# Privacy Handling for Critical Information Infrastructures

Nils Ulltveit-Moe, Terje Gjøsæter, Sigurd 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 potentially private or confidential information from the critical information infrastructures themselves. The paper outlines how the proposed approach can be used to identify, quantify and reduce leakages of private or confidential information and also how privacy and confidentiality risks can be manged, 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 for production transport and distribution of electricity; water supply, food production, transportation infrastructures, Internet and 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 governmental 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)[1] 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. 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 (Prevention, protection and reaction to cyber-attacks on critical infrastructures), can be used to identify and mitigate privacy and confidentiality risks in CII to reduce the gap in security.

The rest of the article is organised as follows: The next Section introduces some cases that demonstrates 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, and Section IV discusses related work. Finally, in Section V concludes the paper and indicate directions for future work.

## II. Motivation and Use Cases

### A. Information Sharing

A reason for identifying and protecting against leakages of private or confidential information, is information sharing between semi-trusted organisations, as mentioned in the introduction. 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, to collaboratively improve the attack detection and mitigation capabilities.

Examples of services that may benefit from such information sharing is 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 [3], [4]. This means that cyber-attacks can be detected and mitigated at a lower cost, since the collaborating organisations can share the initial cost of attack analysis and work needed to develop suitable mitigation strategies. Furthermore, increasing the security may lower the risk of being attacked, at least by cyber-criminals [4].

[1] http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas_roadmap

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 [5]:

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 [6]:

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 important to 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 can be placed as close as possible to the data source [7]. These reactive measures 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 approach, 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 requirements.

Strong security is a prerequisite for privacy, even if the security schemes must be consciously applied to achieve the desired goals. If done right there may also be security benefits. For intrusion detection systems and similar technologies, privacy enhancing technologies may 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. Examples of this is to use an anonymising proxy an application level firewall or simple intrusion detection system that rejects information outside define ranges, parameter overflow attempts or even entropy anomalities, for detecting information leakages [7]. The latter case may even have some synergies with anomaly-based IDS based on learning systems.

Full lifecycle protection is necessary for private or confidential information. This means that such information should be protected using cryptographic means as far as practically possible from the information is generated and until the information is no longer needed. After that, it should be safely deleted, for example by invalidating the encryption key.

Visibility and transparency will be needed in the form of logging and auditing procedures, to ensure nonrepudability as well as that access to sensitive information is warranted and does not get abused. 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. Anonymous access may also be required, for example is the case for transport infrastructures. An example of this is automatic road tolls where cash based services can be used to avoid electronic registration.

It must also be possible to retrofit privacy enhancing technologies in a non-invasive way to existing CIIs, in order to maximise the return on investments on incremental 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, for example based on cryptographic primitives, may be needed in cases where it is be important that information later can be deanonymised. Examples of this include data forensics or tamper resistant audit logs that both ensure protection of the privacy of workers involved in normal scenarios but allow for deanonymisation when events 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 using existing standards, for example the Intrusion Detection Message Exchange Format (IDMEF) by IETF. In addition we will add support for multi-level security based encryption and anonymisation of detailed information (down to element/attribute level) of these and other relevant XML-based formats. This allows for sharing private or confidential information with semi-trusted parties in a secure way, and will also provide detailed control of who may access this information.

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 databases 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 by the attackers, as well as by performing industrial espionage that may harm the critical infrastructure provider financially.

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

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) [9], and structured threat information expression (STIX) [10]. 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 means (e.g. metrics or indicators) for both enforcing and verifying that the privacy policy indeed is functioning correctly are needed. These metrics and indicators can furthermore be useful both from a privacy and security perspective, for example to detect certain attacks (e.g. attacks on the privacy policy or more general attacks, like Denial of Service attacks).

### C. Privacy Metric

The methodology plans to use Shannon entropy as basis for the privacy metric [11]. This is a metric that also previously has been proposed as a privacy metric [12], [13], [14]. Shannon entropy is defined as follows:

$$H_1(X) = \sum_{x \in \chi} P[X = x] log \frac{1}{P[X = x]} \qquad (1)$$

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 for detecting attacks on encrypted protocols like SSH, SSL etc. 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 [15].

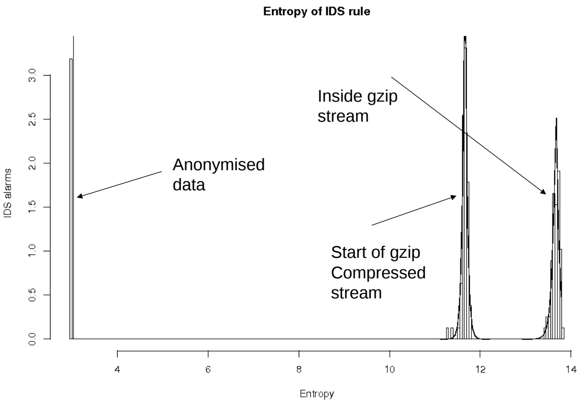

Figure 1. Entropy analysis example (Snort SID 1:1437 Windows Multimedia Download).

This means that techniques like clustering of IDS alarms, or entropy thresholds may be used either 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.

### D. 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.*

Each of these components can use core security elements of the ESB, like Access Control, Encryption, Anonymiser/proxy, Deanonymiser and Secure logging. In addition, each of the components are connected to the ESB via a separate connector module. A network enclave is defined as network or set of networks that are managed by the same security policy, from the same domain. Each of these functions are explained in more detail below:

*1) Information Security Management:* Information Security Management (ISM) performs risk and vulnerability analysis as

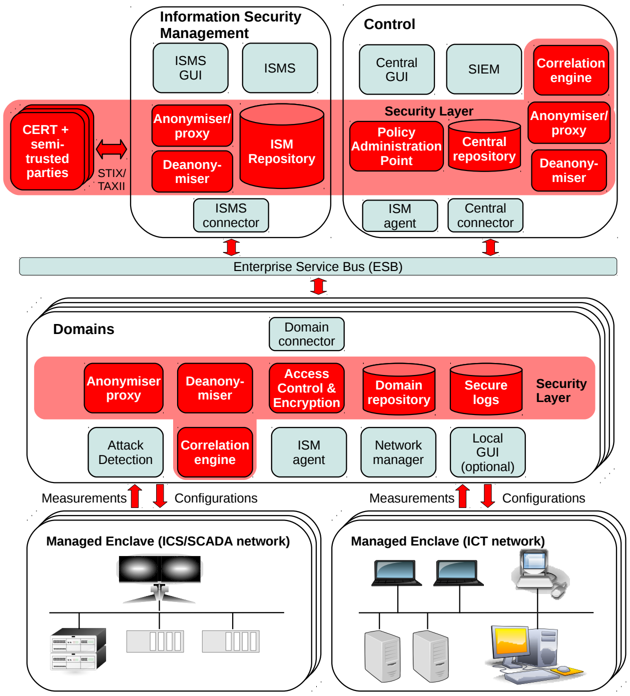

Figure 2. Privacy and Security Architecture.

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. However, most of the ISM repository should be stored on encrypted disk shares, to reduce the performance penalty when accessing this information. This allows trusted services to run simulations and security gap analysis more efficiently than if every database record needed deanonymisation.

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.

*2) 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 that represent 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, that 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 IDS alarms, correlate them, and reanonymise any subsequent correlation alarms. This mitigates some of the drawbacks security analysts have from not being able to investigate anonymised information in IDS alarms.

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 ISM. These metrics are used by ISM to verify the privacy policy and show the efficacy of anonymisation policies.

*3) Domains:* The Domains are used to verify and enforce the privacy and security policy of a given enclave. 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. From a high level perspective, this is done by measuring security and privacy related data from the target Enclave, and having the possibility to reconfigure assets of the managed Enclave using the NETCONF protocol. The Domain may also have a local GUI and a local Domain repository for storing and handling IDS alarms.

The ISM agents perform tests and measurements against the target Enclave. These are agents that in some cases will run on the target equipment (for example based on OpenSCAP) or may run on the network, if active tests are accepted by the security policy (based on OpenVAS). The tests will be based on the OVAL for tests that are automatable and the eXtensible Configuration Checklist Description Format (XCCDF) for tests that cannot be automated. Other ISM agents are able to measure Quality of Service of the target enclave, like availability, bandwidth etc. 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 functionality for secure logging, where only authorised personnel have access to the logs, and where the log data retention time can be configured [16].

### *E. Privacy Policy Management*

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

The methodology supports *planning* of an information protection scheme by supporting development of a privacy policy that 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.

The methodology supports enforcement *(do)* of the privacy policy by allowing for 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 the Open Vulnerability Assessment Language (OVAL) as well as other relevant metrics and indicators required by the risk analysis (e.g. historic attack frequencies for given attack vectors and false alarm rates for countermeasures) can be imported into the ISMS. 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. This 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 whether information which is expected to be encrypted really is that. 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 be used to detect faulty configurations, unexpected traffic etc. They can also be used to trigger actions if privacy leakages 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 that triggers on information that deviates significantly from what the model of normal traffic predicts. Information entropy may also be used to detect some privacy attacks, for example abuse, theft of sensitive information, in some cases concealing of attacks or denial of service attacks, or attacks on encrypted protocols [17]. 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 trigger 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 that can be used to reduce 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.

## IV. Related Work

Many authors consider privacy aspects in systems that can be seen a as a part of CII without focusing specifically on CII aspects. For example, privacy in telecommunication systems was studied in [18], protection of location privacy in telecommunication systems in [19], [20], privacy preserving in sensor networks was studied in [21], [22], privacy in IoT [23], privacy leakage in IDS [8]. However, very few of these studies were focused on privacy in CIIs. Only recently have authors started to focus specifically on privacy aspects in CII. In [24] the authors point at security and privacy concerns that arise in connection with deployment of smart grid. One of the purposes of smart grids is to increase resilience to control system failures and cyber security attacks. However, it also leads to customers sharing more information about their use of energy and therefore expose their private habits and behavior. Usage misinformation injected into control systems can seriously harm electrical infrastructure. In [25] authors present an analysis of security and privacy issues in Smart Grids operating in different Cloud-based environments.

The approach proposed in this paper is different and novel compared to previous approaches. The approach uses an architecture that supports privacy leakage metrics and standardised tests to support the information security management process. This allows for partially automated and verifiable management of privacy and confidentiality for critical information infrastructure, with subsequent concerted deployment of countermeasures where these have been tested and found safe. This reduces the gap between high-level ISMS methodologies and operative measurements and allows for better control of privacy leakages than existing methods do.

## V. 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 is based on existing best practices and standards for information security management, and uses the open risk assessment standard Magerit. The proposed solution uses SOA-based architecture with XACML-based authorisation and anonymisation for integration of measurement agents and countermeasures. The approach will support existing XML-based standards like STIX or IDMEF to protect private or confidential information when attack information or IDS alarms need to be shared between semi-trusted parties. The approach is based on standardised vulnerability test formats, like OVAL and XCCDF to facilitate sharing of test results and best practices.

The proposed approach provides partially automated and verifiable management of privacy and confidentiality of critical information infrastructures, and should significantly increase the efficiency and lower the price of 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.

## References

[1] CrySys lab, "Duqu: A stuxnet-like malware found in the wild, technical report," 2011. [Online]. Available: http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

[2] Crysys lab, "sKyWIper: a complex malware for targeted attacks," 2012. [Online]. Available: http://www.crysys.hu/skywiper/skywiper.pdf

[3] W. Ding, W. Yurcik, and X. Yin, "Outsourcing internet security: Economic analysis of incentives for managed security service providers," in *Internet and Network Economics*, ser. LNCS. Springer, 2005, vol. 3828, pp. 947–958.

[4] S. E. Schechter and M. D. Smith, "How much security is enough to stop a thief? the economics of outsider theft via computer systems and networks," *Financial Cryptography*, vol. 2742, pp. 122–137, 2003.

[5] ENISA, "Resilience metrics and measurements: Technical report," 2011. [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/reports/metrics-tech-report

[6] A. Cavoukian, "Privacy by design," http://privacybydesign.ca/about/principles/, 2009.

[7] N. Ulltveit-Moe and V. Oleshchuk, "Decision-cache based xacml authorisation and anonymisation for xml documents," *Comput. Stand. Interfaces*, vol. 34, no. 6, pp. 527–534, Nov. 2012.

[8] N. Ulltveit-Moe and V. Oleshchuk, "Privacy leakage methodology (PRILE) for ids rules," in *Privacy and Identity Management for Life*, ser. IFIP Advances in Information and Communication Technology, M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, and G. Zhang, Eds. Springer Boston, 2010, vol. 320, pp. 213–225, 10.1007/978-3-642-14282-6_17.

[9] J. Connolly, M. Davidson, M. Richard, and C. Skorupka, "The trusted automated eXchange of indicator information (TAXII)," 2012. [Online]. Available: http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf

[10] The MITRE Corporation, "Standardising cyber threat intelligence information with the structured threat information eXpression (STIX)," 2012. [Online]. Available: http://makingsecuritymeasurable.mitre.org/docs/STIX-Whitepaper.pdf

[11] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948.

[12] S. Clauß and S. Schiffner, "Structuring anonymity metrics," in *Proceedings of the second ACM workshop on Digital identity management*. Alexandria, Virginia, USA: ACM, 2006, pp. 55–62.

[13] G. Smith, "Quantifying information flow using Min-Entropy," in *Quantitative Evaluation of Systems (QEST), 2011 Eighth International Conference on*, Sep. 2011, pp. 159 –167.

[14] L. Sankar, S. Rajagopalan, and H. Poor, "Utility and privacy of data sources: Can shannon help conceal and reveal information?" pp. 1 –7, 2010.

[15] N. Ulltveit-Moe and V. A. Oleshchuk, "Measuring privacy leakage for IDS rules," 2013, submitted.

[16] S. Köpsell and P. švenda, "Secure logging of retained data for an anonymity service," in *Privacy and Identity Management for Life*, M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, and G. Zhang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, vol. 320, pp. 284–298.

[17] J. Goubault-larrecq and J. Olivain, *Detecting Subverted Cryptographic Protocols by Entropy Checking*. Laboratoire Spécification et Vérification, ENS Cachan, France, 2006.

[18] G. M. Køien, "Privacy enhanced cellular access security," in *Proceedings of the 4th ACM workshop on Wireless security*, ser. WiSe '05. New York, NY, USA: ACM, 2005, pp. 57–66.

[19] G. Køien and V. Oleshchuk, "Location privacy for cellular systems; analysis and solution," in *Privacy Enhancing Technologies*, ser. Lecture Notes in Computer Science, G. Danezis and D. Martin, Eds. Springer Berlin / Heidelberg, 2006, vol. 3856, pp. 40–58, 10.1007/11767831_4.

[20] N. Ulltveit-Moe, V. Oleshchuk, and G. Køien, "Location-aware mobile intrusion detection with enhanced privacy in a 5g context," *Wireless Personal Communications*, vol. 57, pp. 317–338, 2011, 10.1007/s11277-010-0069-6.

[21] V. Oleshchuk, "Privacy preserving monitoring and surveillance in sensor networks," in *Frontiers of High Performance Computing and Networking ISPA 2007 Workshops*, ser. Lecture Notes in Computer Science, P. Thulasiraman, X. He, T. Xu, M. Denko, R. Thulasiram, and L. Yang, Eds. Springer Berlin / Heidelberg, 2007, vol. 4743, pp. 485–492, 10.1007/978-3-540-74767-3_50.

[22] A. Michalas, V. Oleshchuk, N. Komninos, and N. Prasad, "Privacy-preserving scheme for mobile ad hoc networks," in *Computers and Communications (ISCC), 2011 IEEE Symposium on*, 28 2011-july 1 2011, pp. 752–757.

[23] V. Oleshchuk, "Internet of things and privacy preserving technologies," in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on*, may 2009, pp. 336 –340.

[24] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *Security Privacy, IEEE*, vol. 7, no. 3, pp. 75–77, may-june 2009.

[25] Y. Simmhan, A. Kumbhare, B. Cao, and V. Prasanna, "An analysis of security and privacy issues in smart grid software architectures on clouds," in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, july 2011, pp. 582 –589.