Security in Transnational Interoperable PPDR Communications: Threats and Requirements

Ramon Ferrús, Oriol Sallent
Signal Theory and Communications Department
Universitat Politècnica de Catalunya (UPC)
Barcelona, Spain
[ferrus, sallent]@tsc.upc.edu

Cor Verkoelen, Frank Fransen
TS information Security
TNO
Den Haag, The netherlands
[cor.verkoelen, frank.fransen]@tno.nl

Jaakko Saijonmaa
Airbus Defence & Space OY
Finland
jaakko.saijonmaa@airbus.com

Claudia Olivieri
System Design Engineer
Selex ES
Genova, Italy
claudia.olivieri@selex-es.com

Michel Duits
Direktoratet for nødkommuikasjon
Nydalen allé 37A
0484 Oslo
michel.duits@dinkom.no

Anita Galin
MSB-Swedish Civil Contingencies Agency
SE 651 81 Karlstad, Sweden
Anita.galin@msb.se

Franco Pangallo, Debora Proietti Modi
Radio Mobile Department
Istituto Superiore delle Comunicazioni (ISCOM)
Rome, Italy
[franco.pangallo,debora.proiettimodi.ext]@mise.gov.it

***Abstract*— The relevance of cross border security operations has been identified as a priority at European level for a long time. A European network where Public Protection and Disaster Relief (PPDR) forces share communications processes and a legal framework would greatly enforce response to disaster recovery and security against crime. Nevertheless, uncertainty on costs, timescale and functionalities have slowed down the interconnection of PPDR networks across countries and limited the transnational cooperation of their PPDR forces so far. In this context, the European research project ISITEP is aimed at developing the legal, operational and technical framework to achieve a cost effective solution for PPDR interoperability across European countries. Inter alia, ISITEP project is specifying a new Inter-System-Interface (ISI) interface for the interconnection of current TETRA and TETRAPOL networks that can be deployed over Internet Protocol (IP) connectivity. This approach turns communications security as a central aspect to consider when deploying the new IP ISI protocol between PPDR national networks. Ensuring that threats to the interconnected communications systems and terminals are sufficiently and appropriately reduced by technical, procedural and environmental countermeasures is vital to realise the trusted and secure communication system needed for the pursued PPDR transnational cooperation activities. In this context, this paper describes the framework and methodology defined to carry out the development of the security requirements and provides a discussion on the undertaken security risk and vulnerability analysis.**

***Keywords*— Inter-System Interconnection; TETRA; TETRAPOL; Public Safety Communications; Emergency Services Communications; Threat, Risk, Vulnerability Analysis; Security Requirements**

I. INTRODUCTION

The Public Protection and Disaster Relief (PPDR) sector brings essential value to society by creating a stable and secure environment to maintain law and order and to protect

Article accepted for publication by IEEE.
DOI: 10.1109/ICT-DM.2015.7402043

For citation use the following:
R. Ferrús et al., "Security in transnational interoperable PPDR communications: Threats and requirements," 2015 2nd International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Rennes, 2015, pp. 88-95. doi: 10.1109/ICT-DM.2015.7402043. URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7402043&isnumber=7402014

the life and values of citizens. PPDR services such as law enforcement, firefighting, emergency medical services and disaster recovery services are pillars of our society organisation. The most important part of the PPDR work is done in the field. Therefore, radiocommunications are extremely important to PPDR organizations to the extent that PPDR communications are highly dependent upon it. Indeed, at times, radiocommunication is the only form of communications available [1].

In Europe, most countries have deployed national PPDR networks based mainly on TETRA and TETRAPOL technologies to serve the communications needs of the diverse PPDR organisations established at national level [2][3]. The use of a single, shared PPDR network at national level facilitates the cooperation between the diverse national PPDR agencies that can be provisioned with the proper coordination talk groups. However, transnational cooperation of PPDR agencies across European Union (EU) member states is still not solved as of today, being one of the reasons the lack of interconnection between the national PPDR networks in different countries. This lack of interconnection prevents the support of roaming services (commonly called migration services in PPDR terminology) so that PPDR teams displaced to a foreign country cannot keep using their communications equipment in the foreign area. The growth of international crime (e.g., drugs, human trafficking) requires joint police operations in the field in areas like cross-border pursuit of criminals, cross-border patrols and controls, etc. The need of cooperation is also growing in the last decade in natural calamities (e.g., flooding, earthquakes), disasters (e.g., bomb attacks, aircraft crashes, chemical nuclear alert) and generally for injured care and transportation, firefighting and support for civil protection. Since national resources are limited, and time is critical in disaster relief, international cooperation enables a greater effectiveness. Such strategy has been proving to be effective as for example between Norway and Sweden that are sharing cross border resources to combat fire or to transport patients. Effective interoperability may greatly reduce such damages if PPDR resources can rapidly operate in foreign areas. Investments needed to achieve transnational interoperability may be well repaid by the reduction of casualties and damages. In this context, the relevance of cross border security operations is already acknowledged at European level and identified as a priority (Schengen Agreements). In addition, according to the article 222 of the Treaty of Lisbon ("mutual solidarity"), the EU shall mobilize member states resources to assist other member states in case of terrorist attacks or in case of natural/man-made disasters. Specific groups of countries (e.g., France-Switzerland, Norway-Sweden, Sweden-Germany, Belgium-Netherlands) are recently cooperating to address communications interoperability for PPDR cross-border operations [3]. Nevertheless, without a harmonised international solution, interoperability will be possible only in localised areas, thus vanishing the benefits of an extensive cooperation. In addition, there is a growing demand of standard interoperability solutions by industry, since new international tenders require multivendor interoperability to avoid single source risks.

In this context, the European research project ISITEP [4] is an ambitious initiative aimed at developing standard operational procedures, technology and legal agreements to achieve a cost effective solution for PPDR interoperability across European countries. End users participating in ISITEP have driven the requirement to guarantee legal, operational and technical coherence. ISITEP will demonstrate full radio interface migration for PPDR resources in diverse scenarios such as Norway-Sweden border, Germany-Belgium-Holland border and Swiss-French border. One of the key outputs expected from the ISITEP project is a new Inter-System-Interface (ISI) interface for the interconnection of TETRA networks based on the evolution of the current ETSI standard for TETRA ISI [5] so that it can be deployed over an Internet Protocol (IP) transport network.

The new interface is referred to as IP ISI and, in addition to enabling the interconnection of TETRA networks, it is intended to be used also for the interconnection between TETRA and TETRAPOL networks and between TETRAPOL networks. While the ultimate goal of the ISITEP project by pursuing the development of the IP ISI is to facilitate the interconnection of the different national TETRA and TETRAPOL PPDR networks deployed across European countries, the consolidation of such IP ISI is expected to facilitate the integration of current narrowband PPDR networks with the forthcoming all-IP PPDR service delivery platforms as well. Indeed, the new IP ISI protocol is based on the Session Initiation Protocol (SIP), which is the currently most used standard for Voice over IP (VoIP) communications. The approach adopted in ISITEP is to allow that the already standardised TETRA ISI Additional Network Features (ANFs) can be exchanged through SIP messages and use the Real-time Transport Protocol (RTP) for the voice traffic encoded with the corresponding codecs. A simplified view of the IP ISI protocol stack is depicted in Figure 1.

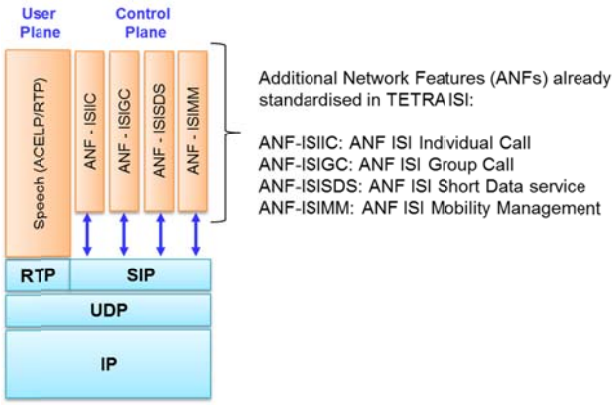

Fig. 1. IP-based Inter-System Interface (IP ISI) for the interconnection of TETRA and TETRAPOL networks

A central aspect of the ISITEP framework for inter-system interoperability between TETRA and TETRAPOL networks based on the new IP ISI protocol is communications security. Ensuring that threats to the interconnected communications systems and terminals are sufficiently and appropriately reduced by technical, procedural and environmental countermeasures is vital to realise the trusted and secure communication system needed for the pursued PPDR

transnational cooperation activities. In this context, this paper describes the overall framework and methodology defined to carry out the development of the security requirements and provides a discussion on the undertaken security risk and vulnerability analysis and its associated security requirements. The focus is placed on the security threats stemming from the use of third-party IP-based international interconnection links between national PPDR networks as well as those resulting from the exposure of network services and features through the ISI interface that can be threated from other interconnected national networks if those are compromised. To this end, the paper is organised as follows. Section II outlines the system's components and the participating entities or subjects that are relevant for the definition of the security requirements. The adopted framework and methodology for security risk and vulnerability analysis is presented in Section III. On this basis, Section IV centres on the analysis of the potential threats stemming from the interconnection infrastructures and from the scenario that the interconnected network has been compromised. An overview of the risk assessment of the identified threats is provided in Section V, together with the main security requirements that have been established. Finally, conclusions are summarized in Section VI.

II. System Overview

ISITEP system proposes the interconnection of a number of TETRA/TETRAPOL networks by means of ISI Gateways (different ISI Gateways are to be developed to cover the use of TETRA and TETRAPOL technologies as well as the use of legacy TETRA ISI [5] by some networks). A general preliminary assumption is that the interconnected end-points (i.e., the TETRA/TETRAPOL networks) are trusted but that the linking network is itself untrusted. Therefore, three separate security zones can be distinguished from a given PPDR network operator point of view and depending on the operational control of the network operator, the location of the specific network element and their connectivity to other network elements. These three zones are: a Trusted Zone, where network operator or service provider's elements and systems reside; a Trusted But Vulnerable Zone, where network elements are operated by the network operator or service provider; but are not necessarily fully controlled by that network operator or service provider or might communicate with Un-trusted Zone elements; and the Un-trusted Zone, which is the zone which includes the network elements belonging to other network operators, service provider or end customers. This trust model is consistent with the one proposed by i3 Forum [6] for carriers and service providers involved in international VoIP interconnections.

As shown in Figure 2, all the equipment that form part of the TETRA/TETRAPOL Switching and Management Infrastructure (SwMI), such as base stations, switching nodes and network management elements, will be located in the Trusted Zone of a given operator. These elements and systems never communicate directly with external domains such as the networks of interconnected partners. As to the placement of the ISI Gateway, a preliminary assumption is that it will also reside in the Trusted Zone of each operator. It's worth noting that it should not be assumed that because an element is in the Trusted Zone it is secure: Trusted Zone elements should be also be protected by a combination of various methods. For example elements may be protected by physical security, system hardening, use of authenticated and encrypted signalling or a separated logical network for communication within the Trusted Zone and with network elements in the Trusted But Vulnerable Zone.

In ISITEP it is proposed to develop a Security Gateway (SEG) to provide enhanced protection to traffic and signalling information running on the interfaces that cross PPDR network operator boundaries. The SEG will be located at Trusted But Vulnerable Zone. The main role of this element is to protect the elements in the Trusted Zone from the security attacks originated in the Un-trusted Zone. In particular, ISITEP security framework grounded on security gateways shall solve two main issues: provide confidentiality and integrity of traffic exchanged among networks; and, prevention of intrusions into the national networks. In the context of VoIP interconnections, the elements equivalent to the SEG are referred to as Network Border Elements or Border Function elements [6].

ISITEP system will allow for the roaming of terminals across networks. Therefore, as an example, terminal #2 whose home network is Network B in Figure 2, will be able to get access to communication services through Network A, which will serve as a visited network. This demands the utilisation and/or development of new security features in the radio interface as well as in the ISI over IP protocol to be developed between the networks. The security, the privacy and the integrity of the existing systems will be maintained while sharing the needed data for interoperability.

TETRA Encryption Algorithms (TEA) can be used to protect information over the air interface, which are a standard for European public safety (i.e., TEA 2) and TETRAPOL security. In TETRA, security is mainly provided through Air Interface Encryption (AIE) and/or through End to End encryption (E2EE). The first mechanism is interoperable across Europe while E2EE does not allow complete interoperability across countries since E2EE is often classified or national specific. On the other hand, according to end users, AIE is suitable for all joint operations apart from Special Forces, which require extra security measures such as E2EE. TETRAPOL has a similar national specific approach but there is no way to manage security configuration from outside the TETRAPOL terminal for security reasons.

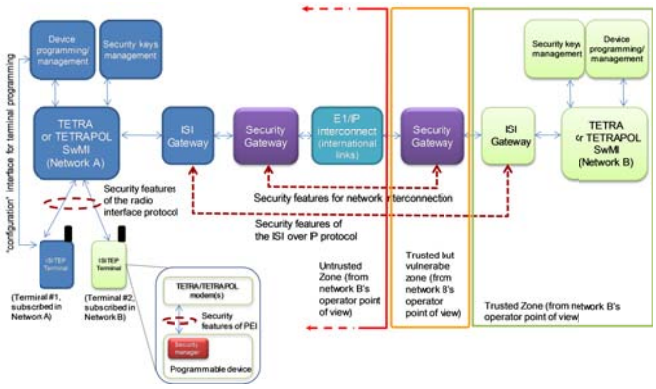

Fig. 2. ISITEP system overview for the development of security requirements

In addition to supporting the migration of legacy TETRA and TETRAPOL terminals, ISITEP is defining an enhanced user terminal that consists of a programmable platform (a smartphone or a Tablet PC) with both TETRA and TETRAPOL modems. ISITEP enhanced terminals are expected to rely on a terminal control interface (e.g. PEI for TETRA and PEI-equivalent for TETRAPOL) in order to interconnect the TETRA/TETRAPOL communication modem(s) with the programmable device that host the applications. As such, security features may also be required to protect such a control interface. ISITEP terminals might also embed a Security Manager to configure existing security parameters according to counterparts and the associated security capability. Additional elements of the TETRA/TETRAPOL systems that are relevant for the security analysis are the elements used to manage the network security keys and the elements used to configure/program terminals.

ISITEP players considered for the analysis of security threats and requirements are those already present in PPDR TETRA and TETRAPOL systems (e.g., PPDR network operators, terminal and system manufacturers, PPDR personnel) plus the ones resulting from the specifics of cross-border, multinational PPDR operations and the use of international connectivity services across nation PPDR networks (e.g., transport or transit services carrier). In addition, a player intruder is considered, which is the role of a party who attempts to breach the confidentiality, integrity or availability of the communication services, or who otherwise attempts to abuse the system in order to compromise services or defraud users, home environments, serving networks or any other party. An intruder may, for example, attempt to eavesdrop on user traffic, signalling data and/or control data, or attempt to masquerade as a legitimate party in the use, provision or management of communication services.

III. Framework and Methodology Used For Security Risk and Vulnerability Analysis

The methodology adopted for the security risk and vulnerability analysis of the ISITEP solution is in line with the main guidelines provided in ETSI Technical Report ETR 332 [7] for security requirements capture. After the formulation of general objectives and identification of the system components, a threat analysis is conducted. A security threat is defined as a potential violation of security. While it is possible to classify security threats in many different ways (e.g., ITU-T Recommendation X.805, 3GPP TR 33.805), the categorisation followed in ISITEP is structured around the central functions enabled by the ISITEP solution (i.e., roaming support, service interworking across the national networks and use of bi-technology ISITEP terminals), yielding to the 10 threat categories described in Table I.

TABLE I. Threat categories considered in the assessment

Threat category	Comment
Threats on visiting users authentication	*Threats associated with the use of current PPDR network security features with roaming terminals*
Threats on air interface encryption	
Threats on the use of disable/enable functionality	
Threats on the use of end-to-end encryption	
Threats from the interconnection infrastructure to a national infrastructure	*Threats associated with the use of third-party international interconnection links between national PPDR networks*
Threats from mismatching security requirements between roaming terminals and visited networks	*Threats associated with the use of terminals in visited networks that may not be subject to the same security standards*
Threats from the interconnected networks	*Threats associated to the exposure of network services and features through the ISI interface that can be threated from other interconnected national networks if those are compromised.*
Threats from exposed interfaces within ISITEP bi-technology terminals	*Threats associated with the use of wireless interfaces for the implementation of the bi-technology ISITEP terminals*
Threats concerning PPDR users' data privacy	*Threats associated with privacy of data exchanges in the communications or gathered/collected in networks. A distinction is done between privacy of the end-users (i.e. first responders) and privacy of citizens who may be the subject of the communication over the PPDR communication system.*
Threats concerning citizens' data privacy	

For each threat category, the potential threats and the kind of attacks that are possible to realise the threat have been addressed. Considered threats belong to one of the following groups [8]: Interception/Eavesdropping; Masquerade ("spoofing"); Loss or corruption of information; Unauthorized access; Forgery; Repudiation; and Denial of service (DoS).

After the identification of the threats, a qualitative risk assessment has been conducted and security gaps identified. The risk assessment has ended up with a priority list, of the identified threats or group of threats, stating which ones are to be considered more severe, more important or more costly than others. Finally, security requirements have been formulated based on the results of the risk assessment for each of the threat categories in Table I.

IV. Threats Assessment from Interconnection Infrastructures and Interconnected Networks

A. Threats from the interconnection infrastructure

The TETRA/TETRAPOL standards do not address the security risks introduced by the interconnection of TETRA or TETRAPOL networks using an open IP interconnection infrastructure. To identify the new threats associated with the deployment of the IP ISI a differentiation can be made between (see Figure 3): (1) Network layer threats targeted at the PPDR network and/or SEG; (2) Network layer threats targeted at the interconnection infrastructure; (3) Application layer threats originating from a legitimate interconnected TETRA network (application layer in this context should be seen as threats targeted at the signalling used by interconnected PPDR networks); (4) and Application layer threats originating from a rogue (simulated) PPDR network. Threats that fall within category (3) are described in next Section IV.B

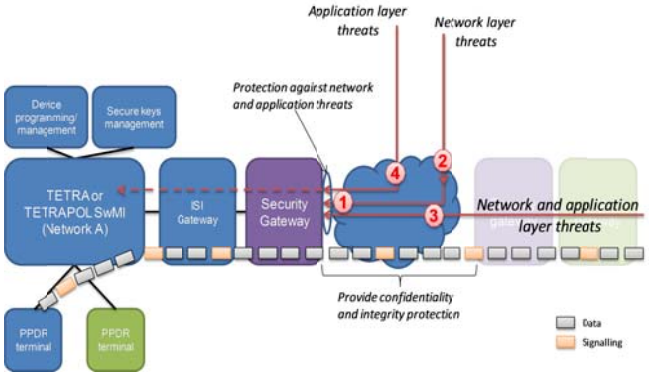

Fig. 3. Threats from the interconnection infrastructure

Threats targeted at the application layer require application layer knowledge (e.g., ETSI 300 392-3-5 ANF Mobility Management services and messages). This knowledge of the application layer, required to implement the security functionality, may be added to the SEG or the ISI Gateway. The type of services implemented/required at the ISI interface influence the type of (and impact of the) threats. For the identification of the threats and the classification of the impact no specific assumptions have been made on the available services in an initial stage.

Furthermore, whether the security measures should be implemented at the SEG or the ISI gateway depends on some architectural aspects/choices that have to be made. For instance, should signalling/application knowledge be added to the SEG which in principle only should prevent network layer attacks? Secondly, if packet inspection is required traffic may not be encrypted at the SEG. During the development of the security architecture these aspects must be taken into consideration.

For the identification of threats the system player intruder is taken as a starting point. Other system players may also introduce threats, e.g. a non-secure development process of TETRA systems may introduce vulnerabilities that can be exploited during deployment. However, this kind of threats (insecure development process) may not be solved by the placement of a SEG and should be addressed within the agreements between the different system players. The identification of the threats will only address those threats in which the intruder is involved and with a technically characteristic which may be exploited during the operational phase of the TETRA ISI.

Based on the above considerations, the following threats have been identified:

- *[T1] Eavesdropping signalling/management/data traffic communicated over the interconnection infrastructure.* Examples are TETRA network authentication messages, TETRA terminal authentication messages, signalling/management traffic for the purpose of TETRA terminal management (e.g., mobility management), ISITEP terminal key management traffic (e.g., session authentication keys) and TETRA terminal traffic (e.g., voice data and/or short data messages) communicated over interconnection infrastructure.
- *[T2] Manipulation of signalling/management/data traffic communicated over the interconnection infrastructure.* Examples are replay of previously captured TETRA network authentication messages with the aim of setting-up a connection between a legitimate and a rogue TETRA network, disrupting active connections and/or spoofing an authenticated TETRA terminal. Also replay of previously captured TETRA terminal management traffic with the aim of e.g., manipulating the group membership as well as replay of previously captured TETRA terminal data (e.g. voice) with the aim of confusing the active TETRA terminal users. Other possible threats are the modification of TETRA terminal data (e.g. short data messages) with the aim of confusing the active TETRA terminal users (requires a Man-in-the-Middle (MitM) attack) and the modification (and forwarding) of TETRA network authentication messages communicated over the interconnection infrastructure to establishing a MitM situation.
- *[T3] DoS to application layer functions.* Examples are the termination of existing voice calls by injecting falsified signalling messages from interconnected infrastructure, the exclusion of ISITEP terminals by injecting falsified disable messages from interconnection infrastructure, the overloading TETRA SwMI systems by flooding these systems with falsified/captured messages from the interconnection infrastructure and the deletion of e.g. group membership of a TETRA terminal via unauthorized access to databases through the SEG.
- *[T4] Unauthorised access to TETRA system functions and data from the interconnection infrastructure.* This includes unauthorized access to SwMI components (e.g. authentication server) from the interconnection infrastructure via the SEG, unauthorized access to data stored on SwMI components due to erroneous Access Control Lists (ACLs) implemented on the SEG and unauthorized deletion of Call Detail Records (CDRs) within the SwMI via unauthorized access through SEG.
- *[T5] Eavesdropping network layer signalling (e.g. SEG signalling) communicated over the interconnection infrastructure.* This includes eavesdropping signalling/management traffic (e.g., key management exchanges) between SEGs for the purpose of establishing a secure interconnection, eavesdropping network authentication messages between the SEG and interconnection infrastructure components (e.g., authentication messages of 802.1AE between SEG and ISP uplink router) and eavesdropping key management traffic exchanged between the SEG and the interconnection infrastructure components.
- *[T6] Manipulation of network layer signalling from the interconnection infrastructure.* This includes replay of

previously captured signalling/management traffic between SEGs with the aim of setting-up a rogue connection with the SEG.

- *[T7] DoS to network layer functions from the interconnection infrastructure.* This includes DoS attacks targeted at the SEG such as: (1) bandwidth overload of the SEG by sending huge amount of non-authenticated/authorized packets; (2) resource overload of the SEG by e.g. setting up a huge amount of legitimate connections (TCP connections); and (3) processing overload of the SEG by e.g. sending a huge amount of packets that must be inspected / filtered by the SEG (authentication requests). This also includes influencing routing from interconnected TETRA or TETRAPOL network of application/network signalling/management/data information towards unauthorized destinations or non-existing destinations (black-hole routing).

- *[T8] Unauthorised access to SEG system/functions and data from interconnected infrastructure.* This includes unauthorized access to the SEG or its management interface through the interconnection infrastructure. Also includes unauthorized access to data stored on SEG due to erroneous ACLs and the unauthorized deletion of loggings stored on the SEG via interconnection infrastructure.

- *[T9] Unauthorised access to network layer functions from home SwMI.* This includes unauthorized access to the SEG or its management interface from the home SwMI as well as unauthorized deletion of loggings stored on the SEG via home SwMI.

B. *Threats from the interconnected networks*

Currently each nation (or network operator) is responsible for the security of its own PPDR network. When PPDR networks are interconnected, a PPDR network is opened for attacks from the other PPDR networks (e.g., a DoS attack to one network or its elements, not security hardened, might also have effects on the other interconnected networks). That is, if one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other system. Threats from interconnected networks could arise from, e.g., security breaches intentionally exploited by attackers in a remote network as well as from (un)intentional misuse and/or wrong configurations on the operation of the ISI services from the interconnected network. Since the security levels may differ per PPDR network (and per country), it is currently not clear what measures have been implemented and what security guarantees can be given. Therefore the security measures implemented at the border of the 'own' PPDR network should consider all connections, whether these are set-up from the interconnection network of a seemingly legitimate PPDR network, as 'untrusted'.

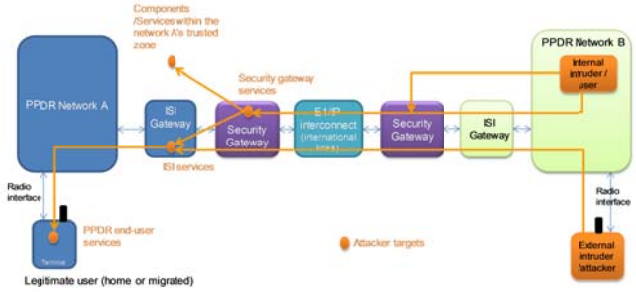

Fig. 4. Threats from within national infrastructure to other national infrastructures

The targets of the potential threats / attacks and the location of the intruders / attackers is depicted in Figure 4 for a general case that considers a (compromised) PPDR network (Network B) that could pose some security risks to an interconnected PPDR network (Network A). As shown in the figure, threats from within interconnected PPDR networks may be originated from:

- External intruders / attackers to the remote interconnected PPDR network (e.g., malicious users/ terminals in one country that may try to misuse or disturb the services of other interconnected networks such as blocking use of the ISI interconnection and also harming communications in the other country).

- Internal intruders / users within the remote interconnected PPDR network (e.g., disgruntled employee, malicious 3rd party with remote access).

Attacks may be targeted at:

- SEG services / functions that protect the PPDR network from the non-trusted zone (i.e., network layer threats). Compromising the security protection of the SEG might also expose to attacks to any component / equipment / service within the trusted zone reachable from the SEG (e.g., access to file systems, databases, access to network remote administration/management services, etc.).

- PPDR network services provided by the interconnected network though the ISI interface (i.e., ISI services). These attacks would be based on a non-legitimate use of application layer signalling originated in the (compromised) remote interconnected PPDR network.

- PPDR users / terminals being served by the attacked network (i.e., PPDR end-user services). Both home and migrating users / terminals could be targeted. These attacks would be based on a non-legitimate use of application layer signalling originated in the (compromised) remote interconnected PPDR network.

Based on the previous classification, the following threats have been identified:

- *[T10] Unauthorised access / DoS / Manipulation to SEG functions by internal intruders / users from a remote PPDR network.* This includes unauthorized access to the SEG functions or its management interfaces from within

Network B, unauthorized deletion/corruption of data/loggings stored on the SEG from Network B, manipulation (e.g., deletion) of security associations from (compromised) trusted peer SEG, resource overload of the SEG. Also includes influencing routing of application layer signalling at the SEG, preventing correct behaviour and thus impacting services, and unauthorized access to internal network services within the trusted zone of Network A via the SEG (e.g., access to file systems, databases, access to network remote administration/management services, etc.).

- *[T11] DoS / Manipulation as a result of a non-legitimate use of ISI interface signalling by internal intruders /users from a remote PPDR network.* This includes the establishment/manipulation/termination of voice, supplementary and data services (SDS, Status) (e.g., flooding of the ISI and the Network A by a huge amount of SDS messages that are send across the ISI from Network B), manipulation of mobility management signalling (e.g., fake registration signalling) and disabling of ISITEP terminals by fake disabling messages from interconnected TETRA or TETRAPOL network. Also includes DoS attack by overloading authentication service and/or signalling capacity of the ISI gateway with fake migration/authentication requests from the remote PPDR network, influencing (existing) calls by spoofing 'emergency calls' (emergency calls have a higher priority and may therefore influence existing (or new) calls that are/will be established over the ISI and unspecified behaviour by the ISI gateway by non-specified ISI packets sent from the interconnected Network B towards the ISI gateway of Network A.
- *[T12] DoS / Manipulation as a result of a non-legitimate use of ISI interface signalling originated by external intruders / attackers from a remote PPDR network. This includes the e*stablishment/manipulation/termination of voice, supplementary and data services (SDS, Status) to terminals connected in the PPDR Network A from external attackers in the remote interconnected PPDR Network B. Also includes DoS by overloading authentication service and/or signalling capacity of the ISI gateway with fake migration/authentication requests from malicious mobile stations attached to the remote PPDR network and unauthorized (unnecessary) activation of international call groups from the interconnected network by using a malicious mobile station in the interconnected Network B.

V. RISK ANALYSIS AND REQUIREMENTS

Based on the framework provided in [9], the occurrence/likelihood and impact of the above identified threats have been qualitatively assessed, leading to the classification provided in Table II. The occurrence likelihood of a threat is estimated as Unlikely (U), Possible (P), and Likely (L). On the other hand, the impact of a threat is estimated as: Low (L) impact, Medium (M) impact, and High (H) impact. The combination of occurrence likelihood and impact value gives the risk that serves as a measurement for the risk that the concerned management function is compromised. Three risk categories are distinguished: Minor (Mi) risk, Major (Ma) risk, and Critical (C) risk. Minor risks arise, if either no essential assets are concerned, or the respective attack is unlikely. Major risks are represented by threats on relevant assets that are likely to occur, even if their impact is less fatal. Critical risks arise when the primary interests of the providers/subscribers are threatened and when a potential attacker's effort to harm these interests is not high.

TABLE II. RESULTS OF THE RISK ANALYSIS AND SECURITY REQUIREMENTS ESTABLISHED PER THREAT

Treat(s)	Occurrence	Impact	Risk	Requirements
T1	P	H	C	R1,R2
T2	P	M	Ma	R2
T3	L	H	C	R2, R5, R7
T4	L	H	C	R2, R3, R4, R5
T5	L	M	C	R6
T6	L	M	C	R6, R8
T7	L	M	C	R5, R7
T8	L	H	C	R8, R9
T9	U	M	Mi	R8, R9, R10
T10	U	H	Mi	R11, R12, R13, R14, R15, R16, R17, R18
T11	U	H	Mi	R15, R16, R17, R18, R19
T12	P	M	Ma	R15, R16, R19, R20, R21, R22

The following requirements have been established:

- R1. Minimum security requirements on the IP interconnection service shall be established.
- R2. ISI control and data plane flows between the two interconnection points in each national network shall be protected from violation of confidentiality, violation of integrity and unauthorised access from the interconnection infrastructure. The protection of the interconnection link should make use of encryption devices at both ends.
- R3. PPDR operator's interconnection points must offer the possibility to filter incoming traffic based on pre-defined policies which guarantees that only legitimate traffic is forwarded to the SwMI.
- R4. It shall be possible to statically and dynamically control which other PPDR operators can access one PPDR operator's network interconnection point.
- R5. The SEG should be able to send alarms to the PPDR operator in case there is a security incident.
- R6. The key management of the encryption devices shall be secure. This is under the responsibility of the operators of the two interconnected networks.
- R7. PPDR operator's interconnection points must offer protection against (D)DoS attacks (e.g. attacks coming from unknown/untrusted sources, volume-based attacks), discarding the packets.

- R8. PPDR operator's network interconnection points shall have recovery mechanisms so that interconnection link can be restored in a timely fashion after any attacks or security issues.
- R9. Stripping/hardening security features shall be implemented in SEG.
- R10. Access to internal interfaces and management services on the SEG shall be protected within the PPDR network.
- R11. PPDR operator's interconnection points must offer protection against (D)DoS attacks from (compromised) interconnected networks (e.g. attacks coming from unknown/untrusted sources, volume-based attacks), discarding the packets.
- R12. It shall be possible to statically and dynamically control which other PPDR operators can access one PPDR operator's network interconnection point.
- R13. PPDR operator's network interconnection points shall have recovery mechanisms so that interconnection link can be restored in a timely fashion after any attacks or security issues.
- R14. PPDR operator's interconnection points must offer the possibility to filter incoming traffic based on pre-defined policies which guarantees that only legitimate traffic is forwarded to the SwMI.
- R15. PPDR operator's interconnection points must offer the ability to monitor and filter traffic (network and application data) received from interconnected PPDR networks, and identify suspicious/abnormal traffic that may lead to e.g. DoS.
- R16. PPDR operator's interconnection points must offer the ability to report on the effectiveness of the security measures taken by the SEG and/ or ISI Gateway (e.g. # of detected incidents, response time after detection of abnormal traffic, send alarms to the PPDR operator in case there is a security incident, etc.).
- R17. PPDR network operators should agree upon and establish (proportional) (multi-lateral / bilateral) security policies / procedures to be enforced in their networks. Validation / Assurance means that agreed security policies / procedures are applied in the interconnected network should be in place.
- R18. Minimum security assurance specifications and security certifications of the interconnection components to be deployed (SEGs, ISI Gateways) should be agreed and enforced by network operators.
- R19. Upon the detection of a security attack through ISI services, it should be possible for the operator to turn down ISI services in a quick and controlled manner. A procedure for risk evaluation and deactivation of ISI connectivity should be established among PPDR operators and PPDR agencies.
- R20. The management and protection of the authentication process against DoS attacks in a PPDR network (e.g., overloading of the authentication server with multiple requests from spoof terminals) shall also consider counter measures to avoid overloading the remote ISI gateway and SwMI in case of authentication requests involving migrated terminals.
- R21. Access to ISI services (e.g., group services, SDS services) should be controlled by every serving network through the proper management of user service rights. Pre-defining rights of visiting users shall be allowed.
- R22. Features and procedures to track stolen / lost terminals and disabling them when migrated in a visited network shall be supported

VI. CONCLUSIONS

Communications security is a central aspect of the ISITEP framework for inter-system interoperability between TETRA and TETRAPOL networks. Ensuring that threats to the interconnected communications systems and terminals are sufficiently and appropriately reduced by technical, procedural and environmental countermeasures is vital to realise the trusted and secure communication system needed for the pursued PPDR transnational cooperation activities.

This paper has provided an overview of the security risk and vulnerability analysis associated with the new functions brought by the ISITEP system. The assessment has focused on those security threats that are relevant to the new communications capabilities in terms of service interworking across multiple national networks and terminal roaming.

The security requirements described in this paper are being considered as an input for the development of other components of the ISITEP project. In particular, security requirements impact on the definition of the secure network solution to national security infrastructure at PPDR national network, the definition of procedures for new national network interconnections and for roaming activation, and guiding the security at network interface, gateway and terminal level.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) THEME [SEC-2012.5.3-4]-[Global solution for interoperability between first responder communication systems - Integration Project] - "Inter System Interoperability for Tetra-TetraPol Networks" under grant agreement n° [312484]-[ISITEP].

REFERENCES

[1] G. Baldini, R. Ferrús, O. Sallent, Paul Hirst, Serge Delmas, Rafał Pisz, "The evolution of Public Safety Communications in Europe: the results from the FP7 HELP project", ETSI Reconfigurable Radio Systems Workshop, Sophia Antipolis, France, 12 December 2012

[2] Simon Forge, Robert Horvitz and Colin Blackman, "Study on use of commercial mobile networks and equipment for "mission-critical" high-speed broadband communications in specific sectors", Final Report, December 2014. Available online at https://ec.europa.eu/digital-agenda/en/news/use-commercial-mobile-networks-and-equipment-mission-critical-high-speed-broadband

[3] Becchetti, C.; Frosali, F.; Lezaack, E., "Transnational Interoperability: A System Framework for Public Protection and Disaster Relief," Vehicular Technology Magazine, IEEE , vol.8, no.2, pp.46,54, June 2013

[4] EU Research Project on “Inter-system interoperablity for TETRA-TETRAPOL networks (ISITEP)”. Project website: http://isitep.eu/

[5] ETSI EN 300 392-3-1, “TETRA V+D ISI General Design”, V1.3.1, August 2010

[6] i3 Forum, “Security for IP Interconnections (Release 1.0)”, May 2011

[7] ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture", November 1996

[8] ETSI TS 102 165-1 V4.2.3 (2011-03), Technical Specification Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); “Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis”

[9] ETSI TR 102 512 V1.1.1, “Security requirements analysis for modulation enhancements to TETRA”, August 2006