Incident Classification

Overview

Don Stikvoort
don@elsinore.nl

23 May 2013

Work partially sponsored by SURFnet

Taxonomies – pros and cons

PROS

- systemisation and regularisation of work
- an opportunity to produce statistics
- an opportunity to observe trends
- a means of communication with management and the media
- a common language for naming threats

CONS

- an increase in the complexity of incident work
- an increase in the duration of Incident Handling
- not a real picture of internet threats
- the difficulty of ambiguous classification

Source: http://www.enisa.europa.eu/activities/cert/support/incident-management

CERT.LV taxonomy (i) - descriptive

- **attacks on the critical infrastructure**
- **attacks on the Internet infrastructure, e.g. root or system-level attacks on any Server System, or any part of the backbone network infrastructure, denial of service attacks**
- **deliberate persistent attacks on specific resources, i.e. any compromise which leads or may lead to unauthorised access of systems**
- **widespread automated attacks against Internet sites, e.g. sniffing attacks, IRC "social engineering" attacks, password cracking attacks**
- **threats, harassment, and other criminal offences involving individual user accounts;**

CERT.LV taxonomy (ii) - descriptive

- **new types of attacks or new vulnerabilities**
- **botnets, i.e. activities related to network of compromised systems controlled by a party which is a source of incident**
- **denial of service on individual user accounts, e.g. mail bombing**
- **forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. e-mail forgery, SPAM and etc.**
- **compromise of single desktop systems**
- **copyright violation.**

SURFcert taxonomy - KISS

- (Administrative)
- Content
- Vulnerable
- Spam
- Abusive
- Probe
- Denial

eCSIRT.net taxonomy - venerable

- Dates 2003, with thanks to Jimmy Arvidsson
- http://www.ecsirt.net/
- Used by several teams in Europe
  - With additions like phishing
- A tad outdated, but still useful !

Incident Class (mandatory input field)	**Incident Type** (optional but desired input field)	**Description / Examples**
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 an identical content.
	Harassment	Discreditation or discrimination of somebody (i.e. Cyberstalking)
	Child/Sexual/Violence/...	Child Pornography, glorification of violence, ...
Malicious Code	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	
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, ...).
	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).
Intrusion Attempts	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, backdoors, cross side scripting, etc.).
		Multiple login attempts (Guessing / cracking of passwords

Attempts	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	new attack signature	An attempt using an unknown exploit.
Intrusions	Privileged Account Compromise	A successful compromise of a system or application (service). This can have been caused remote by a known or new vulnerability, but also by an unauthorized local access.
	Unprivileged Account Compromise	
	Application Compromise	
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. Examples of a remote DoS are SYS- a. PING- flooding or E-mail bombing (DDoS: TFN, Trinity, etc.). However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.).
	DDoS	
	Sabotage	
Information 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 intercepts and access information during transmission (wiretapping, spoofing or hijacking).
	Unauthorised modification of 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 intercepts and access information during transmission (wiretapping, spoofing or hijacking).
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	Selling or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).

eCSIRT.net mkII

- Change/add **only** what is strictly needed
- Backwards compatibility
  - Well known quantity
  - Continue to enable comparisons
- Kept “Incident Class” but changed “Incident Type” into “Incident Examples”
  - Too much granularity does NOT help
- Work done in 2012 by DS with many thanks to Andrew Cormack, Alf Moens, Peter Peters and Xander Jansen
  - ***All which is italics below is new or adapted*, all the rest is original !!!**

1. Abusive Content

Spam : "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.

Harassment : Discreditation or discrimination of somebody (e.g. cyberstalking, *racism and threats against one or more individuals)*

Child/Sexual/ Violence/... : Child Pornography, glorification of violence, ...

2. Malicious Code

Virus :

Worm :

Trojan :

Spyware :

Dialer :

Rootkit :

Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.

3. 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).

4. Intrusion Attempts

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, backdoors, cross site scripting, etc.).

Login attempts : Multiple login attempts (Guessing / cracking of passwords, brute force).

New attack signature : An attempt using an unknown exploit.

5. Intrusions

Privileged Account Compromise :

Unprivileged Account Compromise :

Application Compromise :

Bot :

A successful compromise of a system or application (service). This can have been caused remote by a known or new vulnerability, but also by an unauthorized local access. *Also includes being part of a botnet.*

6. Availability

DoS :

DDoS :

Sabotage :

Outage (no malice) :

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.*

7. Information *Content* Security

Unauthorised access to information :

Unauthorised modification of 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 intercepts and access information during transmission (wiretapping, spoofing or hijacking). *Human/ configuration/software error can also be the cause.*

8. 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.*

9. Vulnerable

***Open for abuse** : Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc*

10. 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.

11. Test

***Meant for testing** : Meant for testing*

Work in Progress

Discussed eCSIRT.net mkII with Rob McMillan (formerly AUScert, now Gartner) and Rogier Spoor (SURFnet) :

- Agreement on validity and usefulness of classification
- Advantages:
  - Backwards compatibility : you can use it **tomorrow**
  - Relatively straightforward and intuitive
- Disadvantages:
  - How to compare an apple with a pear ?
    (e.g. Intrusion vs Malicious Code)
  - Impact/damage aspect is completely missing
- Model based on 2 dimensions, like attack vector and impact ?
  - DS volunteers – any takers ?
  - Get 1 or 2 universities involved ?
  - Maybe this will help: ISO/IEC WD 27035-2.2 ???