European Commission

JRC TECHNICAL REPORTS

# A Taxonomy for Incidents in Communication Systems

Carlo Ferigato, Saša Gligorijević

**2012**

Report EUR 25568 EN

Joint Research Centre

**European Commission**
Joint Research Centre
*Institute for the Protection and Security of the Citizen*

**Contact information**
Carlo Ferigato
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 210, 21027 Ispra (VA), Italy
E-mail: carlo.ferigato@ec.europa.eu
Tel.: +39 0332 786359
Fax: +39 0332 785469
http://www.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

This publication is a Reference Report by the Joint Research Centre of the European Commission.

**Legal Notice**
Neither the European Commission nor any person acting on behalf of the Commission
is responsible for the use which might be made of this publication.

JRC76516
EUR 25568 EN

ISBN 978-92-79-27152-6 (pdf)
ISBN 978-92-79-27153-3 (print)

ISSN 1831-9424 (online)
ISSN 1018-5593 (print)

doi:10.2788/60981

Luxembourg: Publications Office of the European Union, 2012

*Printed in Italy*

# Contents

# Chapter 1

# Introduction

This report deals with the construction of a taxonomy of incidents in communication systems. By taxonomy we mean [15]

> *the systematic distinguishing ordering and naming of type groups within a subject field:* CLASSIFICATION.

The report is organised as follows: the present section concerns a survey of existing taxonomies, glossaries or *controlled languages* for computer security incidents. It starts with a definition of the terms used in this report and a discussion on the use of taxonomies as *measurement tools.* The survey aims at clarifying the importance of the definition of a *common language* for exchanging and gathering information on computer security.

The second section presents the original ideas for the taxonomy proposed with this report. The main assumption is in the definition of the main functions a communication system should perform and in defining a disruption as the lack of one of these functions.

The third section is the actual presentation of the taxonomy. Some examples of classification in this taxonomy of known computer security incidents are added. While the overall aim of this work is at the construction of complete taxonomy for communication systems — including the telecommunication services — the examples provided in this section will mainly deal with disruptions occurring in the Internet domain.

The fourth section presents the future work to be done for continuing the development of the taxonomy proposed here.

## 1.1 Definitions

By *taxonomy* we mean, as in the definition quoted above, the *ordering* of type groups in the subject field of *disruption in communication flows*. By *communication flow* we mean the current social activity of communicating within a net of humans and impersonal (software) agents whose main example is the Internet. This activity includes publication of web sites, access to sensitive data, sending of e-mails and other electronic documents. In this environment, acts of deception performed both by humans and computers happen. The responsibility for such acts are obviously not at the same level in case they are performed by human agents instead of non-human agents. Nevertheless, such acts should be classified in a taxonomy devoted to incidents in communication systems.

As in the literature, the need for a taxonomy in this field is motivated by the fact that:

> *Much of the computer security information regularly gathered and disseminated by individuals and organisations cannot currently be combined or compared because a "common language" has yet to emerge in the field of computer security* [7].

In the following section, a survey of the publications concerning taxonomies related to our theme of investigation is done. This survey includes the so-called *ontologies* and few *glossaries* related to computer security. By ontology we mean a taxonomy apt to be used by some software tool while by glossary we mean a list of items associated to their short description without the objective of constructing an exhaustive classification scheme for the field.

## 1.2 The literature on this subject

The subject of this report is purposely general. We consider *communication systems* with the broad meaning of a net of agents and channels coordinating their behaviour around the electronic documents exchanged. Electronic document has as well the broad meaning of any electronic resource that needs a computer for being displayed. So, web sites, log files of access to systems and records of personal data as well as documents composed in the pdf format are included in this definition.

With this broad spectrum of systems as starting point, there are several existing studies on taxonomies for computer and Internet security that could be considered as relevant to the topic. Starting from the first studies published during the nineties like [14] and [7] to the more recent *ontologies* like [3].

It is remarked that [7] is still today the most complete and quoted — sometimes as *the CERT taxonomy* — taxonomy. For example, it is taken as the basis for a new taxonomy in [10] where the skeleton of [7] is preserved as it is and a new dimension concerning the user's perception of the effect of an *attack* is added. In this work, an indication of the quality of computer attacks is done on the basis of the number of incidents per category of the taxonomy. As a second example, [7] is expanded in [9] with the aim of covering the *security evaluation* of systems. To this end, new terms concerning motivation for attacks and more recent techniques are added. In both cases — [10] and [9] — the original work [7] is kept as the nut for the new taxonomies.

A similar fundamental work exists in the field of *dependability* [1]. This work is the complete report of the analysis started in 1980 of the joint groups "IEEE–Computer Security on fault tolerant computing" and the IFIP WG 10.4 on "Dependable computing and fault tolerance". This work, together with [7] quoted above, constitute as today the most complete and exhaustive taxonomies covering computer security and description of faults in interconnected systems of computers.

For the sake of completeness, it is worth to cite as well the ISO 31000 standard [8] whose *guide 73* [5] — prepared by the ISO Technical Management Board Working Group on *Risk Management Terminology* — contains the basic glossary in English and French on risk management. While not explicitly addressed to the field of computer security, this standard defines the basic high level terms in use while dealing with security of systems, including communication systems.

Among the recent publications it is worth to cite [2] where the focus of the common language and categorisation is in the legal prosecution and few sectors and professions (law, military, academia, private sector). Nevertheless, the technical components are represented in terms of high level categories of terms basically associated to the main hardware devices and software tools. This categorisation lacks the methodological component of an attack and, consequently, of the new terms related to these attacks like *trojan, virus* and so on.

A good effort in the construction of a specific taxonomy for attack tactics and tools is [6]. This article is a remarkable effort in collecting and coherently integrating ideas from the literature. Nevertheless, it is remarked that, in lack of a specific definition of the exploited *vulnerability* while performing an attack, the authors propose to use the general categorisation originally proposed in [7]. In this way, the central contribution of the latter work in the construction of a taxonomy for computer incidents has been confirmed.

A final remark must be done on *glossaries*. An exhaustive glossary for computer security is [16]. While targeted to the finance sector, this glossary is a valuable source of terms and definitions for the overall field of computer security. Another useful glossary is [4]. This work, originated as a RFC — Request For Comments — communication of The Internet Engineering Task Force, is presently used as a base for the standardisation of communications on incidents among the Community Emergency Response Teams (CERT).

# Chapter 2

# Disruption of a strictly organised information flow

After the literature survey done in the previous chapter, a natural question arise: why should a new taxonomy be constructed in the field of computer security and computer-based communication systems? The answer is twofold: first of all the existing taxonomies do not consider communication systems in general as perceived by a normal user; their origin is in engineering and analysis of systems. Secondly, the two main taxonomies mentioned above — [7] and [1] — are based on a strong assumption: the communication system being described has a non predictable behaviour. The *events* within the communication system appear as they were natural hazards and as such these events are described.

What we propose is a distinct perspective: we define the set of fundamental functions that a communication system should perform properly in order to guarantee its effective work and we define an event as the breaking of one or more fundamental functions.

## 2.1 Communication disciplines as functions of a communication system

We assume that a communication system, in order to work properly, must perform correctly the functions described by the *Communication Disciplines*. The *Communication Disciplines* [12] [11] (hereinafter simple the *Disciplines*) are conceived starting from the assumption that computers in our society are a *general medium for a strictly organised information flow*. This assumption is coherent with the contemporary view of the communication network provided by the Internet as a set of channels relating human and non-human agents coordinating their behaviours on the base of the messages exchanged.

While written in the seventies, the *Disciplines* are still today an up-to-date tool for the analysis and design of communication systems. In this report, we will not use the *Disciplines* as an analysis tool for designing new communication systems. On the contrary, we will assume that the communication system we are using — the Internet for short — is functioning properly by implementing in the more efficient and complete way the functions foreseen by the Disciplines. Consequently, we will classify the disruption experienced in the use of our communication system as a lack in one or more of the Disciplines.

In the remaining part of this chapter, we will list and describe the twelve Disciplines and provide some examples related to the functions they foresee. We will provide as well some examples concerning the lack of functioning of a communication system implementing properly all the individual disciplines. While used here as a mean for describing the correct work of the communication system based on the Internet, the Disciplines are more general. For feeding the intuition, some examples will consequently deal with traditional communication system like the post services or the telephone lines.

## 2.2 Synchronisation

*Synchronisation:* the partial ordering in terms of causality as opposed to an absolute ordering in terms of time.

This discipline is concerned with getting proper timing restraints for different activities. Partial orders are used as synchronisation tools since they represent well causality and independence relations between activities. Clocks are not considered as useful synchronisation tools in general, since the hypothesis of clock signals travelling on the net at a speed greater than the messages themselves is rejected.

Typical examples of synchronisation of communications in big organisations are related to the rate of success of telephone calls while trying to reach over the phone some colleague. Designers of banking applications are well aware of synchronisation problems while establishing protocols that guarantee the completion in any case of a bank transaction in case the communication line is interrupted in the middle of a commitment. In the case of coordination for action based on communications with an e-mail system, there is necessarily a delay between sending and receiving. Moreover, who receives a communication is in general not aware of *who else* receives it and *when.* So, while coordinating a group of agents in response to an emergency situation, e-mail can lead to misunderstandings. From the perspective of attacks to communication systems, a typical example of a lack of synchronisation is in the so-called *Denial of Service* attacks. In this case, the lack in synchronisation between requests to web servers and consequent reply is used as a mean for disrupting a communication.

## 2.3 Identification

*Identification:* this discipline is concerned with the identification process that must take place if a message is received from outside.

The identification process is something we experience, for example, while receiving e-mail letters whose header information is altered to make the message appear to come from a known or trusted source; an operation commonly called *e-mail spoofing.* The identification process is obviously more general than e-mail identification, since it is applied to messages at all levels: from low level electric signals to the typographic and stylistic components of a printed document for deciding about the plausibility of its source.

Concerning breaches of communication systems protocols caused by a lack in the identification function, a simple example is provided by the so-called *phishing* technique in which a web site is altered or copied and users are re-directed to this fake site. Obviously, in order to be successful, such kind of breach has to be combined to some wrong *addressing* mechanism. The Discipline *addressing* will be discussed below.

Identification concerns as well more specific processes in communication systems, an example is in the identification of a competence or of an information source. We can experience such lack in identification while, after a search for a specific service or goods in the Internet, the search engine displays as ranked in the first positions advertisements or addresses that do not correspond immediately to the service or goods required.

## 2.4 Copying

*Copying:* this discipline concerns the control of the number of copies of documents and data in relation to the communication channel they are related to.

The importance of the copies of a message becomes clear if we consider documents instead of information in general. Keeping under control the number of copies of confidential documents is the main goal of security officers in many organisations. In fact, the pragmatic value of a copy of a document changes if it is obtained through the official channel of authorisation for making copies, through the reconstruction from other sources of the information it contains or by an act of espionage. Electronic transmission of documents gives to the process more degrees of freedom but is not different in principle from *hard-copying.*

Among the examples of non-authorised copying, we can list copying of credit card numbers, passwords or personal data from a database. A distinction here could be made between non-authorised copies obtained via an explicit non-authorised access to a system or obtained via an access to a system done by exploiting a lack in security design of that system.

## 2.5 Addressing

*Addressing:* in its general form, addressing means the description of a route through a net of channels and agents.

In everyday life, we can experience addressing problems, for example, while looking for somebody competent in a given subject, or while looking for somebody that was able to solve a problem for us in the past. We experience addressing problems as well while continuing a discussion initiated in a meeting by e-mail: in a meeting a communication is addressed in a synchronous way to all of the participants in the meeting and the confirmation of receipt is immediate. On the contrary, while using an e-mail system the first condition is true only in the case of *broad-casted messages* as the addressing mechanism while return receipts are necessarily asynchronous.

In single computer systems, we can experience a lack in the addressing discipline when the paths in the local file system are badly defined and some applications do not work because some data or executable programs are not found.

Addressing through the Internet concerns a complex interaction of technique and human choices. The use of DNS — Domain Name System — for naming and conversion between symbolic names and ip addresses of computers is only one facet of the addressing discipline.

In the modern use of typographical composition of an Internet page, a complex construction of a set of addresses is sometimes needed for obtaining the final form of a document. Components of a document can be addressed dynamically as a consequence of the used browser, geographical location of the user, the history of his access to the Internet, information stored locally as *cookies.*

## 2.6 Naming

*Naming:* the act of giving names is fundamental for the correct functioning of a communication system. Entities cannot be named in an arbitrary or uncontrolled way.

As in the everyday life personal identifiers, telephone numbers and credit cards numbers cannot be attributed in an arbitrary way, in communication systems, the act of naming must be regulated.

At the lowest level of control of a communication system, we experience a lack in attribution of names when individual files or directory names are given in an inconsistent way. At a higher level of complexity, the whole subject of *interoperability* of metadata associated to records or documents exchanged in a communication system depends on distinct naming disciplines in distinct contexts.

At the level of naming of Internet entities, the principal example for the naming discipline is in the collection of procedures associated to the DNS service. Today, this component of the Internet is felt as a weak point.

Another example involving *identification, naming* and *addressing* is related to the ipv4 and ipv6 protocols . The use of the wide range of individual names for devices available through the ipv6, the naming discipline can be seen as a mean for identifying univocally the user of a resource. In this way, some practical and legal problems related to the billing for Internet services and disclosure of the user's names dynamically associated to ipv4 addresses by the Internet providers could be solved technically.

## 2.7 Cancellation

*Cancellation:* this discipline concerns various levels of *correction* or *update* of information.

We can interpret the discipline of cancellation in a simple way as the destruction of a document or its removal from a communication system. Nevertheless, several documents can contain similar information and a discipline that guarantees a complete cancellation is not easy to obtain. Moreover, cancellation can have several pragmatic aspects dependent from the channels over which the order of cancellation and the object of the cancellation order are transmitted.

A simple but abstract example for this discipline is in the revocation of an order that, for being effective, should travel in an opposite way in respect to the path taken by the order itself. In this interpretation, a correct design for a communication system should guarantee that documents run always through cyclic paths.

A more practical example of errors caused by a lack in the correction of an information is in the propagation of the update of the DNS table of addresses in the DNS hierarchy when some symbolic names are re-allocated to new physical addresses. Another example we can find in the Internet world is in the delay in updating cached web pages accessed via some proxy server. In this case, a new page can erroneusly be displayed as the old one and a similar situation can happen with the local cache of the Internet browser. More subtle problems can be caused by the process of *revocation* of digital certificates issued by a certification authority or by some node in a chain of trust.

## 2.8 Composition

*Composition:* This discipline is related to the format taken by an electronic document and the necessity and sufficiency of a specific format for being pertinent to a given communication channel.

An example for this discipline we may find in our common experience – in the standardised formats for official documents. Header, footer, stamps, declaration of affiliation of the signatory of the document can be a necessary condition for the belonging of the document itself to a specific communication channel. In big organisations, a document belongs to a specific workflow if its format is typographically composed in a specific way.

In modern communication systems, metadata are associated to documents and define its identity. Some documents cannot be displayed by dedicated retrieval systems if their metadata is not defined in a specific way. In order to counterfeit an electronic document, its metadata should be counterfeit as well and production of plausible fake documents passes through the reproduction of the right metadata structure for them.

Documents can obviously be used by non-human agents in a line of communication. For example, an electronic document can be a digital certificate. In this case, in order to counterfeit it, together with the correct internal structure of the certificate, the digital signature of the certification authority should be known.

## 2.9 Modelling

*Modelling:* modelling substantially means to understand the reasons and meaning of a model for communication systems that reflect part of the environment in which they are used.

A traditional example of a model of a communication system is in the configuration of the telephone switchboard for big organisations. The decision about how many telephone lines have to be dedicated to the fire brigades, to the internal security, how many to the director's office. In cases of emergency, all the normal users phones have no more access to external lines or are plainly switched off. All these decisions incorporate some element from the environment in which the telephone system has to operate.

A specific error in modelling of communication systems happens when a model working well in a specific context is applied without reflection to another context. We see this situation when, for example, computer tools used with success for forums, blogs or similar *social networks* are used for the organisation of more specific information flows like decision-making processes.

An example of a lack in modelling related to Internet protocols is in the misuse of the collaborative principles implicitly assumed in the first versions of the protocols themselves. The first Internet mail protocol — SMTP, Simple Mail Transfer Protocol, designed exploiting the collaborative effort of several mail servers in delivering the e-mail communications — worked very well in the research environment in which it was designed but has been subject to several modifications and restriction of use for avoiding improper use as soon as it has been applied in the modern Internet environment.

An example that connects economical choices and communication models is in the indexing storage systems for Internet search engines. The first models were based on distributed indexing services willing to share the information collected and allowing for duplications of the indexes. The "winning" model today, on the contrary, is the one of proprietary and centralised indexes.

## 2.10 Authorisation

*Authorisation:* this discipline rules the assignment of access rights and the assignment of the right to issue directives. It schedules the obligations associated to the access rights and the methods of supervision.

Obvious examples of lack in authorisation are in the uncontrolled access to sensitive documents and in directives issued without controlling their execution. As a simple example for this latter case, consider "out-of-office autoreply" messages sent while the owner of the mailbox is present in his office.

More complicated situations — leading sometimes to legal problems — can arise when computers are used as impersonal agents for the execution of Internet attacks. When a third party (not the owner nor the administrator of the computer) uses a weakness in the design of the operating system for gaining its temporary control, to whom should be given the legal responsiblity for having authorised the use of the computer?

## 2.11 Valuation

*Valuation:* this discipline is related to the access to information and the value we are willing to pay for obtaining an information. Here access to the information is not intended as authorisation but as availability.

In the domain of Internet, we can find examples of information hidden in a complicated web site. It is indeed published but practically non-accessible since we do not know where it is.

On the contrary, the apparent ease of access to any kind of web page obtained via the search engines is convincing most of the Internet users that the organisation of the information does not add any value to the information itself. In a naive interpretation, what is not found by the preferred search engine simply does not exist, independently from the order given to list of the retrieved items or from the exclusion of an item from the displayed list.

In this discipline enters as well the filtering of web sites operated by some countries, some times at the level of DNS. In these cases, information disappears from the Internet independently from the organisation and effectiveness in retrieval of the search engines.

## 2.12 Delegation

*Delegation:* This discipline concerns the delegation of tasks from one agency to another in the communication network. Agents can be both personal and impersonal.

Examples of delegation from a personal to impersonal agents are in the mentioned “out-of-office auto-reply” functions provided by e-mail systems or in the “majordomo” senders of mailing lists. In the technical realisation of packet transmission, delegation between nodes for the routing of packets is the basic communication mechanism.

## 2.13 Re-organisation

*Re-organisation:* this discipline is related both to the specification of the system behaviour for reacting to a new situation and to the rules to be followed when a re-organisation is in place somewhere.

All of the reactive systems are subject to some re-organisation. Specific examples of lack in re-organisation can be found in industrial control systems where, for examples, damages are caused by the uncertainty of the rules to be followed when the system is working in a new modality. In the Internet domain, packet transmission is subject to some level of re-organisation in case a communication line is broken.

In the following chapter, the Disciplines will be used as (non mutually exclusive) categories for the classification of Internet incidents.

# Chapter 3

# Taxonomy

## 3.1 Description and method

The classification system we propose is based on the following table:

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | | | | | | | | | | | | | |
| Time | | | | | | | | | | | | | |
| Matter | | | | | | | | | | | | | |
| Process | | | | | | | | | | | | | |
| Result | | | | | | | | | | | | | |

The axes of the table display the two perspectives for the classification of incidents. These two perspectives are: *functional* and *physical*.

On the horizontal dimension, the Disciplines — as explained in the previous chapter — represent the correct functioning of a generic communication system. On the vertical dimension, five generic categories are listed. These categories, whose source is a general schema for the classification of publications [13], represent the "physical" dimension of the incident to the commmunication system we want to categorise. This "physical" dimension is divided in five classes: *space*, *time*, *matter*, *process* and *result*. *Space* and *time* refer, respectively, to the location and time of the incident — origin, target and duration are considered if it is the case — while *matter* refers to the material object of the incident. In our case, by material object of the incident we decided to list both the machines involved or the portion of the communication channels disrupted. The category *process* requires a more detailed explanation: we assume that the use of any communication system is related to some social activity. This activity can be, for example, publication of documents through a web site, retrieval of the documents published in this way, sending or receiveing e-mail communications and so on … Consequently, by *process*, we mean the activity interruped by the fault in the communication system we want to categorise. The category *result* is on the contrary self-explaining: by this term we mean the *output* of the incident.

The points in the table coordinated by the Disciplines and the five vertical categories, when marked by an 'x', represent the functional lack in the communication system we want to categorise.

In the remainig part of this chapter, we will provide some examples and explanation for the categorisation chosen. The ten examples chosen are listed below with their respective references.

1. *The snooping dragon: social-malware surveillance of the Tibetan movement.*
Authors: Shishir Nagaraja, Ross Anderson. Available at:
http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf

2. *Impact of the 2003 Blackouts on Internet Communications - Preliminary Report.*
Authors: James H. Cowie, Andy T. Ogielski, BJ Premore, Eric A. Smith and Todd Underwood, Renesys Corporation www.renesys.com November 21, 2003 (updated March 1, 2004). Available at:
http://www.renesys.com/tech/reports/Renesys_BlackoutReport.pdf

3. *Cyber-war in Estonia and the Middle East.*
Author: Aviram Jenik Network Security, 2009, Issue 4, April 2009, Pages 4–6. Available at:
http://www.sciencedirect.com/science/article/pii/S1353485809700376

4. *Global Energy Cyber-attacks: Night Dragon.*
Available at:
http://www.mcafee.com/ca/resources/white-papers/wp global energy cyberattacks night dragon.pdf

5. *Impact of Hurricane Katrina on Internet Infrastructure.*
Authors: James Cowie, Alin Popescu and Todd Underwood. Available

at:
http://www.renesys.com/tech/presentations/pdf/Renesys-Katrina-Report-9sep2005.pdf

6. *DigiNotar Certificate Authority breach "Operation Black Tulip".* Available at:
http://en.wikipedia.org/wiki/DigiNotar
http://www.rijksoverheid.nl/ministeries/bzk/documenten-en publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html

7. *Evidence of Advanced Persistent Threat: A Case Study of Malware for Political Espionage..* Available at:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6112333

8. *W32. Stuxnet Dossier.* Available at:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

9. *Malicious activity associated with Aurora Internet Explorer Exploit,* US-CERT Alert TA10-055A. Available at:
http://www.us-cert.gov/cas/techalerts/TA10-055A.html

10. *EU sites blocked for anonymous users.* Available at:
http://www.whioam.com/eu sites blocked access by users of anonymizing services

At the present state of development of the method we are not able to give a criterion for distinct associations of lacks in functions (the perspective of the Disciplines) with individual "physical" dimensions. Consequently, when a lack is found, the whole column related to that discipline will be filled in with 'x'. The study about a finer classification relating individual disciplines to individual "physical" dimensions will be the first subject of the future improvements of our method.

In the following sections, a brief description of the incidents listed above will be followed by our proposal of classification in agreement with the table and method described above.

## 3.2 The Snooping Dragon: Social-malware surveillance of the Tibetan movement

In this incident, email attachments appeared to have been the favoured strategy to deliver malicious payloads. The attackers took the trouble to write emails that appeared to come from co-workers: emails were sent to monks, purporting to come from other monks, but that had in fact come from outside. The attackers probably used publicly-accessible mailing-list archives to construct the social-malware emails that they sent to their first targets. The attackers appear to have obtained user passwords through the intrusion and later used these to remotely access the OHHDL (Office of His Holyness Dalai Lama) mail server.

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | India | | x | x | | | | | | | | | |
| Time | 2008 | | x | x | | | | | | | | | |
| Matter | PCs in the Dalai Lama office | | x | x | | | | | | | | | |
| Process | e-mail exchange | | x | x | | | | | | | | | |
| Result | Surveil-lance | | x | x | | | | | | | | | |

Reason for the classification:
Lack in identification of the “fake” letters.
Unauthorised copy of information.

## 3.3 Impact of the 2003 Blackout on Internet Communications

This incident deals with the reliability of Internet during the wide-area failure of the electric power grid in Northeastern US and Canada on 1416

August, 2003. At 16:10 EDT on August 14, a cascading power grid failure rippled across a large sector of the Northeastern US and Ontario, Canada. Within two minutes, the outage was complete across the region. According to the estimates, there were over 9,700 networks in the geographic area affected by blackout. 3,175 networks suffered from abnormal connectivity outages. Of those, more than 2,000 networks suffered severe connectivity outages for longer than 4 hours, and over 1,400 networks for longer than 12 hours (some even longer than 48 hours).

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | U.S.A., Canada | x | x | x | x | x | x | x | x | x | x | x | x |
| Time | 2003 | x | x | x | x | x | x | x | x | x | x | x | x |
| Matter | 3175 subnets | x | x | x | x | x | x | x | x | x | x | x | x |
| Process | All Internet-based processes | x | x | x | x | x | x | x | x | x | x | x | x |
| Result | Network not available from 4 to 48 hours | x | x | x | x | x | x | x | x | x | x | x | x |

Reason for the classification:
Complete unavailability for all of the functions foreseen by the Disciplines.

## 3.4 Cyber-war in Estonia and Middle-East

In April 2007, a massive distributed denial-of service (DDoS) attack overwhelmed most of Estonias Internet infrastructure, bringing online activity almost to a standstill. The targets were not military websites but civilian sites belonging to organisations such as banks, newspapers, internet service providers (ISPs), and even home users. Much of the onslaught came from hackers using ISP addresses in Russia, but the most devastating element in the attack was a botnet which co-opted millions of previously virus infected computers around the globe to pummel the Estonian infrastructure communications. The botnet fooled Estonian network routers into continuously resending useless packets of information to one another, rapidly flooding the infrastructure used to conduct all online business in the country. The attack was centered mainly on small websites which were easy to knock out, but nevertheless was devastatingly effective. Bank websites became unreachable, paralysing most of Estonias financial activity. Press sites also came under attack, in an attempt to disable news sources. ISPs were overwhelmed, blacking out internet access for significant portions of the population. The report does not mention how the computers were infected in the first place, creating a vast network of bot computers.

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | Estonia, Russia | x | | | | | | | x | | | | x |
| Time | 2007 | x | | | | | | | x | | | | x |
| Matter | Several web sites, huge number of PCs | x | | | | | | | x | | | | x |
| Process | All Internet-based government and bank processes | x | | | | | | | x | | | | x |
| Result | Processes interrupted for 2 days | x | | | | | | | x | | | | x |

Reason for the classification:
Lack in modelling for the botnet.
Lack in synchronisation for the denial of service attack.
Lack in re-organisation for the late response of the ISPs to the attack.

Remark:
The overall effect of this incident is a complete lack in the availability of Internet connection for "significant portions of the population" for two days. In this perspective, the incident should have been categorized as a complete blackout as in section 3.3 above. Nevertheless, we would like to keep distinct the two cases since, at least in principle, a rapid re-organisation of the network could have mitigated the effects of the Estonian case.

## 3.5 Global Energy Cyber-attacks: Night Dragon

Starting in November 2009, coordinated covert and targeted cyber-attacks have been conducted against global oil, energy, and petrochemical companies. These attacks have involved social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of remote administration tools (RATs) in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations. In some cases, the files were copied to and downloaded from company web servers by the attackers. In certain cases, the attackers collected data from SCADA (Industrial Process Control) systems.

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | China U.S.A., Taiwan, Grece, Kazakhstan | | x | x | | | | | x | | | | |
| Time | 2009 | | x | x | | | | | x | | | | |
| Matter | Servers of several private companies | | x | x | | | | | x | | | | |
| Process | Data recording and e-mail exchange | | x | x | | | | | x | | | | |
| Result | Copy confidential information | | x | x | | | | | x | | | | |

Reason for the classification:
Lack in modelling for MS Windows, Active Directory vulnerabilities and access to SCADA systems.
Lack in identification for social engineering and phishing.
Unauthorised copy of information.

## 3.6 Impact of Hurricane Katrina on Internet Infrastructure

In 2005, the Gulf Coast of United States was affected by a devastating Hurricane Katrina and caused ravaging through central Florida and Texas, with the most severe destruction occurring in New Orleans, Louisiana and Mississippi. It caused large scale network disruption in some cases up to 72 hours.

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | U.S.A. | x | x | x | x | x | x | x | x | x | x | x | x |
| Time | 2005 | x | x | x | x | x | x | x | x | x | x | x | x |
| Matter | 134 subnets | x | x | x | x | x | x | x | x | x | x | x | x |
| Process | All Internet-based processes | x | x | x | x | x | x | x | x | x | x | x | x |
| Result | Network unavailable for 72 hours | x | x | x | x | x | x | x | x | x | x | x | x |

Reason for the classification:
Complete unavailability for all of the functions foreseen by the Disciplines.

## 3.7 DigiNotar Certificate Authority Breach

DigiNotar B.V. — a subsidiary of VASCO Data Security International based in The Netherlands — was a company providing digital certificate services. Certificates issued include default SSL certificates, qualified certificates and “PKIoverheid” (Dutch Government accredited) certificates.

In July 2011, DigiNotar detected an intrusion into its certificate authority infrastructure resulting in the issue of fraudulent SSL certificates for several popular domains like google.com, microsoft.com, skype.com, addons.mozilla.org, login.live.com, login.yahoo.com, twitter.com, android.com, facebook.com, torproject.org, …

In total, 531 fraudulent certificates were generated by an attacker. The attacker’s original points of entry into the DigiNotar network were two web servers located in the company’s demilitarized zone (DMZ).

The evidence suggests that the hacker was located in Iran and a signature left in a text file points to him being the same attacker who compromised the Comodo certificate authority in March 2011.

It appears that the attacker made available to others one or more certificates and that the one for google.com was used to gain access to Gmail users accounts. The companies and institutions compromised by fraudolent certificates revoked the trust in certificates issued by DigiNotar at different time rates, leaving the users exposed to further exploits for a certain period of time, in some cases until end of September 2011.

Vasco Data Security International announced DigiNotar bankruptcy — after filling for voluntary bankruptcy — on September 20$^{th}$, 2011.

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | The Netherlands, Iran | | | | | | x | x | (x) | | | | |
| Time | 2011 | | | | | | x | x | (x) | | | | |
| Matter | Servers of one Authority Certificates | | | | | | x | x | (x) | | | | |
| Process | Encryption | | | | | | x | x | (x) | | | | |
| Result | Unknown number of users without secure communication channels | | | | | | x | x | (x) | | | | |

Reason for the classification:
Lack in modelling (in parenthesis since the used tactics is not explicitly reported) for the access to the internal network of the company through the DMZ.
Lack in composition for the production of fake certificates.
Lack in cancellation policy for the irregular revocation of the counterfeit certificates.

## 3.8 Malware for Political Espionage

A political figure continued to receive spear-phishing emails that lured him into clicking on shortcuts or opening attachments with file extensions, .doc(x), .xls(x), ... and so on. (Microsoft Office document exploit). A document *.doc sent via email was the “two stage Dropper that injected the malware”. The malware was a narrow-spread espionage software used for exfiltration of email/messaging passwords and documentation related information from the victims computer.

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | Hong Kong, China | | x | x | | | | | x | | | | |
| Time | 2011 | | x | x | | | | | x | | | | |
| Matter | 1 PC | | x | x | | | | | x | | | | |
| Process | e-mail exchange | | x | x | | | | | x | | | | |
| Result | Copy of sensitive information | | x | x | | | | | x | | | | |

Reason for the classification:
Unauthorised copy of information.
Lack in the identification for the phishing e-mail.
Lack in modelling for the “Microsoft Office document exploit”.

## 3.9 Stuxnet

Stuxnet initially spreads via Microsoft Windows, and targets Siemens industrial software and equipment.

Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. The attack was performed with the use of several distinct tactics like zero-day exploits, a Windows rootkit, the first ever PLC rootkit, installation of new drivers, antivirus evasion techniques, hooking code, at least two command and control remote sites . . .

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | Iran plus several other countries | | x | x | | | | x | x | | | | x |
| Time | 2009 - 2012 | | x | x | | | | x | x | | | | x |
| Matter | Some industrial control systems plus 100000 infected hosts | | x | x | | | | x | x | | | | x |
| Process | ICS | | x | x | | | | x | x | | | | x |
| Result | Reprogramming of the ICS | | x | x | | | | x | x | | | | x |

The drivers used needed to be digitally signed. The attackers compromised two digital certificates to achieve this task. Information on the attacked industrial plant was sent to the command and control sites.

To infect their target, Stuxnet would need to be introduced into the target environment. This may have occurred by infecting a willing or unknowing third party, such as a contractor who perhaps had access to the facility, or an insider. The original infection may have been introduced by removable drive.

Reason for the classification:
Unauthorised copy of information for the information sent to the command and control sites.
Lack in composition for the compromised certificates.
Lack in re-oganisation for the Industrial Control System not returning automatically to a safe state.
Lack in modelling for the "zero-day exploits".

## 3.10 Malicious Activity Associated with Aurora Internet Explorer Exploit

Malicious activity detected in mid-December 2009 targeted at least 20 organisations representing multiple industries including chemical, finance, information technology, and media. Investigation into this activity revealed that third parties routinely accessed the personal email accounts of dozens of users based in the United States, China, and Europe.

Further analysis revealed these users were victims of previous phishing scams through which threat actors successfully gained access to their email accounts. The malware used in this incident, exploited a vulnerability in Microsoft Internet Explorer (IE). The vulnerability if successfully exploited, allows for remote code execution.

Among the targeted organisations, Google corporate infrastructure was the primary target, together with the Adobe Systems and several other high profile companies. The attack resulted in IP theft.

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | U.S.A., China, Europe | | x | x | | | | | x | | | | |
| Time | 2009 | | x | x | | | | | x | | | | |
| Matter | Office PC of several companies | | x | x | | | | | x | | | | |
| Process | e-mail exchange | | x | x | | | | | x | | | | |
| Result | Copy of sensitive information | | x | x | | | | | x | | | | |

Reason for the classification:
Unauthorised copy of information.
Lack in identification for the phishing.
Lack in modelling for the Microsoft Internet Explorer vulnerability.

## 3.11 EU sites blocked for anonymous users

In 2012, the European Commission blocked access to public information to anonymous users. Users received the following error message when trying to access the site of the EU Commission: "Network Error (gateway_error) Server overloaded. The gateway may be temporarily unavailable, or there could be a network problem. For assistance, contact your network support team." It was thus shown not transparent and that the IP address was blocked specifically, nor explains why anonymous users were denied access to public information sites.

| | | Synchronisation | Identification | Copying | Addressing | Naming | Cancellation | Composition | Modelling | Authorisation | Valuation | Delegation | Re-organisation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Space | E.U. | | | | | | | | | x | x | | |
| Time | 2012 | | | | | | | | | x | x | | |
| Matter | E.U. web servers | | | | | | | | | x | x | | |
| Process | Access to E.U. public information | | | | | | | | | x | x | | |
| Result | Denied access for a category of users | | | | | | | | | x | x | | |

Reason for the classification:
Lack in an explicit authorisation policy for the access to the EU official web sites.
Difference in value given to information accessed by distinct categories of users.

# Chapter 4

# Plan for the improvement of this taxonomy

The proposed taxonomy and method of classification is subject to several improvements. We foresee three principal directions: 1) from qualitative to comparative measurement; 2) refinement of the “physical” classification; 3) translation to other languages.

Concerning the first point, the proposed taxonomy provides a pure qualitative assessment of the incidents analysed. No comparison is presently possible between two incidents for weighting their relative importance. A first step in this direction could be a pure “counting” of the ‘x’ in the individual tables: to more ‘x’ should correspond a more serious incident. This hypotesis has still to be verified with the cases studied and with the addition of more incidents covering the Disciplines in a more complete way. For example, *delegation* is not presently used for the classification of any incident. A subsequent step in this direction will eventually lead to a numerical “absolute” evaluation of the severity of incidents by associating a number taken from a given scale to each case.

For the second possible improvement, a refinement of the five “physical” categories in the vertical organisation of the tables proposed in the previous chapter. This can be done quite easily in some cases. For example, in case of Internet attacks, the *Space* category could be divided in two distinct locations for origin and target. To the end of the refinement of the “physical” categories, the work already done in [7] and [1] is a valuable base.

Concerning the third possible improvement, we should consider that the final aim of this work is the production of a common nomenclature and valuation process for both the operators and the public at large allowing for a quick reference to the severity of incidents in communication systems. To this end, the availability of the classification system in the main European languages could be a fundamental point for its effective use.

# Bibliography

[1] A. Aviẑienis, J. C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, 2004.

[2] A. Brinson, Robinson A., and M. Rogers. A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investigation*, 3:37–43, 2006.

[3] ENISA. Ontology and taxonomies of resilience, 2011. on-line on October $23^{rd}$ 2012.

[4] Network Working Group. Terena's incident object description and exchange format requirements, 2001. on-line on October $23^{rd}$ 2012.

[5] ISO guide 73. *Risk management — Vocabulary — Guidelines for use in standards.* International Organization for Standardization, Geneva, CH, 2002.

[6] S. Hansman and R. Hunt. A taxonomy of network and computer attacks. *Computers and Security*, 3, 2004.

[7] J. D. Howard and T. A. Longstaff. A common language for computer security incidents. In Sandia National Laboratories, editor, *Sandia Report*, volume SAND98–8667. Lokeed Martin Company, 1998.

[8] ISO-31000. *Risk management — Principles and guidelines.* International Organization for Standardization, Geneva, CH, 2009.

[9] S. Kiltz, A. Lang, and J. Dittmann. Taxonomy for computer security incidents. In L. Janczewski and A. Colarik, editors, *Cyber Warfare and Cyber Terrorism*, Hershey, Pensylvania, U.S.A., 2007. IGI Global.

[10] Kjaerland M. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers and Security*, 25:522–538, 2006.

[11] C. A. Petri. Modelling as a communication discipline. In H. Beilner and Gelenbe E., editors, *Modelling and Performance Evaluation of Computer Systems*, Amsterdam, 1977. North-Holland P. C.

[12] C. A. Petri. Communication disciplines. In B. Shaw, editor, *Computing System Design: Proceedings of the Joint IBM University of Newcastle upon Tyne Seminar*, pages 171–183. University of Newcastle upon Tyne, 1997.

[13] S. R. Ranganathan. *The Colon Classification.* New Brunswick, Rutgers State University, New York, U.S.A., 1965.

[14] G. W. Smith. A taxonomy of security-relevant knowledge. In *Proceedings of the 13$^{th}$ National Security Conference*, pages 776–787, oct 1990.

[15] Taxonomy. *Webster's Third New International Dictionary.* G. & C. Merriam Company, Springfield, Massachusetts, U.S.A., 1961.

[16] L. Wheeler. Security taxonomy and glossary, 2012. on-line on October 23$^{rd}$ 2012.

European Commission
**EUR 25568 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen**

Title: **A Taxonomy for Incidents in Communication Systems**

Authors: Carlo Ferigato, Saša Gligorijević

Luxembourg: Publications Office of the European Union

2012 – 41 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424 (online), ISSN 1018-5593 (print)

ISBN 978-92-79-27152-6 (pdf)
ISBN 978-92-79-27153-3 (print))

doi:10.2788/60981

## Abstract

This report deals with the construction of a taxonomy of incidents in communication systems. By taxonomy we mean the systematic distinguishing ordering and naming of type groups within a subject field: classification.

The report is organised as follows: the present section concerns a survey of existing taxonomies, glossaries or controlled languages for computer security incidents. It starts with a definition of the terms used in this report and a discussion on the use of taxonomies as measurement tools. The survey aims at clarifying the importance of the definition of a common language for exchanging and gathering information on computer security.

The second section presents the original ideas for the taxonomy proposed with this report. The main assumption is in the definition of the main functions a communication system should perform and in defining a disruption as the lack of one of these functions.

The third section is the actual presentation of the taxonomy. Some examples of classification in this taxonomy of known computer security incidents are added. While the overall aim of this work is at the construction of complete taxonomy for communication systems | including the telecommunication services | the examples provided in this section will mainly deal with disruptions occurring in the Internet domain.

The fourth section presents the future work to be done for continuing the development of the taxonomy proposed here.

LB-NA-25568-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

ISBN 978-92-79-27152-6

Publications Office