UNIK4750 - Project Assignment: A Smart Home for Elders

Contents

1 Preface

2 Abstract

Traditionally the security, privacy and dependability (SPD) of a system has been included to the system as an add-on feature. As a result, the system will become highly vulnerable to attacks. In this report we will show a method to integrate the security and privacy into the development of a system. The usage of the method will be shown by using it in the development of a smart home system for elders. The system monitors the health status of patients by continuously analyzing their movement and breathing patterns within their home premises. Radar sensors are used to detect a patient's motion and breathing pattern. In case of any unusal motion or breathing patterns, emergency procedures are initiated. The method have several steps, which are making scenarios and configurations for the system, and having metrics for the system's components with weights. The last step and the core idea of the method is using a multi-metric approach to get security and privacy values in order to compare them to the goals of security and privacy in a system. This way it is possible to find parts of the system which need changes to meet the goals of security and privacy. We will have a short evaluation of the method in the end of the report, explaining why it is a good method and what we consider as weaknesses.

3 Introduction

In this project we will go through a method to add the system security and privacy during the design in order to create a secure and privacy-aware system, which makes the system less vulnerable. We will not go through the dependability aspects as it is not a part of this project. We will then show a use case of how to do the method.

The method is used in order to find the SPD values of a system. When evaluating the numbers you are able to see if there are any changes that need to be done to the system in order to be within the range of the SPD goal of the system.

The system we will use in order to show how the method works is a smart home system for elders. There are three sub-systems, one of them is a sensor system that tracks movement in a house. This is the embedded system. Another sub-system consists of the back-end services to the hospital. The third sub-system is the communication between the embedded system and the back-end. These sub-systems have some components that will be described and evaluated with metrics and weights. Multi-metrics are used in order to get the SPD values, which as mentioned will be compared with the SPD goals.

The rest of the paper is structured as following: The methodology we are following will be described in section 4. Section 5 has a description of the system and the subsystems as well as a description the components in the system. A use case and the evaluation of the use case will be shown in section 6. In section 7 we will evaluate the method we use in this paper.

- $|\text{SPD}_{Goal} - \text{SPD level}| = \leq 10$, green.
- $|\text{SPD}_{Goal} - \text{SPD level}| = > 10, \leq 20$, yellow.
- $|\text{SPD}_{Goal} - \text{SPD level}| = > 20$, red.

Figure 1: SPD Visualization

4 Methodology

In this section we will look into the methodology of how to measure the security and privacy level of a system. The dependability level should also be measured, but is not a part of this project. We have used section 3 from the paper given in the lecture for the course UNIK4750, *Multi-Metrics Approach for Security, Privacy and Dependability in Embedded Systems*(1) as a reference.

To measure the security, privacy and dependability of a system, we must get an overall system level which will be called SPD_{System}. Firstly each of the components will be measured in numbers from 0-100. The combination of the components result in the sub-systems. At last the combination of the sub-systems results in system as a whole, which gives us the SPD_{System}. 0 is absolutely no level of SPDs at all, while 100 is the maximum level of SPD which would be hard to come by.

SPD_{System} is a triplet which consist of each of the SPD attributes' level. The criticality of the system is needed in order to get the SPD_{System} level. The criticality is also a triplet and is defined as the complement of SPD. The criticality is expressed like this: *(Cs, Cp, Cd) = (100, 100, 100) - (s, p, d).*

The system will be used in different scenarios. Each scenario has their own SPD_{Goal}, which is the scenario's requirements of the system. Each of the scenarios have different configurations. The configurations of the sub-systems and their components might be different from each other. By comparing all of the configurations in the whole system to each of the scenarios, we will find the configuration that fits the SPD_{Goal} best. E.g. there are three scenarios. Each of the scenarios can have three different configurations. Then a total of nine configurations gets evaluated to find the most suitable configuration.

As mentioned the evaluation starts by evalutating the components, then the sub-system and at last the system as a whole. Between all of these steps there is a Multi-Metric approach. The metrics is used in order to find the criticality of the components. Each component is evaluated through one or more metrics. Then we have the component criticality, *Component(Cs, Cp, Cd).* The result of these metrics will be combined by using Multi-Metrics, which gives us the (sub-)system's criticality values.

The security, privacy and dependability of the system will be evaluated individually throughout the method, but when comparing with the SPD_{Goal}, all of the attributes will be taken into account. An SPD is acceptable when it ends up as green, which is when the absolute value of the SPD_{Goal} subtracted with the SPD-level is less or the same as 10. Yellow is when the absolute value is between 10 and 20, and red is when the value is above 20. These colors are used to simplify the process when choosing acceptable configurations, (shown in figure 1).

5 System Description

This section presents the system we have chosen to analyze for this project. The system is a home care solution for elders. By monitoring the patients or other peoples movements in a house the system will trigger an alarm if there are abnormal movement or breathing patterns. The alarm should notify nurses or the patient's family, or both.

The system consists of three subsystems which again consists of components, see figure 2. The embedded system is a sensor system that uses radar sensors to keep track of the movements of the patient. The back-end system which builds the interface from the home to the end-user. Then there's the communication between the embedded system and the back-end system. These three subsystems will be described in the following subsections.

5.1 Embedded System

We have based the embedded system (ES) on radar sensors called XeThru(2). The radar sensors are used to monitor a patients movements and breathing patterns in his/her house. The sensors send data to a controller which is the decision-making device placed in the patient's house. The ES has mapped the objects, doors and windows in each room of the house. The house is divided into zones in order for the system to categorize which room the patient is positioned in. There is an integrated clock in the radar sensor. The clock is used by the ES to track the period of time the patient spends in each room. The system also has other functions like keeping track of the frequency of visiting the different rooms in the house, which spot in each room the person is positioned in, which time in the day the room is visited. The system knows the patient's normal patterns of all of these functionalities.

In case of any abnormal patterns of the functions an alarm should be triggered. E.g. if the patient is in the bathroom for an hour in the middle of the day there is a big chance the patient fell on the floor and cannot move. The patient might have a seizure or heart attack if breathing suddenly stops or the breathing pattern changes. If someone comes in through the window in the middle of the night, it is most likely that it is a burglar.

The radar sensor is based on impulse radar technology. The radar sends a radio wave that hits an object, which reflects the wave just like an echo. The distance of the object can be calculated by the time the wave uses back and forth. The sensor has low power consumption and can operate in a temperature range of -40 degrees to 85 degrees. The sensors use WiFi to send data to the controller device.

The sensor controller is the decision-making device. It receives signals from the sensors via the router and passes messages to back-end via the router. The controller has a built-in GSM modem for sending SMS-messages. This device decides when and where to alert if an abnormal pattern of movement or breathing has been detected. Whether it uses the WiFi or GSM to communicate depends on the criticality of the situation.

There may be some issues with the sensor system regarding privacy and security. Of course someone might wreck the devices in a physical way. There are small chances of faults that are not a result of humans tampering with the sensors because of the low power consumption and that it can operate in a wide range of temperatures. Of the same reason, we do not consider the devices shutting down a security issue in this project. When using WiFi, eavesdropping may happen. Since the sensors sends waves on a radio frequency, the data can be blocked by spamming the same frequency band. In other words, it is possible to tamper with the data.

5.2 Back-End

This sub-system consists of devices like the mobile phones, computers and laptops which is connected to the hospital or other emergency units. This back-end system builds the interface from the smart home to the end-user. The end-users are nurses with a phone who could be anywhere, a doctor at a computer at the hospital, and a family member of the patient. They get a notice on their mobile phone or on the hospital back-end service.

The communication to the back-end devices is necessary for the doctors, nurses and carers to make sure someone will notice if something happens to one of the patients. The communication to these back-end devices, configurations and encryptions may vary depending on the situations level of importance and the level of security and privacy the nurses at the hospital or the family of the patient wants.

When an alarm is triggered in a smart home, signals will be sent to the hospital alarming the employees, and an SMS is sent to the nurse and a family member. They could be anywhere, not necessarily at the hospital. If the situation is not critical, the signals will warn only the ones at the hospital office so they can take a closer look at the situation from there and find out if the patient needs a medical check. The computers are basically connected to a big red lightbulb and a bell that makes sound when an incident has occurred.

Basically we have two different types of devices, the mobile phone and the computer. These devices use different types of communication and configurations. The mobile phones use SMS and mobile networks, and the computers are connected to the Internet. This will be further explained in the next section about communication between the ES and the BE.

5.3 ES to BE Communication

In order to send the sensors' information regarding patients to the relevant end-users we have used GPRS and SMS as a mode of communication. We are using mobile network to communicate with the back-end monitoring unit.

The security and privacy in the system mainly depend on the sensitivity of data and the communication channels. GPRS is used to send sensor information to the back-end monitoring. We will keep GPRS message rate low to maintain our goal of high privacy. We will not be so strict with the encryption in that case and we will use 64 bit encryption to encrypt the data sent to the back-end. We are not using 3G mobile link despite of knowing that it is more secure because its coverage shrinks in crowded areas.

despite?

Port metric is also very important to analyse in the SPD metrics. There are different configurations for data gathering through simple network management protocol. We also take the GPRS message rate, communication channel, encryption remote access of the ES in consideration to make the multi-metric analysis.

6 Use Case

This section describes a home care use case for a female patient. We will only go through one of the sub-systems in the use case, the embedded system. At first we will go through the scenarios in the use case, secondly we will show the configurations the system may operate in. The components will be evaluated through metrics before calculating the sub-system criticality by using the multi-metric approach. At that point we can compare the results with the SPD_{Goals}.

6.1 Scenarios

The patient suffers from cancer and dementia. She is a widow, so she lives alone in her house. She has a weekly visit from her nurse. When she got diagnosed with cancer, she wanted her two children to make sure she gets taken good care of if something else would happen, and she does not want to be sent to a nursing

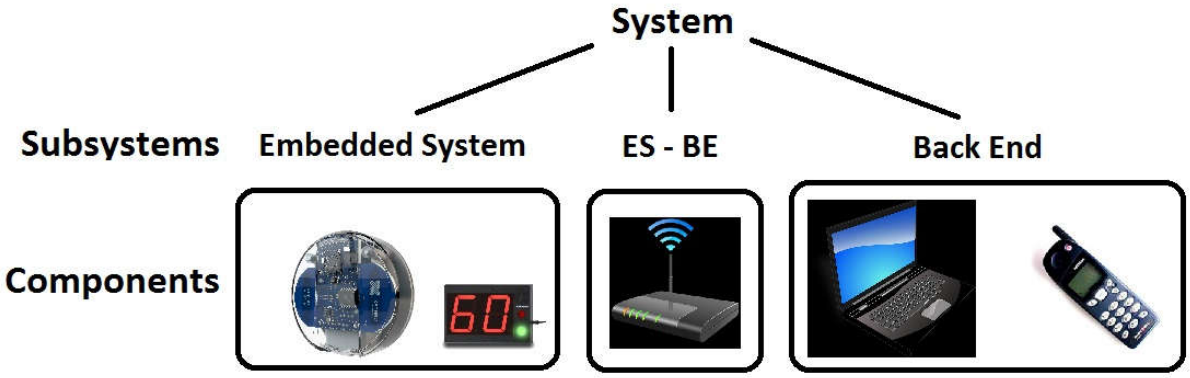

Figure 2: The System

home. Her children decided to go with the solution of having a home care system in her house. They have some requirements for the system, which are these scenarios:

- **Scenario 1:** The patient's family wants full privacy for their loved one as long as everything is fine with her. In order to make sure the system is working, it sends a message to the BE every hour.
- **Scenario 2:** Occurences of abnormal patterns will be informed to the nurses and the patient's doctor at the hospital to their system. The data consists of the time period of the abnormal patterns and data from this time period in order to go through the data. E.g. the patient is positioned on the couch more often and for a longer time period than usually, which might be because the patient is hurt or not feeling well.
- **Scenario 3:** In case of any accidents there is a emergency scenario where an SMS is sent to the nurse, the family and the relevant emergency service. In addition an alarm and relevant information is sent to a backend system. E.g. the patient has not moved from the bathroom for half an hour and the breathing sensor detects abnormal breathing patterns, which might be caused by the patient falling, getting hurt and need to go to the hospital.

The three different scenarios have different privacy and security goals, which we call the SPD_{Goal}. The SPD_{Goal} is compared with the different configurations in order to find the most suitable configurations for the system. The goals and the explanation of the numbers we chose for them are shown below.

- $\mathbf{SPD_{Goal}1 = (55, 80, d)}$. Privacy is more important than the security because information about the patient is sent through WiFi in the house, and high privacy was required from the family. The security value is set to 55 because the security issues are not very critical in this scenario, but confidentiality is needed to meet the requirement. One of the issues is someone blocking the radio frequency would disable the sensors from gathering the data they are supposed to. This would send a notice to the BE, because abnormal data would be detected. The other issue is that someone could collect the data, but they would need to collect data for a long period of time in order for it to be useful. It would probably be easier to look inside the windows to gather the same data.
- $\mathbf{SPD_{Goal}2 = (70, 60, d)}$. Security is more important and has a higher value in this scenario because the sensors are sending abnormal patterns to the hospital back-end system. Encryption of data is

important to prevent the data collection. The patient's information is still going through WiFi in the house, which affect the privacy and confidentiality of the system. Therefore, these values still have to be quite high to meet the family's requirement, but it is also less important than the previous scenario as the patient's information from the sensors need to be sent to the back-end service. Since the information does not need to contain the name or anything to identify the patient or the whereabouts, we can still keep a pretty high privacy goal.

- **$SPD_{Goal}3$ = (75, 10, d)**. In this scenario security is much more important than privacy because it is a life threatening condition. Messages of the patient being hurt must be guaranteed to get delivered to the back-end, which goes under availabilty in security. To be sure it is sent to the right place, the integrity is also considered in this scenario. The information being sent to the back-end needs to have information of the patient's name and whereabouts in order for emergency services to arrive and treat the patient quickly. Because of the situation, the privacy of the information is not being considered and is almost at the lowest value possible. There is still some privacy so that the information is not being collected by anyone. To conclude, the availability and integrity combined with a little confidentiality gives us a high security value in this goal, while the privacy value is low because of the situation.

6.2 Configurations

As we have set up the security and privacy goals based on the scenarios, we will now set up all of the system configurations to fulfill the requirements based on our scenarios. Each scenario has two configurations, so there are a total of six configurations.

- **Conf. A:** No communication between ES and BE. Remote configuration is enabled. WPA2 encryption is used to protect WiFi network from hacking.
- **Conf. B:** ES sends keep-alive messages to BE every 60 seconds. WPA2 encryption is used to prevent hacking of WiFi.
- **Conf. C:** ES observe abnormal patterns and sends data to the hospital back-end service. Data from ES to BE is encrypted with 128 bit key for more security so data cannot be decrypted easily on the internet. ES accept remote configuration from BE. WPA encryption is used to prevent WiFi hacking.
- **Conf. D:** ES sends abnormal patterns information every hour to the BE system at the hospital. Data from ES to BE is encrypted with 128 bit key so data cannot be decrypted easily on the Internet. WPA encryption is used to protect the WiFi network from hacking.
- **Conf. E:** ES detects abnormal motion and breathing patterns. SMS to family members and to emergency services. Remote configuration is required for communication between BE and ES. Data from ES to BE is encrypted with 256 bit encryption. No encryption for WiFi.
- **Conf. F:** ES detects abnormal motion and breathing patterns. A SMS is sent to family members and to emergency services. Data from ES to BE is encrypted with 256 bits for more security. ES sends breathing patterns and motion information every second. No encryption for WiFi.

6.3 Metrics

Now that we have made the configurations, we will select the metrics for each component. The metrics would be the same for any system using the same components. Each of the metrics has their own weight for this system. The weight is a number between 0 and 100 saying how important it is to the system. The metrics

Sensor device metric (radio waves)		
Parameter	Continuously every second	Weight
Cs	50	60
Cp	5	5

Figure 3: Sensor Device Metric

shows a number of the criticality for security and privacy individually. The criticality number is different for different configurations. The higher the number, the more critical. For the message rate metrics, the more messages sent will make a higher number of criticality because there is a higher chance of someone obtaining the data.

6.3.1 Sensor Device Metric

The sensors sends radio waves continuously every second, so the criticality in privacy and security will be the same for all of the configurations. The issue here is that someone might be spamming the same frequency band as the sensor(s) is using. If something happens to the patient at the same time, the availability part of security is not present. An alarm will not be sent, only a notice of abnormal pattern. Since availability is crucial for the sensor in order to have a working system, we set the weight here to 60. The privacy here is not really a big issue because nobody can grab any sensitive or meaningful data from the frequency band, so we set this weight to 5. See figure 3.

6.3.2 WiFi Message Rate Metric

WiFi is used for the communication in the ES. There are two types of WiFi message sending in the ES, the data from the sensors to the controller and the data from the controller to the router (which goes further to the back-end). See figure 4.

Sensor Data to Controller

The messaging from the sensors to the controller happens continuously, so the criticality numbers of privacy and security will be the same for all of the configurations. The system should be available as much as possible, but the chance that the data is in matters of life or death is low and blocking the frequency band would trigger a notice to the BE. Therefore the security weight is set to 20. The privacy is set to 40 and not higher, because for an intruder to get useful data, lots of data needs to be collected and processed. To meet the requirements of the family, the weight cannot be lower.

Controller Data to Router

The messages from the controller to the router happens whenever there are abnormal activities and data is sent to the BE service. The data sent from the controller to the router is important in this case, because we know it is crucial that the data arrives the BE. Therefore availability and integrity is important, and we decided to set the security weight to 60. Privacy issues are not as important as the life and health of the patient in case of an emergency, and the information being sent on a non-emergency scenario does not contain anything to identify the patient, so the privacy weight is set to 15.

WiFi message rate metric

Sensor data to controller

Parameter	Continuously every second	Weight
Cs	40	20
Cp	50	40

Controller data to router (BE)

Parameter (s)	1	2	60	>1h	Not applicable	Weight
Cs	50	45	20	5	0	60
Cp	80	60	25	8	0	15

Figure 4: WiFi Message Rate Metric

Encryption metrics

Parameter	No encryption	WEP	WPA	WPA2	Not applicable	Weight
Cs	70	25	10	5	0	20
Cp	90	30	15	8	0	70

Figure 5: Encryption Metric

6.3.3 Encryption Metric

In the encryption we use WEP, WPA and WPA2. WEP uses a security key in order to secure data transfers. WPA and WPA2 use the same key, but the key changes dynamically. WPA has a higher encryption level than WEP, and WPA2 higher than WPA. The weight of the security is set to 20, while the weight of the privacy is set to 70. This is because of the privacy goals of the system to ensure no information is collected. Encryption for the security is to ensure the messages to be sent to the BE, but in an emergency scenario an SMS is sent aswell. Therefore we do not put much weight on the security for the encryption. See figure 5.

6.3.4 Controller GSM Modem

We set the security weight for data being sent through the GSM modem to 20. This is an incident that only occures if there is an emergency or if the Internet connection is down. The privacy here can be even lower, because life and health is much more important than anything else. So we set this privacy weight to 15. See figure 6.

6.4 Multi-Metrics Approach

The metrics we just showed are used to find the criticality of the sub-system. By getting the right numbers for a configuration from the metrics and their weight, joining them with the multi-metrics approach gives us the SP criticality of the configuration in the sub-system. The mathematical equation used in the multi-metric is shown in figure 7.

SMS message rate metric

Parameter(message)	2	1	0	Weight
Cs	6	3	0	20
Cp	10	5	0	15

Figure 6: SMS Message Rate Metric

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

Figure 7: The RMSWD Formula

Firstly we joined the criticality values for the configurations from metric 3 and metric 4, which is the metrics for the WiFi, by doing the multi-metric approach. Then we did the multi-metric approach with the criticality values of the configurations from the already joined metrics and the criticality values of the configurations from rest of the metrics. This resulted in the criticality values of the sub-system. The SP values are obtained by subtracting the $SP_{Criticality}$ from 100. When the SP values are obtained we can evaluate the system. We have two examples of the comparison of the SP values and the SP Goal. One of them will be described in this subsection, and the other will be described in the next subsection. There are green, yellow and red colors showing how well the numbers of each configuration fits the SP_{Goal}. The function of the colors is described in section 3.

In our first evaluation (see figure 8) we realized that we had misunderstood the encryption of the system, by seeing the red colors and the values for the privacy in scenario 1 and 3. We also could see that the numbers were almost the same for the scenarios. The higher the security goal, the better encryption we added to our system. Even though a system needs encryption for the security attributes confidentality and integrity, this system had really high privacy goals and focuses more on privacy. Since the information being sent in the house is via WiFi from the sensors to the sensor controller and from the controller to the router (and further to the BE), we came to the conclusion that there should have been high encryption when high privacy values are wanted. We changed the encryption in scenario 1 to WPA2 encryption, scenario 2 to WPA and then scenario 3 got no encryption. In this way the encryption fits the privacy goal and also the confidentiality and integrity regarding security. The evaluation ended with a new multi-metric calculation which will be evaluated in the next subsection.

6.5 Evaluation of the ES

Figure 9 shows the second evaluation. By comparing the SP values to the SP_{Goal} we can see that scenario 2 has four configurations that have acceptable values for both security and privacy. Both SP values must be within the acceptable range for the configuration to be acceptable. Scenario 1 have acceptable values for security, but none for privacy, and scenario 3 has some green values for privacy, but none for security.

The figure shows that the metrics which have constant values for each of the configurations makes the numbers be very similar. In this example M1 and M3 are constant. In other words, the system SP values gets similiar for all of the configurations. The system SP values kind of gets locked from getting really high or really low. Because of this is, we think constant values should be considered when setting the SP_{Goal} to

	Criticality										SPD(s,p)							
	C1		C2		C3		C4		Sub-system				Scen. 1		Scen. 2		Scen. 3	
SPD(Goal)													(55, 80, d)		(70, 60, d)		(75, 10, d)	
Multi-metrics	M1		M2		M3 & M4		M5											
	S	P	S	P	S	P	S	P	S	P	S	P	S	P	S	P	S	P
Conf. A	50	5	25	30	25	68	0	0	37	44	63	56	Green	Red	Green	Green	Yellow	Red
Conf. B	50	5	25	30	25	68	0	0	37	44	63	56	Green	Red	Green	Green	Yellow	Red
Conf. C	50	5	10	15	25	68	0	0	36	39	64	61	Green	Yellow	Green	Green	Yellow	Red
Conf. D	50	5	10	15	25	68	0	0	36	39	64	61	Green	Yellow	Green	Green	Yellow	Red
Conf. E	50	5	5	8	50	80	6	10	42	45	58	55	Green	Red	Yellow	Green	Yellow	Red
Conf. F	50	5	5	8	50	80	6	10	42	45	58	55	Green	Red	Yellow	Green	Yellow	Red

Components:	Ws	Wp
C1: Sensor radio waves	60	5
C2: Encryption	20	70
C3: Wifi	30	40
C4: Controller GSM modem	20	15

Metrics	Ws	Wp
M1: Sensor device metrics	100	100
M2: Encryption metric	100	100
M3: Wifi sensor to controller	30	30
M4: Wifi controller to router(BE)	70	70
M5: SMS message rate metric	100	100

Figure 8: Multi-Metrics 1

make a realistic goal.

The metrics that have a high difference in the criticality numbers for the configurations makes a bigger difference of the SP values for the system. The encryption metrics and the WiFi controller to router metrics are those who makes the biggest differences in this use case.

The SMS rate metric does not make much difference in numbers for the configurations, but when not sending any messages the criticality is 0. We thought this would have a certain influence on the system, because a part of the calculation would end up with 0. It seemed to be false in our attempts of proving this.

We can conclude that the encryption is the most important part in this system, and that the constant metric values should be considered into the SP_{Goal} to make the goal more realistic. We also see that using both SMS and internet for sending messages is good in case of network downtime.

For further work we see that we need some changes in the metrics. We did not really know at first that the system cannot change encryption between different scenarios. Therefore configurations should be added to check which of the encryptions is the best option for all of the scenarios. The encryption on the data from the ES to the BE has also been discussed and we have different opinions on this, so that it might need some changes. We would also change the communication channel between the sensors and the sensor controller to for instance ZigBee or bluetooth, which will both save the sensors battery and the security and privacy would be better than when the data gets sent through the router to get to the controller. This would also make the system more secure since the sensors can send data to the sensor controller even though the Internet is down. In other words, the system still works if the Internet is down. In addition the interval of sending data from the sensors to the controller would be changed if there are no movements at all in a room. Instead the sensors should send a keep-alive message to the sensor controller every minute.

	Criticality										SPD(s,p)							
	C1		C2		C3		C4		Sub-system				Scen. 1		Scen. 2		Scen. 3	
SPD(Goal)													(55, 80, d)		(70, 60, d)		(75, 10, d)	
Multi-metrics	M1		M2		M3 & M4		M5											
	S	P	S	P	S	P	S	P	S	P	S	P	S	P	S	P	S	P
Conf. A	50	5	5	8	25	68	0	0	36	38	64	62	Green	Yellow	Green	Green	Yellow	Red
Conf. B	50	5	5	8	25	68	0	0	36	38	64	62	Green	Yellow	Green	Green	Yellow	Red
Conf. C	50	5	10	15	25	68	0	0	36	39	64	61	Green	Yellow	Green	Green	Yellow	Red
Conf. D	50	5	10	15	25	68	0	0	36	39	64	61	Green	Yellow	Green	Green	Yellow	Red
Conf. E	50	5	70	90	50	80	6	10	50	80	50	20	Green	Red	Yellow	Red	Red	Green
Conf. F	50	5	70	90	50	80	6	10	50	80	50	20	Green	Red	Yellow	Red	Red	Green

Components:	**Ws**	**Wp**
C1: Sensor radio waves	60	5
C2: Encryption	20	70
C3: Wifi	30	40
C4: Controller GSM modem	20	15

Metrics	**Ws**	**Wp**
M1: Sensor device metrics	100	100
M2: Encryption metric	100	100
M3: Wifi sensor to controller	30	30
M4: Wifi controller to router(BE)	70	70
M5: SMS message rate metric	100	100

Figure 9: Multi-Metrics 2

7 Evaluation of the Method

The method in this project is used in order to get a secure and privacy-aware system, instead of having privacy and security as an add-on. Having them as an add-on makes the system look secure and privacy-aware, but not considering all of the components in the system makes it vulnerable. This is a strength of the method because the method considers all the components in a system and gets an overall SP_{System} value. Another strength is the weighting of the metrics. The weighting makes the big difference of the SPD values in the method from system to system. It is what makes the method personalize the SPD values for a given system. A strength of the method is also that the complexity of the evaluation process is reduced.

A weakness in the system is when setting the numbers of criticality. Two experts might have a different idea of the criticality number in a metric, but for the exact same reason. Having a standard (more than numbers between 0 to 100) could be a solution to this. Another weakness is the confusion of privacy and the security attribute confidentiality. Even when thinking about the difference in the two of them, it is difficult to part them in a system. So then the question is if the confidentiality should be considered a lot in security or not. This might be more of a weakness for us, than for the method, but since this might be confusing to a lot of people, we suggest that there is a clear definition of how they should be considered in this method. Other suggestions is to split the security attributes or to have a method for setting the SPD criticality for the security. We also suggest that the range of what are the accepted values could also be decided differently in different systems.

References

[1] Garitano, I., Fayyad, S., Noll, J. (2015) *Multi-Metrics Approach for Security, Privacy and Dependability in Embedded Systems.*

[2] XeThru. (2016) *http://www.xethru.com/*