Establishing Trust in Heterogeneous Networks

(Ph.D. Forum)

Dominik Schürmann
Institute of Operating Systems and Computer Networks, TU Braunschweig
Email: schuermann@ibr.cs.tu-bs.de

***Abstract*—Many scenarios require confidential communication and protection against active attackers. The way to establish trust between devices and authenticate these networks depends completely on the scenario. In Body Area Networks human biometrics can serve as a shared secret among devices. In real-time voice communication, the ZRTP protocol allows for interactive trust establishment by recognizing the peer's voice. In asynchronous networks, such as email, other interactive mechanisms have been deployed, such as key fingerprint verification.**

In our research, we are analyzing the security and usability of existing trust mechanisms for heterogeneous networks. Furthermore, we are proposing protocol changes and new mechanisms to establish trust between devices. In this paper an overview is given over existing and upcoming research in this area. For synchronous networks, human biometrics, such as human gait or a peer's voice, are used as trust anchors. For asynchronous networks, the usability of interactive public-key verification mechanism are analyzed as trust anchors.

I. Introduction

Many different types of network communication have emerged over the years. On one end of the spectrum, there are asynchronous store and forward networks, such as email. On the other end, there are synchronous networks, such as real-time voice communication or devices worn on the same body. Either way, devices and their heterogeneous networks are getting more pervasive. They all have in common that their communication should be secured to protect confidential data. It is easy to protect against passive eavesdropping by exchanging shared secrets via Diffie-Hellman (DH) based protocols and then using these secrets for a symmetric encryption. However, only a key exchange that has been authenticated protects against active Man-in-the-Middle (MitM) attacks. Non-interactive authentication is traditionally done by operating Public-Key Infrastructures (PKIs) that work as trust anchors by authenticating public keys. Interactive authentication, such as Bluetooth pairing, is often done via PIN-based approaches or out-of-band communication [1], [2].

In our current research we are focusing on establishing trusted and thus authenticated encryption for heterogeneous networks in an ad-hoc manner without PKIs. The goal is to have no single point of trust and make the trust establishment as easy as possible. In case of real-time communication, especially Body Area Networks, we are looking into human biometrics. For asynchronous communication we are analyzing the trade offs and usability issues in public-key fingerprint verification. Alternatively, we envision the usage of a diverse set of third parties, so that even if one is compromised, an attack can be detected.

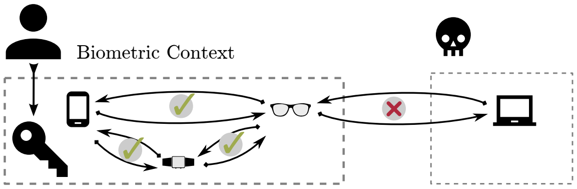


Fig. 1: Biometric context for each person corresponds to one Body Area Network. We propose to use the person's unique gait pattern as the trust anchor.

II. Body Area Networks

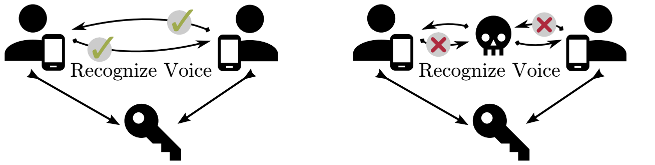
One of the major characteristics of Body Area Networks is the fact that its devices are worn on the same body. Sharing the same physical context means it should be possible to leverage biometric properties unique for this specific body as a trust anchor. We envision spontaneous secure pairing which allows frequent re-pairing (restricted to the time-of-use), and ad-hoc implicit (no manual interaction required) secure authentication bound to an individual. As shown in Figure 1, this should separate the user from active adversaries by generating a shared key that depends solely on the unique biometric property.

Previous research has shown that this should be possible: Cornelius et al. [3] were able to identify devices co-located on the same body and succeeded to show good correlation among all body locations. The authors in [4], [5] employ gait cycles to authenticate a user on his smart-phone by matching the current walking pattern against a previously saved walking template.

In our paper "BANDANA – Body Area Network Device-to-device Authentication using Natural gAit" [6] presented on PerCom 2017, we propose a secure pairing scheme among on-body devices based on common movement patterns due to co-location on the same body. We evaluate its security by statistical analysis of key entropy and provide a technical specification of possible security levels.

III. Real-Time Voice Communication

While it is difficult to retrofit the traditional Public Switched Telephone Network with end-to-end security, it is feasible to protect users of modern VoIP apps. To protect such real-time communication channels, the ZRTP key agreement protocol has been proposed. It is based on the DH key exchange and has been standardized in 2011 as RFC 6189 [7]. Instead of relying on a central PKI, participants are required to compare



(a) The peer's voice serves as the trust anchor

(b) Recognize the peer's voice to prevent active MitM attacks

Fig. 2: ZRTP uses Short Authentication Strings for comparison

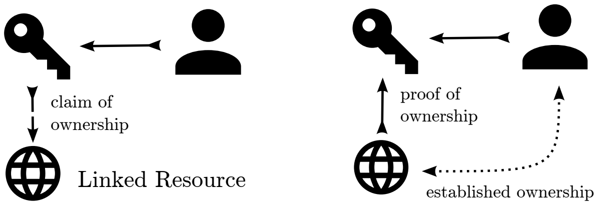
a small number of on-screen characters or words, called Short Authentication Strings (SAS). Thus, the peer's voice is the actual trust anchor in ZRTP and users are required to recognize it from previous conversations (cf. Figure 2a). If done correctly, no one should be able to actively wiretap the call, i.e., perform an unnoticed MitM attack (cf. Figure 2b). The exchanged secrets are utilized to encrypt the stream end-to-end, normally using the SRTP.

While previous research has looked into specific protocol [8] and usability issues [9] in ZRTP, we are currently doing a systematic analysis of desktop and smartphone apps implementing the standard. We uncover issues in their standard conformance by a set of protocol tests and discuss potential areas of improvement to the standard's threat model.

IV. Asynchronous Communication

For asynchronous communication deploying store and forward protocols, such as email, traditional public-key cryptography is implemented. To protect against active MitM attackers, the binding of an email address to a specific public key needs to be verified. If no PKI is involved, this is traditionally done by using public key fingerprints as trust anchors and comparing them manually. While QR Codes can ease this process, fingerprints are also verified via phone calls or exchanged offline via business cards. Here, fingerprints need to be encoded into a human readable representation, e.g., via Hex or Base64 encoding. In "An Empirical Study of Textual Key-Fingerprint Representations" [10] we conducted a study with over 1000 participant evaluating six different textual key-fingerprint representations with regards to their performance and usability. Our findings show that the currently used hexadecimal representation is more prone to partial preimage attacks in comparison to others. Based on our findings, we make the recommendation that two alternative representations should be adopted.

Fingerprints require a manual comparison by each recipient to not rely on a PKI for key verification. We are investigating an alternative idea where a key is not bound to a single PKI. Instead it is linked to several resources on the Internet by mutual proof of control (cf. Figure 3). These proofs can be verified automatically by the recipients and are not bound to a single point of failure. To this end, a URI scheme is introduced which encodes a claim of control over a resource, together with a format for a token to be placed at the referenced site for proof. We will conduct a field study to test the usability and acceptance of our "Linked Identities".



(a) Claim ownership of a resource

(b) Proof ownership using a Linked Identity

Fig. 3: Linked Identities

V. Conclusion

We are investigating interactive and non-interactive mechanisms to establish trust in heterogeneous networks. They are designed to be ad-hoc without central PKIs. We propose new protocols and evaluate existing security and usability aspects.

References

[1] J. Suomalainen, J. Valkonen, and N Asokan, "Security associations in personal networks: A comparative analysis," in *European Workshop on Security in Ad-hoc and Sensor Networks*, Springer, 2007, pp. 43–57.

[2] M. Sethi, E. Oat, M. Di Francesco, and T. Aura, "Secure Bootstrapping of Cloud-managed Ubiquitous Displays," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '14, Seattle, Washington: ACM, 2014, pp. 739–750.

[3] C. Cornelius and D. Kotz, "Recognizing whether sensors are on the same body," in *International Conference on Pervasive Computing*, Springer, 2011, pp. 332–349.

[4] T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," *International Journal of Information Security*, vol. 14, no. 6, pp. 549–560, 2015.

[5] T. Hoang, D. Choi, V. Vo, A. Nguyen, and T. Nguyen, "A Lightweight Gait Authentication on Mobile Phone Regardless of Installation Error," in *Security and Privacy Protection in Information Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July 8-10, 2013. Proceedings*, L. J. Janczewski, H. B. Wolfe, and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 83–101.

[6] D. Schürmann, A. Brüsch, S. Sigg, and L. Wolf, "BANDANA – Body Area Network Device-to-device Authentication using Natural gAit," *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2017, (to appear).

[7] P. Zimmermann, A. Johnston, and J. Callas, *ZRTP: Media Path Key Agreement for Unicast Secure RTP*, RFC 6189 (Informational), Internet Engineering Task Force, Apr. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6189.txt.

[8] K. Bhargavan, C. Brzuska, C. Fournet, M. Green, M. Kohlweiss, and S. Zanella-Béguelin, "Downgrade resilience in key-exchange protocols," in *IEEE Symposium on Security and Privacy (SP)*, May 2016, pp. 506–525.

[9] M. Shirvanian and N. Saxena, "On the security and usability of crypto phones," in *Proceedings of the 31st Annual Computer Security Applications Conference*, ser. ACSAC 2015, Los Angeles, CA, USA: ACM, 2015, pp. 21–30.

[10] S. Dechand, D. Schürmann, K. Busse, Y. Acar, S. Fahl, and M. Smith, "An Empirical Study of Textual Key-Fingerprint Representations," in *25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX: USENIX, Aug. 2016, pp. 193–208.