The SKEMASNET project

Session key management in a spontaneous network

Team name: HGP Team
20094045 - Hyunho Park
20096093 - Gianni M. Ricciardi
20096699 - Pierre Alauzet

Introduction & Motivations

Multiple session key sharing *<- Cryptography problem (Merging two session key into one)*

Let us say that we have 2 spontaneous networks which have their own session key used for creating the network (used for the encryption of all messages in one communication session, and the authentication of members). A session key will be generated by a host and it is unique for every spontaneous network. Then every user of the first network is able to decrypt communications within that network, but not communications of a second network, and vice-versa. When the two networks will merge, we have to find a way to share session keys. Do we create a new session key? Do we choose one of the key or do we merge the 2 session keys? Normally, keys must be distributed securely before encryption can be established in order to get a secure network. But in this case, communication has already been started before merging the two networks. All these questions and issues define our scenario.

Multiple spontaneous networks merging *<- Addressing, Naming problem*

When having two distinct spontaneous networks, question is how can we merge these two into a single network without losing any information? Of course, our goal is to recover all the information of the two previous networks like shared folders, communications, data, etc.

Motivations

In paper [4] we found a comprehensive discussion about the setting of a sp. net. using session keys shared among users, but they don't consider different groups, each one with its own network, desiring to join all together in only one network;

In paper [3] they propose a realistic model about permanent or transient merging of SN, but from a low level point of view (networking, routing, etc.), without considering session keys management.

Problem Definition

Given the scenario described above, the problem we wish to face is the management of security issues when two or more spontaneous networks merge together, and when a spontaneous network is partitioned in two or more groups of users, each one using its own network. In the case of networking established using *spontaneous VPN* (i.e. a VPN among nodes, built using a shared session key), the basic problem is how to manage session keys when two networks merge, in order to build a new VPN in a transparent way for users and applications, and how to have independent networks when subsets of users choose to leave the original network. To provide a full transparency also other aspects, such as naming, addressing and authentication, have to be considered.

Design Considerations

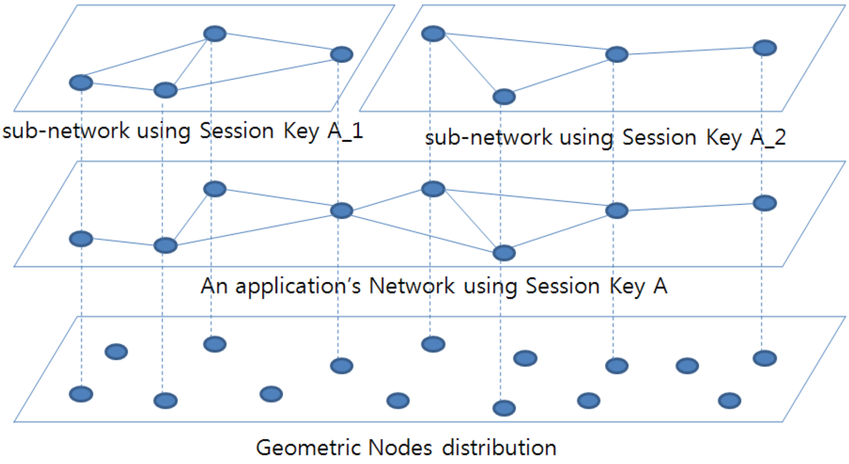
1. Distribute Session key to potential participants.
   - ✓ Advantages of using cryptographic key as session key.
     - ✓ Globally unique session key at any time without reference to central authorities.
     - ✓ A node's session can be remains valid as long as desired.
     - ✓ The node can retain its session key when it moves or the surrounding network topology change.

    - ✓ Multiple session keys can be generated simultaneously.
    - ✓ Independent of centralized public key infrastructure.
  - ✓ For the initial session key a *secure* channel have to be used to transfer the key (e.g. IR, memory card storing the key, etc.)
  - ✓ After the *mother* spontaneous network has been deployed, to create *child* ones the required session keys can be shared using the mother network, before this one disappears.

2. Create a spontaneous network using the distributed session key when an application is starting.

3. When merging two spontaneous VPNs into one, the two different session keys should be merged into one and each member of networks can be continuously access existing resources and newly merged resources using the merged session key.

  - ✓ Necessary a key generating algorithm that allows a key to be merged with other key and make a common key that can be used on the merged network.
  - ✓ Design Addressing, Naming scheme which support network merging.


sub-network using Session Key A_1
sub-network using Session Key A_2
An application's Network using Session Key A
Geometric Nodes distribution

4. When two spontaneous networks have to merge, they could delegate a node in one network to create a new session key: this node can transfer the new key via a secure channel (e.g. an IR connection) to a node belonging to the other network. Then instead of having all remaining nodes connecting to each other (one-to-one as in normal procedure) in order to exchange the new key, we propose to use the two existing networks to propagate the new key. The idea is to have an *automatic* way to propagate the new key, transparent for users and applications.

In a similar way, when some users decide to drop the existing network and deploy a new one, they can share the new key using the former instead of the usual secure channel, in a fast and transparent way. In this case, we will let one of them (the one *delegated* to initialize the new network) to select users belonging to the new spontaneous network.

Approaches

1. Searching for an appropriate key management algorithm.
2. Design Addressing, Naming method using encrypt key.

Expected Result

1. To find a comprehensive solution for session keys management.
2. To let an example application be used during the merging of two spontaneous networks or the partitioning of a spontaneous network into two independent sub-networks.

References

[1] “Establishing trust in pure ad-hoc networks”, Asad Amir Pirzada, Chris McDonald January 2004 ACSC '04: Proceedings of the 27th Australasian conference on Computer science - Volume 26 , Volume 26 (ACM Portal)
[2] “Spontaneous networking: an application oriented approach to ad hoc networking” Feeney, L.M.; Ahlgren, B.; Westerlund, A.; Communications Magazine, IEEE Volume 39, Issue 6, June 2001 Page(s):176 - 181 (IEEE Xplore)
[3] “Implicit merging of overlapping spontaneous networks [mobile ad hoc networks]”, Legendre, F.; de Amorim, M.D.; Fdida, S.; Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th Volume 4, 26-29 Sept. 2004 Page(s):3050 - 3054 Vol. 4 (IEEE Xplore)
[4] “Spontnet: experiences in configuring and securing small ad hoc networks”, Feeney, L.M.; Ahlgren, B.; Westerlund, A.; Dunkels, A.; Networked Appliances, 2002. Liverpool. Proceedings. 2002 IEEE 5th International Workshop on 30-31 Oct. 2002 Page(s):102 - 106 (IEEE Xplore)
[5] “A multiway merging network “, De-Lei Lee, Kenneth E. Batcher Ref : http://www.springerlink.com/content/f072n85t7q5n6757/
[6] http://en.wikipedia.org/wiki/Session_key
[7] http://en.wikipedia.org/wiki/Session_%28computer_science%29
[8] http://www.cytoscape.org/cgi-bin/moin.cgi/Advanced_Network_Merge_and_ID_Mapping
[9] “Virtual Private Ad Hoc Networking”, Jeroen Hoebeke, Gerry Holderbeke, Ingrid Moerman, Bard Dhoedt and Piet Demeester 2006
[10] “Unmanaged Internet Protocol Taming the Edge Network Management Crisis”, Bryan Ford, Massachusetts Institute of Technology, 2004
[11] “Surviving Network Partitioning”, Peter Michael Melliar-Smith Louise Elizabeth Moser 1998

Reading List

[1] “Spontaneous networks: Trust in a world of equals”, Gilaberte, R.L.; Herrero, L.P.; Networking and Services, 2006. ICNS '06. International conference on 16-18 July 2006 Page(s):42 - 42 (IEEE Xplore)
[2] “Friends and foes: preventing selfishness in open mobile ad hoc networks”, Miranda, H.; Rodrigues, L.; Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on 19-22 May 2003 Page(s):440 - 445 (IEEE Xplore)
[3] ”On the design of spontaneous networks using a P2P approach and Bluetooth” Cano, J.; Cano, J.-C.; Manzoni, P.; Ferrandez, D.; Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on 27-30 June 2005 Page(s):125 - 130 (IEEE Xplore)
[4] “Security management for ad-hoc networked resource-limited mobile devices” Sedov, I.; Speicher, S.; Cap, C.; Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th Volume 5, 26-29 Sept. 2004 Page(s):3262 - 3266 Vol. 5 (IEEE Xplore)
[5] “Group Mobility and Partition Prediction in Wireless Ad-Hoc Networks”, Karen H. Wang, Baochun Li, Department of Electrical and Computer Engineering