Information & Security: An International Journal

Androulidakis, Kharchenko, and Kovalenko, vol.35, 2016, 99-120

https://doi.org/10.11610/isij.3505

IMECA-BASED TECHNIQUE FOR SECURITY ASSESSMENT OF PRIVATE COMMUNICATIONS: TECHNOLOGY AND TRAINING

Iosif ANDROULIDAKIS, Vyacheslav KHARCHENKO, and Andriy KOVALENKO

Abstract: Nowadays, almost everywhere, there are a huge number of privately owned telephone exchanges 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 telephone network. Such communications cover most vital infrastructures, including hospitals, ministries, police, army, banks, public bodies/authorities, companies, industries and so on. The purpose of this paper is to raise awareness in regards to security and privacy threats present in private communications, helping both users and vendors safeguard their systems.

This article provides an introduction to private branch exchanges (PBXs) and private communications, and a review of relevant threats and vulnerabilities. Finally, one possible approach to assessment of private communications security is presented, along with appropriate taxonomies. Such approach relies on performing gap analysis and is based on the IMECA technique.

Keywords: PBX, communication, confidentiality, integrity, availability, threat, vulnerability, assessment, IMECA, risk.

1 Motivation

1.1 Main Properties/Attributes, Security of PBXs and Telephony

Apart from the public telephone network we all know, there is a parallel private network, consisting of PBXs. These are privately owned telephone exchanges 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 telephone network. They exist in the form of IP PBXs (using the IP protocol via VoIP technologies) and conventional time division multiplexing (TDM) PBXs (using phone lines). Their software can be offered proprietary or via open source. While communication with

other entities takes place using trunk lines to the public telephone network (or the Internet), internal telephone traffic fully depends on PBXs.[1]

Typically, PBXs involve both hardware and software components, which interact with each other. One of the most important problems of modern PBX is the reliable assessment and assurance of their security level. During the assessment, it is necessary to take into account a set of various features and factors, their interrelations and interactions.

There are several challenging problems in the area of security assessment and assurance for general PBXs, including the following: (1) consideration of all possible vulnerabilities, related to all types of involved components (in general, hardware, software and interfaces), which could appear during all stages of their life cycles, (2) prioritization of such vulnerabilities according to their criticality and severity, and (3) determination of both sufficient and cost-effective countermeasures either to eliminate the identified (or potential) vulnerabilities or to make the vulnerabilities difficult to exploit by an adversary.

Accurate evaluation of the actual level of the vulnerabilities' criticality and severity (and security of the system in whole) is one of the main challenges. Inaccurate estimation can cause additional efforts, costs and may present undesirable level of security risk.

One of the possible ways to consider all possible security vulnerabilities for PBXs is using a process-product approach. Such an approach requires performance assessments not only for products (components of the PBX at different stages of their life cycle), but for all the processes within the product life cycle. Application of process-product approach is inevitable in case of multi-component systems, consisting of both hardware and software.

1.2 Analysis of Related Works

Failure Mode, Effects and Criticality Analysis (FMECA) is an extension of standard formalized technique called Failure Mode and Effects Analysis initially intended for the systems reliability analysis devoted to the specification of failure modes, their sources, causes, criticality, and influence on system's operability.[2] "Failure modes" means the ways, or modes, in which something within a system might fail. Failures are any errors or defects in a form of deviations from normal operation, which can affect the user of such system, and can be potential (that can happen in future) or actual (that have already happened). "Effects analysis" refers to studying the consequences of those failures. In addition, FMECA extends FMEA (Failure Modes and Effects Analysis) by including a criticality analysis, which is used to chart the probability of failure modes against the severity of their consequences.

In the FMEA-technique, all possible failures are prioritized according to consequences severity, frequency and detectability. Such technique is used during design stages in order to avoid failures in a system being developed. The overall purpose of FMEA-techniques is to take actions to eliminate or reduce possible failures.

There are a lot of FMECA technique modifications related to various components, including software (SFMECA), to various levels of I&C hierarchy (HFMECA), to various processes, including design (DFMECA) and others.[3,4] In general cases, Concept and Event Modes and Effect Criticality Analysis may be considered. These modifications are not used to assess PBX security.

IMECA (Intrusion Modes and Effects Criticality Analysis) is a modification to FMECA-technique that takes into account possible intrusions into the system.[5] Mainly, the technique is intended to assess technical vulnerabilities, but can also be propagated to other types of vulnerabilities. During the assessment of PBXs, IMECA can be used in addition to standardized FMECA for safety-related domains, because each vulnerability can become a failure in a case of intrusion into such systems.[6,7]

1.3 The Most Important Security Issues in PBXs

Results of the most important security issues related to private communications are represented by the following subsections.[1]

1.3.1 Confidentiality

Eavesdropping is one of the most important telephony confidentiality threats. Voice communications can be intercepted in many ways, in different time scales in order to be retrieved and analysed later. In turn, fax calls and data traffic can be intercepted and further extracted.

One of technical means intended for providing access to the line can be a simple tap (also known as “bug”) connected in the cable. PBXs often include special hardware modules that perform the task of translating the proprietary digital signals to audible, analog audio. Telephone sets, on the other hand, can be modified to transfer voice while on hook, either with hardware modification or software commands.

One of the possible ways to exclude such type of threat is in activating the monitoring and debugging features that allow real time interception by administrators. There is also third party software for the same goal. Most PBXs offer tools to silently listen to other calls and such tools can be abused.

Another threat is based on call correlation and traffic analysis techniques, as well as call logs analysis, allowing industrial espionage information gathered even without knowing the actual content of the calls.

1.3.2 Integrity

The second major part in the taxonomy of threats deals with integrity attacks. Such attacks on a PBX vary from reprogramming it, installing backdoors for future access, altering data, modification of features and services, up to economic fraud. At the same time, it is possible to alter the communication flow, connecting lines to different destinations that can lead to denial of service and PBX shutdown.

Identification of the caller to the calling party, from one point of view, is the handiest features of telephony, but, from another point of view, can arise whole set of unpleasant acts (harassments, pranks, spam calls, calls from unwanted persons, malicious calls and so on).

From the integrity point of view, the PBX can be the weak link to target the IT platform that is interconnected with it. In a case of suck link to an organization's IT network, an attacker can find an easier point of entry into the critical assets.

1.3.3 Crime-Billing

Crime opportunities pretty widespread in telephone communications area since telephony security is typically weaker compared to IT security. One of the most employed vulnerabilities is due to possibility of unauthorized access to telephone service with the relevant economic losses due to bills. Money laundering through PBXs is also effective, while consequences after a multimillion fraud in calls starting from a company's PBX would lead to financial and business disaster. Even terrorist organizations are thought to be embracing telecom fraud to generate funds.[9,10]

Telecom services are also can be abused be fraudsters, allowing use of the vulnerable infrastructure by non-authorized persons (making free calls or selling these calls via a call selling operation). It is also true that fraudsters can steal expensive components of a PBX. One of possible countermeasures is in protection the PBX boards by the means of cryptography.

Compromised PBXs can also call premium rate services or just high cost destinations that can lead to extensive bills.

1.3.4 Availability

Blocking of PBX communications is relatively easy process. A lack of effective telephone communication can cause annoyance for its users.[11] More importantly, the service of some critical infrastructures can be damaged via blocked communications.[12] Moreover, even strong national economy could suffer up to great degree if a targeted attack was to render useless industry's telecommunication lines. In any case, it is apparent that in the modern demanding business environment a company or organization cannot survive without telephone service.

If the availability of the system is compromised, the administrator's access could be cut off in many ways; external lines could be set out of service; the database containing the setup of the PBX or files from the operating system could be completely deleted and so on.

Another effective denial of service technique can target the software and hardware protection of PBXs. In this way, many of modern PBXs employ protection against unauthorized copying and black market selling utilizing some form of hardware-key, usually based on Field Programmable Gate Array (FPGA) technology.

Availability can also be compromised in a remote way through denial of service in the communication abilities, for example, by another PBX (or an array of PBXs) attacking the target with hundreds of calls per minute.

Intervening the firmware of the PBX, it is possible to force the PBX to perform functions that could lead to physical failure of its electronic components. Another factor is the probability of theft of PBX component; it leads to, first of all, interruptions in the service, economic losses, and, at the same time, the stolen component can host a memory storage element containing valuable (or even sensitive) information.

Finally, availability is not always compromised by attackers: more than often, technical glitches, bugs or environmental disasters cause extended scale and duration service interruption incidents. This is why protection against environmental elements and disasters should be required.

1.3.5 Other Threats

Typical use of a compromised telephone network is to use it as a screen for covering-up illegal activities such as ring operations, drug selling, money laundering and so on. This anonymity can also be exploited to attack other targets, making the compromised PBX an intermediate point and its owner possibly held liable for the attack.

At the same time, the compromised PBXs can be a repository of illegal information to be exchanged by the fraudsters: encrypted messages could be stored by criminals and retrieved by their peers while multiparty calls can take place, organizing actions.

So far technical threats of private communications were examined. However, it is not always necessary to be technically savvy to abuse a telephone network. A very common technique for accessing it is the use of Social Engineering; people who pretend to be someone else use their persuasion to extract valuable information for the network itself or information that can be helpful for infiltrating it. There are two good examples here, one is the use of Social Engineering by a person that impersonates a trusted one (e.g. an employee) via the phone and extracts confidential information from a secretary and the other is a person that gives false information and imperson-

ates a network technician in order to extract information about the whereabouts of the PBX. Gaining in this way the guard's approval to access the PBX he has full access to the network. A survey by the Communications Fraud Control Association provides further examples of social engineering.[13]

1.4 Objectives

The objectives of this chapter are (1) to customize the IMECA-technique and to develop an applicable approach to assessment the level of PBXs security, (2) to present comprehensive cases of such technique implementation and (3) describe appropriate training experience. Such assessment is a crucial part of trainings for both target groups – students and engineers. The rest of the paper is structured as follows: Section 2 represents results of review for threats and vulnerabilities for PBXs and communications. Section 2 describes the underlying concepts of the gap-and-IMECA-based approach, as well as its application to assessment of safety-critical I&C systems. Section 3 provides a methodological-level interpretation of the proposed approach in the context of complex products/systems involved into implementation of PBXs.

Finally, section 4 represents appropriate case study related to training activities in frameworks of the EU funded TEMPUS-SEREIN project "Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains."[14] Last section concludes discussion and describe future steps.

2 Vulnerability Review

2.1 Taxonomy of "Threat-Vulnerability-Attack"

This chapter represents the taxonomy of the main notions used further. Such taxonomy covers the notions of process, product, intrusion, discrepancy, gap, anomaly, vulnerability and attack.

Based on its nature, typical PBX can be decomposed into the following components: data transfer process, activities and appropriate products used to implement such activities (Figure 1). In turn, products can be represented by some software, hardware and connections/interfaces data pass through.

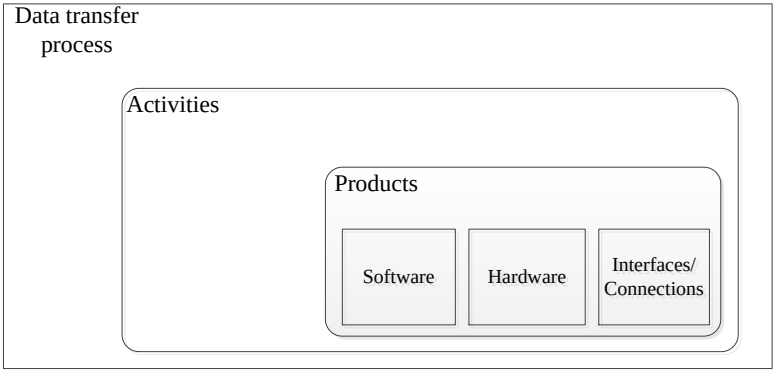

Figure 1: PBX components.

It is possible to outline some important attributes of a process, product and intrusion, as well as their interrelations. All the possible vulnerabilities of PBX are due to products, used in data transfer process, when such products possibly contain some anomalies. Anomalies can appear in a case of non-ideal product development process (Figure 2).

The main notions in Figure 2 are development process and product. Such processes are being implemented through the development stages of product life cycle model in order to produce products. Results of implementation of development processes, which led to the creation of the product, can have effects on possible consequential changes in sub-processes. Each of sub-processes comprises activities, and, in a case of "non-ideal" process, some of them can contain discrepancies.

So, now we can define gap as a set of discrepancies of any single process (which can consist of a set of sub-processes) within the product development process that can introduce some anomalies in a product and/or cannot reveal (and eliminate) existing anomalies in a product. In particular, such anomalies can be caused by imperfection of product specification (or even representation), implementation, verification, and/or other non-compliances.

The taxonomy for the data transfer process represented in Figure 3. Data transfer process is based on a sequence of certain activities. Such activities cover appropriate products, which, in turn, can contain anomalies due to imperfection of their development process. In terms of cyber security, some of the anomalies of the product can be vulnerabilities. Vulnerabilities, in turn, can be exploited by an adversary during intrusion into the product to implement an attack in order to introduce some unintended functionality into the product.

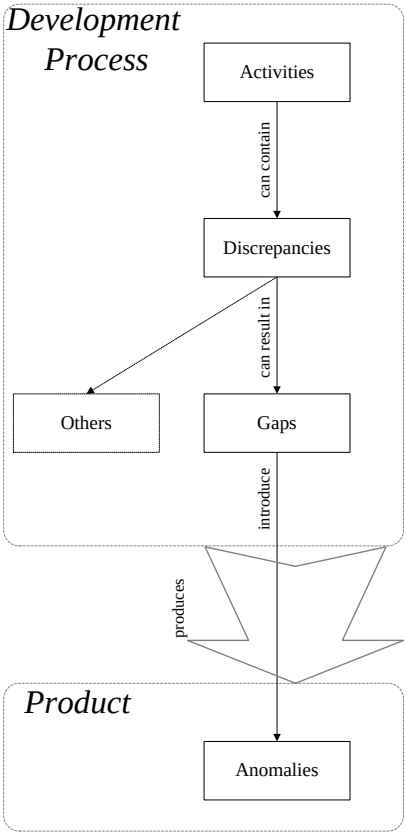

Figure 2: Taxonomy of notions in product development process.

2.2 Threats and Vulnerabilities for PBXs and Private Communication

This section focuses on technical details of PBXs, describing the parts of a PBX, as inevitable part in consequent analysis of threats and vulnerabilities. Figure 4 depicts typical structure of a PBX and it is the basic reference for the further discussion.[1]

Threats of a PBX can arise due to the following their inherent technical features:

- External interfaces: they use a number of technologies and protocols such as ISDN E1/T1, Analog, CAS 2bit, IP, GSM/3G (with FCTs), etc. The medium used can be copper, optical fibers, and wireless technologies including microwave, WiFi, infrared, etc. The “frontier” of the PBX is the demarcation point, that is, the point that interconnects the customer’s network with the external network.

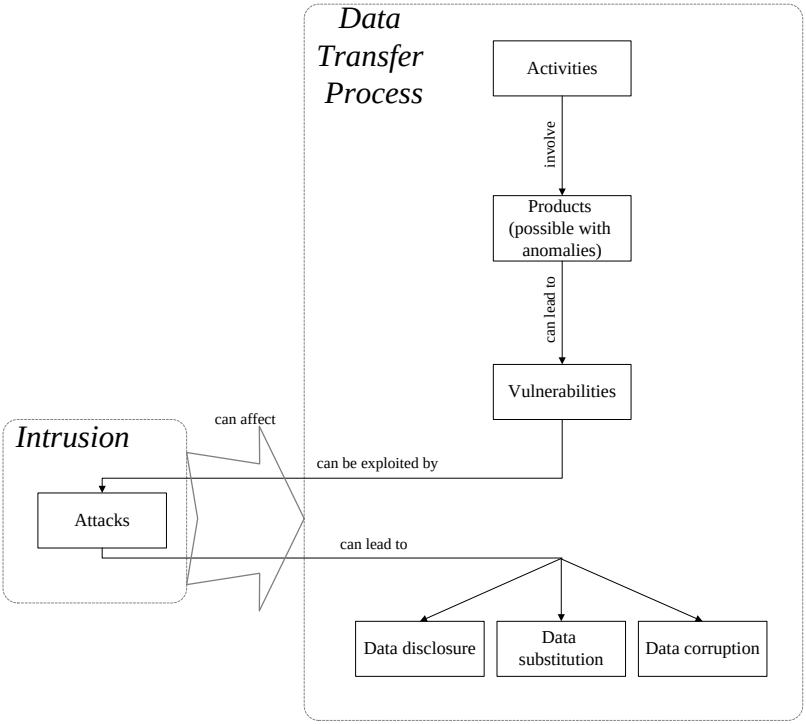

Figure 3: Taxonomy of notions in data transfer process.

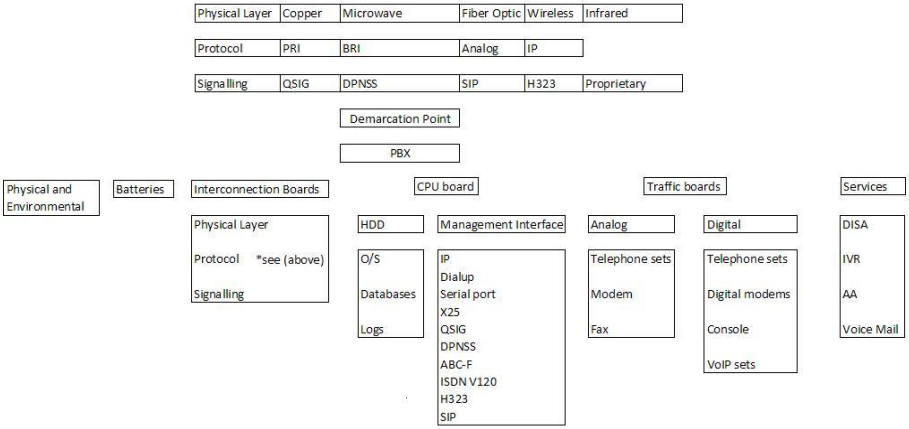

Figure 4: Typical structure of a PBX.

- Cables and distribution frames: distribution frames along with the cabling are the "circulatory system" of the whole infrastructure. The main distribution frame is the part where all internal and external lines are connected to the PBX, the "heart" of this network of cables. It is placed close to the PBX, with one part of it dedicated to the lines coming from the PBX and the other part of it dedicated to the lines leaving towards the users and the external network. The route from the PBX to the set can be many hundreds of meters long, with cables passing through all these distribution frames and ducts. This makes it possible to insert an interception device anywhere in the length of this route, or cross connect phones in parallel, transferring voice from the victim to the listening post.

- Physical parameters: mainly represented by physical location where the PBX is actually located in. Attacks can be facilitated by lax physical security measures. There are many cases where the PBX is placed in the basement or in the corridors of an organization, behind unlocked doors, or even worse, in plain view. There are even cases where informatory signs and labels point to the PBX. Phones in public areas such as the elevator phone or the operator's console are immediate targets. The physical access, for the daring fraudsters, involves actually visiting the PBX or its cabling and performing their malicious actions on-site.

- PBX boards and hardware: most of PBXs are designed using a modular architecture. There is a chassis offering backbone connectivity and various boards are inserted in slots, each board performing a specific action. In any case, almost every single board holds memory chips and microprocessors, while boards serving telephones (usually an even number) show a distinctive pattern that allows a specific phone to be targeted for hardware intervention.

- PBX sets: the main "users" of the PBX are its telephone extensions. A multitude of sets can be connected in a PBXs, given the respective boards exist. The connection from the boards to the sets can be wired or wireless (e.g., DECT), with one pair of two pairs of cables, an optical link or even a distance extension device (repeater). Different sets have different physical, electric, and logical characteristics. Leaving aside an attack to the PBX itself, analog sets need a physical intervention in order to be bugged (should be dismantled to have electronic bugs installed, or have their speed dialling memories read). Digital ones, full of microprocessors, EPROMS, and ICs, are susceptive to both hardware and software attacks. In any case, the goal of the attacker would be to intercept information, not only during a call but also discussions held in the surrounding area of the phone, by making the phone transfer voice while on hook while at the same time it appears as being idle, innocently waiting for calls.

- The CPU and the management port: serving all these sets (and not only), the "heart" of the PBX is the board hosting the CPU. Apart from the CPU, the same board hosts various memory circuits (ROMS, EEPROMS, Flash memories that contain voice guides), HDDs, a floppy disk, and serial or USB ports. The CPU can be connected in a variety of ways to the outside world, in order for the PBX to be managed. There are direct or via modem serial port connections, proprietary protocols (usually linking to a digital set or the console), TCP/IP connectivity over Ethernet, V120 via ISDN, or even X25 in some older models. 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, and H323. There are also proprietary ones from different PBX vendors (e.g., ABC protocol). By monitoring these protocols an adversary can increase HIS target list finding further maintenance modem numbers and IP addresses from interconnected systems. In addition to that, potential targets can be found in modem logs, in routing and host tables and in extra subsystems and functionality present such as Voicemail.

- Software, administration, management suite and station: the administration/management station can be a PC or server running whatever OS. Smaller PBXs require the software to be installed in the external administration server, while larger PBXs typically include the software in their own operating system. The software running can be a closed proprietary operating system or based on generic operating systems specifically modified for the PBX. We will focus only on the management suite since the rest is a topic covered in computer security literature. The management suite allows the provisioning of the PBX, controlling the operation of it, setting up, activating and modifying features, performing maintenance tasks, and so on. There are command line suites, menu driven, and full Graphical User Interface ones. Getting access, a malicious hacker could launch all the attacks described previously against confidentiality, integrity, and availability.

- Low-level tools: besides the everyday tools that administrators use, an array of low level, powerful commands, and tools are available, sometimes non-documented and restricted for highly experienced personnel. They typically allow to secretly listen into other connections (by placing a tap); examine memory contents (hex editor) and change then 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, etc. There are even cases of forgotten, leftover tools from the testing phase that made it to the production, even with undocumented or hardwired (non-changeable) username/passwords. Special codes and key sequences can also enable hidden functionality. Debug-maintenance features are very dangerous in the hands of an attacker since they

can monitor or isolate single lines or whole trunks. They can also provide a signalling analysis, tracing all messages exchanged. Other tools allow direct access and operations to the database, bypassing the management suite. Memory reading with hex editors provided and hot patching is also possible allowing breakpoints to be inserted in the code and possibly elevate user privileges or bypass passwords. Reprogramming the flash memory can enable secret functionality, something that could be exploited by a malware.

- Database: apart from low level tools, there are tools to access the internal database of the PBX. Indeed, all necessary PBX setup and operation information is stored in such a database that can be accessed either from the management session or (even worse) directly from the OS (e.g., via open listening TCP sockets). This functionality although dangerous is important for communicating changes in a network of PBXs. Changes to the settings made via the management suite get reflected in the database. Using the right tools, however, an attacker can bypass the management suite as stated and enter, modify, or delete values directly. This can lead to unexpected results and buffer over flows. Besides that, having full access the intruder can modify features (e.g., remove call barring and elevate call permissions). He can also delete the whole database. Quite interestingly, at least one manufacturer has specific login accounts with the sole purpose of halting the PBX or deleting and reinstalling the settings database, effectively wiping the existing setup.

The most exploited PBX services are the Direct Inwards System Access and Voice Mail.

3 IMECA-based Technique

There are a lot of techniques for the complex systems assessment: FME(D/C)A (Failure Modes, Effects and Diagnostics/Criticality Analysis), FTA (Fault Tree Analysis), RBD (Reliability Block Diagram), MM (Markov's Models), etc. Each of them is suitable for specific types of systems and life cycle stages. Though general procedures of application for the techniques are described by standards and guides, there is no universal solution that could be unambiguously applied to any existing complex system.

3.1 IMECA Analysis

The FMEA is a standard technique that is formalized to be used in reliability analysis devoted to the specification of system failure modes, their sources, causes and influence on operability of the system. "Failure modes" denote the ways something might fail; "effects analysis" refers to studying the consequences of those failures. Examples of failures can be defects or errors; moreover, failures can be either potential (that can potentially happen) or actual (that already happened). FMEA technique implies prior-

itizing of all possible failures according to severity of their consequences, frequency of their occurrence and simplicity of their detection.

Typically, FMEA technique is used during the product design/development stages in order to avoid product's failures in future. During other stages of product's life cycle, the technique is typically used for process control, before and during ongoing operation of the process. The purposes of the FMEA are the following:

- to take preventive actions to eliminate or reduce possible failures, starting with the failures with the highest priority;
- to evaluate risk management priorities for mitigating known vulnerabilities.

IMECA (Intrusion Modes and Effects Criticality Analysis) is a modification of FMEA that takes into account possible intrusions into the system.[7] Since any vulnerability can result in a failure due to successful intrusion/attack, it is convenient to use IMECA to take into account failures caused by intrusions "using" system vulnerabilities.

Nowadays, FMEA and IMECA are not the only methods for complex systems failures and risks analysis. Authors in several related papers proved that IMECA techniques is one of the most convenient and clear in analysis of industrial Supervisory Control and Data Acquisition (SCADA) systems consisting of several hardware and specific software components with different architectures.[7] It was performed an analysis of failures and intrusions effects for software, hardware, stored data, users and a SCADA-based system as a whole.

3.1.1 XMECA Analysis

Modern investigations have shown that FME(D)A process consists of stages that are traditionally performed using "manual" analysis where experts have to process design documents, datasheets, standards etc. This leads to the time- and resources-consuming non-trivial work, where it is highly probable to make errors. To solve this problem, FMEDA automation procedure was suggested7 as the basis for integration of all existing FMEA-based techniques into XMEA that includes F(Failure)MEA, I(Intrusion)MEA, S(Software)MEA, D(Design)MEA, H(Hierarchy)MEA, etc. Such approach allows performing more comprehensive analysis.

3.1.2 Algorithm of IMECA Analysis

The algorithm, which is based on IMECA technique, intended for a comprehensive analysis and assessment of complex products/systems, comprises the following consequent steps [8]:

- identification of gaps within entire product life cycle model;

- application of IMECA technique to create IMECA-table for each of the identified gaps;
- creation of criticality matrix to assess the complex product/system.

The key idea of assessment is in the application of the process-product approach. Therefore, the life cycle model should include detailed representation of life cycle processes and appropriate (sub-)products. Then, it is possible to identify problems (or discrepancies) within the model, i.e. gaps.

Hence, each gap should be represented in a form of a formal description; such a formal description should be made for a set of discrepancies identified within the gap in a way that each identified gap can be represented by a single local IMECA table and each discrepancy inside the gap can be represented by a single row in that local IMECA table. In this way, complete traceability of life cycle processes, appropriate (sub-)products and inherent properties of corresponding discrepancies can be achieved. As a result, the number of local IMECA tables would correspond to the number of identified gaps, and the number of rows within each local IMECA table would correspond to the number of identified discrepancies within the appropriate gap. After completing the appropriate columns, for example on the basis of expert assessment, for all local IMECA tables, each gap is represented by a set of discrepancies with appropriate numerical values. Data within each row of local IMECA tables reveal, in explicit form, the weaknesses of the system aspect under assessment, e.g. intrusion probability and severity.

Further, in order to implement the approach, the following cases are possible, depending on the scope of the assessment:

1. Assessment of the system as a whole. Then, a set of particular IMECA tables (which represent all the identified gaps by a set of discrepancies) should be integrated into the single global IMECA table that reflects the whole system. In this case, each row of the global IMECA table forms the basis for creating a global criticality matrix, which can be used in cyber security assurance process.
2. Assessment of particular (sub-)systems within the system. In this case, it is possible to create an appropriate set of local criticality matrixes that correspond to certain (sub-)systems, based on a set of local IMECA tables.

So, the proposed gap-and-IMECA-based approach to assessment can be expressed in the consequence of actions listed below (see also Figure 5).

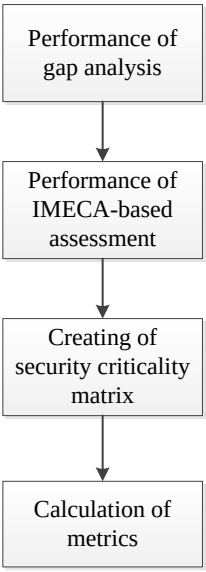

Figure 5: Proposed approach to assurance of cyber security.

Step 1. Performance of GA: identification of security gaps lists for all the components (or modules) of a system, being assessed, during each life cycle stage. Such lists should include both process gaps (in terms of discrepancies) and product cyber security gaps (in terms of vulnerabilities).

Step 2(a). Performance of IMECA-based assessment: determination of an appropriate set of vulnerabilities for each identified during GA process gap, security gap and possible scenarios to exploit the vulnerabilities. So, for each identified discrepancy or vulnerability, there should be created local IMECA table that reflects: attack mode, attack nature, attack cause, occurrence probability, effect severity, and type of effects. In this way, each gap is being represented by one or several rows in a local IMECA table.

Step 2(b). Assessment of appropriate columns (occurrence probability and effect severity) in each particular IMECA table, for example, on the basis of expert evaluation. Then, each row of such a local IMECA table represents security weaknesses, which should be analysed further in context of the whole system.

Step 3. Creating of security criticality matrix to analyse the cyber security risks of system components during different stages. Each row in local IMECA tables forms the basis for creation of security criticality matrix, which reveals the weaknesses of appropriate components in a visual form. The highest cyber security risk corresponds to the highest row in security criticality matrix.

Step 4. Calculation of metrics in order to choose the optimal set of applicable security countermeasures.

3.2 Construction of IMECA Table(s)

In order to illustrate IMECA-based assessment, we present results for some attacks modes possible during PBXs (see Table 1).

3.3 Risk Assessment

In order to analyse the cyber security risks, security criticality matrix should be created. In this way, the following scenarios are possible, which, in turn, depend on the scope of the assessment:

1. Assessment of the complex product/system as a whole: a set of particular IMECA tables (which represent all the identified gaps by a set of discrepancies) should be integrated into the single global IMECA table that reflects the whole system. In this case, each row of the global IMECA table forms the basis for creating a global criticality matrix.

2. Assessment of particular (sub-)systems within the complex product/system: it is possible to create an appropriate set of local criticality matrixes that correspond to certain (sub-)systems, based on a set of local IMECA tables.

In a case of second scenario, it is required to integrate the local criticality matrixes into a global one. The following rule can be used in this case:

$$e_{yz}^{G} = \bigcup_{k=1}^{n} e_{yz}^{L_k}, \tag{1}$$

where e^{G} is an element of the global criticality matrix, e^{L_k} is the corresponding element of the *k*-th local criticality matrix, and *n* is the total number of local criticality matrixes (equal to total number of gaps).

Moreover, the scales for the numerical values of a discrepancy (for example, its probability and severity) for local criticality matrixes can be set to the same value in order to eliminate the necessity of additional analysis during the creation of a global criticality matrix.

It is true for the both above scenarios that the highest risk of the selected assessment aspect corresponds to the highest row in the criticality matrix. In a case of independent gaps and discrepancies, the total risk of *R* can be calculated using the following equation:

Table 1: IMECA table for PBXs.

#	Threat	Vulnerability	Attack mode	Type of effects	Criticality		Counter-measure(s)
					Occurrence probability	Effect severity	
1	Tempera-ture rise	Inadequate air condition-ing/ cooling, envi-ronmental parameters monitoring	passive	Data losses, availability, integrity and confidentiality violation	low	moderate	Adequate air condition-ing/cooling, environmental parameters monitoring
2	Physical tampering	Inadequate physical se-curity, no se-curity-optical scans-checks	Active	Data losses	moderate	high	Proper physi-cal security, regular securi-ty scans-checks, optical checks
3	Intercept executive's voice com-munication	Inadequate physical se-curity, wrong setup	active	Data losses, availability, integrity and confidentiality violation	moderate	high	Proper physi-cal security, regular securi-ty scans-checks, optical checks, correct settings
4	Signaling analysis	Insecure set-tings-debug tools left in operation	active	Data losses, availability, integrity and confidentiality violation	low	low	Proper physi-cal security, regular securi-ty scans-checks, correct parameteriza-tion
5	IP hacking	Inadequate security in the IP part of the network	active	Data losses, confidentiality violation	moderate	moderate	IP network hardening
6	Silent monitor/ secretary monitor/ intrude/ duplex/ au-tomatic an-swer	Improper system pa-rameter-ization	active	Confidentiali-ty violation	moderate	moderate	Proper param-eterization of the system, se-curity checks
7	IVR hack-ing	Improper pa-rameteriza-tion	active	Data losses, confidentiality violation	moderate	moderate	Proper para-metrization of the system, se-curity checks

$$R = \sum_{i=1}^{n} \sum_{j=1}^{m} p_{ij} D_{ij} , \quad (2)$$

where *n* is the total number of gaps, *m* is the total number of rows in the IMECA table, *p* is the occurrence probability, and *D* is the corresponding damage.

Moreover, the criticality matrix can be extended to be *K*-dimensional (where $K>2$) that allows us to consider, for example, the amount of time required to implement the appropriate countermeasures for the assessed complex product/system.

For example, during the assessment of security, the prioritization of vulnerabilities identified on the basis of process-product approach, should be performed according to their criticality and severity, representing their corresponding stages in the cyber security assurance of the given system. The main goal of this step is to identify the most critical security problems within the given set. Prioritization may require the creation of a criticality matrix, where each vulnerability is represented within single rows. In such cases, it is possible to manage the security risks of the whole system via changing the positions of the appropriate rows within the matrix (the smallest row number in the matrix corresponds to the smallest risk of occurrence).

During the performance of GA, the identification of discrepancies (and the corresponding vulnerabilities in case of security assessment), can be implemented via separate detection/analysis of problems caused by human factors, techniques and tools, taking into account the influence of the development environment.

Then, after all identified vulnerabilities are prioritized; it is possible to assure security of the complex product/system by implementing of appropriate countermeasures. Such countermeasures should be selected on the basis of their effectiveness (also, in context of assured coverage), technical feasibility, and cost-effectiveness. But there is an inevitable trade-off between a set of identified vulnerabilities and a minimal number of appropriate countermeasures, which allows us to eliminate vulnerabilities or to make them difficult to be exploited by an adversary. The problem of choosing such appropriate countermeasures is an optimization problem and is still challenging.

4 Case Study and Training Activities

The proposed technique of private communications security assessment is a base of the training module which is developed in frameworks of the TEMPUS project SEREIN. One of the objectives of the project is to develop a few MSc-, PhD- and training modules and courses for students, lecturers, engineers and auditors in area of cyber security assessment and assurance, secure and resilient systems analysis and development.

Training part intended for study and getting of skills to apply different techniques and tools for analysis of industry computer and FPGA-based systems security, choice of countermeasures, support of certification processes for safety and security critical systems and so on. Training part of the project consists of three courses:

- CT1. The techniques and tools for networks security assessment and audit;
- CT2. Industry FPGA-based systems security;
- CT3. Security and resilience assurance cases.

One of the CT1 topics is dedicated to communication security, in particular, security of private communications. Described IMECA-based methodology and technique is a theoretical part of this topic. Training includes step by step learning of the technique:

- analysis of the communication system features in point of view security;
- specifying requirements to the systems taking into account national and international standards or industry guides;
- identification of vulnerabilities for communication;
- development of IMECA table;
- filling and analysis of criticality matrix considering acceptable risk;
- specification of countermeasures for communication system;
- preparation of analysis report.

To support assessment of the system a special tool was developed.[15] This and other tools are studied for cases considering different examples of private communications.

5 Conclusions

The assessment of private communications security and consequent assurance of such attribute is very important and challenging modern problem. This chapter discusses some problems related to assessment of security aspects of private communications on the basis of PBXs.

Proposed here main elements of the approach to cyber security assurance allows decreasing a probability of vulnerabilities exploitation and appearance of security weaknesses into PBXs. Thus, approach implies conducting of gap analysis, based on identification of all possible vulnerabilities, on the basis of product and life cycle processes, and their assessment via application of IMECA technique.

Also, there were presented case study of proposed technique implementation and described appropriate training experience in the scope of SEREIN project, in particular, training modules of the program. This module can be applied for different target groups.

Next steps can be devoted to collection of typical vulnerabilities to update appropriate database and to creation of automated service for PBX security assessment. The developed tool [15] can be integrated into this service.

References

1. Iosif Androulidakis, *PBX Security and Forensics: A Practical Approach* (Springer, 2013). https://doi.org/10.1007/978-1-4614-1656-2.

2. IEC 812, *Analysis Techniques for System Reliability – Procedure for Failure Modes and Effects Analysis (FMEA)* (Geneva: International Electrotechnical Commission, 1985).

3. Robyn R. Lutz, Guy G. Helmer, Michelle M. Moseman, David E. Statezni, and Stephen R. Tockey, "Safety Analysis of Requirements for a Product Family," Proceedings of the 3rd International Conference on Requirements Engineering (ICRE '98) (1998): 24-31. https://doi.org/10.1109/ICRE.1998.667805.

4. Iraj Elyasi Komari, Vyacheslav Kharchenko, Eugene Babeshko, Anatoliy Gorbenko, and Alexander Siora, "Extended Dependability Analysis of Information and Control Systems by FME(C)A-technique: Models, Procedures, Application," in *Fourth International Conference on Dependability of Computer Systems, 2009, DepCos-RELCOMEX'09*, 30 June - 2 July 2009, pp. 25-32. https://doi.org/10.1109/DepCoS-RELCOMEX.2009.13.

5. Anatoliy Gorbenko, Vyacheslav Kharchenko, Olga Tarasyuk, and Alexey Furmanov, "F(I)MEA-technique of Web Services Analysis and Dependability Ensuring," in *Rigorous Development of Complex Fault-Tolerant Systems*, Lecture Notes in Computer Science, vol. 4157 (2006), 153-167. https://doi.org/10.1007/11916246_8.

6. Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing* 1, no. 1 (2004): 11-33. https://doi.org/10.1109/TDSC.2004.2.

7. Eugene Babeshko, Vyacheslav Kharchenko, Anatoliy Gorbenko, "Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring," in *Third International Conference on Dependability of Computer Systems, DepCos-RELCOMEX'08*, 26-28 June 2008, pp. 309-315. https://doi.org/10.1109/DepCoS-RELCOMEX.2008.23.

8. Vyacheslav Kharchenko, Anton Andrashov, Vladimir Sklyar, Andriy Kovalenko, and Olexandr Siora, "Gap-and-IMECA-based Assessment of I&C Systems Cyber

Security," in *Advances in Intelligent and Soft Computing*, ed. J. Kacprzyk (Berlin Heidelberg: Springer, 2012), 149-164.

9. Iosif Androulidakis, "Detecting Cybercrime in Modern Telecommunication Systems," European Police College (CEPOL), Seminar 64/2010, Cyber Crime & High Tech (Athens: May 18-21, 2010).

10. Iosif Androulidakis, "Cybercrime in Fixed Telephony Systems," European Police College (CEPOL), Seminar 62/2011, High Tech & Cyber Crime (Brdo near Kranj, Slovenia: October 20, 2011).

11. Craig Pollard, "Telecom Fraud: The Cost of Doing Nothing Just Went Up," *Network Security*, vol. 2005, no. 2 (2005): 17-19. https://doi.org/10.1016/S1353-4858(05)00202-3.

12. Eric Luiijf and Marieke Klaver, "Insufficient Situational Awareness about Critical Infrastructures by Emergency Management," in *C3I for Crisis, Emergency and Consequence Management*, RTO-MP-IST-086 (Paris: RTO, 2009), paper # 10.

13. Communications Fraud Control Association, *Worldwide Telecom Fraud Survey* (2009).

14. SEREIN TEMPUS project website at http://serein.net.ua.

15. Oleg Illiashenko, Vyacheslav Kharchenko, and Myhailo Ahtyamov, "Security Assessment and Green Issues of FPGA-Based Information and Control Systems," in *Proceedings of the IEEE Conference Digital Technologies DT2013*, Žilina, Slovakia, 29-31 May 2013, pp.85-90. https://doi.org/10.1109/DT.2013.6566309.

About the Authors

Iosif ANDROULIDAKIS holds a BSc in Physics and a PhD and an MSc in Electronics for which he was awarded the Greek State's Scholarships Foundation outstanding performance prize. He has also attended a wealth of seminars, conferences and meetings regarding ICT technologies from companies and institutes such as Alcatel, Cisco, Intracom, Bell Labs, Symbian, Sun Microsystems, MD5, Encode, KPMG, AIT, GRNET, NCSR-Demokritos, FORTH, Onassis Foundation and others. He is a member of IEEE (Technical Committee on Security & Privacy) and ACM (Special Interest Group on Security Audit & Control) as well as editor in ETASR, IJNCM and JDCTA journals. He has also acted as a reviewer in many conferences and journals, as a Programme Committee member in 6 conferences and as a chairman in 4 conference sessions. Finally, he is a certified ISO9001:2000 (Quality Management System) and ISO27001:2005 (Information Security Management System) auditor and consultant. *E-mail*: sandro@noc.uoi.gr.

Vyacheslav KHARCHENKO is currently a Head of Centre for Safety Infrastructure-Oriented Research and Analysis (Ukraine), Doctor of Sciences, Professor, Academic of International Academy of Sciences of Applied Radio Electronics. His current research focuses on development of: multiversion systems theory; methods and means of assessment and ensuring for reliability, survivability, and functional safety of information control and processing systems; technologies for developing and assessment of dependable NPP systems, aerospace complexes, business-critical systems.
E-mail: v_s_kharchenko@ukr.net.

Andriy KOVALENKO is currently associate professor at Kharkiv National University of Radio Electronics (Ukraine), PhD. His current research focuses on issues of software engineering and quality assurance, security of safety-critical systems and features and problems of distributed and internet/intranet systems.
E-mail: andriy_kovalenko@yahoo.com.