Validation method of a telecommunications blackout attack

(student abstract)

Eng. João Amado
Information Warfare / Competitive Intelligence
Post-Graduation Student
Academia Militar
Paço da Rainha, 29
1169-203 LISBOA, Portugal
jamado@netcabo.pt

Maj. Paulo Nunes
CINAMIL
Academia Militar
Paço da Rainha, 29
1169-203 LISBOA, Portugal
pfvnunes@net.sapo.pt

Abstract

This paper presents an evaluation method of telecommunications infrastructure vulnerabilities, allowing the identification of components that can be attacked in order to achieve a communications blackout. Exploring those components it is possible to define a scenario and conduct case studies analysis and experiments that can be used to assess the vulnerabilities of a real world situation.

The conceptual framework basic idea is to identify points that can be attacked using unsophisticated technology in order to achieve serious damages on the different network infrastructures, and to obtain the maximum disruptive effect over the services.

The proposed method uses a top-down approach, starting on the service level and ending on the different network elements that can be identified in the end as the targets for the attack.

Introduction

Many countries like the United States (NSHS, 2002; NSPPCIKA, 2003), Australia (Cobb, 1999) and the Netherlands (Luiijf, 2002), have recently demonstrated major concerns with the security of their critical infrastructures. This is a consequence of the raising importance of vulnerability analysis, especially in the presence of new network threats.

Most of the papers we could find in a literature review focused on the topic of critical infrastructures, stress the fact that electric power grid may be looked as the fundamental pillars of a huge critical infrastructures pyramid. In fact, many authors consensually assume the existence of an interdependencies chain, and started their research creating scenarios about the possible consequences of an electric blackout. After that they usually examined the subsequently affected infrastructures and the affected services based on the reliability and security of telecommunications infrastructures.

One example that we could find in our research on the Internet was the work performed by the Gartner Research and the United States Naval War College, named "Digital Pearl Harbor" in 2002 and again in 2003.

In the scope of our paper we propose a different approach and a new analysis method that consists on starting from a set of communications services used in a specific geographic zone and then identify the telecommunications network elements that must be affected in order to achieve the main goal, to create a communications blackout in a well identified zone during a special event like and high level international summit.

If we use the classification method proposed by John Arquilla and David Ronfelt [ARQUILLA, 2001], then this exercise would correspond to a Netwar situation, but would not be restricted to the concept of a Cyber Attack. In fact, the attack would not only use the Internet but could also consider that some physical action would be necessary to achieve the final goal of disrupting the network functionality over a well defined area (the summit area). The goal of the attack would be a temporary total disruption or denial of services according with Watlz definitions [WALTZ, 1998].

The information collected with this type of studies would be very helpful to be shared between private operators and security agencies in order to identify the weakest security points in the infrastructure ("weakest links") of the different telecommunications network. At the present moment this could even be more relevant due to the recent market liberalization where we have several emergent operators deploying networks that are used to implement all sort of services (sometimes critical ones) without the existence of a single point of contact that would be useful in an emergency situation.

The importance of the telecommunications infrastructure "fragility" could also be drawn and emphasized when we consider the status of the national/international interconnections that are today in the hands of different private entities. Namely, for voice and TCP/IP data networks, where we have carrier-houses or pix-centers that assure the connection between the different operators and the “outside world”, this problem assumes a particular relevance since in most of the time some important security aspects are neglected.

This type of exercises could also be useful for training and to prepare the people that could be involved in a real critical network disruption situation.

The conceptual framework that we will follow in our validation method of a telecommunications blackout attack will encompass a six steps sequential process:

- Scenario Analysis: characterization of the available services and networks in the target area;
- Logical Target Selection: Identification of potential targets according to the perceived services value;
- Target Information Upgrade: additional information in order to upgrade the target information;
- Physical Target Selection: selection of the class of elements more vulnerable in the network;
- Attack Simulation: use of software tools to model and simulate a network attack;
- Virtual Attack Success Assessment: takes place after the simulation period and will allow the evaluation of the network attack effectiveness.

2. Scenario Analysis

The analysis phase would start from the identification of the different services available at the summit area, typically at least the following services would be available (internally and externally):

- Voice over circuit switching network;
- Voice over packet switching network;
- Voice over mobile networks GSM/GPRS, UMTS;
- Data over circuit switching network;
- Data over packet switching network;
- Data over mobile networks GSM/GPRS, UMTS, WiFi, WiMax;
- TV – over microwaves;

For each service an estimation process would be necessary in order to prioritize the most important services to attack. This information would be the input of the next step.

3. Logical Target Selection

For the logical target selection and using a less cost-benefit logic the different values of each of the services must be listed. Theoretically, in order to conduct a proper evaluation of the service value, the number of users using the service should be known. However these values are not easy to calculate and could also lead to a wrong decision because the users relative importance is not all the same. Looking to the social impact of an attack we can see that a high level government executive will be more affected in his activities then a farmer. Considering the visibility of the attack, a journalist would be much more important than someone just walking by. The service utilization could be considered under three different levels, according to a rough estimation – High, Fare, Poor.

As an example of a service usage assessment we present a short view of GSM/GPRS Portuguese Network, Operators and Services for the mobile data and voice services (see Table 1). As in any other European country, where we can have different operators, typically from three to five, covering same geographical areas, in Portugal there are three operators (TMN, Vodafone, Optimus).

Network	Operator	Service	Usage
GSM/GPRS	Optimus	Voice	Fare
		Data	Poor
	TMN	Voice	High
		Data	Average
	Vodafone	Voice	High
		Data	Fare

Table 1 – Service usage assessment for the Portuguese GSM/GPRS Network.

When conducting the target selection process we should also be aware that some less priority target could be used as backup for a priority one. In this example (Table 1), the Optimus Operator network is a less priority one. However due to the mechanism used by the Global System Mobile (GSM), if this Operator network is disrupted the subscribers are able to perform emergency calls (dialing the European emergency number – 112) using other operator network. International subscribers in a roaming situation (subscribers from a different country and using the local national network) would also be able to use other operator network. So, in this example, the good solution to disrupt the GSM Network would be to select all the three different available networks.

4. Target Information Upgrade

After the completion of the logical target selection phase it's necessary to gather additional information in order to upgrade the target information. We will use two examples to explain the information upgrade concept for the selected logical targets, one example for the data and voice services over the GSM/GRPS network and the second one for the internal (in house) data service.

Example 1 – The GSM/GPRS network can be briefly described as shown in figure 1, where are represented its basic components, the interconnection between them and the network elements we can consider.

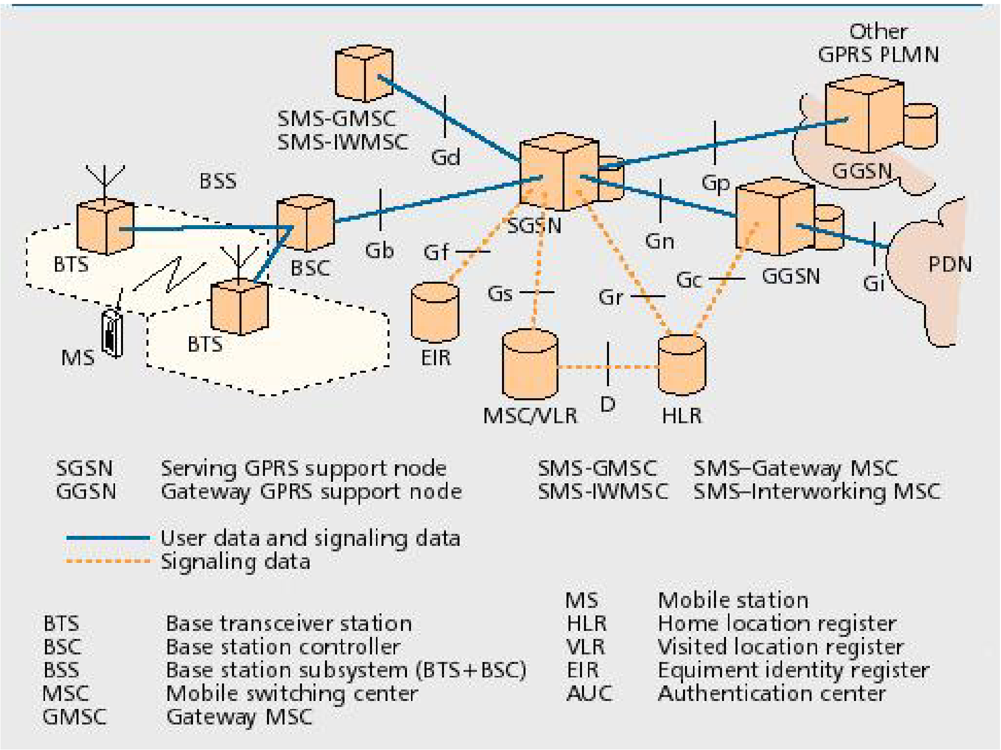

Other GPRS PLMN
SMS-GMSC
SMS-IWMSC
Gd
BSS
GGSN
Gp
BTS
BSC
Gb
Gf
SGSN
Gn
GGSN
Gc
Gi
PDN
Gs
Gr
MS
BTS
EIR
MSC/VLR
D
HLR
SGSN Serving GPRS support node
GGSN Gateway GPRS support node
SMS-GMSC SMS–Gateway MSC
SMS-IWMSC SMS–Interworking MSC
User data and signaling data
Signaling data
BTS Base transceiver station
BSC Base station controller
BSS Base station subsystem (BTS+BSC)
MSC Mobile switching center
GMSC Gateway MSC
MS Mobile station
HLR Home location register
VLR Visited location register
EIR Equiment identity register
AUC Authentication center

Figure 1 – GSM/GPRS network[1] Scenario.

[1] source www.comsoc.org

For all the elements (including the transmissions links) and for all the three operators (identified on table 1) we need to collect information about:

- Model and Type (e.g. Siemens EWSD);
- Provider (e.g. Nokia, Ericsson, Alcatel, Motorola);
- Known vulnerabilities of the system (e.g. in case of loss of energy the Uninterrupted Power Supply will assure the service for a limited number of hours);
- Typical location (e.g. BTS are installed on semi-private spaces on top of buildings, MSC are installed in well guarded buildings with controlled access)

These are typical pieces of information about the network components that can be easily collected in open sources (e.g. Internet) and with informal discussions with people working in the different operators and on the equipment providers.

One of the things that can be highlighted from Figure 1 is the chain type of the network where we can notice that if there is a break in the chain the service will be disrupted. We can also notice that the location of the break from left to right will have a different and growing impact. If the Mobile Switching Center (MSC) is disrupted then many cells can be put out of work. If only the BTS can be disrupted then only a short number of cells (typically three) will be out of work. Other thing that we could point is the number of links connecting all the network elements. Those links correspond to transmission capacity deployed in two different ways (cables and microwave links). In fact many towns use cables (coaxial or cooper), many times under our feet or on the walls of the buildings, or deploy those links using micro waves systems.

Example 2 – The internal (in house) data service (fixed or wireless) is deployed using a Local Network (LAN) using active and passive elements. The most important passive elements are the cables used to connect the active elements, typically a structured cabling system. The active elements are the hubs, routers, firewalls, LAN switches, wireless access points and the servers implementing logical services over the LAN: Domain Name Servers, DHCP Service, Network Files Services, Printers Servers, etc. In the case of a LAN we should consider the hypotheses of blocking the service acting from the outside without the need to go inside to the summit area to disrupt the network. For instance, it would be possible to block a server using a Distributed Deny of Service

(DDoS) [AMADO, 2001], acting from the outside. One other way to block a server would be to explore the way how remote maintenance procedures are performed, namely those that could be available due to a security breakdown.

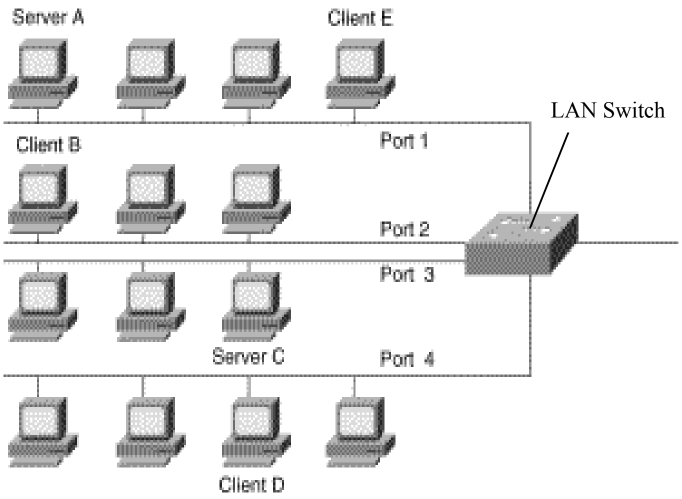


Fig.2 – LAN Scenario.

5. Physical Target Selection

After assessing the vulnerability of all the elements in every network, the next step is to select the class of elements most vulnerable. We will proceed with example 2 to illustrate the level of information needed in this step, starting with a diagram similar to the one on Figure 2.

In this case of the LAN switch would be the selected target, because the disruption of this network component would not only break the communications with the outside world but probably would also disrupt the internal network. So, in this case it would be advisable to collect the maximum available information about the:

- Bugs or holes already know on the software versions of the LAN switch operating system;
- Existence of any network access used for remote maintenance.

If there was no possibility to attack the LAN switch, than we would investigate about the network servers – Server A and Server C, identifying the:

- Operating System;
- Installed applications;
- Supported protocols;

- Access from the outside world.

For each one of the above areas it would be necessary to identify bugs and holes already documented and to verify if they exist on Server A and/or Server C.

If we look to example 1 scenario, we could consider that by observing the locations most used for the BTS, e.g. top of public buildings in the street (see Figures 3 and 4), we would find easy targets that could be disrupted without much effort.

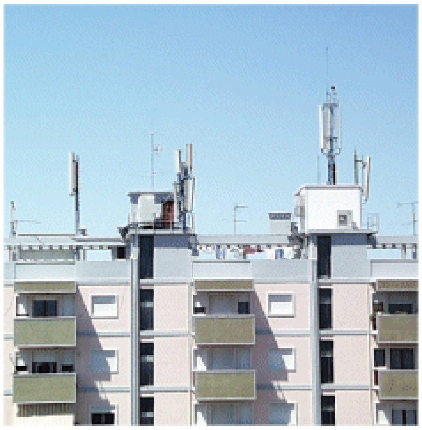


Figure 3 – BTS on the top of a building

A BTS attack would disrupt not only the voice service but also the data service. Due to the separate structure of the GSM/GRPS network the shared elements by the two infrastructures are the BSC/BTS part.

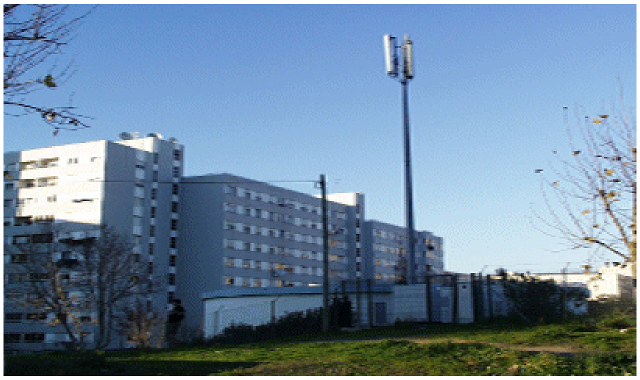


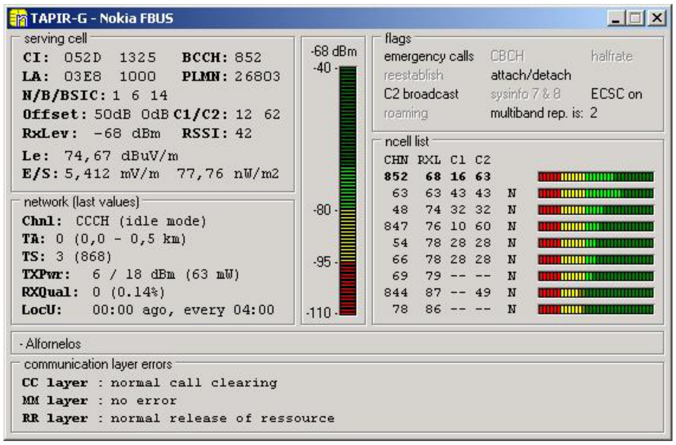
Figure 4 – BTS in open space.

To disrupt the BTS we can consider two possibilities:

- cut the transmission link between the BTS to the BSC;
- cut the power supply.

However due to the fact that all the BTS are equipped with UPS systems the best option will be to cut the transmission link between BTS and BSC.

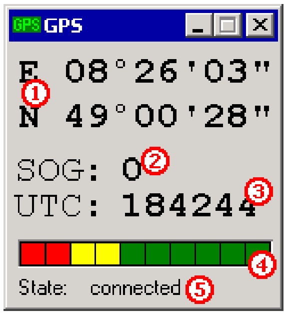
According to this, the next step would be to identify all the BTS from the different operators covering the summit area. The main tool for that task would be a GSM/GPRS handset, connected with a laptop with the proper software (that can be downloaded from the Internet[2]). Basically this is a netmonitor software (see Figure 5) that and can be used to locate the cells covering a specific area, including cell information about operator, distance to cell, primary cell, neighboring cells, etc.



```
CI:  052D  1325   BCCH: 852
LA:  03E8  1000   PLMN: 26803
N/B/BSIC: 1 6 14
Offset: 50dB 0dB C1/C2: 12  62
RxLev:  -68 dBm   RSSI: 42
Le:  74,67 dBuV/m
E/S: 5,412 mV/m  77,76 nW/m2

Chnl:  CCCH (idle mode)
TA:  0 (0,0 - 0,5 km)
TS:  3 (868)
TXPwr:   6 / 18 dBm (63 mW)
RXQual:  0 (0.14%)
LocU:    00:00 ago, every 04:00

emergency calls   CBCH               halfrate
reestablish       attach/detach
C2 broadcast      sysinfo 7 & 8      ECSC on
roaming           multiband rep. is: 2

CHN  RXL  C1  C2
852   68  16  63
 63   63  43  43   N
 48   74  32  32   N
847   76  10  60   N
 54   78  28  28   N
 66   78  28  28   N
 69   79  --  --   N
844   87  --  49   N
 78   86  --  --   N

- Alfornelos

CC layer : normal call clearing
MM layer : no error
RR layer : normal release of ressource
```

Fig. 5 – TAPIR-G Netmonitor software.

It would be important to identify not only the main cell covering the area but also de neighboring cells because when the main cell is distributed the neighboring cells could process some of the traffic if the radio signal is strong enough. So it would be important to identify the signal level of all the cells covering the summit area and to select as targets the ones with a strong radio signal power level (RxLev).



```
E 08°26'03"
N 49°00'28"
SOG: 0
UTC: 184244
State:  connected
```

Fig 6 – GPS Beacon[3]

[2] www.nobbi.com

[3] www.nobbi.com/monitor/index_en.htm

The presented software also has a GPS interface that allows the cell radio equipment detection that will support and facilitate the cell's location task (Figure 6).

Returning to example 1, we can say that this task would end when all the BTS are geographically identified.

6. Attack Simulation

The attack simulation capability will depend upon the possibility to build the necessary tools that can model the different real world scenarios and possible attacks. The building of the tools may involve but is not limited to the development of software, for instance, worms, or any other type of tool necessary to disrupt the physical target.

The purpose is not to use the tool but to demonstrate that the tools meet the attack requests. In the scope of the present work we should demonstrate that for instance a worm is undetectable by the actual existent anti-virus. However the worm would not be distributed and would be destroyed after the simulation.

In the case presented at example 1, the transmission paths to be interrupted should be identified. Additionally we will also have to clarify how this interruption would be executed for each of the identified BTS.

7. Virtual Attack Success Assessment

After ending the simulation period and with the help of people from the different network operators and other technicians, it would be possible to:

- conclude if it is possible to perform this type of attack;
- evaluate the impact of the attack, showing for how many time it would be possible to disrupt the communications, and what would will have to be the necessary effort for the service restoration;
- evaluate the amount of effort needed to prepare, coordinate and perform the attack;
- what skills would be necessary the attacker to have in order to perform this type of attack.

Additionally some shortcomings and “wick points” are also expected to be identified in the network infrastructure. This information would be available not only for the network operators but also for the agencies responsible for the national telecommunications security.

8. Conclusions

With the use of the presented method it will be possible to create very realistic scenarios allowing the simulation of severe attacks to the telecommunications infrastructures. The main message is that instead of spending innumerous efforts to disrupt the basic infrastructure, a well planned attack can be conducted without much effort but with serious disruptive effects. Like this it will be possible to affect an important event by creating a complete blackout situation during some hours.

Although in a simplistic way, the presented scenarios would be useful to identify the “weakest links” of a network. We think that the proposed method can reveal itself to be helpful in the prevention of this kind of attacks that may very likely happen in near future.

References

AMADO, João. *Hackers: Técnicas de Defesa e de Ataque* FCA Lidel 2004.

ARQUILLA, John; Ronfelt, David. *Newtork and Netwars*. National Defence Research Institut RAND, 2001.

CAETANO, Paulo e GARCIA, Rita (2003). “Portugueses em Perigo”, in *Revista FOCUS*, 27 de Agosto, pp.96-100.

COBB, A. (1999). “Critical Infrastructure Attack: An Investigation of the Vulnerability of an OECD Country”, in Netherlands *Annual Review of Military Studies 1999 on Information Operations*, Tilburg University Press, Tilburg, pp. 201-221.

COOPER, P. (1996). “US Lawmakers Examine Vulnerabilities of Internet”, in *Defense News*, 27 Maio – 02 Junho, p.37.

LUIIJF, Ir. et al (2003). *In Bits and Pieces,* available in INFODROME, http://www.infodrome.nl/.

LUKASIK, Stephen (1999). “Defending Information-Dependent Infrastructures”, em *Information Impacts Magazine*, Setembro.

NSHS, (2002). *National Strategy for Homeland Security,* available in White House Office of Homeland Security, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

NSPPCIKA, (2003). *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* available in White House Office of Homeland Security, http://www.whitehouse.gov/pcipb/physical_strategy.pdf,.

WALTZ, Edward. *Information Wafrare Principles and Operations*. Artech House 1998.

www.comsoc.org