Role of authorization in wireless network security

Pasi Eronen
Nokia Research Center
pasi.eronen@nokia.com

Jari Arkko
Ericsson Research NomadicLab
jari.arkko@nomadiclab.com

Extended abstract — September 1, 2004

1 Introduction

Wireless security work has largely focused on authentication and key exchange, and using the resulting security association for encryption and integrity protection of individual packets. Authorization has often been considered something that "just happens" at some step, and when authorization is explicitly considered, it is often simplified to sending an authenticated identity and other parameters to a "policy black box" and receiving a yes/no answer back.

We think this picture of authorization is both misleading and insufficient. In this extended abstract, we focus on the role of authorization in public wireless networks. We first illustrate some problems, then discuss the relationship of authorization to, e.g., handoffs and accounting, and finally sketch some ideas about how these issues could be better handled in future protocols.

2 Challenges

2.1 Business aspects

Our first observation is that enforcing policies that are mainly about money ("anyone who pays is allowed") is different from enforcing policies about authenticated identities ("anyone in the RD_Employees group is allowed access"). Much of this difficulty comes from having multiple players and many different business models.

For instance, getting WLAN access might involve not only the client and the AP, but local access network or WISP, a mediating network or a roaming broker, a home ISP, and an enterprise buying the service from the home ISP on behalf of its employees. And these are only for authorization—actually routing the user's IP packets is a separate issue.

Another aspect is that different business models are used. Traditional subscription-based access with postpaid billing is the case often considered, but even, e.g., prepaid is already quite different. And then we get things like credit card payment, buying an access code printed on paper from the coffee shop counter, or paying for the access code by a mobile phone text message.

Practically any protocol includes some usually unstated assumptions about the players and their business models in its design, and new uses often stretch the limits. Even common messages take somewhat different semantics depending on the situation. For instance, within a single ISP a RADIUS Access-Accept message could mean "yes, give access", while in roaming case it might be better interpreted "yes, I agree to pay you the costs of this session according to our contract".

To take an another example, as the result of the "authentication and key exchange" phase, the local WISP or its access points do not necessarily know any authenticated identifier for the client.

2.2 Modular decomposition of protocols

Multi-party systems are often specified as sets of two-party protocols, each of which tries to be as independent as possible from the others. This simplifies specification and gives some flexibility, but the boundaries between the protocols can also lead to difficulties.

For instance, the "802.11i/EAP/RADIUS system" does not authenticate any identifier of the access point to the client. This is perhaps not too surprising, given the roots of EAP and RADIUS in the dial-up world—and that there is not even any good name for the protocol of which 802.11i, EAP and RADIUS are sub-protocols of!

Protocol boundaries also restrict what can be done. For instance, current WLANs do not have any protocol or communication channel for exchanging authorization related information between the client and the AAA proxies.

Current experience suggests that such a channel would be useful for many purposes, including retrieving information about the access network (not necessarily about a single AP), its relationships with roaming brokers, and the services it provides before fully authenticating to the network [2, 3]. This information would be useful for, e.g., deciding which access network to use, which credentials to use, and whether a handoff might be possible.

Since there is no proper channel to use, people have resorted to tricks like using non-integrity-protected fields in EAP, and using EAP for other purposes than authenticating the client, such as passing network information from

This document has been produced partially in the context of the Ambient Networks project. The Ambient Networks project is part of the European Community's Sixth Framework Program for research and is as such funded by the European Commission. All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors' view.

AAA proxies to the client using a proprietary EAP method (iPass, Microsoft's WPS).

2.3 Fast handoffs

Authorization is also related to fast handoffs (in this abstract, meaning handoffs not involving the home AAA server). In particular, the handoff can succeed only if the new AP is covered by the home network's "promise to pay", and in inter-operator case, the new AP accepts the promises of this home network. Currently what exactly is covered by the implicit promise in RADIUS Access-Accept is not explicitly defined; and neither is this information communicated to the client.

Communicating this scope explicitly is not without problems, though: it limits the types of policies that can be used by the home network, since the policy has to be interpreted at the access network, and thus represented in the protocol used between them (such as RADIUS). A simple, if unrealistic, example would be allowing a user to access only APs whose MAC address is even. If technical advances increase the potential scope of handoffs, more realistic policies can also cause problems: for instance, limiting a user to a particular geographic location, access technology, or service usage restrictions. [1]

Handoffs also complicate the issue of authorization and session related state in the network. For instance, session termination initiated by the home network requires keeping track of where the client is. A naive implementation might lead to "chasing the fly around the room" type of situation: the client moves around to avoid disconnection.

2.4 Accounting

Another type of authorization state held at the network is related to accounting. Traditional postpaid, where the accounting records are processed in batches later, can be often considered separately from authorization during the session, but, e.g., prepaid ties these two together.

Depending on the circumstances, prepaid balance reservations may be handled by a separate AAA proxy in the network. In this case, either the scope of fast handoffs is limited by the scope of this proxy, or fast handoff signaling also needs to move the state to the new AAA proxy.

Many existing systems also lack a channel for communication accounting-related information to the client: e.g., showing the user the cost of the service, or redirecting the user to a web page for recharging his or her prepaid account (but without dirty "browser hijack" tricks).

3 Conclusions: Sketching a solution

This is work in progress, and we have not considered yet the details of how the proposal would be implemented in, e.g., 802.11 networks or some future networking technology. However, we have identified some issues that we feel should be taken into account.

Allow reuse of existing user databases and credentials—One of the few issues EAP got right, even though in some circles the common wisdom seems to be, amazingly enough, exactly the opposite: each protocol should use its own credentials.

Avoid hardcoding business models and policies into protocols—This cannot be totally avoided, but keep things flexible (e.g., EAP/802.11i makes credit card payments difficult).

Do not design components in a vacuum—While modular decomposition is important, it is as important to get the decomposition right. Especially the multi-party nature of the problem should be taken into account. Also, keeping security totally separate from the protocol that does the real work (setting up wireless connectivity between systems) is not a good idea: create a protocol for doing the work securely instead (cf. 802.11/11i relationship).

Make the entities involved first class citizens—The entities need to be named; that is, given identifiers that can be used as intended destination of messages, and can be mentioned in messages sent to some third entity.

The identifiers are not necessarily long-term or human readable. Using identifiers that can be authenticated without any infrastructure, in practice meaning hashes of public keys, may simplify the architecture by decoupling user interface issues (e.g., two entities can agree that they are talking to the same third party without knowing a human readable identifier for it), and solving issues such as "MAC address ownership"

Provide proper communication channels between the entities—Entities involved in authorization should be able to communicate both prior, during, and after network attachment. The communication channels should be secure and support efficient multiplexing of different messages.

Be explicit—Explicitly communicate properties and expectations about other parties' actions. For instance, identities of the involved parties (not just the client and AP), their capabilities, and policies that other entities are expected to follow.

Consider authorization state in handoffs—Some kind of signaling that involves other entities than old and new AP, such as a local AAA proxy, may be needed for proper authorization, either during or after the handoff.

Acknowledgments

We would like to thank Hannes Tschofenig, Pekka Nikander, and Vesa Torvinen for interesting discussions.

References

[1] B. Aboba et al., "Extensible Authentication Protocol (EAP) Key Management Framework", work in progress (draft-ietf-eap-keying-03), 2004.

[2] J. Arkko and B. Aboba, "Network Discovery and Selection Problem", work in progress (draft-ietf-eap-netsel-problem-01), 2004.

[3] E. Hepworth et al., "Considerations about Network Selection", IEEE 802.11 WG, document 802.11-04/0691r0, 2004.