Visualization of Privacy Risks in Software Systems

George O. M. Yee

Computer Research Lab
Aptusinnova Inc.
Ottawa, Canada
email: george@aptusinnova.com

Dept. of Systems and Computer Engineering
Carleton University
Ottawa, Canada
email: gmyee@sce.carleton.ca

***Abstract*—Software systems can be found in almost every aspect of our lives, as can be seen in social media, online banking and shopping, as well as electronic health monitoring. This widespread involvement of software in our lives has led to the need to protect privacy, as the use of the software often requires us to input our personal information. However, before privacy can be protected, it is necessary to understand the risks to privacy that can be found in the software system. Indeed, such understanding is key to protecting privacy throughout the system's range of application. This paper presents a straightforward method for effectively visualizing and identifying privacy risks in software systems, and illustrates the method with examples.**

Keywords-software; system; privacy; risks; visualization.

I. INTRODUCTION

Numerous software systems targeting consumers have accompanied the rapid growth of the Internet. Software systems are available for banking, shopping, learning, healthcare, and Government Online. However, most of these systems require a consumer's personal information in one form or another, leading to concerns over privacy. For these systems to be successful, privacy must be protected.

Various approaches have been used to protect personal information, including data anonymization [1] and pseudonym technology [2]. Other approaches for privacy protection include treating privacy protection as an access problem and then bringing the tools of access control to bear for privacy control [3]. However, these approaches presume to know where and what protection is needed. They presume that some sort of analysis has been done that answers the question of "where" and "what" with respect to privacy risks. Without such answers, the effectiveness of the protection comes into question. For example, protection against house break-ins is ineffective if the owner only secures the front door without securing other vulnerable spots such as windows. An effective break-in risk analysis would have identified the windows as additional locations having break-in risks (where and what) and would have led to the windows also being secured. The result is a house that is better protected against break-ins. In the same way, privacy risk identification considering "where" and "what" is essential to effective privacy protection - this work proposes a visual method for such identification.

The objectives of this paper are to a) propose an effective method for visualizing privacy risks in software systems to identify where and what risks are present, and b) illustrate the method using examples. The method is limited to the identification of privacy risks. It does not include estimating the likelihood of a risk being realized.

In the literature, there are significant works on security threat analysis but very little work on privacy risk identification using visualization. In fact, the only works that are directly related to privacy risk identification appear to be those on "privacy impact assessment (PIA)", originating from government policy [4]. PIA is meant to evaluate the impact to privacy of new government programs, services, and initiatives. PIA can also be applied to existing government services undergoing transformation or re-design. However, PIA is a long manual process consisting mainly of self-administered questionnaires. It is not focused on software systems nor does it employ visual techniques as proposed in this work.

This paper is organized as follows. Section II defines privacy, privacy preferences, privacy risks, and what they mean for software systems. Section III presents the proposed method for privacy risk visualization, together with examples. Section IV discusses related work. Section V presents conclusions.

II. PRIVACY

As defined by Goldberg et al. in 1997 [5], privacy refers to the ability of individuals to *control* the collection, retention, and distribution of information about themselves. This leads to the following definition of privacy for this work.

DEFINITION 1: *Privacy* refers to the ability of individuals to *control* the collection, purpose, retention, and distribution of information about themselves.

Definition 1 is the same as given by Goldberg et al. except that it also includes "purpose". To see that "purpose" is needed, consider, for example, that one may agree to give out one's email address for the purpose of friends to send email but not for the purpose of spammers to send spam. This definition also suggests that "personal information", "private information" or "private data" is any information that can be linked to a person; otherwise, the information would not be "about" the person. Thus, another term for private information is "personally identifiable information (PII)". These terms are used interchangeably in this paper. In addition, controlling the "collection" of information

 ISBN: 978-1-61208-493-0

implies controlling *who* collects *what* information. Controlling the "retention" of information is really about controlling the *retention time* of information, i.e. how long the information can be retained before being destroyed. Controlling the "distribution" of information is controlling to which other parties the information can be *disclosed-to*. These considerations motivate the following definitions.

DEFINITION 2: A user's *privacy preference* expresses the user's desired control over a) *PII* - what the item of personal information is, b) *collector* - who can collect it, c) *purpose* - the purpose for collecting it, d) *retention time* - the amount of time the information is kept, and e) *disclosed-to* - which other parties the information can be disclosed-to.

DEFINITION 3: A *privacy risk* is the potential occurrence of any action or circumstance that will result in a violation of any of the components PII, collector, purpose, retention time, and disclosed-to in a user's privacy preference.

For example, Alice uses an online pharmacy and has the following privacy preference:

PII: name, address, telephone number
Collector: A-Z Drugs
Purpose: identification
Retention Time: 2 years
Disclosed-To: none

This preference states that Alice allows A-Z Drugs to collect her name, address, and telephone number, and that A-Z Drugs must: use the information only to identify her, not keep the information for more than 2 years, and not disclose the information to any other party.

This work considers only privacy risks as defined in Definition 3. The privacy preference components PII, collector, purpose, retention time, and disclosed-to have, in fact, been enacted by privacy legislation as fully describing the privacy rights of individuals in many countries, including Canada, the United States, the European Union, and Australia [6]. Thus, this work is consistent with privacy legislation, and treating only privacy risks defined by Definition 3 does not overly reduce the generality of this work.

III. METHOD FOR PRIVACY RISK VISUALIZATION

The proposed method for privacy risk visualization assumes the following common characteristics of a software system:

a) The software system requires the user's personal information in order to carry out its function. For example, an online bookseller requires the user's address for shipping purposes.
b) The software system may transmit the information (e.g., move it from one group to another within the software system's organization), store the information (e.g., store the information in a data base), and make use of the information to carry out its function (e.g., print out shipping labels with the user's address).

The method is based on the notion that the *location* of personal information gives rise to privacy risks. The importance of location is reflected in physical security, where sensitive paper documents are kept in a locked safe (a location) to protect privacy, rather than being left on a desk (a location). For a software system, storing the user's personal information in an encrypted database with secure access controls is the equivalent of storing it in a safe, with corresponding reduced privacy risks. The method, then, consists of i) determining all the possible locations in the software system where the user's personal information could reside, and ii) evaluating at each of these locations the possible ways in which the user's privacy preferences could be violated. The complete method is as follows:

A. Method for Privacy Risk Visualization

1. Draw the paths of all personal information flows within the software system, based on characteristic b) above, namely, that personal information can be transmitted, stored, and used. Use a solid arrow to represent the transmission of personal information items that are described by privacy preferences. Label the arrow with numbers, where each arrow number corresponds to a description of a personal data item in a legend. Use a square to represent the storage of personal information. Use a circle to denote the use of the information. Use a dashed rectangle to enclose circles or squares into physically distinct units. For example, two circles representing two uses would be enclosed by a dashed square if both uses run on the same computing platform. Physically separate units allow the identification of risks for any data flow between them. Circles or squares not enclosed by a dashed rectangle are understood to be already physically separate units. Label the squares and circles with letters. Each such label corresponds to a description of the type of storage or the type of use as indicated in the legend.
2. Use dashed arrows, numbered in the same way as the solid arrows in Step 1, to add to the drawing all non-personal information flows, if any, that are involved with the transmission, storage and use of the personal information. Non-personal information is information that is not personal or not private, i.e. information that cannot identify any particular individual, e.g., the price of something. The resulting drawing is called a Personal Information Map (PIM). Figure 1 illustrates steps 1 and 2 for the software system of an online seller of merchandise, e.g., Amazon.com, that requires the user's name, address, merchandise selection, and credit card number. These are considered as three personal information items where name and address together are considered as one item. Figure 1 also shows three non-personal information flows (4, 5, 6). The dashed rectangle enclosing A, B, and C indicates that A, B, and C all run on the same physical computing platform.

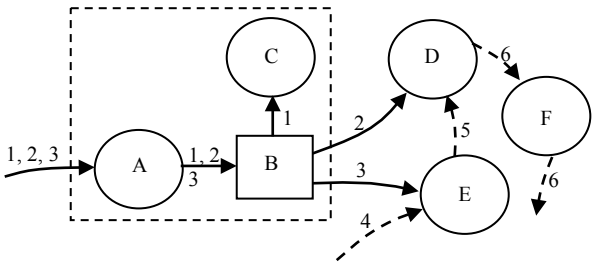
 ISBN: 978-1-61208-493-0

3. Inspect the PIM resulting from step 2, and for each location (flow arrow, storage square, and use circle) and each personal information item, enumerate the possible ways in which a privacy preference may be violated in terms of violations of any of *PII*, *collector*, *purpose*, *retention time*, and *disclose-to* (see Section II). This may be achieved by asking risk questions for each component, as suggested in Table 1, and drawing conclusions based on security and systems knowledge and experience. The risk questions are "how" questions, based on the idea that a risk arises where there is some way (i.e. how) for a violation to occur. Record the results in a Privacy Risks Table containing two columns: the left column for records of the form "(PII_1, PII_2, …/ locations)" and the right column containing the corresponding privacy risks. The Privacy Risks Table is the goal of the method. Table 2 illustrates this step for the online seller of Figure 1.

It is important to note that the PIM resulting from Step 2 is not a program logic flow diagram and one should not try to interpret it as such. It shows *what* PII is required, *where* PII goes, *where* PII is stored, and *where* PII is used, corresponding to the notion that the location of personal information is key to understanding privacy risks, as mentioned above.

TABLE 1. Risk Questions

Component	Risk Questions
PII	How can the user be asked for other PII, either intentionally or inadvertently?
collector	How can the PII be received by an unintended collector either in addition to or in place of the intended collector?
purpose	How can the PII be used for other purposes?
retention time	How can the PII retention time be violated?
disclose-to	How can the PII be disclosed either intentionally or inadvertently to an unintended recipient?



Legend:
A: receive and store data
B: database
C: print shipping label
D: pack item for shipping
E: charge credit card
F: send shipping status to buyer
1: name and address
2: item selected
3: credit card number
4: company account number
5: payment status
6: shipping status

Figure 1. PIM for an online seller of merchandise.

TABLE 2. Partial Privacy Risks Table Corresponding to Fig. 1

(PIIs / locations)	Privacy Risks
(1, 2, 3 / path into A); (2 / path into D); (3 / path into E)	Man-in-the-middle attack violates *collector*, *purpose*, and *disclose-to*; for path into A, user could be asked for personal information that violates *PII*
(1, 2, 3 / A, B); (1 / C); (2 / D); (3 / E)	Trojan horse, hacker, or SQL attack (for B) violates *collector*, *purpose*, and *disclose-to*; for B, information could be kept past *retention time*

Adding non-personal information flows in Step 2 is important to help identify potential unintended leakages of PII. For example, consider a "produce report" use circle that "anonymizes" (any obvious links to the information owner removed) PII and combines the result with non-personal information to produce a report for public distribution. The fact that both PII and non-PII flow into "produce report" could lead to identifying a personal information leakage risk.

It is recommended that this method be applied by a privacy risks identification team, consisting of no more than three or four people, selected for their technical knowledge of the software system and the work procedures and processes of the software system's organization. Good candidates for the team include the software system's design manager, test manager, and other line managers with the required knowledge. The team should be led by a privacy analyst who must also be knowledgeable about security threats and who should have the support of upper management to carry out the privacy risks identification. A definite advantage of the team approach would accrue to step 3, where the enumeration would be more thorough by virtue of more people being involved.

B. A more substantial example

Consider PatientBilling, a patient billing system running in a doctor's office. PatientBilling makes use of two business software systems: an accounting system PatientAccounting and an online payment system PatientPay.

Table 3 shows the user's personal information required by each system. The user provides her private information to PatientBilling which then discloses this information to PatientAccounting and PatientPay.

The proposed method for privacy risks visualization is carried out as follows:

Table 3. Personal Information Required

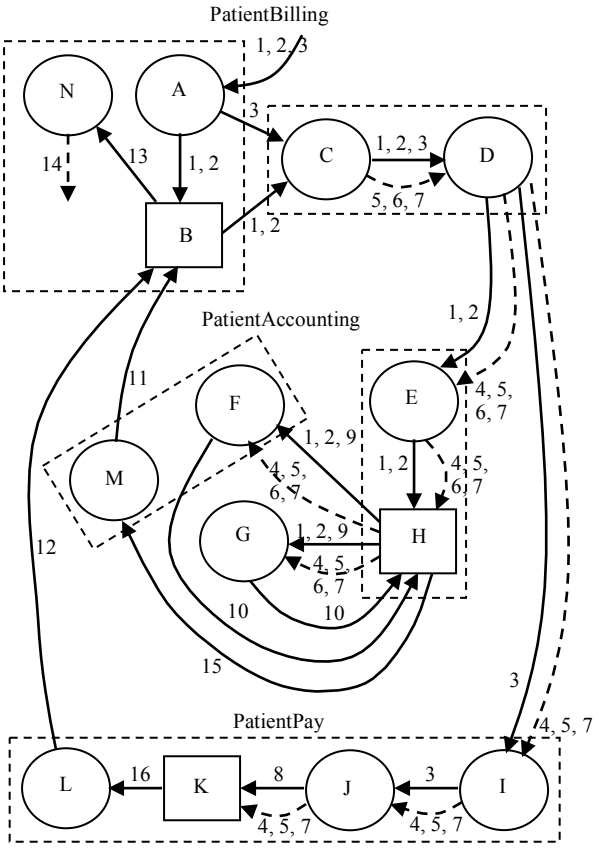
Software System	Patient Personal Information Required
PatientBilling	name and address, health complaint (patient name, health problem, health problem resolution), method of payment details (name, credit card number, credit card expiry date, health insurance number, health insurance expiry date)
PatientAccounting	name and address, health complaint (as above)
PatientPay	method of payment details (as above)

 ISBN: 978-1-61208-493-0

Steps 1 and 2: Draw the PIM for each software system (see Fig. 2**).** As shown in Figure 2, the following uses of personal information are extra to the core function of each system. First, both PatientAccounting (M) and PatientPay (L) send activity reports back to PatientBilling that contain personal information. These reports contain selections and re-arrangements of personal data (15, 16). Second, PatientBilling produces a publically accessible report for the medical association, giving statistics on the patients seen. To produce this report, PatientBilling (N) selects, re-arranges, and anonymizes personal data (13). Third, PatientAccounting allows its employees to partially work from home (G). Finally, the patient's method of payment details are used without being stored in databases.

Step 3: Enumerate privacy risks at private information locations. Table 4 gives a partial Privacy Risk Table for locations in Figure 2 that have interesting or serious privacy risks. The theft of personal information means that the information is under the control of an unintended party. Clearly, this can violate the corresponding privacy preference or preferences in terms of violating *collector*, *purpose*, *retention time*, and *disclose-to*. The risk of personal information theft arises so often that it is convenient to call it *CPRD-risk*, from the first letters of collector, purpose, retention time, and disclose-to.

To illustrate this step, the risks in the first 3 rows of Table 4 were obtained as follows. For the first row, it was noticed that the personal information flows through transmission paths connecting physically distinct units. The risk questions of Table 1 were then considered, leading to possible man-in-the-middle attacks that give rise to CPRD-risk. In addition, violations of PII are always possible unless strict controls are in place against it. For the second row, it was observed that the associated personal data are input to information use processes (e.g., A, C, D). The risk questions of Table 1 were again considered, leading to possible Trojan horse or hacker attacks that again give rise to CPRD-risk. For the third row, it was noticed that personal data are stored in databases. Once again the risk questions were considered, leading to possible SQL attacks against the databases, giving rise to CPRD-risk. In each of these three cases, knowledge of the system (personal data locations) and knowledge of information security (possible attacks) were needed to identify the risks. The remaining risks in Table 4 were derived in a similar fashion.



Legend:

A: receive and store data	E: receive and store data
B: database	F: update ledgers at work
C: process billing	G: update ledgers at home
D: disclose data	H: database
1: name and address	I: receive and forward data
2: health complaint	J: charge credit card or insurance; update doctor's account
3: method of payment details	K: database
4: doctor id	L: compose payment report
5: billing id	M: compose accounting report
6: time spent with patient	N: compose report for medical association
7: billing amount	14: anonymized report for medical association
8: doctor account update	15: accounting data
9: current ledger record	16: payment data
10: updated ledger record	
11: accounting report	
12: payment report	
13: patients seen data	

Figure 2. PIM for PatientBilling, PatientAccounting, and PatientPay.

IV. RELATED WORK

The literature on works by other authors, dealing *directly* with privacy risk visualization for software systems, appears to be non-existent. However, the following authors have written on topics that are related to privacy risk analysis. Hong et al. [7] propose the use of privacy risk models to help designers design ubiquitous computing applications that have a reasonable level of privacy protection. Their privacy risk model consists of two parts: a privacy risk analysis part and a privacy risk management part. The risk analysis identifies the privacy risks while the risk management part is a cost-benefit analysis to prioritize the risks and design artifacts to manage the risks. Visualization is not used.

A second class of related work applies privacy risk analysis to specific application areas. Biega et al. [8] propose a new privacy model to help users manage privacy risks in their Internet search histories. They assume a powerful adversary who makes informed probabilistic inferences about sensitive data in search histories and aim

TABLE 4. Partial Privacy Risks Table Corresponding to Fig. 2

(PIIs / locations)	Privacy Risks
(1, 2, 3 / path into A); (1, 2 / path between B and C, path between D and E); (3 / path between A and C, path between D and I); (12 / path between L and B); (11 / path between M and B)	Man-in-the-middle attacks lead to CPRD-risk; corresponding to 1, 2, 3, the patient could be asked for personal information that violates PII (i.e. asked for PII other than 1, 2, 3).
(1, 2, 3 / A, C, D); (13 / N); (1, 2 / E); (1, 2, 9 / F, G); (15 / M); (3 / J); (16 / L)	Trojan horse, or hacker attacks on the personal information use circles lead to CPRD-risk.
(1, 2, 11, 12 / B); (1, 2, 10 / H); (8 / K)	Potential SQL attacks on B, H, and K lead to CPRD-risk.
(13 / N)	A bad anonymization algorithm can expose personal information, leading to CPRD-risk.
(1, 2, 9 / G)	An insecure home environment, e.g., people looking over the shoulder or printed personal information lying on a desk in the clear, can also lead to CPRD-risk.
(1, 2, 9 / G)	If an employee works from home on a laptop and carries the laptop back and forth between home and work, possible theft or loss of the laptop can also lead to CPRD-risk for any of 1, 2, or 9 that might be temporarily stored in the laptop.
(1, 2, 9 / G)	If an employee works from home on a home PC and stores 1, 2, 9 on a flash memory stick, carrying the memory stick back and forth between home and work, possible theft or loss of the memory stick can also lead to CPRD-risk.

for a tool that simulates the adversary, predicts privacy risks, and guides the user. Paintsil [9] presents an extended misuse case model and a tool that can be used to check the presence of known misuse cases and their effect on security and privacy risks in identity management systems. Das and Zhang [10] propose new design principles to lessen privacy risks in health databases due to aggregate disclosure. None of these works employ visualization.

A third class of related work is of course the work on privacy impact analysis (PIA) [4] (Section I).

A fourth class of related work consists of security and privacy threat analysis, e.g., Nematzadeh and Camp [11]. Security and privacy threats are related risks. For example, a Trojan horse attack (security threat) can lead directly to the lost of private data (privacy threat). These works also do not use visualization as described here.

A fifth class of related work concerns earlier work on privacy visualization by this author. Yee [12] presents a notation for representing the software and hardware components of a computer system as well as the data flows between the components. It then checks each component for vulnerabilities that could violate a privacy policy. It differs from this work in terms of the notation (lower level than this work), the method of identifying vulnerabilities, and the use of privacy policies. Yee [13] featured the first use of the PIM but for web services only and involved privacy policies. In this work, we have extended the PIM to software systems in general and removed the need to work with privacy policies.

Finally, there remains a class of related work that also involves visualization of risks but with different goals than in this work. They are works on the visualization of information intended to assist the decision making process under risk or improve the understanding of system security and risks. They differ from this work as follows: a) they concern the visualization of *security* risks rather than privacy risks, b) their goals are to assist in decision making or improve security understanding, whereas the goal of this work is to identify privacy vulnerabilities, and c) their visualizations are lower level in general and resemble more the objects being visualized, whereas this work uses a high level more abstract visualization. Three works representative of this class are Daradkeh [14], Takahashi et al. [15], and Kai et al. [16]. Daradkeh evaluates an information visualization tool for the support of decision making under uncertainty and risk. Takahashi et al. discuss the architecture of a tool for security risk visualization and alerting to increase security awareness. Kai et al. present a security visualization system for cloud computing that displays security levels computed over information gathered at monitoring points. Their visualization system is similar to visualizations provided by a security information and event management system (SIEM) [17].

V. CONCLUSION AND FUTURE WORK

This work has proposed a straightforward method for visualizing privacy risks applicable to software systems, focusing attention on locations involving PII. Although the likelihood of a risk being realized is not covered, identifying the risks is a necessary first step.

Some of the strengths of the method include: a) provides a structured way to identify privacy risks, b) easy-to-use graphical notation, and c) focuses attention on the locations that involve PII.

Some weaknesses of the method are: a) drawing the PIM and filling out the Privacy Risks Table require expertise in how personal information is used as well as expertise in security and privacy, b) the method is manual and is prone to error, and c) the method can never identify all the risks. Weakness a) is unavoidable as even expert systems must get their expertise from people. Also, this "weakness" is common to many analytical methods, e.g., designing good software. Weakness b) can be addressed by building tools for automatically drawing the PIM. Similar tools already exist for rendering a software architecture diagram from the reverse engineering of code, e.g., Nanthaamornphong et al. [18], and it should be feasible to build a similar tool to draw a PIM. Furthermore, automated analysis of the PIM should be feasible by using a rules engine to automate the enumeration of privacy risks, based on machine understanding of the graphical notation in this work. These automations should improve both the accuracy of the PIM and the identification of the privacy risks. Weakness c) may

 ISBN: 978-1-61208-493-0

also be unavoidable, as it is due to the nature of security, that no system can be completely secure. However, the above automated tools and rules engine should improve risk coverage.

Future work includes the automations mentioned above, as well as a validation of the effectiveness of the approach. For this validation, it is envisioned that a software system with known privacy risks (reference risks), would be defined to act as the reference system. Different teams of privacy and security experts who do not have prior knowledge of the reference risks would then be invited to apply the approach to the reference system. Their results would be compared to the reference risks to gage the effectiveness of the approach. If the risks found by the teams were fewer than the reference risks, then a follow-up analysis could point to the reasons for the discrepancy and could give insight into ways to improve the approach. On the other hand, if the risks found were more than the reference risks, then it may be concluded that the approach is highly effective.

REFERENCES

[1] V. S. Iyengar, "Transforming Data to Satisfy Privacy Constraints", Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'02), Edmonton, Alberta, pp. 279-288, 2002.

[2] R. Song, L. Korba, and G. Yee, "Pseudonym Technology for E-Services", chapter in Privacy Protection for E-Services, edited by G. Yee, Idea Group, Inc., 2006.

[3] C. Adams and K. Barbieri, "Privacy Enforcement in E-Services Environments", chapter in Privacy Protection for E-Services, edited by G. Yee, Idea Group, Inc., 2006.

[4] Treasury Board of Canada Secretariat, "Directive on Privacy Impact Assessment", available as of March 27, 2016 from: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308

[5] I. Goldberg, D. Wagner, and E. Brewer, "Privacy-Enhancing Technologies for the Internet", IEEE COMPCON'97, pp. 103-109, 1997.

[6] G. Yee, L. Korba, and R. Song, "Legislative Bases for Personal Privacy Policy Specification", chapter in Privacy Protection for E-Services, edited by G. Yee, Idea Group, Inc., 2006.

[7] J. I. Hong, J. D. Ng, S. Lederer, and J. A. Landay, "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems", Proceedings, 2004 Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, Cambridge, MA, USA, pp. 91-100, 2004.

[8] J. Biega, I. Mele, and G. Weikum, "Probabilistic Prediction of Privacy Risks in User Search Histories", Proceedings of the 1st International Workshop on Privacy and Security of Big Data, pp. 29-36, Nov. 2014.

[9] E. Paintsil, "A Model for Privacy and Security Risks Analysis", Proceedings of the 5th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-8, May 2012.

[10] G. Das and N. Zhang, "Privacy Risks in Health Databases From Aggregate Disclosure", Proceedings of the 2nd ACM International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'09), article no. 74, June 2009.

[11] A. Nematzadeh and L. J. Camp, "Threat Analysis of Online Health Information System", Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'10), article no. 31, June 2010.

[12] G. Yee, "Visualization for Privacy Compliance", Proceedings of the 3rd International Workshop on Visualization for Computer Security (VizSEC'06), pp. 117-122, Nov. 2006.

[13] G. Yee, "Visual Analysis of Privacy Risks in Web Services", Proceedings of the IEEE International Conference on Web Services (ICWS 2007), pp. 671-678, July 2007.

[14] M. Daradkeh, "Exploring the Use of an Information Visualization Tool for Decision Support under Uncertainty and Risk", Proceedings of the International Conference on Engineering & MIS 2015 (ICEMIS'15), article no. 41, 2015.

[15] T. Takahashi, K. Emura, A. Kanaoka, S. Matsuo, and T. Minowa, "Risk Visualization and Alerting System: Architecture and Proof-of-Concept Implementation", Proceedings of the First International Workshop on Security in Embedded Systems and Smartphones (SESP'13)", pp. 3-10, 2013.

[16] S. Kai, T. Shigemoto, T. Kito, S. Takemoto, and T. Kaji, "Development of Qualification of Security Status Suitable for Cloud Computing System", Proceedings of the 4th International Workshop on Security Measurements and Metrics (MetriSec'12), pp. 17-24, 2012.

[17] Wikipedia, "Security information and event management", available as of June 12, 2016 from: https://en.wikipedia.org/wiki/Security_information_and_event_management

[18] A. Nanthaamornphong, K. Morris, and S. Filippone, "Extracting UML Class Diagrams from Object-Oriented Fortran: ForUML", Proceedings of the 1st International Workshop on Software Engineering for High Performance Computing in Computational Science and Engineering (SE-HPCCSE'13), pp. 9-16, 2013.

 ISBN: 978-1-61208-493-0