Autonomic Security for Home Networks

Mohamad Aljnidi and Jean Leneutre

CNRS - UMR 5141 LTCI - ENST - INFRES department
46, rue Barrault - 75013 Paris - France
{Mohamad.Aljnidi, Jean.Leneutre}@enst.fr

Abstract. Home networks are becoming prevalent and interest in their security is increasing. We introduce in this paper an autonomic security model, in which we deal with a home network as an ad hoc network in general, but also we consider its particularities. We show how autonomy is required in different aspects of the proposed solution. Above all, we address autonomy to minimize the intervention of home users, who generally lack experience, in the management of the security infrastructure.

1 Introduction

Such as all communication networks, a home network is prone to security attacks. However, a home network needs special security solutions, taking into consideration its ad hoc nature, in addition to other particularities, including but not limited to, longterm inter-device relations, quasi-static topology, diversity of networking technologies, heterogeneity of devices and inexpert administrators.

We study security of home networks in the context of a research about autonomic security for mobile networks. Our main assumption is that home devices can depend on the existence of each other under time constraints; Because a home is an ultimate meeting point for its mobile devices, we can define T as the longest time for which a device can be away from home. The value of T goes from some hours to a couple of days according to mobility needs or preferences.

Security solutions for ad hoc networks address decentralization and self-organization [1] [2]. This is also required for the special case of home networks [3], but we can impose limitations thanks to home particularities, using the constant T for instance. A Previous research [4], which we generalize and enhance in a part of our work, defines a home network as a longterm community, and eventually proposes a certificate-based decentralized model. Another one [5], which inspired us in terms of security architecture, proposes a generic design for a self-organized security system that can be applied in the case of home networks.

2 Requirements

Devices of a home network are not homogeneous nodes. If we use asymmetric cryptography we will have performance problems with light-duty devices. If we use symmetric cryptography we will loose the chance for a better security implementation in heavy-duty devices.

Requirement $\Re$1: A security process should be able to adapt itself to the cryptographic capabilities of the involved devices.

Devices of a home network may belong to a single resident. In this case, we can consider that there is a trust relationship between devices. We may have the same situation with devices that belong to many residents who trust each other. In general, a home network would be shared by many family members of different ages, and maybe temporary users such as guests. In this case for example, trust is not necessarily complete between devices.

Requirement $\Re$2: A security process should refer, when needed, to authorization rules defined according to levels of inter-device trust.

A home network is subject to variations in device population [4]. According to $\Re$2, and in terms of generalization of [4], we also deal with variations in trust levels. Moreover, our model implies variations in the security management infrastructure. In all cases, a variation might compromise the network.

Requirement $\Re$3: Variations in device population, inter-device trust levels or security management infrastructure should happen securely.

A home device is usually expected to make part of a home network over a long period. In other words, longterm inter-device relations are to be established. It's more efficient to secure the whole relation between two devices instead of securing each communication separately. Besides, we should avoid compromising the network during a relation establishment. On the other hand, according to $\Re$1 and $\Re$2, we need to categorize secure relations according to the differences between the involved devices in terms of capabilities and trust levels.

Requirement $\Re$4: Inter-device secure relations should be securely established and categorized according to device capabilities and trust levels.

We designate certain heavy-duty devices as authority nodes. The main role of such devices is to manage variations. Besides, they may assume a security server role during the establishment of secure relations, especially when light-duty devices are involved. Actually, the constant T assumption is made to prove that authority nodes can always be considered available for relation establishments. This eventually implies a limitation of decentralization, which we can sometimes avoid if the relation establishment is between heavy-duty devices. Anyway, this limitation can be acceptable since relation establishments are occasional in a home network. However, this authority-related type of centralization becomes important if it persists during data exchange in a secure relation.

Requirement $\Re$5: Devices bound by a secure relation of any category should be able to communicate securely without any contact with a third party.

Each device in the home network stores security information for its relations. An authority node stores additional security information to be used as management data during variations and relation establishments. Security management data are updated on an authority node after the variations that involve it. An authority node may not be involved in a variation, but it is expected afterward to have updated its security management data accordingly.

Requirement $\Re$6: Authority nodes should be able to synchronize their security management data after network variations.

3 Device Categories

We categorize home devices according to their computation and storage capabilities ($\Re$1). We suppose that a security platform is to be installed on each home device before adding it to the network. At installation time, a device evaluation module automatically determines the device category according to a security configuration policy (self-configuration [6]). The installed modules work either as applications, or as the constituents of an autonomic security layer supporting the application layer. In both cases, the installed platform is irrespective of the underlying networking technologies.

We consider two device categories: LD (Light-duty Device): the device can support symmetric cryptography and store a limited set of symmetric keys, and HD (Heavy-duty Device): the device can be an LD, and besides, it can support asymmetric cryptography and store its asymmetric key data and a set of certificates and access control policies.

We suppose that the security system can be asked to exclude a certain communication port on a device. This exclusion is used to insecurely communicate with a device that can't even be an LD, which avoids constraints on existing networks. This is also useful for isolation of external communications. Nevertheless, the data exchanged internally with an excluded port is automatically monitored according to a protection policy(self-protection [6]).

4 Security Model

The home network is a set of device communities. A mutual trust relation relies the devices of one community ($\Re$2). A device is in the security perimeter of the network if it belongs to one of its communities. A single HD in a community is selected to be its authority node, while any other HD of it can be a delegated authority node. The loss or breakdown of a main or a delegated authority node is automatically detected, and the system eventually designates another HD as a replacement (self-healing [6]). We suppose that the home network includes one HD at least. This guarantees that there is always an HD that can be designated as a main or a delegated authority node in many communities, especially in temporary cases of emergency. Delegated authority nodes assume security management temporarily while accompanying devices away from the home network coverage for a period greater than T. This way, neither a variation nor a relation establishment will be blocked for more than a period of T. In other words, we can export a home subnetwork with all the functionalities of the security system.

We define nine secure network variations ($\Re$3): Two variations are related to trust levels: community integration or revocation. Three others are related to the security management infrastructure: authority replacement, delegation or delegation termination. And finally, four variations are related to the device population: insertion, removal, banishment or reinsertion. Reinsertion is used to cancel a banishment. An autonomic operation of synchronizing security management data among authority nodes (self-optimization [6]) is carried out within and after variations ($\Re$6).

Secure Authority-Authority Relations (AAR) are automatically created after community integrations, and secure Authority-Device Relations (ADR) are automatically created after device insertions or reinsertions (self-configuration [6]). Creation and distribution of keys and certificates automatically take place when AAR and ADR relations are established.

A secure relation can be created between any two devices of the network ($\Re$4), if they are in the security perimeter, even if they don't belong to the same community. When such a relation is created between two devices, they can communicate securely using the distributed keys or certificates and independently of any other device in the network ($\Re$5). Authentication protocols, which may involve authority nodes depending on device categories, are needed ($\Re$4) for establishing an HHR (HD-HD Relation), an HLR (HD-LD Relation) or an LLR (LD-LD Relation). A relation-dedicated symmetric key is created for an HLR or an LLR, while certificates are used in an HHR.

Authorization policies are exchanged ($\Re$4) in the context of an AAR, and during the establishment of a secure relation between two devices of different communities ($\Re$2). We categorize the result as a Low-Trust Relation (LTR), compared to High-Trust Relations (HTR) between the devices of one community. HD devices can store authorization policies, while an LD asks its interlocutor for permission proofs during communications in the context of an LTR.

5 Conclusion

We presented the main ideas and guidelines of a security model, which is the basis of our first research work in terms of autonomic security solutions for mobile networks. It opens the door for future research tracks, including but not limited to, intra-device autonomic security elements, inter-community autonomic security information negotiation and synchronization, and specification of self-management high-level policies for mobile networks.

References

1. L.M.Feeney, B.Ahlgren, A.Westerlund: Spontaneous networking: an application-oriented approach to ad hoc networking. Communications Magazine, IEEE **39**(6) (2001) 176–181
2. L.Zhou, Z.J.Haas: Securing ad hoc networks. IEEE Network (1999)
3. C.M.Ellison: Home network security. Intel Technology Journal **6**(4) (2002)
4. N.Prigent, C.Bidan, J-P.Andreaux, O.Heen: Secure long term communities in ad hoc networks. In: First ACM workshop on Security of Ad Hoc and Sensor Networks, Fairfax, Virginia (2003)
5. T.Messerges, J.Curkier, T.Kevenaar, L.Puhl, R.Struik, E.Callaway: A security design for a general purpose, self-organizing, multi-hop ad hoc wireless network. In: First ACM workshop on Security of Ad Hoc and Sensor Networks, Fairfax, Virginia (2003)
6. J.O.Kephart, D.M.Chess: The vision of autonomic computing. Computer **36**(1) (2003) 41–52