Chae Hoon Lim
Moti Yung (Eds.)

LNCS 3325

Information Security Applications

5th International Workshop, WISA 2004
Jeju Island, Korea, August 2004
Revised Selected Papers

Springer

Chae Hoon Lim Moti Yung (Eds.)

Information Security Applications

5th International Workshop, WISA 2004
Jeju Island, Korea, August 23-25, 2004
Revised Selected Papers

Springer

Volume Editors

Chae Hoon Lim
Sejong University
Department of Internet Engineering
98 Gunja-Dong, Kwangjin-Gu, Seoul, 143-747, Korea
E-mail: chlim@sejong.ac.kr

Moti Yung
Columbia University
Department of Computer Science
S. W. Mudd Building, New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2005920313

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.6.5

ISSN 0302-9743
ISBN 3-540-24015-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11352440 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3325

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Lecture Notes in Computer Science

For information about Vols. 1–3291

please contact your bookseller or Springer

Vol. 3412: X. Franch, D. Port (Eds.), COTS-Based Software Systems. XVI, 312 pages. 2005.

Vol. 3406: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVII, 829 pages. 2005.

Vol. 3403: B. Ganter, R. Godin (Eds.), Formal Concept Analysis. XI, 419 pages. 2005. (Subseries LNAI).

Vol. 3398: D.-K. Baik (Ed.), Systems Modeling and Simulation: Theory and Applications. XIV, 733 pages. 2005. (Subseries LNAI).

Vol. 3397: T.G. Kim (Ed.), Artificial Intelligence and Simulation. XV, 711 pages. 2005. (Subseries LNAI).

Vol. 3391: C. Kim (Ed.), Information Networking. XVII, 936 pages. 2005.

Vol. 3388: J. Lagergren (Ed.), Comparative Genomics. VIII, 133 pages. 2005. (Subseries LNBI).

Vol. 3387: J. Cardoso, A. Sheth (Eds.), Semantic Web Services and Web Process Composition. VIII, 148 pages. 2005.

Vol. 3386: S. Vaudenay (Ed.), Public Key Cryptography - PKC 2005. IX, 436 pages. 2005.

Vol. 3385: R. Cousot (Ed.), Verification, Model Checking, and Abstract Interpretation. XII, 483 pages. 2005.

Vol. 3382: J. Odell, P. Giorgini, J.P. Müller (Eds.), Agent-Oriented Software Engineering V. X, 239 pages. 2005.

Vol. 3381: P. Vojtáš, M. Bieliková, B. Charron-Bost, O. Sýkora (Eds.), SOFSEM 2005: Theory and Practice of Computer Science. XV, 448 pages. 2005.

Vol. 3379: M. Hemmje, C. Niederee, T. Risse (Eds.), From Integrated Publication and Information Systems to Information and Knowledge Environments. XXIII, 321 pages. 2005.

Vol. 3378: J. Kilian (Ed.), Theory of Cryptography. XII, 621 pages. 2005.

Vol. 3376: A. Menezes (Ed.), Topics in Cryptology – CT-RSA 2005. X, 385 pages. 2004.

Vol. 3375: M.A. Marsan, G. Bianchi, M. Listanti, M. Meo (Eds.), Quality of Service in Multiservice IP Networks. XIII, 656 pages. 2005.

Vol. 3368: L. Paletta, J.K. Tsotsos, E. Rome, G. Humphreys (Eds.), Attention and Performance in Computational Vision. VIII, 231 pages. 2005.

Vol. 3366: I. Rahwan, P. Moraitis, C. Reed (Eds.), Argumentation in Multi-Agent Systems. XII, 263 pages. 2005. (Subseries LNAI).

Vol. 3363: T. Eiter, L. Libkin (Eds.), Database Theory - ICDT 2005. XI, 413 pages. 2004.

Vol. 3362: G. Barthe, L. Burdy, M. Huisman, J.-L. Lanet, T. Muntean (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 257 pages. 2005.

Vol. 3361: S. Bengio, H. Bourlard (Eds.), Machine Learning for Multimodal Interaction. XII, 362 pages. 2005.

Vol. 3360: S. Spaccapietra, E. Bertino, S. Jajodia, R. King, D. McLeod, M.E. Orlowska, L. Strous (Eds.), Journal on Data Semantics II. XI, 223 pages. 2004.

Vol. 3359: G. Grieser, Y. Tanaka (Eds.), Intuitive Human Interfaces for Organizing and Accessing Intellectual Assets. XIV, 257 pages. 2005. (Subseries LNAI).

Vol. 3358: J. Cao, L.T. Yang, M. Guo, F. Lau (Eds.), Parallel and Distributed Processing and Applications. XXIV, 1058 pages. 2004.

Vol. 3357: H. Handschuh, M.A. Hasan (Eds.), Selected Areas in Cryptography. XI, 354 pages. 2004.

Vol. 3356: G. Das, V.P. Gulati (Eds.), Intelligent Information Technology. XII, 428 pages. 2004.

Vol. 3355: R. Murray-Smith, R. Shorten (Eds.), Switching and Learning in Feedback Systems. X, 343 pages. 2005.

Vol. 3353: J. Hromkovič, M. Nagl, B. Westfechtel (Eds.), Graph-Theoretic Concepts in Computer Science. XI, 404 pages. 2004.

Vol. 3352: C. Blundo, S. Cimato (Eds.), Security in Communication Networks. XI, 381 pages. 2005.

Vol. 3350: M. Hermenegildo, D. Cabeza (Eds.), Practical Aspects of Declarative Languages. VIII, 269 pages. 2005.

Vol. 3349: B.M. Chapman (Ed.), Shared Memory Parallel Programming with Open MP. X, 149 pages. 2005.

Vol. 3348: A. Canteaut, K. Viswanathan (Eds.), Progress in Cryptology - INDOCRYPT 2004. XIV, 431 pages. 2004.

Vol. 3347: R.K. Ghosh, H. Mohanty (Eds.), Distributed Computing and Internet Technology. XX, 472 pages. 2004.

Vol. 3346: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), Programming Multi-Agent Systems. XIV, 249 pages. 2005. (Subseries LNAI).

Vol. 3345: Y. Cai (Ed.), Ambient Intelligence for Scientific Discovery. XII, 311 pages. 2005. (Subseries LNAI).

Vol. 3344: J. Malenfant, B.M. Østvold (Eds.), Object-Oriented Technology. ECOOP 2004 Workshop Reader. VIII, 215 pages. 2005.

Vol. 3342: E. Şahin, W.M. Spears (Eds.), Swarm Robotics. IX, 175 pages. 2004.

Vol. 3341: R. Fleischer, G. Trippen (Eds.), Algorithms and Computation. XVII, 935 pages. 2004.

Vol. 3340: C.S. Calude, E. Calude, M.J. Dinneen (Eds.), Developments in Language Theory. XI, 431 pages. 2004.

Vol. 3339: G.I. Webb, X. Yu (Eds.), AI 2004: Advances in Artificial Intelligence. XXII, 1272 pages. 2004. (Subseries LNAI).

Vol. 3338: S.Z. Li, J. Lai, T. Tan, G. Feng, Y. Wang (Eds.), Advances in Biometric Person Authentication. XVIII, 699 pages. 2004.

Vol. 3337: J.M. Barreiro, F. Martin-Sanchez, V. Maojo, F. Sanz (Eds.), Biological and Medical Data Analysis. XI, 508 pages. 2004.

Vol. 3336: D. Karagiannis, U. Reimer (Eds.), Practical Aspects of Knowledge Management. X, 523 pages. 2004. (Subseries LNAI).

Vol. 3335: M. Malek, M. Reitenspieß, J. Kaiser (Eds.), Service Availability. X, 213 pages. 2005.

Vol. 3334: Z. Chen, H. Chen, Q. Miao, Y. Fu, E. Fox, E.-p. Lim (Eds.), Digital Libraries: International Collaboration and Cross-Fertilization. XX, 690 pages. 2004.

Vol. 3333: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part III. XXXV, 785 pages. 2004.

Vol. 3332: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part II. XXXVI, 1051 pages. 2004.

Vol. 3331: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part I. XXXVI, 667 pages. 2004.

Vol. 3330: J. Akiyama, E.T. Baskoro, M. Kano (Eds.), Combinatorial Geometry and Graph Theory. VIII, 227 pages. 2005.

Vol. 3329: P.J. Lee (Ed.), Advances in Cryptology - ASIACRYPT 2004. XVI, 546 pages. 2004.

Vol. 3328: K. Lodaya, M. Mahajan (Eds.), FSTTCS 2004: Foundations of Software Technology and Theoretical Computer Science. XVI, 532 pages. 2004.

Vol. 3327: Y. Shi, W. Xu, Z. Chen (Eds.), Data Mining and Knowledge Management. XIII, 263 pages. 2005. (Subseries LNAI).

Vol. 3326: A. Sen, N. Das, S.K. Das, B.P. Sinha (Eds.), Distributed Computing - IWDC 2004. XIX, 546 pages. 2004.

Vol. 3325: C.H. Lim, M. Yung (Eds.), Information Security Applications. XII, 472 pages. 2005.

Vol. 3323: G. Antoniou, H. Boley (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 215 pages. 2004.

Vol. 3322: R. Klette, J. Žunić (Eds.), Combinatorial Image Analysis. XII, 760 pages. 2004.

Vol. 3321: M.J. Maher (Ed.), Advances in Computer Science - ASIAN 2004. XII, 510 pages. 2004.

Vol. 3320: K.-M. Liew, H. Shen, S. See, W. Cai (Eds.), Parallel and Distributed Computing: Applications and Technologies. XXIV, 891 pages. 2004.

Vol. 3319: D. Amyot, A.W. Williams (Eds.), Telecommunications and beyond: Modeling and Analysis of Reactive, Distributed, and Real-Time Systems. XII, 301 pages. 2005.

Vol. 3318: E. Eskin, C. Workman (Eds.), Regulatory Genomics. VIII, 115 pages. 2005. (Subseries LNBI).

Vol. 3317: M. Domaratzki, A. Okhotin, K. Salomaa, S. Yu (Eds.), Implementation and Application of Automata. XII, 336 pages. 2005.

Vol. 3316: N.R. Pal, N.K. Kasabov, R.K. Mudi, S. Pal, S.K. Parui (Eds.), Neural Information Processing. XXX, 1368 pages. 2004.

Vol. 3315: C. Lemaître, C.A. Reyes, J.A. González (Eds.), Advances in Artificial Intelligence – IBERAMIA 2004. XX, 987 pages. 2004. (Subseries LNAI).

Vol. 3314: J. Zhang, J.-H. He, Y. Fu (Eds.), Computational and Information Science. XXIV, 1259 pages. 2004.

Vol. 3313: C. Castelluccia, H. Hartenstein, C. Paar, D. Westhoff (Eds.), Security in Ad-hoc and Sensor Networks. VIII, 231 pages. 2005.

Vol. 3312: A.J. Hu, A.K. Martin (Eds.), Formal Methods in Computer-Aided Design. XI, 445 pages. 2004.

Vol. 3311: V. Roca, F. Rousseau (Eds.), Interactive Multimedia and Next Generation Networks. XIII, 287 pages. 2004.

Vol. 3310: U.K. Wiil (Ed.), Computer Music Modeling and Retrieval. XI, 371 pages. 2005.

Vol. 3309: C.-H. Chi, K.-Y. Lam (Eds.), Content Computing. XII, 510 pages. 2004.

Vol. 3308: J. Davies, W. Schulte, M. Barnett (Eds.), Formal Methods and Software Engineering. XIII, 500 pages. 2004.

Vol. 3307: C. Bussler, S.-k. Hong, W. Jun, R. Kaschek, D.. Kinshuk, S. Krishnaswamy, S.W. Loke, D. Oberle, D. Richards, A. Sharma, Y. Sure, B. Thalheim (Eds.), Web Information Systems – WISE 2004 Workshops. XV, 277 pages. 2004.

Vol. 3306: X. Zhou, S. Su, M.P. Papazoglou, M.E. Orlowska, K.G. Jeffery (Eds.), Web Information Systems – WISE 2004. XVII, 745 pages. 2004.

Vol. 3305: P.M.A. Sloot, B. Chopard, A.G. Hoekstra (Eds.), Cellular Automata. XV, 883 pages. 2004.

Vol. 3303: J.A. López, E. Benfenati, W. Dubitzky (Eds.), Knowledge Exploration in Life Science Informatics. X, 249 pages. 2004. (Subseries LNAI).

Vol. 3302: W.-N. Chin (Ed.), Programming Languages and Systems. XIII, 453 pages. 2004.

Vol. 3300: L. Bertossi, A. Hunter, T. Schaub (Eds.), Inconsistency Tolerance. VII, 295 pages. 2005.

Vol. 3299: F. Wang (Ed.), Automated Technology for Verification and Analysis. XII, 506 pages. 2004.

Vol. 3298: S.A. McIlraith, D. Plexousakis, F. van Harmelen (Eds.), The Semantic Web – ISWC 2004. XXI, 841 pages. 2004.

Vol. 3296: L. Bougé, V.K. Prasanna (Eds.), High Performance Computing - HiPC 2004. XXV, 530 pages. 2004.

Vol. 3295: P. Markopoulos, B. Eggen, E. Aarts, J.L. Crowley (Eds.), Ambient Intelligence. XIII, 388 pages. 2004.

Vol. 3294: C.N. Dean, R.T. Boute (Eds.), Teaching Formal Methods. X, 249 pages. 2004.

Vol. 3293: C.-H. Chi, M. van Steen, C. Wills (Eds.), Web Content Caching and Distribution. IX, 283 pages. 2004.

Vol. 3292: R. Meersman, Z. Tari, A. Corsaro (Eds.), On the Move to Meaningful Internet Systems 2004: OTM 2004 Workshops. XXIII, 885 pages. 2004.

Preface

The 5th International Workshop on Information Security Applications (WISA 2004) was held on Jeju Island, Korea during August 23–25, 2004. The workshop was sponsored by the Korea Institute of Information Security and Cryptology (KIISC), the Electronics and Telecommunications Research Institute (ETRI) and the Ministry of Information and Communication (MIC).

The aim of the workshop was to serve as a forum for new conceptual and experimental research results in the area of information security applications from the academic community as well as from industry. The workshop program covered a wide range of security aspects including cryptography, cryptanalysis, network/system security and implementation aspects.

The program committee received 169 papers from 22 countries, and accepted 37 papers for a full presentation track and 30 papers for a short presentation track. Each paper was carefully evaluated through peer review by at least three members of the program committee. This volume contains revised versions of 36 papers accepted and presented in the full presentation track. Short papers were only published in the WISA 2004 preproceedings as preliminary versions and could be published elsewhere as extended versions.

In addition to the contributed papers, Professors Gene Tsudik and Ross Anderson gave invited talks, entitled *Security in Outsourced Databases* and *What Does 'Security' Mean for Ubiquitous Applications?*, respectively.

Many people helped and worked hard to make WISA 2004 successful. We would like to thank all the people involved in the technical program and in organizing the workshop. We are very grateful to the program committee members and the external referees for their time and efforts in reviewing the submissions and selecting the accepted papers. We also express our special thanks to the organizing committee members for making the workshop possible. Finally, we would like to thank all the authors of the submitted papers and the invited speakers for enabling an interesting workshop program.

December 2004

Chae Hoon Lim
Moti Yung

Organization

Advisory Committee

Man Young Rhee	Seoul National Univ., Korea
Hideki Imai	Tokyo Univ., Japan
Chu-Hwan Yim	ETRI, Korea
Bart Preneel	Katholieke Universiteit Leuven, Belgium

General Co-chairs

Pil Joong Lee	POSTECH/KT, Korea
Sung Won Sohn	ETRI, Korea

Steering Committee

Kil-Hyun Nam	Korea National Defense Univ., Korea
Sang Jae Moon	Kyungpook National Univ., Korea
Dong Ho Won	Sungkyunkwan Univ., Korea
Sehun Kim	KAIST, Korea

Organization Committee

Chair	Kyo Il Chung	ETRI, Korea
Finance	Im Yeong Lee	SoonChunHyang Univ., Korea
Publication	Ji Young Lim	Korean Bible Univ., Korea
Publicity	Hyung Woo Lee	Hansin Univ., Korea
Registration	Jae Cheol Ha	Korea Nazarene Univ., Korea
Treasurer	Hyungon Kim	ETRI, Korea
	Sang Choon Kim	Samchok National Univ., Korea
Local Arrangements	Jae Kwang Lee	Hannam Univ., Korea
	Khi Jung Ahn	Cheju National Univ., Korea

Program Committee

Co-chairs	Chae Hoon Lim	Sejong Univ., Korea
	Moti Yung	Columbia Univ., USA
Members	Giuseppe Ateniese	Johns Hopkins Univ., USA
	Tuomas Aura	Microsoft Research, UK
	Feng Bao	Institute for Infocomm Research, Singapore
	Colin Boyd	QUT, Australia
	Dario Catalano	ENS, France
	Kijoon Chae	Ewha Womans Univ., Korea
	Gene Itkis	Boston Univ., USA
	Jong Soo Jang	ETRI, Korea
	Yonghee Jeon	Catholic Univ. of Daegu, Korea
	Jonathan Katz	Univ. of Maryland, USA
	Angelos Keromytis	Columbia Univ., USA
	Seungjoo Kim	Sungkyunkwan Univ., Korea
	Yongdae Kim	Univ. of Minnesota at Twin Cities, USA
	Klaus Kursawe	KU Leuven, Belgium
	Taekyoung Kwon	Sejong Univ., Korea
	Chi Sung Laih	National Cheng Kung Univ., Taiwan
	Kwok-Yan Lam	Tsinghua Univ., China
	Chae Ho Lim	Securitymap, Korea
	Kanta Matsuura	Tokyo Univ., Japan
	Refik Molva	Institut Eurecom, France
	Pascal Paillier	Gemplus, France
	Josef Pieprzyk	Macquarie Univ., Australia
	Zulfikar Ramzan	DoCoMo Labs, USA
	Pankaj Rohatgi	IBM Research, USA
	Bimal Roy	Indian Statistical Institute, India
	Jaechul Ryu	Chungnam National Univ., Korea
	Kouichi Sakurai	Kyushu Univ., Japan
	Diana Smetters	Palo Alto Research Center, USA
	Bulent Yener	Rensselaer Polytechnic Institute, USA
	Okyeon Yi	Kookmin Univ., Korea
	Heungyoul Youm	SoonChunHyang Univ., Korea
	Avishai Wool	Tel Aviv Univ., Israel
	S. Felix Wu	UC Davis, USA

Table of Contents

Network/Computer Security

Public Key Schemes I

Intrusion Detection I

Watermarking/Anti-spamming

Public Key Schemes II

Intrusion Detection II

Digital Rights Management

e-Commerce Security

Efficient Implementation

Anonymous Communication

Side-Channel Attacks

Impacts of Security Protocols on Real-Time Multimedia Communications*

Kihun Hong[1], Souhwan Jung[1], Luigi Lo Iacono[2], and Christoph Ruland[2]

[1] School of Electronic Engineering, Soongsil University, 1-1, Sangdo-dong, Dongjak-ku, Seoul 156-743, Korea
kihun@cns.ssu.ac.kr, souhwanj@ssu.ac.kr
[2] Institute for Data Communications Systems, University of Siegen, Germany
{lo_iacono,ruland}@nue.et-inf.uni-siegen.de

Abstract. International Standards Committees like ITU and IETF have produced several security protocols for real-time multimedia communications. But, applying those security mechanisms may results in non-trivial degradation to real-time communications. This paper investigates the impacts of the standard security protocols on the delay, packet overhead, quality of service, and other features of real-time communications. Some of analytical and experimental results show the suitability of the security protocols.

1 Introduction

Emerging Internet applications transmit multimedia content more broadly. Some examples of existing multimedia applications are audio and video conferencing systems, media on demand and pay per view services, groupware for distributed collaborative working and Internet gaming. Internet multimedia communication is characterized by two different communication paths: one is used to exchange signaling data and the other serves for the transport of the media streams. The transport channels between the multimedia endpoints are established by the signaling path. Available signaling standards are the H.323 [1] components H.225.0 [2] and H.245 [3] of the ITU-T and SIP [4] and RTSP [5] of the IETF. H.323 and SIP are mainly used in IP telephony environments whereas RTSP focuses on media on demand services. The transport path supports the data stream transmission. Since the transmitted data has real-time properties, QoS aspects like delay, packet loss and jitter have to be considered. The reason e.g. why media streams are using the transport services provided by UDP instead of the ones offered by TCP is that the reliability and congestion avoiding mechanisms of TCP cause uncertain delay. Security for Internet multimedia communication has to consider both paths, whereas the signaling path does not demand for additional requirements than conventional Internet applications. The transport path instead does demand for additional requirements. The integration of security services into the media stream transmission has certainly an impact on these parameters.

* This work was supported by Korea Research Foundation Grant (KRF-2001-042-E00045).

C.H. Lim and M. Yung (Eds.): WISA 2004, LNCS 3325, pp. 1–13, 2004.

In this paper we examine different security mechanisms suitable for real-time-oriented IP communication by focusing on the influences on the QoS. First we introduce available standards. Afterwards a list of criteria is presented which is the basis for our investigations and evaluations. In section 3 we present our results concluding what can be realized with the existing approaches and which problems are still open. In section 4 we describe our implementations and make the performance comparison of some security protocols based on communication overhead and error propagation. The results of our investigations are concluded in section 5.

2 Security Standards for Multimedia Communication

Different approaches exist to secure multimedia. IPsec as IP-level security protocol is one possible candidate. SSL/TLS relies on TCP and is therefore not suitable for securing UDP-based multimedia communication. Two more security mechanisms residing at the application layer are the standards H.235 [8] and SRTP [9]. H.235 is part of the umbrella standard H.323 of the ITU-T. SRTP is currently a RFC standard developed within the IETF.

2.1 IPsec

IPsec [6] is standardized within the IETF and provides security services for the Internet Protocol. It is mandatory for IPv6 and optional for IPv4. IPsec offers two security protocols, which can be used independently:

- **Encapsulating Security Payload (ESP)**
  The ESP provides the security services data confidentiality, integrity, anti-replay service, and limited traffic flow confidentiality.
- **Authentication Header (AH)**
  The security services provided by AH are integrity, and anti-replay service.

IPsec can be used to encrypt the media stream (IPsec in transport mode). Within H.323 the H.245 capability exchange messages indicate the support of IPsec. When a media channel is opened the logical channel procedures signals the use of IPsec. Another possibility is to establish a secure channel between two security gateways (IPsec in tunnel mode). In this case the multimedia application is not aware of the SA and therefore no specific signaling is needed. The signaling path (RAS, H.225.0, H.245, SIP, RTSP) can also be secured by IPsec.

2.2 H.235

H.323 [1] comprises a multitude of ITU-T standards with regard to multimedia communication. That makes it a so called umbrella standard. Not only signaling protocols (e.g. H.245, H.225.0) are part of H.323 but also codecs (e.g. G.711, H.261), transport protocols (RTP) and so forth. Finally the H.235 [8] standard describes security services for H.323. H.235 considers security services for both the signaling messages (RAS, H.225.0, and H.245) and the media stream (RTP) transmission. Among the

provided security services usually more than one mechanism or algorithm can be used to achieve a security service. This flexibility can result in non-interoperable implementations. Therefore the ITU-T has specified two security profiles which mandate certain mechanisms and algorithms:

- **Baseline Security Profile**
  The baseline security profile provides message authentication/integrity for the signaling path. An option of the baseline security profile is the voice encryption profile, which offers media stream encryption.
- **Signature Security Profile**
  The signature security profile is suggested as an option suited for large environments where the mutual password or symmetric key assignment is not feasible. The signature security profile provides authentication, integrity, and non-repudiation for the signaling messages by using digital signatures. This profile can be used in conjunction with the Baseline Security Profile.

H.235 enables furthermore a so called media anti-spamming to detect flooding attacks.

2.3 SRTP

The Real-time Transport Protocol (RTP) [11] is the most widely used protocol for real-time data. Nearly every Internet multimedia application relies on RTP to packetize the data output by the codecs. RTP itself doesn't provide security mechanisms except the encryption of the packet payload. The Secure RTP (SRTP) [9] instead provides confidentiality and authentication for RTP as well as for RTCP. Furthermore a protection against replay attacks is included. SRTP is defined as a profile of RTP according to the Audio Video Profiles (AVP) [12] and is registered as "RTP/SAVP".

The encryption of SRTP or SRTCP packets is optional whereas the authentication for RTCP is mandatory but optional for RTP.

3 Comparing Criteria

3.1 Provided Security Services

3.1.1 Scope of Protection

IPsec provides authentication of the IP payload and parts of the IP header and encryption of the IP payload. All layers above benefit by IPsec security services. H.235 considers confidentiality and anti-spamming for RTP only. SRTP offers confidentiality, and message authentication and protection against replay-attacks for RTP and RTCP.

3.1.2 Confidentiality

The Encapsulating Security Payload (ESP) of IPsec provides confidentiality for IP datagrams. The format is designed to support a variety of encryption algorithms. The only mandatory cipher is DES operated in the cipher block chaining (CBC) [15] mode.

To encipher RTP packets, H.235 uses following algorithms in CBC-Mode: RC2, DES, and 3DES.

To encrypt the payload of RTP packets in SRTP a pseudorandom keystream is generated, which is XORed with the payload. AES [14] in Segmented Integer Counter (SIC) mode [15, 16, 17] is the default encryption scheme used to generate the keystream. AES in f8 mode [18] is defined additionally. Both modes operate the block cipher in encryption mode only SRTP is extensible to any other transform.

3.1.3 Data Integrity and Message Authentication

To increase the usability of the statistical values provided by RTCP reports it is very important to ensure the integrity of those values like inter-arrival jitter and packet loss rate. The authenticity of control messages like e.g. the BYE packet is even more important. Therefore message authentication and data integrity is not renounceable. Since real-time multimedia systems require a minimal latency of the media packets, in case of bit errors and lossy encoding in RTP payload, it is more useful to use the damaged data than to discard it as unauthentic instead of retransmission. But it is hard to find a difference between forged contents and simple bit errors.

The security protocol AH within IPSec provides data integrity and message authentication for IP packets. The message authentication is based on the use of Message Authentication Codes (MAC). The AH must support two MAC algorithms: HMAC/MD5 (96 bit) and HMAC/SHA-1 (96 bit) [19]. The MAC is calculated over IP header fields that don't change during transmission and payload.

Integrity of RTP and RTCP streams in H.235 is for further study. If an attacker modifies RTP payloads, the receiver decrypts the encrypted portion of the packet and processes the payload using the media codec whether the packet was modified or not. The anti-spamming mechanism described in section 3.1.6 provides a light-weighted RTP packet authentication.

The authenticated portion of a SRTP packet consists of the RTP header followed by the (encrypted) payload of the SRTP packet. Thus, if the header or the payload is modified, SRTP discards the packet. HMAC/SHA-1 [19] is the default algorithm for providing integrity and message authentication in SRTP. The problem of HMAC/SHA-1 is the fixed and large size of the MAC (20 octets). In SRTP it is truncated to the leftmost 32 bit. [19] mentions, that a truncation to less than the half of the generated output of the HMAC increases the possibility to attack the MAC because of the birthday-attack-bound. SRTP doesn't mandate the MAC to 32 bit. Alternatively other MAC algorithms can be used.

3.1.4 Packet Source Authentication and User Authentication

All of the schemes don't provide a method for packet source authentication. None of the analyzed security protocols has a mechanism to provide source authentication in Multicast configurations. Several schemes have been published and suggested to overcome this problem [20, 21, 22, 23], but without success of standardization.

User authentication in IPsec relies on the main mode of the IKE protocol using digital signatures. Though IPsec supports several authentication manners like pre-