

How to Protect a Hospital Against Cyber Attacks

Alain Guinet

Abstract Hospitals have not been prepared to face cyber attacks. Their core objective is to take care about patients by curing them efficiently. In this paper we propose a vulnerability assessment approach, to highlight the information system weaknesses of a hospital. By defining a map of the information system which considers the most critical assets (i.e., the units which manage the core information), the most likely attack scenarios with the worst consequences are constructed. By studying these scenarios, we suggest mitigation countermeasures, based on a reorganization of the digital information system into isolated sub-systems. Our objective is to be more resilient to cyber attacks, by increasing the required complexity for hacker's crimes and by limiting the damages of attacks.

keywords Cyber attacks • Hospital vulnerability
Information system mapping • Partitioning • Defence

1 Introduction

A study published by the Institute for Critical Infrastructure Technology in 2016, specifies that 72% of the US health care societies have been targeted by cyber attacks during 2012, 47% of the US people which accessed to the health care system have been victims of corrupted medical data, due to hackers. The cyber attacks are a sad reality in health care systems. Hospitals have not been prepared to face such a cyber war. Their core objective is to take care about patients by curing them efficiently. In this paper we propose a vulnerability assessment approach, to highlight the weaknesses of the digital information system of a hospital. By defining a map of the information system which considers the most critical assets (i.e., the units which manage the core information), the most likely attack scenarios

A. Guinet (✉)

DISP, Institut National Des Sciences Appliquées de Lyon, (Université de Lyon),
21 Av. Jean Capelle, 69621 Villeurbanne, France
e-mail: alain.guinet@insa-lyon.fr

© Springer International Publishing AG 2017

P. Cappanera et al. (eds.), *Health Care Systems Engineering*, Springer Proceedings
in Mathematics & Statistics 210, https://doi.org/10.1007/978-3-319-66146-9_1

with the worst consequences are constructed. By studying these scenarios, we suggest mitigation countermeasures, based on a reorganization of the digital information system into isolated sub-systems. Our objective is to be more resilient to cyber attacks, by increasing the required complexity for hacker's crimes and by limiting the damages of hacker's attacks.

In a second section, we present the different types of hackers and we illustrate their motivations with some cyber attack stories, from the health care sector. In a third section, we propose an approach to reduce the hospital vulnerability in cyber attack situations. This approach is based on a consensus mapping of the information system which enables us to find possible breaches which can be used by hackers. After having defined some scenarios, we discuss in the fourth section how to use the map of the hospital information system to define countermeasures, in order to mitigate the cyber attack scenarios.

2 The Cyber Attack Sources

Cyber attacks can be motivated by claiming, illegal gains or violence, as described hereafter.

2.1 *Hacktivists*

Hacktivists try to make propaganda by obtaining media attention in order to promote their values. These hackers can also act for enjoyable reasons. Cyber attacks from hacktivists are disruptive. The most common hacktivist attack is a denial of service (DDoS) attack, which overloads a hospital's server with undesired traffics in order to halt the regular operations of the server. A watering hole attack is another cyber attack in which the hacktivist seeks to infect websites in order to send its propaganda or malware to end users. The goal is to infect a server and gain access to the end users by the compromised server. The capabilities of hacktivists are: a low level of organisational support, a poor financial backing, a small network of members and limited capacities for computing/networking.

On April 2014, protesting on a child custody case, who was being kept at Boston Children's hospital against the wishes of him/her parents, the hacktivist group Anonymous launched multiple distributed denial-of-service attacks that targeted the hospital's servers and hamstrung its operations for a week (<https://www.bostonglobe.com/business/2014/04/24/hacker-group-anonymous-targets-children-hospital-over-justina-pelletier-case/jSd3EE5VVHbSGTJdS5YrfM/story.html>).

2.2 Terrorists

The main terrorist objectives are to spread terror and to kill people. Terrorists try to cause violence and damage, in order to destabilize the hospital and the patients. Cyber attacks from terrorists are destructive. The different forms of cyber attacks are: espionage, theft, sabotage and personal abuse. A possible attack can be information system hacking, in order to change patient prescription, medical test results or the formulation of pharmaceutical receipts. The capabilities of terrorists are: a high level of organisational support, a good financial backing, an efficient network of members, numerous possibilities to subcontract to hackers without ethic for computer virus developments.

At the Def Con hacking conference in 2011, Jay Radcliffe has suggested a technique for attacking a insulin pump that it is used to deliver insulin to a patient. He hacked into the pump by remotely accessing the wireless monitoring system. He demonstrated that the approach could have been used to deliver lethal insulin doses to a patient (<http://www.reuters.com/article/us-rapid7-radcliffe-idUSKBN0E929K20140529>).

2.3 Criminals or State Sponsored Hackers

Cyber criminals try to generate profit through the exploitation or through the racketeering of hospital data or patients' data. Cyber attacks from criminals can be disruptive or destructive. The most common criminal attack is the ransom-ware attack, which encrypts files in an information system. If the hospital does not pay the ransom, the files are destroyed. Phishing is another form of criminal attack which consists to steal personal information data (e.g. bank identity) without violence. The user opens a malicious email from a false government agency and gives confidential information about the hospital or a patient. A delinquent has the same capacities such as a Hacktivist. The state sponsored hackers or cybercriminal groups such as mafia versus triad can be viewed as terrorists. Criminals always seek easier targets because they often do not have a plethora of resources.

On February 2016, a Southern California hospital was a victim of a cyber attack, which interfered with day-to-day operations. The CEO said that the shutdown has not affected patient care. Several hospital staff members said the computer system was hacked and was being held on a ransom of 3.4 billion in bit coins, and in exchange, the hackers would send back the key codes to restore the system. In reality the California's Hollywood Presbyterian Medical Centre shelled out 40 bit coins, or about \$17,000, in order to regain access to its electronic health records. (<http://www.nbclosangeles.com/news/local/FBI-LAPD-Investigating-Hollywood-Hospital-Cyber-Attack-368703121.html>).

3 The Cyber Attack Approach

We propose the following vulnerability assessment approach to face the above situations.

1. Find the threat sources: Reviewing historical data on cyber attacks, we specify the adversary profile, their potential actions, their capabilities, and their motivation, as done above.
2. Define critical assets: Identifying the care units and the technical units of the hospital which use digital information as input or output or for management. We locate the critical assets regarding to their contribution to the information system, i.e. the units which are the most likely and the easiest to be faced with a computer virus and which are the most damageable regarding to lost information and the hospital added value ... An IDEFØ model enables us to map the critical assets.
3. Calculate critical asset attractiveness: Realize an analysis based on pairing of each critical asset and of each threat source by brainstorming, in order to identify potential vulnerabilities per adversary, and to better evaluate the ease of causing damages, according to adversary's motivation.
4. Define Threat Scenarios: Based on the attractiveness of the critical assets per adversary, the most likely (i.e. the easiest target for the most motivated adversary) attack scenarios with the worst consequences are constructed.
5. Assess Threat Scenarios: Scenarios are studied to evaluate their consequences, to propose possible counter-measures in order to reduce the risk to an acceptable level by a cost/benefit analysis. This step is repeated until all relevant scenarios are mitigated and are instrumented with an efficient response plan. The IDEFØ map of the critical assets is studied to mitigate the threats regarding to their propagation, knowing that infection is propagated through digital exchanges. A mixed linear program is proposed to help the decision maker regarding to mitigation.

3.1 The Information System Mapping as a Tool

IDEFØ [1] is a method designed to model the events, data, and activities of an organization or a system. The IDEFØ model helps to organize the analysis of a system and allows promoting good communication between the analysts and the users. It enhances user involvement and allows us to obtain consensus models [2] which are a basic requirement when actors are multidisciplinary such as physicians, nurses, technicians, engineers, administrative staff, managers, etc. The analysis of the system is represented as a collection of hierarchically organized diagrams with a limited number of elements: boxes which represent activities or physical units, or equipment, and arrows to model physical, information, order flows, data stores etc.

IDEFØ will assist us in identifying on one hand units and services which manage digital information, i.e. which could be a source of computer virus by Internet, USB keys, user access privileges, and on the other hand connections which could be a propagation way for contamination by exploiting the data flows. An IDEFØ model will be firstly created for our hospital analysis (Figs. 1 and 2) and it will be used to identify the critical assets regarding to information management, and secondly to generate a network mapping (Fig. 3) in order to evaluate the weaknesses of the network and to study scenarios including countermeasures. Arrows model only information and data stores are represented as mechanism arrows. By default, reading and writing are allowed for data stores.

In Fig. 1, the hospital units/services use different information files which contain the core elements of their missions (bed planning for the central booking, patient medical files for care units, etc.). The patient identification is the connexion data between these different files to enforce the integrity of the information system but could be a contamination way. Internet access is provided to each unit/service and it defines a potential infection source. Regarding this user view, information is decentralized and can be physically isolated, mainly if information is virtually partitioned on the same server.

In Fig. 2, all of the units use the patient medical files, and can corrupt them. Internet is reserved to hospital wards. The patient monitoring system is dedicated to ICU but it is linked to other care units by the patient medical files. Information is centralized and cannot be easily fragmented except maybe for ICU.

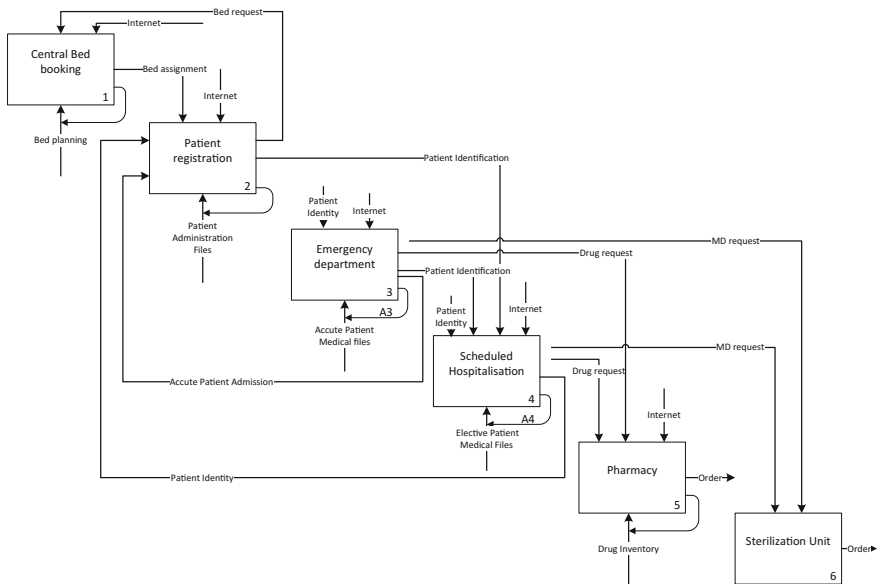


Fig. 1 The global model of the hospital

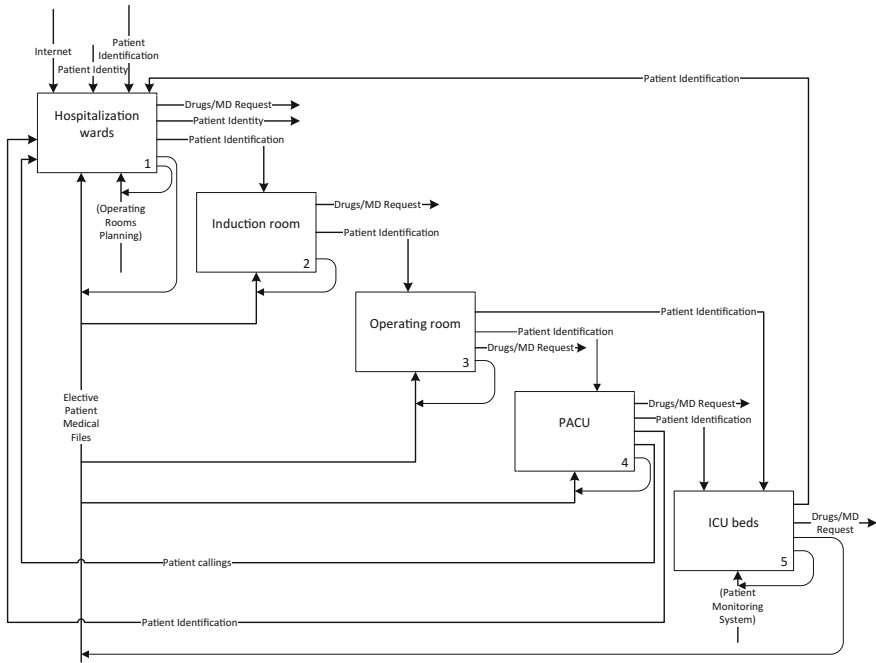


Fig. 2 The detailed model of the scheduled hospitalization

To calculate the information system mapping, we export from the IDEFØ model the different connexions between the leaves (services/units) of the decomposition tree of IDEFØ diagrams.

The result is modelled by a binary matrix (see Fig. 3) where the lines/columns represent the leaves, and the intersections between lines and columns identify the presence (1) or absence (0) of a digital connexion which could be a contamination way between two critical assets. Such binary matrix will be used to define the most resilient information system architecture. Data stores are supposed to be attached to users. If two data stores of two different users are virtually partitioned on the same server, a digital connexion between the two users is added in both ways, because a potential infection risk exists by cohabitating on the same server. Demilitarized zones can also be modelled specifying WIFI access as explained below.

3.2 The Critical Assets

According to the IDEFØ model (Figs. 1 and 2), some critical assets have been identified. They represent the units which manage core information about patients, activities, employees, etc.

	A1	A2	A31	A32	A33	A34	A35	A36	A41	A42	A43	A44	A45	A5	A6
A1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
A2	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0
A31	0	1	1	1	1	0	1	1	0	0	0	0	0	0	0
A32	0	0	1	1	1	0	1	1	0	0	0	0	0	1	1
A33	0	0	1	1	1	0	1	1	0	0	0	0	0	1	1
A34	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
A35	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0
A36	0	0	1	1	1	0	1	1	0	0	0	0	0	1	1
A41	0	1	0	0	0	0	0	0	1	1	1	1	1	1	1
A42	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
A43	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
A44	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
A45	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
A5	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
A6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Fig. 3 The information system mapping

Emergency department and scheduled hospitalization: The patient medical files from emergency and hospitalization wards are collections of personal data about patient diagnosis, patient treatments, patient laboratory tests, medical reports, etc. The patient medical files are accessible by all the care units. They allow deciding: the patient’s pathway, the laboratory exams, the drug prescriptions, etc.

Patient registration: The patient administrative files managed by the patient registration unit contain information about personal data (names, addresses, phone number, bank details, etc.), insurance identification, relatives’ information ... The patient administrative files enable the patient financial support, the communication with patient’s relatives, etc. They are at the origin of all patient files. The database is managed by a software suit, which links the medical files, the bed planning and the operating room planning. Patient registration uses websites of health care insurance companies.

Patient registration and central bed booking: The patient registration enables to manage remotely patient admissions by physician and the central bed booking calculates the bed planning which assigns a bed to each patient over a horizon of four weeks. The bed planning allows scheduling the activity of several care units: radiology, surgery, nursing, pharmacy, etc. It is shared by all the care units, and enables to supervise all the nursing and medical activities. The bed planning is also a coordination tool between emergency and hospitalization wards.

Intensive care unit: The patient monitoring system of ICU supervises the oxygen/drug supply to patient requiring intensive cares. The blood pressure, the heart rate, the ECG signal, etc., are vital parameters which are monitored and can trigger nursing/physician alerts. The SCADA system is used to manage the ICU beds [3]. It manages the supervisory control, data acquisition system and pumps' control. The SCADA (Supervisory Control And Data Acquisition) system is potentially vulnerable to disruption of service [4], or to manipulation of data that could result in lack of vital safety for patients.

3.3 The Critical Asset Attractiveness

Based on a brainstorming, the attractiveness of the critical assets has been discussed, by pairing each critical asset and each threat source. For “Scheduled hospitalisation (Elective patient medical files) and Emergency department (Acute patient medical files)”, the threats can be:

- **Hacktivists:** The identification of patients requiring an abortion or of the surgeons practicing abortion, and the diffusion of such information on social networks could be a goal of hacktivists.
- **Criminals:** The patient medical files contain confidential information about patient test results and patients' treatments. Such information can be sold to malicious financial companies.
- **Terrorists:** Patients suffering from AIDS, could be identified by terrorists, and could be individually targeted by further criminal actions. Patient's blood types can be changed to mass casualties.

3.4 The Threat Scenarios

The revenge: An employee has been recently fired. He/she approaches a hacker and he convinces him to destroy the hospital network by encrypting the servers. The hacker inserts a worm to get the network node plan, then she/he remotely jeopardises the network introducing crypto-lockers. All the hospital activities are out of order except the ones working with paper and autonomous equipment, i.e. diagnostic devices such as the radiology department. The emergency department has to

stay closed and the elective activity must be stopped. The risk of errors is dramatically increased. The whole information system is corrupted. On the financial side, the hospital probably lost \$1 million a day in billing.

The murdering: An important politician is in a surgery unit. He/she has just favoured in Parliament the approval of a law in favour of the abortion/euthanasia. A criminal paid by domestic terrorists, infiltrates the hospital information system, and next jeopardizes the patient monitoring system of ICU beds. After the surgery the Politician requires an ICU bed. The politician is killed by disruption of ICU monitoring system that has been compromised (drug dosage and/or ventilation). The SCADA system which manages the supervisory control and data acquisition system of ICU beds was unprotected. Data was not encrypted and could be easily read and modified in order to deliver a lethal dose.

4 The Scenario Assessment with the Information System Mapping

Most of works on information system defence are based on attack graphs to find system breaches and to select countermeasures [5, 6]. Attack graphs have an exponential complexity and are not easily understandable by users [7]. The architecture of the information system is very few questioned [8]. As countermeasures, investments on software are favoured instead of investments on system architecture which require heavier system upgrades due to information system integration. Since this latter is less sensitive in hospital due to the job variety (surgery, nursing, pharmacy, accommodation, etc.) and as the information system network is bounded, we favour information system architecture study. This focus is recommended by the French Network and Information Security Agency (ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information) [9].

4.1 *The Strongly Connected Components of the Information System*

Figure 3 presents a map of the hospital information system. This map is modelled by a matrix where the N nodes represent the critical assets and the arrows define the digital exchanges between the critical assets. If we calculate the minimum number of strongly connected components of this graph [10] with a computation complexity of N^3 , we define sub-graphs which are totally linked and which can be easily contaminated if one of the nodes of the sub-graph is infected. May be, a strongly connected component can be easily compromised but the damages can be limited to the sub-graph if it is physically isolated. The transitive closure gives us an idea of the information system vulnerability.

Our proposal is to create independent sub-graphs to reduce the damage consequences caused by cyber attacks while minimizing the drawback of disconnected sub-graphs [9]. Partitioning data through physically independent sub-systems on one hand reduces the contamination (propagation of viruses by transitivity), also increases the complexity of a potential cyber attack corrupting the whole data, and on the other hand allows the information system to run partially after an attack. Five strongly connected components have been identified in the IDEFØ graph. They lead to define five natural sub-graphs which represent the elective patient activity (A1, A2, A41, A42, A43, A44, A45), the acute patient activity (A31, A32, A33, A35, A36), the pharmacy (A5), the sterilization unit (A6) and a single room (A34: the waiting room of the emergency department which could be demilitarized and enable the patient's relatives to access WIFI). By isolating the information system into five independent sub-systems, we do not enable the sharing of the patient identification between units/services and of the units' requests to the pharmacy/sterilization, by a digital way. Encrypted barcodes identifying patients/products (i.e. only little information) can be an efficient and secure way to exchange data via paper. Information is transmitted by hand.

As mitigation countermeasures, our matrix enables us: to complicate cyber-attacks by partitioning the information system into independent subsystems, to favour the service continuity limiting potential cyber-attacks, to specify attack graphs using simulation [11], to define demilitarized zones for a safe use of internet, and to assess the access rights by units or services, respecting confidentiality and security.

4.2 *The K Partitioning Problem*

The transitive closure proposes a natural partitioning of the graph into sub-graphs. The strongly connected components represent the critical assets which share the same information and cannot be separated without a heavy loss of digital information exchanges. If we hypothesize that such partitions become physically independent regarding to digital information exchanges, a minimum of information exchanges is lost by partitioning the graph into sub-graphs corresponding to the strongly connected components. To go further, we propose a mixed linear model to partition the graph into at least K components, on one hand with weighted arcs in order to take into account the information traffic level between nodes and on the other hand with weighted critical assets to evaluate the damages of a corrupted partition. The mixed linear model must be used after calculating the transitive closure of the graph, in order to take into account all transitive links.

Data:

- N: number of system components, K: the minimum number of partitions,
- $c(i, j)$: it is equal to 1 if system component i is linked as input with system component j ,

- $d(i)$: potential damage of critical asset i when corrupted (disruption of activity, data restoration),
- $w(i, j)$: data traffic from the system component i to the system component j , expressed in working hours to evaluate the potential loss of digital traffic.

Variables:

- $X(i, k)$: this binary variable is equal to 1 if i is assigned to partition k ,
- $Y(k)$: this binary variable is equal to 1 if at least one node has been assigned to partition k ,
- $Loss(i, j)$: real variable, the link from i to j is deleted and it results a loss of $w(i, j)$ traffic,
- $Dmax$: real variable, maximum damage of a partition when corrupted.

Objective function:

$$\text{Minimize}(Z) = \sum_{i=1}^N \sum_{j=1}^N Loss(i, j) + Dmax \quad (1)$$

We minimize the losses of traffic knowing that partitions are not linked, and the maximum damages to a partition. We hypothesize an attack to only one partition instead of the entire information system.

Constraints:

$$\sum_{k=1}^N X(i, k) = 1 \quad \forall i = 1, \dots, N \quad (2)$$

A system component i must belong to one and only one partition.

$$X(i, k) + X(j, k) - 1 \leq c(i, j) \quad \forall i, j, k = 1, \dots, N \quad (3)$$

A pair of system components i and j belonging to the same partition, must exchange traffic.

$$\sum_{i=1}^N X(i, k) \leq N * Y(k) \quad \forall k = 1, \dots, N \quad (4)$$

$$\sum_{i=1}^N X(i, k) \geq Y(k) \quad \forall k = 1, \dots, N \quad (5)$$

$$\sum_{k=1}^N Y(k) \geq K \quad (6)$$

A partition must contain at least 1 system component. We count the number of partitions which must be greater than K .

$$Loss(i, j) \geq w(i, j) * X(i, k) - w(i, j) * X(j, k) \quad \forall i, j, k = 1, \dots, N \quad (7)$$

$$Loss(i, j) \geq w(i, j) * X(j, k) - w(i, j) * X(i, k) \quad \forall i, j, k = 1, \dots, N \quad (8)$$

The calculation of loss of traffic is done taking into account the links between system components belonging to different partitions.

$$\sum_{i=1}^N d(i)*X(i,k) \leq Dmax \quad \forall k = 1, \dots, N \quad (9)$$

The calculation of the potential damages is done. The maximum damage is sought.

Comments:

We have modelled a mixed linear program to solve a K partitioning problem, where K is greater or equal than a given number, the number of nodes per partition is unconstrained. We minimize on one hand the sum of the weighted arcs between partitions (i.e. lost links), and on the other hand the partitioning risk depending on the critical assets which belong to the same partition. We hypothesis a cyber attack limited to only one sub-system. The resulting K partitioning problem is NP hard [12]. The damages of critical assets are calculated regarding to the activity disruption which is evaluated by the lost turnover and the restoration cost of the information system (i.e. the software loading, the backup recovery, the data update due to the failure period). The traffic losses take into account the working hours to transmit information by hand (data input, barcode scanning, data printing, etc.). All costs are expressed in Euros. The cost horizon reference is one month.

We have solved our mathematical program with the Cplex solver in a few seconds. If K is equal to the number of strongly connected components, the number of partitions is most of the time equal to K and the assignment of components to partitions is the same that was calculated by transitive closure. Only a great variety of traffic costs or a large diversity of damage costs of critical assets introduces changes in the number of partitions. If the graph is a strongly connected graph, than it results just one partition. The mixed linear model will be of a great help to study the partitioning problem with increasing successive values of K.

4.3 *Feedback of Partitioning by Scenario*

Regarding the revenge scenario, the hacker has to steal the authentication and the identification of five employees who have an authorized access to the five partitions, in order to corrupt the whole system. If the fired employee has still an access to one of these partitions, the ransom-ware attack is limited. A paper kit system can be used to enable the continuity of service of the damaged assets (unit/service) whose data are encrypted [13], and the restoration of the corrupted equipments with an offline redundant hardware can be part of the solution.

The murdering scenario is more complicated because the patient monitoring system of ICU belongs to a partition which includes two kinds of data: SCADA data and patient medical files. Both data could be corrupted to kill the VIP, the medical prescription and/or the SCADA parameters. If we isolate the patient monitoring system of ICU in a 6th partition, the parameters of the intensive care

bed will be specified by the anaesthesiologist and the data will not be remotely corrupted. The large information feedback from ICU monitoring which is no more automatically transmitted to the patient medical files, can be transferred with an encrypted USB key. Restrictive access to both systems managing the files, the denial of unauthorized programs, adoption of redundant hardware offline with backups, can be other ways to protect the hacked information sub-system.

Considering both scenarios, internet accesses are necessary: for bed booking (allowing remotely accesses for physicians) patient registration (enabling accesses to the insurance websites) and hospitalization wards, which define the first strongly connected component, for the physicians of the emergency department (which represents the second strongly connected component) and for pharmacy (which is the fourth strongly connected component). However, some restrictions must be recommended: the email access and internet access must be denied as far as possible for the emergency department and the pharmacy on the application server and its connected objects; only physicians/pharmacists might have an email access and internet access on their personal computers by an independent WIFI server; the non encrypted USB keys must be prohibited, and internet accesses must be checked on a daily basis for application servers [14].

5 Conclusion

In this paper we have proposed an approach to assess the vulnerability of hospitals against cyber attacks. After potential hacker identification, we suggest first to define the critical assets of information system in terms of units/services which manage core information about patients, employees, etc. Second, the attractiveness of critical assets is specified per adversaries. The modelling support to find the weaknesses of the hospital information system is a map resulting from an IDEFØ analysis. This map represents the digital exchanges between units/services. Third, some scenarios which represent the most likely critical assets to be attacked with the most potential damages are studied, and the consequences of cyber attacks are analysed thanks to the information system map. By calculating the partitioning of the information system by a transitive closure, we can propose mitigation countermeasures. To go further, a mixed linear program has been modelled to find the best set of sub-systems for the hospital information system, by minimizing losses of digital traffic between the independent sub-systems and contamination damages to components belonging to the same sub-system. This work is the continuation of the Threats project: <http://www.threatsproject.eu/project.html>.

References

1. IDEFØ, Integration Definition for Function Modelling (IDEFØ) Draft Federal Information Processing Standards Publication (1993). <http://www.idef.com/Downloads/pdf/idef0.pdf>
2. Bevilacqua, M., Ciarapica, F.E., Paciarotti, C.: Business process reengineering of emergency management procedures: a case study. *Saf. Sci.* **50**, 1368–1376 (2012)
3. Malavika, S.: Automized intensive care unit (AICU). *Int. J. Adv. Electr. Electr. Eng.* **1**, 11–14 (2012)
4. Venkateswarlu, G.: Expert and SCADA based centralized patient monitoring and escorting system. *Int.J. Adv. Res. Electr. Electr. Instrum. Eng.* **3**, 13089–13098 (2014)
5. Phillips, C., Painton-Swiler, L.: A graph-based system for network-vulnerability analysis. In: 9th ACM Conference on Computer and Communications Security, pp. 71–79. ACM Press, Charlottesville, VA, USA (1999)
6. Poolsappasit, N., Dewri, R., Ray, I.: Dynamic security risk management using bayesian attack graphs. *IEEE Trans. Depend. Secure Comput.* **9**, 61–74 (2012)
7. Yeh, Q.J., Jung-Ting Chang, A.: Threats and countermeasures for information system security: a cross-industry study. *Inf. Manag.* **44**, 480–491 (2007)
8. Noel, S., Jajodia, S.: Understanding complex network attack graphs through clustered adjacency matrices. In: Proceedings of the 21st Annual Computer Security Applications Conference, IEEE, pp. 1–10 (2006)
9. ANSSI, 40 essential measures for a healthy network. <http://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/> (2013)
10. Yelowitz, L.: An efficient algorithm for constructing hierarchical graphs. *IEEE Trans. Syst. Man Cybern.* **6**, 327–329 (1976)
11. Kuhl, M.E., Sudit, M., Kistner, J., Costantini, K.: Cyber attack modelling and simulation for network security analysis. In: Proceedings of the 2007 Winter Simulation Conference, pp. 1180–1188
12. Kernighan, B.W., Lin, S.: An efficient heuristic procedure for partitioning graphs. *Bell Syst. Tech. J.* **49**, 291–307 (1970)
13. Grange, H., Leynon, J.: Crisis management plan: preventive measures and lessons learned from a major computer system failure, HCSE 2015. In: Proceedings in Mathematics and Statistics. Springer, Lyon, France, pp. 203–214 (2015)
14. Scott, J., Eftekhari, P.: Hacking Healthcare IT in 2016, Institute for Critical Infrastructure Technology. <http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf> (2016)