TECHNICAL SCIENCES
Abbrev.: Techn. Sc., No 15(1), Y 2012

SEAMLESS COMMUNICATION FOR CRISIS MANAGEMENT

***Wojciech Wojciechowicz*[1,13], *Jacques Fournier*[2], *Miroslav Konecny*[3], *Stefan Vanya*[3], *John Stoodley*[4], *Phil Entwisle*[4], *Daniel M. Hein*[5], *Aurel Machalek*[6], *Apostolos Fournaris*[7], *Mikel Uriarte*[8], *Oscar Lopez*[8], *Shaun O'Neill*[9], *Hans Bradl*[10], *Zoltan Balogh*[11], *Emil Gatial*[11], *Ladislav Hluchy*[11], *Tomasz Mirosław*[12], *Jan Zych*[1]**

[1] ITTI sp. z o.o., [2] CEA-LETI Minatec, Gardanne, France, [3] Ardaco a.s., [4] QinetiQ Ltd., [5] Institute of Applied Information Processing and Communication, Graz University of Technology, [6] University of Luxembourg, [7] University of Patras, [8] NEXTEL S.A., [9] British Association of Public Salety Communications Officials, [10] Infineon Technologies AG, [11] Institute of Informatics, Slovak Academy of Sciences, [12] BUMAR sp. z o.o., [13] Institute of Computing Science, Poznań University of Technology

Key words: SECRICOM, Seamless communication, crisis management, Multi Bearer Router (MBR), Push To Talk (PTT), SECRICOM Silentel, Secure Docking Module (SDM), Secure Agent Infrastructure (SAI), Communication Security Monitoring and Control Centre (CSMCC), Seventh Framework Programme (FP7), Trusted Computing.

Abstract

SECRICOM – Seamless Communication for crisis management was a research and development project, realised within the Seventh Framework Programme (7PR). The aim of this project was to develop reference solution based on existing infrastructure, which will be capable to ensure secure and efficient communication for operational crisis management. The project was an answer to the European Security Research Advisory Board (ESRAB) report, in which key requirements for a communication system have been stated.

Secure and efficient communication system is a necessity for effective crisis management. It is assumed that such infrastructure may significantly increase rescue actions effectiveness. Currently, however, there are cases when various services (not only domestically but also internationally) use heterogeneous telecommunications systems. It results in the lack of or significant problems with mutual communication. Such situation is often considered problematic and posing a threat to the effective rescue actions.

For this purpose, a secure and multi-platform communications system (SECRICOM Silentel) has been developed within SECRICOM project. The Multi Bearer Router (MBR) optimise the backbone network by the use of multiple bearers and dynamic adjustment to various conditions. Advance mechanisms enhancing end-user devices' security – Secure Docking Module (SDM) – have been developed using Trusting Computing principles. Secure Agent Infrastructure (SAI) ensures – based on agents' infrastructure – secure access to distributed data. The system is supplemented with network monitoring platform – Communication Security Monitoring and Control Centre.

The SECRICOM project resulted in a communication system prototype, which is capable of ensuring interoperability as well as secure and efficient communication for operational crisis management. This system has been demonstrated on several occasions to the stakeholders.

PONADSYSTEMOWA ŁĄCZNOŚĆ DO ZARZĄDZANIA KRYZYSOWEGO

***Wojciech Wojciechowicz*[1,13], *Jacques Fournier*[2], *Miroslav Konecny*[3], *Stefan Vanya*[3], *John Stoodley*[4], *Phil Entwisle*[4], *Daniel Hein*[5], *Aurel Machalek*[6], *Apostolos Fournaris*[7], *Mikel Uriarte*[8], *Oscar Lopez*[8], *Shaun O'Neill*[9], *Hans Bradl*[10], *Zoltan Balogh*[11], *Emil Gatial*[11], *Ladislav Hluchy*[11], *Tomasz Mirosław*[12], *Jan Zych*[1]**

[1] ITTI sp. z o.o., [2] CEA-LETI Minatec, Gardanne, France, [3] Ardaco s.s., [4] QinetiQ Ltd., [5] Institute of Applied Information Processing and Communication, Graz University of Technology, [6] University of Luxembourg, [7] University of Patras, [8] NEXTEL S.A., [9] British Association of Public Salety Communications Officials, [10] Infineon Technologies AG, [11] Institute of Informatics, Slovak Academy of Sciences, [12] BUMAR sp. z o.o., [13] Instytut Informatyki, Politechnika Poznańska

Słowa kluczowe: SECRICOM, „bezszwowa" komunikacja, zarządzanie kryzysowe, Multi Bearer Router (MBR), Push To Talk (PTT), SECRICOM Silentel, Secure Docking Module (SDM), Secure Agent Infrastructure (SAI), Communication Security Monitoring and Control Centre (CSMCC), siódmy program ramowy (7PR), Trusted Computing.

Abstrakt

SECRICOM – Seamless Communication for crisis management to projekt badawczo-rozwojowy, który został zrealizowany w ramach siódmego programu ramowego (7PR). Celem projektu było wypracowanie bezpiecznej i, co ważne, bazującej na istniejącej infrastrukturze platformy komunikacyjnej do operacyjnego zarządzania kryzysowego. Projekt ten stanowi odpowiedź na raport European Security Research Advisory Board (ESRAB), w którym określono najważniejsze wymagania odnośnie do systemu komunikacji.

Bezpieczny i wydajny system komunikacji jest warunkiem koniecznym do efektywnego zarządzania w sytuacjach kryzysowych. Przyjmuje się, że taka platforma jest w stanie znacząco zwiększyć efektywność prac służb ratunkowych. Obecnie jednak są przypadki, gdy służby ratunkowe (nie tylko na arenie międzynarodowej, lecz także podczas działań w jednym kraju) korzystają z niejednorodnych systemów telekomunikacyjnych, co często skutkuje brakiem lub istotnymi problemami z wzajemną łącznością. Sytuacja ta jest postrzegana jako problematyczna i stanowi zagrożenie dla efektywnego działania służb ratunkowych.

W ramach projektu SECRICOM opracowano system międzyplatformowej, bezpiecznej łączności SECRICOM Silentel. Za optymalizację transmisji danych (w tym wykorzystanie wielu nośnych oraz dynamiczne dostosowywanie się do warunków) w sieci dystrybucyjnej oraz szkieletowej odpowiada Multi Bearer Router (MBR). Zaawansowane mechanizmy zwiększające bezpieczeństwo urządzeń końcowych – Secure Docking Module (SDM) – opracowano z wykorzystaniem pryncypiów Trusted Computing. Secure Agent Infrastructure (SAI) zapewnia – oparty na infrastrukturze agentów – bezpieczny dostęp do rozproszonych danych. System uzupełnia platforma nadzoru nad siecią – Communication Security Monitoring and Control Centre.

Jako rezultat projektu zbudowano oraz kilkukrotnie zademonstrowano prototypową wersję systemu komunikacji. System ten jest zdolny do zapewnienia interoperacyjnej, bezpiecznej i wydajnej łączności w zarządzaniu w sytuacjach kryzysowych.

The SECRICOM Project

The SECRICOM project was a FP7 collaborative and integration research project, addressing the Security Theme in Call FP7-SEC-2007-1 in Topic SEC-2007-4.2-04 Wireless communication for EU crisis management. The

main aim of the project was to create Seamless Communication for Crisis Management for EU Safety.

The project was started in September 2008 and finished – as planned – after 44 months (April 2012). The budget was 12.468.847 (incl. 8.606.791 co-funded from FP7 programme) and the project have been realised by 14. partners from:

– **Industry** – QinetiQ (project coordinator), BUMAR, Hitachi, Infineon.

– **SME** – Ardaco (technical coordinator), CEA-LETI, Geothermal Anywhere, iTTi, Nextel.

– **University** – Universite du Luxembourg, Institute of Informatics, Slovak Academy of Sciences, Graz University of Technology, University of Patras.

– **End-user** – British APCO.

Figure 1 presents the structure of the project.

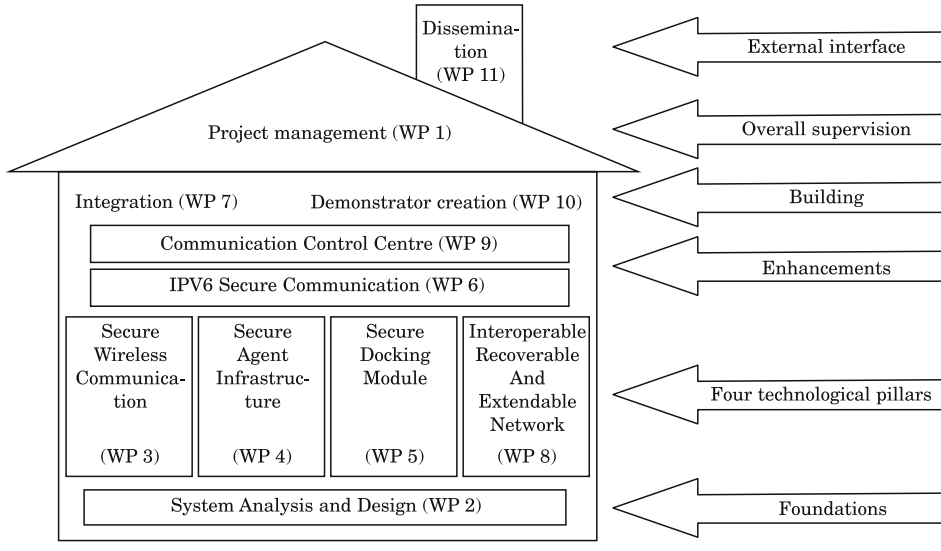

Fig. 1. Project structure

Source: SECRICOM Grant Agreement Annex I – Description of Work.

Motivation

The SECRICOM project has been established in response to the European Security Research Advisory Board (ESRAB) report (published in September 2006) in which the key requirements of new communication infrastructure have been proposed:

– Secure in terms of protection against tapping and external intrusion.

– Trusted in the sense of behaving as expected by meaning minimising the threats for failure to be a basis for creating emergency solutions.

– Providing enhanced connectivity between various networks and devices.

– Ensuring transmission of different data types such as multimedia (e.g.: voice, picture, video sequences), geopositioning, etc.

– Supporting advanced search functions embedded in the infrastructure itself (Meeting the challenge.)

The above mentioned requirements are in line with the current market needs, including:

– Growing demand for seamless, resilient and secure communication among various emergency communication systems required by public safety organizations and their users.

– Necessity of ubiquitous multimedia communication, available everywhere, coupled with real-time access to relevant information in the crisis area.

– Need for recoverability and alternative restoration of damaged communication cells for infrastructure functionality.

– Requirement of authorization, authentication, data protection against misuse, quick and flexible data acquisition whilst retaining Push To Talk simplicity of operation.

– Interoperability and interconnectivity of existing communication platforms (SECRICOM Grant Agreement Annex I – Description of Work).

The SECRICOM project was intended to fulfil those requirements, and provide interoperable and efficient communication system dedicated to first responders. The main innovations areas of the SECRICOM projects are:

– Interconnectivity of commercial (e.g. GSM, UMTS, Citizen Band) and specialized communication systems (e.g. TETRA).

– Seamless and secure interoperability of existing mobile devices already deployed.

– Efficient multi-bearer network utilisation,

– Software layer based on mobile agents' paradigm.

– Security based on chip-level trusted module.

Concept

The SECRICOM project was aimed at a reference security platform development for EU crisis management operations with two essential ambitions:

1. Solve or mitigate problems of contemporary crisis communication infrastructures (e.g. TETRA, GSM, Citizen Band, IP) such as poor interoperability of specialized communication means, vulnerability against tapping and

misuse, lack of possibilities to recover from failures, inability to use alternative data carriers as well as high deployment and operational costs.

2. Add new smart functions to existing services which will make the communication more effective and useful for users. Smart functions will be provided by distributed IT systems based on an agents: infrastructure. Achieving these two project ambitions will allow creating a pervasive and trusted communication infrastructure fulfilling crisis management users requirements, ready for immediate application.

The SECRICOM solution was based on four technological pillars:

1. Secure and encrypted mobile communication based on existing infrastructures (e.g. TETRA, GSM, UMTS networks) – secure Push To Talk.

2. Improved interoperability among various existing communicating systems, creating recoverable networks with seamless connectivity.

3. Introduction of distributed systems and the agent paradigm forming a smart negotiating system for parameterization and independent handling of requests essential for immediate reaction.

4. Security based on trusted hardware enhancing the data confidentiality and the users privacy (SECRICOM Grant Agreement Annex I – Description of Work).

The SECRICOM infrastructure was designed mainly for crisis management communication (rescuers, fire brigades, special forces, police, healthcare, etc.), but during the project's live cycle also other potential end-users have been identified. The SECRICOM delivers an interface between selected systems currently deployed for crisis management and new generation systems which could be developed in next decade, such as SDR. An important goal is to enable seamless and secure interoperability between currently used radio systems. Achieving the latter will ensure that already invested resources are preserved; also, developments and emerging technologies can be used in the future.

The SECRICOM implementation principles were as follows:

- Provide value to end-users.
  - Learn from end users.
  - Provide new services and applications.
- Supplement existing technologies (not replace).
- Integrate with existing systems (like TETRA).
- Open interfaces to support extensibility (no vendor lock-in).
- Security built deep inside (not an afterthought).
- High availability/reliability.
  - Throughout testing.
  - Support of multiple bearers – MBR.
  - Graceful degradation and QoS.
  - On-site deployable infrastructure.

SECRICOM architecture

The communication system architecture is smart and innovative concept that allows technical interoperability, and in terms of this, is able to extend communications across different agencies and across different countries. The SECRICOM is also technically expandable, thus able to extend communications to places where it is usually not capable of achieving ubiquitous operations.

It is foreseen, that the features of SECRICOM project will impact directly to communications systems and communication networks for Emergency services, but the project's results and technology could be used by civilian markets as well.

SECRICOM system is based on following technologies:

– SECRICOM Silentel – a client-server communication system using IP protocol. It optimizes and protects the way teams of people communicate without being concerned about misuse of information. Regardless of whether device is used to communicate, the connection is secure and safe. The basis of the system is PTT technology, a two-way communication system, which works like a two-way radio, however, with the possibility of transfering voice and other data types (e.g. multimedia, text messages, control data, etc.).

– Secure Docking Module – in order to provide security for agents that dock on to a trusted agent network, the SECRICOM project proposes the usage of Secure layer based on hardware module so-called Secure Docking Module (SDM). The design of SDM is based on Trust Computing principles.

– Secure Agent Infrastructure – designed for mobile services with agent-like features (mobility, pro-activity) which would execute on secure devices. In general, it consists of interconnected trusted (TS) and untrusted servers (US). Each agent has features and "abilities", which are used for the enactment of certain processes. The processes enactment is designed for the management of crisis situations in which information collection from multiple untrustworthy environments is required.

– Communication Security Control Centre – collects information to assure the secure status of the SECRICOM system, presenting it at a fixed location.

– Multi Bearer Router – an intelligent adaptive routing device enabling seamless inter-networking in a multi-bearer, multi-node, mobile environment designed to optimise network performance whenever users operate in environments where connectivity is poor

– IPv6 – All the modules developed for SECRICOM are eligible to cope with an IPv6 environment. The modules like SECRICOM PTT, Secure Docking Module, Multi-Bearer Router and Communication Security Control Centre are capable of handling the IPv6. This protocol and its impact on secure communi-

cation was studied and described in details by University Luxembourg. The SECRICOM's compatibility with the IPv6 is confirmed by IPv6 Forum, where the IPv6 Silver Ready Logo have been awarded.

General SECRICOM network architecture is presented in the Figure 2.

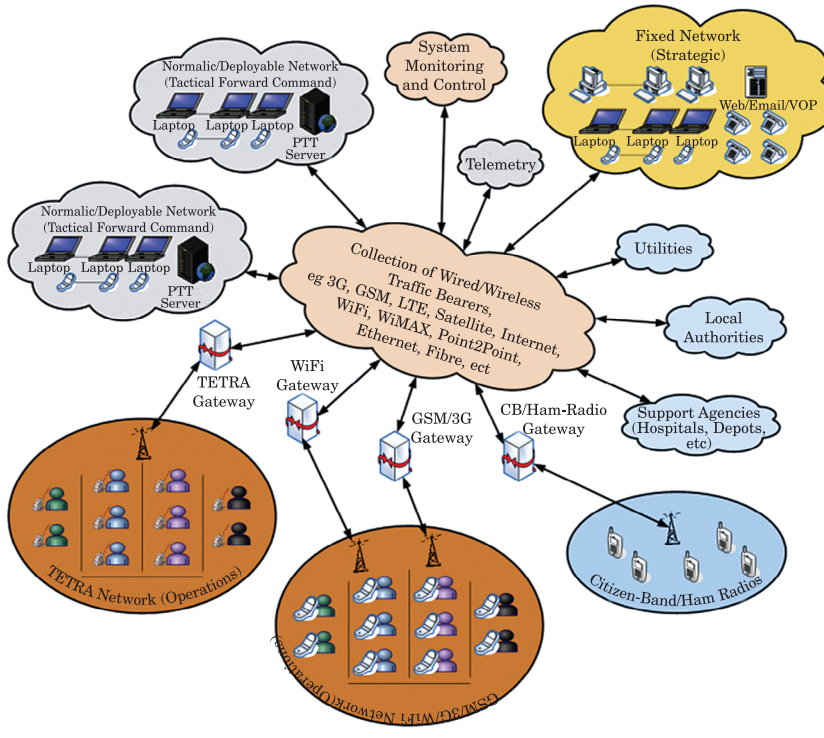

Fig. 2. SECRICOM Network Architecture
Source: SECRICOM Deliverable D2.1 – Analysis of external and internal system requirements.

Push To Talk (SECRICOM Silentel)

SECRICOM Silentel is a client-server communication system. The application has been designed to support the First Responders in their day-to-day missions, as well as critical situations. The main aim of this solution is to optimise and protect the communication between end users in a seamless way, using existing infrastructure (incl. end users terminals and network infrastructure). The communication between endpoints is encrypted to prevent any transmitted data (voice, text, images, position, status, etc) from misuse. The

user requirements were defined in SECRICOM User Requirements[1]. The key features include:

1. Voice communication.
   a. One-to-one full duplex.
   b. One-to-many half-duplex group call (Push To Talk).
2. Online group management.
3. Instant text messaging,
4. Smart text messaging.
5. Data delivery.
6. Video communication.
7. User location information and mapping, based on GPS.

The system is based on the IPv4/IPv6, which facilitates the system's scalability as well as integration with other technologies. The solution's High Level Architecture is given in the Figure 3.

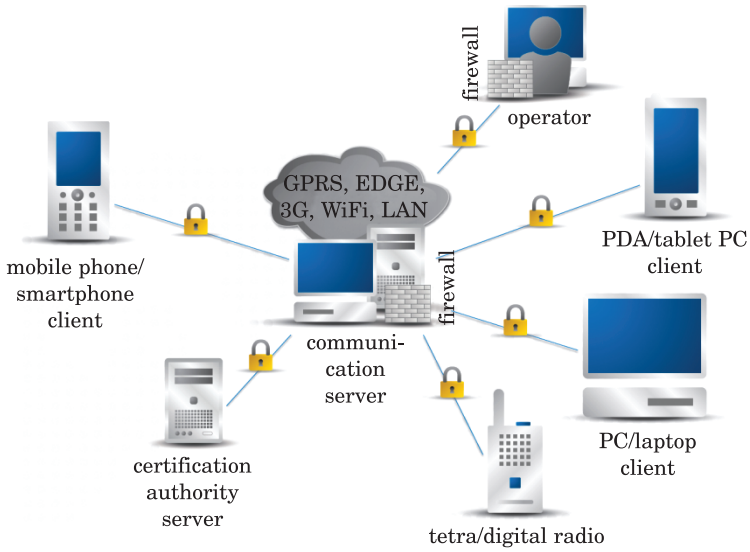

Fig. 3. Secricom Silentel (PTT) high level architecture
Source: ARDACO dissemination materials.

Main parts of SECRICOM Silentel architecture are as follows:

– Communication Server – switching centre module to provide communication services to all system's users.

– Certification Authority – trust module for server and users certification creation, validation and revocation.

[1] D2.1 – Analysis of external and internal system requirements.

– Operator Studio – user management tool (incl. personal contact list definition).

– End user application – software application to be deployed on end user's terminal. Currently several implementations on various operating systems are available – incl. Symbian, Windows Mobile, iOS, Windows and Android.

– SECRICOM gateways – device to provide interoperability with some legacy networks (e.g. TETRA, Citizen Band).

Multi-Bearer Router

The routers that are currently used in managing major incidents and crisis situations tend to be inflexible and inefficient when it comes to meeting the following requirements:

– Interfacing to selected communication systems which are taken into the field.

– Interfacing to a number of communication systems which have survived a major incident or were brought into the incident zone by a supporting agency.

They do not provide a sufficient level of resilience to enable the business processes and operations to continue to operate in areas where existing communication systems and infrastructure are either destroyed by an incident or poor in its original form.

The Multi-Bearer Router (MBR) technology has been designed to fill that gap. It is an intelligent adaptive routing device enabling seamless internetworking in a multi-bearer, multi-node, mobile environment designed to optimise network performance whenever users operate in environments where the connectivity is poor. There is a need for SECRICOM solution to seamlessly support different types of user traffic (with different QoS and security requirements) over different communication bearers (with a range of capabilities), depending on the end user environment (e.g. disaster relief with ad hoc communications, mobile working with dynamically changing access to communications service provider networks). Leveraging legacy communication systems is possible due to integrating together modern satellite communications, mature security, provisioning private networks, open architectures, application persistence and ubiquitous mobile broadband. Conceptually, the SECRICOM's MBR performs two functions:

– Allows creating an efficient network-of-networks as the basis for business focused traffic delivery (roaming-like) across different networks. This network-of-networks is achieved by transparently integrating available communication and network systems (both wireless and wired forms); and making

intelligent and flexible traffic routing decisions based on multiple factors, e.g. user application, availability and reliability of networks, effective bandwidth, cost and security.

– Provides a gateway for SECRICOM end systems and devices to the created network-of-networks through a single Service Access Point (SAP).

The MBR is independent of the type of traffic and is intelligent enough to inhibit inappropriate data streams such as video, for example, over unsuitable bearers whilst still maintaining the bearer usage for other systems. The technology allows highly confidential data to always be routed over the TETRA bearer. It simultaneously routes less sensitive high bandwidth data, such as still photographs, video or CCTV images, over other high capacity bearers. If one of these bearers is lost, the application routes seamlessly over an alternative bearer, with no need for user intervention and no interruption to the service. The Multi-Bearer Router features a unique intelligent policy engine. This constantly monitors the constituent network capabilities and modifies traffic delivery policies dynamically according to pre-defined business needs and the level of services available. This enables the user to automatically use the available networks with the least impact on performance and without the risk of security compromise. The flexible policies are tailored to meet objectives such as operational imperatives, user needs and specific application requirements.

Key benefits include:

– Increases efficiency through provisioning of mobile broadband.
– Fast and reliable access to information for better situational awareness.
– Improves communication coverage.
– Prioritises business critical information flow.
– Supports minimal configuration in field.
– Provides unified access to all available communications services.

Secure Docking Module

Communication security is a well-established in today's networked computers. Security expert Eugene Spafford once said using secure communication technologies, such as SSL, is similar to "using an armored truck to transport rolls of pennies between someone on a park bench and someone doing business from a cardboard box". This refers to the communication channel being secure due to technologies like SSL and SSH, when used with strong cryptographic algorithms such as RSA, elliptic curve cryptography and AES. So what about the communication end-points? "Park benches" and "cardboard boxes" have no place in a secure communication infrastructure,

such as the one developed by the SECRICOM project. This is the gap that the Secure Docking Module wants to close.

General purpose computing platforms such as PCs, laptops and mobile phones are all vulnerable to over-the-network software attacks. The enormous amount of known vulnerabilities in operating systems and applications is testament to this vulnerability. A wide variety of malicious software is known to exploit such vulnerabilities to take over unsuspecting computing platforms. Malicious software on a computing platform used in crisis management is unacceptable. For SECRICOM to be able to leverage the power of mobile computing platforms for crisis management, as for example with the Secure Agent Infrastructure, the security of the computing platforms must be established.

The Secure Docking Module is a platform-software-configuration verification device. When malicious software infects a computing platform, it usually integrates itself into the attacked platform. This integration changes the platform software configuration. Now, if an external arbiter could detect this change of software configuration, it might be able to deem the platform insecure for use within a crisis management infrastructure. Thus, spreading of the malicious software to other computing platforms in the network would be hindered. The Secure Docking Module is just such an arbitration device.

The Secure Docking Module works in conjunction with the Trusted Docking Station. The Trusted Docking Station uses recent security additions to commodity-of-the-shelf computing platforms to achieve two goals. First, the Trusted Docking Station provides the ability to measure and attest a platform's software configuration. Second, it establishes a strongly isolated execution environment for crisis management applications. Thus, the Trusted Docking Station is capable of reliably reporting its software configuration to the Secure Docking Module. In addition, it provides an execution environment where each software component is protected by virtualization technology form other components of the system.

The Secure Docking Module provides the cryptographic resources required to access the SECRICOM crisis management infrastructure. If a SECRICOM software component wants to connect to the SECRICOM network it reports the software configuration of its execution environment to the Secure Docking Module. The Secure Docking Module then proceeds to check the integrity and freshness of the platform software configuration report using cryptographic algorithms. If the integrity and freshness of the report are verifiable, the Secure Docking Module will validate the platform software configuration. Only if the platform software configuration is valid, does the Secure Docking Module provide its cryptographic resources to the Trusted Docking Station, and thus to the SECRICOM software component. In this way only platforms with a verified software configuration and approved applications are able to connect to the SECRICOM infrastructure.

Secure Agent Infrastructure

One of the challenges of the communication infrastructures for crisis management is to add new smart functions to existing services which would make the communication more effective and helpful for users. The aim is to provide smart functions via distributed information systems which should provide a secure distributed paradigm to achieve confidentiality and access to resources. In the SECRICOM project requirements, design and implementation of such distributed information system – called Secure Agent Infrastructure (SAI) was enacted.

Requirements for such infrastructure were to provide a smart negotiating system for parameterization and independent handling of access requests to achieve rapid reaction. By fulfilling these goals a pervasive and trusted communication infrastructure satisfying the requirements of crisis management authorities and ready for immediate application was introduced. SAI represents one of the core parts of the SECRICOM communication infrastructure.

In crisis situations there are requirements to collect information from legacy systems of various organizations and from human operators in order to semi-automatically manage the crisis mitigation process or to enact decisions at various management levels. This collection of information must be enacted in a secure manner while ensuring trust between both parties – information consumers and information providers. Many actors participate in a crisis situation. Information gathering is enacted by secure agents either from legacy systems or from human end-users through mobile devices. Agent technology was selected due to the ability to fulfill such requirements through support of mobile and dynamically deployable executable code.

Additionally agents require safe secured place to store sensitive information (such as cryptographic credentials) and provide interfaces to retrieve these keys, ways to attest a platform and provide interface to safely communicate with legacy systems – all these functionalities are provided to the agent platform by a hardware module called Secure Docking Module (SDM) which was also developed in scope of the Secricom projects.

The SDM allows agents to dock on a secure communication infrastructure by ensuring the state of the device it is supporting. The SAI is a distributed system and operates on confidential data. Therefore, the system must protect its integrity against data loss/theft and data modification. In a distributed system, data protection concerns are not limited to data transmission. As the data is processed in different physical computing platforms it must be established that all data processing entities adhere to the same security policy for the data.

The data security policy adherence is enforced by ensuring the software configuration of a computing platform before it is connected to the SECRICOM infrastructure. To this end the SDM protects communication keys and credential information and only releases this information to the host platform if this platform is in an approved software configuration. The process of establishing the fact that a platform has an approved software configuration is called local attestation verification.

Conceptually, the SDM protects a small set of key pairs for asymmetric cryptography, but in general is capable of protecting arbitrary data up to a specific size. The SDM's key protection facilities are a standard function, which could already be implemented with today's smart cards or hardware security modules. The SDM extends this standard function by only releasing these keys to a host device if and only if this host device is in a trusted state. This host device is called Trusted Docking Stations (TDS).

Communication Security Monitoring and Control Centre

The main purpose of the Communication Security Monitoring and Control Centre (CSMCC) is to provide Security Model, suitable for secure and interoperable communications under crisis, which could be applied in the SECRICOM communication infrastructure. The Security Model defines the properties, capabilities, processes and controls that a secure infrastructure should contain to protect against various threats.

Key features of SECRICOM Communication Security Monitoring and Control Centre:

– Increased protection of assets: various protection mechanisms which control access and usage policies, scalable network architecture, auditing tools, and security assurance monitoring.

– Improved threat detection: new traffic patterns and event management policies and correlation for anomalous events

– Enhanced reaction for hostile environments: increased network resilience by enhancing IT structure, traffic blocking and isolating as well as alternative routing

– Fast recovery for crisis critical communications: quick and efficient recovering plans and mechanisms. One of the main strengths and unique features of the CSMCC platform in SECRICOM is the set of custom agents that have been deployed along the communication infrastructure. These enhanced agents provide new detection and action capabilities, such as adaptive routing features in case of network failure or congestion and VoIP traffic monitoring.

Additionally, Security Middleware Services and Framework was developed to measure, document and maintain the security of SECRICOM services, which are based on telecommunication services.

Designing the communication infrastructure security monitoring and control centre, started with a risk assessment of the SECRICOM system. It consisted of a deep analysis of the operating system, in order to define key assets, identify their security vulnerabilities and should risk occur, evaluate its impact. The outcome of risk assessment was a set of security requirements that the SECRICOM security model fulfils to provide an effective security management. This has been supported by a team of users who updated and validated these security requirements. The analysis of the security requirements results in a number of countermeasures and security mechanisms that are used to mitigate the level of risk and protect the SECRICOM systems against any kind of security threats. Finally, all these security principles and guidelines are aggregated into the SECRICOM security model in order to ensure continuous security of communication infrastructure in a continuous way. The security model is supported by a security middleware named Communication Security Monitoring and Control Centre (CSMCC) that provides not only a collection of security information and security status monitoring capabilities, but also active control mechanisms. They provide enhanced protection, improved detection, faster reaction and stronger risk mitigation, more effective incident impact mitigation and quicker restoration.

Conclusions

In this article we considered the SECRICOM project as an answer to the interoperability problems between first responders' communication systems. Those problems stem from different communication networks used by various rescue services, low security level and thus high vulnerability to different threats. The SECRICOM system was designed to provide unified, secure and seamless communication between various end-users and to improve the effectiveness of their work during crisis situation.

This paper provided a survey of all the technologies used within the SECRICOM system. The SECRICOM project has successfully fulfilled all requirements and designed a prototype capable of:

– Exploiting & optimizing existing communication systems.

– Enhancing interoperability among heterogeneous secure communication systems.

– Enhancing interconnectivity between different networks and User Access Devices.

– Interfacing towards emerging SDR systems.
– Mitigating key capability gaps faced by users of existing systems.

Thus, the "Seamless Communication for Crisis Management" proof of concept has been achieved. The SECRICOM has also been successfully demonstrated to the stakeholders during national as well as European events, including:

– BAPCO 2010 in Business Design Centre, London, UK.
– Civil Protection NATO Seminar in Lest Training Village, Slovakia.
– BAPCO 2011 in Business Design Centre, London, UK.
– ASTER 2011 in Żagań, Poland.
– SECRICOM demonstration 2012 in Portsmouth Technology Park, UK.

where the positive feedback have been received.

Acknowledgments

This work was supported by the SECRICOM project (EC FP7-SEC-2007 grant 218123).

Translated by AUTHORS

Accepted for print 30.06.2012

References

FOURNARIS A., HEIN D., SCHEIBE M., FOURNIER J., VERDIER M. 2010. *Design of the Secure Docking Module.* Infineon Technologies AG.

GATIAL E., BALOGH Z., HLUCHÝ L. 2010. *Platform for distributed execution of agents for trusted data collection*. Procedia Computer Science, 1: 2023-2032.

GOBAN-KLAS T., SIENKIEWICZ P. 1999. *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania.* Wydawnictwo Postępu Telekomunikacji, Kraków.

HLUCHÝ L., BALOGH Z., GATIAL E. 2010. *Distributed agent-based architecture for management of crisis situations using trusted code execution*. SAMI 2010 8th International Symposium on Applied Machine Intelligence and Informatics Proceedings, pp. 25–30.

Meeting the challenge: the European Security Research Agenda. European Security Research Advisory Board, September 2006 – http://ec.europa.eu/enterprise/policies/security/files/esrab–report–en.pdf

SCHEIBE M., HEIN D., REYMOND G., FOURNIER J., FOURNARIS A.P., HUDEK V., SLOVAK L. 2011. *SECRICOM WP5 Design of the Chip and Emulator*. Technische Universität Graz.

SECRICOM D2.1 – Analysis of external and internal system requirements.

SECRICOM Dissemination materials.

SECRICOM Grant Agreement Annex I – Description of Work.

WOJCIECHOWICZ W., ZYCH J. 2011. *Koncepcja infrastruktury telekomunikacyjnej o podwyższonej niezawodności*. In: *Bezpieczeństwo współczesnego świata – Informatyka, technika i gospodarka*. Red. Z. Dziemianko, WSHiU Poznań.