Threat Scenario Dependency-Based Model of Information Security Risk Analysis

Basuki Rahmad, Suhono H Supangkat, Jaka Sembiring, Kridanto Surendro

Institut Teknologi Bandung, Indonesia

Summary
Asset dependency paradigm can help us to represent the phenomena of risk dependency on the relevant assets. This paper is aimed to propose the information security risk analysis model, based on the threat-scenario dependency paradigm to represent the asset dependency. Two current approaches of asset dependency representation, threat dependency and security dimension dependency, still have limitations on consistency and the formulation of control's role to reduce the risk. The proposed model can improve the consistency of threats mapping and the control's roles to reduce the likelihood and degradation value of threat.

Key words:
Security Risk Analysis, Threat Scenario Dependency, Bayesian Network.

1. Introduction

Today, IT Risk Management is getting more important [1], as shown by recent survey by ISACA [3]. In general, we can classify the portfolio of IT Risk in project risk, IT Continuity risk, Information Asset risk, vendor & third party risk, application risk, infrastructure risk and strategic risk [2]. But this paper will be focused on the system-level risk: the relation of technical risk (application, infrastructure and facility) and the business risk impacted by the technical risk.

Risk analysis is a part of the risk management cycle, consists of risk identification and risk estimation [4]. We need a security risk management to assure that the risk is mitigated adequately by considering the business needs and organization limitation.

There are several standards/frameworks we can refer as a guidance of information security concepts or information security analysis approach, such as ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, EBIOS, Mehari, Magerit, IT Grundschutz, OCTAVE. We will refer those standards/frameworks in this paper.

In nutshell, current standards/frameworks have provided an adequate guidance on the information security main concepts such as asset, control, threat, vulnerability. Those standards/frameworks also provide several alternatives to analyze an information security risk.

But there are critical limitations in the current approach, especially in the domain of security. First, security terminology is vaguely defined; this leads to confusion among experts as well as the people who should be counseled and served [5]. Second, decisions are often made by managers who do not understand the depth and complexity of the underlying IT infrastructure and therefore base their decisions more on intuition than on a thorough cost/benefit analysis. IT-security personnel are often not involved in the decision making process, and if they are, they have a hard time explaining the complex situation to the decision makers in a proper way [5]. Third, today most companies choose to adapt existing standards than a thorough security threat analysis. That's more practical, though security managers still face the difficulties when they must take a decision based on the several scenarios within the chosen framework [6].

Because of those limitations, information security ontology is proposed. In general, we can classify information security to specific ontology and global ontology. Several previous researches have created specific ontologies in the domain of security, such as Hecker with his privacy ontology [7], Coma with Context Ontology [8] and Vorobiev with his security attack ontology for web services [9]. Global ontologies, provide all security main concepts and its relations, such as Herzog et. al [10] and Ekelhart et. al [11].

Fenz et. al, based on the Ekelhart ontology, then developed an information security analysis approach using Bayesian Network to represent threat to threat dependency [12]. This approach can improve the efficiency of risk management cycle, because all the knowledge of security and IT architecture has been stored in the ontology format.

Next section will discuss more focus in the asset dependency concept for an information security risk analysis.

Manuscript received August 5, 2010
Manuscript revised August 20, 2010

2. Problem Formulation

Asset dependency paradigm can help us to represent the phenomena of risk dependency on the relevant assets. Most standards/frameworks represent the final risk at the threat level where those threats assumed independent each other. This approach has a limitation to capture the real world phenomena of asset dependency. For example, we have a data center wherein we have several servers running several business applications. If our data center is damage, say because of earthquake, all hardware there have a damage potential too. If our servers attacked by denial of service, for example, their availability will effect to the business application availability.

Fenz et al in [12] propose the threat dependency, as illustrated in Fig.1.

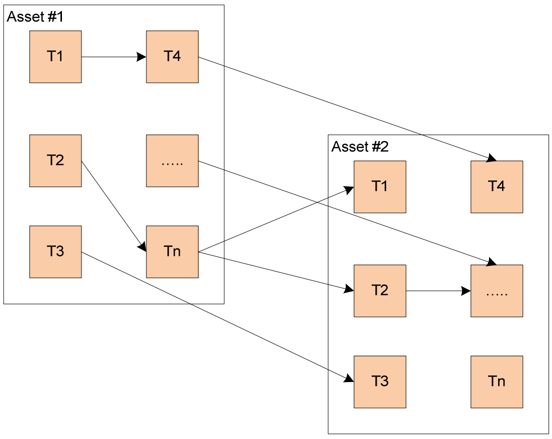

Fig. 1 Fenz: Threat dependency

Then based on the threat dependency, Fenz et al proposed threat probability determination using Bayesian Network, as illustrated in Fig.2..

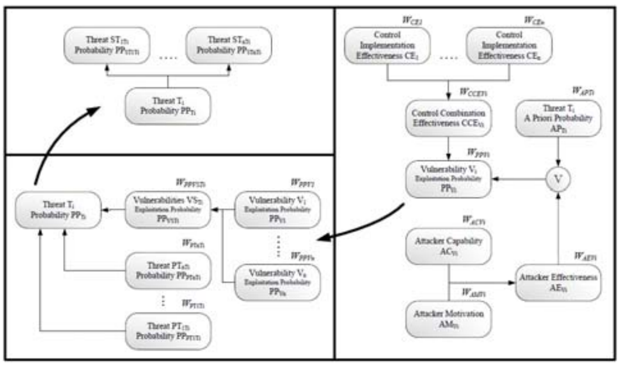

Fig. 2 Fenz: Threat probability determination

Though the threat dependency-based approach provides an alternative of asset dependency in the perspective of asset, but it still has limitations.

1. Threat valuation still limited on likelihood
2. There is no pattern can be used for threats mapping. So if we face a different IT Architecture context, we have a potential of human error on it.

In the different perspective, Magerit provides the security dimension (such as Confidentiality, Integrity, Availability) dependency between relevant assets, as an alternative of asset dependency [13] [14]. Magerit is the only one of standards/frameworks that has a asset dependency concept. The asset dependency concept in Magerit is managed the asset layer relationship as illustrated in Fig.3.

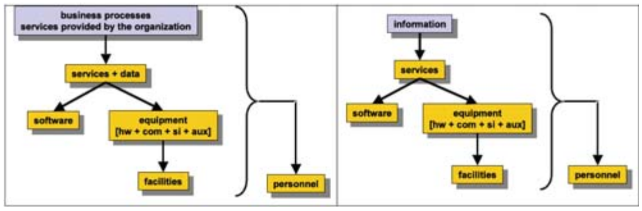

Fig. 3 Magerit Asset Layering Dependency

Based on the asset layer relationship, the security dimension dependency between two assets can be illustrated in Fig. 4.

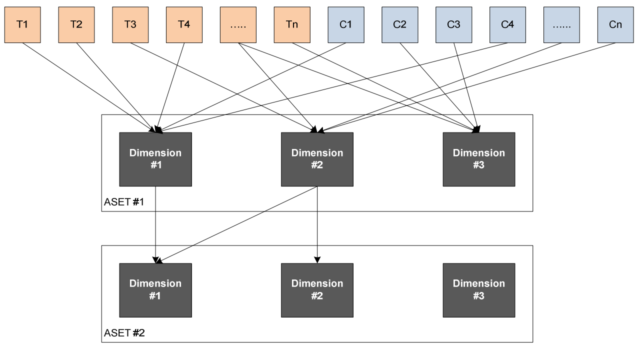

Fig. 4 Magerit Security Dimension Dependency

Magerit's security dimension dependency offer more simple approach, but still has two limitations:

1. Threat identification for each security dimension has a "over-valued" or "under-valued" of degradation value, because it decided by an assesor justification. This can be happen because Magerit doesn't provide the pattern to classify threat based-on its degradation level to security dimension.

2. Magerit doesn't differentiate clearly what control types can reduce the likelihood of threat and what control types can reduce the degradation of threat, though Magerit in its method [13] has stated that two roles of controls.

In nutshell, though the threat dependency and the security dimension dependency have provide a significant contribution in the asset dependency paradigm in security risk analysis, there are still potential problems in consistency, miss-valued of threat and the role of controls.

3. Main Concept References

Before we discuss the proposed model, this section will give a brief explanation about the main concepts used in the proposed model: asset, threat and control.

3.1 Assets

The concept of asset represents entities involved in the information system operation. We refer ISO/IEC 27005 [4] and Mehari knowledge-base [15] to develop the asset catalogue as illustrated in Table 1.

Table 1: Asset Catalogue

CODE	DESCRIPTION
BP	Business Processes
SW	Software
SW.BAP	Business Application: Industry specific solution of standard package
SW.DBMS	System management database
SW.MD	Middleware or package system that facilitate the integration between business applications
DI	Data & Information
DI.DB	Data & Information managed by DBMS
DI.FLSVR	Data & Information as a file server and not managed by DBMS
DI.MED	Media to store data/information
HW	Hardware
HW.SVR	Servers (including its system software)
HW.STO	Storage (including its system software)
HW.WS	Workstation (including its system software)
HW.NW	Network hardware (including its system software)
COM	Communication Network
COM.LAN	Local Area Network (LAN)
COM.EXN	Extended Network, connects LAN to the wider communication network (WAN, MAN, Internet, etc)
AUX	Auxiliary equipments
AUX.HVAC	HVAC system (*Heating, Ventilating, Air Conditioning*)
AUX.PWR	Electrical power source
AUX.CBL	Telecommunication and electrical cabling
PHY	Physical Facility
PHY.DC	Data Center or Disaster Recovery Center
PHY.WR	Working room
PER	Personnel
PER.USR	User personels that operate information system
PER.CST	IT Staff user that conduct a information system custodian or technical support

3.2 Threats

In this paper we use a threat catalogue as illustrated in Table 2. This catalogue is a combination of Magerit [14] and ISO/IEC 27005 [4].

Table 2: Threat Catalogue

CODE	DESCRIPTION
Natural	
N1	Fire
N2	Flood
N3	Lightning
N4	Seismic phenomena
N5	Volcanic phenomena
N6	Storm/hurricane
Environmental or Technical Failure	
ET1	Water damage
ET2	Electromagnetic interference from device
ET3	Industrial electromagnetic explosion
ET4	Short Circuit
ET5	Power failure
ET6	Pollution
ET7	Hardware failure
ET8	Network failure
ET9	Software failure
ET10	Unsuitable temperature or/and humidity conditions
ET11	Media degradation
ET12	HVAC failure
Human Accidental	
HA1	User's error
HA2	Administrator's error
HA3	Configuration Error
HA4	Organizational deficiencies
HA5	Malware diffusion
HA6	[Re]-routing error
HA7	Sequence error
HA8	Information leaks
HA9	Information modification
HA10	Incorrect information entry
HA11	Information degradation
HA12	Destruction of information
HA13	Disclosure of information
HA14	Bug on software
HA15	Defects in software maintenance or updating
HA16	Defects in hardware maintenance
HA17	Defects in network maintenance
HA18	System failure due to exhaustion of resources
HA19	Staff shortage
Human Deliberate (malicious)	
HD1	Spying by a foreign state or a mafia (using important resources)

HD2	Vandalism from outside: bullets or objects thrown from the street, etc.
HD3	Vandalism from inside: by people authorized within the premises (personnel, sub-contractor, etc.).
HD4	Terrorism: sabotage, explosives left close to sensitive premises
HD5	Hardware theft
HD6	Network equipment theft
HD7	Malicious erasure of networking configurations
HD8	Malicious erasure of hardware configurations
HD9	Saturation of the network caused by a worm
HD10	Malicious and repeated saturation of IT resources by a group of users
HD11	Distorted data entry or fiddling of data
HD12	Intentional erasure (direct or indirect), theft or destruction of program or data containers
HD13	Intended access to data or information and disclosure of information
HD14	Document or media theft
HD15	Malicious erasure (directly or indirectly) of software on its storage
HD16	Malicious modification (direct or indirect) of the functionalities of a program or of the operation of an office program (Excel, Access, etc)
HD17	Illegal usage of software
HD18	Intrusion to system by third party whose contract with organization
HD19	Malicious erasure of software configurations
HD20	Absence or strike of IT operational personnel
HD21	Masquerading of user identity
HD22	Abuse of access privileges
HD23	Software misuse
HD24	Hardware misuse
HD25	Network misuse
HD26	Document misuse
HD27	Malware diffusion
HD28	[Re]-routing message
HD29	Sequence alteration
HD30	Unauthorized access
HD31	Traffic analysis
HD32	Eavesdropping
HD33	Software manipulation
HD34	Denial of service
HD35	Extortion
HD36	Social engineering

For every threat we define the likelihood value. This value represent represents two intrinsic values, the likelihood of threat occurrence and the likelihood of exploitation scale to information security dimension.

3.5 Controls

To improve the role of control, we refer Mehari's control types [15]. The combination of control types to threat value reduction is illustrated in Table

Table 3: Control's role to Threat Reduction

Control Type	Threat Likelihood Reduction	Threat Degradation Reduction
Preventive	X	
Dissuasive	X	
Protection		X
Palliative		X
Recuperative		X

In this research, we refer the control catalogue provided by ISO/IEC [16] [17]. Each control is mapped to above control types.

4. Proposed Model

4.1 The Concept of Threat Scenario

As a base of our model, we propose the concept of threat scenario. The rationale of this concept is that all threats can be classified based on its characteristic of attack. We adopt the attack type classification of EBIOS [18] to construct our threat scenario concept. Table 4 illustrates six attack classifications of EBIOS.

Table 4: EBIOS Threat Attack Type

Threat Scenario		Description
USG	the hijacking of uses	goods are diverted from their media framework User rating (use of features available, planned or permitted) without being altered or damaged;
ESP	espionage	goods carriers are observed, with or without equipment further, without being damaged
EXD	exceeded limits of operation	goods carriers are overloaded or used beyond their limits of operation
DMG	damage	the goods are damaged materials, partially or completely, temporarily or permanently;
MOD	modifications	goods are processed materials
LOP	loss of property	goods carriers are insane (lost, stolen, sold, given ...) without being altered or damaged, so it is possible exercise property rights.

4.2 Threat Scenario Dependency

We also propose threat scenario dependency, consists of threat scenario – security dimension dependency, threat scenario – threat scenario dependency (represent asset dependency) and threat scenario – threat dependency, as illustrated in Tabel 5, 6 and 7.

Table 5: Threat Scenario – Security Dimension

ASET	Threat Scenario	Security Dimension		
		C	I	A
Business Process	USG	X	X	X
	ESP	X		
	EXD			X
	DMG		X	X
	MOD	X	X	X
	LOP			X
Software	USG	X	X	X
	ESP	X		
	EXD			X
	DMG			X
	MOD	X	X	X
	LOP	X		X
Data (DB & FLSVR)	USG	X	X	X
	ESP	X		
	DMG		X	X
	MOD		X	
	LOP	X		X
Data (MED)	USG	X	X	X
	ESP	X		
	DMG			X
	LOP	X		X
Hardware	USG	X	X	X
	ESP	X		
	EXD			X
	DMG			X
	MOD	X	X	X
	LOP	X		X
Network	USG	X	X	X
	ESP	X		
	EXD			X
	DMG			X
	MOD	X	X	X
	LOP	X		X
Auxiliary Equipment	EXD			X
	DMG			X
Physical Facility	DMG			X
Personnel	USG			X
	ESP	X		
	EXD		X	X
	DMG			X
	LOP	X		X

Threat scenario – threat scenario dependency can be used to represent asset dependency in more generic pattern compared to threat dependency (by Fenz et al) and security dimension dependency (by Magerit).

Table 6: Threat Scenario – Threat Scenario

Threat Scenario	Depend on	
	Same layer	Other layer
Business Process		
BP.USG	-	PER.USR.USG SW.BAP.USG DI.DB.USG DI.FLSVR.USG DI.MED.USG COM.LAN.USG COM.EXN.USG
BP.ESP	-	PER.USR.ESP SW.BAP. ESP DI.DB. ESP DI.FLSVR. ESP DI.MED. ESP COM.LAN. ESP COM.EXN. ESP
BP.EXD	-	PER.USR.EXD SW.BAP.EXD COM.LAN.EXD COM.EXN.EXD
BP.DMG	-	PER.USR.DMG SW.BAP. DMG DI.DB. DMG DI.FLSVR. DMG DI.MED. DMG COM.LAN. DMG COM.EXN. DMG
BP.MOD	-	SW.BAP. MOD DI.DB. MOD DI.FLSVR. MOD COM.LAN. MOD COM.EXN. MOD
BP.LOP	-	PER.USR.LOP SW.BAP. LOP DI.DB. LOP DI.FLSVR. LOP DI.MED. LOP COM.LAN. LOP COM.EXN. LOP
Data & Information		
DI.DB.USG	-	SW.DBMS.USG HW. STO.USG
DI.DB.ESP	-	SW.DBMS. ESP HW. STO. ESP
DI.DB.DMG	-	SW.DBMS. DMG HW. STO. DMG
DI.DB.MOD	-	SW.DBMS. MOD HW. STO.MOD
DI.DB.LOP	-	SW.DBMS. LOP HW. STO. LOP
DI.FLSVR.USG	-	PER.USR.USG PER.CST.USG HW. STO.USG
DI.FLSVR.ESP	-	PER.USR.ESP PER.CST.ESP HW. STO.ESP
DI.FLSVR.DMG	-	HW. STO.DMG
DI.FLSVR.MOD	-	PER.USR.EXD PER.CST.EXD HW. STO.MOD
DI.FLSVR.LOP	-	HW. STO.LOP
DI.MED.USG	-	PER.CST.USG
DI.MED.ESP	-	PER.CST.ESP
DI.MED.DMG	-	PHY.DC.DMG
DI.MED.LOP	-	-
Software		
SW.BAP.USG	SW. MD.USG	HW.SVR.USG PER.CST.USG PER.USR.USG
SW.BAP.ESP	SW. MD.ESP	HW.SVR.ESP PER.CST.ESP PER.USR.ESP
SW.BAP.EXD	SW. MD.EXD	HW.SVR.EXD
SW.BAP.DMG	SW. MD.DMG	HW.SVR.DMG

Threat Scenario	Depend on	
	Same layer	Other layer
SW.BAP.MOD	SW. MD.MOD	HW.SVR.MOD
SW.BAP.LOP	SW. MD.LOP	HW.SVR.LOP
SW. DBMS.USG	SW.BAP.USG	HW.STO.USG PER.CST.USG
SW. DBMS.ESP	SW.BAP.ESP	HW.STO.ESP PER.CST.ESP
SW. DBMS.EXD	SW.BAP.EXD	HW.STO.EXD
SW. DBMS.DMG	SW.BAP.DMG	HW.STO.DMG
SW. DBMS.MOD	SW.BAP.MOD	HW.STO.MOD
SW. DBMS.LOP	SW.BAP.LOP	HW. STO.LOP
SW. MD.USG	-	HW.SVR.USG PER.CST.USG
SW. MD.ESP	-	HW.SVR.ESP PER.CST.ESP
SW. MD.EXD	-	HW.SVR.EXD
SW. MD.DMG	-	HW.SVR.DMG
SW. MD.MOD	-	HW.SVR.MOD
SW. MD.LOP	-	HW.SVR.LOP
Communication Network		
COM.LAN.USG	-	PER.CST.USG HW.NW.USG
COM.LAN.ESP	-	PER.CST.ESP HW.NW.ESP
COM.LAN.EXD	-	HW.NW.EXD PER.CST.EXD PER.CST.DMG PER.CST.LOP
COM.LAN.DMG	-	HW.NW.DMG
COM.LAN.MOD	-	HW.NW.MOD
COM.LAN.LOP	-	HW.NW.LOP
COM.EXN.USG	-	PER.CST.USG HW.NW.USG
COM.EXN.ESP	-	PER.CST.ESP HW.NW.ESP
COM.EXN.EXD	-	HW.NW.EXD PER.CST.EXD PER.CST.DMG PER.CST.LOP
COM.EXN.DMG	-	HW.NW.DMG
COM.EXN.MOD	-	HW.NW.MOD
COM.EXN.LOP	-	HW.NW.LOP
Hardware		
HW.SVR.USG	-	PER.CST.USG
HW.SVR.ESP	HW.NW.ESP	PER.CST.ESP
HW.SVR.EXD	-	AUX.HVAC.EXD AUX.HVAC.DMG AUX.PWR.EXD AUX.PWR.DMG AUX.CBL.EXD AUX.CBL.DMG PER.CST.EXD PER.CST.DMG PER.CST.LOP
HW.SVR.DMG	-	PHY.DC.DMG
HW.SVR.MOD	-	-
HW.SVR.LOP	-	-
HW. STO.USG	-	PER.CST.USG
HW. STO.ESP	HW.NW.ESP	PER.CST.ESP
HW. STO.EXD	-	AUX.HVAC.EXD AUX.HVAC.DMG AUX.PWR.EXD AUX.PWR.DMG AUX.CBL.EXD AUX.CBL.DMG PER.CST.EXD PER.CST.DMG PER.CST.LOP
HW. STO.DMG	-	PHY.DC.DMG
HW. STO.MOD	-	-
HW. STO.LOP	-	-
HW.NW.USG	-	PER.CST.USG
HW.NW.ESP	-	PER.CST.ESP
HW.NW.EXD	-	AUX.HVAC.EXD AUX.HVAC.DMG AUX.PWR.EXD AUX.PWR.DMG AUX.CBL.EXD AUX.CBL.DMG PER.CST.EXD PER.CST.DMG PER.CST.LOP
HW.NW.DMG	-	PHY.DC.DMG
HW.NW.MOD	-	-
HW.NW.LOP	-	-
HW.WS.USG	-	PER.USR.USG
HW.WS.ESP	HW.NW.ESP	PHY.USR.ESP
HW.WS.EXD	-	AUX.HVAC.EXD AUX.HVAC.DMG AUX.PWR.EXD AUX.PWR.DMG AUX.CBL.EXD AUX.CBL.DMG PER.CST.EXD PER.CST.DMG PER.CST.LOP
HW.WS.DMG	-	PHY.WR.DMG
HW.WS.MOD	-	-
HW.WS.LOP	-	-
Auxiliary Equip.		
AUX.HVAC.EXD	-	PER.CST.EXD PER.CST.DMG PER.CST.LOP
AUX.HVAC.DMG	-	PHY.DC.DMG
AUX.PWR.EXD	-	PER.CST.EXD PER.CST.DMG PER.CST.LOP
AUX.PWR.DMG	-	PHY.DC.DMG
AUX.CBL.EXD	-	PER.CST.EXD PER.CST.DMG PER.CST.LOP
AUX.CBL.DMG	-	PHY.DC.DMG PHY.WR.DMG
Physical Facility		
PHY.DC.DMG	-	-
PHY.WR.DMG	-	-
Personnel		
PER.USR.USG	-	-
PER.USR.ESP	-	HW.WS.ESP
PER.USR.EXD	-	PHY.WR.DMG
PER.USR.DMG	-	-
PER.USR.LOP	-	-
PER.CST.USG	-	-
PER.CST.ESP	-	HW.WS.ESP
PER.CST.EXD	-	PHY.WR.DMG
PER.CST.DMG	-	-

Threat Scenario	Depend on	
	Same layer	Other layer
PER.CST.LOP	-	-

Threat scenario – threat dependency is important because the value of threats will determine the value of threat scenario.

Table 7: Threat Scenario – Threat

Asset	TSC	Threat			
		N	ET	HA	HD
Business Process	USG	-			
	ESP				
	EXD				
	DMG				
	MOD				
	LOP				
Software	USG			HA6, HA7, HA8	HD17, HD21, HD22, HD23, HD30
	ESP				HD1, HD32
	EXD		ET9	HA14, HA15	
	DMG			HA5	HD3, HD27
	MOD			HA2, HA3, HA15	HD16, HD19, HD28, HD29, HD33
	LOP				HD15
Data (DB & FLSVR)	USG			HA8, HA13	HD13
	ESP				HD1, HD32
	DMG			HA5, HA12	HD3, HD12
	MOD			HA1, HA9, HA10	HD11
	LOP				
Data (MED)	USG			HA8, HA13	HD13, HD26
	ESP				HD1
	DMG	N1, N2	ET1, ET10, ET11	HA9, HA11, HA12	HD3, HD4, HD12
	LOP				HD14
Hardware (SVR, STO, WS)	USG				HD21, HD22, HD24, HD30
	ESP			HA18	HD1, HD32
	EXD		ET10	HA5, HA16	HD10, HD34
	DMG	N1, N3	ET6		HD3, HD4
	MOD			HA2, HA3, HA16	HD8, HD18, HD27
	LOP				HD5
Hardware (NW)	USG				HD21, HD22, HD24, HD30
	ESP			HA18	HD1, HD32
	EXD		ET10	HA5	HD10, HD34
	DMG	N1, N3	ET6		HD3, HD4
	MOD			HA2, HA3, HA16	HD8, HD18, HD27
	LOP				HD6
Communication Network	USG			HA6, HA7, HA8	HD21, HD22, HD25, HD30
	ESP				HD1, HD31, HD32
	EXD		ET8	HA5, HA18	HD9, HD10, HD34
	DMG				HD3, HD4, HD27
	MOD			HA17	HD28, HD29
	LOP				
Auxiliary Equipment	EXD		ET5, ET12		
	DMG	N1, N2, N3, N4, N5, N6	ET1, ET2, ET3, ET4		HD2, HD3, HD4
Physical Facility	DMG	N1, N2, N3, N4, N5, N6	ET1, ET2, ET3, ET4		HD2, HD3, HD4
Personnel	USG				HD21, HD22, HD35
	ESP				HD1, HD36
	EXD		ET10	HA4	
	DMG	N1, N2, N4, N5, N6			HD4
	LOP			HA19	HD20

Three dependency patterns will be used as a base of a proposed model, discussed in the next section.

4.3 Proposed Model

Our proposed model is illustrated in Fig 5. This model will be represented in the probability statement of Bayesian Network.

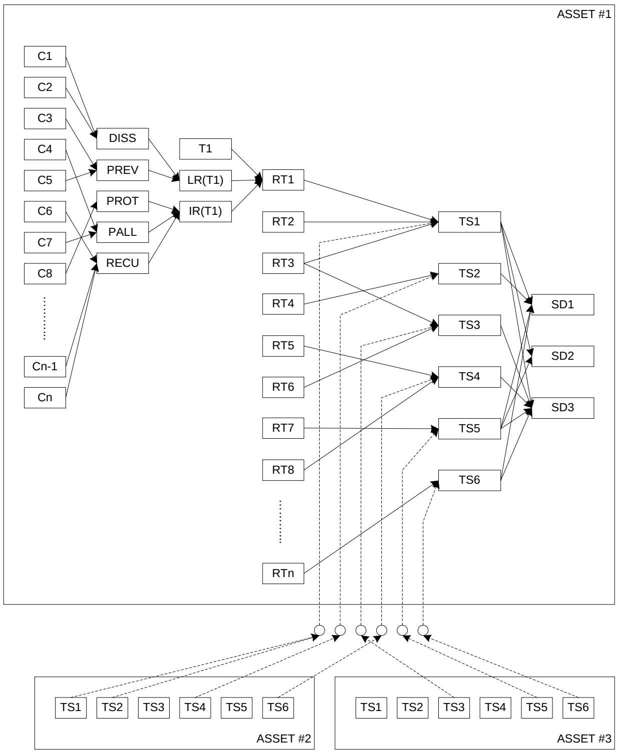

Fig. 5 Conceptual Model

Where,

- SD_i : Information security dimension {Confidentiality, Integrity, Availability}
- TS_i : threat-scenario
- RT_i : reduced-Threat
- T_i : Threat
- LR (T_i) : Control combination effectiveness for Threat likelihood-factor reduction
- IR (T_i) : Control combination effectiveness for Threat impact-factor reduction
- DISS : Control combination effectiveness for dissuasive controls
- PREV : Control combination effectiveness for Preventive controls
- PROT : Control combination effectiveness for protective controls
- PALL : Control combination effectiveness for palliative controls
- RECU : Control combination effectiveness for recuperative controls
- C_i : Single control effectiveness

It is assumed that the risk has a finite set of probability status (expressed as a vector of probability distribution [high, medium, low]). Because of the vector expression of risk, all relevant variables (threat scenario, threat, control) are also expressed in probability distribution vector.

4.3.1 Risk on the Information Security Dimension

The information security dimension risk is a function of its accumulated potential of exploitation and its value, expressed below:

$$P(\vec{R}_{SD_i}) = P(\overrightarrow{SD}_{SD_i}) * P(\vec{V}_{SD_i}) \qquad (1)$$

Where $P(\vec{R}_{SD_i})$ is a probability of the information security dimension risk, $P(\overrightarrow{SD}_{SD_i})$ is a probability of information security dimension being exploited and $P(\vec{V}_{SD_i})$ is a value of the information security dimension.

The probability of information security dimension being exploited $P(\overrightarrow{SD}_{SD_i})$ is a function of the relevant threat-scenarios, represented as a conditional probability as below:

$$P(\overrightarrow{SD}_{SD_i}) = P(\overrightarrow{SD}_{SD_i} | \overrightarrow{TS}_{1_{SD_i}} \ldots \overrightarrow{TS}_{n_{SD_i}}) \qquad (2)$$

Where $\overrightarrow{TS}_{1_{SD_i}}$ are relevant threat-scenarios to the information securitydimension.

4.3.2 Probability of Threat-Scenario

As can be shown from the Fig.5, the probability of threat-scenario is a function of relevant other threat-scenarios and relevant reduced-threats. To make easier the understanding, we use two additional nodes for calculation: reduced-threat combination and relevant threat-scenario combination.

$$P(\overrightarrow{TS}_i) = P(\overrightarrow{TS}_i | \overrightarrow{CTR}_{TS_i}, \overrightarrow{CTS}_{TS_i}) \qquad (3)$$

Where $P(\overrightarrow{TS}_i)$ is probability of threat-scenario, $\overrightarrow{CTR}_{TS_i}$ is a combination of relevant reduced-threats to threat-scenario $\overrightarrow{TS}_i$ and $\overrightarrow{CTS}_{TS_i}$ is a combination of relevant threat-scenarios to threat-scenario $\overrightarrow{TS}_i$.

The combination of reduced-threats to threat-scenario $\overrightarrow{TS}_i$ is a function of relevant reduced-threats, as expressed in the conditional probability below:

$$P(\overrightarrow{CTS}_{TS_i}) = P(\overrightarrow{CTS}_{TS_i} | \overrightarrow{TS}_{1TS_i} \ldots \overrightarrow{TS}_{nTS_i}) \qquad (4)$$

Where $(\overrightarrow{TS}_{1TS_i} \ldots \overrightarrow{TS}_{nTS_i})$ is a threat-scenario list of relevant assets. And the combination of reduced-threats is a function of relevant reduced-threats, as expressed in the conditional probability below:

$$P(\overline{CTR}_{TS_i}) = P(\overline{CTR}_{TS_i} | \overline{TR}_{1TS_i} \dots \overline{TR}_{nTS_i}) \qquad (5)$$

Where $(\overline{TR}_{1TS_i} \dots \overline{TR}_{nTS_i})$ is a relevant reduced-threat list to threat-scenario TS_i.

4.3.3 Probability of Reduced-Threat

Reduction of Threat can be divided on two types: reduction of likelihood-factor and reduction of exploitation-factor that can cause the impact on asset's value. Because of this reason, the probability of reduced-threat can be expressed below:

$$P(\overline{RT}_i) = P(\overline{T}_i) * (1 - P(\overline{LR}_{Ti})) * (1 - P(\overline{IR}_{Ti})) \qquad (6)$$

Where $P(\overline{RT}_i)$ is a probability of reduced-threat, $P(\overline{T}_i)$ is a probability of threat before reduced, $P(\overline{LR}_{Ti})$ is a probability of control combination effectiveness to reduce the likelihood-factor and $P(\overline{IR}_{Ti})$ is a probability of control combination effectiveness to reduce the exploitation-factor.

By this proposed approach, it's possible to express the influence of the low effectiveness of control, though the probability of threat is very high. This approach also can be used as an alternative of the positive and positive-negative point scale used to express the role of effectiveness to threat, as implemented by Fenz [19].

4.3.4 Control Combination Effectiveness

Control combination effectiveness for likelihood reduction will be determined by the effectiveness of controls whose *Dissuasive* and *Preventive* type. Probability of T_i likelihood reduction is a function of control combination effectiveness of *Dissuasive* control type and *Preventive* control type.

$$P(\overline{LR}_{Ti}) = \frac{\alpha_1 * P(\overline{DISS}_{Ti}) + \alpha_2 * P(\overline{PREV}_{Ti})}{\alpha_1 + \alpha_2} \qquad (7)$$

Where $P(\overline{DISS}_{Ti})$ is a control combination effectiveness of relevant dissuasive controls and $P(\overline{PREV}_{Ti})$ is a control combination effectiveness of relevant preventive controls.

We have weighted values for *Dissuasive* and *Preventive.* In our opinion, the role of *Preventive* to reduce the threat likelihood value is bigger than *Dissuasive* because *Preventive* controls can prevent the threat event directly where *Dissuasive* control type is aimed to increase the risk perspective if threat happens. Because of this reason, we propose the ratio of weighting α_1: α_2=1:2.

Control combination effectiveness for exploitation-factor reduction will be determined by the effectiveness of controls whose *Protective, Palliative* and *Recuperative* type.

$$P(\overline{IR}_{Ti}) = \frac{\beta_1 * P(\overline{PROT}_{Ti}) + \beta_2 * P(\overline{PALL}_{Ti}) + \beta_3 * P(\overline{RECU}_{Ti})}{\beta_1 + \beta_2 + \beta_3} \qquad (8)$$

Protective controls are aimed to limit or detect the degradation before that degradation propagates. Palliative and recuperative controls are aimed to restore the loss because of degradation. By considering the magnitude of impact reduced, we propose the ratio of weighting β_1:β_2:β_3=1:2:2.

Control combination effectiveness of each type can be expressed as a conditional probability of relevant controls, as shown below:

$$P(\overline{DISS}_{Ti}) = P(\overline{DISS}_{Ti} | \vec{C}_{1Ti} \dots \vec{C}_{nTi}) \qquad (9)$$

$$P(\overline{PREV}_{Ti}) = P(\overline{PREV}_{Ti} | \vec{C}_{1Ti} \dots \vec{C}_{nTi}) \qquad (10)$$

$$P(\overline{PREV}_{Ti}) = P(\overline{PREV}_{Ti} | \vec{C}_{1Ti} \dots \vec{C}_{nTi}) \qquad (11)$$

$$P(\overline{PALL}_{Ti}) = P(\overline{PALL}_{Ti} | \vec{C}_{1Ti} \dots \vec{C}_{nTi}) \qquad (12)$$

$$P(\overline{RECU}_{Ti}) = P(\overline{RECU}_{Ti} | \vec{C}_{1Ti} \dots \vec{C}_{nTi}) \qquad (13)$$

Where $(\vec{C}_{1Ti} \dots \vec{C}_{nTi})$ are relevant controls for every control types.

5. Comparison to other approaches

Based on the above explanation, we can summarize the comparison of the proposed model to the other relevant approaches as shown in the table below:

ITEMS COMPARED	ISO/IEC 27005	EBIOS	Mehari	Magerit	IT Grundschutz	Fenz et al	PROPOSED MODEL
Knowledge-base							
- Asset		X	X	X	X	X	X
- Safeguard/Control		X	X	X	X	X	X
- Threat		X	X	X	X	X	X
- Vulnerability						X	
Asset Dependency Approach							
- Threat Dependency						X	

- Threat-Scenario Depend.							X
- Dimension dependency				X			
Risk Analysis Approach							
- Control Effectiveness			X	X		X	X
- Likelihood reduction	X	X	X	X	X	X	X
- Impact reduction				X			X
- Bayesian-Network support						X	X

6. Conclusion

Asset dependency can be improved with the concept of threat scenario dependency. The existence of generic pattern (threat scenario – security dimension dependency, threat scenario – threat scenario dependency and threat scenario – threat dependency) can be used as a guidance when modeling the IT Architecture and analyze threats, so the human error potential can be reduced.

The proposed model also can improve the accuracy of risk measured because the model provides the control's role more explicitly.

References

[1] Basel Committee of Banking Supervision, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework", Bank for International Settlement, 2004

[2] Ernie Jordan and Luke Silcock, "Beating IT Risks", John Wiley & Sons, 2005

[3] ISACA, "Top Business/Technology Issues: Survey Results", ISACA, 2008

[4] *ISO/IEC 27005: Information Technology – Security Techniques – Information Security Risk Management,* ISO/IEC, 2008

[5] M. Donner, "Toward a security ontology," *IEEE Security and Privacy*, vol. 1, no. 3, pp. 6–7, May/June 2003. [Online]. Available: http://dlib.computer.org/sp/books/sp2003/pdf/j3006.pdf

[6] Andreas Ekelhart, Stefan Fenz, Markus Klemen, Edgar Weippl, "Security Ontologies: Improving Quantitative Risk Analysis", *Proceedings of the 40th Hawaii International Conference on System Sciences* (HICSS'07), 2007

[7] Hecker, M., S.Dillon, T., Chang, E. (2008): Privacy Ontology Support for E-Commerce, *IEEE Internet Computing,* pp. 54-61, IEEE Computer Society

[8] Coma, C., Cuppens-Boulahia, N., Cuppens, F., Cavalli, A.N. (2008): Context Ontology for Secure Interoperability, *2008 Third International Conference on Availability, Reliability and Security,* pp. 821-827, IEEE Computer Security

[9] Artem Vorobiev , Jun Han (2006): Security Attack Ontology for Web Services, *Second International Conference on Semantics, Knowledge, and Grid (SKG'06),* pp. 42, IEEE Computer Security

[10] Almut Herzog, Nahid Shahmehri, Claudiu Duma. *An Ontology of Information Security*. International Journal of Information Security and Privacy 1(4). Pages: 1-23. 2007

[11] Andreas Ekelhart, Stefan Fenz, Markus Klemen, Edgar Weippl, "Security Ontologies: Improving Quantitative Risk Analysis", *Proceedings of the 40th Hawaii International Conference on System Sciences* (HICSS'07), 2007

[12] Fenz, S. Ontology- and Bayesian-based Information Security Risk Management. TU Wien Dissertation, 2008

[13] Públicas, M. d. *Magerit Version 2 – Methodology for Information Systems Risk Analysis and Management: I – The Method.* Ministerio de Administraciones Públicas, 2006

[14] Públicas, M. d. *Magerit Version 2 – Methodology for Information Systems Risk Analysis and Management: II – Catalogue of Elements.* Ministerio de Administraciones Públicas, 2006

[15] CLUSIF. *Mehari 2007: Knowledge Base.* CLUSIF, 2007

[16] ISO/IEC. *ISO 27001:2005 - Information Technology - Security Techniques - Information Security Management Systems – Requirement, 2005*

[17] ISO/IEC. *ISO 27002:2005 - Information Technology - Security Techniques - Information Security Management Systems - Code of Practice, 2005*

[18] ANSSI. *EBIOS: Bases de connaissances.* ANSSI, 2010

[19] Fenz, S. *Ontology- and Bayesian-based Information Security Risk Management.* TU Wien Dissertation, 2008

Basuki Rahmad is a PhD student at School of Electrical Engineering & Informatic (STEI), Institut Teknologi Bandung. He obtained his undergraduate and master degree in electrical engineering from STEI – Institut Teknologi Bandung 2000 and 2004 respectively. He also holds professional certification related to information system assurance: CISA and CISM from ISACA.

Suhono H. Supangkat is a professor at STEI, Institut Teknologi Bandung, Indonesia. He obtained his undergraduate degree from STEI – Institut Teknologi Bandung (1986), master degree from Meisei University Tokyo (1994) and Doctoral degree from University of Electro Communications Tokyo (1998). His focus research is in the information assurance, IT Governance, telecommunication policy.

Jaka Sembiring is an associate professor at STEI, Institut Teknologi Bandung, Indonesia. He obtained an undergraduate degree form electrical engineering – Institut Teknologi Bandung, Master and doctoral degree in electrical engineering from Waseda University. His focus research is in signal processing and stochastic systems.

Kridanto Surendro is an associate professor at STEI – Institut Teknologi Bandung, Indonesia. He obtained an undergraduate and master degree from Industrial Engineering, Institut Teknologi Bandung, and doctoral degree in Computer Science from Computer Science, Keio University, Tokyo. His focus reseach is in the information system, IT Governance, IT Risk Management, Strategic IT Plan.