On a Malware Targeting Private Telephony Networks during Cyber Conflict

Iosif I. Androulidakis, *Member, IEEE*, Vasileios Vlachos, and Yori Kamphuis

Abstract **—Telecommunication networks have long ago entered the Critical Infrastructure domain. Apart from the public telephony network, there is a parallel private telephony network, consisting of Private Branch Exchanges (PBXs) that serve the communication needs of private or public entities. Their penetration in the market is substantial. As a result, thousands of PBX installations are present in every country serving many times more users in vital infrastructures (including health, safety, security, economy, energy). Therefore, attacking PBXs can have critical effects that disrupt society and can clearly be used in warlike situations. PBXs are an integral part of the critical infrastructure, along with the public telephony network. The contribution of this work focuses on the theoretical and practical capabilities of a malware able to target PBXs. Such an occurrence would have devastating effects on the communication confidentiality, integrity and availability.**

Keywords **—critical infrastructure; cyber conflict; malware; private telephony networks; PBX; virus.**

I. Introduction

Cyberspace has allowed new attack techniques to be developed. Viruses and other types of malicious software play an important role in this new field of war. Modern Computer viruses can be utilized to launch cyber attacks [1]. Specifically during warlike situations, bringing down or hampering telecommunications can have serious effects as in the Russian-Georgian conflict [2], [3], [18], [19], [20], [22].

Wars are becoming increasingly more technological. Some of the technologies may change, but the principles of acquisition, corruption and denial of information resources remain intact [4]. One of the main drivers behind this technology spurt is cybercrime [3], [21].

Former USA president Bill Clinton reconfirmed that telecommunication networks had entered the Critical Infrastructure (CI) domain long ago [6]. Apart from the public telephony network, there is a parallel private network, consisting of Private Branch Exchanges (PBXs) [5]. These are privately owned equipment that serves the communication needs of private and public entities, making connections among internal telephones and linking them to other users in the public telephony network. They exist in the form of IP PBXs (using the IP protocol) and conventional Time Division Multiplexing (TDM) PBXs (using phone lines) and their software can be offered as proprietary or as open source. While communication with other entities takes place via the public telephony network (or the Internet), internal telephone traffic fully depends on PBXs. Thousands of installations are present in most countries, serving a vast amount of users. The total number of PBXs (TDM and IP) in North America was 12 million in 2010 with increasing rates [7].

The possible effectiveness of malware targeting critical infrastructure has been proved on a world scale by the Stuxnet worm [8], [9]. Despite the fact that data communication security has arguably received significant attention lately, PBXs, however, have mostly been left unprotected and forgotten. Similar to the development of PC viruses, PBX malware could follow a comparable development. A PBX malware could take down telecommunications, intercept sensitive calls, harvest data from call logs and also contribute to psyops during war. Moreover, due to VoIP proliferation and convergence of data and voice, PBXs are now closely connected to the IT infrastructure as voice and fax are sharing the same data transmission paths. This causes the potential effects of PBX disruptions to have a broader impact [10], [23].

II. PBXs as a Critical Infrastructure Target

PBXs serve Hospitals, Ministries, Police, Army, Security Agencies, Banks, Public bodies/authorities, Companies, Industries and so on. Even if the core public network is operating normally, unintentional or targeted damages and attacks in PBXs can cause significant instability and problems. Effectively bringing down PBXs puts a nation's critical infrastructures at risk. Along with the public telephony network, PBXs are an integral part of the critical infrastructure. Therefore, sophisticated PBX attacks can be used in warlike situations.

The lack of understanding and acting upon the interdependencies of critical infrastructures has been documented in numerous occasions [11]. This may cause unexpected cascading effects, which has led various entities to call for joining efforts to obtain a better perspective of these cascading effects and interdependencies. [12], [13]. Like other initiatives, such as the ENISA/Rauscher's [14], a renewed focus on PBXs can guide Europe's networks to becoming more resilient [15].

In general, eavesdropping communications makes organizations dealing with confidential information liable. A lack of effective telephone communication can cause annoyance for its users [16], but could also prove lethal if a hospital's phones system is disconnected. Recent incidents demonstrate that even technical malfunctions can

Corresponding author Iosif I. Androulidakis is with MPS Jožef Stefan, Ljubljana, Slovenia (email: sandro@noc.uoi.gr)

Vasileios Vlachos is with Technological Institute (TEI) of Larissa, Greece (email: vsvlachos@gmail.com).

Yori Kamphuis is with Coblue Cybersecurity, Enschede, The Netherlands (email: yori@coblue.eu).

endanger human life if the hospital communications system is out of service [17]. The fact that telephony network outages can have serious consequences in such a combination of events became clear by the 9/11 terrorist attacks on the World Trade Center. This led to increased difficulties in arranging rescue and recovery [11], [30].

The situation in Georgia proved that communications are essential for the police, the army and all the security agencies in general [2].

III. The Malware

The malware's algorithmic block is presented in Fig 1. The malware searches for targets to infect, verifies that they are indeed PBXs, utilizes an exploit to gain access to the target system depending on the actual PBX brand and type, uploads in their operating system the corresponding compatible version of the payload, stays stealth for as long as it is programmed to, activates the weaponized code, looks for other PBXs to continue its propagation and finally erases the log files and exits.

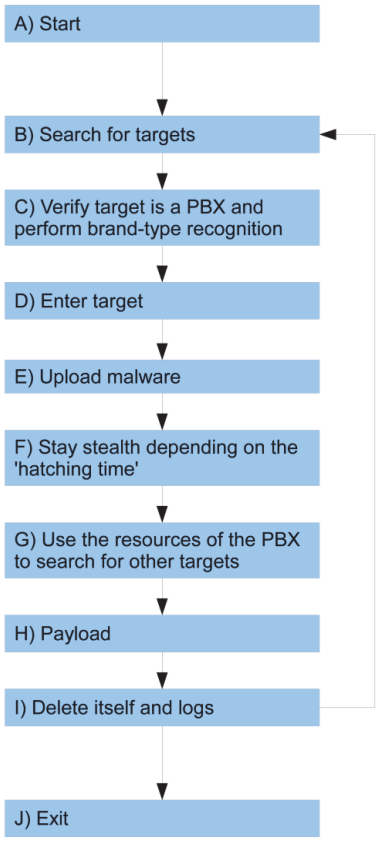

Fig. 1. Algorithmic block operations.

A. Start

The malware can be entered to the system via the known infection means. First and foremost a UNIX based PBX system exposes a wide attack surface. As a general-purpose operating system a number of lax configured or not properly updated network services may act as the infection gateway. The initiation of the infection process can take place in any PC inside the network perimeter of the organization, as the malware can propagate undistributed in the absence of a firewall in an internal network. As long as the malware is capable of identifying and infecting PBX systems it will need only a foothold in the victims LAN (Local Area Network).

The launch of the malware can take place from a compromised PC (preferably belonging to a company owning a PBX), or an already manually compromised PBX. Given the convergence of voice and data infrastructure, the malware could utilize computer networks spreading its functionality too. In that case, compromised computers can actively participate in the search for other PBXs and new PCs to infect. Another possible and particular effective way to contaminate a PBX with a virus is by planting the malware directly to the PBX. This method requires physical access to the system possibly combining some form of social engineering [24]. A third semiautomatic combinatorial approach is to use USB baiting, which is a social engineering technique that targets innocent users persuading them to use weaponized USB sticks. Thereafter, each time the USB stick is inserted in a new PC it will infect the system without leaving network traces at all.

B. Search for targets

At this step, the malware will try to find information about other PBXs in close relation to the already infected host. The administration protocols for the management and interconnection of PBXs include PSTN and ISDN dialup over respectively analog or digital lines, generic networking protocols such as IP, X25, Frame-relay and telephony specific signaling protocols such as QSIG, DPNSS,SS7, SIP, H323 and proprietary ones from different PBX vendors. By monitoring these protocols, the malware progressively increases its target list including maintenance modem numbers and IPs. In addition, targets can be found in modem logs, in routing and host tables and in extra subsystems and functionality present such as Voicemail. Fig. 2 shows a Screenshot from a PBX's hosts file, listing the close-by PBXs and CPUs.

```
(106)xa00106> cat /etc/hosts
10.1.255.255    broadcast
127.0.0.1       loopback
#; Site
10.1.1.1        xa00101
10.1.1.2        xb00101
10.1.1.3        m00101
10.1.1.4        s00101
10.1.85.1       xa00101_C1
10.1.85.2       xb00101_C1
10.1.85.3       m00101_C1
10.1.85.4       s00101_C1
#; Site
10.1.8.1        xa00102
10.1.8.2        xb00102
10.1.8.3        m00102
10.1.8.4        s00102
10.1.92.1       xa00102_C1
10.1.92.2       xb00102_C1
10.1.92.3       m00102_C1
10.1.92.4       s00102_C1
#; Site
10.1.15.1       xa00103
10.1.15.2       xb00103
10.1.15.3       m00103
10.1.15.4       s00103
10.1.99.1       xa00103_C1
10.1.99.2       xb00103_C1
10.1.99.3       m00103_C1
10.1.99.4       s00103_C1
```

Fig. 2. Hosts file listing interconnected PBXs.

In case the data gathering step does not yield any results, a more active step, known as "war dialing", is required. This means the attacker dials as many as possible numbers in a given range, trying to find modem carriers or other tones that denote the presence of a computer/PBX. This is possible due to the DID (Direct Inwards Dialing) or DDI (Direct Dial In) service offered by all telecom

providers, allowing an external user to reach a specific extension without the need to call the operator that would manually connect the call.

According to previous research war dialing, leading to the maintenance modem of a PBX, can be particularly effective, reaching even 70% success, by dialing only given extensions and not the whole range [25].

To help automate the data gathering step, the malware could possibly include an initial list of targets, manually compiled from yellow pages, to facilitate the spreading. This hit-list could contain the published numbers of Ministries, Banks, Industrial facilities, Companies etc., so that the malware could try war-dialing on them. A tracking mechanism should be also deployed, possibly via a command and control center, so that the same PBXs are not attacked twice.

C. *Verify the target is a PBX*

Once a connected system is found, the malware would assess if it is a PBX. Most PBXs have distinctive login prompts or error messages which makes the estimation of the brand type a trivial task.

D. *Enter-Break into the target*

Given that the brand of the PBX has been identified, the malware will try default passwords on the target. It is well known that PBX maintenance platforms and ports tend to have the default passwords enabled. Long password lists with the default ones are widely available [26]. Furthermore, there are cases of hard-wired passwords in the code of PBXs which cannot be changed.

The password list of the malware will be gradually extended, since it will also have the ability to harvest new passwords from the attacked systems during its spreading. Indeed, PBXs with UNIX-like operating systems maintain a password file, as seen in Fig. 3. This provides login names for which the respective passwords can possibly be brute forced. This step would be of little success since most PBXs limit the password trials.

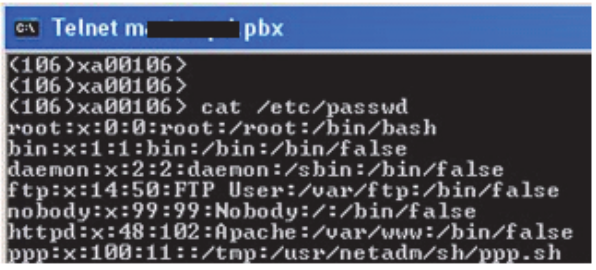

Fig. 3. Passwd file of a PBX.

In the unlikely event that none of the default passwords work the malware could attack using known vulnerabilities for the specific platform. This option heavily depends on the platform of the host PBX. In order to use specific tools and commands, the host PBX should be using a general purpose operating system. Should all means fail, the malware would abandon the break-in process and return to the previous step, locating another target.

Counterintuitively, low end and cheaper PBXs are less vulnerable than the larger PBXs with richer functionality. The configuration of a small PBX is practically impossible to be attacked in order to intercept or change the integrity of data from outside since such PBXs do not offer any remote access to the administrator at all. As a matter of fact, their programming usually takes place by dialing special codes issuing the respective commands, using a phone already connected in the PBX. Even with the absence of remote administration, however, they are still subject to denial of service attacks, internal fraud and hardware modifications.

E. *Upload itself and the payload*

At this step the malware uploads its propagation vector and the payload to the compromised PBX. They are both specific for each brand-type, but the whole "package" for all possible brand-types could be uploaded in library files, in order to be transferred to new targets, connected to the already compromised PBX. It is usually the case that 2-3 specific brands cater for the largest percentage of PBXs in most countries, depending on a vendors' market share. The PBX malware could be tailored to proceed with only the most usual platforms per country, thus being more compactly sized and more effective.

F. *Hatch period*

According to well-known virus propagation models, the payload is usually not immediately activated, in order to facilitate the spreading of the malware. Should the malware immediately manifest, administrators could possibly detect and remove it before having the chance to spread to more systems. On the other hand, a very long period of inactivity could result in the malware being detected in a routine check. For the specific malware, the PBX scanning and data harvesting could start early, since they are non-invasive. Thereafter, when enough new targets are found and compromised, the actual payload could activate itself. A command and control center could again supervise the process.

G. *Find other PBXs*

After the inactive period of step F. scanning for new targets will start. Initially this could include a low-profile activity, such as data gathering from files present in the O/S of the PBX. Subsequently, the active out-dialing to targets would start, during the night and holidays as to remain unnoticed as much as possible. The whole process iterates back to step b), before either a time trigger or a command from the control center forces the malware to activate its payload as follows:

H. *Activate the payload*

The "payload" of the malware is the part of it that performs the malicious action. We will examine possible exploitation scenarios in the following sections.

I. *Delete itself and logs*

Having already infiltrated new targets and having activated its payload in the current target, the malware would try to hinder the forensics process by deleting itself and the related logs associated with it. Moreover it could even wipe the O/S of the target. Records in call logs are registered after a call ends, since they have to contain information about the duration of the call. In the case where the malware has propagated with a modem dial up

call, it is impossible to delete the record that points to the number of the previous PBX that infected the present one. This is particularly important in low end PBXs that do not offer advanced O/S functionality such as time scheduled jobs (like UNIX crontables). In such PBXs the malware has to call the target many times, each time deleting the logs associated with its previous functionality. However, the last call will remain logged, unless the malware proceeds to a full wipe and crash-shutdown of the PBX.

IV. Availability Attacks

The malware could affect the availability of the system. It could cut off administrator's access by changing passwords, disabling remote access and shutting down the connectivity to IP and serial port communications. Incoming and outgoing lines could be deliberately set out of service, effectively isolating the PBX from the outside world. More aggressive actions could involve deleting the database which contains the setup of the PBX or critical O/S files that could completely halt the switch. Interestingly, at least one manufacturer has specific login accounts with the sole purpose of halting the PBX or deleting and re-installing the database, effectively wiping the existing setup. By extending this approach it is possible to overwrite the firmware of the boards of the PBX using its firmware update tools.

An effective denial of service technique can target the software and hardware protection of PBXs. Modern PBXs employ protection against unauthorized copying and black market selling utilizing some form of hardware-key, usually with an FPGA integrated circuit. The FPGA holds a specific hash that is coupled to the hardware present in the PBX. If somebody tampers the protection mechanism, the PBX will enter a limited functionality mode and eventually will shut down, protecting the vendor's revenue streams and the PBX from illegal interventions and black market exploitation. Specifically for PBXs exported to third countries, the hardware key can only be shipped from the manufacturing country since the local dealers do not have access to it, further extending the time needed to restore its functionality.

A remote denial of service in the communication layer can be achieved by another PBX (or an array of PBXs) attacking the target with hundreds of calls per minute. This attack could be used against the better protected PBX where the malware could not gain access. It blocks effectively the incoming and outgoing lines and the legitimate users cannot use them anymore since they are constantly busy. As an example, a typical E1 PRI European ISDN line offers 30 voice channels (23 with T1 lines used in USA). Assuming short calls of 10 seconds, including the setup time, a rate of 180 calls per minute can be achieved against the target. A medium size PBX with 3 E1 lines can launch 540 calls per minute against a given target. This would easily overwhelm most small PBXs. In a full ISDN environment with call setup times of less than 1 sec, the whole duration of the call could be as short as 2 seconds, yielding a 2700 calls per minute rate from the same 3 E1 setup. But, even if the target has enough capacity in lines, it could be well possible that the shear rate of calls causes a bottleneck in another part of the system, e.g. the automated attendant or the IVR (Interactive Voice Response) platform. This "blocking of lines" scenario closely resembles the denial of service and the distributed denial of service attacks of the computer networks, where instead of packets, calls are now flooding it.

At this point, another interesting effect of the repeated calls attack could be the overloading of international circuits. Indeed, the international circuit's capacity is usually limited. With an array of PBXs calling random destinations abroad, the links could be saturated and the country cut off from the international network. In order for the attack to fully succeed, it should be launched against PBXs that are being served from all possible international connectivity providers. Since communication circuits are two-way, the attack would have the same effect using compromised PBXs in the target country only, performing outgoing calls, or compromised PBXs in other countries performing incoming calls towards the target country.

A non-confirmed and to the best of our knowledge not researched, yet somehow plausible, attack on PBXs is by intervening in the firmware of the PBX. That could possibly command the PBX to perform functions that could lead to physical failure of its electronic components. Especially for analog lines, that employ relays, an attack could force the relays into a constant rapid on-off loop that would ultimately burn them. This could cause the ringing signal to permanently be applied in a phone, burning its ringer circuit. Looped reboots or file access could also damage the hard disc of the PBX.

Most of the above-mentioned attacks have not been materialized yet, but even simple technical issues as in the case of the St. Cloud Hospital made obvious the risks for the public health due to communication outage in health institutions [17]. Recently, cybercriminals have targeted the public safety answering points (PSAPs) during an extortion scheme against organizations of the private sector [32]. The latest developments indicate that malicious entities offer Telephony Denial of Service (TDoS) attacks as a service ranging from $5 per hour to 40$ for a whole day [33]. As a result, the victim cannot be reached from his financial institution in case of abnormal financial transactions [34].

V. Integrity Attacks

As experienced administrators can attest, it is easier to find the cause of a malfunction when it manifests as a complete lack of service than it is to find out what is wrong when the system misbehaves or when the error appears sporadically. Thus, the malware could create more damage by forcing the PBX to function incorrectly rather than launching a full denial of service. Changing settings is sometimes more effective than completely shutting service altogether. For example, randomly forwarding or swapping numbers among users can cause havoc and it simultaneously takes more time to realize what is wrong.

Deleting or changing the respective call and operation logs would cover the entry and the trails of the attackers. At the same time, it is possible to alter the communication

flow, connecting lines to different destinations (possibly utilizing a man in the middle attack). As stated before, harming the integrity of data in specific files and memory locations can lead to denial of service and PBX shutdown.

Staying with the integrity analysis we will also examine two non-technical effects of such a malware, psyops and fraud. Examples of such functionality would be to play propaganda messages to all internal users. It could also connect callers and incoming lines to recorded messages. Messages could be played by PAs (public address system-loudspeakers) connected to the PBX. Furthermore, constantly ringing phones, or phones ringing in the middle of the night could cause severe discomfort, annoyance or even fear as a part of psyops.

On the economic size, as was seen in the introduction, the costs attributed to telecom fraud, and specifically PBXs are not easily appreciated reaching $72 billion to $80 billion [27]. Even terrorist organizations are thought to be embracing telecom fraud to generate funds [28]. Compromised PBXs calling premium rate services or high cost destinations such as overseas or satellite networks can lead to extensive bills. Consider 100 compromised PBXs in a country, each calling such services or destinations a thousand times per day. Assuming a cost of 10 Euros per call yields a total of 1 million Euros per day in bills. At least in one case, criminals created losses of $55 million to the victim corporations, entities and other long distance carriers. Press sources link this incident with terrorist groups related to Al-Qaeda [35].

VI. Confidentiality Attacks

Voice communications could be intercepted in real time or recorded in the compromised system to be downloaded and analyzed later. Calls can be rerouted to other destinations, possibly utilizing a man in the middle attack too. With call correlation and traffic analysis techniques, interesting connections can be revealed. Industrial espionage information can be gathered even without knowing the actual content of the calls, but only the identities of the parties. As an example, if the logs reveal a flow of calls between a company and the patent office a safe assumption is that a new product is on its way to be patented. Respectively, key suppliers can be found and so on. A more sophisticated attack could lead to substantial information leakage. In particular it is possible to automate the whole process in order to parse the intercepted audio files and decode touch-tones to credit card numbers [31].

Data harvesting would also be an essential function of this malware. Among the harvested information threatening the confidentiality would be forwarded numbers in the forward tables as well as mobile phones and personal numbers present in the logs and stored in the memory of the phones. Many users are also saving personal codes such as PINs in the memory of the phone which could also leak.

Most modern systems save the numbers of the speed dialing entries in the PBXs' memory and databases rather than the phone itself. Older analog PBXs were relying on the phone's memory to store numbers. With that respect, older systems were more secure since the attacker would have to physically extract the data from the memory of the phone (possibly by stealing or replacing the target's phone), while now he can do the same by just reading the respective entries in the PBXs operating system.

It must be noted that the PBX can be the weak link to target the IT platform that is interconnected with it. Despite that, there is also another great risk: users connecting modems in their phone lines to bypass enforced internet access policies. They do that by connecting their PCs to the telephony network via the PBX using remote access programs to work from home. An attacker could find these modems using war dialing, control their PCs and enter IT network, bypassing firewall security.

VII. Malware Implementation

The implementation of the proposed malware is trivial for a skilled adversary. Most modern PBXs are executed atop of a UNIX based OS and hence they provide the full functionality of similar systems such as powerful shells, compilers as well as fully parameterized cron jobs, services and daemons. More importantly UNIX based PBX systems suffer from the same vulnerabilities of a general purpose system. Therefore the attacker can easily utilize available exploits for the particular UNIX platform and fine-tune the payload to the specific functionalities of interest of the PBX system. In addition to that, as most PBX systems are not treated as critical infrastructure, they are not updated regularly, thus prolonging the life cycle of the existing exploits.

For those PBXs that do not utilize such an operating system, there is usually some form of proprietary scripting or interpreted language for the specific platform. Even if they are absent, automation and testing tools such as Expect [29], can always be used in the attacking node, effectively controlling the PBX under attack, as if the code was executing in the target. In a similar way, many terminal emulators have their own scripting language that can be used to command the target PBX from the attacking PBX session.

The payload can directly manipulate the configuration settings of the management platform of the PBX or use lower level commands and tools. Indeed, most PBXs have a list of commands and tools (sometimes undocumented) that can provide access to the interworking of the switch. Deliberately not getting specific at this point, depending on the brand there exist commands to:

- Secretly listen into other connections by placing a tap (see Fig. 4) or by rerouting the traffic
- Examine memory contents (hex editor) and change them on the fly
- Verify if a line is busy and if so, enable an intrusion
- Send binary commands directly to the CPU or to specific boards
- Send keypresses in a set as if they were pressed by its user
- Set out of service trunks and sets
- Monitor the signaling in the ISDN lines, in the sets and in the PBX itself
- Monitor the keys pressed in a set
- Dump the contents of the database holding settings and

accounts
• Force a connection among two sets (effectively eavesdropping) (see Fig. 4)
• Send direct commands to the set (i.e. switch the microphone on).

VIII. Conclusions

PBXs practically serve all vital societal sectors, forming a part of the critical infrastructure, along with the public telephony network. As such, a malware targeting PBXs would have a devastating effect on communications' confidentiality, integrity and availability (especially during wartime). Threats include denial of service, interception of calls, data harvesting, psyops, economic fraud and money laundering. This work has explored the possibilities and the technical details for a new malware, the effects it could have, the actors involved in these attacks and what the most likely targets are. Given the arsenal of tools already available and the way PBXs operate, the occurrence of such a malware is a plausible scenario. Further work will be focused on the modeling of the behavior of the malware and the implementation of an actual prototype which will help to raise further awareness on the issue, leading also to more effective security measures.

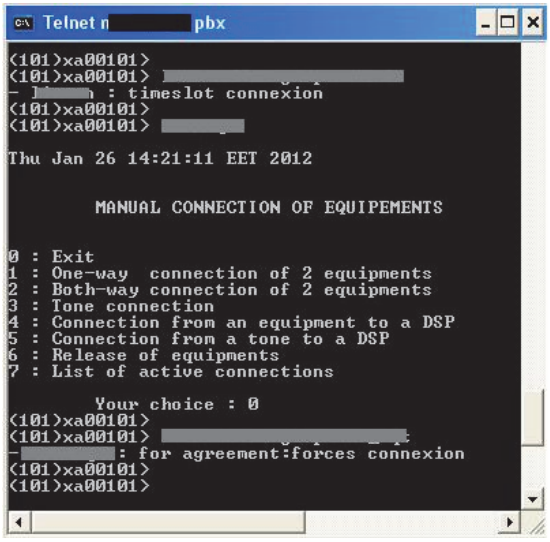

Fig. 4. Commands to multiplex or force connection among two sets (effectively eavesdropping).

References

[1] M. Hypponen, Mikko, "Cyber espionage in practice," in *CCD COE International Conference on Cyber Conflict*, Tallinn, Estonia, 2011.
[2] M. Akhvlediani, "The fatal flaw: the media and the Russian invasion of Georgia," *Small Wars & Insurgencies*, 20 (2), 2009, pp. 363-390, 2009.
[3] J.P. Farwell and R. Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, 1, 2011, pp. 23-40.
[4] D.E. Denning, *Information warfare and security*, 1st edition Addison-Wesley Professional, 1999.
[5] Council of the European Union, "COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," European Union, 2008.
[6] K. Geers, *Strategic Cyber Security*, Tallinn, Estonia, 2011.
[7] A. Sulkin, "2009 Enterprise Communications Market Results: Cisco Retains Leadership Status in a Down Market," NoJitter. http://www.nojitter.com/post/224200939/2009-enterprise-communications-market-results-cisco-retains-leadership-status-in-a-down-market?pgno=1
[8] T. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer* 44(4), 2011, pp. 91-93.
[9] R. Langner, "The first deployed cyber weapon in history: Stuxnet's architecture and implications," in *CCD COE International Conference on Cyber Conflict,* Tallinn, Estonia, 2011.
[10] C. Pollard, Craig, "Telecom Fraud: the cost of doing nothing just went up," Insight Consulting (White Paper), 2005.
[11] E. Luiijf and K. Marieke, "Insufficient situational awareness about Critical Infrastructures by Emergency Management," TNO Defence, Security and Safety, 2011.
[12] M. Grimalia and L. Fortson, "Improving the Cyber Incident Damage and Mission Impact Assessment," *IAnewsletter* 11 (1), 2008.
[13] J. Healey, "Four ways to address cyberconflict - and how analytics can help," *Intelligence Quarterly - Journal of Advanced Analytics* (Q4 2011), 2011, pp. 32-34.
[14] K. Rauscher, "ENISA Expert Group on Research Priorities in the Areas of Networking and Information Security for Resilient Networks," Athens, Greece: ENISA, 2009.
[15] I. Androulidakis, "PRETTY (PRivatE Telephony securitTY) – Securing the private telephony infrastructure," *Information & Security: An International Journal* 28 (1), 2012.
[16] BBC News, "Exeter hospital phones 'cannot understand Devon accent'," 2011, http://www.bbc.co.uk/news/uk-england-devon-14649238
[17] St. Cloud Times Minnesota, "BRIEF: Fire causes problem for hospital phones," St. Cloud, Minnesota, 2011, http://www.newsorganizer.com/article/brief-fire-causes-problem-for--ac0a083204b6cc060f0c2d0edede85fa/
[18] R. Ottis, "Theoretical Offensive Cyber Militia Models," in *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington D.C., 2011.
[19] Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9 (4), 2010, pp. 384-410.
[20] M. Fraser, "Geopolitics 2.0 (ARI)," Real Instituto Elcano ARI, 2009.
[21] C. Miller, "Why the Bad Guys are Winning the InfoSec War," in *CCD COE International Conference on Cyber Conflict,* Tallinn, Estonia, 2011.
[22] I. Bremmer and D. Gordon, "The geopolitics of cybersecurity," 2011, http://eurasia.foreignpolicy.com/posts/2011/01/12/the_geopolitics_of_cybersecurity
[23] EWI, "EastWest Institute ASPR handout," EastWest Institute.
[24] K.D. Mitnick and S.L. William, *The Art of Deception: Controlling the Human Element of Security*, Wiley, 2003..
[25] I. Androulidakis, "On the Importance of Securing Telephony Systems," *WSEAS TRANSACTIONS ON COMMUNICATIONS* 8 (1), 2009, pp. 102-111.
[26] Virus.org. "Default Password," 2012, http://www.virus.org/default-password/
[27] CFCA, Communications Fraud Control Association, "Worldwide Telecom Fraud Survey," 2009.
[28] CFCA, Communications Fraud Control Association, "Worldwide Telecom Fraud Survey," 2003.
[29] D. Libes, *Expect: Scripts for Controlling Interactive Processes*, Berkeley, 1991, CA, USA: University of California Press.
[30] A. Townsend and M. Moss, *Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications Center for Catastrophe*, Preparedness and Response & Robert F. Wagner Graduate School of Public Service New York University, 2005.
[31] PBX System Compromise and Data Mining from Digital Audio Files, Trustwave Spiderlabs, 2010.
[32] B. Krebs, "DHS Warns of 'TDos' Extortion Attacks on Public Emergency Networks," 2013, https://krebsonsecurity.com/2013/04/dhs-warns-of-tdos-extortion-attacks-on-public-emergency-networks/#more-19472
[33] B. Krebs, "Busy Signal Service Targets Cyberheist Victims," 2011, http://krebsonsecurity.com/2011/12/busy-signal-service-targets-cyberheist-victims/
[34] Federal Bureau of Investigation, "The Latest Phone Scam Targets Your Bank Account," 2010, http://www.fbi.gov/news/stories/2010/june/phone-scam
[35] V. Lisa, "Manila AT&T hackers tied to terrorist attack in Mumbai," 2011, http://nakedsecurity.sophos.com/2011/11/30/manila-att-hackers-tied-to-terrorist-attack-in-mumbai