Grant Agreement Number: **248113/O70**

Project acronym: **IoTSec**

Project full title:

Security in IoT for Smart Grids

D 0.5
Scientific Paper

Due delivery date: M12

Actual delivery date: M12

Organization name of lead participant for this deliverable:

UNIK

Dissemination level		
PU	Public	**X**
RE	Restricted to a group specified by the consortium	
CO	Confidential, only for members of the consortium	

Deliverable number:	D 0.5
Deliverable responsible:	UNIK
Work package:	WP0
Editor(s):	Seraj Fayyad

Author(s)	
Name	**Organisation**
Josef Noll	UiO
Seraj Fayyad	UNIK

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V01	22.09.2016	Final version	Seraj Fayyad

1 ABSTRACT

This deliverable presents one of the scientific papers of IoTSec. Internet of Things, People and Services (IoTPS) systems have become increasingly popular in modern times. And this popularity increases the importance of measurable Security, Privacy, and Dependability (SPD). One of the crucial aspects for system SPD enhancement is reliable evaluation for system SPD level. The evaluation of SPD level for IoTPS system has many challenges, such as the heterogeneity among the components. Considering the challenges of IoTPS system, several approaches are proposed to evaluate system SPD level. One of these approaches, is Multi Metrics (MM) approach. This approach is considered as comprehensive approach, because of its features. Some of MM approach features target the scalability and applicability within the architecture of unlike systems. To enhance the comprehensiveness of MM approach, we propose an extension for the approach to consider the impact of components interconnection on SPD level.

The information on the paper is available at IoTSec.no/publications,

1. S.Fayyad and J.Noll. "Components Interconnection Consideration In Multi Metrics Approach", CENTRIC 2015, pp 21-27, ISBN: 978-1-61208-440-4

2 CONCLUSIONS

This paper considers systems of systems in the Internet of People, Things and Services (IoPTS). It provides an extension of the Multi Metrics approach including interconnections of components in the system. The Multi Metrics (MM) approach assesses the security, privacy and dependability (SPD) triplet of a component, a sub-system and the total system.

The specific use case analysed is the privacy analysis of a medical system for diabetes measurements. The system consists of a glucometer interacting with a mobile device over Bluetooth, and a host application for mointoring of the application. The example is based on two metrics, authentication and encryption, being applied both for the application and the mobile operating system. The result of applying the MM method leads to privacy levels of the system, providing a privacy level between 40 and 70 for the application.

The proposed extension considers interconnections between components. In the envisaged use case, the interconnection is explicitly dominant for the mobile operating system (OS). The OS is surrounded by 4 components, and has 6 reachable components. The analysis using the interconnection extensionof the MM approach leads to a reduced privacy level being between 28 and 50 for the Mobile OS.

Components Interconnection Consideration In Multi Metrics Approach

Seraj Fayyad

University of Oslo/UNIK
Oslo, Norway
Email: seraj@unik.no

Josef Noll

University of Oslo/UNIK
Oslo, Norway
Email: josef@unik.no

***Abstract*—Internet of Things, People and Services (IoTPS) systems have become increasingly popular in modern times. And this popularity increases the importance of measurable Security, Privacy, and Dependability (SPD). One of the crucial aspects for system SPD enhancement is reliable evaluation for system SPD level. The evaluation of SPD level for IoTPS system has many challenges, such as the heterogeneity among the components. Considering the challenges of IoTPS system, several approaches are proposed to evaluate system SPD level. One of these approaches, is Multi Metrics (MM) approach. This approach is considered as comprehensive approach, because of its features. Some of MM approach features target the scalability and applicability within the architecture of unlike systems. To enhance the comprehensiveness of MM approach, we propose an extension for the approach to consider the impact of components interconnection on SPD level.**

***Index Terms*—components interconnection; interconnection weighting equation; mHealth system; IoTPS; Multi-Metrics; security level; privacy level; dependability level.**

I. Introduction

Internet is transforming from communication highway between computers into a backend system connecting hybrid networks. Within these hybrid networks, people, services, things (sensors, actuators) and computers are connected as one. A good example for IoTPS systems is smart grid system, which consists of diversity subsystems. The interaction of Subsystems provides powerful services, such as grid monitoring and remote controlling.

Another kind of IoTPS systems is mHealth systems. This type of system defined by Adibi as the practice of eHealth assisted by smartphones, which are used to capture, analyze, process, and transmit health-based information from sensors and other biomedical systems [1]. Some of provided services by this kind of systems are regular monitoring, real time advising, auto-notification in emergency cases and also affection of emotional states as stated by Cipresso et al. [2].

Eloff et al. envisaged that an IoTPS system will require focus on security and privacy [3]. Despite of many advantages of IoTPS systems, these systems arise new security, privacy and dependability concerns. One of these concerns, is the heterogeneity among subsystems, which complicates system SPD evaluation and satisfaction. Another concern, is the new open area for exploitation of the system, such as the mobile of the patient in mHealth systems.

Garitano et al. propose a Multi Metrics (MM) approach, being a comprehensive and dynamic approach for the evaluation of SPD level for a given IoTPS system [4]. They demonstrate the MM approach applicability by performing it on the smart vehicle IoTPS system. Noll et al. demonstrate more features of the MM approach, such as applicability on huge IoTPS system (e.g smart grid) and scalability [5].

This paper enhances the MM approach, by considering the impact of interconnection on the SPD level. The paper is organized as follows: In Section II, we give an overview of related work. In Section III, we elaborate the proposed extension for MM approach. In Section IV, we demonstrate proposed extension, by applying it on mHealth system as use case. In Section V, we present our conclusion.

II. Related work

Different approaches have been developed for analyzing of IT system risks. Based on the envisaged focus, Manadhata and Wing classified these approaches into attacker-centric approaches and design or system-centric approaches [6].

Attacker-centric approaches, are based mainly on the knowledge about the system attacks. Usually, these approaches collect and analyze attacks-related data, such as; system vulnerabilities, goals of system attackers and detected malicious activities. For the collection of attacks-related data different resources could be used, such as; Intrusion Detection System (IDS) and National Vulnerabilities Database (NVD) [7]. Based on collected data, these approaches build system-attacks model, to analyze the risks of IT system.

The most popular attack models are: attack graph [2], [8], attack trees [9] and Bayesian network [10]. Wang et al. propose an attack graph-based probabilistic model, to quantify the security of IT system network [11], [12]. Wang et al. propose attack graph analysis to be used as a knowledge base for correlating IDS received Alerts, hypothesizing missing alerts, and predicting future alerts [13]. Xie et al. use Bayesian networks incorporated with IDS alerts to analyze the security risks of the IT system [10]. Schneier proposes the analysis

 ISBN: 978-1-61208-440-4

of system risks using knowledge about attackers coupled with attack trees [14]. Dantu et al. propose the usage of attack graph coupled with the behavior of attacker to analyze the risks of IT system [15].

System-centric approaches concentrate on system design and architecture for risk analysis. Manadhata and Wing propose methodology for software system's attack surface measurement [6]. The concept of proposed methodology considers attack surface comparable to system security level (the smaller the surface, the more secure the system)

Howard et al. propose attackability metric to measure system security level, through the measurement of system attack surface from three dimensions [16]. These dimensions are: targets and enablers, channels and protocols, and access rights. Howard et al. refer to the increasing of attack surface and reduction of security level, caused by increasing of targets, channels, and generosity of access rights.

Garitano et al. propose MM approach for the evaluation of SPD level for a given IoTPS system [4]. One of the important MM approach features is the comprehensiveness. It starts with component evaluation, then sub-systems evaluation and ends up with the entire system evaluation. Garitano et al. demonstrate that, different configurations cause different SPD level. Which demonstrate the possibility for SPD level enhancement, through changes in system configurations. Noll et al. demonstrate the scalality and applicability of MM approach, by applying it on large and complex system, such as smart grid [5].

Interconnection has a general impact on system SPD and component SPD, in particular. For instance, a successful attack on the monitoring compontent of a smart vehicle will exploit the privacy of the vehicle rider. Fayyad and Noll state some examples, which reflect the impact of interconnection on the SPD level [17]. The evaluation of the MM approach was not sensitive to interconnection, thus the failure of components with high interconnection is not appropriately considered. In this paper, we introduce an extension for MM approach, which addresses interconnection impacts. We demonstrate proposed extension by applying it on mHealth system. Which shows, that similar SPD level for a given components could vary based on the interconnection of these components.

III. Multi Metrics APPROACH extension

A. Multi Metrics Approach

The MM approach is system-centric approach for the evaluation of SPD level for a given system. As Garitano et al. [4] and Noll et al. [5] have given comprehensive overviews on the MM approach, this paper concentrates on the effect of interconnections of components.

A security evaluation using the MM approach assumes a hierachical architecture for the system of systems. As shown in Figure 1; the evaluation starts at component level, then evaluates the subsystem and finally addresses the entire system, resulting in a system SPD level.

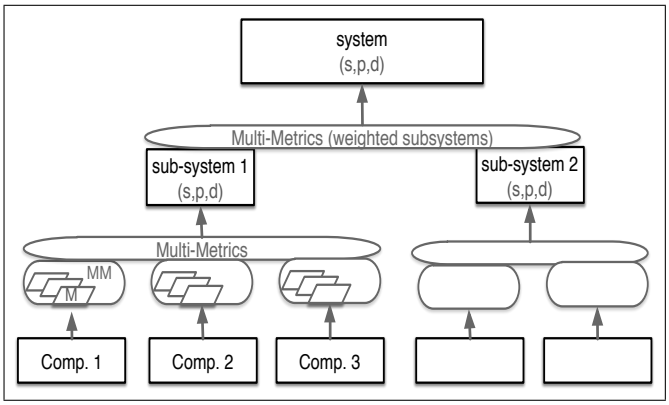

Fig. 1. MM evaluation hierarchical levels, with M indicating a Metrics analysis

In the MM evaluation, the SPD level for an evaluated entity is represented as a triple (S, P, D). Each element of the triple should be described by a value range from 0 to 100. Although, the evaluation ends up with SPD level, SPD criticality is used during the whole evaluation process. From a technological point of view, criticality of a system or a component is more easy to address. SPD criticalities or (Criticality of Security, Criticality of Privacy, and Criticality of Dependibility) (Cs, Cp, Cd) reflect the operation condition like ideal, good, acceptable, or failure. SPD criticalities are defined as complement to SPD triple,

$$(Cs, Cp, Cd) = (100, 100, 100) - (S, P, D). \quad (1)$$

At the components level, the SPD level for a given component is evaluated using a set of metrics. The identification of metrics is performed based on the expected impact of components on a given service. At a later stage, we foresee a framework of metrics being used for evaluations following the MM approach. The final goal is an integrated evaluation for a system, consisting of sub-systems and components.

The MM approach combines the sub-systems using Root Mean Square Weighted Data (RMSWD)(2). The RMSWD formula consists of two parameters, a weight parameter w and a criticality parameter x. Parameters values are within the (0-100) range. In the MM approach, the weight parameter represents the significance of the component or a subsystem on the behaviour of the total system. The criticality parameter represents the operation condition of a component of a subsystem, being e.g. ideal, good, critical or failure.

$$C = \sqrt{\sum_i \left(\frac{x_i^2 w_i}{\sum_i^n w_i} \right)} \quad (2)$$

To summarize the MM approach; the evaluations of metrics for a component are integrated to find the criticality of a component, expressed in terms of security, privacy and dependability. Later, the SPD criticalities of components for a subsystem are integrated using RMSWD and result in a subsystem SPD criticality. Lastly, SPD criticalities of subsystems are integrated

 ISBN: 978-1-61208-440-4

using RMSWD to produce the criticality of a system. The (S, P, D) of a system is then calculated using equation (1).

B. Interconnection Consideration and Positioning

Component interconnection causes reduced security, privacy or dependability, as the failure of one component will not only affects the respective sub-systems, but all sub-systems connected to the component. Let us consider the case of three components (A, B, C) and their interactions. For instance, a body sensor C, which send data to mobile application A, over a Bluetooth connection B. Successful attack on A authentication could enable attacker to reveal the transmitted data confidentiality over B, although it is fully confidential during transmission. Also, a successful attack on A authentication, could enable attackers to inject some malicious scripts, impacting the transmission protocol, which make B or C unavailable. Thus, the SPD of component A impacts the SPD of components B and C and vise versa.

To consider the impact of interconnection on SPD levels, we propose a default metric for interconnection evaluation. The proposed metric is positioned on a level between component and subsystem in MM architecture. Figure 2 shows the proposed positioning of interconnection metric as part of the MM approach.

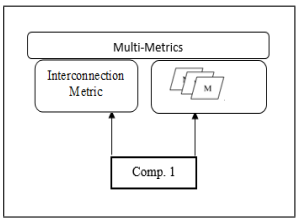

Fig. 2. Interconnection metric positioning within MM

The reason of positioning the interconnection metric in a higher level is, that interconnections impact all components and their SPD parameters. Thus, the evaluation of interconnection for a given component is integrated with component SPD level, where, Formula (2) is used as integration operator.

C. Interconnection Metric

Fayyad and Noll consider system, as a set of interconnected components interact through message passing and/or controlling [17]. Based on this consideration, Fayyad and Noll define an interconnection graph for system components (Definition 1), which model the interconnection and interaction of system components.

Definition 1: Given a set of Components C, having a set of control relations, $Rc \subseteq C \times C$, and a set of data relation $Rd \subseteq C \times C$, then the components interconnection graph G is the directed graph $G(C, Rc \cup Rd)$ (C is the vertices set and $Rc \cup Rd$ the edge set).

Directed graph meant, that the relations or edges between components have a direction associated with them. This direction could be in two way or one way, such as relation between control unit and actuator, which has one way direction from control unit to actuator.

By analyzing of interconnection graph for system components, Fayyad and Noll propose interconnection-based weighting algorithm [17]. The proposed algorithm ends up with a weighting equation (3), which weights the interconnection for specific component.

$$W(c) = S + R + 2C_T + D + A + (\sum_{v=0} \frac{1}{DIST(c,v)}) + V_R \quad (3)$$

- c: targeted component for weighting, where $c \in C$ and C, is set of all components in the system.
- R: number of sub/system components reachable from weighted component c.
- S: number of components reachable from weighted component c through one edge within system interconnection graph. In other words, surrounded component for component c is a component, which interact directly with c without any intermediate component.
- V_R: number of system valuable or key components, reachable from c.
- C_T: number of control relation or edges between weighted component c and other system components.
- D: number of data relation between weighted component c and other system components.
- A: component c activation rate.
- v: valuable component within the system.
- $DIST$: number of components between c and v components.

Activation rate is considered as the frequency of component activation per time unit. Where, activation rate value ranges from 0 to 1. The higher the value the more active the component. Thus, 0 is when, the component is totally inactive, and 1 when, the component is continuously active. When the component is not active, the SPD level of the component does not impact the SPD levels of interconnected components. On other hand, if component is continuously active, then, its SPD level is continuously impacts the SPD level of interconnected components. This mean, activation rate for a given component influences the impact of other parameters in equation (4) on the SPD level of interconnected components. Thus, we propose new optimization for equation (3) for the use in proposed extension. The optimization is represented in equation (4), in which, activation rate is considered as multiplication factor, instead of summation factors. Interconnection metric based on equation (4) to measure interconnection weight for a given component.

$$W(c) = A(S + R + 2C_T + D + (\sum_{v=0} \frac{1}{DIST(c,v)}) + V_R) \quad (4)$$

Based on the need, for equal evaluation of components activation rate, evaluation rate for all components should be evaluated to the same time unit. Thus, a system engineer should evaluate activation rate of component to the smallest time unit. For instance, Let us consider the case of a system

 ISBN: 978-1-61208-440-4

with two components $c1$ and $c2$. $c1$ activation rate is $60/h$ and $c2$ activation rate is $5/min$. For equal interconnection evaluation, activation rate for $c1$ should be used as $1/min$ and for $c2$ as $5/min$.

D. Interconnection Metric Calibration

In MM approach, the SPD level for a given component is represented with a value range from 0 to 100. On the other hand, interconnection metric based on equation (4) resulted value, could vary based on system architect out of (0 to 100) range. Thus, for the integration of the result from interconnection metric with component SPD level, equation (4) result should be calibrated to (0 to 100) range.

To calibrate equation (4) resulted value to (0-100) range, we define architecture-based reference value, as representing maximum weight of interconnection for a component within given system. Let us consider m as a component within given system, and its interconnection weight is the maximum weight. Then, the values of its parameters in equation (4) will be as follow:

- A = 1.
- R = number of all system components(max number of components reachable from m).
- S = number of all system components(max number of components surrounded m).
- C_T = number of all control edges within system interconnection graph.
- D = number of all data edges within system interconnection graph.
- V_R = number of all valuable components within the system.

By having maximum weight of interconnection, the weight of component 'c' could be calibrated to (0-100) range, as shown in equation (5).

$$Weight_c(c) = \frac{Weight(c)}{Weight(m)} \quad (5)$$

Where:
c: given component within the system.
m: most interconnected component within the system.
$Weight_c(c)$: calibrated weight for a value within (0 - 100).
$Weight(c)$: component evaluated weight using equation (4).
$Weight(m)$: system maximum weight of interconnection.

IV. USE CASE

This section demonstrates the proposed extension for MM approach, using the evaluation of Privacy level SPD_p as one of the SPD triple for two selected components. At the start, it gives an overview about Gravid+ system. subsequently, it performs high level analysis for Gravid+ system based on MM approach with concentration on two components. Later, it measures the interconnection of the two components using interconnection metric. Lastly, it evaluates SPD_p level for the two components under different configurations based on MM approach and proposed extension.

A. Gravid+ System:

Gravid+ system elaborated by Garnweidner et al. aims to monitor blood sugar levels in pregnant women with gestational diabetes and assists them with follow up care, such as; diet and exercise [18]. The architecture of Gravid+ system shown in Figure 3 consists mainly of glucometer device interacts with mobile device over Bluetooth connection. The mobile device, host mobile app, which processes and saves glucometer submitted measurements.

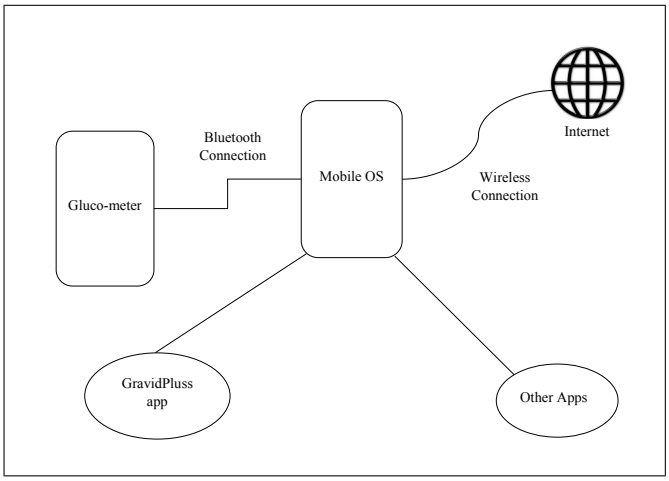

Fig. 3. Gravid+ architecture.

Sub/systems or components, such as other mobile apps hosted on the patient mobile may impact the SPD level of the system, although its not apart of the system. For instance, from privacy perspective, through internet, an attacker could violate one of the mobile apps vulnerabilities and gain access to mobile device. By gaining access to the mobile device, the attacker could violate Gravid+ data confidentiality. Thus, for the analysis of system SPD level, all sub/systems impact the SPD level of the system should be included in analysis.

B. System Components and Metrics

To simplify the demonstration of proposed extension for MM approach, we apply high-level analysis of Gravid+ system. In this analysis, each illustrated nodes within Figure 3 is considered as component. For each of these components a set of metrics are defined as shown in table I. To concentrate on the impact of proposed extension on SPD level, we concentrate on two components (Mobile OS and Gravid+ app), which have different interconnection within Gravid+ system. Where, we assume the performing of similar metrics (authentication and encryption) on the two components,

The analysis of the two components considering SPD_p only. As already stated, MM approach concludes with the SPD level, but SPD criticality is used during the entire evaluation process, as it is shown within tables II to V. The metrics which used in the analysis are:

- Gravid+ app metrics

TABLE I. SYSTEM COMPONENT MAXIMUM POSSIBLE WEIGHT.

Component	*Metrics*
Glucometer	Authentication pairing metric
Bluetooth connection	Encryption metric
Mobile device OS	Encryption metric, Authentication metric
Other apps	number of apps metric
Gravid+ app	Encryption metric, Authentication metric

– Authentication metric(w=40): evaluates the Cp resulted from authentication activation by accessing of Gravid+ app or not (Evaluation is shown in Table II).

TABLE II. GRAVID+ APP AUTHENTICATION METRIC.

Parameters	*Authentication ON*	*Authentication OFF*
Cp	30	70

– Encryption metric (w=30): evaluates the Cp resulted from having App data ciphered or not (evaluation is shown in Table III).

TABLE III. GRAVID+ APP ENCRYPTION METRIC.

Parameters	*Encryption ON*	*Encryption OFF*
Cp	10	60

- Mobile OS metrics
  – Authentication metric(w=40): evaluates the Cp resulted from having authentication activated to access the mobile device or not (evaluation is shown in Table IV).

TABLE IV. MOBILE OS AUTHENTICATION METRIC.

Parameters	*Authentication ON*	*Authentication OFF*
Cp	30	70

– Encryption metric(w=30): evaluates Cp of having data ciphered by Mobile OS or not, using service, such as $encryptdevice$ service in Android OS. One of such service benefits is data protection from offline revealing. (evaluation is shown in Table V)

C. Performing of Interconnection Metrics

To weight the interconnection for a component, using equation (4), the interconnection graph for system components should be initiated. Based on this graph, the values of parameters in equation (4) are driven. Figure 4 shows initiated interconnection graph for Gravid+ system.

Based on the interconnection graph of Gravid+ system, values of interconnection parameters for mobile OS are driven. (shown in Table VI), based on these values, interconnection weight of mobile OS is 23.5.

Parameters of Gravid+ app and their values, are shown in Table VII, based on these values, interconnection weight of Gravid+ app is 12.

TABLE V. MOBILE OS ENCRYPTION METRIC.

Parameters	*Encryption ON*	*Encryption OFF*
Cp	10	60

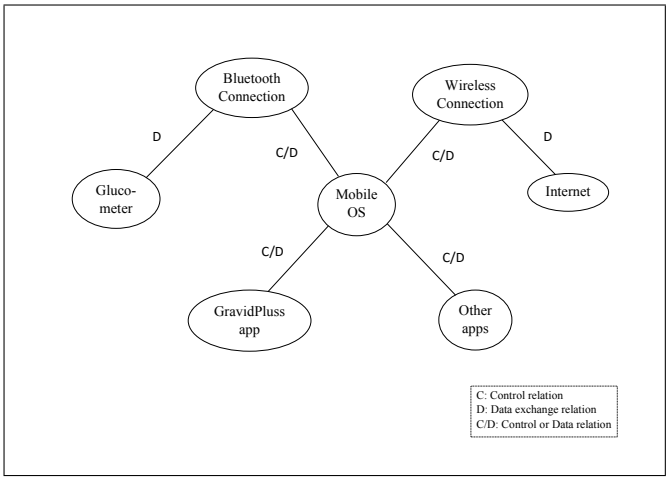

Fig. 4. Gravid+ interconnection graph.

For the calibration of $Weight(c)$ for a given component 'c', system maximum weight of interconnection should be calculated. Table VIII shows parameters of maximum weight and their values in Gravid+ system, based on these values, maximum weight is 28.

By performing equation (5), mobile OS $Weight_c$ is 84 and Gravid+ app $Weight_c$ is 43.

D. Evaluation

Table IX and table X respectively show the evaluation of Gravid+ app Cp and mobile OS Cp under different configurations. $Cp1$ represents the evaluation of configurations based on MM approach. $Cp2$ represents the evaluation of con-

TABLE VI. MOBILE OS INTERCONNECTION PARAMETERS.

Parameters	*Value*	*Note*
S	4	Mobile OS surrounded by 4 components
R	6	Mobile OS has 6 reachable component
V_R	1	Valuable component is only Gravid+ app
C_T	4	Mobile OS has 4 control relations or edges
D	4	Mobile OS receives and sends data from/to 4 components
A	1	Assumption it is continuously active
DIST	2	The distance to the (Gravid + app) is 2 two components (Mobile OS, Gravid+ app)

TABLE VII. GRAVID+ APP INTERCONNECTION PARAMETERS.

Parameters	*Value*	*Note*
S	1	Gravid+ app surrounded by Mobile OS
R	6	Gravid+ app has 6 reachable component
V_R	1	The component is Valuable itself
C_T	1	has one control relation with Mobile OS
D	1	Gravid+ app receives and sends data through Mobile OS
A	1	Assumption it is continuously active
$DIST$	1	Min distance to the app itself

TABLE VIII. SYSTEM COMPONENT MAXIMUM POSSIBLE WEIGHT.

Parameters	*Value*	*Note*
S	6	Supposing that all system components within system surround objective component
R	6	Reachable component in two way from objective component.
V_R	1	Valuable component is only Gravid+ app
C_T	4	Number of control edges within, interconnection graph are 4 .
D	6	Number of data edges within, interconnection graph .
A	1	Component is continuously active
$DIST$	1	Component is valuable by itself

figurations based on MM approach enhanced with proposed extension. Thus, $Cp2$ values resulted from the integration of $Cp1$ with the output of interconnection metric for the component ($Weight_c$). Where, for the two components, the weight of interconnection metric is considered as 30, and the weight of component ($Cp1$) as 70.

TABLE IX. GRAVID+ APP EVALUATION

Encrypt-/Auth-	*M1*	*M2*	*Cp1*	*Cp2*	P_L
Conf.(ON,ON)	10	30	24	31	69
Conf.(ON,OFF)	10	70	53	50	50
Conf.(OFF,ON)	60	30	45	44	66
Conf.(OFF,OFF)	60	70	66	60	40

TABLE X. MOBILE OS EVALUATION

Encrypt-/Auth-	*M1*	*M2*	*Cp1*	*Cp2*	P_L
Conf.(ON,ON)	10	30	24	50	50
Conf.(ON,OFF)	10	70	53	64	36
Conf.(OFF,ON)	60	30	45	59	41
Conf.(OFF,OFF)	60	70	66	72	28

As shown in Table IX and Table X, the $Cp1$ results, of an evaluation of two components lead to the same value. On other hand, $Cp2$ are differentiated based on the interconnections of each components. Thus, the SPD_p will differ. This lead to system SPD level differentiation based on internal interconnection of this system.

V. CONCLUSION

This paper considers systems of systems in the Internet of People, Things and Services (IoPTS). It provides an extension of the Multi Metrics approach including interconnections of components in the system. The Multi Metrics (MM) approach assesses the security, privacy and dependability (SPD) triplet of a component, a sub-system and the total system.

The specific use case analysed is the privacy analysis of a medical system for diabetes measurements. The system consists of a glucometer interacting with a mobile device over Bluetooth, and a host application for mointoring of the application. The example is based on two metrics, authentication and encryption, being applied both for the application and the mobile operating system. The result of applying the MM method leads to privacy levels of the system, providing a privacy level between 40 and 70 for the application.

The proposed extension considers interconnections between components. In the envisaged use case, the interconnection is explicitly dominant for the mobile operating system (OS). The OS is surrounded by 4 components, and has 6 reachable components. The analysis using the interconnection extension of the MM approach leads to a reduced privacy level being between 28 and 50 for the Mobile OS.

VI. ACKNOWLEDGMENT

The authors would like to thanks the JU Artemis nSHIELD project for the development of the methodology, and the use cases showing the applicability of the approach. We would also like to thank Movation and the Research Council of Norway for enabling and supporting the PhD work.

REFERENCES

[1] S. Adibi, Ed., *Mobile health*. Springer, 2015, ISBN:9783319128160.
[2] P. Cipresso, S. Serino, D. Villani, C. Repetto, L. Sellitti, G. Albani, A. Mauro, A. Gaggioli, and G. Riva, "Is your phone so smart to affect your state? An exploratory study based on psychophysiological measures," *Neurocomputing*, vol. 84, pp. 23–30, 2012.
[3] J. Eloff, M. Eloff, M. Dlamini, and M. Zielinski, "Internet of People , Things and Services - The Convergence of Security, Trust and Privacy," *Proceedings of the third International CompanionAble Workshop IoPTS, Brussels*, 2009.
[4] I. Garitano, S. Fayyad, and J. Noll, "Multi-metrics approach for security, privacy and dependability in embedded systems," *Wireless Personal Communications*, vol. 81, no. 4, pp. 1359–1376, 2015.
[5] J. Noll, I. Garitano, S. Fayyad, E. Åsberg, and H. Abie, "Measurable Security, Privacy and Dependability in Smart Grids," *Journal of Cyber Security and Mobility*, vol. 3, no. 4, pp. 371–398, 2015.
[6] P. K. Manadhata and J. M. Wing, "An attack surface metric," *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371–386, 2011.
[7] "National Vulnerability Data Base," 2015, URL: https://nvd.nist.gov/ [accessed: 2015-09-21].
[8] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 217–224, 2002.
[9] J. Dawkins, C. Campbell, and J. Hale, "Modeling network attacks: Extending the attack tree paradigm," *Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection*, pp. 75–86, 2002.
[10] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using bayesian networks for cyber security analysis," *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, pp. 211–220, 2010.
[11] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, "An attack graph-based probabilistic security metric," *Data and applications security XXII*, pp. 283–296, 2008.
[12] L. Wang, A. Singhal, and S. Jajodia, "Measuring the overall security of network configurations using attack graphs," *Proceedings of the 21st annual IFIP WG 11.3 working conference on Data and applications security*, pp. 98–112, 2007.
[13] L. Wang, A. Liu, and S. Jajodia, "Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts," *Computer communications*, vol. 29, no. 15, pp. 2917–2933, 2006.
[14] B. Schneier, "Attack trees," *Dr. Dobb's journal*, vol. 24, no. 12, pp. 21–29, 1999.
[15] R. Dantu, K. Loper, and P. Kolan, "Risk management using behavior based attack graphs," *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, vol. 1, pp. 445–449, 2004.
[16] M. Howard, J. Pincus, and J. M. Wing, Eds., *Measuring relative attack surfaces*. Springer, 2005, pages:112-140.
[17] S. Fayyad and J. Noll, "Security and Safety Composition Methodology," *CENTRIC 2014*, pp. 60–65, 2014.
[18] L. Garnweidner, I. Borgen, I. n. Garitano, J. Noll, and M. Lukasse, "Designing and Developing a Mobile Smartphone Application for Women with Gestational Diabetes Mellitus Followed-Up at Diabetes Outpatient Clinics in Norway," *Healthcare*, vol. 3, no. 2, pp. 310–323, 2015.

 ISBN: 978-1-61208-440-4