Table 2. The STR Matrix

Conformance	Conformance	40	30	10	20
Secure Information Flow	**Secure Information Flow**	**10**	**10**	**0**	**5**
Freshness	**Freshness**	**5**	**2**	**1**	**1**
Fair Exchange	**Fair Exchange**	**10**	**2**	**0**	**2**
Usability	**Reduce risks**	**20**	**20**	**5**	**5**
	Consistent APTs	**20**	**20**	**10**	**10**
	Available security	**20**	**20**	**1**	**7**
	Manageable security	**30**	**0**	**0**	**10**
Attack/Harm Detection	**Attack/Harm Detection**	**30**	**20**	**0**	**10**
Physical Protection	**Physical Protection**	**20**	**10**	**0**	**10**
Access control	**Authorization**	**10**	**30**	**5**	**5**
	Identification	**10**	**30**	**5**	**5**
	Authentication	**10**	**30**	**5**	**5**
Manageability	**Accountability**	**20**	**10**	**2**	**7**
	Security Auditing	**5**	**0**	**0**	**5**
Availability	**Resource allocation**	**22.5**	**22.5**	**1.5**	**7.5**
	Expiration	**22.5**	**22.5**	**1.5**	**3.75**
	Response time	**15**	**15**	**0.75**	**3.75**
Non-repudiation	**Non-repudiation**	**10**	**20**	**0**	**5**
Integrity	**Software Integrity**	**7.5**	**4.44**	**0.38**	**1.47**
	Personal Integrity	**10**	**6.6**	**1.66**	**2.1**
	Hardware Integrity	**5**	**4.44**	**1.66**	**2.1**
	Data Integrity	**7.5**	**4.44**	**0.83**	**1.05**
Privacy	**Traces**	**3**	**0**	**0**	**1.65**
	Cardinality	**6**	**0**	**0**	**3.3**
	Consent and notification	**1.5**	**0**	**0**	**1**
	Attribution	**12**	**0**	**0**	**0**
	Aggregation	**6**	**0**	**0**	**3.3**
	Encryption	**9**	**17.1**	**5**	**2.31**
	Confidentiality	**40**	**20**	**0**	**10**
	Anonymity	**12**	**22.8**	**0**	**3.3**
Security requirements	**Security Requirements Sub factor/**	**Administrator**	**Teacher**	**Student**	**Technician**
			Stakeholders		

Table 3: The RFC Matrix

Security requirements	Security Requirements Sub factor	Functional Components					
		Virtual library	**Online course admin**	**Course Management**	**Registration**	**Communications tool**	**No failure**
Conformance	Conformance	0	$1.66\ 10^{-3}$	**$3.32\ 10^{-3}$**	0	$1.66\ 10^{-3}$	$9.93\ 10^{-1}$
Secure Information Flow	Secure Information Flow	$4.2\ 10^{-2}$	$4.2\ 10^{-2}$	**$8.4\ 10^{-2}$**	0	$4.2\ 10^{-2}$	$7.9\ 10^{-1}$
Freshness	Freshness	0	$1\ 10^{-3}$	**$2\ 10^{-3}$**	0	$1\ 10^{-3}$	$9.97\ 10^{-1}$
Fair Exchange	Fair Exchange	0	$1\ 10^{-3}$	**$2\ 10^{-3}$**	0	$1\ 10^{-3}$	$9.97\ 10^{-1}$
Usability	Reduce risks	0	0	**0**	$3\ 10^{-3}$	0	$9.97\ 10^{-1}$
	Consistent APTs	$5\ 10^{-4}$	$5\ 10^{-4}$	**$10\ 10^{-4}$**	0	$5\ 10^{-4}$	$9.97\ 10^{-1}$
	Available security	$3\ 10^{-3}$	$3\ 10^{-3}$	**$6\ 10^{-3}$**	$3\ 10^{-3}$	$3\ 10^{-3}$	$9.82\ 10^{-1}$
	Manageable security	0	$3\ 10^{-3}$	**$6\ 10^{-3}$**	$3\ 10^{-3}$	$3\ 10^{-3}$	$9.85\ 10^{-1}$
Attack/Harm Detection	Attack/Harm Detection	0	$24.4\ 10^{-3}$	**$48.8\ 10^{-3}$**	0	$24.4\ 10^{-3}$	$9.024\ 10^{-1}$
Physical Protection	Physical Protection	0	$0.7\ 10^{-3}$	**$1.4\ 10^{-3}$**	$0.7\ 10^{-3}$	$0.7\ 10^{-3}$	$9.965\ 10^{-1}$
Access control	Authorization	0	$4.2\ 10^{-3}$	**8.410^{-3}**	$4.2\ 10^{-3}$	$4.2\ 10^{-3}$	$9.79\ 10^{-1}$
	Identification	0	$4.2\ 10^{-3}$	**8.410^{-3}**	$4.2\ 10^{-3}$	$4.2\ 10^{-3}$	$9.79\ 10^{-1}$
	Authentication	0	$4.2\ 10^{-3}$	**$8.4\ 10^{-3}$**	$4.2\ 10^{-3}$	$4.2\ 10^{-3}$	$9.79\ 10^{-1}$
Manageability	Accountability	$3\ 10^{-3}$	$3\ 10^{-3}$	**$6\ 10^{-3}$**	$3\ 10^{-3}$	$3\ 10^{-3}$	$9.82\ 10^{-1}$
	Security Auditing	$3\ 10^{-3}$	$3\ 10^{-3}$	**610^{-3}**	$3\ 10^{-3}$	$3\ 10^{-3}$	$9.82\ 10^{-1}$
Availability	Resource allocation	0	$3.3\ 10^{-3}$	**$6.6\ 10^{-3}$**	0	$3.3\ 10^{-3}$	$9.868\ 10^{-1}$
	Expiration	$3.3\ 10^{-3}$	$3.3\ 10^{-3}$	**$6.6\ 10^{-3}$**	$3.3\ 10^{-3}$	$3.3\ 10^{-3}$	$9.802\ 10^{-1}$
	Response time	$3.3\ 10^{-3}$	$3.3\ 10^{-3}$	**$6.6\ 10^{-3}$**	$3.3\ 10^{-3}$	$3.3\ 10^{-3}$	$9.802\ 10^{-1}$
Non-repudiation	Non-repudiation	$2\ 10^{-2}$	$3.3\ 10^{-2}$	**$3.3\ 10^{-2}$**	$1\ 10^{-2}$	$3.3\ 10^{-2}$	$8.71\ 10^{-1}$
Integrity	Software Integrity	$7\ 10^{-3}$	$7\ 10^{-3}$	**$14\ 10^{-3}$**	$7\ 10^{-3}$	$7\ 10^{-3}$	$9.58\ 10^{-1}$
	Personal Integrity	0	0	**0**	0	0	1
	Hardware Integrity	0	$7\ 10^{-3}$	**$14\ 10^{-3}$**	$7\ 10^{-3}$	$7\ 10^{-3}$	$9.65\ 10^{-1}$
	Data Integrity	0	$7\ 10^{-3}$	**$14\ 10^{-3}$**	0	$7\ 10^{-3}$	$9.72\ 10^{-1}$
Privacy	Traces	0	0	**0**	$3.33\ 10^{-2}$	0	$9.667\ 10^{-1}$
	Cardinality	0	0	**0**	0	0	1
	Consent and notification	0	0	**0**	0	0	1
	Attribution	0	0	**0**	0	0	1
	Aggregation	0	0	**0**	0	0	1
	Encryption	0	0	**0**	0	0	1
	Confidentiality	$2\ 10^{-2}$	$3.33\ 10^{-2}$	**$8.33\ 10^{-2}$**	$1\ 10^{-1}$	$3.33\ 10^{-2}$	$7.3\ 10^{-1}$
	Anonymity	0	0	**0**	0	0	1

Table 4: The FCT matrix

Threats Components	BroA	InsC	DoS	CryptS	DOR	InfL	Buff	CSRF	CSS	FURL	InjecF	MFile	No Threats
Virtual library	0,000	0,000	0,0195	0,978	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Online course admin	0,090	0,231	0,231	0,000	0,099	0,000	0,066	0,002	0,004	0,140	0,132	0,000	0,000
Course Management	**0,206**	**0,103**	**0,135**	**0,000**	**0,135**	**0,069**	**0,135**	**0,005**	**0,000**	**0,191**	**0,010**	**0,022**	**0,000**
Registration	0,108	0,000	0,235	0,231	0,198	0,000	0,023	0,000	0,000	0,000	0,000	0,000	0,000
Communications tools	0,165	0,000	0,176	0,176	0,132	0,012	0,314	0,003	0,000	0,000	0,008	0,002	0,000
No Failure	0,793	0,769	0,764	0,022	0,802	0,930	0,685	0,994	0,995	0,808	0,868	0,997	1,000

Table 5: The T Vector

Threats	**Probability**
Broken authentication and session management (BroA)	$4.20\ 10^{-3}$
Insecure communication (InsC)	$3.00\ 10^{-3}$
Denial of service (Dos)	$3.08\ 10^{-3}$
Insecure cryptographic storage (CrypS)	$7.00\ 10^{-4}$
Insecure direct object reference (DOR)	$7.00\ 10^{-4}$
Information leakage and improper error handling (InfL)	$7.00\ 10^{-4}$
Buffer overflow (Buff)	$1.00\ 10^{-4}$
Cross Site Request Forgery (CSRF)	$4.20\ 10^{-4}$
Cross Site Scripting (CSS)	$1.80\ 10^{-4}$
Failure to restrict URL access (FURL)	$9.80\ 10^{-3}$
Injection flaws (InjecF)	$2.17\ 10^{-3}$
Malicious file execution (MFile)	$5.04\ 10^{-4}$
No Threats	$974.44\ 10^{-3}$

Table 6: Mean Failure Cost based on an e-learning functional architecture

Stakeholders	**FSRM** for e-learning systems
System administrator	645,162
Teacher	456,572
Student	81,991
Technician	209,429

10 Conclusion

This paper illustrates an original theoretical and practical contribution which is benefic to the top security managers or providers of e-learning systems. Also, it leads to improve and support the knowledge of measurements and risk management for other systems:

We develop a new functional security risk management model (FSRM). It is compatible with the different architectures, implementations and platforms such as (cloud, LMS, web service, mobile technology and MOOC...). This model can be used in common with the variety of implementations and technical specifications. The risk is easily identified, assessed, managed and perceived for one system and between different members' risk management processes. Our functional security risk management model will be also a metric for software verification at the early stages of development of large systems or complex real-time software.

Our Future works focus on developing a functional security risk analysis model for every system's function. It is useful for future empirical reuse and security asset's identification. This information can also be used to provide feedbacks at the modelling layer.

REFERENCES

[1] A. Al-Ajlan and H. Zedan, Why Moodle, 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, IEEE computer society, 2008.

[2] A. B. Aissa, A. Mili, R. K. Abercrombie, and F. T. Sheldon, Modeling Stakeholder/Value Dependency through Mean Failure Cost, Proceedings of 6th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW), ACM International Conference, 2010.

[3] A. B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, Defining and Computing a Value Based Cyber-Security Measure, Information Systems and e-Business Management Volume 10, Issue 4 , pp 433-453 , 2012-12-01, DOI: 10.1007/s10257-011-0177-1, Springer-Verlag, 2012.

[4] A. B. Aissa, Vers une mesure économétrique de la sécurité des systèmes informatiques. Doctoral dissertation, Faculty of Sciences of Tunis, submitted, Spring 2012.

[5] A. Mili and F.T. Sheldon, Measuring Reliability as a Mean Failure Cost, in Proc. HASE, pp.403-404, 2007.

[6] A. Mili, and F. T. Sheldon, Challenging the Mean Time to Failure: Measuring Dependability as a Mean Failure Cost, in Proceedings of 42nd Hawaii International Conference on System Sciences (HICSS-42), Waikoloa, HI, pp. 10, 2009.

[7] A.Tangsuksant, and N. Prompoon, Risk assessment using functional modeling based on object behavior and interaction. In The 4th international Joint Conference on Computer Science and Software Engineering, Khon Kaen, 2007.

[8] B. Karabacak, I. Sogukpinar, ISRAM: information security risk analysis method, Computer and Security, Elsevier. Vol 24, pp. 147-159, 2005.

[9] D. L. Nazareth and J. A. Choi: System Dynamics Model for Information Security Management. Information and Management. Elsevier, 2014.

[10] E. Weippl, Security In E-Learning, eLearn Magazine, Association for Computing Machinery (ACM), article from, vol. 16, p. 03-05, 2005

[11] E.W.T. Ngai, J.K.L. Poon, and Y.H.C. Chan, Empirical examination of the adoption of WebCT using TAM, Computers and Education, Elsevier vol. 48, pp. 250-267, 2007.

[12] F. Alkhateeb, E. AlMaghayreh, S. Aljawarneh, Z. Muhsin, and A. Nsour. E-learning Tools and Technologies in Education: A Perspective. E-learning, 2010.

[13] F. T. Sheldon, R. K. Abercrombie, and A. Mili, Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission, IEEE Proceedings of the 42nd Annual Hawaii International Conference on System Sciences (HICSS-42), (CD-ROM), Waikoloa, Big Island, Hawaii, January 5-8, 2009, Computer Society Press, 2009.

[14] Final Report of Task Group IST-049, Improving Common Security Risk Analysis, 2008.

[15] H. H. Ammar, T. Nikzadeh and J. B. Dugan, A methodology for risk assessment of functional specification of software systems using colored petri nets. In Software Metrics Symposium, 1997 Proceedings Fourth International (pp. 108-117), IEEE, 1997.

[16] H. H. Ammar, T. Nikzadeh and J. B. Dugan, A methodology for risk assessment of functional specification of software systems using colored petri nets. In Software Metrics Symposium, 1997 Proceedings Fourth International (pp. 108-117), IEEE, 1997.

[17] L. B. A. Rabai, N. Rjaibi, and A. B. Aissa, Quantifying Security Threats for E-learning Systems, IEEE Proceedings of International Conference on Education and E-Learning Innovations- Infrastructural Development in Education (ICEELI' 2012- http://www.iceeli.org/index.htm), July 1-3, Sousse, Tunisia, Page 482 487, 2012.

[18] L.Wang, A. Singhal, and S. Jajodia, Toward measuring network security using attack graphs. In Proceedings of the 2007 ACM workshop on Quality of protection (pp. 49-54). ACM, 2007.

[19] M. Colobran, Modeling human perceived security: A conceptual framework and its application to health, Computers in Human Behavior, 2016.

[20] M. Machado, E. Tao, Blackboard vs. Moodle: Comparing User Experience of Learning Management Systems, 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, WI, October 10 13, 2007.

[21] M. Nickolova, E. Nickolov, Threat Model For User Security In E-Learning Systems, International Journal Information Technologies and Knowledge, 1(1), 341-347, 2007.

[22] N. Rjaibi and A. B. Aissa, The empirical data base for quantifying security threats. Retrieved Jan, 2013, from https://docs.google.com/file/d/0B0Z2laATxEo7Tlk2TGd4elJjNFk/Edit

[23] N. Rjaibi and L. B. A. Rabai, Expansion And Practical Implementation of The MFC Cybersecurity Model via a Novel Security Requirements Taxonomy, International Journal of Secure Software Engineering (IJSSE), 6(4), 32-51, October-December 2015.

[24] N. Rjaibi and L. B. A. Rabai, Functional specification to support security risk assessment of large systems, 7th Computer Science On-line Conference 2018 (CSOC 2018), April 25-28, 2018, the Springer Series: Advances in Intelligent Systems and Computing, Springer

[25] N. Rjaibi and L. B. A. Rabai, New classification of Security Requirements for Quantitative Risk Assessment, Analyzing the Role of Risk Mitigation and Monitoring in Software Development, IGI Global, Analyzing the Role of Risk Mitigation and Monitoring in Software Development. IGI Global, 2018. 100-117. Web. 20 Jun. 2018. doi:10.4018/978-1-5225-6029-6.ch007

[26] N. Rjaibi, L. B. A. Rabai, A. B. Aissa and A. Mili, Mean failure Cost as a Measurable Value and Evidence of Cyber security: E-learning Case Study, International Journal of Secure Software Engineering (IJSSE), Vol 4, Issue 3, September-December 2013.

[27] N. Rjaibi, L. B. A. Rabai, A. B. Aissa and M. Louadi, Cyber Security Measurement in Depth for E-learning Systems, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). Vol 2, No 11, pp 107-120, November-2012.

[28] N. Rjaibi, L. B. A. Rabai, H. Omrani, A. B. Aissa, Mean Failure Cost as a Measure of Critical Security Requirements: E-learning Case Study, Proceedings of The 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'12, Las Vegas, Nevada, USA), July 16-19, CSREA Press, pp. 520-526, 2012.

[29] N.H. MohdAlwi, and I.S. Fan, E-Learning and Information Security Management, International Journal of Digit Society (IJDS), vol. 1, no. 2, 2010.

[30] P. Feiler, R. Gabrielp, J. Goodenough, et al. Ultra-large-scale systems: The software challenge of the future. Software Engineering Institute, vol. 1, 2006.

[31] R. Böhme, Security Metrics and Security Investment Models, In Advances in Information and Computer Security (pp. 10-24). Springer Berlin Heidelberg, 2010.

[32] R. Bojanc, B. Jerman-Blazic, An economic modelling approach to information security risk management. International Journal of Information Management, 28(5), 413-422, Elsevier, 2008.

[33] R. K. Abercrombie, F. T. Sheldon, and A. Mili, Managing Complex IT Security Processes with Value Based Measures, Proceedings of 2009 IEEE Symposium on Computational Intelligence in Cyber Security (CICS '09), Nashville, TN, April 1, 2009.

[34] R. M. Savola, A Security Metrics Taxonomization Model for Software-Intensive Systems, Journal of Information Processing Systems, Vol.5, No.4, 197-206, December 2009.

[35] R. Savola, On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems, International Journal of Computer Science and Network Security, VOL.10 No.1 230-239, January 2010.

[36] S. A. Butler, Security attribute evaluation method: a cost-benefit approach. In Proceedings of the 24th international conference on Software engineering (pp. 232-240). ACM, 2002.

[37] S. Kumar and K. Dutta, Investigation on Security In Lms Moodle, International Journal of Information Technology and Knowledge Management, vol. 4, No. 1, pp. 233-238, January-June 2011.

[38] S. Myagmar Adam, J. Lee William Yurcik, Threat Modeling as a Basis for Security Requirements, In Symposium on Requirements Engineering for Information Security, 2005.

[39] U.Saluja and N. B. Idris, Information Risk Management: Qualitative or Quantitative? Cross industry lessons from medical and financial fields, Journal of Systemics, Cybernetics and Informatics, 10(3), 2012.

[40] W. A. Jansen, NIST IR 7564: Directions in security metrics research, National Institute of Standards and Technology, US Dept. of Commerce, Gaithersburg, 2009.

[41] Web PAGE : https://docs.google.com/file/d/0B0Z2laATxEo7Tlk2TGd4elJjNFk/edit

[42] X. Liu, A. E. Saddik and N. D. Georganas, An implementable architecture of an e-learning system, CCECE 2003-CCGEI 2003, Montreal, IEEE, 2003.

[43] Z. A. Khanjari, S. Kutti, and M. Hatem, An Extended E-learning System Architecture: Integrating Software Tools within the E-learning Portal, The International Arab Journal of Information Technology, vol. 3, no.1, January 2006.