

A Proof of Concept Implementation and Evaluation of a Zero Configuration Authentication Option for EAP-TLS

Carolin Latze
Department of Informatics
University of Fribourg
Bd. de Perolles 90
1700 Fribourg
Switzerland

Ulrich Ultes-Nitsche
Department of Informatics
University of Fribourg
Bd. de Perolles 90
1700 Fribourg
Switzerland

Almost all the authentication protocols used in IEEE 802.11 based networks require the distribution or retrieval of user credentials before the first connect of a user. Obviously when talking about commercial public wireless LANs, such a pre-authentication process is absolutely necessary. However, there might be cases when such a preauthentication process does only introduce more complexity. One could imagine a company network where all new devices are registered and whitelisted using their MAC address. Since MAC filtering is not very secure, it might be desired to reconfigure the devices automatically on first connect to use a more secure authentication method like EAP-TLS. In 2007, [1] presented a TLS extension that allows to use the Trusted Platform Module (TPM) Identity certificates as TLS client certificates. Since the TPM is a trusted entity that can be identified uniquely worldwide and since the process of obtaining TPM Identity certificates can be automated, such certificates are perfectly suited for a zero configuration scheme in EAP-TLS. The basic idea behind that scheme is to allow the client to request a new certificate during the TLS handshake after the server sent its list of acceptable Certificate Authorities (CAs).

This talk gives a short introduction into the theory of the EAP-TLS zero configuration option published first in [2]. Furthermore, a (yet unpublished) proof of concept implementation will be shown that allows to evaluate the concept. The implementation has been done using the gnutls TLS library [3] and shows pretty good results regarding performance and usability. Furthermore in order to evaluate the correction of the zero configuration option, a theoretical proof will be presented based on the logic presented in [4].

Bibliography

- [1] C.Latze, U.Ultes-Nische, F.Baumgartner: *Strong Mutual Authentication in a User-Friendly Way in EAP-TLS*, 15th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2007), Split - Dubrovnik, Croatia, September 2007
- [2] C.Latze, U.Ultes-Nitsche, F.Baumgartner: *Towards a Zero Configuration Authentication Scheme for 802.11 Based Networks*, IEEE Conference on Local Computer Networks (LCN 2008), Montreal, Canada, October 2008
- [3] <http://www.gnutls.org>
- [4] N. Durgin, J. Mitchell, D. Pavlovic: *A compositional logic for protocol correctness*, Proceedings of the 14th IEEE Computer Security Foundations Workshop, 2001