THREAT TAXONOMY

CONTACT INFORMATION

Calle Olímpico Francisco Fernández Ochoa, 9
28923 Alcorcón (Madrid) Spain
Mail: consortium@ism3.com
Phone:+ 34 620 527 478

LEGAL DISCLAIMER

This is an informational document, and it doesn't represent legal or professional advice from the ISM3 Consortium, the authors or reviewers of this document. This document is offered as is without any warranty of completeness, accuracy or timeliness. The ISM3 Consortium, the authors and reviewers of this document disclaim any implied warranty or liability.

LICENSE AND COPYRIGHT

Founding Members

ESTEC Security (http://www.security.estec.com/) - Canada

First Legion Consulting (http://www.firstlegion.net/) - India

Global4 (http://www.g4ii.com/) - Spain

M3 Security (http://www.m3-security.net/) - USA

Seltika (http://www.seltika.com) – Colombia

1 Introduction

For effective communication information security professionals use a rich vocabulary with very specific and sometimes even personal meaning.

The ISM3 Consortium has published a Glossary that uses operational definitions, this are definitions that are not subjective or observer dependent.

Risk assessment methods use a model of the organization, a threat taxonomy, a vulnerability taxonomy, a control taxonomy and a way to combine them to reach a Risk figure. Unfortunately, a common agreement on the classes of threats that exists and the controls that can mitigate them is not available.

Using ISM3 concepts and definitions, it is possible to classify threats depending on who is the agent of the threat (accidents, errors, attacks) what is the object of the attack (repositories, messages, services, sessions, interfaces, channels) and what are the effects of the attack. As threat to instructions and credentials can lead to more serious consequences, instructions and credentials, that are stored in repositories or messages are mentioned explicitly.

Threats can be classed as well depending on the mechanism of the attack, error or accident. As often effective protection can be established against attacks whatever the mechanism used, this taxonomy is not using mechanism as a classification criterion.

2 Threat Taxonomy

Type of Incident	Losses / Effect	Asset / Object				Agent / Subject	Agent Gains
Accident	Failure to destroy expired information or systems	*repository*	*message*	*credential*	*instruction*	Forces of nature	Not applicable
	Destruction of valid information	*repository*	*message*	*credential*	*instruction*		
	Corruption of valid information	*repository*	*message*	*credential*	*instruction*		
	Loss of valid information	*repository*	*message*	*credential*	*instruction*		
	Aging of information	*repository*	*message*	*credential*	*instruction*		
	Unauthorized access, eavesdropping, theft and disclosure of information	*repository*	*message*	*credential*	*instruction*		
	Improper use of authorized access to information or systems	*repository*	*message*	*credential*	*instruction*		
	Improper recording of access to information	*repository*	*message*	*credential*	*instruction*		
	Failure to stop systems at will	*service*	*channel*	*interface*	*session*		
	Destruction of valid systems	*service*	*channel*	*interface*	*session*		
	Corruption of valid systems	*service*	*channel*	*interface*	*session*		
	Loss of valid systems	*service*	*channel*	*interface*	*session*		
	Unauthorized access, eavesdropping, theft and disclosure of channels	*service*	*channel*	*interface*	*session*		
	Failure of authorized access	*service*	*channel*	*interface*	*session*		
	Underperformance or Interruption of valid system services	*service*	*channel*	*interface*	*session*		
	Improper use of authorized access	*service*	*channel*	*interface*	*session*		
	Improper recording of use of systems	*service*	*channel*	*interface*	*session*		
	Outdated systems	*service*	*channel*	*interface*	*session*		

Type of Incident	Losses / Effect	Asset / Object				Agent / Subject	Agent Gains
Error	Failure to destroy expired information or systems	*repository*	*message*	*credential*	*instruction*	People	Not applicable
	Destruction of valid information	*repository*	*message*	*credential*	*instruction*		
	Corruption of valid information	*repository*	*message*	*credential*	*instruction*		
	Loss of valid information	*repository*	*message*	*credential*	*instruction*		
	Aging of information	*repository*	*message*	*credential*	*instruction*		
	Unauthorized access, eavesdropping, theft and disclosure of information	*repository*	*message*	*credential*	*instruction*		
	Improper use of authorized access to information or systems	*repository*	*message*	*credential*	*instruction*		
	Improper recording of access to information	*repository*	*message*	*credential*	*instruction*		
	Failure to stop systems at will	*repository*	*message*	*credential*	*instruction*		
	Destruction of valid systems	*service*	*channel*	*interface*	*session*		
	Corruption of valid systems	*service*	*channel*	*interface*	*session*		
	Loss of valid systems	*service*	*channel*	*interface*	*session*		
	Unauthorized access, eavesdropping, theft and disclosure of channels	*service*	*channel*	*interface*	*session*		
	Failure of authorized access	*service*	*channel*	*interface*	*session*		
	Underperformance or Interruption of valid system services	*service*	*channel*	*interface*	*session*		
	Improper use of authorized access	*service*	*channel*	*interface*	*session*		
	Improper recording of use of systems	*service*	*channel*	*interface*	*session*		
	Outdated systems	*service*	*channel*	*interface*	*session*		

Type of Incident	Losses / Effect	Asset / Object				Agent / Subject	Agent Gains
Attack	Failure to destroy expired information or systems	*repository*	*message*	*credential*	*instruction*	Corporate Raiders Hackers Professional Criminals Spies Terrorists Vandals	Feeling of accomplishment Political Gain Financial Gain Knowledge Gain Status Gain
	Destruction of valid information	*repository*	*message*	*credential*	*instruction*		
	Corruption of valid information	*repository*	*message*	*credential*	*instruction*		
	Theft of valid information	*repository*	*message*	*credential*	*instruction*		
	Aging of information	*repository*	*message*	*credential*	*instruction*		
	Unauthorized access, eavesdropping, theft and disclosure of information	*repository*	*message*	*credential*	*instruction*		
	Improper use of authorized access to information or systems	*repository*	*message*	*credential*	*instruction*		
	Improper recording of access to information	*repository*	*message*	*credential*	*instruction*		
	Failure to stop systems at will	*repository*	*message*	*credential*	*instruction*		
	Destruction of valid systems	*service*	*channel*	*interface*	*session*		
	Corruption of valid systems	*service*	*channel*	*interface*	*session*		
	Theft of valid systems	*service*	*channel*	*interface*	*session*		
	Unauthorized access, eavesdropping, theft and disclosure of channels	*service*	*channel*	*interface*	*session*		
	Failure of authorized access	*service*	*channel*	*interface*	*session*		
	Underperformance or Interruption of valid system services	*service*	*channel*	*interface*	*session*		
	Improper use of authorized access	*service*	*channel*	*interface*	*session*		
	Improper recording of use of systems	*service*	*channel*	*interface*	*session*		
	Outdated systems	*service*	*channel*	*interface*	*session*		