Orhan Ermiş
Thesis Supervisor: Prof. M. Ufuk Çağlayan
Thesis Co-supervisor: Prof. Emin Anarım

NEW DYNAMIC GROUP KEY AGREEMENT PROTOCOLS AND THEIR FORMAL ANALYSIS AND APPLICATIONS

Abstract

The essence of dynamic group key agreement protocols is to help compute a secure key for a group communication with a dynamic set of participants in distributed systems. Dynamic group key agreement protocols are expected to be used in applications such as conference communications, file sharing systems and mobile ad hoc networks. In dynamic group key agreement protocols, the number of participants may vary in time because of participants are joining or leaving a group. The security of such operations is affected by the existence of backward confidentiality and forward confidentiality, respectively. There are a number of problems related to the use of existing dynamic group key agreement protocols: (i) inefficient fault detection in conference communications, (ii) lack of privacy, violation of availability, inefficient participant revocation, dependency for key escrow in file sharing systems and (iii) insecure cluster head selection in mobile ad hoc networks. In this thesis, we first introduce an improved Dynamic Conference Key Agreement Protocol with dynamic group capabilities to provide better performance in fault detection and correction. Then, we show the application of the proposed protocol on Three-Tier Secure File Sharing System with efficient participant revocation. Second, we propose another Key Agreement Protocol with Partial Backward Confidentiality. The partial backward confidentiality property is a novel security property that allows a new participant to compute the last valid group key just before joining the group. In relation to this protocol, we propose a Private File Sharing System. Third, we propose a Group Key Agreement Protocol for Mobile Ad hoc Networks. In this protocol, we introduce the new concept of secure cluster head selection.

PUBLICATIONS

Journals

1. Ermiş, O., Bahtiyar, Ş., Anarım, E., and Çaglayan, M.U., “An improved conference key agreement protocol for dynamic groups with efficient fault correction”, Security and Communication Networks, 8 (7), 1347-1359 SCI-E
2. Ermiş, O., Bahtiyar, Ş., Anarım, E., and Çaglayan, M.U., “Key Agreement Protocol with Partial Backward Confidentiality”, Computer Net- works Journal, Elsevier, Status: (Minor Revision) SCI-E
3. Ermiş, O., Bahtiyar, Ş., Anarım, E., and Çaglayan, M.U., “A Secure and Efficient Group Key Agreement Protocol for Mobile Ad Hoc Networks”, Ad Hoc Networks Journal, Elsevier Status: (Minor Revision) SCI-E

International Conferences

1. Ermiş, O., Bahtiyar, Ş., Anarım, E., and Çaglayan, M.U., “A Comperative Study on the Scalability of Dynamic Group Key Agreement Pro- tocols”, Submitted to International Conference on Availability, Reliability and Security, ARES 2017.
2. Ermiş, O., Bahtiyar, Ş., Anarım, E., and Çaglayan, M.U., “Open problems for group-key agreement protocols on Vehicular Ad-hoc Networks”, Connected Vehicles and Expo, ICCVE, 2013 International Conference on, 828-831.
3. Ermiş, O., Bahtiyar, Ş., Anarım, E., and Çaglayan, M.U., “An improved fault-tolerant conference-key agreement protocol with forward secrecy”, Proceedings of the 6th International Conference on Security of Information and Networks SIN2013, ACM, 306-310.

4. Bahtiyar, Ş, Ermiş, O., and Çaglayan, M.U., “A Framework for Trust Assessment of Security Systems on Flexible Networks”, Submitted to The 15th International Conference on Future Internet of Things and Cloud, FiCloud 2017.
5. Bahtiyar, Ş, Ermiş, O., and Çaglayan, M.U., “Adaptive Trust Scenar- ios for Mobile Security”, International Conference on Mobile Web and Information Systems, MobiWIS 2016, 137-148.
6. Çantalı, G., Ermiş O., Gür, G., Alagöz, F., and Çaglayan, M.U., “Lightweight context-aware security system for wireless Internet access”, Communications and Network Security, CNS 2015 IEEE Conference on, Poster Session, 765-766.

National Conferences

1. Çataklı, T., Ermiş O., Tunca, C., Işık, S. Ersoy, C., and Çaglayan, M.U., “Real Life Implementation and Energy Performance Evaluation of Group Key Exchange Protocols in Wireless Sensor Networks”, Akademik Bilişim, 2016
2. Çantalı, G., Ermiş O., Gür, G., Alagöz F., and Çaglayan, M.U., “Lightweight context-aware security system for wireless Internet access”, Akademik Bilişim, 2016.
3. Erdem , M.D., Ermiş O., Tunca, C., Işık, S. Ersoy, C., and Çaglayan, M.U., “Group Key Management in Wireless Sensor Networks”, Akademik Bilişim, 2015
4. Ermiş, O., Bahtiyar, Ş., Anarım, E., and Çaglayan, “Group Key Exchange Protocols”, Akademik Bilişim, 2014
5. Ermiş O., Anarım, E., and Çaglayan, M.U., “A New Conference Key-Agreement Protocol”, Akademik Bilişim, 2013

Defense Jury Members

1. Prof M. Ufuk Çağlayan	Boğaziçi University (Thesis Supervisor)
2. Prof M. Emin Anarim	Boğaziçi University (Thesis Co-Supervisor)
3. Prof. Fatih Alagöz	Boğaziçi University
4. Prof. Tuna Tuğcu	Boğaziçi University
5. Prof. Albert Levi	Sabancı University
6. Prof. Semih Bilgen	Okan University

Defense Date: 23.05.2017