M O T I A

Modelling Tools for Interdependence Assessment in ICT Systems

(JLS/2009/CIPS/AG/C1-016)

Mid-Term Report

Project activities during the first year

Version 1.0

Leading organization for this Activity:

ENEA.

With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme'
European Commission - Directorate-General Justice, Freedom and Security'

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

Dissemination Level	**PU** Public

Editor(s)	**ENEA: Gregorio D'Agostino**
Author(s)	**(Caspur) Maria Cristina Brugnoli, Emiliano Casalicchio** **(CNR-IIT) Enrico Gregori, Chiara Orsini** **(ENEA) Gregorio D'Agostino**
Contributor(s)	**(ENEA) Gregorio De Nicola** **(MIX-IT srl) GianMarco Clerici, Valeria Rossi** **(Namex) Francesco Ferreri, Flavio Luciani** **(Regione Toscana) Giovanni Armanino, Angelo Marcotulli** **(Telcom Italia) Maurizio Cardarilli, Biagio Di Carlo** **(TOP-IX) Luca Cicchelli, Andrea Rivetti**

Activity 1	**Mid Term Report**
Remarks	

Changes	Authors and added contributes	Date
	Gregorio D'Agostino	28/05/2011

Review	
Approval date	
Remarks	

Table of Contents

Introduction....4
General Definitions....7
Activity I Main Outcomes: “Identifying relevant Entities and their Mutual Relations”....9
Operator Characterization....9
Protocol Characterization....9
Physical infrastructure classification....9
Application Domain Characterization....10
IP Analysis....10
Activity II Main outcomes: “Topological Analysis”....12
Data collection....12
Automated Ip recognition Methods....13
Measurement tools....13
Pro and con....14
Linking Autonomous Systems to the physical layer....14
Simulation Epidemic Malware Spread....17
Research plan and overall design....19
Introduction....19
Objectives....19
Methodology and profile of the participants....20
MOTIA Interview Schedule....21
Annexes....24
Conclusions....27
References....28
Glossary of employed basic definitions....29

Introduction

Quality and quantity of main services provided to our modern society has been steadily increasing during last thirty years. In order to improve their performance and to enhance their reliability, the infrastructures have been endowed with increasingly complex connection networks allowing their governance optimization and reducing number of people to be allocated to that purpose. Some of such infrastructures have been regarded as critical as they provide fundamental services for any modern technological society [1].

In this context, during the last decade, a lot of efforts have been devoted to provide evidence of dependencies among the main (critical) infrastructures and to discuss their mutual dependencies. Dependencies have been outlines and classified according to several different perspectives [2]. Nevertheless, not so many efforts have been devoted to quantify such dependencies, that is to provide meaningful indices to size the intensities of Critical Infrastructure (CI) mutual dependencies. The MOTIA project has the ambition to define a methodology for providing quantitative estimates of such dependencies for the Information and Communication Technology (ICT) sector standalone. Hereafter those quantitative estimates will be referred to as "metrics" even though from a strict mathematical point o view the term "measure" should have been preferred. Unfortunately in the CI jargon "measure" refers to the counter-measures token by the operators upon undesired event occurrence or dwelling situations, in order to mitigate negative impacts.

Information and Communication Technology represents a broad term employed to refer to all technical means used to handle information and allow communication. In the present paper and basically in the entire MOTIA project focus will be on Internet, meant as all the means employed to convey information throwout different application and protocols (mostly the TCP-IP protocol Suite).

Several services (if not all of them) directly or indirectly rely on network communications. From very simple servicies such as Flight or Hotel reservation to very complex ones such us our project reference “case study” (the Italian “Sistema Pubblico di Connettività” SPC hereafter), as a general rule, the entities providing the service to people have an absolutely insufficient level of awareness of their dependence on physical infrastructures, on operators and especially on underlying Basic Internet Services (UBIS) such as the Domain Name Servers (DNS). Almost all commercial providers and possibly even the Internet Service Providers (ISP) thrust the Internet (human, physical and logical) infrastructure without entering its mechanisms and disregarding any information on its vulnerabilities, robustness and resiliency. The MOTIA project represents an attempt to assess a methodology to approach the problem of dependence (or interdependence); following that methodology, in principle, any enduser may quantify its dependence on physical infrastructure, logical internet organization and UBIS.

The main steps to be performed follow:

1) Identifying and classifying the most relevant ICT networks and their elements (transport, inter-operability application and cooperative application) at the different layers of ICT network stack. Given the scope of the analyses, humans involved in ICT systems management and service end-users will be accounted for, as well as physical devices. Emerging technologies, forthcoming ICT operators, developing trends and related integration problems will also be framed.

2) Acquiring valuable information about the different relations existing among these elements taking into account physical, geo&logical dependencies. Codify these information into structures able to provide useful hints about relevance and criticality of each element.

3) Merging the most significant information acquired into a single multi-graph representation.

4) Identifying a set of metrics capable to represent the degree of network dependability, network service level and impact factor.

5) Quantifying, via the proposed metrics, the degree of inter-dependency existing among the ICT

The ambitious purpose of the project is to assess a strategy to analyse interdependent ICT network, thus providing suggestions to improve robustness (or resilience) of the whole system while keeping or even improving the Quality of Service.

So far the first two topics have been realized and other activities have been initiated. The dissemination activity has started immediately after the kickoff meeting. A web site has been realized by means of the "drupal 6" open source product that allows for both internal data sharing among consortium partners and project advertizement. The domain names www.motia.eu and motia.eu have been both allocated to the project web site.

The activity IV of the project, consists into the application of the designed methodology to an italian representative case-study represented by the Italian Connectivity Pubblic System (SPC i.e. Sistema Pubblico Connettività). It will be coordinated by the DigitPA project partner. The SPC represents the Italian aggregated system to provide Public Administration Services via a shared interface. Through the SPC, the user may achieve information on his/her own or other official state with respect to several Italian Institutions, such as: Erario (Taxes/Revenue Department), Anagrafi dei Comuni (City Halls' Office Register), Procure e Tribunali (civil and penal law-courts) and others. Certificate information are made available while respecting Italian laws on privacy and requiring a unique act of protected Registration. Italian long term plans foresee to provide access to almost all public Acts and Information through SPC. The basic characteristics of the system have been presented and discussed in the second project Meeting. The complexity of the testbed is supposed to inform the whole system. A complete success of the MOTIA project would be the adoption of the assessed methodology by a wide range of European companies or public institutions. A partial success would be the redesign of the italian SPC based on the project outcomes.

By the time this report is presented, the project is almost half the way: identification of Boundaries and relation among infrastructure has been performed (see devoted deliverable for details) and the methodology for the topological analysis of the internet has been assessed. As lateral activities, malware propagation modelling and topological analysis of the Italian internet at Autonomous System level have been partly performed. The analysis of dependencies at service level will be the main focus of the project and has already started; nevertheless preliminary results are only available in a very rough form and can not be disseminated yet.

In the last decade several projects were started to achieve a better knowledge of the Internet infrastructure. The activity II had the target to analyze the state of the art of the ongoing Internet measurement projects are related to the target of the Motia Project. We have divided the section into two main parts. The first subsection focuses on the very limited activity that has been performed to gain a better knowledge of the physical and Data link components of the Internet Infrastructure. The second subsection focuses on the IP level. Research on the analysis of the Internet infrastructure at the IP Level started almost ten years ago, but is far from being completed. There have been some attempts to get Internet descriptors at the IP level but these data were shown to be inaccurate due to limitations on the topology discovering tools and due to the tendency of the ISPs (Internet Service Providers) to treat their IP infrastructures as a confidential key component of their business. The topology discovery projects were more successful in the discovery of the Internet topology at the AS (Autonomous System) level and there are several freely available internet descriptors that were obtained by these projects. Available dataset were built setting up a measurement infrastructure that

collects topology data obtained either via “traceroute” software or via Border Gataway Protocol (BGP) update messages.

Details concerning each of the first two activities may be found in the devoted deliverables.

Activity III has already started and an analysis of automated means to analyse an infrastructure at service level has been presented at Project meeting III.

Three technical meeting has been organized to brief about developments and assess the follow up of each activity.

One of the concerns of the MOTIA consortium is to understand whether the project addresses questions relevant to the real end users. In this context, by representative End User or simply enduser is intended a public or private entity deeply relying on the ICT and providing significant services or good to the people. In order to evaluate the interest of endusers on the project topics and possible results, a set of interviews has been realized with some italian enduser: “Poste Italiane” (the incumbent Italian postal operator, “ABI” (Associazione Italiana Banche), the Italian association for banks, and ENAV, the Italian monopolistic private company for flights control. A modern approach to interviews has been implemented. A round table with the enduser was foreseen to take place in Bruxelles on October 2010; the consortium has experienced a lot of difficulties to bring representative european enduser at that table and the event has been delayed and possibly withdrawn.

A draft of the project (to date) achievements is be reported in the next sections, larger information are be available in deliverable format at project site (http://www.motia.eu).

The remaining part of the present document is organized as follows: In the first chapter very basic defintion of the concept of “dependence” is introduced; the following chapters shortly summarize the results of activity I and II respectively; a short chapter is devoted to sketch malware epidemics simulations; the final chapter reports on the preliminar work performed to evaluate the impact analysis of the project on endusers and reports on the enduser suggestions for the project.

All along the paper, the OSI (Open Systems Interconnection) model is continuously referenced [3] with its seven levels (L1-7): physical, data link, network, transport, session, presentation, application; in many cases a simplified view will be employed based on three levels only: Transmission, Ip and Application.

General Definitions

Infrastructure is a very recurrent term employed to refer to a set of physical, logical and possibly human components deviced to provide a service. ICT infrastructures are the complex human systems devoted to elaborate, store and echange information.

Dependence is a wide term indicating the need of an infrastructure (or a component) of an other to perform its functioning. The former general definition may be implemented in many different respects. During last decades a lot of definition have been introduced to measure different characteristics of the mutual relation among different systems or components. Several definitions are reported in annex A.

Several of the different concepts introduced in the Risk analysis are worth employed to measure dependence. While not refusing the risk analysis, the Motia approach aims at extracting the cause-effect relationships disregarding the probability (or the likelihood) of occurrence of undesired events. The need of quantities based on impacts rather than on total risk is consistent with the EU (2009) directive on recognition of European Critical Infrastructures (CI), where they are identified based on potential consequences of their damage upon natural hazards or deliberate anthropic attacks. More precisely the global impact of an undesired event is due to two different factors the direct damage of the infrastructure (or infrastructures) and the cascading effects. The interdependence, in a strict sense, does not relate to the probability of a event nor to the final impact on the people (and their social organization), yet on the way it propagates in the infrastructure. More precisely the project intends to measure (when possible) to what extent a damage in a system (or component) may reflect on an other; or, conversely, to what extent a system or component depends on an other. A metric will be a positive function in the [0,1] range measuring such dependence. The unitary value will represent a total dependence, that is the lack of a system (or component) leads to a complete inoperability of an other; while the null value of dependence indicates that functioning in unaffected by the system (or component) loss.

To be more quantitative let us first start from the quantitative definition of “risk”:

$$R_e \overset{\text{def}}{=} L_e \cdot I_e \quad ;$$

were R_e represents the *risk* associated with an undesired event “*e*”, L_e represents the *likelihood* (or the probability) of such an event and I_e represents the *impact* (or the *loss*) it produces.

When all possible undesired event are known, an inequality to estimate the total risk associated with the infrastructure can be stated:

$$R \leq \sum_{e \in E} R_e \quad ;$$

where the sum is over all undesired events and the equality holds for a set of mutually excluding (disjoint) events:

$$R = \sum_{e \in E} R_e \quad .$$

When an incomplete set of disjoint undesired events is known, a lower bound of the total risk can be obtained:

$$R < \sum_{e \in E'} R_e \quad ;$$

where the set E' reprensents a proper subset of E.

Many dependence indices defined in the literature are based on assumptions on the likelihood of undesired events. The typical example is the reliability defined as (an estimate of) the probability for a component to experience a failure and often measured by means of the “Mean Time to a Failure”, (MTTF) that is the average time for a failure to occur. To completely describe the reliability of a component the probability of a failure as a function of time should be given; the syntetic MTTF parameter allows to evaluate it under appropriate hypoteses.

The loss associate with an event L_e deserves some further discussion. The European commission indicated three main impact parameters based on “casualities”, “economic loss”, and “loss in public thrustworthy”. However one tries to measure such impacts, they are hetorogeneous and hence difficult to compare or combine; therefore for each of them (or for a a suitable combination of them) one has to introduce a specific means to evaluate the impact.

Private (profit) operators and asset owners employ their own impact functions basically based on their economic loss and loss in their public image (that is customers' thrust). In principle, despite their official positions, casualties or other other damages their malfunctioning may cause on society are accounted as they have consequences on the first two items or may lead to penal prosecution of managers (in case human responsibility may be foreseen). On the other hand, the perspective of the State Members and the European Union is slightly different as final cost of service, people health and costumers satisfation must be accounted for. Which ever the perspective, in order to perform an impact analysis, one needs to know the three different functions representing and measuring the three losses L_e.

When dealing with most of services and especially on ICT ones, losses are usually indirect consequences while the original failure propagates in the system leading to a degradation (or deny) of service. To measure the impact of the resulting level of service (upon an event) is extremely relevant topic that is far from the purposes of the MOTIA project. The basic idea of “dependence” is the cause-effect relationship among the initial undesired event and the resulting QoS (Quality of Sevice) or inoperability level.

The work package V will clarify the meaning of the former focus and will provide quantitative indices associated with the different possible definitions. At the end of this publication a Glossary containing several terms related to risk and dependence analysis is reported to clarify the meaning of employed terms.

Activity I Main Outcomes: “Identifying relevant Entities and their Mutual Relations”

The first activity of the project has been devoted to the identification of the basic entities involved in the ICT reality. As a very complex infrastructure the global ICT world involves physical, logical and human, active and passive components. An adequate abstraction of the problem (“problem posing”) represents a pre-requisite for any Analysis and Modelling (A&M).

In the MOTIA project both physical and logical infrastructures have been dealt with, while keeping human organization (meant as human capability do take decisions) apart. Modelling of human behavior as customers, endusers, operators, asset owners, rulers etc represents a very important part of the problem that has been purposely neglected. Therefore the focus has been on physical infrastructures characterization and entities managing them.

Operator Characterization

A basic categorization of the operators can be summarized as follows:

1. Operators owning their physical infrastructure and providing services on top of it
2. Operators buying or hiring physical infrastructures (dark fiber) from (1) and providing services on top of it
3. Operators running services based on lower layer services provided by third parties (that can be both (1) or (2))

It is worth stressing that a clearcut separation of the three typologies is not always feasible as, basically due to anti-trust regulations, very often operators own just a part of their asset (typically a “backbone”) and rely on former monopolist for the access (last mile) and complete covering of their customer target. Therefore hybrids represent a rule more than an exception.

The knowledge of operators interdependence and their (ownership and governance) hierarchy deeply influences the quality of the services (QoS) deployed in the net. Moreover outlining dependence on actual asset owners may unveil critical dependence on incumbent national carriers that a pure legal responsibility approach may hidden.

It is extremely important to make a distinction between the legal responsibility and operative involvement on the deployment of a complex service on the net. The Motia project is devoting a lot of efforts to understand enduser perspective; to this purpose preliminary interviews have been performed. From such interviews (especially with bank operators) a clearcut problem emerged (among many others). When buying IP connectivity, Deny of Service is often foreseen in the legal contracts and it may lead to possible refunds. However this does not enhance the resilience of the service, neither provides any awareness of vulnerabilities or improves response capabilities upon undesired events.

Protocol Characterization

An other important classification (at logical level) is related to the communication protocols. Communication protocols are typically organized as a stack and each layer of the stack isolates (from a logical/physical point of view) a part of the system/network. To date the majority of the deployed services rely on TCP-IP or (UDP) communication protocols and the project has been focused on those.

Physical infrastructure classification

The classification of communication links and devices at physical level may also influence the capability of the infrastructure to convey the information: bandwidth, robustness, resilience are a direct consequence of the physical support (and the way it is managed). The wide variety of means (wireless and cabled, based on fiber or copper) together with the appropriate protocols to handle

them are discussed in the forthcoming deliverable of activity one to be published at project web site. However, most of the A&M do not depend on infrastructures details and are basically related to the topology of the system and capacities of the established connections.

Application Domain Characterization

Each application domain offers functionalities to a specific set of customers that can be other application domains or end users. Therefore, application domain can be classifies on the basis of the other application domains they interact with. This classification of application domains allow to identify functional boundaries among applications. The distributed application architectural model has been embraced. Each application domain is characterized by a different architectural/computational model. The knowledge of the architectural/computational model allows to identify the actors/systems involved in the inter-system, intra-system interactions.

The methodology adopted to identify relationships and boundaries among different ICT networks and systems is basically outlined in the following. Each phase is widely discussed in details in the first Activity Report to appear on the MOTIA web side.

1) Identification of the communication protocol reference model. We consider the TCP/IP reference model, that implicitly introduce three vertical boundaries separating the infrastructure to transport signals (the physical layer), the infrastructure to transfer data packets (the Internet layer) and the infrastructures to implement internet applications (the Application layer). The project will study relationships (dependencies and inter-dependencies) among these layers and inside each layer.

2) Identification of the boundaries among ICT systems and networks at application layer. At Application layer we will identify boundaries among networks and systems working at the same layer. The goal of the project is to provide a general characterization of boundaries rather than a characterization for a specific system. The boundaries identification is performed in two steps:

a) identifying the application domain of interest for the MOTIA project and the related communication protocols used at application layer;

b) classifying the applications on the base of "who" will use them (customer services, utility services and internet services). These classes of applications themselves constitute the boundaries and the protocols allow to understand what are the relationships among classes. Dependencies between application classes are intra-domain, while relationships among components of an application are inter-domain.

3) Identification of the relationships among ICT systems and networks at application layer: i.e. discovering of relationships among networks and systems working at the same layer. The goal of the project is to provide a general characterization of relationships rather then a characterization for a specific system. To achieve this goal we will identify the computational models the applications are based on.

The identification of the computational models plays a fundamental role to understand (independently on the specific application), what are the actors/components involved, what are the interactions among components belonging to a specific system/network and what are the interactions among components belonging to different systems/networks. This relationship identification is fundamental to characterize and identify inter-domain and intra-domain dependencies.

IP Analysis

A network is generally intended as a set of hosts connected to one or more Local Area Networks (LAN), in turn interconnected, that all together form an administrative domain: in the Internet an IP network is the minimum unit to implement a routing policies over a packet-based network.

The network concept embodies many different things differing in nature and size, ranging from a home wi-fi network that connects a laptop or two, up to the network of a large organization with thousands of hosts connected to hundreds of LANs (Local Area Networks), geographically

distributed across multiple continents. In few words Internet can be regarded as a “Net of Nets”. The elemental unit for inter-domain routing policy can be selected of different sizes. The MOTIA project has (mostly) selected the Autonomous System (AS) [18] as basic constituent of the global think. The management of packets exchanged between interconnected AS is typically delegated to specialized hosts (gateway or IP router [Errore: sorgente del riferimento non trovata] located at their boundaries. Nowadays, the routing protocol utilized on AS’s border routers is the BGP-4 [17].

Many types of network can be implemented as an overlay network of Internet, like peer-2-peer networks used for file sharing. Many virtualization layer can be added upon an IP network, via different technical features, like MPLS (Multi Protocol Label Switching), or any kind of VPN (Virtual Private Network), like a simple IP tunneling. Most of the applications (and consequently the project analysis) are based on such higher level virtualization.

The linkage (mutual connection) of any two networks, can take place in basically three ways: via “transit”, an upstream network or a chain of upstreams; via a direct link (direct or private peering) or via “public peering” by an IXP (Internet eXchange Point). The above three ways to interconnect networks are not mutually exclusive, since typically large networks adopt more than one to guarantee the network’ reliability and availability. Moreover, redundant connections (more instances of the same method) may be established to increase reliability. In the Internet model, upstream networks are typically identified with the Internet Service Providers (ISP). Each ISP has assigned one or more AS Numbers to manage its routing policy to the rest of the Internet. Internet global connectivity is therefore guaranteed by a mesh of IP network connections between ASes. The ISP form a Tier Hierarchy, according to “who provides transit to who”. Such a hierarchy represents a significant (yet unofficial) business “ranking” of the ISPs. There is a small number of very large ISPs that don’t purchase Internet transit from anyone else, and they just peer among themselves and sell transit to all other smaller ISPs. They are the so called Tier-1 Internet providers. The other tiers follow orderly. The tier level represents a natural ranking of “dependence”. Quantification of such dependencies by means of “metrics” will be one of the purposes of the Motia project.

As can be seen, the MOTIA approach is very orthodox. This is due to the need to provide “best practice” and trustworthy results. Details on the approach are reported in the already mentioned deliverable I.

Activity II Main outcomes: “Topological Analysis”

The present paragraph aims at defining the support that topological analysis of complex networks (representing Critical Infrastructures at the highest level of abstraction) might provide to provide insights and to identify basic interdependency mechanisms and effects. The Internet infrastructure (or any other ICT infrastructure) can be initially regarded (an modeled) as a mathematical object, a graph, consisting of different elements such as nodes and arcs (or links) which are functional elements connecting the nodes. Despite its simplicity (the graph metaphor does not account for the complexities related to the structure of nodes, the type of information that flows in its links etc.), the graph represents a useful mathematical object since it is able to store and resume a number of relevant properties of the network. The former can be unveiled by evaluating topological graph’s properties by means of mathematical tools.

The main purpose of the present chapter is to provide a basic discussion on the topological approach to the internet (or other ICT net) analysis. The results of this preliminary analysis, can be valuable to understand basic features of the very complex infrastructures one has to deal with.

Graph analysis is an old branch of mathematics. However, much work has been devoted in this domain during the last years as the methodological approach (the reduction of complex systems to graphs) has been used to study a large variety of complex systems: genomics, biological objects, social aggregation of humans (crowds) etc. Technological and virtual objects (the Internet, the WWW etc.) have been studied by first reducing their structure and complexity into a simple graph. This approach has been also adopted to understand complex phenomena acting in these systems, such as growth mechanisms (often complex systems grow with no external supervision; the growth mechanism is thus a critical information able to unveil relevant properties of the system under study), synchronization etc.

Several seminal works have been published in recent years on these topics [5, 6, 7]: the reader is referred to these work for a deeper and mathematically rigorous treatment. Basic concepts have been reported here for self-consistency purposes.

Data collection

The first problem to be faced when dealing with the analysis of Critical Infrastructures in general and especially the Internet is data collection. Correctness and completeness of data represent prerequisites to perform any reliable analysis,

The straightest (and most effective) means to achieve reliable data is represented by the direct provision from the asset owners or asset managers, that is collecting them from the private or public entities having a direct commitment in the operation of the infrastructures. Apart from direct acquisition, other methods can be used to (partially) bypass data unavailability and to allow, at least, a partial reconstruction of the actual system topology.

Data are often available in the form of GIS (Geographic Information System) databases that can be used in appropriate viewer allowing immediate data contextualization and their merging in wider complex scenarios.

Direct acquisition, however, usually encounters several drawbacks that have been identified and, ipso facto, undermine the accessibility of data to be used in the analysis. Among them, it is worth quoting the following:

a) privacy laws may forbid or limit data release; b) when owned by private companies, data access can be restricted for both security and marketing policies; c) data are stored by the CI owners in complex formats, rich of details, such as GIS and similar format on proprietary databases which, although being accessible, cannot be used as a whole and downloaded; d) data are spread among different public or private subjects: asset owners, governmental institutions, market operators etc. e) private and public subjects may exhibit poor capability to extract required information from their own internal organization. f) means to provide connectivity (namely devices, cables of different

types and communication protocols) are tremendously heterogeneous both at physical and application level.

Apart from direct access methods, further methods can be employed to (partially) bypass data unavailability and to allow, at least, a partial reconstruction of the actual system topology. It is worth stressing that the use of the automated techniques mentioned above may provide a part of the topological structure of the net, but asset owners and connection providers may impose legal constraints to consumer contracts to prevent such 'parasitic acquisition'. On the other hand, government authorities might impose transparency constraints to connectivity commerce supporting critical services on TCL systems. To the best of our knowledge almost nothing has been done in this respect, while Banks, financial agencies, postal service providers and many significant "endusers" are claiming for a policy. Legal regulation is not expected to be the elective solution by neither the providers nor the end-users, nevertheless the knowledge of limits and known vulnerabilities seems to be the basis for a synergistic approach.

The problem of net topology recognition will be further detailed in the present document.

Automated Ip recognition Methods

The Internet is often described as a network of networks, a global system of interconnected computer networks using the standardized Internet Protocol Suite. A connected group of one or more IP prefixes run by one or more network operators having a single and clearly defined routing policy is identified as an Autonomous System (AS). An AS shares routing information with other ASes using the Border Gateway Protocol (BGP). Establishing connections is driven more by business factors than attempts to optimize performance. As stated before, there are two main classes of connections: provider-customer and peer-to-peer. In the former, an AS (customer) pays another AS (provider) to obtain Internet access (transit). In the latter, two networks' (peers) customers exchange traffic between each other for their mutual benefit. Peer-to-peer connections can be settlement-free or paid, depending on the ASes interacting and the type of contract stipulated. In this context, a peculiar role is played by Internet Exchange Points (IXPs). The former are physical infrastructures which allow ASes to exchange Internet traffic, usually by means of mutual peering agreements, leading to lower costs (and, sometimes, lower latency) than in up- stream provider-customer connections.

An Internet AS-level topology can be easily described as an undirected graph: nodes represent ASes while edges indicate the presence of one or more BGP connections between two AS's. There are several sources of Internet AS-level topology data (datasets hereafter) obtained by different projects obtained using different methodologies which yield quite dissimilar topological views of the Internet. Most of the studies rely either on BGP-based data or on traceroute experiments. In both cases, the datasets represent biased views of the actual topology and are also largely incomplete. To date, few efforts have been spent to provide a detailed analytical comparison of the most important topology properties extracted from the different data sources.

Measurement tools

To date there is no specifically designed tool to derive topology information on the Internet, therefore researchers had to derive it using various indirect measurements that provide some information on the existence of ASes and the connections between them. Internet AS-level topology data collected within the framework of these projects were obtained by using different methodologies that yield quite different topological views of the Internet. To build the Internet AS-level topology, each project used different tools to gather data from the Internet. Some tools, based on traceroute measurements, take dynamical snapshots of the Internet by gathering a sequence of IP hops (via either UDP or ICMP probe packets) along the forward path from the source to a given destination. Other tools gather both static snapshots of the BGP routing tables and dynamic BGP data in the form of BGP message dumps (UPDATEs and WITHDRAWALs BGP messages).

Data collected by the traceroute and BGP approaches are very reliable, but, unfortunately, they are largely incomplete.

Datasets links can be gathered by three methodologies: active probing: datasets are obtained by traceroute-like methods (e.g. Ark, Dimes [9]); passive measurement: it relies on an observation point within the network capturing live data from a portion of the network (e.g. CAIDA AS relationships, Robtex, Cyclops); public published information retrieval e.g. Internet Routing Registers [16].

Pro and con

Having a complete and up-to-date view of Internet is a real challenge. There are several issues dealing with the following matters: inter-domain routing is not guided by technical features, it is mainly ruled by economic factors; BGP sessions are not always public, some ASes connections are confidential; business relationships are confidential too and they need to be inferred by some heuristic algorithm; business relationships have a lot of background details (which affect routing), provider to customer and peer to peer classes alone are not able to capture the full heterogeneity of Internet market (e.g peering can be settlement free or paid).

Linking Autonomous Systems to the physical layer

A useful study on the incompleteness of AS level data has been performed in [15], where the authors highlight that missing connections can be categorized into two classes: hidden connections and invisible connections. Hidden connections are defined as connections not observed by the monitors, but that could be possibly revealed at a later time (e.g. backup connections). Invisible connections are defined as connections that are impossible to observe with the current set of monitors (e.g. peering connections established between small ASes that will not be announced to any other AS). The evidence for missing links led us to merge together the most significant available projects. A more detailed description of this procedure will be discussed in the following of this paper. Each project has its own specific set of monitors, in different geographical locations and connected with different AS's. Thus, each project contributes with its own view of the Internet. Merging multiple data sources will not solve the problem of invisible links, but should improve the knowledge of the Internet AS-level topology.

In this report three Internet AS-level topology datasets have been considered; they are all publicly available and represent the most frequently used by the research community: The IPv4 Routed/24 AS Links dataset.1 This dataset is handled by CAIDA (Cooperative Association for Internet Data Analysis) [8] using the Archipelago2 (Ark) measurement infrastructure. The latter is composed by a worldwide distributed set of active monitors, which continuously send Scamper3 probes to destination IP addresses, which, in turn, are connected to a central server. Next, the IP addresses found are mapped to AS numbers with Route Views BGP tables and the AS-level topology is retrieved. Probes are carried out by TCP-, UDP-, and ICMP-based traceroute measurements and Paris traceroute variations. IPv4 prefixes are created using updated Route Views BGP tables. The Distributed Internet MEasurements and Simulations (DIMES) [9] dataset. This dataset is collected and archived by an Israeli scientific research project launched in September 2004 using an infrastructure composed by a geographically distributed set of agents downloaded by volunteers located all over the World. Each of these agents performs traceroute probes to a shared subset of IP addresses collected from a BGP prefix database and sends gathered data to a central server which collects them and infers the topology. Further details are available in [9]. The Internet Topology Collection at the Internet Research Lab (IRL) dataset. This dataset, created by a team of researchers at UCLA () , infers the topology using BGP routing tables and UPDATEs collected by several ongoing projects (i.e. Route Views, RIPE Routing Information Service (RIS), Abilene and collecting BGP data through route and looking "glasses" servers.

The above three datasets were originally built using two different methodologies. In the MOTIA Activity II all the collected data have been merged using the same methodology; thus forming two different datasets referred to as: Traceroutes: the union of DIMES and CAIDA datasets, BGP: the IRL dataset.

In addition, in this paper we often use the following dataset: Merge: the fusion of DIMES, CAIDA and IRL datasets.

It is worth noting that all data gathered from each of the projects were analyzed and checked before being regarded as "correct". Specifically, as a result of such screening, the following have been removed from the resulting topology: ASNs declared as private by IANA, AS 23456 which, according to RFC 4893 is reserved and assigned for AS TRANS, AS 3130 which, according to the Cyclops website, shows false AS adjacencies due to an experiment by Randy Bush.

Comparing the DIMES and CAIDA traceroute-derived graphs, we can see that the sets of their constituent connections are quite different, i.e. 51.9% of connections are common to both datasets, while 22.4% are only present in CAIDA, and 25.7% are only present in DIMES. From the above considerations, we can draw the following conclusions: (a) both datasets enrich the Traceroutes dataset: (b) measuring procedures using the same tool (traceroute) can lead to substantially different results.

Hereafter the topologies inferred from Traceroutes, BGP and Merge datasets will be referred to as Traceroutes, BGP and Merge topologies, respectively. Furthermore, we will still continue to use the expressions Traceroutes and BGP methodologies.

Table 1: Autonomous System recognition: comparison of the different dataset.

Dataset	Number of Nodes	Number of Connections
CAIDA	28821	73271
IRL	37258	121634
MERGE	37258	144416

By analyzing the number of nodes in Table 1, we can observe that traceroute-based methods are able to discover a smaller number of ASes compared to BGP methods, while a very limited number of nodes (27 out of 34,955) were discovered by Traceroutes methods, but not by BGP methods. An analysis of the number of connections indicates that Traceroutes and BGP complement each other very well (e.g. Traceroutes increases the number of connections discovered by BGP by about 20%). Only 37.6% of the connections in the Merge dataset were discovered by both methods, while the remaining 62.4% of the connections was discovered either by the Traceroutes (21.9%) or by the BGP (40.5%) methods.

An additional topology data source is potentially represented by Internet registries, however their content is not completely reliable since the entries are inserted manually by administrators. Our tools are currently not able to distinguish which entries are out- dated or subject to human error from those which may be useful for our purposes. For this reason, we will not consider the Internet registries as data source in our work.

3.6 Recognition Process Validation

Despite significant efforts spent to obtain an accurate picture of the Internet connectivity structure at the level of individual autonomous systems (ASes), much has remained unknown in terms of the quality of the inferred AS maps that have been widely used by the research community. In this Section we assess the quality of the inferred Internet maps through case studies of a sample set of ASes.

Since the main italian IXP (MIX, NAMEX, Regione Toscana and TOPIX) belong to the Motia consortium, we were able to validate the inferred connectivity among different ASes. We have considered the ground truth connectivity information provided by the IXP's and compared those data with our Internet dataset. A direct comparison between the ground truth and inferred topology maps yield insights into questions such as which parts of the actual topology are adequately captured by the inferred maps, which parts are missing and why, and what is the percentage of missing links in these parts. This information is critical in assessing, for each class of real-world networking problems, whether the use of currently inferred AS maps or proposed AS topology models is, or is not, appropriate.

Given that the public view captures almost all the AS nodes and customer-provider links, it provides an adequate data source for studies on AS-topology metrics including network diameter; growth rates and trends for the number of stub ASes; and quantifying customer multihoming [ ] (where multihoming here does not account peer links).

Given that the public view is largely inadequate in covering peer links, and given that these peer links typically allow for shortcuts in the data plane, relying on the public view can clearly cause major distortions when studying generic graph properties such as node degrees, path lengths, node clustering, etc.

If we suppose that Internet connections crossing IXPs are likely to be peering relationships, then we can confirm that current Internet topologies lack for many peering connections, as expected. Statistical quantitative Data concerning missed and hidden links will be reported in the deliverable II (available at project site) and in forthcoming publications.

Simulation Epidemic Malware Spread

Among the ancillary activities of the project is worth mentioning the “epidemics”. Depending on the nature of the malware it propagates according to different net topologies. When malwares requiring local execution are involved the effective net is represented by the topological proximity structure at the application level. As an example one may think at virus propagating vie e-mail; in that case the topology to be accounted for is represented by the social net of individuals sending and receiving messages. On the other hand, when the malware replicates or activates at transport devices (routers, servers etc) the topology to be involved is that of the physical network (L2 in the OSI schema).

Once the proper topology is selected one may predict the diffusion of malware in the net under the proximity hypothesis, that is by assuming that only directly linked nodes may infect each other. In that case, one may simulate infection similarly to that of an actual disease such as the flu or common cold. Figure 1 shows the typical spread of a common infection along a network of 611 nodes. To be defined, the employed topology is that of the Italian internet at AS level, nevertheless, due to the considerations above about the active infection mechanism, the results can be appropriate only in very special cases when an AS-AS propagation can be conceived. It is worth noting that (in the typical epidemic path) a part of the population (nodes) has never been touched by the malware, while the remaining part consists of refractary nodes (those where countermeasures make a second infection impossible) and defunct nodes (those, if any, which function has been definitely compromised by the malware damage).

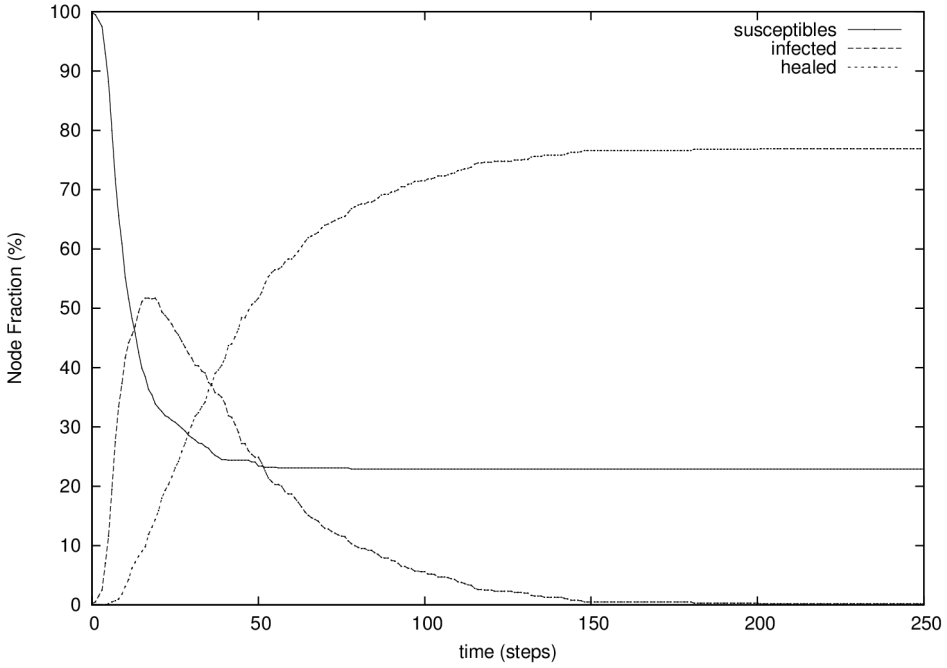

Figure 1: Typical Trajectory of an epidemic spread of a malware in the Italian Net at Autonomous System (AS) level. It is worth noting that some 25% of AS’s have not been infected at all.

The effectiveness of malware propagation is also origin (the initial infected node) dependent. The total amount of infected node is a function of the origin and (its percentage) represents an index of vulnerability. The higher the index the vulnerable the system. An unitary level for a node implies always a total infection when the epidemic starts from there, whereas a null value indicates no propagation at all.

Figure 2 reports the percentage of infected nodes as a function of the propagation rate, that was assumed to be uniform all over the net. As it can be seen, no drastic change is observed at special propagation rates, while the infected population increases exponentially with the propagation rate.

It is worth noting that, providing the correct net topology is available, one may infer the most vulnerable point for a malware attack. On the other hand, by exploring topology changes one may suggest, possible net designs to reduce the epidemic speed propagation.

The application reported in the present section may appear “out of context”; it has been included to provide evidence of possible applications. The analysis of the SPC case study will provide applicable results.

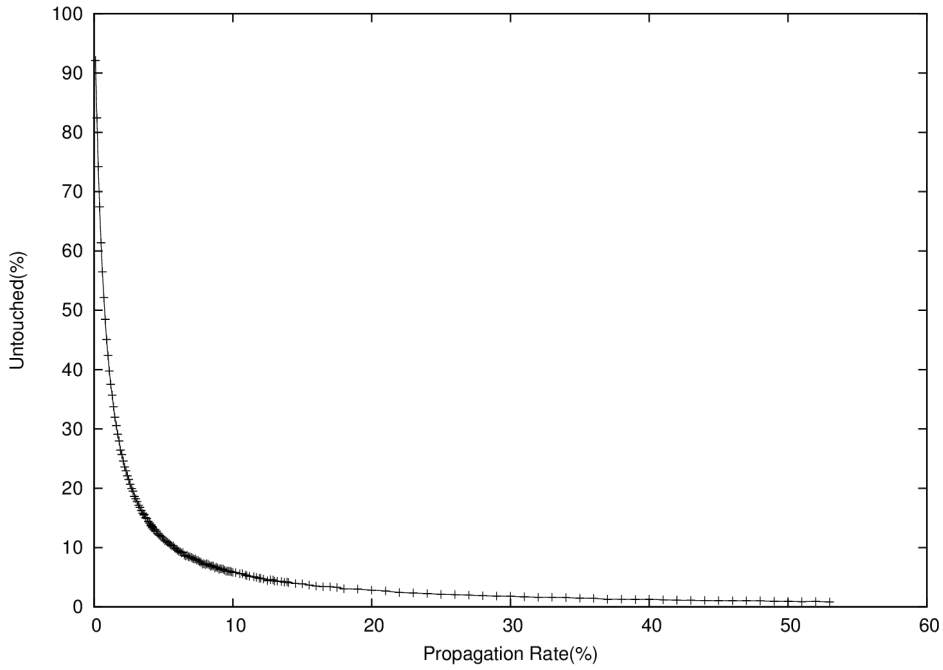

Figure 2: The fraction of infected node as a function of the propagation rate. A typical exponential behavior is observed as expected

Research plan and overall design

Introduction

The objective of the MOTA project is to investigate the nature and characteristics of interdependencies among ICT infrastructure components. In light of this work a specific and ad hoc qualitative research activity has been designed to collect, investigate, analyse and define the needs and characteristics of the MOTIA potential target groups (end-user of the ICT infrastructure) in order to better define the MOTIA project objects and to support the on-going R&D activities. The work - realised and coordinated by CASPUR with the support of ENEA – has been performed through the realisation of a number of qualitative in-depth interviews with experts and representative of organisations that make an extensive and massive use of the ICT use infrastructure and that also use the same infrastructure is deploying their services internal structure personnel or to external clients.

Objectives

Main objectives of the work are as follows:

Realise and extensive study on the impact of Critical ICT Infrastructure in a number of different the application (with particular focus on the domains envisioned din the project)

Study and evaluate the impact of Critical ICT Infrastructure use on the considered application domains

Involved Italian and international experts and make them aware of the project results and activity and collect from them advices, suggestions and recommendations for the project activity and future work

Provide inputs and recommendation for the dissemination and overall impact assessment activities of the project

improve the overall project visibility (including its objectives, and specific results and forthcoming results)

start up a MOTIA expert community (composed by both the academic and industrial communities) on the basis of which future R&D and dissemination activities will be built.

In regard to the specific feedback and inputs to be collected from the end-users we envision the following:

Analysing user feedback and responses when end-user came into contact with MOTIA concept and methodology. The goal is to gain better of understanding of responses from specific target groups than make a quite extensive use of ICT infrastructure services and facilities;

Obtaining suggestions and ideas that for service deployment including is- sues of distribution, promotion and pricing. The interviews should also feedback on how and in which terms to explain and present the MOTIA concept to other end user or to the other publics (including the general public).

Based on these issues/topics to lead the in-depth discussion we planned additional interview schedule aimed to:

Analyse experiences and perceptions associated with different events, services, technologies sand applications while using ICT infrastructure services;

• Identify needs associated with the ICT infrastructure services (with regard to services, equipment, wireless telecommunication technologies, support services, contract and personnel, relations and links with the operators and so.).

Methodology and profile of the participants

Qualitative research is the first step in an iterative and user-centred process. The qualitative methodology (in-depth interviews) used within the MOTIA project aims to support and improve the development and implementation of the MOTIA methodology as well as developing hypotheses for future research by analysing users needs and feedbacks on technologies, services in regard to ICT infrastructure. The participants to be involved in the project qualitative research and interviewed will be managers and decision makers belonging to organisations and companies that make an extensive use of the ICT infrastructure, technologies and services. During the interview they will provide their view (at both personal and high level) on the MOTIA project and methodology, and ICT infrastructure. The data obtained through the in-depth interviews will be therefore gathered and analysed to identify final suggestions and recommendations for the MOTIA project.

Next steps will be focussed on prosecution of the work to be realised trough:

1. a quantitative research (questionnaires and semi-structured interviews) to assess the work realised with the interviews. The use of quantitative tools will enable the possibility of gathering simplified and less structured data from a larger group of participants. It will enable also the possibility of involving a higher number of participants for non-Italian countries.

2. A final assessment of the results obtained through the interview and the questionnaires to be realised with the organisation of a dedicated Roundtable to be organised with expert and end users coming from other European countries to investigate and extend the project results outside the Italian test case.

2.4 Expected results

Research results will including the overall analysis of the in-depth interview realised, with a specific focus on overall and final recommendations to be provide also at EU decision-makers level and will specifically provide insights on the following:

Deskwork research on the state of the ICT technologies use, needs, and characteristics focalised for specific application domains;

State of the art for ICT critical infrastructures characteristics, innovation, issues and improvement needs for the different application domains;

Evaluation of the potential impact and interest for the MOTIA project with particular regard to the MOTIA project concept and how it is explained, presented and disseminated;

Evaluation of the potential impact of the MOTIA methodology and foreseen improvements (both on the technical and non-technical side) in the ICT infrastructure in each application domain;

Suggestions and recommendation for the overall project improvements and continuation of the work;

Start up and expansion ICT infrastructure R&D community (also including other EU and international funded projects).

MOTIA Interview Schedule

Presentation

We tried to better understand how target groups would react to MOTIA concept and project aims. We also expected to obtain suggestions for improving the MOTIA methodology and concept presentation (for current and future dissemination activities). To collect such information a list of issues was set up to understand in depth user needs and to inform about the project initial results. The list of issues as been used to conduct the interviews realise with the participants and tasks form of the following so-called interview schedule.

Interview schedule

WARM UP

Presentation of the researcher, and of the project (very brief introduction without entering too much in the details), of the objectives of the work and of the interview. Explain how the data will be managed, gathered and finally treated and analysed and who will be the owner. Explain that other participants from other organisations will be (or have been) already involved; explain why the participant has been chosen to participated to the interview.

During this phase the project concept and activities will only VERY briefly introduced. This is important as initial feedback from the participants needs to be collected without “speaking for the participant”.

FIELD

Characteristics of the organisation to which the participant belongs. Daily work activities, responsibilities, needs and objectives (with focus on new technologies and ICT instruments tools used by the organisation).

ICT and TLC TECHNOLGIES

How and which technologies are used in the organisation. Collect feedback on any issues, benefit, needs, cost, operators they work with, and so

Focus on the people in the organisation that are in charge for selecting and defining the technologies to be used. What are their needs? What are the needs of the client (if any) to which the organisation is providing services? What kind of decision do they take? How is the process of selecting and using specific technologies?

FOCUS on CRITICAL INFRASTRUCTURES

The set of question is quite similar to the earlier on, but needs to be focussed on the Critical infrastructures topic. What is the general opinion of the participant on this topic? Are there any

specific activity done in its organisation? Which activities in particular? Why is your organisation so dependent on the characteristic of the TLC infrastructure? What happens if the infrastructure has some failures? What are the procedure and preventive action that the organisation takes in place to avoid such failures?

What kind of services of the TLC infrastructure are more relevant for them? Why? What is changes in the use of such technologies in the last years? What is foreseen in the next years?

How would they like to improve their existing infrastructure? What is the relation with the operator that provides the infrastructure? Does he provide any additional services? Are there any legal boundaries that have been considered and identified?

If there any specify event that you could report to us? What did happen in that case? How did you solve the problem at the end? Are there any lesson learnt on this?

In regard to the other European countries are there any relevant experiment to be mentioned? Why? Can you provide us some examples? What are instead the positive aspect of the Italian experience? And the negative ones?

In regard to the relevance of the Critical infrastructure for your organisations do you think there are important lesson learnt that could be forwarded to other organisations operating in different field and domains?

MOTIA CONCEPT

Present very briefly the MOTIA project and its objectives (at a very general level, without too many explanations, just providing the keywords used in the website and in the project abstract and dissemination material). Collect a very first feedback. What is clear? What is not clear? What you would suggest to eliminate? What to be introduces? Why? Which are the most important words/keywords? what are they so relevant?

MOTIA IMPACT

Going into the details of the MOTIA, also presenting its specific objectives, activities, and expected results. Ask the participants what are its feelings? In you opinion which could be the overall impact of the project? Why? How do you see the relevance of the project in different application domains?

Do you think the proposed methodology present and innovation aspect? Why? Is there any comparable methodology and measurement that is actually used in the filed? Are they relevant? Why? Could the MOTIA project benefit of their results?

What do you like most of the MOTIA? And why? What are the most interesting aspects of the project and why? Do you think that the project could have impact on the ICT critical infrastructure RTD field? What are the main improvements that the project could bring?

What do you think is missing into the MOTIA project? What would you like to add or to improve? Why? Do you think that the Critical infrastructure topic would benefit of different RTD approaches and activities? Why? Could you give us an example?

PLUS and MINUS and SUM UP

Investigate the actual interest of the participants for the MOTIA project. Is the concept clear, are the research activities sufficiently details and clearly explained? In your opinion is the project clearly

explained considering the target users and the scientific community that it should address? How would you present the MOTIA project to other people? what terms you would use? On the basis of this first set of question collect a number of indications and suggestions for to improve the project concept and overall presentation

On the basis of this is the project interesting for the participants? Why? Are there any expected results of the MOTIA that could be interesting for the organisation he participant is representing? How could the results be relevant for the field in which the organisation is working? And why? On the basis of this set of questions collect suggestions and recommendations to improve the project activity and the project dissemination and promotion. Collect also information on other possible end users that would be interested in participating to the concept assessment activity (both at a national and international level).

CLOSE and THANKS

Thank and conclude. Ask the participation about any question he would like to ask and/or if any explanation is needed on the research activity he has been involved in. Present again briefly the objectives of the work and of the interview just realised, the fact that it will be useful and remind the purpose for which it has been realised.

Annexes

End user information sheet: Poste Italiane Spa

End user and website

POSTE ITALIANE SpA

Participants

Head of ICT Security Services

Profile

TLC Infrastructure

Services

No of employees

End user information sheet: ENAV

End user and website
ENAV
Participants
Head of ICT Security Services
Profile

TLC Infrastructure

Services

No of employees

End user information sheet: ABI LAB

End user and website

Participants
Head of ICT Security Services
Profile

TLC Infrastructure

Services

No of employees

Conclusions

The Motia project represents an attempt to provide a methodology to quantify interdependencies among different entities in the ICT sector. The project is half the way and two basic steps have been realized: the identification of relevant entities and their relations and boundaries, and the definition of a methodology for a topological recognition of the internet at Autonomous System level.

The project has already started a “research pla and overall design” to enhance the project impact and allow its evaluation procedure acquiring useful information on significant endusers’ perspectives by means of suitable interviews.

Simulations of epidemics malware propagation have been performed to provide insights on the system vulnerabilities at topological level.

This report represents a plot for the forthcoming work and a short presentation of partial results.

References

[1] Council Directive 2008/114/EC 8 December 2008

[2] S.M. Rinaldi, J.P. Peerenboom, and T.K.Kelly, “Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies”, IEEE Control Systems magazine, pp. 11-25, December 2001.

[3] http://www.itu.int/rec/T-REC-X.200-199407-I/en

[4] E. Gregori, A. Improta, L. Lenzini, and C. Orsini, “The impact of IXPs on the AS-level topology structure of the Internet”, Computer Communications, vol. 34, no. 1, pp. 68 ? 82, 2011.

[5] R. Albert, A.-L. Barabasi, Rev. Mod. Phys., 74 (2002) 47.

[6] S. Boccaletti et al., Phys. Reports, 424 (2006) 175.

[7] L.A.N. Amaral et al., Proc. Nat. Acad. Sci. USA, 97 (2000) 11149.

[8] "The IPv4 Routed/24 AS Links Dataset”, Y. Hyun, B. Huffaker, D. Andersen, E. Aben, M. Luckie, K.C. Claffy, and C. Shannon, http://www.caida.org/data/active/ipv4_routed_topology_aslinks_dataset.xml.

[9] Yuval Shavitt and Eran Shir. “2005. DIMES: let the internet measure itself”. SIGCOMM Comput. Commun. Rev. 35, 5 (October 2005), 71-74. DOI=10.1145/1096536.1096546 http://doi.acm.org/10.1145/1096536.1096546

[10] http://www.robtex.com “IRL (non cyclops) - Internet Research Lab UCLA”

[11] Ricardo Oliveira, Dan Pei , Walter Willinger, Beichuan Zhang, Lixia Zhang, "The (in)Completeness of the Observed Internet AS-level Structure", IEEE/ACM Transactions on Networking, February 2010. http://irl.cs.ucla.edu/

[12] ROUTE VIEWS University of Oregon Route Views Project http://www.routeviews.org/

[13] Routing Information Service (RIS) http://www.ripe.net/data-tools/stats/ris

[14] http://ndb7.net.internet2.edu/bgp/

[15] Ricardo Oliveira, Dan Pei , Walter Willinger, Beichuan Zhang, Lixia Zhang, "The (in)Completeness of the Observed Internet AS-level Structure", IEEE/ACM Transactions on Networking, February 2010.

[16] http://www.irr.net/docs/list.html

[17] RFC 4271

[18] RFC 1930

[19] RFC 1812

[20] D. Pei, W. Willinger, B. Zhang, L. Zhang, R.V. Oliveira, The (in)completeness of the observed Internet AS-level structure, IEEE/ACM Transactions on Networking (TON) 18 (1) (2010) 109–122.

BIBLIOGRAPHY

[EBN08]Brian Eriksson, Paul Barford, and Robert Nowak. Network discov- ery from passive measurements. SIGCOMM Comput. Commun. Rev., 38(4):291–302, 2008.

Glossary of employed basic definitions

The function of a system (or component) is the scope it is designed or employed for

A **failure** is an event for which a system (or a component) does not provide the service it was designed for.

Fault is a condition (defect) of a system (or a component) design inducing malfunctioning**.**

Dependence represents the condition for which a system (or a component) is required for the functioning of an other system (or component).

Fault-tolerance is the property that allows a system to continue functioning upon the failure of one or more of its components.

Dependability is a (set of) numerical index measuring the reliability of a system or a component as a consequence of its characteristics of integrity, truthfulness, and trustfulness. It represents a parameter to evaluate the quality of dependence.

Th Dependability may be further qualified by Attributes:

Availability - promptness to provide the correct service

Reliability – capability to provide continuity of correct service. A reliability index is represented by the mean time to a failure.

Safety - absence or a low level of risk for injuries on the user(s) and the environment

Integrity – absence or marginal presence of system (or component) alteration and the service it provides.

Maintainability – the extent of capability for a system or component to undergo modifications and repairs.

Prevention: Capability to forecast undesired events and to design appropriate measures to mitigate or get rid of it.

Fault-prevention: capability to design fault free systems or components.

Fault-Removal: the action amend a system (or component) design or real time behavior to eliminate a flaw.

Outage is an event when a system is not capable to provide its service. By extension it also represents the period of time during which the system does not provide the service.

Recovery is the set of (forecast or real time) operations required to obtain proper functioning upon errors.

Restoration it the set of actions to be implemented to bring the system to its normal functioning state after an undesired event.

Survivability is the capability of a system (or a component) to provide the service it is devised for upon attacks, failures or accidents.

Resilience is the capability of a system (or a component) to

Resistence is a measure of the intensity of attacks, failures or accidents a system (or component) is capable to sustain continuing to provide its service.

Operational fault is a fault due to inappropriate way to operate a system (or component).

Vulnerability of a system (or a component) is a weakness in its design or operation that allows malfunctioning upon undesired events: deliberate attacks, stochastic faults or natural hazards.

Threat is a foreseen undesired event (deliberate attacks, stochastic faults or natural hazard) that may induce a malfunction of the system (or component).

Fault Tree Analysis is a technique to infer the risk backward starting from a given hazard or undesired event chain.
Quality of Service (QoS)
Event Tree Analysis is a discipline that inductively predicts chains of events as consequence of any possible undesired event named **initiator**.

Resilience is the the ability of a system (or component) to withstand and recover from undesired or unplanned events.

Resilience is the ability of the network to provide and maintain an acceptable level of **service** in the face of various **faults** and **challenges** to .**normal operation**

Resilient networks aim to provide acceptable service to applications:

- ability for users and applications to **access information** when needed, e.g.:
    2. Web browsing
    3. distributed database access
    4. sensor monitoring
    5. situational awareness
- maintenance of end-to-end communication association, e.g.:
    7. computer-supported cooperative work
    8. video conference
    9. teleconference (including VoIP calls)
- operation of distributed processing and networked storage, e.g.:
    11. ability for distributed processes to communicate with one another
    12. ability for processes to read and write networked storage

disrupts the normal operation

Adversity is an unplanned event or condition that challenges the system possibly (or potentially) disrupting the normal operation.

Accountability

Attack Intentional execution of a threat by an intelligent adversary

DoS denial-of-service

DdoS attack: is an attack coming from a wide group of machines aimed at a DoS.

Authentication

Authorization

Availability is the Probability of a full operable system (or component) of being operable after some time t.

Confidentiality is a property of information unavailable or disclosed to **unauthorized** individuals, entities or cyber processes

the Disruption Tolerance is he ability of a system (or subsystem) to tolerate disruptions in connectivity among its components

MTBF (**Mean Time Between Failures**)
Expected value of the **time** between failures, including the time to repair. MTBF = MTTF + MTTR

MTTF (**Mean Time to Failure**)
Expected value of the failure density function.

MTTR (**Mean Time to Repair)**
Expected value of the repair time density function.

Fault Tolerance The ability of a system to tolerate faults such that **service failures** do not result.

Data integrity: "Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed"

Quality of Service (QoS)

Operability: is and indx representing the percentage of the service that a system (or a component) is able to provide. Full operability is represented by an unitary value, whereas an out of order system (or component) has assigned a null oparability value.

Inoperability is the opposite of operability