Incident Classification / Incident Taxonomy according to eCSIRT.net – *adapted*

International Version
Don Stikvoort, 11 Jan – 19 Dec 2012
(version mkVI of 31 March 2015)
Many thanks to various reviewers, most notably so
Andrew Cormack, Xander Jansen, Alf Moens and Peter Peters

What is in *italics* has been added or adapted from the old eCSIRT.net Incident Classification (de facto) standard, which was based on earlier work by Jimmy Arvidsson. Note that only the following changes have occurred to the base categories:

- **'information security' ➔ 'information *content* security' : because the term 'information security' is too generic and wide ranging**
- **added '*vulnerable*'**
- **added '*test*'**

Also, the 2nd column used to be a sub-classification in the original model. However this will only give rise to much confusion if this were to be used inbetween organisations. Therefore it is strongly advised to stick to the main categories, and only use the 2nd column as examples, for clarification. Of course, for internal purposes one could use these subcategories in a ticketing system – but the question is still then : is that worth the extra analysis effort.

Last but not least – bear in mind that this is not an exclusive taxonomy. Incidents can well involve more classifications. How to handle this is not a function of this document, but rather of how a CSIRT organises their incident tracking system. The choice usually is – is it allowed that an incident has more than 1 classification? This is theoretically the best approach, though it can muddle up incident statistics and needs to be carefully considered. Or is only 1 classification allowed? And then a judgment call is needed what is the most significant of the classifications for that specific incident.

Incident Class*ification*	**Incident *Examples***	**Description / *Explanation***
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a *functionally comparable* content.
	Harmful Speech [1]	Discreditation or discrimination of somebody (e.g. cyber stalking, *racism and threats against one or more individuals*)
	Child/Sexual/ Violence/...	Child Pornography, glorification of violence, ...
Malicious Code [2]	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), *port scanning*.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

[1] Was "harassment" – legally the term "harmful speech" is more correct, as it includes harassment, discrimination and defamation
[2] "Malicious code" refers to malicious software inserted into a system. The vector that caused the insertion is not apparent here. The vector can be an "intrusion" from the outside, but also a USB stick, or other internal vector.

Intrusion Attempts [3]	Exploiting of known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions [4]	Privileged Account Compromise	A successful compromise of a system or application (service). This can have been caused remote*ly* by a known or new vulnerability, but also by an unauthorized local access. *Also includes being part of a botnet.*
	Unprivileged Account Compromise	
	Application Compromise	
	Bot	
Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. *DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks.* However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – *or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.*
	DDoS	
	Sabotage	
	Outage (no malice)	
Information *Content* Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). *Human/configuration/software error can also be the cause.*
	Unauthorised modification of information	

*[3] An "attempt" refers to the mechanism used to **try** and create an intrusion. The intrusion may have failed – or not.*
*[4] An "intrusion" will as rule of thumb be the result of a **successful** intrusion attempt.*

Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	*Offering* or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	*Masquerading as another entity in order to persuade the user to reveal a private credential.*
Vulnerable	*Open for abuse*	*Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc*
Other	All incidents which don't fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.
Test	*Meant for testing*	*Meant for testing*