Security Framework for Integrated Networks

Ammar Alkassar, *Member, IEEE,* and Christian Stüble
Sirrix AG security technologies, D-66407 Homburg/Saar
Saarland University, Cryptography and Security Research, D-66123 Saarbrücken

***Abstract*— In the last few years extensive efforts have been done to consolidate the manifold network environments. The needed services are integrated in a clearly arranged network and thus, decreasing costs and personnel overhead.**

Research in network and distributed systems security has provided significant contributions for well-known security problems. However, this is mostly done on the cost of expense, scalability and performance.

In this paper, we discuss the limitation of current security mechanisms in heterogenous networks and present a general-purpose security framework for integrated networks which overcomes with the shortcomings of the present situation.

***Index Terms*— Integrated Networks, Multilayer Security, Cryptography**

I. The Quest for Unified Security

The operating environment of military networks has changed drastically during the last decade. NATO and its member nations are continuously rationalizing their communication capabilities [1], making them more flexible and suited to respond to the need for fast, (both large and small) deployments. In this context, several networks with different technical characteristics are employed. Satisfying the requirement for secure multi-services in such environments has become an even greater challenge than in the past.

However, the challenge of a general-purpose, multi-services and integrated network has been already taken up by the ATM-based B-ISDN.

Many technical and industrial contributions favor an IP-based concept for an integrated network, where all services are delivered above the IP-layer and all data is encapsulated within IP-packets. Where this enables cross-domain mobility, there is, for several years, a debate whether IP is a suitable choice as a general-purpose packet-oriented communication protocol. The major argument against IP is the absence of any quality-of-service (QoS) guarantees. Particularly, when delivering services, which require a constant bit rate, e.g. voice or video, QoS becomes essential.

There are many proposals for providing QoS especially in military networks (see [2]), mainly based on the DiffServ and IntServ models, even for upcoming wireless networks (see [3]) and with real-time support [4], [5].

However, most of the proposed approaches only solve parts of the problem but pay no attention to the difficulties of securing real-time services like voice and video without affecting their QoS. Further problems are due to changes in technological developments and user requirements. Traditionally, interoperability has been achieved through the development of interoperable communications equipment that operates over a homogeneous transport infrastructure. Thus, most of security mechanisms in classified networks implement link layer security, e.g., encryption and data integrity. The link layer approach achieves better reliability and efficiency in terms of computing and bandwidth capacities. However, current developments in communications technologies (CDM, TDM, IP, ATM, etc.) have fragmented the infrastructure. This has resulted not only in non-interoperable solutions, but also pointed out the deficiencies of the link-layer approach: firstly, cross-domain mobility cannot be provided at link-layer. Secondly, services in integrated networks should be technology-independent and thus, realizing end-to-end security at link-layer is a difficult task in an heterogenous network environment.

We propose a security framework for integrated networks that both ensures secure end-to-end communication in an heterogenous network environment and provides the essential QoS requirements for real-time services delivery. The proposed framework represents a fundamental shift in the traditional paradigm. In place of the development of individual secure communication products that are designed to interoperate between themselves, the approach defines a secure interoperable architecture that allows any participant with probably different trust base to build interoperable solutions to a common set of architectural and protocol standards. By using this approach, strategic planners are able to interoperate seamlessly with their forward deployed tactical forces as well as to more readily communicate with both their allies and national civilian government counterparts.

Moreover, it minimizes costs by exploiting the rapidly evolving commercial investment in state-of-the-art COTS infrastructures (i.e. cellular). This strategy, coupled with common protocols, ensures that interoperability with legacy systems is maintained.

The rest of the paper is organized as follows: In Section II we analyze the security and functional requirements of the security framework, describe the problems that occur in the considered context and sketch related work. In Section III, we present the proposed architecture and discuss the main mechanisms in Section IV. Last but not least we consider implementational aspects in Section V and conclude with an outlook of further research in Section VI.

Christian Stüble, E-mail: stueble@acm.org
Ammar Alkassar, E-mail: alkassar@ieee.org
The work of A. Alkassar is supported in part by the Konrad-Adenauer Foundation.

II. Requirements Analysis

A. Security Requirements

Traditionally, "security" of a system is related to its capability to enforce a given security policy. The used mechanisms can be grouped into access control and information flow control, while the underlying security objectives can be grouped into the main categories confidentiality, data integrity and authentication:

Access Control manages rights of subjects to objects. The general way to model an access control policy is to define an access control matrix:

$$S \times O \times R \rightarrow \{true, false\}$$

with the set of all subjects S, the set of all objects O and the set of all rights R [6].

Information Flow Control. While access control facilities manage rights between subjects and objects (information containers), information flow control facilities control real information flows between subjects and objects [7], [8]. E.g., in military applications, all *unauthorized* flows of information has to be prevented.

Confidentiality is the main security target and means the service used to keep the content of information secret from all but those authorized to have it. Besides the classic confidentiality of the payload data, the security policy can also define "meta-information" such as time of emission, classification level, final destination address etc. as confidential. Then, hiding these information becomes also an important and challenging task. Establishing confidential ad hoc-links to some unknown-entity, e.g., using collaborative key-agreement protocols like Diffie-Hellman, is somewhat tricky and can only provides secrecy against passive attacks.

Data Integrity and Authentication Authenticity is the property of being genuine. For a message, authenticity is equivalent to integrity of both the message content (data integrity) and of the message origin, and possibly of other meta-information. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. This is not feasible without allocation of additional bandwidth.

B. Functional and Usability Requirements

However, the most secure network is of no use if the fundamental usability requirements with respect to the environment are not provided. Henceforth, the main task is to design a framework that both guarantees the indispensable security requirements and provides the necessary usability and functional requirements. Below, we present an overview of requirements that are, especially in classified or military environments, of remarkable relevance.

Cross-Domain Mobility and Seamless Hand-over: Not only the deployment of network gateways divides the network into many domains. Classic domain borders are cells of mobile telecom or wireless local-access networks. Other dividing lines tear domains into networks with different environments, e.g., in strategic and tactical (network) domain, with different attacker capabilities and trust requirements. Also, networks with different protocol-cores like ATM-based or IP-based networks comprise different domains. Users are prone to roaming across multiple geographically and organizational adjacent domains. Throughout the paper the term "domain" refers to an unique local access network with characteristic security requirements and attacker capabilities, (semi-)autonomous management and enforcement of different (security) policies.

Additionally, in a military network environment nodes are highly mobile under dynamic network conditions. Thus, in this environment mobility management is needed to ensure that nodes can be located quickly and packet delivery operates properly in the presence of mobility of nodes, networks without affecting the ongoing multi-media session.

Thus, seamless hand-over is an important feature, protecting the user from taking notice during any roaming between adjacent domains. Particularly, the current user's security and multi-service environment are kept invariant and thus, enabling an automatic and high-mobility facility, e.g., for mobile military units or even whole headquarters transfered to the theater.

Efficient Cross-Domain Support: Domains of similar network characteristics are treated as realm [9]. Any network application may communicate across multiple realms. This puts an additional burden on the security infrastructure of integrated networks requiring it to be able to adapt to environments with scarce resources in terms of power, bandwidth and jamming-freeness and evolve once more resources become available. Other resources are inherent in the device, e.g. computing performance and size. Various environments could be characterized by different transmission technologies like wireless and protocols.

Thus, it is inevitably to optimize the employed security mechanisms (schemes and protocols) in terms of efficiency, robustness and fault-tolerance, providing universal and scalable efficiency to realize the stipulated security requirements inside each domain as well as between different realms.

Whereas some researchers argue that security gaps are introduced whenever data packets have to pass through different network realms [10], we propose a framework that enables a rupture-free connection with end-to-end security.

Multi-services Requirements: A basic concept of integrated communication networks like ISDN or ATM is to support the uninterrupted delivery of various services, e.g. data, voice and video, and thus, providing an adequate Quality-of-Service (QoS).

Depending on the application QoS is an essential parameter, especially in tactical networks: Digital battlefields have different settings from the existing communication networks and the constantly-changing tactical environment may demand many real-time needs in both data collection and data delivery [11]. Talking about QoS with regards to security, two mainly orthogonal matters are considered: Firstly, data payload has different priority and thus, some packets should have an higher claim on network resources than other packets. Furthermore, there are requirements for multi-level priority and preemption as discussed in [12], [13]. Because of the importance of QoS in military environments, many proposals for Military oriented QoS (M-QoS)-mechanisms [14] have been made on the past

few years.
Secondly, real-time applications delivering voice, for instance, requires a short and constant packet delay. Both requirements of the transmission technology as well as th delivered service have to be considered carefully. Roughly speaking, one could remark that, it is a good practice that the employed security schemes should not affect the QoS more than the transmission technology does itself.
Today's security suites do not take QoS into consideration in an appropriate manner: Either special, adapted and non-inter-operable security mechanisms are employed, e.g., in GSM, ISDN or ATM encryption devices or a completely general-purpose security suite like IP-Sec or TLS is employed disregarding the requirements of that services like low delay or small packeting.
Transparency Condition: The end-to-end paradigm treats the network as a passive, packet-delivery system that may use the lower-layer headers in the packet routing or a circuit-switched system providing a virtual path with out-of-band signaling, but should never change the upper-layer portions of the end-to-end packets or link.
This paradigm should be maintained while employing security gateways at domain borders.
This puts high demands on the used cryptographic schemes, some security mechanisms like integrity-ensuring schemes could not deal with this restriction at all.

III. Basic Concept: Multi-Layer Security Architecture

Basically, we propose a multi-layer security architecture for integrated networks that ensure secure end-to-end communication in an heterogenous network environment. Moreover, the design provides efficient cross-domain mobility, multi-services requirements, transparency and multi-level security.
Layer-Independent Framework: Today's security suites and protocols are developed for certain communication protocols allocated inherently to selected layers (according to the OSI-reference model). For instance, IP-Sec protocol-suite encrypts and authenticates the payload within IP packets at the network layer while the popular TLS security suite allocates its security mechanisms at the transport layer and thus enabling even authenticated sessions. Other security protocols renounce end-to-end security, and employ only link-layer security like many wireless security protocols, e.g. IEEE802.11 WEP.
The link-layer approach is appealing due to technology-adapted and high efficient mechanisms which are often implemented in hardware, requiring less CPU performance. On the other hand, the higher-layer approach provides end-to-end security and independence from communication-protocol and transmission technology.
To dissolve the deficiencies of the single-layer approach we propose a multi-layer alternative in which the security mechanisms are allocated at different layers controlled by the management plane of the security framework.
Thus, both link-layer security mechanisms and higher-layer mechanisms are combined giving rise the benefits of both approaches.
Collaborative Link Layer Protection: The collaborative link layer protection is part of the multi-layer architecture and incorporates essential security mechanisms into the link-layer featuring stable performance and efficiency, e.g. the ciphering mechanisms.
Multi-Layer Integration: Actually, common security suites operate on one layer without collaborating with other protocols or suites on other layers. As a result, double encryption or even triple encryption en route may happen to application payloads. That incurs considerable processing overhead both at the devices and the gateways.

Basically, the proposed architecture *"Unified Security for Real-Time Communications"*(UniSeT) integrates QoS-critical security services like encryption, data integrity and label processing on top of layer one while the non topical security services like entity authentication and key exchange (which are also necessary for encryption and data integrity) are implemented in the upper layer of the OSI reference model.

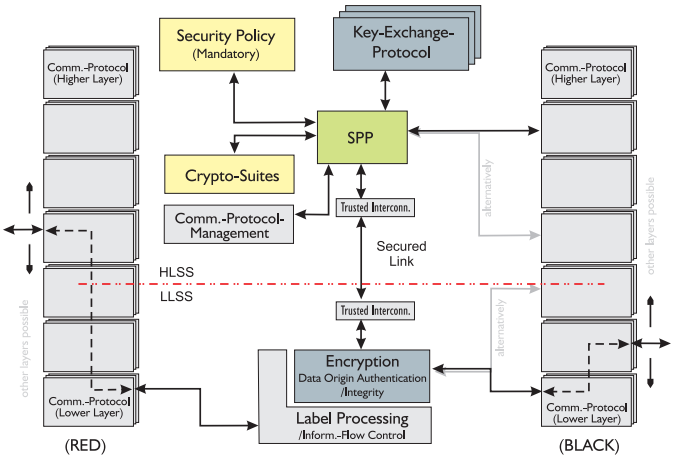

Fig. 1. Arrangement of the security framework

A. Vertical Allocation of the Security Services

More generally, the security mechanisms are mainly arranged within two groups:
Lower-Layer Security Services (LLSS) include all mechanisms that apply to the payload data. Typical LLSS are payload encryption, integrity and data origin authentication schemes and label processing for enforcing information flow control. The LLSS are adapted to the basic communication protocol.
Higher-Layer Security Services (HLSS) group session-oriented security mechanisms that are independent from the particular transmitted data. E.g., schemes for entity authentication, key-exchange protocols and security policies including access control and information flow policies. Therefore, the HLSS are general-purpose. Furthermore, they include the security management of the framework.

The core element of the security framework is the management plane, controlling each of the HLSS, the LLSS and the *Security Signaling Protocol*, *SSP* according to a mandatory security policy as shown in Fig.1

The main task of the SPP is to exchange the signaling information that are necessary for providing end-to-end security services.

To satisfy the transparency condition and to enable the implementation in current network infrastructures, SSP and the HLSS are implemented either using an end-to-end out-of-band or in-band connection. Also, they need a reliable connection similar to the data exchange protocol and should be therefore placed above the transport layer.

B. Horizontal Allocation of Security Services

The relationship between HLSS and LLSS is 1-to-n, i.e. one HLSS-instance can serve several LLSS-instances. Thus, there are two possibilities for placing the security services:

Firstly, all security services are placed in the same device. While the HLSS act system-wide each communication interface is provided with its own LLSS. That enables cross-domain mobility. E.g., a mobile device connected via its GSM-interface to some other entity, say in the Internet, could change seamless to its Wireless-LAN interface still using the same session with its parameters, keys etc.

Secondly, both security services groups are distributed over different devices and connected via the available communications stack. For instance, when building a virtual private network (VPN), i.e., tieing corporate networks and terminals together, a mandatory security policy have to be enforced at the domain borders by security gateways. Because the probable heterogenous corporate network employs different technologies, e.g., an ISDN telecommunication network and an Ethernet-based data-network, several gateways are used. Thus, it is reasonable to have a (physical or logical) domain-wide *Management Unit (MU)*, performing the HLSS whereas the LLSS act directly at the domain borders.

Anyway, the communication between HLSS and the LLSS instances have to be secured: In the first case, by enabling an secure inter-process communication. Both, HLSS and LLSS have to be trusted processes (see also V-C). In the second case, e.g. by using efficient symmetric techniques for encryption and data authentication which could be integrated very efficiently even in embedded systems. However, there are no critical real-time or QoS-requirements.

The main trust source of the system is the *Trust and Policy Management Unit (TPMU)*, which defines security policies and classify both objects and subjects and thus, define trust domains. The TPMU could be part of a hierarchical trust system.

IV. Security Services

The modular architecture provides the ability to include any number of different cryptographic algorithms (within the constraints of the protocols) to allow many trust domains with distinct cryptographic suites such as NATO, national, UN or other coalition forces, etc. without concern over interference or other co-habitation issues.

The logical alignment of security mechanisms to different layers makes it obvious to address the encryption services by adopting the common hybrid encryption paradigm: *cryptographic key exchange* is performed by the first system to provide all participants with same private session key k. Then the data is encrypted by the second scheme using k.

A. Authenticated Key Exchange

The key exchange is performed within the HLSS by the respective module, which acts above layer 5 as mentioned earlier. Therefore, it is conceivable that the SPP messages are delivered over an packet-oriented connection-less network while the encrypted data of a real-time application is delivered over an connection-oriented circuit-switched network. The *key-exchange service* could be delivered using additional network resources i.e. by setting up a new connection (out-of-band) or using the same channel (in-band) by postponing the channel availability (time multiplexing). The first alternative one would use in networks with dynamic allocation of bandwidth like ATM-networks while for fixed-bandwidth systems like ISDN the second alternative is rather used.

B. Encryption

The *encryption service* is done in terms of the OSI-reference model at the top of layer 1 (as part of LLSS) and could be implemented very efficiently in hardware using ASIC or FPGA-chips (see [15], [16]) as shown in Fig.2. That guarantees less in delay and computing resources.

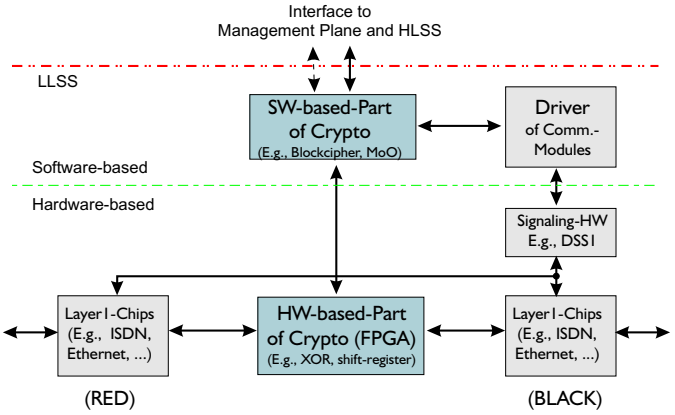

Fig. 2. Hardware-supported design of LLSS

Nevertheless, there are a lot of issues that have to be recognized in the context of telecomunications networks. Particularly it turned out that stream ciphers (or block ciphers used in special block modes like CFB) suits much better the requirements of real-time applications than block ciphers. For instance, the cipher feedback encryption mode (CFB) that turns a block cipher into an appropriate stream cipher allows the transmission of units shorter than the block-cipher lengths (and which is necessary in short-framed networks like ISDN) to be encrypted and sent without delay and message expansion. Furthermore, it provides robustness by the capability of resynchronizing after loss of transmission units (e.g. frame slip). However, stream ciphers like CFB are inefficient in such applications since for every transmission unit, regardless

how short, a call to the block cipher is needed, e.g., for encrypting ISDN payload with 128-bit AES the efficiency only comes to 6,3% which is very unsatisfying. A possible solution, *Optimized Self-Synchronizing Mode of Operation OCFB*, [17] enables both optimal efficiency and robustness.

C. Integrity and Data Authenticity

Incorporating integrity schemes and related data authentication mechanisms into the framework is much more difficult. In principle, without allocating additional bandwidth there is no possibility to embed the authentication information in the payload. However, there are several possibilities to cope with this problem. Firstly, one can simply request additional bandwidth from the network. This is an obvious possibility in packet-oriented networks like IP or ATM. Note, that this additional capacities only needs minimal QoS requirements. Secondly, one can compress the plain-text on-the-fly before encrypting and thus, make additional bandwidth available. This is only possible if the plaintext has a lower entropy than the communication channel. That solution seems to be opportune, e.g., while encrypting voice over fixed channels like in ISDN networks. Another promising possibility is embedding the integrity information in the encoded speech signals [18].

D. Information Flow Enforcement

The ability to enforce a given security policy, and to dynamically adapt enforcement rules to new requirements, has for a long time been a goal of interest of the military and many organizations. Obviously, a multi-purpose security framework for integrated networks should be flexible enough to support different security policies, e.g., Chinese Wall [19] or Multi-Level Security [20]. Since in critical applications, all *unauthorized* information flows have to be prevented, not only access rules but also information flow rules have to be enforced.

Practice has frequently shown that some functions of a secure system always have to be able to bypass access control or information flow rules. E.g., a network packet encryption facility uses information of the input packet to generate a plaintext header of the output header – leading to a deliberated information flow.

Rushby introduces in [21] the idea of a separability kernel containing of trusted processes that are allowed to bypass security rules. This idea can simply be transferred to a security framework (see Figure 3): a small number of trusted components (*security gateways*) separate different terminals or domains from each other. Since security gateways are the only components that can bypass security rules, the correct enforcement of security policies does not depend on the correct behavior of untrusted terminals and users. Obviously, enforcing a security policy is only meaningful if *all* communication channels, e.g., ISDN, ATM and IP, can be controlled by one integrated framework.

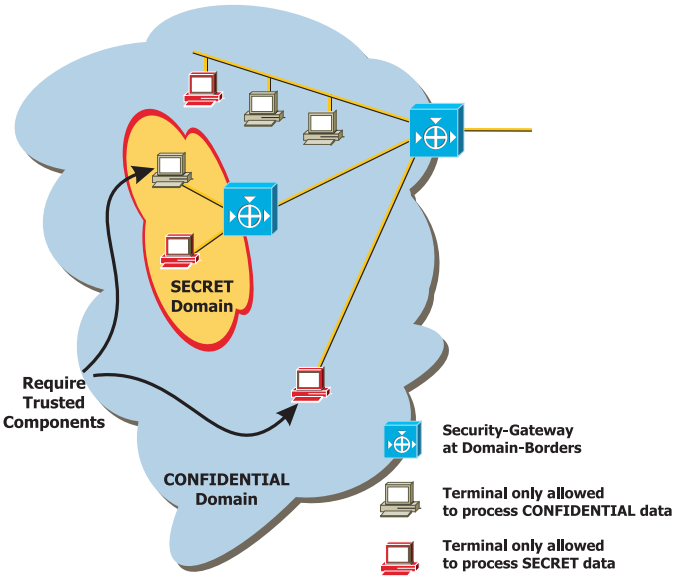

Fig. 3. Security gateways separate domains of terminals at their network boundaries. Trusted terminals are explicitly allowed to break the domain-specific security policy.

V. Security Gateways

Regarding the physical allocation of the services, the framework provides two different realizations of the security gateway: dedicated hosts and a software-based implementation.

A. Dedicated Hosts

A security gateway that is implemented as a dedicated host connects two segregated networks with different trust domains, while the transparency property is provided by ensuring that security gateways enforce the security policy but do not affect the routed data otherwise.

In order to avoid misunderstandings, we point out that the dedicated host security gateway should not be mixed up with a *media-gateway*. A media-gateway ties different realms together. For instance, the wireless-LAN access point links the wireless realm with the IP-network. The payload arrives at the gateway as secured (or unsecured) data, e.g., as ciphertext (or plaintext resp.), and the task of the latter is to perform the media- and protocol-transformation without affecting the included security mechanisms. The media-gateway is not an implicit part of the security framework, but in order to design a universal framework one has to understand how such gateways work and to minimize the effects on the used security mechanisms. [1]

B. Software-based

Alternatively, security services of the security gateway can be implemented as part of the software stack (e.g., operating system) of a client. A software-based implementation has three important advantages: first, it is required whenever the

[1] In some cases it is useful with respect to efficiency to combine Media-Gateways and security gateways. In this case, the Media-Gateway is simply an additional module within the UniSeT-Architecture.

controlled unit is not part of a fixed network, e.g., when using mobile equipment like notebooks, mobile phones or personal digital assistants. Second, the use of software-based security gateway makes sense if only a single unit has to be protected. Third, a software-based realization makes modifications of the network or trust topology more flexible.

Moreover, if the software implementation is based on a secure operating system, it is possible not also to enforce security policies on a host basis, but also on an application basis. E.g., an operation system with multi-level security capabilities allows two applications of different trust domains to be executed in parallel on the same machine.

C. Increasing the Trustworthiness of Security Gateways

While research on protocols, cryptography, languages, user interaction, etc. has provided solutions to a wide range of security related problems, all these solutions depend on the security of the underlying system, especially the operating system. While the integrity of host-based security gateways can be protected by the IT-environment, e.g., walls, locks and doors, conventional operating systems like Microsoft Windows or Linux lack in dependable mechanisms to support security policies. In addition, architectural weaknesses and the inherent insecurity resulting from complexity, make common operating systems insufficient for top-security applications, e.g., for processing secret or top secret classified data. Moreover, common hardware and software architectures do not provide adequate mechanisms, like *secure booting*, that are required to enforce security policies even if local users are untrusted.

There are different approaches to increase security of operating systems: common approaches like SE-Linux [22] and SINA-Linux used by the German Security Agency (BSI) enhance the security by tempering a common Linux operating system. Since the complexity and size of these systems is still very high, we pursue to reduce complexity by another, microkernel based, approach.

The PERSEUS architecture [23] separates the security-critical hardware from the remaining software system (including the conventional operating system) and defines two classed of applications, untrusted and trusted.

Although the security of the conventional operating system (which is now only a task of the PERSEUS security kernel) is not improved, highly-critical applications that are protected by the security kernel can be executed *in parallel* to the conventional operating system. Moreover, PERSEUS allows several instances of the conventional operating system, e.g., with different trust domains, to be executed in parallel.

Another advantage of the PERSEUS platform is the very small trusted computing base (TCB), which enables an efficient evaluation, e.g. according to the Common Criteria . This is especially essential in the treated environment [24].

VI. Conclusion & Outlook

This paper discusses requirements and problems of allocating security functions into integrated networks in heterogenous environments with respect to classical telecommunication services like voice delivery. Furthermore, we present a multi-layer security framework that ensures secure end-to-end communication in an heterogenous network environment and that provides efficient Cross-Domain Mobility, Multi-Services Requirements, Transparency and Multi-Level Security.

Open work is marked by providing inter-operable interfaces that are capable with the various types of networking equipment currently used in the respective networks.

References

[1] *FNBDT: End-to-End Security Workshop*, Royal Military Academy, Brussels, Feb. 2003. NATO NC3A CIS.

[2] R. Goode, P. Guivarch, and M. Stell, "Quality of service in an ip crypto partitioned network," In *MILCOM 2002. 21st Century Military Communications Conference* [25], pp. 1154–1159.

[3] H.B. Parekh, "Improved mobility and qos in tactical wireless ip networks," In *MILCOM 2002. 21st Century Military Communications Conference* [25], pp. 455–460.

[4] Jiejun Kong and Mario Gerla, "Providing real-time security support for multi-level ad-hoc networks," In *MILCOM 2002. 21st Century Military Communications Conference* [25], pp. 1350–1355.

[5] A. Dutta, K.D. Wong, J. Burns, R. Jain, A. McAuley, K. Young, and H. Schulzrinne, "Realization of integrated mobility management protocol for ad-hoc networks," In *MILCOM 2002. 21st Century Military Communications Conference* [25], pp. 448–454.

[6] M. Harrison, W. Ruzzo, and J. Ullman, "Protection in operating systems," *Communications of the ACM*, vol. 19, no. 8, pp. 461–471, Aug. 1976.

[7] Butler Lampson, "A note on the confinement problem," *Communications of the ACM*, vol. 16, no. 10, pp. 613–615, 1973.

[8] Dorothy E. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, MA, 1982.

[9] M. Fisk and W. Feng, "Interactions of realm boundaries and end-to-end network applications," Tech. Rep. Unclassified Report (LAUR) 00-3631, Los Alamos National Laboratory.

[10] Wu chun Feng, "Securing wireless communication in heterogeneous environments," In *MILCOM 2002. 21st Century Military Communications Conference* [25], pp. 1101–1106.

[11] Marek Kwiatkowski, "A concept of differentiated services architecture supporting military oriented quality of service," in *WITSP'2002: The 1st Workshop on the Internet, Telecommunications and Signal Processing*, Univ. of Wollongong, Australia, Dec. 2002, IEEE.

[12] J. Kingston, "Dynamic precedence for military ip networks," In *MILCOM 2000. 21st Century Military Communications Conference* [26], pp. 475–479.

[13] P. Blackmore, P. George, and M. Kwiatkowski, "A quality of service interface for military applications," In *MILCOM 2000. 21st Century Military Communications Conference* [26], pp. 470–474.

[14] M. Kwiatkowski and P. George, "A network control and management framework supporting military quality of service," in *MILCOM 1999. Military Communications Conference*, Atlantic City, NJ, Oct. 1999, vol. 2, pp. 1161–1165, IEEE.

[15] A. J. Elbirt, W. Yip, B. Chetwynd, and Christof Paar, "An FPGA implementation and performance evaluation of the AES block cipher candidate algorithm finalists," in *AES Candidate Conference*, 2000, pp. 13–27.

[16] Ammar Alkassar and Alexander Geraldy, "The SIC!-project: Low-level design of an ISDN-encryption-system," Tech. Rep. 203-A, Saarland University, Saarbrücken, Germany, Feb. 2000.

[17] Ammar Alkassar, Alexander Geraldy, Birgit Pfitzmann, and Ahmad-Reza Sadeghi, "Optimized self-synchronizing mode of operation," in *Proceedings of the 8th International Workshop on Fast Software Encryption*, Yokohama, Japan, Apr. 2001, Lecture Notes in Computer Science, pp. 87 – 91, Springer-Verlag, Berlin Germany.

[18] J.D. Gibson and M.G. Kokes, "Data embedding for secure communications," In *MILCOM 2002. 21st Century Military Communications Conference* [25], pp. 406–410.

[19] D.F.C Brewer and M.J. Nash, "The chinese wall security policy," pp. 206–214.

[20] R. Feiertag, K. Levitt, and L. Robinson, "Proving multi-level security of system design," in *Proc. 6^{th} ACM Symposium on Operating Systems Principles*. ACM, 1977, pp. 57–65, IEEE.

[21] J. Rushby, "Proof of separability: A verifcation technique for a class of security kernels," in *Proc. 5^{th} Int. Symp. on Programming*, Berlin, 1982, pp. 352–362, Springer-Verlag, Berlin Germany.
[22] Peter Loscocco and Stephen Smalley, "Integrating flexible support for security policies into the Linux operating system," Tech. Rep., U.S. National Security Agency (NSA), Feb. 2001.
[23] Birgit Pfitzmann, James Riordan, Christian Stüble, Michael Waidner, and Arnd Weber, "The PERSEUS system architecture," Tech. Rep. RZ 3335 (#93381), IBM Research Division, Zurich Laboratory, Apr. 2001.
[24] Mark Aldrich, "Secured systems and ada: a trusted system software architecture," in *Proceedings of the conference on TRI-Ada '94*. 1994, pp. 282–292, ACM Press.
[25] *MILCOM 2002. 21st Century Military Communications Conference*, vol. 1, Anaheim, CA, Oct. 2002. IEEE.
[26] *MILCOM 2000. 21st Century Military Communications Conference*, vol. 1, Los Angeles, CA, Oct. 2000. IEEE.