

EmpiRE, Ottawa, Canada
August 24th, 2015

WHICH SECURITY CATALOGUE IS BETTER FOR NOVICES?

Katsiaryna Labunets¹, Federica Paci², Fabio Massacci¹

¹University of Trento, Italy (<name.surname@unitn.it>)

²University of Southampton, UK (F.M.Paci@soton.ac.uk)



UNIVERSITY
OF TRENTO



The Problem

- Several methodologies and standards to identify threats and possible security requirements are available
 - Standards: ISO 27005, US NIST 800-53, UK's IAS
 - Methods: STRIDE, SABSA, COBIT, Eurocontrol or SESAR's SecRAM
- Any risk assessment needs expertise in domain and security



Where to find expertise?

- Experts are expensive and busy
- Non security experts + catalogue → does it work?
Maybe, yes. [REFSQ'15]
 - Non-experts + general or domain-specific catalogue ~ Security experts without a catalogue
 - Domain-general: BSI IT-Grundschutz Catalogue
 - Domain-specific: Eurocontrol's ATM Security Risk Management Toolkit
- But which catalogue is better for novices with no domain and no security expertise?
 - Domain-general vs. domain-specific

Catalogues' Scales

- BSI IT-Grundschutz Catalogue
 - Introduction → 40 pages
 - Assets → 375 pages
 - Threats → 723 pages
 - Security Controls → 3078 pages
- Eurocontrol's ATM Security Risk Management Toolkit
 - Guidance Material → 100 pages
 - ATM specific Threats → 57 pages
 - Pre-event ATM controls → 72 pages
 - Post-event ATM controls → 27 pages
- Remotely Operated Tower Scenario
 - Operational Focus Area Description → 100+ pages
 - Essential scenario description → 24 pages

Research Method

- Goal
 - Evaluate the effect of using domain-general vs. domain-specific catalogues on the *actual efficacy* and *perception* of a security risk assessment method applied by novices
- Treatments
 - Novices with a domain-general catalogue (GENCAT)
 - Novices with a domain-specific catalogue (DOMCAT)
- Context
 - ATM Domain – Remotely Operated Tower Scenario
 - Security Method – SESAR Security Risk Assessment Method
 - Catalogues
 - GENCAT: BSI IT-Grundschutz Catalogues
 - DOMCAT: Eurocontrol's ATM Security Risk Management Toolkit
 - Participants: 18 MSc students in Computer Science

Metrics

- Actual Efficacy (AE)
 - whether the treatment improves performance of the task
- Perceived Efficacy (PE)
 - Perceived Ease Of Use – PEOU
 - the degree to which a person believes that using a treatment would be free of effort
 - Perceived Usefulness – PU
 - the degree to which a person believes that a treatment will be effective in achieving its intended objectives
- AE Null Hypothesis
 - No difference between the treatments in identified threats/controls
- PE Null Hypothesis
 - No difference between the perceived efficacy (PEOU, PU) by the participants

Measurements

- Actual Efficacy
 - Quantity (num of threats and security controls reported by groups)
 - counted by authors
 - Quality of threats and security
 - 3 independent experts in ATM security
- Perceived Efficacy
 - Perceived Ease of Use + Perceived Usefulness
 - Measured by mean of post-task questionnaires on 1-5 Likert scale

Group ID	Threats Quality	Security Controls Quality	Comments
Align Text Middle			The assessment itself looks Due to unclear understandin assets, there are parts of the accurate.
G01	2 - Poor	2 - Poor	Threats: 1.) To keep assessment clea group made up their own thr
G02	3 - Fair	3 - Fair	Thoroughly made assessme of some actual operational c Threats: 1.) Those present are releva

2 / 6

Part I - Method (32 questions)

Read questions carefully. The positive and negative statements of the questions are mixed. The questionnaire has an opposing statements format, so

G03

If you agree strongly with the statement on the left, check the leftmost box (1).
If you agree, but less strongly, with the left statement, check box #2 from the left (2).
If you agree with neither statement, or find them equally correct, check the middle box (3).
If you agree, but less strongly, with the right statement, check box #2 from the right (4).
If you agree strongly with the statement on the right, check the rightmost box (5).

Part III - BSI IT-Grundschutz Catalogs (14 questions)

Read questions carefully. The positive and negative statements of the questions are mixed. The questionnaire has an opposing statements format, so

If you agree strongly with the statement on the left, check the leftmost box (1).
If you agree, but less strongly, with the left statement, check box #2 from the left (2).
If you agree with neither statement, or find them equally correct, check the middle box (3).
If you agree, but less strongly, with the right statement, check box #2 from the right (4).
If you agree strongly with the statement on the right, check the rightmost box (5).

Note: For ease of r

N				
1.	If I need to ider project at work possible			
2.	If I need to ider future project a SECRAM if por	N	1 2 3 4 5	
3.	SECRAM help the threats	1.	If I need to identify threats in a future project at work, I would use IT-Grundschutz catalog of threats if possible	If I need to identify threats in a future project at work, I would avoid IT-Grundschutz catalog of threats if possible
4.	SECRAM help the security cr	2.	If I need to identify security controls in a future project at work, I would avoid IT-Grundschutz catalog of security controls if possible	If I need to identify security controls in a future project at work, I would use IT-Grundschutz catalog of security controls if possible
5.	I found SECR	3.	I found IT-Grundschutz catalogs easy to use	I found IT-Grundschutz catalogs difficult to use
6.	If working as a customer who would use SEC	4.	Finding specific threats for a different context would be easy with IT-Grundschutz catalog of threats	Finding specific threats for a different context would be difficult with IT-Grundschutz catalog of threats
7.	If working as a customer who controls, I wo	5.	Finding specific security controls for a different context would be difficult with IT-Grundschutz catalog of security controls	Finding specific security controls for a different context would be easy with IT-Grundschutz catalog of security controls
8.	If I must identif course, I would	6.	If working as a freelance consultant for a customer who needs help finding threats, I would use IT-Grundschutz catalog of threats	If working as a freelance consultant for a customer who needs help finding threats, I would avoid IT-Grundschutz catalog of threats
9.	If I must identif project course,	7.	If working as a freelance consultant for a customer who needs help finding security controls, I would avoid IT-Grundschutz catalog of security controls	If working as a freelance consultant for a customer who needs help finding security controls, I would use IT-Grundschutz catalog of security controls
10.	SECRAM proc			
11.	SECRAM was			
12.	I found SECR			

Is Quantity Useful?

- Quantity of threats/controls makes no sense with catalogue



Security Engineering Report on Remotely Operating Tower¹

Author:
 1: *Ted Mosby*¹
 2: *Robin Scherbatsky*¹

OBJECT OF EVALUATION¹

We analyzed the identity and access management, web applications and database, and network and the security of the remotely operating tower system. We have targeted systems installed at remote digital network and devices that are installed both at the remote airport and remote tower.¹ We understood how the remotely operating tower operates and what it needs to operate effectively. We have identified, we targeted the main threats, with high risk, that should be controlled. In the first place, we focused on the identity and access management of the system. We identified elements that will impact users' identification and access to and of the system. Then, we analyzed web applications and functions of the remotely operating tower system where, our concern was the service. Therefore we started and come up with risks that affect the operation of the remotely operating tower system. We examined network and infrastructure section, where our main concern was the communication between web applications and the infrastructures installed on the remote airport and also the system's security itself.¹

In the analysis of this work we have assumed different assumptions, some of them are:¹
 - The remote tower is located in the city and in normal security premises.¹
 - The communication between the web application and devices installed at the remote airport is through the web (internet).¹
 - Employees could be technical and non-technical staffs of SESAR.¹
 - The electric power is not interrupted at the airport premises as well as at the remote tower.¹
 - The remotely operating tower system has its own secured data center.¹

SUMMARY OF FINDINGS¹

In the remotely operating tower system, we have identified some assets of SESAR which includes provision of service, airport flight data, user credential data, digital network and surveillance data. In this report we have also discovered high-level risks or threats which will harm assets mentioned above and assets of the party. The identified threats include hackers, employee, system failure, natural disasters and so on. And we have also proposed security control mechanisms for the identified risks such as strengthen access and identity management solution, install malware intrusion detection systems, increase awareness of employees on security risks, preparing backup items such as cameras, sensors and so on.¹
 We have described the complete summary of results in the document DF-G02-summary_of_results.excel submitted as integral part of this report.¹

Experimental Protocol

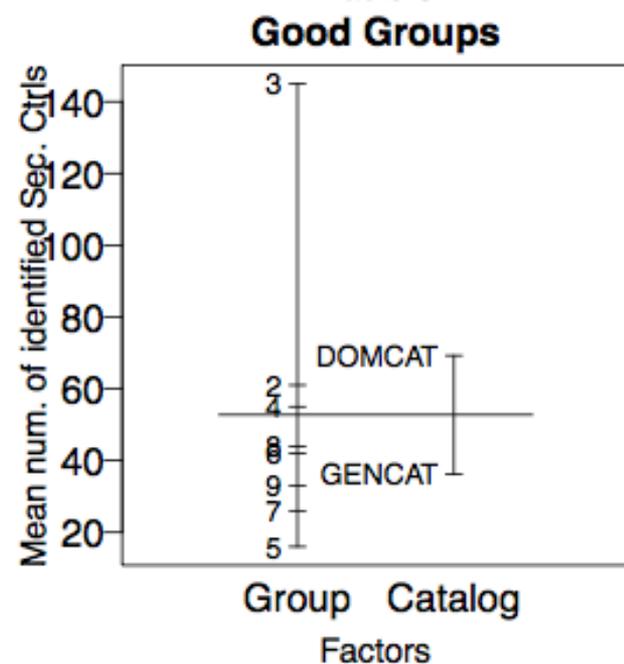
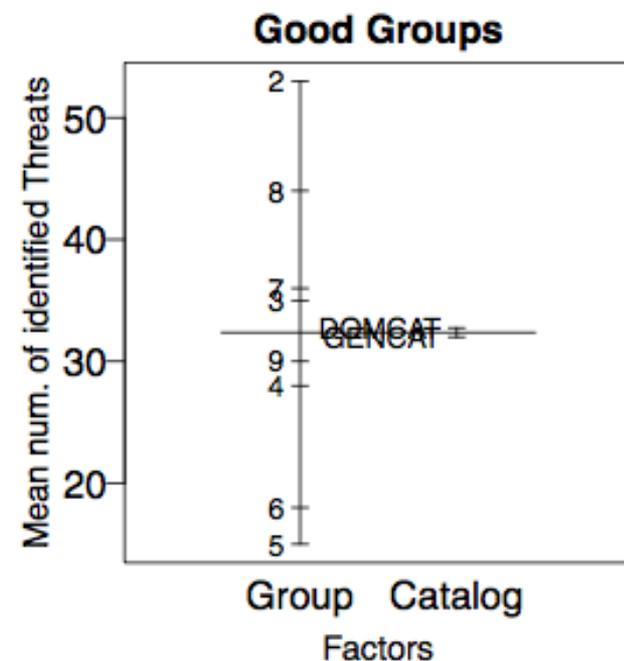
- Training
 - Application scenario
 - 1 hour training by ATM domain expert
 - Method
 - 8 hours tutorial by EUROCONTROL expert
- Application
 - 6 hours to revise the security risk assessment
 - 2 post-task questionnaires to collect participants' perception of:
 - the method
 - the catalogues
- Evaluation
 - 3 ATM security experts evaluated the quality of threats and security controls

Results: Actual Efficacy

- Quantity
 - # threats: DOMCAT ~ GENCAT
 - # sec. controls: DOMCAT > GENCAT
 - No statistical significance
- Quality (median values)

	DOMCAT	GENCAT
Threats	3.33	3
Sec. controls	3.33	3.67

- No statistical significance
- We would need
 - Threats quality: 38 groups
 - Sec. controls quality: 101 groups



Results: Perceived Efficacy

- Method with Catalogues

	DOMCAT	GENCAT	Req. # participants
Median PEOU	4	3	2968
Median PU	4	3	10 (we had 18)

- Catalogues

	DOMCAT	GENCAT	Req. # participants
Median PEOU	4	3.5	35
Median PU	4	3	746

- We would need or bigger difference (2.5 vs. 4.5) in the results OR more participants

Summary

- Conclusions
 - Which catalogue is better for novices? – **Both may work**
 - Method + domain-specific catalogues → higher PU
 - Quantitative metrics do not work for catalogues comparison
- Open questions
 - Comprehensibility of the results
 - Replication on a large risk assessment
- Ads
 - Want to join the effort? → we are looking for replications
 - More Info? → <http://securitylab.disi.unitn.it>