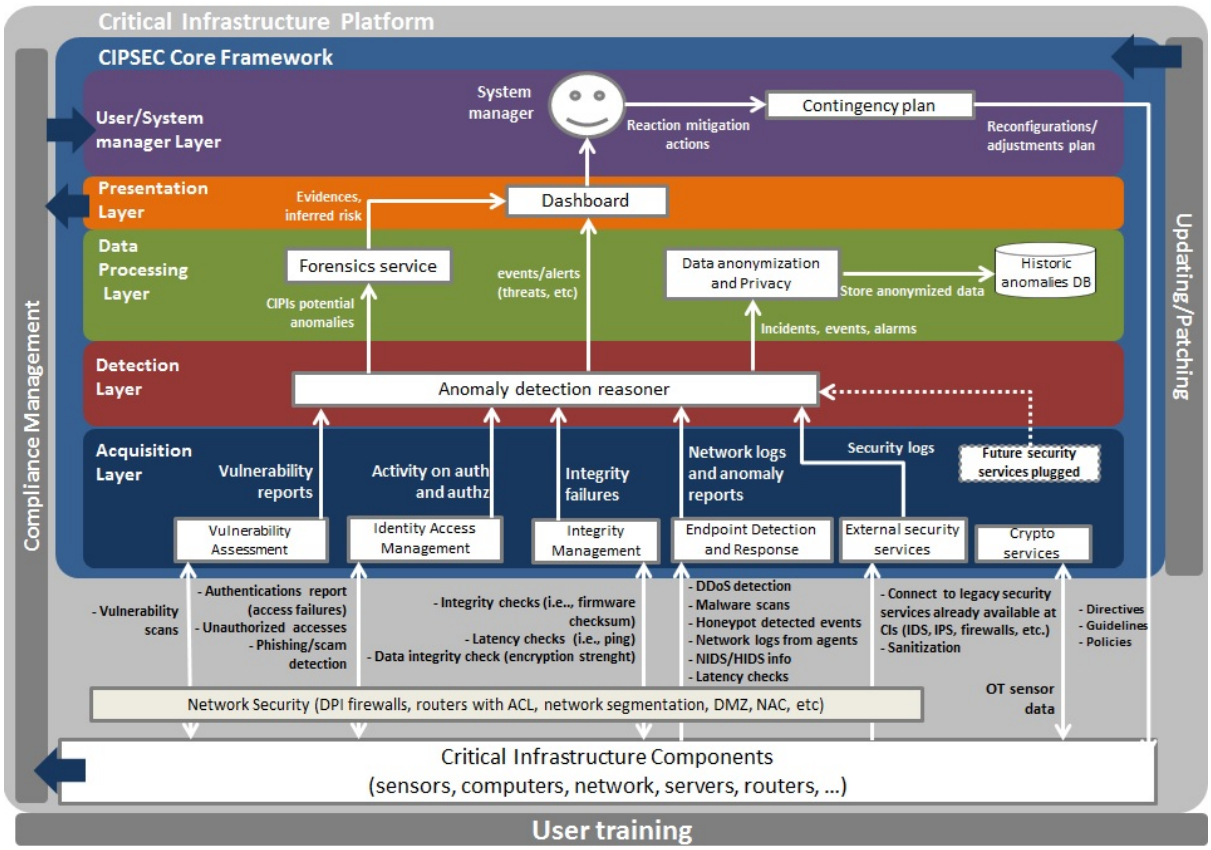

Figure 1. CIPSEC Reference Architecture for protecting of critical infrastructures.

DATA PRIVACY TOOL

Background on cybersecurity logs and privacy protection mechanisms

Logs are pieces of information that sequentially register the events affecting a system; therefore, when seen aggregated, they constitute evidence of the system behavior. Said diagnosis is fundamental to scrutinize and then fix a given issue, even more in the cybersecurity realm where thousands of attackers are permanently generating incidents that threaten the integrity of critical systems connected to the Internet.

Usually, logs contain a lot of granular information on the related event, starting with a time stamp. Cybersecurity logs may include, e.g., IP addresses, process IDs, hardware information and event descriptions.This information is stored in text files formatted to guarantee its agile reading and processing. For instance, two formats extensively used to store logs are XML and JSON. Both have interesting features based on labels to present information as name-value pairs, e.g., "ID: 123456" or "Alarm type: critical". Namely, the attributes or information elements of a log are organized using a name (or label) of the attribute and its corresponding value (the raw data). This way of representing information in logs significantly facilitates further selection and replacement (transform) of sensitive attributes.

Roughly speaking, protecting said information against privacy threats builds on these two operations: *selection* of sensitive attributes in the logs and *transformation* of corresponding values to a more private version. This is more deeply described in this document, where our proposal is presented. Although the definition of said operations depend on the context (sharing policies, organization concerns, etc.), the modern ways to structure logs are decreasing the complexity of performing these operations of selection (search) and transform (replace).

First, to protect privacy, sensitive attributes (the target) must be defined and then detected in logs. In practice, this task consists in searching for specific information in plain text. Given the vast log data that cybersecurity systems could generate, such searching for specific items might be daunting if it is expected to be done manually by a human operator. Fortunately, technology can now be used to automatize the detection of this type of attributes. Moreover, the most common logging formats are based on labeling every single piece of information contained in the log. Thus, once the sensitive attribute (or its label) is defined, it is not difficult to retrieve it from the logs along with its value. If the data within logs were not appropriately formatted, sensitive information should be located by looking

for specific syntax patterns that such information present in logs. For instance, if IP addresses were considered as sensitive information, the privacy protecting approach could start detecting IP addresses in logs by resorting to its unambiguous syntax. Then, searching for a pattern of four numbers separated by dots would eventually lead the system to find said IP addresses. Regular expressions are powerful constructions that can be used to represent and search such patterns.

After finding the attribute in cybersecurity logs, it has to be protected to preserve the privacy of involved companies or individuals. This implies modifying or transforming the value of the attribute to obfuscate any sensitive information there contained. This task is also referred to as *sanitization* in the sense that it "cleans" data from too distinctive attributes. To do so, some anonymization or sanitization mechanisms are commonly implemented. These mechanisms are described in the following lines.

Suppression is the simplest strategy to protect privacy in this context. It consists in completely eliminating sensitive information, which can be interpreted as replacing it for a blank or any meaningless string. This implies that no trace of said sensitive data is left which may directly affect the utility of the logs.

Generalization is rather a less destructive anonymization approach. It builds on replacing sensitive information with more general but still meaningful data. For instance, if the sensitive piece of data is the IP address 192.168.1.1, a generalized version would be 192.168.0.0. In contrast with suppression, generalization could keep some utility from the data in log records, depending on the deep of generalization attained.

Pseudonymization is a mechanism that consists in replacing identifying information by artificial identifiers, also called pseudonymous. Since said pseudonymous would be used instead of the original identifier, each time the latter appears, it is possible in practice to recover the original information from its pseudonymized version. Also, if such identifiers are only used for identifying purposes, pseudonymizing them would not affect the utility of information.

As briefly described, the resulting utility of cybersecurity logs may be more or less affected depending on the anonymization mechanism used to protect privacy.

Privacy risks from disclosing cybersecurity logs

In general, logs contain a lot of information since they are aimed at describing the state of a system at a given point in time. Further, an aggregated set of logs should enable an administrator to have a general view of the performance of said system. In particular, the specific amount of data items (we will call them attributes) present in a log record will depend on the level of granularity set in the logging service. Interestingly, some equipment, e.g., networking devices, allow to be configured with such high levels of granularity that manufacturers explicitly warn about the risk of saturating storage or processing resources. Thus, logs could become extremely detailed pieces of data describing a system where companies and individuals are involved.

Cybersecurity logs might include very sensitive data since they are commonly associated with vulnerabilities and security threats. If that information fell into the wrong hands, it could cause severe damage to the data owners. Besides, the level of granularity of security logs is usually higher to afterwards enable the detection of security breaches (which use to be provoked by undercover interactions), so more and more attributes are included in logs to improve protection to the same extent. As a consequence, the potential leakage of this information implies serious privacy risks for the entities involved, not only due to the weaknesses that such logs could reveal to attackers, but also due to the increased detail of the information.

Ironically, the risk of leaking this information does not necessarily come from deliberate attacker intrusions to steal it, but from the voluntary release of such logs when sharing them to other partners. In fact, sharing cybersecurity logs has become a common practice among organizations as a collaboration mechanism to enhance the effectiveness in detecting and preventing security threats. The attributes characterizing a security incident in a system, e.g., IP addresses, file names, sizes, can be shared with system administrators with the aim to help other systems detect or prevent related threats. More specifically, information sharing enables sharing partners to enhance their defensive capabilities, i.e., detecting, responding, and recovering from cybersecurity incidents. As a matter of fact, the collective aggregation of shared security logs is currently the main input fueling powerful antivirus and network security devices.

Despite the great benefits that sharing cybersecurity logs may bring, some challenges still remain. One of said challenges is safeguarding sensitive information that might be included in these logs, i.e., protecting the privacy of the entities whose information is shared. The violation of privacy in this context (e.g., due to the disclosure of personally identifiable information) may have serious consequences, particularly for companies, such as the ones listed below:

Table 1. Some attributes whose disclosure in cybersecurity logs might jeopardize privacy.

Attribute	Privacy risk
IP address	May enable identification of users and organizations.
e-mail address	May enable identification of users and organizations.
path names	Could disclose user names, directory hierarchies.
patching information	Could reveal software updating calendars, thus when
software versions	Along with other attributes, could enable fingerprinting and identification of users.
incident description	When associated with an origanization, could unveil its vulnerabilities.
organization name	May allow attackers to identify an organization.

- financial loss,
- legal action,
- loss of reputation,
- exposure to protection capabilities.

As explained above, the nature of cybersecurity information contained in logs is inherently sensitive since it includes several attributes and also some very punctual data items that may reveal strategic operations of systems regarding their security. Virtually every computing device and application are enabled to generate this type information, especially if they engage networking or Web interactions. Some examples of sensitive information that could be included in cybersecurity logs are described next.

Timestamp. A time stamp is fundamental to determine the moment when an security incident occurred. The exact date and time of the incident allow to correlate other events that could contribute on the investigation of the threat. However, if coupled, e.g., with individuals, temporal data could also help attackers perform the same correlation to unveil patterns (a person's sleep time, a company's patching calendar) to violate privacy.

IP address. IP addresses individuate devices so that security issues can be associated with the entity where the incident has been generated. Nevertheless, in the same line, IP addresses are key information for privacy attackers to identify the individuals and companies involved. In fact, an IP address could unequivocally represent an individual or a family, so the security logs related to their interactions would reveal such tight association. The mere availability of this information enables further security attacks (denial of service, fingerprinting) to companies, which could reveal even more indicators about potential victims (privacy violations).

IP addresses are not the only data items with this individuating capability. Other attributes that may appear in security logs such as user names, host names and MAC addresses have similar identification capabilities, although their presence is not as common as IP addresses. There are also apparently innocuous indicators that are contained in cybersecurity logs that can serve as identifying parameters when combined, e.g., software version and patch level information, hardware information, system event, file access, etc. Interestingly, the resulting combination of said attributes can be seen as a fingerprint of the associated entity and could be used as an identifier by itself.

Any indicator or attribute included in logs could reveal further sensitive information. The specific privacy risk, however, depends on the context, i.e., on the background information available for the attacker, and his objective, but also on the particular status of the potential victim. For example, path names could disclose information about the work a user might be performing, or operating system and patches names may reveal the preferences of a company regarding their network or software implementation (which it had been keeping secret). Disclosing such information in logs that will be shared may represent a privacy violation for users or the company whether or not the parameters included are critical for each entity.

Besides identifying attributes or other complementary indicators, the information included in cybersecurity logs may be very specific when generated by specialized devices such as routers, antivirus servers, intrusion protection systems, forensic toolkits, SIEMs (security information and event management systems), etc. Moreover, these logs contain very critical information since it is commonly derived from assessment routines, i.e., contemplates "refined data" (which in practical terms implies more and more valuable data). This information might span vulnerability alerts, system artifacts, attack alerts, or summary reports, whose disclosure is a direct threat for the privacy of the entities involved.

The risk to privacy when sharing cybersecurity logs is seriously exacerbated when CIs are involved since the corresponding entities and their workers are more exposed given the strategic role they are playing. In Table 1, we describe some attributes whose disclosure in cybersecurity logs may imply serious privacy risks.

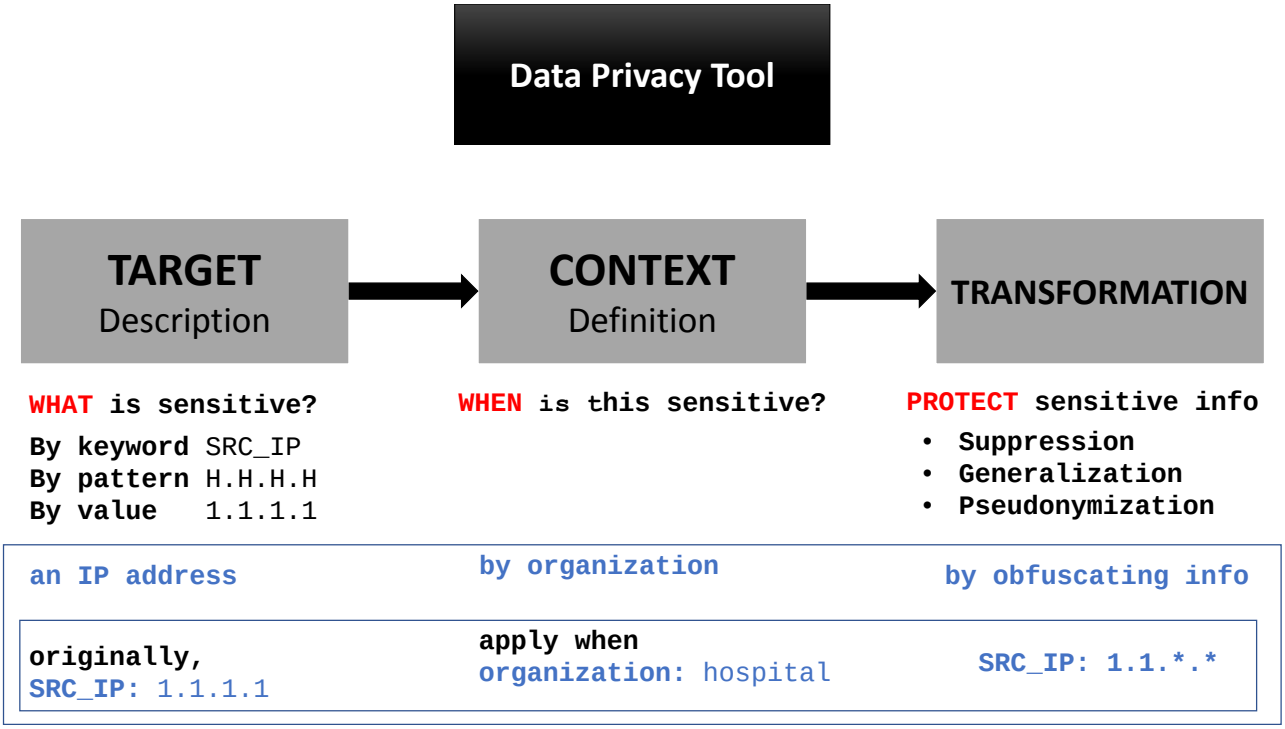

Figure 2. Architecture of the data privacy tool.

Architecture of the data privacy tool

The objective of our DPT is offering privacy for individuals and institutions in a context where cybersecurity logs have to be shared among different partners. While disclosing and aggregating such data may improve the capabilities of security solutions in CIs, the high granularity of logs and the sensitive attributes there contained may jeopardize privacy. Thus, we devise a tool to protect this sensitive data by anonymizing it. This tool encompasses the components described below.

Target description

The first step in protecting privacy in cybersecurity logs is determining the set of sensitive attributes that will have to be sanitized. Said otherwise, the specific target of the anonymization mechanisms has to be defined since logs use to hold a lot of information.

The level of sensitivity, however, depends on the specific context in which users and companies perform (their interests, needs, worries, adversaries, etc.). Moreover, although some attributes might be defined as sensitive by default (e.g., identity numbers), or automatic mechanisms could be created to "recognize" them, the operators of the DPT should always have the last word when deciding what attributes to protect by defining a privacy policy.

Evidently then, to locate sensitive attributes and their values within the data provided by logs, some language might be necessary for the user to describe the corresponding targets. If logs were generated by CIs without any visible structure, patterns should be found to detect the sensitive attribute, e.g., looking for quartets of decimal numbers separated by commas to find IP addresses (which the operator would have defined as sensitive). Fortunately, to facilitate its exploitation and analysis, logs are commonly generated in structured formats, sometimes even in hierarchical trees, such that the information be organized according to certain logic and that every attribute value is labeled.

As logs are presented through standard approaches and attribute values are indexed through labels, it is straightforward to refer to such attributes to then retrieve their values. For instance, let us suppose that the operator is interested in preventing individuation of his company in the logs generated by their devices. Thus, he might have to detect identifying data in logs, such as IP addresses, to anonymize them and protect privacy. There may be different approaches to search for IP addresses in a log, as described below.

- **By keyword.** Within cybersecurity logs, IP addresses are usually labeled with a keyword such as SRC_IP (source IP) or DST_IP (destination IP) or any other. Knowing such keyword, it is pretty easy to obtain the sensitive value associated in the corresponding log.

```
{'AlarmEvent': {
'USERNAME': '', 'SRC_IP': '188.112.63.117', 'BACKLOG_ID':
'839301cfd5b54179847535ffa3e29adc', 'DATE': '2018-07-17
09:00:16',
'DST_IP': '84.88.67.117', 'USERDATA7': '', 'USERDATA6': '',
'FILENAME': '', 'PRIORITY': 4, 'RELIABILITY': 10,
'ORGANIZATION': 'hospital', 'SENSOR':
'AD14C6F3975ED9860E32190EA3DF2535', 'SID_NAME':
'directive_event: Detected access to SAMBA in Honeypot',
'USERDATA2': '', 'USERDATA3': '', 'USERDATA1': 'tcp',
'PROTOCOL': 6, 'RISK': 4, 'USERDATA4': '', 'USERDATA5': '',
'EVENT_ID': '04447d36c0614e3fbe70b5b4612adf2e', 'USERDATA8':
'', 'USERDATA9': '', 'PLUGIN_NAME': 'cyber-monitor',
'DST_IP_HOSTNAME': '00000000', 'RELATED_EVENTS':
'[899f11e885a4080027ea052cd289c2dc,899f11e885a4080027ea052cd2
b27c90]', 'PASSWORD': '', 'PLUGIN_SID': '2', 'CATEGORY':
'Recon', 'SRC_IP_HOSTNAME': '00000000', 'SUBCATEGORY':
'Scanner'}
```


Figure 3. Sample of logs generated by the CIPSEC framework.

- **By pattern.** If the sensitive data to be anonymized is not systematically associated with an index or label, a pattern could be used to look for such data. In the IP address example, e.g., we could look for any group of four numbers from 0 to 255 separated by dots, which could be symbolically represented as X.X.X.X.
- **By value.** Still in the case when no specific keyword is available, the value of the sensitive attribute could be directly searched in the logs. The drawback of this approach is evidently that this search spans a single value while the firs two may encompass a wider spectrum of values.

Since the first step to protect privacy in cybersecurity logs involves searching for a string (keyword, pattern or value) in a piece of text, it is worth noting that, at an implementation level, the use of regular expressions is highly recommended for such tasks. See Figure 2 where this component of target description of our DPT is depicted as it would work with the other two components described in the next subsections.

Context definition

As stated in the previous section, the sensitivity of some data item is subject to the context where its owner performs. In the same line, the privacy protection mechanism required will vary according to the specific needs and characteristics of the subjects involved. The context-definition component then enables the user of our DPT to set any restriction or condition on the application of the privacy protection strategy.

While a lot of restrictions could be integrated, there is one in which we are interested for the CIPSEC framework. Since three different pilots or organizations are sharing their cybersecurity logs, the user of the DPT could opt for anonymization or not depending on the organization he belongs to. For instance, air quality monitoring might not involve sensitive attributes for the organization generating such data so could decide not anonymizing their data. Other more complex scenarios may be characterized, e.g., by a company having very specific needs on anonymizing attributes that in other contexts might not be critical to protect. In brief, the scope in which our DTP is used may also define the operation of the DPT.

In Figure 2, we illustrate this component within the whole architecture of this tool.

Transformation

Once sensitive information and context are defined, sensitive data has to be transformed in order to protect privacy. Said transformation implies perturbing attribute values so that, e.g., identifiers no longer serve to identify individuals, or that sensitive values provide less specific information regarding individuals or companies.

The transformation component in the architecture of our DPT is implemented through the anonymization mechanisms described in Section 3.1. As explained above, such mechanisms will replace the original sensitive value with another (at least less specific) string. Figure 2 shows how this component is integrated in the architecture of our DPT.

It is worth noting that when transformation has to be done dynamically (i.e., when replacing according to a a predefined pattern), regular expressions are also very useful as with target description.

```
"SRCIP":{
      "ORGANIZATION":"all",
      "ACTION":"generalization",
      "TYPE":"ip_address",
      "KRE":"^SRC_IP$",
      "VRE":"",
      "SRE":""
},
"USERDATA":{
         "ORGANIZATION":"all",
         "ACTION":"suppression",
         "KRE":"^USERDATA*",
          "VRE":"",
         "SRE":""
},
```

```
"ORG":{

      "ORGANIZATION":"hospital",
      "ACTION":"pseudonymization",
      "TYPE":"organization",
       "KRE":"^ORGANIZATION$",
      "VRE":"",
      "SRE":""
 }
```

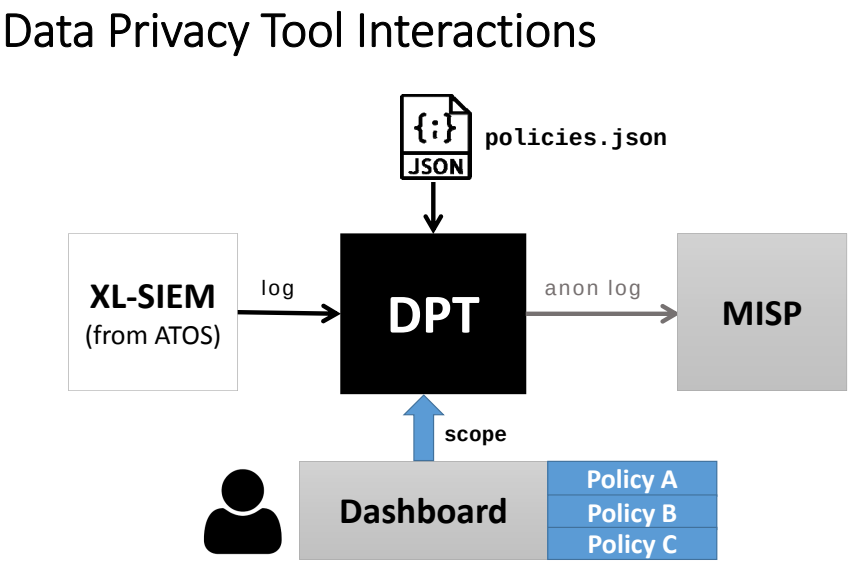

Figure 5. Interactions of the DPT with different components of the CIPSEC framework.

Privacy policies

In order to enable users to set the context of their privacy protection, a privacy policy has to be defined. A privacy policy is essentially a list of named rules that include the parameters that characterize the anonymization of sensitive information, i.e., the description of the specific attribute to be anonymized, the transformation mechanism to use, and any other criterion (e.g., the organization whose logs will be anonymized).

IMPLEMENTATION AND INTEGRATION IN THE CIPSEC FRAMEWORK

As explained throughout this article, cybersecurity logs enable the intelligent protection provided by the CIPSEC framework. Meanwhile, our DPT aims at preserving the privacy of individuals and organizations involved in such logs when shared among different partners. All the logs generated by several security devices in the CIPSEC infrastructure are aggregated and formatted in standard JSON format in real time to then be stored in a security information and event management server (XL-SIEM). Figure 3 depicts a sample of these logs that are further available for sharing in a Malware Information Sharing Platform (MISP).

As mentioned in Section 3, our DPT has three main inputs that guide the anonymization process: the cybersecurity logs that are fueled by the XL-SIEM; a privacy policy, also as a file formatted in JSON (an example is depicted in Figure 4); and a scope that indicates the organization that is executing the anonymization process. The latter

argument enables the user to anonymize only the logs that belong to his organization. After logs are anonymized, they are sent to the MISP for sharing purposes.

Finally, for the sake of usability, the control of the execution of the DPT and the selection of the privacy policy is delegated to a graphical user interface integrated in the dashboard of the CIPSEC framework. Figure 5 illustrates the components mentioned in this section and their corresponding interactions, while Figure 6 shows how a single anonymized log record would look. As a side note, our DPT is implemented using Python.

Related work

The concerns on the privacy risks from cybersecurity data are not new. The Government Accountability Office (GAO) of the USA already reports in (*High risk series: An update. Ensuring the security of federal information systems and cyber critical infrastructure and protecting the privacy of personally identifiable information* 2015) how the advances in technology have given rise to important challenges to ensure the privacy of personally identifiable information. The GAO recommends implementing privacy practices to protect personal identifying information, especially when managed in critical infrastructures. But in a wider scope, severe regulation is currently been applied in the USA and Europe (*General Data Protection Regulation (GDPR)* 2016) to protect privacy at every context, essentially by given users great control over their data. Though these documents acknowledge the increasing need to protect privacy, they are regulatory approaches that require implementation according to the specific domain.

Several approaches can be found in the literature that describe privacy preserving mechanisms on unstructured data (e.g., any type of log data). Those mechanisms are based on sanitization (through suppression, generalization, or any kind of perturbation) of such data. Some works address related mechanisms (Sánchez and Batet 2015), not only focused on protecting privacy but also on preserving the utility of sanitized data (Sánchez, Batet, and Viejo 2014). Interestingly, some of such approaches even consider the semantics of the text to be sanitized to get more efficient mechanisms (Sánchez, Batet, and Viejo 2013; Chakaravarthy et al. 2008). Unlike those works, our approach focuses on privacy preserving within cybersecurity data in the particular context of the CIPSEC framework.

With regards to the exchange of threat information several initiatives are exploiting their possibilities. For example, the DiSIEM project [1] uses it to empower Security Information and Event Management systems by exporting and importing data about incidents detected, allowing for the update of detection rules according to the information imported. DiSIEM also uses MISP as platform for the exchange of information although the privacy considerations are something not considered so far. Also, in 5G networks it is considered the usage of Threat Intelligence Exchange capabilities to import and export incident information across the network slices considered in 5G infrastructures [2].

CONCLUSIONS

Cybersecurity data generated in the form of logs is very prone to including sensitive information about individuals and organizations, even more so when such logs belong to CIs. The strategic importance of such data, then, makes those individuals and organizations common targets of privacy adversaries. The EU project CIPSEC integrates the cybersecurity information systems of three CIs to improve their threat detection and reaction capabilities. However, since this integration involves sharing such cybersecurity data, there are privacy risks that must be tackled.

The solution we propose addresses this issue by pre-processing logs to anonymize sensitive attributes according to a privacy policy that defines a particular context. Enabling users to set privacy policies is definitely the most important and complicated task since many factors have to be considered to define not only what data to anonymize, but also when and how. Fortunately, the logs generated by information systems are currently represented using more structured and flexible formats (e.g., JSON), which, along with the power of regular expressions to define context, significantly facilitate matching and dynamically perturbing string-based attributes.

As a work in progress, there are several avenues to enhance our privacy tool. Perhaps the most important pending work has to do with assessing the impact of the anonymization mechanisms on the practical utility of cybersecurity logs. Undoubtedly, data perturbing strategies reduce the quality of of the information involved so a balance must be reached to protect privacy while minimizing utility loss. Moreover, standardization of the definition of privacy policies is necessary to simplify the configuration of the anonymization mechanisms. This could be a daunting task so automating it according to the requirements of users and organizations might certainly help. Furthermore, a challenge in data sanitization is the reidentification risk posed by inferences based on several attributes exploited simultaneously. Finally, in the same line, more usable (probably graphical) interfaces could be developed to enable end users to provide the parameters of a personalized context in order to better guide the anonymization process of cybersecurity logs.

[1] DiSIEM project web page: http://disiem-project.eu/

[2] D3.1. Initial resilience and security analysis: http://5g-monarch.eu/wp-content/uploads/2018/06/5G-MoNArch_761445_D3.1_Initial_resilience_and_security_analysis_v1.0.pdf

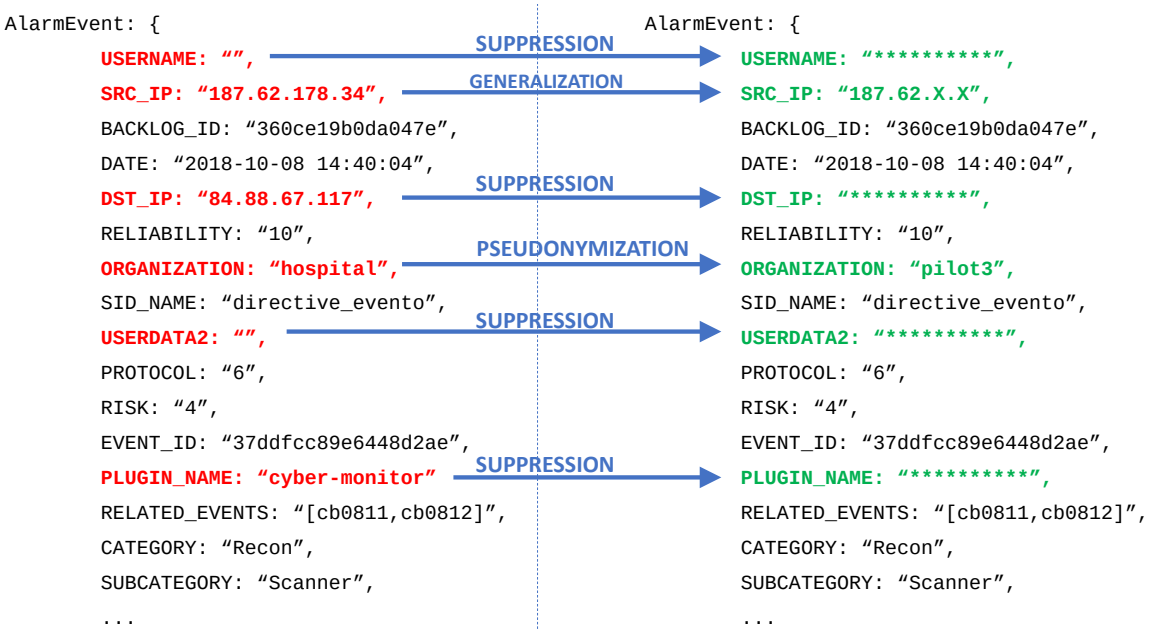

Figure 6. A view on how the privacy in cybersecurity logs could be protected through different anonymization mechanisms.

ACKNOWLEDGMENT

The authors gratefully ackowledge the support of Ahmad Mohamad Mezher for this contribution. This work has been funded by the European Commission through the H2020 project "CIPSEC", grant agreement 700378. Aditional support has been obtained from the Spanish Ministry of Economy and Competitiveness (MINECO) through the projects "INRISCO", ref. TEC2014-54335-C4-1-R, and "MAGOS", ref. TEC2017-84197-C4-3-R.

REFERENCES

Chakaravarthy, V. T., Gupta, H., Roy, P., and Mohania, M. K. (Oct. 2008). "Efficient techniques for document sanitization". In: *Proc. ACM Int. Conf. Inform., Knowl. Mgmt. (CIKM)*. Napa Valley, CA, pp. 843–852.

Edwards, J. (2018). "Someone is trying to take entire countries offline and cybersecurity experts say ítś a matter of time because 'it's really easy'". In:

High risk series: An update. Ensuring the security of federal information systems and cyber critical infrastructure and protecting the privacy of personally identifiable information (Feb. 2015). Rep. Congr. Cmte. GAO-15-290. U.S. Gov. Account. Office (GAO), pp. 235–254.

General Data Protection Regulation (GDPR) (Apr. 2016). Regul. (EU) 2016/679, Eur. Parliam.

House, T. W. (Feb. 2013). "Presidential Policy Directive – Critical Infrastructure Security and Resilience". In:

Moyer, E. (Sept. 2010). "Stuxnet worm hits Iranian nuclear plant". In: *https://www.cnet.com/news/stuxnet-worm-hits-iranian-nuclear-plant/*.

Sánchez, D. and Batet, M. (Apr. 2015). "C-Sanitized: A privacy model for document redaction and sanitization". In: *J. Assoc. Inform. Sci., Technol.* 67.1, pp. 148–163.

Sánchez, D., Batet, M., and Viejo, A. (Nov. 2013). "Minimizing the disclosure risk of semantic correlations in document sanitization". In: *Inform. Sci.* 249, pp. 110–123.

Sánchez, D., Batet, M., and Viejo, A. (Sept. 2014). "Utility-preserving sanitization of semantically correlated terms in textual documents". In: *Inform. Sci.* 279, pp. 77–93.

Swinford, S. (Apr. 2018). "Russia preparing to mount cyber-attack on Britain's 'critical infrastructure', GCHQ and FBI warn". In: *https://www.telegraph.co.uk/politics/2018/04/16/russia-preparing-mount-cyber-attack-britains-critical-infrastructure/*.

Woollaston, V. (May 2017). "Wanna Decryptor ransomware appears to be spawning and this time it may not have a kill switch". In: *https://www.wired.co.uk/article/wanna-decryptor-ransomware*.