Poster: Friend or Foe? Context Authentication for Trust Domain Separation in IoT Environments

Markus Miettinen
TU Darmstadt, Germany
markus.miettinen@trust.tu-darmstadt.de

Jialin Huang
TU Darmstadt, Germany
jialin.huang@trust.tu-darmstadt.de

Thien Duc Nguyen
TU Darmstadt, Germany
ducthien.nguyen@trust.tu-darmstadt.de

N. Asokan
Aalto University and University of Helsinki, Finland
asokan@acm.org

Ahmad-Reza Sadeghi
TU Darmstadt, Germany
ahmad.sadeghi@trust.cased.de

1. MOTIVATION

The Internet of Things (IoT) is rapidly emerging, resulting in a growing demand for guaranteeing its security and privacy. Imagine the following scenario: In a not so distant future you have just purchased a number of Internet-of-Things (IoT) appliances for your smart home. You are standing in your living room and would like to have these new devices wirelessly connect to each other and your home network. The set of your own devices in your network constitute your *trust domain*. Most IoT devices are equipped with environmental sensors, e.g., for monitoring ambient luminosity, audio, or temperature. A breach in your trust domain could leak such sensor data, and hence potentially sensitive private information about your behavior and habits, to outsiders.

Therefore, you want to make sure that none of your devices accidentally connect to your neighbor's home network. You also want to make sure that *only your own* devices are granted access to your trust domain. The devices could use appropriate service discovery and key exchange protocols to establish secure communication links with each other and other devices like the home WiFi router. But how can your devices distinguish between other devices that belong to your trust domain and devices of your neighbors that happen to lie within wireless communication range? That is, how can devices in a trust domain (e.g., your home) authenticate each other?

2. PREVIOUS APPROACHES

One approach is to ask user's interaction to facilitate authentication as in Bluetooth Secure Simple Pairing [4]. However, user-mediated "manual authentication" is not appropriate for IoT scenarios for two reasons. First, even a simple interaction requirement quickly becomes burdensome if users have to repeat it separately for dozens or hundreds of devices in their IoT domains such as smart homes. Second, many IoT devices lack the necessary hardware (such as user I/O or NFC peripherals) for manual authentication.

Another approach which is common practice today for admitting a new WiFi-enabled IoT device into a user's domain is to involve a smartphone to assist in the process. The user downloads an app from the device vendor and uses it to connect to the new device over an ad-hoc WiFi connection and transmit WiFi network access credentials thereby allowing the new device to join his trust domain. This approach, however, is vulnerable to an active man-in-the-middle.

One may also try to authenticate IoT devices using similar approaches as done in wireless sensor networks [1]. These approaches are, however, based on pre-distributing key material to devices before deployment. In future IoT environments such key pre-distribution is not feasible. First, IoT devices will be manufactured and shipped by hundreds of different device vendors all over the world. It is not likely that all of them would share mutual security associations required for establishing a common key pool from which to draw pre-distributed keys. Second, different users might be using devices coming from the same vendor, thus sharing the same key pool. It is impossible to distinguish different users' devices based on their pre-distributed keys.

The idea of using shared entropy extracted from ambient context of two co-located devices provides potential solutions for IoT devices authentication [2, 3]. However, existing context-based authentication schemes have limitations that make them unsuitable for IoT settings. They are either distance-critical, or lack a clear feasibility analysis. For example, practical constraints related to the entropy loss incurred by the error-correcting codes were not considered in previous work, and these constraints turn out to be quite strict in these context-based designs.

3. OUR CONTRIBUTION

To overcome the above limitations we propose a scalable context authentication approach for trust domain separation for IoT devices leveraging ambient context information, like audio, sensed by on-device sensors. Our scheme can assist users to securely admit IoT devices into their trust domains with minimal user interaction. Our main contributions are:

WiSec'16 July 18-22, 2016, Darmstadt, Germany

ACM ISBN 978-1-4503-4270-4/16/07.
DOI: http://dx.doi.org/10.1145/2939918.2942422

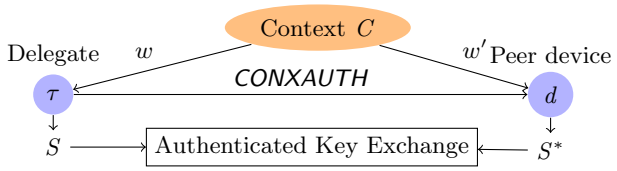

Figure 1: Context authentication and key exchange

- Context authentication approach for trust domain separation in IoT environments utilizing the error correcting capability of fuzzy extractors. Our approach is implemented on Android.
- Security analysis showing strict limits for context entropy and bit similarity. We evaluate our scheme based on empirical data and demonstrate its feasibility.

4. SYSTEM DESIGN

We use context authentication to allow devices to determine that they are co-located in a context C of the user's trust domain $\mathcal{D}$, which is composed of all the user's IoT devices d. By context C, we mean a distinct subspace of $\mathcal{D}$ where the sensed ambient environment like luminosity and audio is similar, e.g., a room in the user's apartment.

We utilize two kinds of devices: context-specific *delegates* τ and a *domain master* M, e.g., the user's smartphone, that is used to manage IoT devices in $\mathcal{D}$. The user assigns delegate τ for each context C of $\mathcal{D}$ by setting up a strong security association between τ and M, e.g., by traditional manual pairing. This is done only once for each context, so the user burden remains manageable. The main adversary of concern are external devices that do not belong to trust domain $\mathcal{D}$ but are located in close proximity of the devices in C so that they can communicate over a proximity channel in the same way as legitimate peer devices.

The key part of our solution is a *context authentication* protocol as depicted in Fig. 1. First, delegate τ and peer device d derive context fingerprints w and w', respectively, from their observations of the ambient context like changes in the noise level or luminosity in C. Since τ and d are co-located in the same context C, these fingerprints will be similar. This similarity is used to authenticate the mutual context by running the CONXAUTH protocol over the wireless channel (e.g., WiFi or Bluetooth). CONXAUTH, uses fuzzy extractors for correcting errors between w and w' caused by inevitable variations in sensing. Delegate τ publishes error-correcting information which d uses to correct its fingerprint w' to be identical with w, given that w and w' are similar, i.e., if their Hamming distance $\mathsf{dist}(w, w')$ is below a given threshold t. Delegate τ and d then use their (corrected) fingerprints to derive context authentication secrets S and S^*, respectively. If $\mathsf{dist}(w, w') \leq t$, the authentication secrets will be identical, i.e., $S = S^*$.

Delegate τ and d then use S in an authenticated key exchange protocol run over the wireless channel to confirm the authentication and to agree on a secure link key. Admission to the trust domain is then granted by the domain master M, e.g., after requesting confirmation from the user.

5. EVALUATION

The error-correction-capable fuzzy extractor is applied as a main primitive in our context authentication protocol.

Table 1: Average min-entropy rate and number of extracted bits of fingerprints during active times of day.

Exp.	Entropy rate	Bit rate/h	Active time
Home 1	0.92	122.61	08:00–22:00
Home 2	0.95	194.46	08:00–22:00
Home 3	0.97	239.65	08:00–22:00
Office 1	0.92	225.22	10:00–18:00
Office 2	0.89	101.46	10:00–18:00
Office 3	0.96	203.99	10:00–18:00
Office 4	0.93	149.08	10:00–18:00
Office 5	0.91	96.41	10:00–18:00

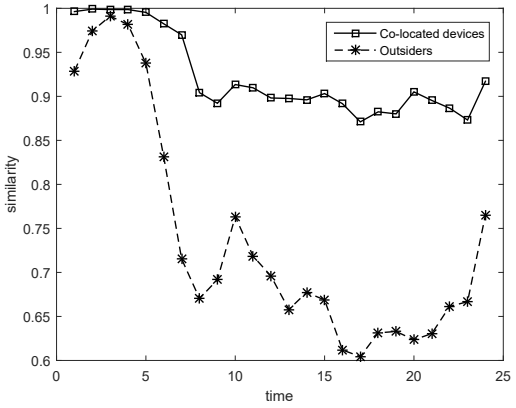

Figure 2: Average similarity of fingerprints of co-located and non-co-located devices in a domestic context

Here, two factors are critical for security: 1) the entropy rate and 2) the similarity of the sensed context fingerprints. The security properties of fuzzy extractors impose tight constraints on these factors. Our analysis shows that the similarity of context fingerprints should be at least 80%, and have an entropy rate of at least 0.85.

To evaluate the feasibility of our protocol, we collected context measurements in several different contextual settings, including domestic and office environments. Results of the entropy rate of and similarity of fingerprints between co-located devices are shown in Tab. 1 and Fig. 2. As we can see, they also fulfil the above requirements.

6. ACKNOWLDEGMENTS

This work was supported in part by the German Science Foundation (project S2, CRC 1119 CROSSING), the European Union's Seventh Framework Programme (609611, PRACTICE), and the German Federal Ministry of Education and Research within CRISP.

References

[1] D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. *ACM Trans. Inf. Syst. Secur.*, 2005.

[2] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani. Context-based zero-interaction pairing and key evolution for advanced personal devices. In *ACM Conference on Computer and Communications Security*, 2014.

[3] D. Schürmann and S. Sigg. Secure communication based on ambient audio. *IEEE Transactions on Mobile Computing*, 12, 2013.

[4] J. Suomalainen, J. Valkonen, and N. Asokan. Standards for security associations in personal networks: a comparative analysis. *IJSN*, 4, 2009.