Privacy Handling for Critical Information Infrastructures

Nils Ulltveit-Moe, Terje Gjøsæter, Sigurd M. Assev, Geir M. Køien and Vladimir Oleshchuk
Faculty of Science and Engineering
University of Agder
Jon Lilletuns vei 9, 4879 Grimstad, Norway

Abstract—This paper proposes an architecture and a methodology for privacy handling in Critical Information Infrastructures. Privacy is in this respect considered as both the risk of revealing person-sensitive information, for example from critical infrastructures in health institutions, but also to identify and avoid leakage of confidential information from the critical information infrastructures themselves. The architecture integrates privacy enhancing technologies into an enterprise service bus, which allows for policy-controlled authorisation, anonymisation and encryption of information in XML elements or attributes in messages on the service bus. The proposed methodology can be used to identify, quantify and reduce leakages of private or confidential information. It also suggests privacy enforcement mechanisms to increase the resilience against sensitive information leakages caused by cyber attacks.

I. INTRODUCTION

Critical infrastructures are commonly defined as assets that are essential to the operation of a society and its economy. Examples include facilities and infrastructure for production, transport and distribution of electricity, water, food; as well as transportation infrastructures. Other examples are Internet, telecommunication networks and banking systems. This paper considers critical information infrastructures (CIIs) that support or control such systems.

The essential questions covered in this paper is: How can we protect private or confidential information in a CII without compromising security or in other ways hindering the functionality of the system?

Recent Advanced Persistent Threats (APTs) like the Duku worm and Flame are government-backed cyber-attack tools that are designed to perform cyber-espionage on CII. This malware can perform functions like recording audio, take screenshots, log keyboard activity and network traffic, as well as try to interrogate information from nearby Bluetooth devices etc. [1], [2]. In addition to APTs, traditional cyber-crime is also proliferating with an ever increasing capability to also target CII. Traditional security protection measures have largely failed to detect these threats, which means that computer networks (including CII) must be handled as if they were fundamentally insecure.

EU is working towards implementing a European Information Sharing and Alert System (EISAS) that allows sharing of information and best practices between European Computer Emergency Response Teams, in order to mitigate and reduce the effect of transnational cyber-crime [3]. Proper handling of private or confidential information will be required for such an information sharing and alerting system. This paper outlines how our methodology, which will be demonstrated in EU-project PRECYSE, can be used to identify and mitigate privacy and confidentiality risks in CII.

The rest of the article is organised as follows: The next section gives motivation and use cases that demonstrate how privacy has become more important for Critical Information Infrastructures, and discusses why a methodology for privacy protection in CII is needed. Section III proposes an approach for privacy handling in CII based on the privacy by design criteria, it discusses how information leakage control can be implemented and how Shannon entropy can be used as a privacy leakage metric. Section IV describes the privacy and security architecture which is based on an Enterprise Service Bus (ESB), and section V describes the privacy policy management methodology. Section VI discusses related work, and section VII concludes the paper and indicates directions for future work.

II. MOTIVATION AND USE CASES

Information sharing, as mentioned in the introduction (e.g. EISAS), will necessitate identification and protection measures against leakage of private or confidential information, to collaboratively improve the attack detection and mitigation capabilities. A challenge with such information sharing is the sensitive nature of CII, which means that information about the topology, processes, configurations or services running on the critical infrastructure often is considered confidential information. In some cases (e.g. health institutions), the information may also contain person sensitive information. This means that such information must be adequately protected or anonymised, if attack related information is to be shared with outsourced MSS providers or other semi-trusted parties. Semi-trusted here means that a service provider is only trusted see the amount of private or confidential information that from a strict interpretation of need is required to do the security operations. The service provider is not trusted to see private or confidential information in general. This is different from current IDS practices, where all information is assumed at the same security level and there typically is not any transparency.
with regards to what is being monitored, who has seen what nor any possibilities to distinguish between information of different security levels.

Examples of services that may benefit from such information sharing are security services like intrusion detection systems (IDS), anti-spam, anti-virus, patch handling etc. It is also useful for peer-to-peer collaboration between CERTs or other organisations.

It is in general beneficial to share attack and vulnerability information between organisations, since this increases security, and outsourcing or collaborating on detecting and managing cyber-attacks gives a networking effect [4], [5]. This means that cyber-attacks can be detected and mitigated at a lower cost, since the collaborating organisations can share both the initial cost of attack analysis and the work needed to develop suitable mitigation strategies. Furthermore, increasing security lowers the risk of being attacked [5]. The main challenge is how much information you are willing to share with these semi-trusted parties, given that information from the CII may be private or confidential by nature.

This means that there are some inhibitors against information sharing [6]:

1) Often a culture against sharing (suspiciousness);
2) Lack of awareness on how to protect information;
3) Lack of technical solutions and standards to enforce protection of sensitive information.

In the following section, we describe how the PRECYSE project aims at mitigating these inhibitors, as well as handling other challenges related to privacy in CII.

III. PRIVACY HANDLING FOR CII WITH PRECYSE

A. Privacy by Design

Privacy by Design (PbD) is an initiative centered around 7 Foundational Principles [7]:

1) Proactive not Reactive; Preventative not Remedial
2) Privacy as the Default Setting
3) Privacy Embedded into Design
4) Full Functionality Positive-Sum, not Zero-Sum
5) End-to-End Security Full Life Cycle Protection
6) Visibility and Transparency
7) Respect for User Privacy, Keep it User-Centric

The PRECYSE methodology aims at supporting the PbD principles by using an approach that embeds privacy into the design. A proactive approach for CII privacy protection, where privacy is embedded into the design, is clearly desirable yet not always attainable. It is therefore important to also implement and deploy effective reactive protection of existing critical infrastructures, for example by implementing privacy-enhancing proxies which support anonymisation, pseudonymisation or encryption of data. These should be placed as close as possible to the data source and should have privacy as the default setting, so that a deliberate decision is required to reduce the privacy protection of the system. An example of this, is to implement firewall settings or anonymisation policies using a default DENY policy, where only information that is known to not violate privacy or confidentiality is revealed to semi-trusted third parties. An important and necessary element to implement reactive privacy is to identify the privacy and confidentiality requirements, which for example can be defined based on privacy and security impact assessments.

Strong security is a prerequisite for privacy. The security schemes must furthermore be selected and applied with privacy in mind to achieve the desired goals. If done right there may also be security benefits from privacy enhancements. For intrusion detection systems and similar technologies, privacy metrics can be used to reduce the amount of false alarms, which reduces the costs of such operations [8]. Another possible synergy is that authorisation mechanisms aimed at providing privacy-enhanced operation also may be used for security purposes. Similar cryptographic techniques can be used to protect private and confidential information. Entropy-based privacy metrics are also useful from a security perspective to detect certain attack variants, like Denial of Service attacks or attacks on encrypted protocols [9]. Privacy-enhanced database techniques can for example be used to limit data loss from databases due to system integrity attacks like SQL injection or buffer overflow exploits [10]. Anonymisation policies for individual elements or attributes in XML messages can be used to implement range checks to reject data outside sensible operating ranges, for example to reduce the risk of buffer over-flow attacks on web services [11] etc. These examples show that there are significant security benefits from implementing privacy enhancing technologies.

Full lifecycle protection is necessary for private or confidential information. This means that such information as far as practically possible should be protected using cryptographic means, from the moment information is generated and until the information is no longer needed. After that, it should be safely destructed, for example by invalidating relevant encryption keys as proposed in [12].

Visibility and transparency will be needed in the form of logging and auditing procedures, to ensure that access to sensitive information is warranted and does not get abused while non-repudiation is maintained. Last, but not least, respect for user privacy implies that critical infrastructures storing private user data should have procedures for informed consent, so that users know what their sensitive data will be used for. The users should also have the possibility to control their own information (update, correct or delete profiles) about themselves. Such functionality can for example be implemented using the PrimeLife framework [13].

It must also be possible to retrofit privacy enhancing technologies in a non-invasive way to existing CIIIs, in order to maximise the return on investments on improvements to existing CIIs. This typically means that existing parts of the infrastructure, critical to the operation of production processes, may be required to be left untouched by security or privacy enhancing technologies, whereas attacks and privacy leakages will need to be detected at the gateways or at services exposed to the Internet.
Pseudonymisation or encryption may be needed in cases where it is important that information later can be deanonymised. Examples of this include data forensics or tamper resistant audit logs that ensure protection of the privacy of workers involved in normal scenarios, but allows for revealing the identities when incidents need to be investigated.

B. Information Leakage Control

As mentioned in Section II, there are several inhibitors against information sharing; including suspiciousness, lack of awareness and lack of technical solutions to enforce protection of the sensitive information. The PRECYSE project aims at mitigating these inhibitors by adding components that can detect information leakages and enforce a privacy policy to reduce these leakages. Enforcement will be based on a reversible anonymisation scheme that supports encryption and anonymisation of information down to XML element/attribute level. Reversible anonymisation means that information which is defined as sensitive is anonymised, however a specification on how to undo the anonymisation is stored encrypted together with the data [14]. This allows for reversing the anonymisation using a deanonymiser tool, and also allows for fine-grained control over how information is being anonymised and presented [14]. This approach is different from traditional pseudonymisation, where a unique cryptographic value represents or refers to the private or confidential information.

The approach furthermore supports multi-level security by specifying an XACML anonymisation policy that compartmentalizes information in XML documents into different encrypted security levels based on XPath expressions, so that only authorised stakeholders can reverse the anonymisation for given security levels. This is built as an extension of the XACML decision cache based anonymiser in [11], and supports both traditional irreversible anonymisation and reversible anonymisation as described above. The scheme amongst others supports key sharing based on threshold cryptography to enforce separation of duties constraints, for example to ensure that a privacy officer and security officer need to agree to disclose data. This allows for sharing private or confidential information with semi-trusted parties in a secure way, and also provides detailed control of who can access this information, including support for time-limited data retention based on the time-based encryption scheme in [12].

Private or confidential information may leak via different sources. Information leakage may occur accidentally, for example through data queries, error messages or sent data. Another problem is that insiders mistakenly may send sensitive information, for example via email on mobile phones, or by misconfiguration of services, for example wrong access rights on web servers or if databases are exposed to the Internet without proper authentication and authorisation.

Cyber-attacks may cause even more harmful information leakages, by revealing information about system weaknesses that may be abused, as well as by performing industrial espionage which may harm the critical infrastructure provider financially.

Information leakage control is in other words needed for several reasons. The above examples show that sensitive information needs to be protected to avoid eavesdropping. Furthermore unintended flows of sensitive data, for example due to misconfigurations, negligence or human error should be identified and restricted.

Information leakage control is also required to support sharing of best practices and attack information, amongst others for:

- outsourced Managed Security Services (MSS);
- exchange of attack related information between Computer Emergency Response Teams (CERTs) or peer organisations;
- exchange of countermeasures and best practices for mitigating attacks between different organisations that collaborate on improving the security.

This can be done using emerging standards like the trusted automated exchange of indicator information (TAXII) [15], and structured threat information expression (STIX) [16]. Common for all these cases, is that a set of semi-trusted organisations need to collaborate by sharing information that may be considered private or confidential. This means that appropriate mechanisms (e.g. metrics or indicators) are needed for enforcing and verifying that the privacy policy indeed is functioning correctly.

C. Privacy Metric

The methodology plans to use Shannon entropy as basis for the privacy metric [17]. This is a metric that also previously has been proposed as a privacy metric [18], [19], [20]. Shannon entropy is defined as follows:

$$ H_1(X) = \sum_{x \in X} P[X = x] \log \frac{1}{P[X = x]} $$  \hspace{1cm} (1)
where $X$ is a discrete random variable and $\chi$ is the set of all values (symbols) $X$ can take. Shannon entropy is useful to detect anomalies in information being transmitted, for example unintended information leakages, anomalous information or services, detection of Denial of Service attacks by analysing information dispersion and also for detecting attacks on encrypted protocols like SSH, SSL etc [9]. Figure 1 illustrates how entropy analysis may be performed. It shows the entropy probability distribution of Snort IDS alarms triggering on the IDS rule with SID 1:1437 Windows Multimedia Download. Entropies are calculated over all octets of the payload excerpt in the IDS alarm. The results from the experiment shows that IDS alarms where the payload has been anonymised clearly stand out as a separate cluster with no variance. In addition, it can be observed that the IDS rule triggers on two main types of traffic: the start of the compressed video stream and compressed data inside the video stream. The entropy of the first cluster is lower, since this includes the compression dictionary used to decode the video stream. Furthermore, the standard deviation of the entropy may be used as a metric that indicates privacy leakage [8].

Techniques like clustering of IDS alarm entropies to identify groups of IDS alarms with similar properties, for example representing different attack vectors, can then be used as part of a privacy enforcement scheme [21]. Alternatively, entropy thresholds can be used to verify that a privacy policy is operating correctly, or as part of a privacy policy enforcement scheme, for example to anonymise data streams that by investigation are shown to leak a significant amount of private or confidential information.

IV. PRIVACY AND SECURITY ARCHITECTURE

PRECYSE aims at providing a methodology and tools supported by checklists, indicators and metrics to both identify and mitigate such information leakages using a set of concerted countermeasures as illustrated in Figure 2. The architecture protects private or confidential information in a separate security layer. The architecture for protecting critical infrastructure mainly consist of three components: Information Security Management, Control and Domains. These components use core security elements of the ESB, like Access Control, Encryption, Anonymiser, Deanonymiser and Secure logging. In addition, each of the components are connected to the ESB via a separate connector module. Each of these functions are explained in more detail below:

A. Information Security Management

Information Security Management (ISM) performs risk and vulnerability analysis as well as high-level selection of security controls using the ISMS tool. The ISM repository contains information about assets, infrastructure topology, identified vulnerabilities as well as high-level definition of safeguards and vulnerability tests. This information is considered very valuable, but also dangerous if it falls into the wrong hands. All information in the ISM Repository is therefore considered confidential/graded and must be protected according to best practices for managing EU Confidential Information (EUCI). Information Security Management is separated from security operations in the Control module, to reduce the risk of privacy or security attacks by correlating information in these databases. Furthermore, confidential information about vulnerabilities, assets, topology or configurations may additionally be stored encrypted and anonymised according to the ISM security policy, so that deanonymisation only can be performed by trusted stakeholders or services.

Most of the ISM repository should be stored on encrypted disk shares, to avoid simple plaintext attacks on the data. Sensitive data can furthermore if needed be protected using database encryption proxies like CryptDB. This is a practical approach for encrypting sensitive data in existing databases like MySQL or PostgreSQL which allows relatively simple (but common) SQL queries to be performed on encrypted data [10].

Furthermore, the ISM module allows exchange of threat, vulnerability and attack mitigation information to Computer Emergency Response Teams (CERTs) and other semi-trusted parties, by being able to export anonymised and/or encrypted attack and threat information from the ISM repository.

B. Control

Control contains the main functionality for the SOC, like Security Incident and Event Management (SIEM), Central repository storing IDS alarms and other events, and the Correlation engine. The latter correlates different IDS alarms, and may send out correlation alerts if combinations of IDS alarms...
representing attack scenarios are identified. The Control may also contain the Policy Administration Point (PAP) as part of the Security layer. This is used to manage privacy and security policies, for example to set an anonymisation policy for IDS alarms or to manage XACML authorisation or security keys. The functionality in the PAP will be restricted on a role basis to authorised personnel, so that for example a privacy officer can manage the privacy policies and a security officer can manage other authorisations. Policy administration may be done centrally if the SOC is run in-house, or in a separate Domain, if the Control is outsourced.

Security analysts will handle IDS alarms and perform attack investigations on the Central GUI. The SIEM solution and Central repository support storing anonymised or encrypted IDS alarms in IDMEF format, based on an XACML authorisation and anonymisation policy. This allows for having privacy-enhanced intrusion detection services, where elements or attributes of IDS alarms, which may leak private or confidential information, can be anonymised and/or encrypted based on a privacy policy. Anonymised or encrypted IDS alarms may also be stored in the central repository, so that only authorised security analysts can access this information. Access to this information is furthermore logged using a secure log server (not shown in the figure). It is assumed that the central correlation engine can run as a trusted service, so that it can deanonymise necessary information in IDS alarms, correlate them in time or across IDS sensors, and anonymise any subsequent correlation alarms generated on the basis of these. This mitigates some of the drawbacks security analysts have from not being able to investigate anonymised information in IDS alarms. The reversible anonymisation scheme allows for fine-grained access to the underlying information, which means that only necessary information, as defined in the XACML privacy policy, will be available for the alarm correlation system. This reduces the need for performing operations on encrypted values. However, the reversible anonymisation scheme can if necessary be extended to support such operations, since the anonymised XML elements or attributes can take any value, including using homomorphic encryption or other schemes which allow calculating or comparing encrypted values.

There are furthermore ISM agents that are able to provide risk metrics (e.g. historic frequency and type of attack) as well as privacy leakage metrics and indicators to the ISMS module. These metrics are used to verify the privacy policy and show the efficacy of anonymisation policies. One way to measure the efficacy of an anonymisation policy for a given information element or attribute, is to measure the Shannon octet entropy of the anonymised data, which will have zero or close to zero standard deviation if the anonymisation or encryption policy works as expected, assuming sufficiently long input [21], [8].

C. Domains

The Domains are used to verify and enforce the privacy and security policy of a given target network enclave. A network enclave is defined as network or set of networks that are managed by the same security policy, from the same domain [22]. The main functions of the Domain is to perform attack detection, network management, vulnerability assessments and tests, and correlate IDS alarms and other events within a Domain. It is assumed that IDS alarms will be correlated on two levels - both within a Domain and at Central level, to reduce the number of IDS alarms that need to be sent to Central level.

The ISM agents perform tests and measurements against the target Enclave. These are agents that in some cases will run on the target equipment (e.g. OpenSCAP2) or may run on the network, if active tests are accepted by the security policy (e.g. OpenVAS3). The tests will be based on the Security Content Automation Protocol (SCAP) suite of standards [23], which amongst others includes the Open Vulnerability Assessment Language (OVAL) for tests that are automatable and the eXtensible Configuration Checklist Description Format (XCCDF) for defining test suites of OVAL tests. ISM agents will also be used to verify and measure the efficacy of privacy and security policies within a given Domain. This means that privacy-enhanced IDS also is supported within the Domain in a similar way as for the Control module. Access control and encryption can also be controlled per Domain.

The ESB will also support secure logging, where only authorised personnel have access to the logs and where the log data retention time can be configured, based on the solution in [12].

V. PRIVACY POLICY MANAGEMENT

The methodology is based on the well-known Plan Do Check Act (PDCA) model of improvement, which amongst others is used by the ISO27000 set of security management standards [24].

The methodology supports planning of an information protection scheme by supporting development of a privacy policy which includes elements like anonymisation, encryption, access control, key-management, trust handling related to digital certificates, privacy leakage measurements etc. Privacy metrics can be used during the planning process to quantify the risk of leaking private or confidential information from critical infrastructures, and also for identifying where these leakages are.

The methodology supports enforcement (do) of the privacy policy by allowing central management of safeguards and countermeasures based on a risk assessment that identifies the major risks from a privacy or confidentiality perspective. This will be implemented as an open methodology with supporting tools based on a service oriented architecture. The solution will be based on the Open Source Information Security Management System (ISMS) Verinice, which will be integrated with other tools (both existing tools like Snort, OSSEC and OpenNMS, as well as PRECYSE specific tools). The tools will be integrated using the ESB, so that vulnerability tests based on OVAL as well as other relevant metrics and indicators

---

2 OpenSCAP: http://www.open-scap.org
3 OpenVAS: http://www.openvas.org
required by the risk analysis can be imported into the ISMS (e.g. historic attack vector frequencies, false alarm rates or privacy leakage metrics). This information can then be used for evaluating the overall system risk as well as analysing the effect of introducing various countermeasures against the identified risks, which allows the system administrator to select the countermeasures that best protect against the identified risks.

Furthermore, the methodology is able to check that the privacy policy works as intended, by deploying measurement agents which verify:

- that the privacy policy is configured as expected;
- that the policy is operative;
- and verify the expected level of information opacity (transparent/mixed/encrypted), i.e. that the information behaves as expected.

Entropy metrics can be used to assert that information which is expected to be encrypted or anonymised is being enforced according to the privacy policy. They can also be used to verify that encrypted traffic does not run where this is not expected (for example on a process control network), to enforce a transparent network policy. The metrics can furthermore be used to detect faulty configurations, unexpected traffic etc. They can also be used to trigger actions if privacy leaks exceed given thresholds, or if hypothesis testing shows that a statistical model of the underlying traffic is no longer supported. This allows for verifying that the privacy policy remains effective over time. This is closely related to anomaly-based intrusion detection which triggers on information that deviates significantly from what the model of normal traffic predicts. Information entropy may also be used to detect some privacy or confidentiality attacks, for example abuse, theft of sensitive information, concealing of attacks, or attacks on encrypted protocols [9]. OVAL tests will be used to verify automatically whether system configurations can be considered secure and if encryption keys and digital certificates are properly protected.

If the measurements detect significant deviations from what is expected, then this can be used to trigger corrective actions to be performed, which triggers a new iteration of improvement actions (risk analysis, control selection etc.). Corrective actions can for example be to improve IDS rules or to anonymise or encrypt information in IDS alarms that by inspection is found to leak private or confidential information. It may also involve improving other privacy controls, for example to ensure that confidential information as far as practically possible is kept encrypted. Overall, this will provide a structured approach for reducing leakage of private or confidential information from security operations according to the need-to-know principle to a much larger degree than what is possible today.

VI. Related Work

The proposed privacy handling methodology and architecture is based on existing standards like ISO27001 [24], Magerit risk analysis [25], and relevant NIST standards, e.g. [26], [27], [23]. The ESB components are based on XML Encryption and Signature [28], [29], XACML and SAML [30], [31] and IDMEF for IDS alarms [32]. We have not been able to find any examples of ESB-architectures that support privacy-enhanced operation, however xESB is somewhat related by being a security-enhanced ESB [33]. xESB allows for enforcing monitoring, preventive and reactive policies both for access control and usage policies, and it supports indicators that help SOA administrators assess the effectiveness of their policies. xESB only supports coarse-grained access control of information on a message basis, and does not support fine-grained authorisation, anonymisation and confidentiality protection down to elements or attributes of XML messages as our solution does.

Privacy enhanced operation is supported by adding suitable privacy controls and by using privacy metrics to verify that a privacy policy is being enforced. Other methodologies that incorporate privacy requirements into the design process are for example the PriS method [34] and eTVRA [35]. These are high-level methodologies that are useful in an early design phase of a privacy-enhanced system, but they are less well suited for managing and reducing privacy gaps during operation, since they lack suitable privacy metrics and the necessary privacy controls. They can therefore be considered complementary rather than competing to the proposed method.

Fine-grained anonymisation of information in XML documents was first proposed in [36]. This early solution is not based on XACML and does not support anonymisation of data. An XACML-based privacy-centred access control system is proposed in [13]. This solution focuses on credential management to provide users with control over their data. Our solution is different by supporting fine-grained reversible anonymisation of information in XML documents. The above mentioned system can therefore be considered complementary to our approach, and may be useful if user profiles containing personally identifiable information need to be managed.

The proposed anonymisation method is also related to the field of privacy-enhanced intrusion detection systems, which first was proposed by [37]. Other related works on privacy-enhanced IDS are [38], [39], [40], [41]. Common for all of these is that different pseudonymisation schemes are used to implement privacy-enhanced IDS. Our solution is different by proposing an XACML-based reversible anonymisation scheme, which furthermore is not restricted to anonymising IDS alarms, but also can anonymise XML-based protocols in general.

VII. Conclusions and Future Work

In this article, we have proposed a privacy and confidentiality enforcement methodology and architecture for critical information infrastructures. The methodology and supporting tools are based on existing best practices and standards for information security management, and uses the open risk assessment standard Magerit [25]. The proposed solution uses a SOA-based architecture with XACML-based authorisation
and anonymisation policies that allow fine-grained authorisation, anonymisation or encryption of content in messages on the service bus down to XML element or attribute level. The approach can be used to add confidentiality protection to information in existing XML-based standards like STIX or IDMEF. This is useful to protect private or confidential information when attack information or IDS alarms need to be shared between semi-trusted parties. The approach furthermore uses standardised vulnerability test formats, like OVAL and XCCDF to facilitate sharing of test results and best practices.

The methodology is based on the well-known Plan-Do-Check-Act model of improvement, and can provide verifiable management of privacy and confidentiality of critical information infrastructures. The approach uses quantitative privacy leakage metrics that can be measured automatically, which should significantly increase the efficiency and lower the price of privacy and security assessments compared to existing ISMS methods, which largely are based on qualitative metrics and manual data entry.

Future work includes implementation, testing and validation of the privacy-preserving CII risk management methodology and architecture. Investigating other privacy metrics than Shannon entropy, for example k-anonymity or l-diversity is also left as future work.

ACKNOWLEDGMENT

This paper has been partially supported by the project «PRECYSE – Protection, prevention and reaction to cyber-attacks to critical infrastructures», funded by the European Commission under the FP7 programme with contract number FP7-SEC-2012-1-285181, http://www.precyse.eu.

Also thanks to the anonymous reviewers for good suggestions on improving the paper.

REFERENCES


