# PRETTY (PRIVATE TELEPHONY SECURITY) - SECURING THE PRIVATE TELEPHONY INFRASTRUCTURE

Iosif ANDROULIDAKIS

**Abstract:** Private Branch Exchanges (PBXs) are privately owned equipment that serve the communication needs of a private or public entity making connections among internal telephones and linking them to other users in the Public Switched Telephone Network (PSTN) or other communication networks. Even if the core public network is operating normally, unintentional or targeted damages and attacks in PBXs can cause significant instability and problems. Furthermore, interception of calls is a very sensitive issue that affects all of us. In that sense, it is not an exaggeration to state that PBXs are part of a nation's critical infrastructure. Much has been said and done regarding data communication security but PBXs have been left unprotected, forgotten and waiting to be attacked. This contribution outlines a targeted, centralized project in order to both educate the users and secure their telephony systems. It compromises of educational, policy, auditing, technical, documentation, hardware and software solutions and actions that could be implemented under a joint project.

**Keywords:** PBX, PBX security, Telephony, Critical Infrastructure, PSTN.

## Introduction

Private Branch Exchanges (PBXs) are privately owned equipment that serve the communication needs of a private or public entity making connections among internal telephones and linking them to other users in the Public Switched Telephone Network (PSTN) or other communication networks.[1] There are millions of lines installed in every country and they essentially complement the public network. Economy, Health, Security, Private and Public sector they all rely on communication capabilities. Even if the core public network is operating normally, unintentional or targeted damages and attacks in PBXs can cause significant instability and problems [2] as well as significant financial losses.[3] Furthermore interception of calls is a very sensitive issue that affects all of us.

EU defines Critical Infrastructure as "The physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a se-

rious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU countries."[4] Hence, it is not an exaggeration to state that PBXs are part of a nation's critical infrastructure.[5]

## PBX Threats

Communications Fraud Control Association (CFCA) in a 2009 survey announced that the annual global fraud losses are in the range of $72-$80 billion for 2008 up 34% from the results of 2005.[6] 27% of companies reported losses greater than 5% of their revenue. Among the top 3 fraud loss categories, 20% of losses (~ $15 billion) is attributed to Compromised PBX/Voicemail Systems. In a complimentary survey, telecommunications fraud is a widespread problem that generally costs operators between 3 % and 8 % of their annual revenue, in addition to severely damaging their reputation and jeopardizing their customer relationships. This amounts to more than USD 44 billion globally.

An older survey (2003) of CFCA again states: "With respect to the causes of the growth of telecom fraud, some telecom providers did report that global fraud losses had partly risen due to an increase in worldwide terrorism. Terrorist organizations embrace telecom fraud to generate funds by illegally gaining access to a network and then reselling the service". Apart from the economic impact, the link of PBX abuse to terrorism is a danger that this proposal aims to help combat.

In Figure 1, we are presenting in a graphical way the threats that PBXs and Telephony systems generally face. Drawing from an earlier work of the author,[7] with the help of the captions in the figure, we briefly taxonomize the threats as follows:

Targeting integrity, unauthorized modem and other telephony devices bypass IT infrastructure's security measures providing an entry to the system via the telephone network [Caption 1]. In the confidentiality domain, a classical way of interception is the use of special devices or "bugs" as they are mostly referred to [Capt. 2], possibly combined with internal abuse [Capt. 3]. More elaborate interception techniques include the man in the middle attacks, where signals are intercepted, decoded and then transmitted back to their original destination [Capt. 4]. Apart from confidentiality, issues, financial loss is also a major parameter. With telephony fraud taking place unnoticed for a substantial period, the accountant soon receives the bill in a box rather than in an envelope [Capt. 5].

Proceeding, to other threats, using social engineering[8] techniques a person can extract vital information from a secretary over the phone (e.g. a username and a password to login to the network [Capt. 6]). Impersonating a network technician [Capt. 8] a malicious person can even access the PBX itself or the operator's console [Capt. 7],

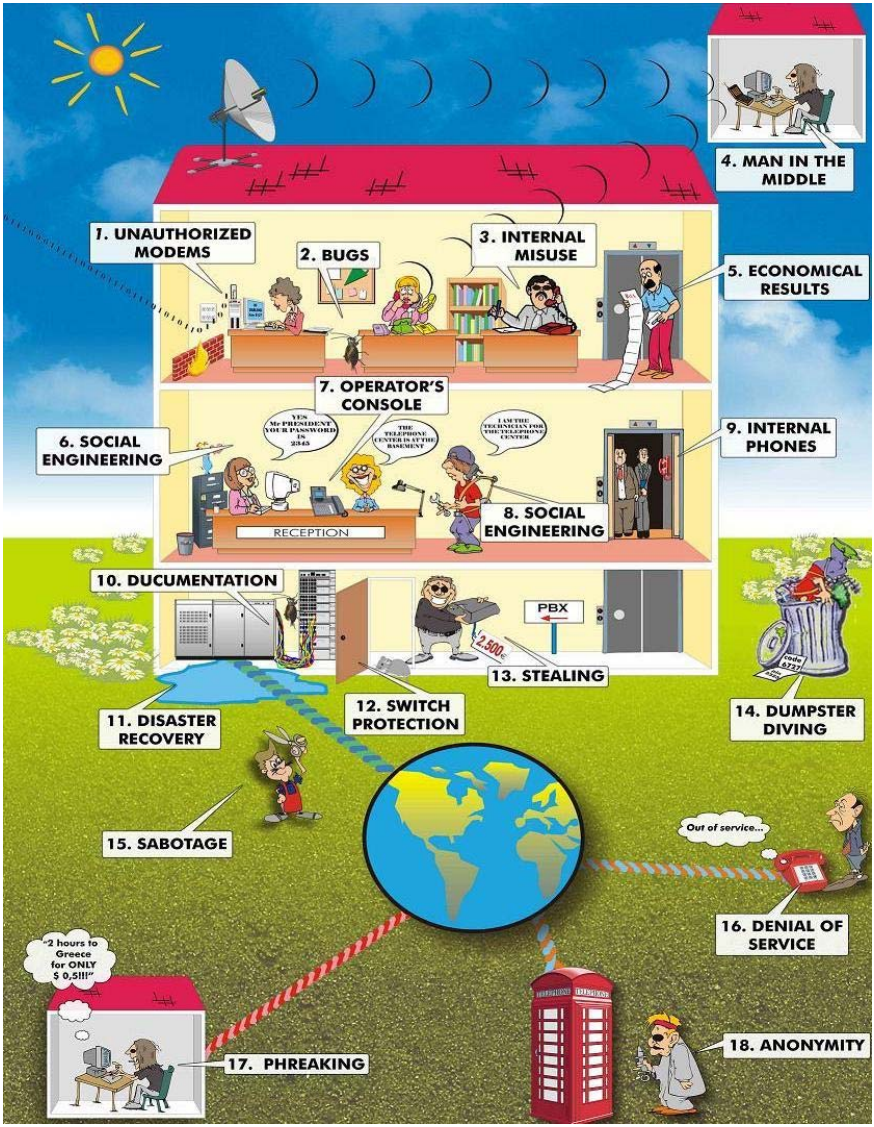


Figure 1: Taxonomy of Telephony Threats.

which is a powerful set, able to change system's settings. At the same time, internal phones placed in publicly accessed areas (e.g. in the lobby or in the elevator) are sensitive point in a company's telephone network [Capt. 9].

Equipment, patching and connections should all be well documented [Capt. 10], helping among other things overcome problems from natural disasters [Capt. 11]. There is no need to "advertise" the location of the PBX and it should be placed in properly secured areas [Capt. 12]. Indeed, modern telephone exchanges use expensive and easily removed and carried out boards so a couple of minutes would be enough for an incident to take place causing not only financial damage but an outage too [Capt. 13].

Outside the perimeter of the company, lack of means and procedures to properly dispose of sensitive information can lead to attacks based on "dumpster diving" [Capt. 14] that provide outsiders valuable information about our security. In the Availability domain, denial of service attacks render the telephony service unavailable. This can be achieved by causing physical damage [Capt. 15] or using software techniques, banning telephones from placing or receiving calls. [Capt. 16].

The array of attackers compromises of insiders and outsiders. At the lower end of the impact scale are skilled individuals, usually teenagers trying to break in just for the challenge. More malicious individuals are trying to earn personal benefits by deploying various illegal activities such as call sell operations using stolen codes and accesses [Capt. 17]. At the other end of the spectrum is the organized crime. As noticed earlier, compromised telephone networks are often used in order to cover-up illegal activities such as terrorist and ring operations, drug selling, money laundry etc [Capt. 18].

Following this prompt taxonomy, it is immediately clear that a targeted, centralized project has to be presented in order to both educate the users and secure their telephony systems. The rest of the paper proposes the methodology to design this project and the parts of the sub-actions themselves.

## Methodology of the proposed project

The methodology to design, implement and disseminate the results of the project is described in the following sections:

*User and System Requirements.* In the early phase of the project, the requirements will be set up focusing on confidentiality, integrity, and availability of PBXs as well as ease of use for the operators. As a first step, the requirements of PBX systems from an operational point of view will be collected and analyzed. Furthermore, an un-elastic requirement will be not to hinder at all the PBX's functionality after the implementation of the software and hardware tools proposed.

*Research and Development.* A substantial part of the project will be devoted to research and development of methodologies, software and hardware. A model consist-

ing of rules and situation descriptions will be researched in order to develop an expert system that will assist in creating and maintaining higher security for the operation of a PBX system through adoptable guidelines for PBX operators It will encompass standard operating procedures, Security policies and Disaster recovery plans and Methodologies to help dealing with Fraud, Detection and prediction of maintenance problems as well as auditing.

The different aspects of securing the Telecommunication Providers services will also be studied. Specifying the possible attacks and fraud scenarios and approaches will help preventing and handling those misuses. Detection and prevention techniques will be developed, leading to appropriate mechanisms and a framework for providing secure infrastructures. Further, applicability of state of the art security solutions will be evaluated for their usability for Telecommunication Providers services protection. Finally, apart from software solutions, a hardware PBX firewall8 will be designed in order to provide an extra layer of security, irrespectively of operators' behavior. In any case, it is interesting to note that the methodology used, will be able to cover both classical PBXs and VoIP ones that present among other things different challenges.[9]

*Implementation*. The implementation phase will lead to prototype installations and solutions, stemming from the results of research. In order to test the efficiency of these means and recommendations, the Software and Hardware solutions will be implemented in a selected number of PBXs serving Banks, Hospitals, Public bodies, Ministries, Industry, Universities etc. In addition, the expert system and guidelines will be presented to these PBXs' operators. The increase of the security level will be demonstrated by the security audits performed before and after implementation. This phase will cover, among others, all the security aspects outlined in the NIST report.[10]

*Dissemination of results*. An equally important part of the work, the dissemination of results will aim at the broadest possible audience. The expert system will be publicized and educational material will be distributed to ministries of telecommunications and to telecom providers. Actions to raise awareness will include Conferences and seminars, targeted for both specialists and the public.

## Description of Specific Actions

As described previously, the purpose of this proposal is to establish multithreaded actions in order to help mitigate the security risks that PBXs face. As such it complies of an array of scientific Research & Development actions as well as practical implementations and demonstrations. More specifically, there are three main axes which form the pillars of the Scientific and Technological Objectives that the project will cover. These pillars with the corresponding sub-actions are the following:

1. Education and awareness raising

1.1. Educational programs

1.2. Actions to raise awareness: Conferences; Production of educational materials; Surveys to make the problem widely known

1.3. Knowledge transfer

2. Research & Development

2.1. Securing the interaction of VoIP and WEB2- Security implications of VoIP integration with WEB2.0 platform applications

2.2. Forensic Analysis in NGN

2.3. Standard operating procedures

2.4. Security policies

2.5. Disaster recovery plans – Methodologies

2.6. Software development: Fraud detection techniques; Detection and prediction of maintenance problems; Expert System with adoptable guidelines for PBX operators; Expert System to help auditing

2.7. Hardware solutions, including the a PBX firewall

3. Practical implementation of the project's outcome

3.1. Security audits

3.2. Patching and securing equipment

3.3. Documentation.

## Impact PRETTY will Have on PBX security

As stated in the risks section, various surveys point a link between terrorists and PBX fraud. Most of the actions described in this proposal are particularly focused on cyber defence. Cyber attacks vary from plain social engineering [11] to the most technically advanced. With that in mind we propose such an array of actions, both in the theoretical and the practical domain, focusing not only on technology but on the human factor too. The project will successfully prevent cyber attacks issued by criminal organisations against telecommunication networks. It will help securing PBXs and provide information about possible attacks. It will act both proactively and reactively. In the first sense, it will help administrators properly administer their systems. They will be offered tools to better perform auditing as well as everyday functions. Customizable guides and polices, with the help of an expert system will be part of their everyday operations. Reactively, in cases of incident, they will be offered the right procedures and tools to perform disaster recovery steps. The special firewall envisioned will add another layer of security, on top of the others. A very important parameter is the general user awareness that will be accomplished through seminars and conferences.

Developing efficient and real-time monitoring, detection, diagnosis and reaction approaches, the software and hardware tools presented will provide early signs of malfunctions that could be attributed to fraud or actions of mischief. Logs from lots of nodes and thousands of users are typical examples of cases found in large scale PBXs.

Using real-time detection/prevention module to analyze in real-time multiple event streams (logs, alerts generated by other modules) and according to actual set of detection methods it will detect threats. This approach will allow proposed solution:

1. to be able to monitor even very large PBX infrastructures
2. to easily add new detection methods
3. to integrate the module with other systems.

Feedback from this module could immediately be fed to the expert system to propose in real time the best means to combat the threat and mitigate the risk.

By protecting PBX from Denial of Service attacks, an increased critical infrastructures reliability, resiliency and security will be achieved. By enforcing better management and auditing, early signs of possible problems are immediately spotted and administrators act relevantly following the guidelines that the expert system proposes. In the unlikely event of a system collapse, the Disaster Recovery framework will be the last solution to timely restore services. For security enhancement per se, every single action of the project, as described in the relevant sections adds to the goal.

The interconnection with other public and open networks causes security problems, and successful attacks may have significant effects. PBXs do not exist by themselves. An integral part of their functionality is the interconnection with the public telecommunications network. This interconnection, in case of a distributed denial of service, encompassing an array of compromised PBXs could severely harm the functionality of the public network. At this point, we must stress the importance of the interconnection of PBXs with the IT infrastructure. There are lots of cases where a successful PBX attack, proves to be the easiest way to enter the data network, bypassing even correctly set up firewalls.

In addition, with the emergence of new web services, companies, universities and governmental departments have quickly shown interest and started embracing them. The VoIP providers, in turn, started investigating how they could benefit from these new opportunities. Some VoIP SMEs have already integrated to some Web2.0 platforms applications allowing a subscriber to set up free conference calls with users that are subscribers of this platform or not. These applications also offer the opportunity to chat, send SMS and MMS. Enhancing Web2.0 platforms with multimedia services hides a growing business involving at the time being pre-paid services and advertise-

ment. Unfortunately, this business, if the appropriate measures are not taken, will certainly be the subject of abuse and fraud. Part of the project will be aiming at securing the multimedia applications integrated with the Web2.0 platforms by preventing attacks and mitigating service abuse, thus protecting the VoIP providers against revenues losses and users against fraud. This will be achieved by providing a complete solution for the VoIP providers to help them define an efficient Telco2.0 detection and prevention strategy. Next Generation Network (NGN) is an ecosystem predominated by packetization, where VoIP, IPTV and FMC are only three of plethora of hopes NGN gives to telecommunication service providers. One can do everything over IP, especially in this age of convergence of services and applications. However, VoIP, FMC and all other forms of NGN also bring with it greater security risks, and users illiterate about telecom fraud end up paying the price for it. In regards to analyzing, testing and benchmark the performance capabilities of PBX infrastructures, the expert system will allow the automatic reporting capability, producing among other things a security factor. As such, the teams that will undertake the penetration testing of the PBXs (dissemination part of the work) will follow the methodology suggested, outputting a measurable security indicator. This metric is expected to drastically change, from lower security scores to higher, when measured before and after the implementation of the project's solutions. In the legal context, EU nations will get closer to the goals of meeting national and international mandates and challenges. Money laundering through telecom-PBX fraud is one example. Furthermore, enhancement of protection against unauthorized interception of calls and call logs is an issue that will be handled. Providing better and more secure functioning PBXs, we address the fears of personal data leakage. Closing, an integral part of the project is its great scale dissemination phase that will form the opportunity for networking and exchange between the stakeholders to facilitate the emergence of common European solutions. The active participation of end users (e.g. public authorities, relevant EU agencies) will be essential. A network of partners, encompassing Academia, Companies and Industry and cross-country operations will be formed. In addition the demonstration of the deliverables of the project, will take place in a diverse list of PBXs, serving Banks, Hospitals, Public bodies, Ministries, Industry and Universities. The feedback collected will help shape common European solutions since technology itself is the same. The seminars and conferences scheduled will help raise awareness both in the general public and in the specialized category of PBX administrators.

## Conclusion

Much has been said and done regarding data communication security but PBXs have been left unprotected, forgotten and waiting to be attacked. Checking the proper operation and ensuring the safety of PBX as well as protection against unauthorized use and access is usually left to the owner. This has also been stated in various security

manuals of vendors.[12] This has of course tremendous effects since due to economic and technical difficulties, in essence it is impossible to guarantee that the proper measures are taken. This contribution outlined a targeted, centralized project, compromising of educational, policy, auditing, technical, documentation, hardware and software solutions and actions, in order to both educate the users and secure their telephony systems. It will hopefully form the basis for actual implementations by various stakeholders.

## Notes:

[1] Wikipedia, *PBX*, http://en.wikipedia.org/wiki/Pbx, March 2007.

[2] Iosif Androulidakis, "PBX security," *2nd Pan-Hellenic Conference on Electronic Crime*, Athens, 23-26 November 2004.

[3] C. Pollard, "Telecom fraud: the cost of doing nothing just went up, White paper", Insight Consulting, Feb 2005; D. West, "De-Mystifying Telecom Fraud", Telecom Business, July 2000; V. Blake,, "PABX Security, Information Security Technical Report", vol. 5, no. 2. (2000), 34-42.

[4] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm.

[5] The importance of private telephony in critical infrastructure has also been documented in D. Denning, *Information Warfare and Security* (Addison-Wesley Professional, 1998).

[6] Communications Fraud Control Association (CFCA), Worldwide Telecom Fraud Survey, CFCA, 2009.

[7] Iosif Androulidakis, "WSEAS Transactions on Communications," 8:1 (January 2009): 102-111.

[8] NIST, "PBX vulnerability analysis", special publication 800-24, 2001.

[9] T. Walsh, D. Kuhn, "Challenges in securing voice over IP", IEEE Security & Privacy, vol. 3, no. 3, May-June 2005, 44-49.

[10] NIST, "PBX vulnerability analysis", special publication 800-24, 2001.

[11] K. Mitnick, W. Simon, *The Art of Deception: Controlling the Human Element of Security* (Willey Publishing, 2002).

[12] See for example *Avaya Products Security Handbook* (November 2002).

**IOSIF ANDROULIDAKIS** (BSc in Physics and PhD and MSc in Electronics) has served as Head of the Telephony Department in the Network Operations Centre of the University of Ioannina, Greece. He has an active presence in the ICT security field having authored more than 25 relative papers and having presented more than 50 relative talks and lectures in international conferences and seminars in 15 countries. His research interests focus on security issues in PBXs (private telephony exchanges) where he has more than 15 years of experience, as well as in mobile phones and embedded systems, and holds two patents. He is a member of IEEE (Technical Committee on Security & Privacy) and ACM (Special Interest Group on Security Audit & Control). Finally, he is a certified ISO 9001:2000 quality systems auditor as well as a certified auditor and consultant for ISO 27001:2005 Information Security Management Systems. *E-mail*: sandro@noc.uoi.gr.