Information Society Technologies (IST)

Deliverable No: D.WP.JRA.6.3.7

Deliverable title:
Security considerations for Next Generation Internet

Deliverable version N°:	1
Sending date:	2006-11-30
Editor's name:	Jens Oberender, Markus Fiedler
Lead contractor N°:	56, 49
Dissemination level:	PU
URL reference of the workpackage:	http://www.eurongi.org/member/WP_JRA_63/

Project acronym: Euro-NGI.

Project full title: Design and Engineering of the Next Generation Internet, towards convergent multi-service networks.

Type of contract: NETWORK OF EXCELLENCE.

Contract N°: 507613.

Project URL: http://www.eurongi.org

Information Society Technologies (IST)

Sixth Framework Programme

Editor’s name: Jens Oberender, Markus Fiedler

Editor’s e-mail address: jens.oberender@uni-passau.de, markus.fiedler@bth.se

With contributions of the following partners:

Partner Number	Partner Name	Contributor Name	Contributor e-mail address
56	University of Passau	Jens Oberender Hermann de Meer	jens.oberender@uni-passau.de demeer@fmi.uni-passau.de
49	Blekinge Institute of Technology	Markus Fiedler Henric Johnsson Charlott Eliasson	markus.fiedler@bth.se henric.johnsson@bth.se cel@bth.se
36	WUT	Zbigniew Kotulski Aneta Zwierko Tomasz Ciszkowski Wojciech Mazurczyk	zkotulsk@tele.pw.edu.pl azwierko@tele.pw.edu.pl T.Ciszkowski@tele.pw.edu.pl wmazurczyk@tele.pw.edu.pl
29	TLC Group Pisa	Michele Pagano Christian Callegari	m.pagano@iet.unipi.it christian.callegari@iet.unipi.it
38	IT	André Zúquete	avz@det.ua.pt
30	Coritel	Erasmo Atteo AntonLuca Robustelli	eatteo@its.na.it antonluca.robustelli@coritel.it

Project acronym: Euro-NGI.

Project full title: Design and Engineering of the Next Generation Internet, towards convergent multi-service networks.

Type of contract: NETWORK OF EXCELLENCE.

Contract N°: 507613.

Project URL: http://www.eurongi.org

Summary

1 Introduction

Security will play a dominante role in future communications. While an increasing number of users have access to a huge variety of services, at the same time, they are exposed to global security risks in an increasingly hostile environment. Thus, there is an obvious risk of using the common network for increasingly critical processes (e-commerce, e-health, etc.), while at the same time the ever-increasing possibilities of accessing the Internet, e.g. though wireless or mobile networks pose new challenges of keeping the level of security high enough and to answer the trust that users put in ICT systems. Security breaches – whether they are real or just rumours – might keep people from using Internet and its services. In the short run, this implies reduced income for application, service and network providers; in the long run, Internet's basic reputation might be severely damaged. Protection against misuse or attacks is therefore a vital objective to establish, maintain and strengthen the trust of users and service providers of information technology. Thus, considerations for maintaining security are important for future network architectures.

The overall target for the EuroNGI workpackage JRA.6.3 aims at establishing security (linked to quality and pricing) as an integral part of Next Generation Internet services (A4C = authentication, authorization, accounting, auditing and charging). Users should become more aware of risks and should be provided with integrated, adequate, negotiable and easy-to-manage security facilities. In order to decrease the risk that security is dropped by users struggling with tiresome security settings, the whole security process should be streamlined and integrated, with security measures being adequate in terms of resource needs.

Security aspects to be considered are manifold. They depend on the role of a communication participant (user, service provider, network operator, equipment vendor, "third parties" such as banks, or trusted authorities), on the management and organization of security services, and on the technical methods used to support security objectives (technical security). Security levels are relative and depend on both the strength of the measures to protect the information assets as well as the strength of the attacker.

Security considerations for the Next Generation Internet includes authenticity, integrity and anonymity. Scenarios to be dealt with are network communications with specific requirements, such as mobility. Communications can occur using the physical infrastructure and overlay networks like Peer-to-Peer. The field of security is dominated by heavy-weight preventive methods. Another trend is economic security, i.e. adaptive cryptographic protocols that fit low capability devices.

This deliverable is structured as follows. Chapter 2 reports on research projects, in this workpackage the STEEP consortium proposed actions for the PASR 2005 and 2006 calls. Chapter 3 lists ongoing activities in the fields authentication, cryptographic methods, anonymity and voting. Chapter 4 provides a brief conclusion and outlook.

2 Mid-term/long term evolution in this area

The trend towards universal connectivity in terms of “anything-over-IP-over-anything” will most likely hold on. Depending on the access scenarios, different levels of risk, cost and configuration effort incurred to end users will exist in the mid-term.

For instance, in Internet Multimedia System (IMS)-based Next Generation Networks (NGN), particular efforts to provide security are undertaken. In such scenarios, TriplePlay services such as telephony and TV are provided within a “walled garden” (i.e. the domain of the network provider), which significantly lowers the risk of malicious access from outside. Still, through the third TriplePlay service, traditional Internet access, users may still be exposed to attacks from outside. Such risks can be reduced by operating firewalls and anti-virus software. Those extra services are usually charged to the end user.

Wireless LAN hotspots in public areas (e.g. airports, major hotels, conference centers, etc.) have become very popular. Still, the majority of those access points provide AAA mainly for charging purposes, however renouncing to encryption, as the configuration procedure would become even more tedious when network keys are to be distributed. Also, Virtual Private Networks (VPN) connectivity usually needs a lot of (manual) configuration effort. There is an obvious risk that impatient users rather renounce to security measures than to insecure network connectivity. Yet another problem domain is that of unconscious usage of wireless devices especially in ad-hoc communication scenarios. For instance, a Bluetooth-equipped phone or computer can easily be infected when being discovered and sent a file containing a virus that is not discovered by some locally installed antivirus software. In general, users have to be prepared that someone else finds a possibility to “enter” their systems somehow, which makes systems to protect access to stored information and *Digital Right Management* strategies unavoidable in some cases.

During the recent years, peer-to-peer applications have attracted an immense number of users. While mostly used to distribute files (music, movies, software, etc.), these self-organizing applications have the potential of distributing malicious software. Owners of precious content need to protect it, for instance by using Digital Right Management solutions. On the other hand, their self-organization potential might also be used to implement security measures and services in a distributed and scalable way.

In order to provide for future secure communications granting *confidentiality*, *integrity*, *accountability*, *availability*, *accessibility* and *anonymity*, Internet-based services, their users and their devices will need to be sheltered in a much better way in the future than what is the case today. Consciousness of the risks is important, but just knowledge alone can’t protect users from choosing inappropriate levels of security. Users, their processes and devices need to be sheltered by trustworthy, *provable security services* to a much larger extent than what is the case today. This holds in particular for mission-critical services, e.g. e-health, e-voting, remote control, e-business etc., as security problems might turn into trust problems between the corresponding parties (e.g. citizens and authorities). Such a security service will need to addresses A5 (= authentication, authorization, accounting, anonymity and auditing). Basically, *security has to become yet another Quality of Service (QoS) parameter*. As security measures impact performance and can be costly in terms of resource usage, and both capital and operational expenditures, the type of security measures and its corresponding strengths have to be carefully chosen. This imposes the need for *quantitative assessment* of risks and security offerings in order to tailor the security service to the task to be performed. Given the multitude of access possibilities, *seamless* security across different domains will become vital for successful security provisioning.

The concept of "*Always Best Security*" will become very important, amongst others offering adaptive and in particular *Lightweight Security* solutions to be used when both risks and resources are limited. Much work has been put into the proposal and implementation of new and stronger security solutions. However, less effort has been directed towards the actual act of determining a sufficient security level with respect to different criteria. There are concerns when strong security is unnecessarily used, since the load on the processor and the power consumption is increased (even though we believe that the processing overhead is of greater concern than the power consumption). By offering security based on a need determined by a decision model it is possible to optimize security such as to reduce the cost. Performance and efficiency issues are particularly important in environments with constrained capacity. A further step would involve the development of a type of *cognitive security*, not in the psychological sense, but as a notion of cognitive technology. Cognition refers to the act of processing or knowing, including awareness, recognition, judgment, and reasoning. In this specific case, the envisioned system would be able to sense the environment, learn how to handle threats and then take countermeasures to improve the overall security.

Besides preventive methods such as pre-selecting security measures and levels for certain types of task, reactive methods need to be enabled by continuous *monitoring* of the security conditions and – if necessary – adapting the security level (e.g. by switching from lightweight to more advanced security mechanisms) and/or issuing alarms.

Last but not least, the user will have to be relieved from the need to "puzzle" together a security solution, balancing risk level and price-worthiness. This will decrease the "human risk factor". On the other hand, the user should also be warned about risks and selected countermeasures to a much broader extent than what is the case today. The common goal of all these approaches is to provide the user with trust in the communication such that the service of interest is felt to be a utility and not a risk.

3 Projects

This chapter presents a short summary of the collobrative project actitiy of the EuroNGI workpackage JRA.6.3 « Security ». The spread of excellence activities enabled ten of the workpackage members to contribute to a project proposal in response to the EU call for prepatory action for security research.

3.1 Security in Telecommunication Environment Protection (STEEP 2005)

Future B3G (Beyond 3rd Generation) Networks require appropriate security designs. This proposal extends the IP Multimedia Subsystem (IMS) to enables crisis management based on deployed B3G infrastructure.

A spin-off group of EuroNGI members established in April 2004 to respond to the EU-call Preparatory Action for Security Research 2005 (PASR-05). Initial partners were: Consorzio di Ricerca sulle telecomunicazioni (Co.Ri.TeL)/Italy, the Norwegian University of Science and Technology (NTNU)/Norway and Centre for Quantifiable Quality of Service in Communication Systems (Q2S) /Norway, the Blekinge Institute of Technology (BTH)/Sweden, Instituto de Telecomunicações (IT-Aveiro)/Italy, Warsaw University of Technology (WUT)/Poland and University of Passau (UP)/Germany. The spin-off group submitted the collabrative project "Security in Telecommunication Environment Protection". Unfortantely, we did not receive funding from the European Union.

3.2 Security in Telecommunications Equipments oriented to Emergency management through Peer-to-peer services (STEEP 2006)

The spin-off group STEEP 2005 (see above) decided for redesign of the proposal for the 2006 call (PASR-06) and invited 4 additional partners: Telefónica Investigación y Desarrollo, Sociedad Anónima Unipersonal (Telefonica)/Spain, Consorzio di ricerca per lo sviluppo di prodotti, servizi e sistemi integrati per la gestione, la tutela e la valorizzazione dell'ambiente e del territorio (TELLUS)/Italy, Italtel SpA(ITL)/Italy and ITware Informatikai Szolgáltató és Kereskedelmi Kft. (ITWARE)/Hungary. The spin-off group submitted a proposal on "Security in Telecommunications Equipments oriented to Emergency management through Peer-to-peer services". Again, the spinoff group did not receive funding from the European Union for the STEEP proposal. Meanwhile, some partners were not able to deliver results in these fields. Therefore we restrict our presentation to the targeted scenario.

Starting from the analysis of the *IP Multimedia Subsystem* (IMS) structure we draw a clear picture of the current and future security challenges for Beyond 3rd Generation (B3G) services and applications deployed on networked, IP based, systems which creates the same kind of security vulnerabilities and threats already experienced on Internet. To cope with such challenges, a security management system offering a wide variety of security services will be placed at the operator's disposal. It will include standardised protocols such as IPsec and Diameter along with innovative lightweight encryption techniques which, through a novel management scheme, will confer a trustable appeal to the IMS prototype operability. Security will be improved by coupling both signalling and media flows. Effective methods for anonymous authentication and data protection will be included as well. Our architecture fits both intra- and inter-domain scenarios. In the latter case it promotes the role of certification authority towards external third party service providers.

The STEEP proposal fulfills three fields specified in the PASR-06 call.

1) Optimising security and protection of networked systems.
Aim: "to analyse established and future networked systems and services, such as communications systems and services, utility systems and services, transportation facilities, networks for (cyber) commerce and business as well as identification of their interdependencies, with regard to the security of use and vulnerabilities, to show how to minimise socio/economic impact of, and implement protective security measures against both electronic and physical threats."

Key activities for Projects are development and demonstrations of:
– Measures (incl. resulting risk assessments) for enhanced protection and assurance of utility systems and services, or transportation facilities critical to maintain security in an enlarged Europe, in particular for (i) drinking water supply or oil/natural gas supply, (ii) industrial sites or (iii) land, water borne and multimodal transport.
– Prevention, protection, response and alert capabilities to improve the dependability and resilience of control systems for (networked) infrastructures.

2) Enhancing Crisis Management (including evacuation, search and rescue operations, control and remediation).

Aim: to address the operational and technological issues from three perspectives: crisis prevention (including risk assessment) operational preparedness and management of declared crises. This includes activities in relation to life threatening substances (CBRN or explosives).
Key activities for Projects are development and demonstrations of:
– Shared information management tools and models to facilitate the efficient integration of diverse emergency and management services for (i) humanitarian operations and (ii) rescue tasks in support of the external policies of the EU with an emphasis on security aspects and attention to organisational structures, inter-organisational co-ordination and communication, distributed architectures and human factors.
– Joint, cross-border control and command systems for emergency and management services in the domain of security operations.
– Technologies and protocols for decontamination of CBRN substances for personnel, equipment and facilities.

3) Achieving interoperability and integrated systems for information and communication.
Aim: to develop and demonstrate interoperability concepts for information systems and technologies in the domain of security, enabling the linking of existing and new assets to offer improved performance and enhanced adaptive functionality. In addition, attention must be given to organisational and semantic aspects, dependability, protection of confidentiality and integrity of information. To support interoperability, system providers need to involve end-users and standardisation issues.

Key activities for Projects are development and demonstrations of:
– Novel concepts and architectures for information exchange between national administrations for pan-European e-government services in the domain of security.

– Novel concepts and architectures for wireless communication and information exchange systems for pan-European and (inter-)national emergency and management services. The architecture should allow for the integration of multi-purpose, specific modules for waveforms and cryptography.

The project proposal has been built up on two types of contributions which respectively are:

1. Improvements to the IMS security capabilities,
2. Addition of a P2P overlay within the IMS architecture whose security capabilities have been reinforced.

The reinforced IMS security structure can be used to interconnect utility systems in a reliable and effective manner, and at the same time it can include a P2P architecture which not only increases and facilitates the systems' interoperability but becomes a powerful means for emergency conditions. These logical considerations suggest to separately treat the two types of contributions.

Being the former propaedeutic to the latter, the project was meant to begin with the definition of the security adjuncts to improve the IMS security capabilities. At the same time a research activity was planned on P2P topics.

The possibility to proceed in parallel with the two different subjects derived from the variegated skills which the partners offer. When the IMS security advancements is sufficiently consolidated, the partners specialised in the field of utility systems management can be appropriately involved in order to direct the design efforts towards a final users application showing the effectiveness of the achieved results for the management of utility systems. For such reasons two separate work-package groups were identified, respectively dedicated to the fulfilment of the two above-mentioned types of contributions. Such groups were: WP Group 1, dedicated to IMS improvement; WP Group 2, which includes the activities for the P2P infrastructure.

In order to better control the different types of actions to undertake for the achievement of the objectives, the two groups of work-packages, WP group 1 and WP group 2, in turn, were divided into two different subsections which, respectively, are: Industrial research and pre-competitive development.

A further type of work-package was added in order to take care of the management of the whole project.

IMS Security Improvements

Our logical approach derives from the analysis of a business scenario which includes all the actors that can be interested in information exchange and network communication either for business or for social reasons, or for lawful duty, or for entertainment (enterprise, e-commerce, banking, whole retailers, application service providers, telecom operators, public entities etc.)

The objective of such analysis is to identify the security issues from different points of view and provide the conditions for all of them to properly inter-operate. To this end we will study in deep details a real-time multimedia communication set-up taking into account both legacy and B3G technology potentials.

A set of necessary activities have been identified through which we will address the domain of security in three different aspects, which respectively are: security improvements related to a communications infrastructure, new services and features to facilitate interoperability, and management of emergency conditions.

The main activities related to security improvements are:

- Security metrics and their management (e.g. SLA, Service Level Agreement);
- Access Networks (Authentication process at the access network level);
- Core network access (Registration and authentication with the home network);
- Set-up of secure signalling path (identification of a suitable path which guarantees reachability, confidentiality and integrity);
- Session management (Signalling and session authentication);
- Service Access (Authentication and authorization);
- Set-up of secure media path (Identification of suitable path which is able to guarantee confidentiality and integrity);
- Service fruition (It refers to all the security aspects of media transmission);
- Security and AAA issues for inter-domain information exchange and interoperability advances;
- Performance evaluation (Evaluation of the impact determined by the security functionalities.

The above listed activities brought us to split up the work in a set of coherent work packages which cover all the identified topics.

Several milestones have been defined in order to keep control of the work progress so that a possible divergence of the achieved results might be rapidly made up to through appropriate corrective actions so as to reach the planned expectations.

Since we are considering an inter-domain scenario we will first consider the rules and the modalities for systems interoperability, then we will focus our attention on the means to add on the IMS structure which, in our opinion, can be considered the main networking infrastructure for the next future. We will analyse the IMS architecture and in particular we will investigate on both the session control details and security deployment tools which will introduce innovative features to the IMS security capabilities.

Complementary knowledge of the partners has become a strength point for the project since it is possible to cover all the items which have been listed above. Separate experiments will be independently carried out in different laboratories located in the different countries in order to accelerate and make more profitable and comfortable the studies. However integration will not be affected because each prototype will logically include standardised interfaces representing the hinges necessary to put together all the different parts.

P2P Services

Interoperability between systems and services does not only depend on the availability of standard interfaces, but also on the possibilities to make devices interact easily and appropriately in order to share information.

To increase such interoperability functionality we propose Peer-to-Peer (P2P) overlay structure which fits the IMS architecture and relies on the IMS security functionalities. A peer based concept has the advantage that security-related decisions can be processed at the network edge, instead of processes at the network operator outside the reach of users. The crisis management example makes use of the powerful and simple operational modalities of this P2P service. Fast distribution of prioritised information can support emergency teams heavily. The P2P paradigm is also well suited for cross-platform integration between rescue teams.

A P2P Overlay is able to collaborate with IMS architecture elements. For transmission efficiency, existing IMS concepts can be utilized by the participants of the P2P overlay.

Three main objectives are to be realised within P2P structure which respectively are dynamic trust, content assessment, and scheduling. Peers collect reputation data either from the central entities or neighbourhood. Content is classified by delivery priority, secrecy level, and trust. The classification is used for scheduling, where urgent deliveries must be processed first.

Besides, related to the P2P overlay structure, another scenario can be considered to deal with the spreading of information in crisis management situations, across an IMS network. This information would be, initially, in the form of SMS messages, although MMS message spreading could also be studied.
This kind of system would be very useful for public administrations in crisis management, enabling them to send emergency messages (evacuation orders, public safety communications, etc). By using P2P techniques, this spreading of messages would be much faster and scalable.

The emergency scenario will also feature secure video communications within emergency forces. The integration of in-the-field devices with stationary based devices must be fulfilled.

The environment demands for high availability and robustness. We combine current methods with IMS features to enforce security.

Two partners will bring aboard the field experience:

- Civil Protection Office of the Municipality of Naples (Italy), for crisis and emergency management scenarios;
- Tellus Consortium, for utilities and transportation communication management scenarios.

The emergency cases can be split in:

- Minor, as adverse meteorological conditions, instability and damage of road and built structures, drinking water supply defaults, electric supply defaults, difficult social and sanitary situations, etc.
- Major, as seismic risk, volcanic risk, hydro-geological risk, forest fire risk, industrial risk, etc.
- Public events, as large sport and cultural events, mass events during holidays, etc.

To manage such scenarios, a communication network with high grade of security is strictly needed, for following main info exchange:

- Land and environment control information exchange;
- Risk scenarios elaboration
- Coordination of emergency groups
- Early warning data transmission
- Connection among Emergency groups

3.3 STEEP Contribution to FP7

Work on these topics will be continued also because they appear within the FP7 ICT - INFORMATION AND COMMUNICATION TECHNOLOGIES draft (ver.1).

Furthermore, a new proposal will be prepared for submission in the 1st call of FP7 by strengthening and widening the content and the appeal of the above-mentioned project by means of the inclusion of new research subjects such as ad-hoc networking, a general service infrastructure, network and service resiliency.

Such new research topics will represent an adjunct and at the same time an improvement of the already mentioned issues related to security, the AAA infrastructure and P2P frameworks, which will still form the skeleton of the future planned research activity.

4 Research Fields

4.1 Cryptographic Protocols

[KZ05a] proposes the use of graphs as basic objects in security protocols. While having all the functionality of their number based counterparts; such protocols can have extended capabilities, especially useful in the field of verification and analysis. The scalability and transitivity for graph related properties allow for addressing protocols of increasing complexity. These features also cater for new challenges in the future, for instance ones resulting from a quantum computing paradigm.

A model of Boolean neural network is proposed as a substitute of a block cipher. Such a network has functionality of the block cipher and one additional advantage: it can change its cryptographic properties without reprogramming, by training the network with a new training set. The construction of the network is presented with an analysis of the applied binary transformations. Also three methods of training the network (what corresponds to the re-keying of a block cipher) are presented. Their security and effectiveness are analyzed and compared. [KK05a], [KK05b], [KK06a], [WUT5]

A new agent-based scheme for secure electronic voting is proposed in [ZK06a]. It is universal and can be realized in a network of stationary and mobile electronic devices. The proposed mechanism makes possible to implement a user interface simulating traditional election cards, semi-mechanical voting devices or utilize purely electronic voting booths. The security mechanisms applied in the system are based on the verified cryptographic primitives: the secure shared secret scheme and Merkle's puzzles. Due to pre-computations at the stage of agents' generation, the voter must do almost no computations. The proposed distributed trust architecture makes the crucial stage of sending votes elastic, reliable, and effective.

4.2 Anonymity Protocols

Protocols that enable user anonymity will become a major research focus. Governments are required to establish ballot voting in secret, but at the same time they protect the state, and therfore defend crime and terrorist activities. Powerful attackers challenge these protocols e.g. with traffic analysis. The anonymity protocols must withstand these attacks for the sake of freedom speech.

4.2.1 Taxonomy of anonymity protocols

Network communications require special protocols to ensure anonymity, e.g. the hiding of communication relationships. In any network, routers and therefore also attackers are capable to discover relations between sender and receivers. Anonymity protocols route messages through an overlay network, which hides communication relationships. The so-called mixer nodes "mix up" many incoming connections with many outgoing connections, so that an advisory cannot easily determine the actual routing of a single observed message. The anonymity set is enlarged, i.e. the proof that a sender originated a certain message is prevented.

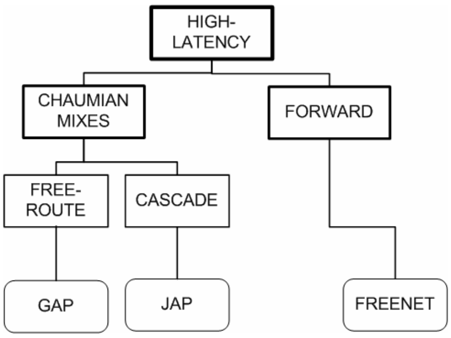

Figure 4.2.1: High Latency Anonymity Protocols.

This work classifies existing anonymity protocols [UP1]. The two main categories follow from the delay that effects out of anonymous message delivery. High-latency (HL) protocols (cf. Figure 4.2.1) gain a high degree of anonymity by mixing large number of packets. This is accomplished by delaying incoming packets and shuffling their order before sending them onto their corrrsponding route. The reason to do so, is to prevent leaking path information to an powerful advisory, that taps all outgoing connections. HL protocols enable information control, i.e. powerful attacks can be sensed. E. g. an advisory wants to learn a path to an anonymous receiver by sending large amounts of data. The anonymity overlay will disregard fast message delivery, because the increased level of traffic could be observed and might offend the anonymity of the receiver. A sample HL application is anonymized EMail. Engineered HL Protocols are Gap, JAP (AN.ON) and Freenet.

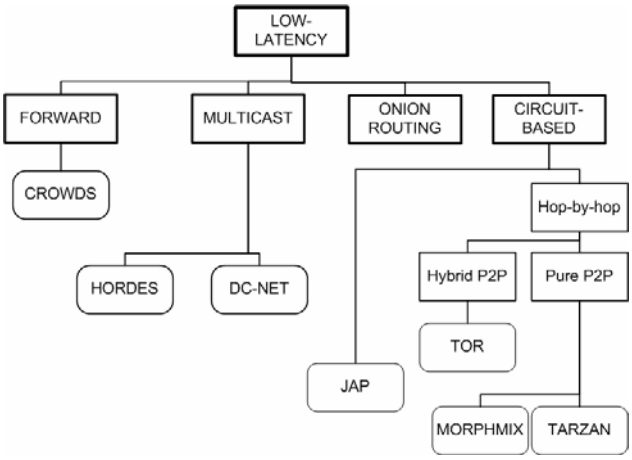

Figure 4.2.2: Low Latency Anonymity Protcols.

For communications like web browsing, interactive dialogs round-trip-times in the magnitude of many seconds are inacceptable. Low Latency (LL) protocols shrink down additional delays. Additional measures like dummy traffic protect the anonymity of the participants. The route establishment distinguishes four different classes (cf. Figure 4.2.2): forward networks (sender constructs route), multicast, onion routing and circuit-based. The last approach establishes virtual circuits in advance, which can be utilized by muliple communication channels. Recent applications use LL protocols for anonymous web service retrieval (crowds) and peer-to-peer based anonymization overlay (TOR).

4.2.2 An electronic voting system supporting vote weights

Electronic voting protocols should respect some basic properties of elections, namely accuracy, democracy, privacy and verifiability [CC97]. One of those properties, democracy, states that "*each eligible voter is allowed to vote and to vote at most once*". This property is a normal requirement in most electoral processes but in some scenarios the votes from some persons have, or should have, a different weight than the other votes. However, as of today we have no knowledge of electronic voting systems with support for weighted votes.

Supporting weighted votes means that, when voting, a voter's vote is worth ***w*** votes. To implement this service in REVS (a Robust Electronic Voting System), several requirements were considered. The basic requirement was to minimize the modifications on the protocol of REVS, in order to reduce the probability of introducing new vulnerabilities in the final protocol. Other more specific requirements were scalability, efficiency, usability and anonymity.

REVS uses RSA [RSA78] keys and Chaum's algorithm [Chaum84] for blindly signing votes from authorized voters. For supporting weights we extended this behavior by using sets of RSA keys for the signing process. But, for saving time and space, we used sets of RSA keys sharing the same modulus. As far as we know, this was never used before.

Our solution for supporting weighted votes was implemented in the code of REVS, which is publicly available[1]. REVS is fully implemented in Java, which makes its deployment very easy.

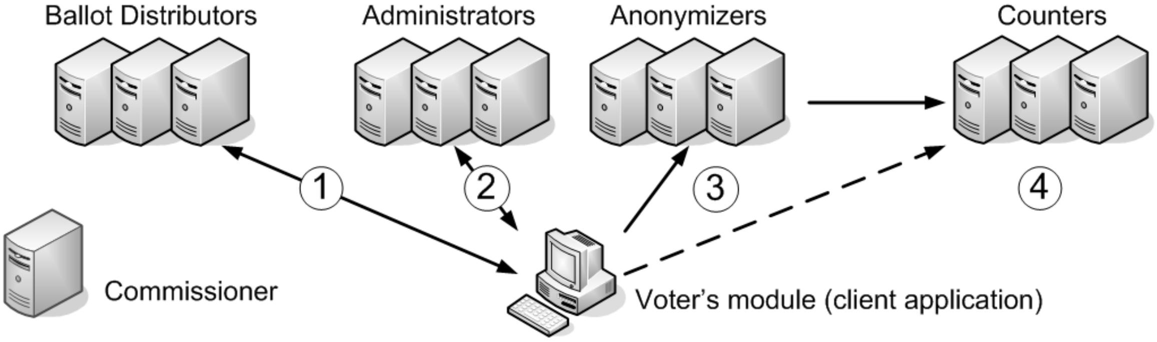

Figure 4.2.3: Extended REVS architecture.

REVS is a blind-signature based voting system designed for secure and robust electronic voting [JZF03], [LJZ+04], [Joaq05]. The REVS architecture, depicted in Figure 1, includes a client application, an electoral Commissioner, and a set of electoral servers: Ballot Distributors, Administrators, Anonymizers and Counters. All electoral servers can be arbitrarily replicated for improving load balance, availability or for preventing collusion-based frauds. Valid votes can be cast repeatedly in several Counters, and even in the same Counter, without affecting the final tally. Figure 1 also presents REVS' protocol steps: (1) bulletin download; (2) voter authorization and vote blind signing; (3) vote submission; and (4) vote counting.

[1] http://www.gsd.inesc-id.pt

Solutions

The basic idea of this work is to give a weight to a vote (or to a voter) and, at some point in the system, multiply the vote by its weight. We chose to cast different signatures on votes for different weights. For each of the N Administrators are given W different signing keys, one for each possible weight, and the knowledge of the weight, w, for each voter. Furthermore, Administrators return to a voter the weight bound to its vote by the Administrator's signature. This solution requires minor changes in the protocol.

The Counters are given $N \times W$ different validation public keys (WKpub table), one for each Administrator and possible weight. For each vote they use a set of N public keys, corresponding to the signing keys representing the same weight. When voters download a bulletin for a particular election they also get their weight and the public keys of all Administrators bound to the weight or, otherwise, the WKpub table used by Counters.

The knowledge of weights bound to keys does not provide information on specific voters; and the knowledge of a voter's weight is official knowledge. This way, except in special circumstances, privacy is ensured.

Optimizations

The number of Administrator's asymmetric key pairs grows proportionally with the number W of weights. This has an impact on scalability, both in the generation and storage of $N \times W$ key pairs. However, the production of multiple RSA signing keys has an opportunity to minimize this scalability issue. Namely, the process for creating W RSA keys for a single entity can create the modulus, n, once and latter use the same n for making all RSA keys.

Using the same modulus n for all key pairs of each Administrator has several advantages. First, we save computational time and space when computing the key pairs, since only two large prime values, p and q, need to be generated per Administrator. Second, we save memory and bandwidth for storing and transmitting the WKpub table.

This optimization cannot be extended to encompass all Administrators´ key pairs; because when we have several d values for the same modulus n, all d values must be known only by the key pair owner. Otherwise, the owner of one d value could discover all other d values using the common modulus attack [Simm83], [MOV01].

Computing blind signatures using different key pairs

The voter's application only gets the voter's weight in the replies of Administrators. But this raises a problem, because the Chaum's RSA-based blind signature scheme used in REVS requires the voter knowing in advance the key pairs that Administrators will use (thus, knowing in advance the voter's weight) according to the algorithm.

We handled this problem by changing the blind signature computations and not the protocols messages. Given the fact that all key pairs of an Administrator have the same modulus n, the process can use all W public keys for blinding. Then, unblinding is done with W-1 public keys, where the key not used is the key of the voter's weight.

When we have a single weight (W=1), it can be shown that the calculations are exactly the same that were performed in the original REVS system.

Security evaluations

The security of REVS was already evaluated and discussed when it was proposed (cf. [JZF03], [LJZ+04]). Our solution in this work, in terms of security, is capable of enforcing a correct use of vote weights, but presents some privacy issues that may appear when small sets of voters share the same weight. Furthermore, the shared modulus optimization for the RSA signing keys does not, as far as we can see, introduce new vulnerabilities in the voting protocol. Namely, all the known shared modulus attacks do not apply to our protocol.

Conclusions and future work

Our solution relies on using sets of signing key pairs to represent the different weights allowed in an election. We also presented a performance enhancing solution for making the, sometimes large, set of RSA signing key pairs from the same modulus.

To the best of our knowledge, this is the first electronic voting system supporting vote's weights and also the first usage of optimizing the ***W*** RSA key pairs per entity.

Regarding the requirement of anonymity, there is still a problem for the case of a single voter with a weighted vote. This is a fundamental problem, since it also exists in paper-based elections. We tried to find a solution to this problem without interfering with the basic characteristics of REVS, but at the end we rejected all the ideas. Consequently, and in the context of REVS, our main issue for future work is to deal properly with this privacy issue.

4.2.3 Protection of mobile agents against traffic analysis

[KKK04], [WUT21] provide a description of a traffic analysis problem. We start from the real-life origins of this type of attack. Then we provide adversary models and assumptions on the network. Next, we outline few instances of possible attacks. Keeping high level of abstraction allows us to discuss traffic analysis prevention for various types of abstract networks and paradigms, for instance: packet networks, wireless environment, ad-hoc networks, real-time systems and mobile agent systems. We describe standard countermeasure (padding, routing) and discuss their limitations. Next, traffic analysis prevention metric is outlined. We summarize countermeasures with discussion of tradeoffs, which are inevitably associated with them. In addition, we discuss how excessive use of countermeasures against traffic analysis produce side channels, which will benefit the attacker.

4.3 Authentication

Authentication, the process of verifying the identity of a network user, still remains an important research topic. Mobility and group communication have new requirements. Man-in-the-middle attacks can still gain knowledge and then bypass some authentication mechanisms. New internet devices have restricted capabilities, so that they cannot participate in strongly secured contexts. A new trend are economic security methods that adopt to the existing resource apabilities.

4.3.1 Anonymous authentication of mobile agents

The mobile agent systems have been well known for years, but recent developments in the mobile technology (mobile phones, middleware) and the artificial intelligence created new research directions. Currently being widely used for the e-commerce and network management are entering into more personal areas of our life, e.g., booking airline tickets, doing shopping, making an appointment at the dentist. Future agents are becoming more like our representatives in the Internet than simple software. To operate efficiently in their new role they need to have the same capabilities as we do, showing their credentials when required and being anonymous when needed. Still they have to fulfill all security requirements for agent systems, including confidentiality, integrity, accountability, and availability. The paper [ZK04a] focuses on providing mobile agents with anonymity and privacy. The proposed schemes are based on different cryptographic primitives: the secret sharing scheme and the zero-knowledge proof. The paper also includes a discussion of security of the proposed schemes.

4.3.2 Anonymous group authentication

[ZK05b], [WUT15] provide a description of a new protocol for group authentication. With a recent development of networking grows an users' demand for anonymity. On the other hand, all service providers, due to the legal regulations have to be able to exactly trace an entity that performed every single action, sent a specific data and so on. Finding a reasonable trade-off between these two requirements is quite hard. In this paper we propose a protocol that provide a user within a group with the anonymity (for outside world the users within a group cannot be identified) and when needed provide a trusted authority with a possibility to identity each user.

4.3.3 Toward Adjustable Lightweight Authentication for Network Access Control

The increasing use of Internet access networks raises the demand for secure and reliable communication for both users and businesses. Traditionally, the aim has been to provide the strongest possible security. However, with the demand for low-power computing it has become desirable to develop security mechanisms which efficiently utilize available resources [Joh05]. The tradeoff between performance and security plays an important role.

In general, strong security is added even if there is no attack. The implementation of strong and resource demanding security often implies more than a secure system; it may deteriorate the performance of a device with limited resources and pave the way for new threats such as resource exhaustion. It is, therefore, unwise to use strong cryptographic algorithms for devices with limited resources in the absence of an adversary. It is more efficient to begin with lightweight security, taking further measures when an attack is detected.

4.3.4 Authentication in P2P networks and mobile ad-hoc networks (MANETs)

[WZK05b], [WUT17] describe a new protocol for authentication in Peer-to-Peer systems. The protocol has been designed to meet specialized requirements of P2P systems, such as lack of direct communication between peers or requirements for controlled anonymity. At the same time, a P2P authentication protocol must be resistant to spoofing, eavesdropping and playback, and man-in-the-middle attacks. The protocol is studied for a model P2P storage system that needs to implement file access rights.

The pervasiveness of wireless communication recently gave mobile ad hoc networks (MANET) a significant researcher's attention, due to its innate capabilities of instant communication in many time and mission critical applications. However, its natural advantages of networking in civilian and military environments make them vulnerable to security threats. Support for anonymity in MANET is an orthogonal to security critical challenge we faced in this paper. We propose a new anonymous authentication protocol for mobile ad hoc networks enhanced with a distributed reputation system. The main objective is to provide mechanisms concealing a real identity of communicating nodes with an ability of resist to known attacks. The distributed reputation system is incorporated for a trust management and malicious behavior detection in the network. The end-to-end anonymous authentication is conducted in three-pass handshake based on an asymmetric and symmetric key cryptography. After successfully finished authentication phase secure and multiple anonymous data channels are established. The anonymity is guarantied by randomly chosen pseudonyms owned by a user. Nodes of the network are publicly identified and are independent of users' pseudonyms. In [CK06a], [WUT19] we presented an example of the protocol implementation.

4.4 Integrity

4.4.1 Protection of mobile agents integrity by a method using zero knowledge protocols

The recent developments in the mobile technology (mobile phones, middleware) created a need for new methods of protecting the code transmitted through the network. The oldest and the simplest mechanisms concentrate more on integrity of the code itself and on the detection of unauthorized manipulation. The newer solutions not only secure the compiled program, but also the data, that can be gathered during its journey and even the execution state. Some other approaches base on prevention rather than detection. The papers [ZK05c], [ZK07], [WUT24] describe a new idea of securing mobile agents. The presented method protects all: the code, the data and the execution state. The proposal is based on a zero-knowledge proof system and a secure secret sharing scheme, two powerful cryptographic primitives. The paper also includes security analysis of the new method and comparison to currently most widespread solutions.

4.4.2 A new protocol of data integrity and authenticity for VoIP, using digital watermarking

In [MK06a], [MK06b], [MK06c], [MKc], [WUT29], we propose a new, lightweight, no bandwidth consuming authentication and integrity scheme for VoIP service based on SIP as a signalling protocol. This solution exploits digital watermarking and it is shared password mechanism. Nowadays, there are many applications of this technique, such as solving copyright protection problems, but we propose to use it to secure the transmitted audio and signalling protocol that IP Telephony is based on simultaneously. This solution can be the potential answer to the problem VoIP faces today: finding a scalable and universal mechanism for securing VoIP traffic (voice and the signalling protocol messages) at the same time. It can greatly improve, if we combine it with existing security mechanisms, overall IP Telephony system's security.

4.5 Scalable security

4.5.1 Always Best Security

The overall focus of the thesis [Joh05] is on adjustable and lightweight authentication protocols for network access control (see also Section 4.3.3 Toward Adjustable Lightweight Authentication for Network Access Control). The thesis studies the performance degradation of strong security using empirical tests on IP security (IPSec) with a visual bottleneck indicator based on the time-discrete fluid flow model and throughput histogram differences [JQF+05]. The results emphasize the possibility of a Denial-of-Service (DoS) attack against IPSec itself.

The redundant authentication performed in a Wireless Local Area Network (WLAN) also motivates the development and evaluation of novel lightweight authentication protocols for the link and network layer [WJN04], [ZSW+03], [JNF+02], [JNW+04]. The developed authentication protocols are resource efficient, per-packet based, and robust in terms of handling packet loss. The protocols are further used as part of a hierarchical defense structure, which has been implemented and evaluated, in order to mitigate protocol based DoS attacks [JWQ+06].

Finally, the thesis "Toward Adjustable Lightweight Authentication for Network Access Control" presents the concept of Always Best Security (ABS) [Joh05], [JIF+06] and a practical decision making model based on the Analytic Hierarchy Process. The model takes a number of factors into consideration, including subjective and objective aspects of security in order to select an adequate authentication level. It is a flexible model which formalizes quantitative and qualitative considerations of a defined set of criteria, keeping Quality-of-Service in mind.

4.5.2 Scalable security with elements of economy of security

[GK05a] describes the model for selecting disaster recovery strategies for information system. The risk assessment covers the threats and vulnerabilities related to the problem of losing the availability of information processes in the particular information system model. The analysis takes under consideration the relationships between the components of information system in order to find the risk of availability lost propagation within the system. That is the basis for finding the candidate disaster recovery strategies, which have to fulfil these basic requirements. Such an approach allows shifting these ones, which are basically not suitable for the security requirements of the information system. The preliminary accepted strategies are to be analyzed regarding to the estimated cost of implementation and maintenance. The next phase covers the detailed analysis of confidentiality and integrity risks in the candidate strategies. The level of risk related to the confidentiality and integrity of information processed in the disaster situation using given strategy is to be estimated.

Electronic services in dynamic environment (e.g. e-government, e-banking, e-commerce, etc.), meet many different barriers reducing their efficient applicability. One of them is the requirement of information security when it is transmitted, transformed, and stored in an electronic service. It is possible to provide the appropriate level of security by applying the present-day information technology. However, the level of protection of information is often much higher than it is necessary to meet potential threats. Since the level of security strongly affects the performance of the whole system, the excessive protection decreases its reliability and availability and, as a result, its global security. In [KK05c], [KK05d], [KK05e], [KK05f], [WUT12], we present a mechanism of adaptable security for digital information transmission systems (being usually the crucial part of e-service). It makes it possible to guarantee the adequate level of protection for actual level of threats dynamically changing in the environment. In our model the basic element of the security is the Public Key Infrastructure (PKI) is enriched with specific cryptographic modules.

4.6 Intrusion Detection

Security attacks become a daily thread. Research in the field of intrusion detection searches for new, untrained attacks. New techniques in network protocols help improve their natural robustness, such as VoIP communications.

The use of Intrusion Detection Systems (IDSs) has emerged as a key element in network security. In this paper we present the design and the validation of an Anomaly based Network IDS, named Self Learning Intrusion Detection System (SLIDS), able to identify new ad hoc attacks [ACG+06]. SLIDS has a modular structure, that not only provides flexibility and extensibility features, but also permits to deal with a wide range of attacks, exploiting various vulnerabilities of TCP/IP stack. The paper presents the system architecture, as well as experimental tests carried out to evaluate the performance of SLIDS both with the well known DARPA data set and with actual traffic, highlighting its effectiveness in detecting different kinds of attacks.

5 Conclusions

This deliverable is the last one of the EuroNGI work package WP.JRA.6.3 “Creation of Trust by Advanced Security Mechanisms” and focused on security considerations for Next Generation Internet. An outlook onto the anticipated development within the area of security as perceived by the partners that are active in this work package was provided. Recent project proposals initiated by members of this workshop were described, and recent contributions of the partners as follow-up of the work reported in the deliverables D.WP.JRA.6.3.2—5 were discussed. Areas of special interest include cryptographic protocols, anonymity, intrusion detection, and in particular authentication and integrity protection, which are central to the topic of the work package. The issue of quantifiable security is addressed in a parallel deliverable, D.WP.JRA.6.3.6. Application domains of special interest covered Voice over IP, mobile services and e-voting. In the latter domain, the results of a joint project involving two partners were shown. Regarding architectures, particular attention was paid to Peer-to-Peer (P2P) and ad-hoc networking scenarios.

A major trend for security solutions can be described by a couple of added values such as scalability, self-configuration and quantifiabiliy, targeting “Always Best Security” with minimal user interference in order to yield better acceptance of security solutions. A particular promising area is the combination of P2P and security, both regarding security in P2P systems and P2P as a means for establishing security. In the follow-up Network of Excellence, particular attention will be paid to the convergence of quality perception (WP.JRA.6.1), economy (WP.JRA.6.2) and security (WP.JRA.6.3) in order to provide users with well-performing, well-priced and trustworthy services.

A. Bibliography

[ACG+06] Davide Adami, Christian Callegari, Stefano Giordano, Giada Landi, Michele Pagano. Design, Implementation, and Validation of a Self-Learning Intrusion Detection System, IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation (MONAM 2006).

[Bold06] Bolduan, Gordon. Controlled Anonymity -- Anonymous Communication with Less Abuse Potential. Diploma Thesis. University of Passau, 2006

[CC97] L. Cranor and R. Cytron. Sensus: A security-conscious electronic polling system for the Internet. In Proc. of the Hawaii Int. Conf. on System Sciences, Wailea, Hawaii, USA, 1997.

[Chaum84] David Chaum. Blind signature system. In Advances in Cryptology – CRYPTO '83 Proc., pages 153–153, New York, USA, 1984. Plenum Press.

[CK06a] T.Ciszkowski, Z.Kotulski, ANAP: Anonymous Authentication Protocol in Mobile Ad hoc Networks, X Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2006. pp. 191-203. ISBN 83-918247-8-0. PDF

[CKa] T.Ciszkowski, Z.Kotulski, ANAP: Anonymous Authentication Protocol in Mobile Ad hoc Networks, arXiv.org e-Print archive, (http://arxiv.org/abs/cs.CR/0609016).

[Dure99] B. DuRette. Multiple Administrators for Electronic Voting. Bs.C thesis, 1999.

[FOO92] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A Practical Secret Voting Scheme for Large Scale Elections. In Advances in Cryptology – AUSCRYPT '92 Proc. (LNCS 718), Queensland, Australia, 1992. Springer-Verlag.

[GK05a] A.Gałach, Z.Kotulski, Risk assessment in disaster recovery strategies development, in: R.J. Scherer, P. Katranuschkov, S.-E. Schapke [eds], CIB-W78 2005, *22nd Conference Information Technology in Construction*, Dresden 19-21 July 2005, pp. 455-462. PDF PDFextended ISBN 3-86005-478, CIB Publication No. 304. ITC Digital Library

[Her97] M. Herschberg. Secure Electronic Voting Using the World Wide Web. Master's thesis, MIT, 1997.

[JIF+06] H. Johnson, L. Isaksson, M. Fiedler, and S. F. Wu, A Decision Method for Finding Adequate Authentication, In Proceedings of the International Conference on Systems (ICONS'06), IEEE Computer Society Press, April 2006.

[JNF+02] H. Johnson, A. Nilsson, J. Fu, S. F. Wu, A. Chen and H. Huang, SOLA: A One-bit Identity, Authentication Protocol for Access Control in IEEE 802.11, In Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'02), Taipei, Taiwan, Vol 1, pp. 768-772, November 2002.

[JNW+04] H. Johnson, A. Nilsson, S. F. Wu and F. Zhao, Lightweight Authentication for Bluetooth, In Proceedings of the first International Conference on Mobile Computing and Ubiquitous Networking (ICMU) 2004, NTT DoCoMo R&D Center, Yokusuka, Japan. January 2004.

[Joaq05] Rui Joaquim. A fault tolerant voting system for the internet. Master's thesis, IST/ UTL, February 2005.

[Joh05] H. Johnson, Toward Adjustable Lightweight Authentication for Network Access Control, PhD Dissertation, School of Engineering, Blekinge Institute of Technology, Sweden, December 2005.

[JQF+05] H. Johnson, B. Qaisrani, M. Fiedler, S. F. Wu, and A. Nilsson, Analysis of IPSec Performance, Proceedings of Promote IT 2005, ISBN 91-44-03875, Studentlitteratur, Lund, May 2005.

[JWQ+06] H. Johnson, S. F. Wu, B. Qaisrani, M. Fiedler, and A. Nilsson, Hierarchical Defense Structure for Mitigating DoS Attacks, In Proceedings of the IEEE 5th International Conference on Networking (ICN'06), IEEE Computer Society Press, April 2006.

[JZF03] Rui Joaquim, André Zúquete, and Paulo Ferreira. REVS – A Robust Electronic Voting System. IADIS Int. Journal of WWW/Internet, 1(2), December 2003.

[KK05a] P.Kotlarz, Z.Kotulski, On application of neural networks for S-boxes design, in: P. S. Szczepaniak, J. Kacprzyk, A. Niewiadomski, Advances in Web Intelligence: Third International Atlantic Web Intelligence Conference, AWIC 2005, Lodz, Poland, June 6-9, 2005. Lecture Notes in Artificial Intelligence, LNCS 3528, pp. 243-248, Springer, Berlin 2005. ISBN: 43-540-26219-9. link

[KK05b] P.Kotlarz, Z.Kotulski, Application of neural networks for implementation of cryptographic functions, in: Leszek Kiełtyka [ed.], *Multimedia in Business and Education*, Vol. 1, pp. 213-218, Białystok 2005. ISBN 83-9182218-7-0.

[KK05c] B.Księżopolski, Z.Kotulski, On scalable security model for sensor networks protocols, in: R.J. Scherer, P. Katranuschkov, S.-E. Schapke [eds], CIB-W78 2005, *22nd Conference Information Technology in Construction*, Dresden 19-21 July 2005, pp. 463-469. PDF ISBN 3-86005-478, CIB Publication No. 304. ITC Digital Library

[KK05d] B.Księżopolski, Z.Kotulski, On probabilistic modeling of incident occurrence in electronic processes, in: W. Burakowski, L.Bella [ed.], Proceedings of the 7th NATO Regional Conference on Military Communications and Information Systems RMCIS 2005: Technologies for the Military Transformation, pp. 297-305, ISBN 83-920120-3-8. PDF

[KK05e] B.Księżopolski, Z.Kotulski, On a concept of scaled security: PKI-based model with supporting cryptographic modules, in: J.Wachowicz [ed.], Electronic Commerce Theory and Applications pp. 73-83. Technical co-sponsorship : IEEE, Gdańsk 2005, ISBN 83-88617-42-7. PDF

[KK05f] B. Księżopolski, Z. Kotulski, On a concept of scalable security: PKI-based model with supporting cryptographic modules, in: J.Eder, H-M.Haav, A.Kalja, J.Penjam [Eds.], Advances in Databases and Information Systems, 9th East-European Conference on Advances in Databases and Information Systems, ADBIS2005, pp.221-232, Tallin.2005, ISBN 9985-59-545-9, CEUR vol. 152, ISSN 1613-0073.

[KK05g] K. Kulesza, Z. Kotulski Countermeasures against traffic analysis for open networks, IX Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2005, pp. 129-135 PDF. ISBN 83-918247-6-2

[KK06a] P.Kotlarz, Z.Kotulski, Neural network as a programmable block cipher, in: J.Pejaś, I. El Fray, Kh. Saeed [Eds], ACS 2006. Proceedings of 13th International Multiconference on Advanced Computer Systems, October 18-20, 2006, Międzyzdroje, Poland, Vol. 1, pp. 311-320. ISBN 83-87362-75-1. PDF

[KK06b] P.Kotlarz, Z.Kotulski, Security Analysis of a Neural Network-based Encryption System, *6th International Conference Multimedia in Business and Education*, 25-27 October 2006, Kielce.

[KK06c] B.Księżopolski, Z.Kotulski, Adaptable security mechanism for dynamic environments, *Computers & Security*, Elsevier ISSN: 0167-4048 (in print)

[KKK04] K.Kulesza, Z.Kotulski, K.Kulesza, On mobile agents resistant to traffic analysis, Electronic Notes in Theoretical Computer Science, Volume 142, Pages 1-254 (3 January 2006), Proceedings of the First International Workshop on Views on Designing Complex Architectures (VODCA 2004), Bertinoro, Italy, 11-12 September 2004, Edited by M. ter Beek and F. Gadducci, pp.181-193, Elsevier, ISSN: 1571-0661, link.

[KZ05a] K.Kulesza, Z.Kotulski, Addressing new challenges by building security protocols around graphs, in: B.Christianson, B.Crispo, J.Malcolm, M.Roe, Security Protocols – 11th International Workshop, Revised Selected Papers, Lecture Notes in Computer Science 3364, pp.301-306, Springer, Berlin 2005. ISBN 3-540-28389-7. link

[LJZ+04] Ricardo Lebre, Rui Joaquim, André Zúquete, and Paulo Ferreira. Internet Voting: Improving Resistance to Malicious Servers. In IADIS Int. Conf. Applied Computing 2004, Lisboa, Portugal, March 2004.

[MK06a] W.Mazurczyk, Z.Kotulski, New VoIP traffic security scheme with digital watermarking, Safecomp2006, Lecture Notes in Computer Science 4166, pp. 170 - 181, Springer, Heidelberg 2006. ISBN 978-3-540-45762-6 link

[MK06b] W.Mazurczyk, Z.Kotulski, New security and control protocol for VoIP based on steganography and digital watermarking, Annales UMCS, Informatica, AI 4 (2006), pp. xxx. ISNN 1732-1360. PDF (in printing)

[MK06c] W. Mazurczyk, Z. Kotulski - Covert channel for improving VoIP security. in: J.Pejaœ, I. El Fray, Kh. Saeed [Eds], ACS 2006. *Proceedings of 13th International Multiconference on Advanced Computer Systems*, October 18-20, 2006, Międzyzdroje, Poland, Vol. 1, pp. 361-370. ISBN 83-87362-75-1. PDF

[MKc] W.Mazurczyk, Z.Kotulski, Alternative security architecture for IP telephony based on digital watermarking, arXiv.org e-Print archive, (http://arxiv.org/abs/cs.CR/0506076).

[MKd] W.Mazurczyk, Z.Kotulski, New security and control protocol for VoIP based on steganography and digital watermarking, arXiv.org e-Print archive, (http://arxiv.org/abs/cs.CR/0602042).

[MOV01] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 2001. 5th Printing.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Comm. of the ACM, 21(2), February 1978.

[Simm83] Gustavus J. Simmons. A “weak” privacy protocol using the RSA crypto algorithm. Cryptologia, 7(2):180–182, 1983.

[WJN04] S. F. Wu, H. Johnson, A. Nilsson, SOLA: Lightweight Security for Access Control in IEEE 802.11, IEEE CS Journal “IT Professional”, vol. 6, no.3, pp 10-16, May/June 2004.

[WZK05a] A Wierzbicki, A.Zwierko, Z.Kotulski, A New Authentication Protocol for Revocable Anonymity in Ad-hoc Networks, in: M.H. Hamza [ed.], Proceedings of the IASTED International Conference on Communication, Network, and Information Security, CNIS 2005, November 14-16, Phoenix, Arizona, USA, IASTED Acta Press, Anaheim, USA, pp. 30-35, ISBN: 0-88986-537-X. link

[WZK05b] A Wierzbicki, A.Zwierko, Z.Kotulski, Authentication with controlled anonymity in P2P systems, In: Hong Shen, Koji Nakano [Eds.], Proceedings of the 6th International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT 2005, Dalian, China, December 5-8, 2005. pp.871-

875. IEEE Computer Society, 2005. ISBN 0-7695-2405-2, IEEE Computer Society Digital Library. link

[WZKa] A.Wierzbicki, A.Zwierko, Z.Kotulski, A new authentication protocol for revocable anonymity in ad-hoc networks, arXiv.org e-Print archive, (http://xxx.lanl.gov/abs/cs.CR/0510065).

[ZK04a] A.Zwierko, Z.Kotulski, Mobile agents: preserving privacy and anonymity, in: L.Bolc, T. Nishida, Z. Michalewicz, [eds] Intelligent Media Technology for Communicative Intelligence, Second International Workshop, IMTCI 2004, Warsaw, Poland, September 13-14, 2004. Revised Selected Papers, Lecture Notes in Computer Science 3490, pp. 246-258, Springer, Heidelberg 2005. ISBN 3-540-290-35-4. link

[ZK05b] A.Zwierko, Z.Kotulski, A new protocol for group authentication providing partial anonymity, 1st EuroNGI Conference on Next Generation Internet Networks - Traffic Engineering /NGI 2005 / Rome, April 18-20 2005. in: Next Generation Internet Networks, 2005**,** pp. 356 – 363, ISBN: 0-7803-8900-X (softbound), ISBN: 0-7803-8901-8 (CD-ROM), *Proceedings IEEE*, *IEEEXplore*. link

[ZK05c] Zwierko, Z. Kotulski, Security of mobile agents: a new concept of the integrity protection, IX Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2005, pp.239-249 PDF ISBN 83-918247-6-2

[ZK06a] A.Zwierko, Z.Kotulski, An efficient agent e-voting system with distributed trust, In: Maurice H. ter Beek, Fabio Gadducci, [eds.], Proceedings of VODCA 2006, Second International Workshop on Views On Designing Complex Architectures, Bertinoro, Italy, 16-17 September 2006., pp. 85-101. PDF , to appear: ENTCS, Elsevier

[ZK07] A.Zwierko, Z.Kotulski, Security of mobile agents: a new concept of the integrity protection, arXiv.org e-Print archive, (http://xxx.lanl.gov/abs/cs.CR/0506103).

[ZKb] A.Zwierko, Z.Kotulski, Integrity of Mobile Agents: A New Approach, International Journal of Network Security, 4 (2), pp.201-211, 2007, ISSN 1816-353X (Print), ISSN 1816-3548 (Online)

[ZSW+03] F. Zhao, Y. Shin, S. F. Wu, H. Johnson, and A. Nilsson, RBWA: An Efficient Random-Bit Window-based Authentication Protocol, In Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'03), San Francisco, USA, pp. 1379-1383, December 2003.