Comparison of Existing Threat Catalogues

1 Introduction

Almost every risk assessment methodology (see also comparison provided by ENISA [EN]) comes with at least a short list of example threats. We have not found any prior analysis work that would explain how-to create, structure and maintain a threat catalog.
The below comparison table contains a sample collection of threat catalogs that are prominent in our environment. The table is by far not exhaustive but serves to illustrate the differences in extent, scope and structure.

1.1 Audience and Context

The audience and the application (context) of a threat catalog is determining the best suitable structure. The audience determines the abstraction level as well as the best breadth and depth of the threat catalog.
If the threat catalog is targeted to home users the abstraction level should be low and everything that goes beyond the “top 5 threats” would be overwhelming the home-user. The threat list of Melani for example clearly target home users. On the other end of the spectre we find the threat catalogue of BITs that targets IT security administrators of enterprises.
The application (context) determines how to best structure the threat description. If a threat catalog is used to prompt risk scenarios in a risk analysis then it is helpful to have examples of how the threat can manifest (threat agents, and potential impact). If the threat catalogue is used to advice in best practices to mitigate the most common risks then links to controls are a very valuable enhancement.

1.2 Focus and Origin

Most of the available catalogs are either from government sponsored IT security programs or from commercial risk management frameworks. Open-source organizations like OWASP, or other well known organizations like ISO/IEC, CERT, SANS and OASIS do (surprisingly) not provide any threat catalogs. Microsoft [MI] has in our opinion at the time of this writing the most sophisticated threat modeling approach (with publicly available tool support) but also Microsoft does not explicitly publish a threat catalog. However there is a built-in attack catalog.

1.3 Catalog structure

A well thought through structure of the threat catalog will facilitate risk-analysis and architectural design. We found that the threat catalog of BSI offers a structure that lends itself well to the workflows of both security architects as well as general IT risk analysts. Both the navigatability as well as the examples support the understandability.

1.4 Size and coverage

Among the catalogs with global target audience, ISF [IS], CRAMM [CR], and BITS [BI] we have found that BITS has the greatest coverage, both in depth and breadth, with over 600 threats it is by far the most extensive catalogue.

1.5 Mappings

Corporate IT Risk/Security standards can be based on different best practice collections. To support the workflows and governance needs of company the threat catalog should map the threats against the required controls that mitigate the threat impact. For governance reasons it is also helpful to have a mapping between the threats and

the corresponding policy/standard statements that require the consequential risk to be mitigated. In this respect ISF provides the most complete and the most uptodate set of materials (with the risk assessment method IRAM, the “standard of good practice” as a policy framework and a rich set of supporting implementation guidelines).

Name	BSI (Germany)	BITS	ISF	CRAMM	MELANI	Microsoft Threat Model
URL	http://www.bsi.de/english/gshb/manual/t/t01.htm	http://www.bitsinfo.org/downloads/Publications%20Page/BITS%20Kalculator/bitskalculatorspreadsht.xls	(Not publicly available)	(Not publicly available)	http://www.melani.admin.ch/themen/00103/index.html?lang=de	http://www.microsoft.com/downloads/details.aspx?familyid=59888078-9daf-4e96-b7d1-944703479451
Focus/Origin	Operational Risks	Operational Risks	CIA Risks for information systems	Operational Risks	Attacks through internet	Application Security Risks
Catalog context	-> Base IT security manual	-> Risk Measurement -> Basel II -> Financial Services	Information Risk Assessment Methodology and Security Incident Analysis	Information Risk Assessment Methodology	Advice for home computer security	Threat modelling tool
Catalog structure	5 chapters: - Force majeur - Organiz. shortcomings - Human failure - Technical failure - Deliberate acts	-> Threat categories and generic risks are a flat list -> covering: Physical threats Legal threats Criminal threats Operational threats human error threats	Structured list with main categories: - External attack - Theft - Service interruption - Internal Misuse - Unforeseen effect of change - Malfuntion	Simple list	Simple list	Structured list with typical application targets attacks
Catalog Size	370 Threats for all 5 chapters	-> 70 Threat Categories -> Over 600 generic risk descriptions	49 Threats	37 Threats	12 specific threats (attack methods and vulnerability sources)	36 detail attacks in 19 higher level attacks
Mapping to ISO Other mappings	NO	YES To vulnerabilities To Basel II requirements To mitigating controls	NO	No To mitigation actions To asset groups	No To mitigating actions	No To mitigation actions
Last updated	2004	2004	Continous	Continuous	N/A	N/A

Table 1: Comparison of existing threat catalogs