GENERIC SECURITY CASES FOR INFORMATION SYSTEM SECURITY IN HEALTHCARE SYSTEMS

Y. He, C.W. Johnson

**Univerisity of Glasgow, UK*
yingh@dcs.gla.ac.uk, Christopher.Johnson@glasgow.ac.uk.

Keywords: Healthcare System, System Security, Generic Security Case, Security Incidents.

Abstract

Numerous data breach incidents have been reported in recent years and there is a continuing requirement to protect patient and clinician confidentiality. However, the diversity of security products, tools and techniques in the market place make it very hard for management to ensure that they have implemented coherent countermeasures to meet organisations higher-level objectives. This paper focuses on the problems that arise in implementing and maintaining cyber-security policies in large, complex healthcare organisations. We address these problems by the use of graphical argumentation techniques. In particular, we show how the Goal Structuring Notations (GSN) can be extended from applications in safety-critical systems. Security arguments presented with GSN can help managers to reason about cyber-security policies and procedures by bringing together claims and the evidence that supports them in a structured and coherent way. A further objective of this paper is to show how GSN can be used to construct security arguments that are informed by the analysis of previous security incidents in healthcare organisations. In particular, we present two generic security cases that embody the recommendations from incidents involving the United States' Veterans' Affairs (VA) administration and Shenzhen Hospital in China. These case studies were deliberately chosen to show how lessons learned in one country might inform security management in other healthcare systems. We also show that security cases can be created at a level of abstraction that support reuses and at the same time capture detailed recommendations from security incidents.

1 Introduction

Information Security refers to "the preservation of confidentiality, integrity and availability (CIA) of information" [1]. Achieving these objectives is non-trivial because there is a growing range of security threats from phishing, rootkits, back doors, botnets, malware infection and so on. Moreover, new vulnerabilities are continuously detected. The national vulnerability database lists over 50,000 security problems with 15 new vulnerabilities per day [3]. The e-Crime Report 2011 from KPMG stresses the increasing importance of protecting data because of the damage that cyber-incidents cause to the reputation of many organisations [2]. Thus, Information Security continues to be a major concern. Many security solutions and techniques have been developed, including Anti-virus Software, Threat Analysis tools, Data Loss Protection (DLP) tools, Security Standards, Security Best Practices and so on. The diversity of products, tools and techniques in the market place make it very hard for management to ensure that they have implemented coherent countermeasures. It can be difficult to develop and sustain a coherent argument about the ways in which existing security mechanisms meet organisation's higher-level objectives. As a result, weaknesses can persist even when a great efforts and expertise has been devoted to the implementation of security policies.

This paper focuses on the problems that arise in maintaining cyber-security policies in large, complex healthcare organisations. We have chosen to focus on this domain because there is a continuing requirement to protect patient and clinician confidentiality. According to a recent Internet Threat Report by Symantec, the healthcare sector accounts for 43% of all reported data breaches [4]. A variety of security standards and regulations has been established to support healthcare security, including the US Health Insurance Portability and Accountability Act (HIPAA) [5], the Federal Information Security Management Act (FISMA) [6], ISO 27000 Series and GB/T22239-2008, etc. [7].

The proliferation of security guidance creates its own problems. Many healthcare organizations collate their security policies, procedures and audit requirements across hundreds of pages of text. Staff often fail to read these lengthy documents. It can also be difficult to navigate the guidance to identify those sections of a cyber-security policy that apply to particular IT infrastructures. Finally, it can be hard to gain an overview of how many different security arguments fit together within more complex security management systems. In this paper, we address these problems by the use of Goal Structuring Notations (GSN) [8].

This paper is also motivated by the numerous, well publicised security breaches that have occurred around the globe, in recent years. Despite the efforts devoted in meeting security standards during system design, security incidents are reported with regularity. A report from the Privacy Rights Clearinghouse (PRC) focuses on the significant financial costs associated with three incidents involving medical records during 2011 [9]. Those data loss incidents are not new. In particular, this paper focuses on the United States' Veterans' Affairs (VA) data loss cases in 2007 [10]. These incidents share some features in common: (1) Sensitive data were not properly encrypted; (2) Security policies were not effectively enforced or communicated to staff; (3) Incidence handling and response were delayed. It seems that the industry has not learned the lessons from previous security incidents.

A further objective of this paper is to show that GSN can be used to construct generic security cases that are informed by the analysis of previous security incidents in healthcare organisations. The argumentation structures are generic because they are deliberately created at a level of abstraction that enables their application across a number of complex organisations with very different security policies. In addition to the Veterans' Affairs (VA) case study, mentioned above, subsequent sections refer to the Shenzhen Hospital in China. We have demonstrated the generic nature of the approach by applying insights to support patient confidentiality in healthcare organisations across North America, China and Europe. System weaknesses and vulnerabilities identified from these incidents are linked to security objectives and to the solutions recommended in existing standards, policies and procedures.

2 Argument and Goal Structuring Notations

2.1 Argumentation Techniques

"An argument is a reason or set of reasons given in support of an idea, action or theory." [11]. Argumentation techniques have been widely used within safety-critical systems to support the development of safety cases. A safety case is defined as "a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment." [13]. Safety cases are increasingly being used in different industries. For instance, the Presidential enquiry into the Deep Water Horizon accident advocated the use of safety cases across the US gas and oil industry [14]. Safety cases are also a requirement of UK Ministry of Defence Standard 00-56 [15].

ISO 15026 introduces the concept of a security assurance case [18]. These can be defined as "a documented body of evidence that provides a convincing and valid argument that a system is adequately secure for a given application in a given environment". Goodenough has used the Goal Structuring Notations to structure security arguments across different stages of the software development life cycle [16]. Unfortunately, security cases have not been widely used in system security management and there are no publicised examples of their use to protect patient confidentiality across the healthcare industries.

2.2 Goal Structuring Notations (GSN)

Security Arguments can be presented using text-based or graphical notations. Some people prefer verbal presentation. For instance, Holloway has presented five styles of text-based representations for safety arguments [19]. However, the resulting documents are usually lengthy and can be difficult to review. The logic of the argument is often lost in large volumes of paper documentation. Graphical Notations, address these limitations [20]. Examples include Claims-Argument-Evidence (CAE) and Goal Structuring Notations (GSN).

The CAE technique was introduced by Bloomfield in 1998; "Claim is about a property of the system or some subsystem. Evidence is used as the basis of the argument, which can be facts, assumptions, or sub-claims, derived from a lower-level sub-argument. Argument is used for linking the evidence to the claim, which can be deterministic, probabilistic or qualitative. Inference is the mechanism that provides the transformational rules for the argument" [13]. The Goal Structuring Notations (GSN) was developed in the early 1990s and has undergone significant development and refinement since then. Within Europe, GSN has been adopted by a growing number of companies for the presentation of safety arguments within safety cases [17]. In this paper we extend the application of GSN to analyse the security arguments deployed by healthcare organisations, especially in the aftermath of data breaches.

The GSN notations present arguments by creating relational structures between goals, sub-goals, solutions, strategies and contexts [8].

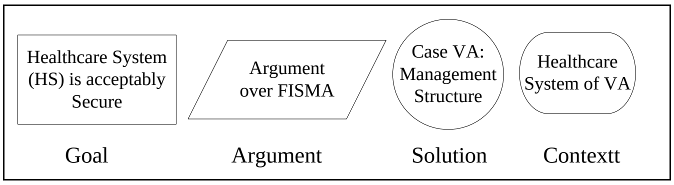
Healthcare System (HS) is acceptably Secure
Argument over FISMA
Case VA: Management Structure
Healthcare System of VA
Goal
Argument
Solution
Contextt

Figure 1: Notations Introduction

Figure 1 shows the core symbols used in GSN. A goal is a claim, the statements that the goal structure is designed to support. Evidence exists to support the truth of the claimed goal which can be documented by providing a solution in GSN. Strategies are inserted between goals at two levels of abstraction, to explain how the top-level goal is addressed by the aggregation of the goals presented at the lower level. Context is used to declare supplementary information and provide adequate understanding of the context surrounding the claim/strategy. Usually it clarifies concepts in the claim/strategy [8].

3 Case Studies and Generic Security Cases

As mentioned in the introduction, this paper draws on the recommendations that were identified following two previous data breaches in US and Chinese healthcare institutions. The findings in each case are used to develop generic security arguments following Kelly's top-down approach to safety-case development [8]. The structure starts with top goal identification, followed by the introduction of context information. The strategies are then identified for providing reasons why the claimed goal is true. The goal structure continues to be developed in this way until it is clear that no further decomposition is needed and the goal can be directly supported by appealing to evidence. In our case studies, the recommendations identified from the incidents are linked to the security objectives and solutions recommended in existing standards, policies and procedures. In the generic security cases, the recommendations from VA case will be linked to General Controls of FISMA [6] and the findings from the Shenzhen (SZ) case will be linked to the security controls of GB/T22239-2008 [7].

3.1 VA Data Loss 2007 [10]

On January 22, 2007, a Veterans Health Administration (VHA) Information Technology (IT) Specialist assigned to the Research Enhancement Award Program (REAP) Birmingham, AL, reported that a VA-owned external hard drive was missing from the REAP office. This was believed to contain numerous research-related files including individually identifiable health information for over 250,000 veterans. The drive also contained data from the Centres for Medicare & Medicaid Services (CMS), Department of Health and Human Services (HHS), on over 1.3 million medical providers.

The investigation of the incident by the VA Office of the Inspector General revealed that the Birmingham REAP managers did not take adequate security measures to protect sensitive data from potential loss or disclosure. External hard drives were purchased with little consideration given to how sensitive data would be secured. Rather than utilize encryption software managers relied on employees not to remove external hard drives from their office and to store them in a safe when not in use. These measures were not adequately monitored by managers to ensure employee compliance.

The IT Specialist was improperly given access to multiple data sources, allowing him to accumulate and store vast amounts of individually identifiable health information that was beyond the scope of the projects he was working on. The local REAP Data Security Plan did not comply with VA policies on data protection by not mandating encryption for portable devices.

The IT Specialist violated the terms and conditions under which the IRB granted HIPAA waivers for the involved protocols. In doing so, the IT Specialist failed to properly safeguard individually identifiable health information, thereby placing vast amounts of HIPAA and Privacy Act protected information at risk.

The report into this incident also makes it clear that the REAP senior managers frequently were not physically present at REAP to supervise daily operations.

Lessons learned and Recommendations

Security Policy, The auditor general's report makes it clear that security policy should ensure personally identifiable information and other sensitive data stored on removable storage devices is encrypted and properly protected. The higher-level aim is to avoid placing data at unnecessary risk of disclosure. Data security plans for research projects should comply with applicable information security policies and privacy policies;

Sensitive Information, The access to the data should comply with policies regarding the release of individually identifiable health information and sensitive information;

Authentication Processes, Policies and Procedures needs to be defined for authorizing access to data for research purposes;

Access Control, Access control should comply with policies regarding the release of individually identifiable health information. Different levels of access control need to be managed carefully, especially when programmer level access is provided for research purposes. Care must be taken when access is project specific or when access continues beyond a single project throughout an individual's term of employment. If necessary, appropriate actions must be taken to remove programmer access from individuals who do not meet the necessary conditions; for example when moving to a new research position;

Position Description, The IT Specialist's role was inaccurately designated as creating a moderate risk of inadvertent disclosure. This was inconsistent with his programmer privileges and resulted in less extensive background investigations. This incident illustrated the need for validation of the risk assessments that are associated with staff recruitment and the subsequent allocation of access privileges for sensitive data;

Administrative Action, The subsequent investigations argued that "appropriate administrative action" should be taken against the people involved in this incident. These concerns not only focused on the problems that led to the data loss but also to problems in the response once the loss had been reported;

Government-wide risk analysis, This data loss affected several Federal Agencies and raised concerns over the need for Government-wide criteria for assessing risk associated with data loss;

Management Structure, A dysfunctional management structure is likely to lead to an overall breakdown of management oversight, controls, and accountability of an organization. This includes the establishment of an accurate functional description and performance plan to clarify managers' responsibilities, the clarification of reporting relationship and line authority over all research programs.

GSN Structure VA Case

According to FISMA, General Controls are the policies and procedures that apply to a large segment of an agency's information systems. These General Controls include Security Management, Access Controls, Configuration Management, Segregation of Duties and Contingency Planning [6]. For each of these five General Controls areas, several critical elements are essential for establishing adequate controls. Figure 2 presents the Generic Security Case created for the Data Loss Incident of VA. The indexes in the goal description link the goals to the corresponding part of security standard items. The word "acceptably" is used because absolute security is unachievable. Individual organizations define their own security criteria on the level of security achievable.

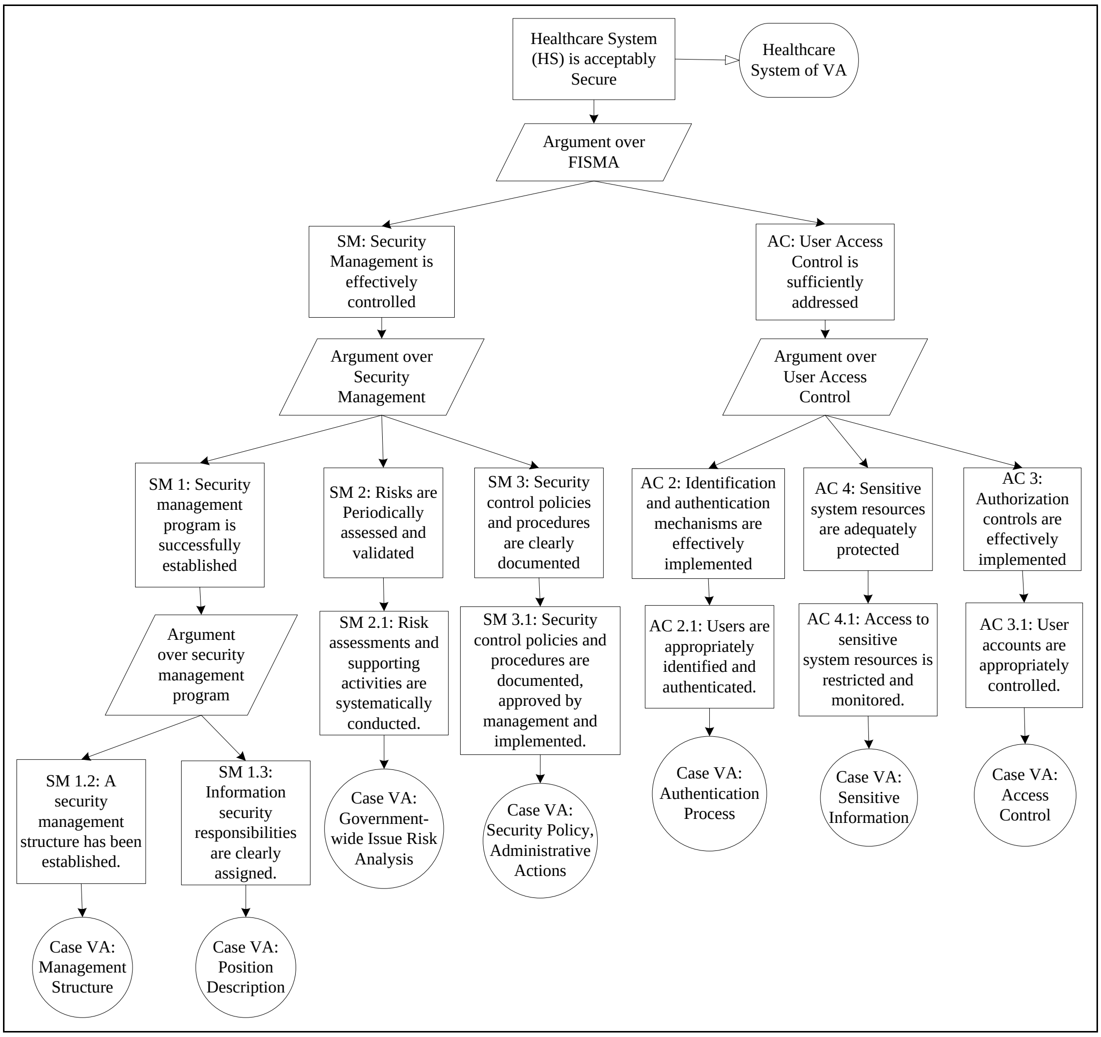
Healthcare System (HS) is acceptably Secure
Healthcare System of VA
Argument over FISMA
SM: Security Management is effectively controlled
AC: User Access Control is sufficiently addressed
Argument over Security Management
Argument over User Access Control
SM 1: Security management program is successfully established
SM 2: Risks are Periodically assessed and validated
SM 3: Security control policies and procedures are clearly documented
AC 2: Identification and authentication mechanisms are effectively implemented
AC 4: Sensitive system resources are adequately protected
AC 3: Authorization controls are effectively implemented
Argument over security management program
SM 2.1: Risk assessments and supporting activities are systematically conducted.
SM 3.1: Security control policies and procedures are documented, approved by management and implemented.
AC 2.1: Users are appropriately identified and authenticated.
AC 4.1: Access to sensitive system resources is restricted and monitored.
AC 3.1: User accounts are appropriately controlled.
SM 1.2: A security management structure has been established.
SM 1.3: Information security responsibilities are clearly assigned.
Case VA: Government-wide Issue Risk Analysis
Case VA: Security Policy, Administrative Actions
Case VA: Authentication Process
Case VA: Sensitive Information
Case VA: Access Control
Case VA: Management Structure
Case VA: Position Description

Figure 2: Generic Security Case of Data Loss Incident of VA

3.2 SZ Data Disclosure 2008 [12]

In 2008, the healthcare information of pregnant women was disclosed from the hospital of city of Shenzhen, China. A cyber-attack was able to compile up to 40, 000 items of healthcare information including pregnant women's name, baby's birth date, home address, mobiles, etc. into disks. This information was updated monthly, adding up to 100, 000 items in total. The information was sold to businesses who were aiming to use it to promote their products immediately after the babies were born. These products included milk, baby sitter services, pregnant women fitness classes, etc through phone calls or messages. The data breach results in a loss of confidential data but also significant distress from the intrusive nature of these marketing activities. The victims recognised that the information available to the marketing teams (names, mobiles, address, estimated birth date, etc.) had been provided for registration in the hospital.

IT professionals in healthcare system analyzed the background and causes of the data disclosure incident. The task was complicated because healthcare information system (HIS) are a relatively new innovation in China. Mangers were focused more on business functionalities rather than system security. The lack of attention on security issues results in the abuse of privileges and illegal connection to the systems. Several issues are identified from this security incident, (1) the security awareness training was not effectively educated. (2) Security policies were not clearly documented. (3) Deficiencies were found in networking security design and the system solely relied on Firewalls and Anti-virus Software. (4) No system security assessment or audit plan was in place.

Lessons learned and Recommendations

Security Policies, including security controls, position responsibility, etc. were not clearly defined. Subsequent enquires recommended that security policy needed to comply with security standards, without which security controls are unlikely to be effectively implemented;

Security Training, the people involved in data disclosure activities has not realized their responsibility of keeping personally identifiable information secure and the fact that they will be responsible for their illegal behaviours. It is recommended that security awareness training needs to be educated regularly;

Sensitive Information Protection, the sensitivity level of the information has not been clearly defined. It is recommended that the sensitivity level of the information needs to be defined in compliance with GB/T22239-2008;

Security Audit and Assessment, there was no system security assessment or audit plan in this case, without which it is hard to identify system vulnerabilities. It is recommended that system security assessment or audit plan needs to be created in compliance with GB/T22239-2008;

Network Security, the network security solely relied on Firewalls and Anti-virus Software. It is recommended that network security control needs to be defined and implemented in compliance with GB/T22239-2008.

GSN Structure SZ Case

According to GB/T22239-2008, there are five classified security levels to ensure information security. Different level of requirement details is provided per different security level. Organizations need to decide which level their systems should be aligned with according to their own security objectives. In this paper, we will use GB/T22239-2008 as baseline foundation for building the Generic Security Case for SZ case. Figure 3 presents the Generic Security Case of Data Disclosure Incident of hospitals in City of Shenzhen.

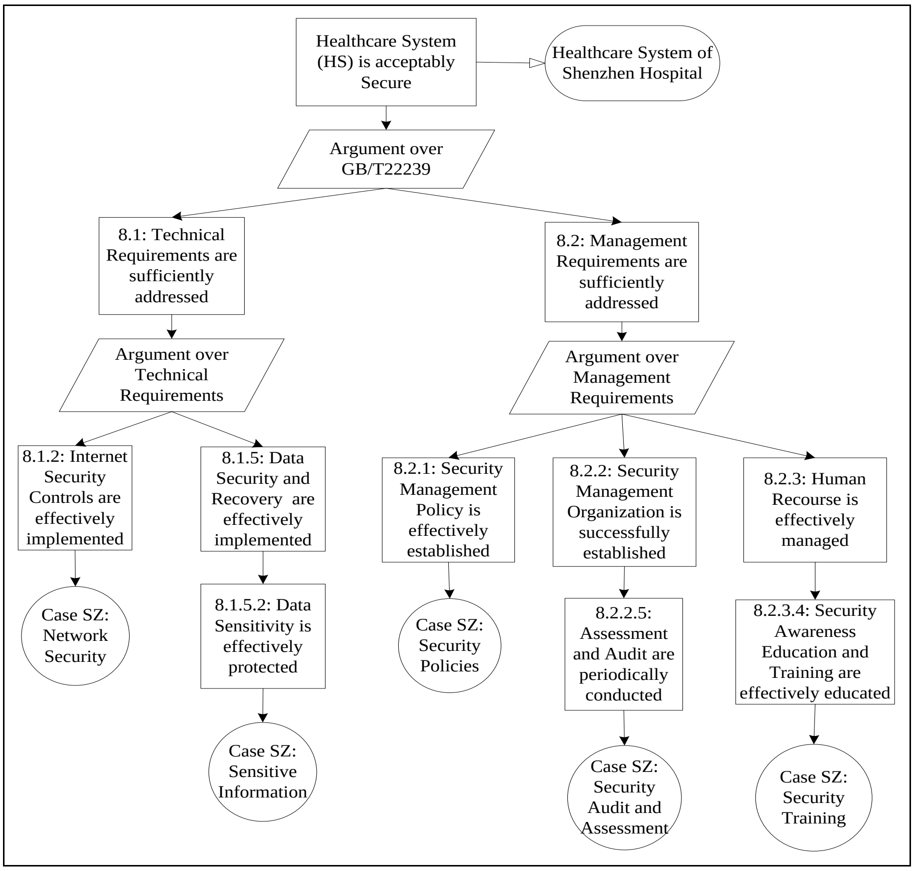
Healthcare System (HS) is acceptably Secure
Healthcare System of Shenzhen Hospital
Argument over GB/T22239
8.1: Technical Requirements are sufficiently addressed
8.2: Management Requirements are sufficiently addressed
Argument over Technical Requirements
Argument over Management Requirements
8.1.2: Internet Security Controls are effectively implemented
8.1.5: Data Security and Recovery are effectively implemented
8.2.1: Security Management Policy is effectively established
8.2.2: Security Management Organization is successfully established
8.2.3: Human Recourse is effectively managed
Case SZ: Network Security
8.1.5.2: Data Sensitivity is effectively protected
Case SZ: Security Policies
8.2.2.5: Assessment and Audit are periodically conducted
8.2.3.4: Security Awareness Education and Training are effectively educated
Case SZ: Sensitive Information
Case SZ: Security Audit and Assessment
Case SZ: Security Training

Figure 3: Generic Security Case of Data Disclosure Incident of hospitals in City of Shenzhen, China.

4 Reusability of Generic Security Cases

Instead of mapping security recommendations to security policies of individual healthcare systems, we link them to security standards that are widely accepted within this industry. Those cases inherent the level of abstraction from the security standards and the feature that can be easily customized and reused in different healthcare organizations. This section argues that insights from previous security incidents can be used to draft generic recommendations for the development and operation of future systems, using GSN.

Scenario 1, for knowledge share. The generic security cases captured the knowledge including security issues. They also identified solutions and security policy concerns. The GSN helped to present key relationships between each of these components of a security argument. The resulting diagrams can be shown to new system security engineers to provide information on how to deal with similar security incidents in the future. A recurring comment in the reports that we have studied is that neither engineers nor managers have time to read the hundreds of pages that document the recommendations from previous security incidents. It is also possible for organizations to edit these diagrams by replacing nodes with their own security issues, recommendations and, standards when these differ from those given in the generic security cases.

Scenario 2, *for system security assessment*. Previous data loss incidents share a number of security issues in common [9]. In consequence, organizations can use generic GSN diagrams to assess their own systems to determine whether or not they might suffer from the same vulnerabilities that have affected similar systems. This will help reduce the chances of repeating the same mistakes in industry.

5 Conclusions

The diversity of products, tools and techniques in the market place make it very hard for management to ensure that they have implemented coherent countermeasures. Generic security cases presented in this paper can help reason about system security by bringing together security standards and evidences that support them in a structured and coherent way. This is the first attempt to extend the Generic Modelling approach from safety area. Two detailed case studies are presented for constructing the generic security cases. Instead of mapping security recommendations to security policies of individual healthcare systems, we link them to security standards that are widely accepted within this industry. The argument structure inherent the level of abstraction from the security standards and the feature that can be easily customized and reused in different organizations. This paper also presents two scenarios where the generic security cases could be reused.

Acknowledgements

This research is funded by China Scholarship Council.

References

[1] "ISO/IEC 27001 Information Security", *ISO/IEC*, (2005).

[2] "The e-Crime Report 2011", *KPMG*, (2011). http://www.kpmg.com/CZ/cs/IssuesAndInsights/Articles Publications/Press-releases/Documents/KPMG_E-Crime-report-2011.pdf.

[3] National Vulnerability Database, http://nvd.nist.gov/, Last visited: 03/07/2012.

[4] "Internal Security Threat Report 2011 Trends", *Symantic Corparation*, Volume 17, (2012).

[5] "Summary of the HIPAA Privacy Rule", *U.S. Department of Health and Human Services, Office for Civil Rights*, (2003).

[6] "FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM)", *United States Government Accountability Office*, (2008).

[7] "GB/T22239—2008 Information Security Technology – base line for classified protection of information system", *AQSIQ/SAC*, (2008).

[8] "DRAFT GSN STANDARD VERSION 1.0", *University of York*, (2010).

[9] "Data Breaches: A Year in Review", *Privacy Rights Clearinghouse*, (2011).

[10] Report No. 07-01083-157, "Administrative Investigation Loss of VA Information VA Medical Center Birmingham, AL", *VA Office of Inspector General*, (2007).

[11] Oxford Dictionary online, Available at: http://english.oxforddictionaries.com/.

[12] China E Healthcare, http://www.chinaehc.cn/index.php?option=com_content &view=article&id=1937:2010-04-01-09-38-35&catid=15:medical-reforming&Itemid=15.

[13] R E Bloomfield, P G Bishop, C C M Jones, P K D Froome. "ASCAD—Adelard Safety Case Development Manual Adelard", (1998).

[14] "Deep Water, The Gulf Oil Disaster and the Future of Offshore Drilling, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling", (2011).

[15] "UK Ministry of Defence Standard 00-56: Safety Management Requirements for Defence Systems", *Crown Copyright 2005*, (2005).

[16] John Goodenough, Howard Lipson, Chuck Weinstock. "Arguing Security - Creating Security Assurance Cases", *Carnegie Mellon University*, (2007).

[17] Tim Kelly. "A Systematic Approach to Safety Case Management", *SAE International*, (2003).

[18] "ISO/IEC 15026-2:2011, Systems and Software Assurance", *ISO/IEC*, (2011).

[19] C. Michael Holloway. "Safety case notations: Alternatives for the non-graphically inclined?" *3rd IET International Conference on System Safety,* The Institutions of Engineering and Technology, Birmingham, UK, (2008).

[20] Robin Bloomfield, Peter Bishop. "Safety and Assurance Cases: Past, Present and Possible Future – an Adelard Perspective", *Making Systems Safer*. Part 2, 51-67, (2010).