Advanced Device Authentication: Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things

Rainer Falk and Steffen Fries
Corporate Technology
Siemens AG
Munich, Germany
e-mail: {rainer.falk|steffen.fries}@siemens.com

***Abstract*—Robust and practical device authentication is an essential security feature for cyber physical systems and the Internet of Things. After giving an overview on device authentication options, several proposals for advanced device authentication means are presented to increase the attack robustness of device authentication. A well-known cryptographic device authentication using a symmetric cryptographic key or a digital certificate for device authentication can be extended with additional validations to check the device identity. Ideas from advanced human user authentication means like multi-factor authentication and continuous authentication are applied to enhance device authentication.**

Keywords–device authentication; Internet of Things, embedded security, cyber security.

I. INTRODUCTION

The need for technical information technology (IT) security measures increases rapidly to protect products and solutions from manipulation and reverse engineering [1]. This scope is further broadened to also include operational technology (OT). Cryptographic IT security mechanisms have been known for many years, and are applied in smart devices (Internet of Things, Cyber Physical Systems, industrial and energy automation systems, operation technology) [2]. Such mechanisms target authentication, system and communication integrity and confidentiality of data in transit or at rest.

A central security mechanism is authentication: By authentication, a claimed identity is proven. Authentication of a person can be performed by verifying something the person knows (e.g., a password), something the person has (e.g., a physical authentication token, smart card, or a passport), or something the person is (biometric property, e.g., a fingerprint, voice, iris, or behavior).

Advanced authentication techniques make use of multiple authentication factors, and performing authentication continuously during a session. With multi-factor authentication, several independent authentication factors are verified, e.g., a password and an authentication token. With continuous authentication, also called active authentication, the behavior of a user during an authenticated session is monitored to determine if the authenticated user is still the one using the session.

While advanced authentication techniques like multi-factor authentication and continuous authentication are known for human users, it seems that these technologies have not yet been applied for device authentication.

With ubiquitous machine-oriented communication, e.g., the Internet of Things and interconnected cyber physical systems, devices have to be authenticated in a secure way. This paper presents and investigates approaches for advanced device authentication.

After describing single device authentication means in Section II, the combination of authentications is covered in Section III. The advantages of enhanced device authentication factors to increase the security level of Internet of Things systems and Cyber Physical Systems is investigated in Section IV. Section V summarizes related work. Section VI concludes with a summary and an outlook. Note that the paper investigates different options for providing enhance authentication from a conceptual point of view. The options are discussed in the context of system design and require an implementation as the consequent next step.

II. DEVICE AUTHENTICATION MEANS

As for users, authentication of a device can be based on different authentication factors, similar to user authentication means [8]:

- Something the device knows: credential (device key, e.g., a secret key or a private key)
- Something the device has (integrated authentication IC, authentication dongle)
- Something the device is (logical properties, e.g., the device type, configuration data, firmware version; physical properties: physical unclonable function (PUF), radio fingerprint)

Besides these well-established authentication factors, more unconventional authentication factors can also be used:

- Something the device does (behavior, functionality, e.g., automation control protocol)
- Something the device knows about its environment (sensors)
- Something the device can (functional capability, actuators)

 ISBN: 978-1-61208-512-8

- The context of the device (neighbors, location, connected periphery)

Different usages in IoT systems apply device authentication:

- Identity Authentication toward a remote system (access control, communication security). May be a supervisory system, or a peer device.
- Network access security (IEEE 802.1X [3], mobile network access authentication [4]).
- Original device authentication
- Attestation of device integrity
- Attestation of device configuration

The remainder of this section provides an overview about device authentication means. The authentication would typically be performed by an authentication server that, after successful authentication, may allow access to further system specific data directly or issues a temporal token (e.g., SAML assertion [5], OAUTH token [6], short-term X.509 certificate [7]).

A. Cryptographic Device Authentication

The authentication of a device allows a reliable identification. For authentication, a challenge value is sent to the object to be authenticated. This object calculates a corresponding response value, which is returned to the requestor and verified. The response can be calculated using a cryptographic authentication mechanism, or by using a PUF [1].

For cryptographic authentication, different mechanisms may be used. Examples are keyed hash functions like HMAC-SHA256 or symmetric ciphers in cipher block chaining (CBC-MAC) mode, or symmetric ciphers in Galois counter mode (GMAC) up to digital signatures. For the symmetric ciphers, AES would be a suitable candidate. Common to keyed hashes or symmetric key based cryptographic authentication approaches is the existence of a specific secret or private key, which is only available to the object to be authenticated and the verifier. One resulting requirement from this fact is obviously the need for robust protection of the applied secret key. Also, asymmetric cryptography can be used for component authentication. A suitable procedure based on elliptic curves has been described in [24]. Also in this use case, the secret key has to be protected on the authenticating component.

The device is authenticated as only an original device can determine the correct response value corresponding to a given challenge. The verifier sends a random challenge to the component that determines and sends back the corresponding response. The verifier checks the response. Depending on the result, the component is accepted as genuine/authenticated or it is rejected.

Various approaches are available to realize a cryptographic device authentication:

- Software credential: Credentials are hidden in software, configuration information, or the system registry. Be aware that practices of storing cryptographic credentials in firmware or cleartext configurations are weak [11][12]. However, techniques for whitebox cryptography are available that hide keys in software [13].
- Central processing unit (CPU) and microcontroller integrated circuits (IC) with internal key store: Some modern CPUs resp. microcontrollers include battery-backed SRAM or non-volatile memory, e.g., security fuses, that can be used to store cryptographic keys on the IC [14]. Also, an internal hardware security module (HSM) or secure execution environment can be included (e.g., Infineon Aurix with integrated HSM [15], or ARM TrustZone [16]).
- Separate authentication ICs can be integrated (e.g., Atmel CryptoAuthentication ECC508A [17] , Infineon Optiga Trust E [18]).
- Crypto controller (e.g., Infineon SLE97 [19]).
- Trusted platform module (TPM 1.2 [20], TPM 2.0 [21], TPM automotive thin profile [34]).

B. Device Authentication based on Device Properties

Physical and logical properties of a device can be verified as part of a device authentication. For this purpose, information about the device properties can be provided in a cryptographically protected way. In particular, an attestation, a digitally signed information confirming properties of a device, can be created by a protected component of the device.

Properties of the device can be logical information (software version, device configuration, serial number of components of the device) or physical properties of the device that can be determined by sensors or a PUF [9].

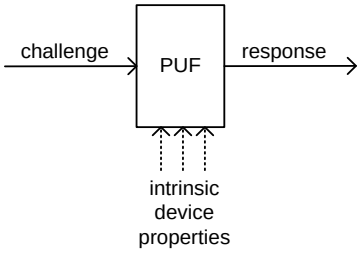

Figure 1. Challenge-Response-PUF

Fig. 1 shows the basic concept of a PUF [1]. A PUF performs a computation to determine a response value depending on a given challenge value. Intrinsic device properties influence the PUF calculation so that the calculation of the response is different on different devices, but reproducible – with some bit errors – on the same device.

A PUF is used here for device authentication in a different way: It is by itself not a strong authentication. Instead, a cryptographically protected attestation can be used to attest physical properties of a device that are measured using a PUF. So, a PUF is not used directly for authentication, but indirectly as integrated device sensor to measure physical properties of the device. It can be considered as a "two-factor device authentication" where the PUF is used as second authentication factor.

 ISBN: 978-1-61208-512-8

C. Authentication based on Device Context and Monitoring Information

Information about the context of a device can be used, e.g., the device location, or information about the environment of neighbor devices, the network reachability under a certain network address, or over a certain communication path.

The device context is determined and checked. The context information can be provided by the device itself, or the device's context information can be requested from a context server. One example from industrial environments is the system and device engineering, which basically provides information about the type and functionality of connected devices. Hence, it can be used to retrieve information about the devices deployment environment. The device location can be obtained using known localization technologies, e.g., global navigation satellite systems (GNSS) as GPS, GALILEO, BEIDOU, GLONASS, or localization using base stations (WLAN, cellular, broadcast) and beacons [22].

Furthermore, the device operation can be monitored: The behavior of the main, regular functionality of the device can be monitored and checked for plausibility.

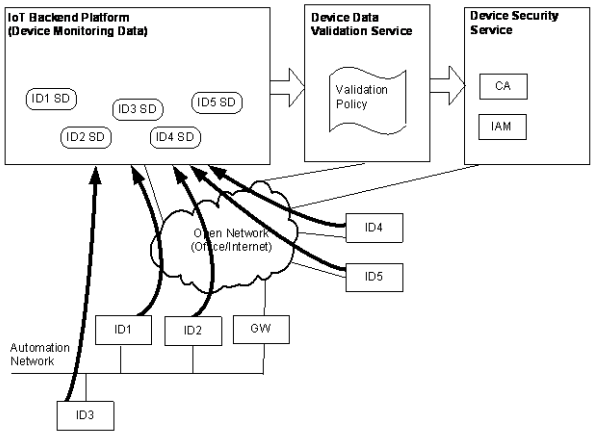

Figure 2. Validation of Device Monitoring Data

Fig. 2 shows an example for an IoT system with IoT devices (ID1, ID2, etc.) that communicate with an IoT backend platform. The devices provide current monitoring information about their status, measurements, etc. to the backend platform (e.g., for predictive maintenance). The backend platform maintains the data for the IoT devices (ID1 SD, ID2 SD, etc.) as IoT device supervisory data ("digital twin"). Furthermore, context information about the environment of a device can be provided by the device itself using its sensors, or by neighboring devices.

The devices authenticate, e.g., using a device certificate, towards a device security service that maintains information about registered devices and their permissions. Furthermore, the device security service can issue and revoke device credentials (e.g., device certificate, authentication tokens).

In addition, a device data validation service can ensure that the device operation can be monitored, supporting also a continuous verification of the devices purpose. The validation service requests information about the IoT device supervisory data of supervised devices and checks it for validity using a configurable validation policy. Hence, the behavior of the main, regular functionality of the device can be monitored and checked for plausibility. Additionally, some arbitrary dummy functionality can be realized for monitoring purposes (e.g., predictable, pseudo-random virtual sensor measurement).

If a policy violation is detected, a corrective action is triggered: provide alarm message for display on a dash board (the alarm message can be injected in the device supervisory data set of the affected device maintained by the IoT backend platform). Furthermore, an alarm message can be sent to the IoT backend platform to terminate the communication session of the affected IoT device. Moreover, the device security service can be informed so that it can revoke the devices access permissions, or revoke the device authentication credential.

D. Authentication based on Device Capability

The authenticity of a control device can be verified by checking that a device can in fact perform a certain operation. The device is given an instruction to perform a certain test operation. It is checked that the device can perform a certain computation on provided test data: The device is given a set of input parameters (test data) and has to provide the correct result that is a valid result of the computation. The computational function could be a cryptographic puzzle involving a secret. The functionality can be realized by software/firmware on the control device, by a programmable hardware (FPGA), or by a periphery device (e.g., separate signal processor or IO device). Furthermore, it can be verified that a device can act on the expected physical environment (proofing that it has control on a certain effect in the physical world). The effect is observed by a separate sensor device. In an embodiment, the separate sensor device may provide an assertion.

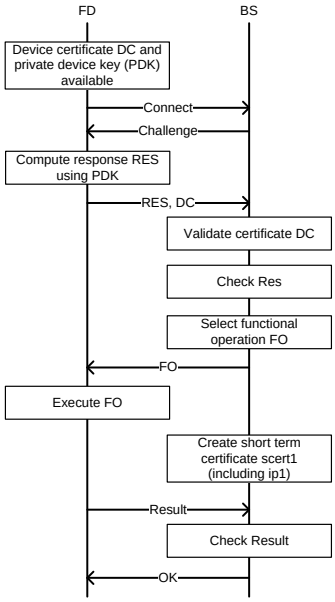

Figure 3. Verification of Device Capability

 ISBN: 978-1-61208-512-8

Fig. 3 shows a possible message exchange. The functional capability check is performed over a cryptographically authenticated communication link (e.g., transport layer security (TLS) protocol [25]). A device passes the authentication if both its cryptographic authentication is valid and its functional operation (FO) is verified successfully. For a successful attack, where a fake device is to be accepted, it is not sufficient that the attacker has access to the used cryptographic key. In addition, the attacker has to realize the expected functionality of the real device.

An example for combining authentication and the property to control a specific environment can be given by the recently established letsencrypt [38] infrastructure. Here, a (web)server applies for an X.509 certificate to be used for authentication in the context of https connections made to the web server. The certificate will be issued once the server can prove that it controls the domain it is requesting a certificate for. The proof is provided by putting dedicated information onto a random address in the applying servers address space. If this information can be retrieved externally, the proof of control is provided.

III. COMBINED DEVICE AUTHENTICATIONS

This section describes various advanced options for device authentication where multiple device authentications are combined.

A. Multi-Factor Device Authentication

A device can support multiple independent authentications. These authentication options may be performed iteratively.

In particular, an initial cryptographic device authentication can be used to setup an authenticated communication session with an authentication server. Additional checks can be performed to complete the device authentication, e.g., in the scope of a specific application.

B. Separate Re-authentication Connection

In communication security, a secure session is established by an authentication and key agreement protocol (e.g., IKEv2, TLS authentication and key agreement). The authentication is typically performed for each communication session.

It is proposed that a single device has to set-up multiple authenticated communication sessions. The device has to re-authenticate regularly towards a backend system respectively a separate authentication server using a first communication session. If this is not done, the second communication session is terminated or blocked by the backend system. This realizes a form of continuous device authentication where a device is continuously re-authenticated during a communication session, but without degrading the main communication link for which delays and interruptions shall be avoided.

The second communication session can be used for real-time / delay sensitive control traffic. The communication session will often be established for a long time (e.g., months). The re-authentication of the device can be performed independently using a second communication session without interfering with the second communication session (interruptions, delays during re-authentication). Note that the different communication sessions may terminate at different points in the backend systems. Hence, besides the multiple authentication sessions from the device, there needs to by a synchronization of the authentication sessions in the backend.

Also, the re-authentication of the first connection may be used to create a dynamic cryptographic binding with a further (separate) security session. This property can be used, to ensure that the entities involved in a separate security session know, that there is a persistent first session with either the same entity or a different entity. This approach may be used for instance in publish/subscribe use cases to ensure, that there is a persistent connection with the publish/subscribe server, while actually having an end-to-end communication session between the clients.

C. System Authentication

In industrial control systems and the Internet of Things, often a set of field devices will be used to realize a system. It is proposed to check the authentication of a set of devices (system authentication) that have to authenticate towards a backend system. A single device is accepted as authenticated only as long as a defined set of associated devices, forming the system, authenticates as well (with plausible context of the devices, e.g., network connectivity, location). The devices may have a different criticality assigned to enable a distinction between necessary and optional devices.

The communication link of a device (as member of a group) is set to an active state (permission to send/receive data) only if all required devices of the group have authenticated successfully. Thereby, an attacker cannot perform a successful attack by setting up only a single fake device. A single device is accepted as authenticated only as long as a defined set of associated devices authenticates as well (with plausible context, e.g., network connectivity, location).

IV. EVALUATION

The security of a cyber system can be evaluated in practice in various approaches and stages of the system's lifecycle:

- Threat and risk analysis (TRA) of cyber system
- Checks during operation to determine key performance indicators (e.g., check for compliance of device configurations).
- Security testing (penetration testing)

During the design phase of a cyber system, the security demand is determined, and the appropriateness of a security design is validated using a threat and risk analysis. Assets to be protected and possible threats are identified, and the risk is evaluated in a qualitative way depending on probability and impact of threats. The effectiveness of the proposed enhanced device authentication means can be reflected in a system TRA. The proposed enhancements to simple cryptographic device authentication can lead to a reduction

 ISBN: 978-1-61208-512-8

of the probability and/or the impact of a threat, so that the overall risk for successful attacks is reduced.

Two exemplary threats affecting a device are given (using for this example a simple qualitative assessment metric of low/medium/high):

- An attacker obtains device authentication credential by attacking the authentication protocol (probability: medium, impact: high; risk: high).
- An attacker succeeds in exploiting an implementation vulnerability of a device to get root access to the device and manipulate the device functionality (probability: high, impact: high; risk: high).

With selected additional protection measures, the risk can be reduced to an acceptable level: A device authentication credential cannot be used by an attacker for a successful attack as the device credential alone does not allow for a successful device authentication. With functional verification of device capability, a manipulated device can be detected. For a successful attack, the attacker would have to ensure continuously the correct operation of the device as verified by the capability check, which increases the effort for the attacker. While in real-world attack models, it is never possible to prevent all attacks, the presented countermeasures help to increase the required effort for a successful, undetected attack.

V. Related Work

Authentication within the Internet of Things is an active area of research and development. Gupta described multi-factor authentication of users towards IoT devices [29]. The Cloud Security Alliance published recommendations on identity and access management within the IoT [30]. Ajit and Sunil describe challenged to IoT security and solution options. Authentication systems for IoT where analyzed by Borgohain, Borgohain, Kumar and Sanyal [32].

Al Ibrahim and Nair have combined multiple PUF elements into a combined system PUF [33].

An "automotive thin profile" of the Trusted Platform Module TPM 2.0 has been specified [34]. A vehicle is composed of multiple control units that are equipped with TPMs. A rich TPM manages a set of thin TPMs, so that the vehicle can be represented by a vehicle TPM to the external world.

For electric vehicle charging, a vehicle authentication scheme has been described by Chan and Zhou that involves two authentication challenges, sent over different communication links (wireless link, charging cable) to the electric vehicle.

Host-based intrusion detection systems (HIDS) as SAMHAIN [36] and OSSEC [37] analyze the integrity of hosts and report the results to a backend security monitoring system.

Continuous user authentication, i.e., the checking during a session whether the user is still the same as the authenticated one, has been described by [26] and [27].

VI. Conclusion

Robust and practical device authentication is an essential security feature for cyber physical systems and the Internet of Things. The security design principle of "defense in depth" basically means that multiple layers of defenses are designed. This design principle can not only be applied at the system level, but also at the level of a single security mechanism.

This paper proposed advanced device authentication means to increase the attack robustness of device authentication. A well-known cryptographic device authentication can be extended with additional validations to check the device identity. The paper described how ideas from advanced human user authentication like multi-factor authentication and continuous authentication can be applied to device authentication.

The consequent next step addresses the integration of a selection of enhanced authentication means as proof of concept to verify the concept as such and also the supremacy in comparison with single authentication schemes.

References

[1] R. Falk and S. Fries, "New Directions in Applying Physical Unclonable Functions", The Ninth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), pp. 31-36, 23-28 August 2015, Venice, Italy, Thinkmind, available from: https://www.thinkmind.org/index.php?view=article&articleid=securware_2015_2_20_30028, last access: January 2016

[2] IEC 62443, "Industrial Automation and Control System Security" (formerly ISA99), available from: http://isa99.isa.org/Documents/Forms/AllItems.aspx , last access: April 2016

[3] "IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control", IEEE standard, 802.1X-2010, available from https://standards.ieee.org/findstds/standard/802.1X-2010.html , last access April 2016

[4] G. Horn and P. Schneider, "Towards 5G Security", 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), Helsinki, Finland, 20-22 August, 2015, available from http://networks.nokia.com/sites/default/files/document/conference_paper__towards_5g_security_.pdf , last access April 2016

[5] Wikipedia, "Security Assertion Markup Language", available from https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language , last access April 2016

[6] J. Richer, "User Authentication with OAuth 2.0", available from http://oauth.net/articles/authentication/ , last access April 2016

[7] E. Gerck, "Overview of Certification Systems: X.509, CA, PGP and SKIP", MCG, 1998, available from http://mcwg.org/mcg-mirror/certover.pdf , last access April 2016

[8] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication", Proceedings of the IEEE, vol. 91, issue 12, pp. 2021 – 2040, 2003

[9] C. Herder, Y. Meng-Day, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial", Proceedings of the IEEE, vol. 102, nr. 8, pp. 1126-1141, Aug. 2014, available from:

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6823677, last access: January 2015

[10] R. Falk and S. Fries, "Advances in Protecting Remote Component Authentication", International Journal on Advances in Security, vol 5, nr. 1-2, pp. 28-35, 2012, Available online: http://www.iariajournals.org/security/ , last access: April 2016

[11] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A Large-Scale Analysis of the Security of Embedded Firmwares", 23rd USENIX Security Symposium, August 20–22, 2014, San Diego, CA, available from https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-costin.pdf , last access April 2016

[12] R. Santamarta, Identify Backdoors in Firmware By Using Automatic String Analysis, 2013, available from http://blog.ioactive.com/2013/05/identify-back-doors-in-firmware-by.html , last access April 2016

[13] J. A. Muir, "A Tutorial on White-box AES", Cryptology ePrint Archive, Report 2013/104, available from https://eprint.iacr.org/2013/104.pdf , last access: April 2016

[14] M. Balakrishnan, "Freescale Trust Computing and Security in the Smart Grid", Freescale white paper, document number: TRCMPSCSMRTGRDWP REV 1, 2013, available from http://cache.nxp.com/files/32bit/doc/white_paper/TRCMPSCSMRTGRDWP.pdf , last access April 2016

[15] Infineon, "Highly integrated and performance optimized 32-bit microcontrollers for automotive and industrial applications",2016, available from http://www.infineon.com/dgdl/TriCore_Family_BR-2016_web.pdf?fileId=5546d46152e4636f0152e59a1581001d

[16] ARM: "Building a Secure System using TrustZone Technology", ARM whitepaper PRD29-GENC-009492C, 2005 - 2009, available from http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf , last access April 2016

[17] Atmel, "ATECC508 Atmel CryptoAuthentication Device", summary datasheet, 2015, available from http://www.atmel.com/images/atmel-8923s-cryptoauth-atecc508a-datasheet-summary.pdf , last access April 2016

[18] Infineon, "Optiga Trust E SLS32AIA", product brief, 2016 available from http://www.infineon.com/dgdl/Infineon-OPTIGA%E2%84%A2+Trust+E+SLS+32AIA-PB-v02_16-EN.pdf?fileId=5546d4624e765da5014eaabac63f5a38

[19] Infineon, "SOLID FLASH™ SLE 97 Family", product brief, 2012, available from http://www.infineon.com/dgdl/Infineon-SOLID_FLASH_SLE_97_Family_32-bit_High_Performance-PB-v08_12-EN.pdf?fileId=db3a30433917ea3301392ec288fc4ff0 , last access April 2016

[20] Trusted Computing Group: "TPM Main Specification", Version 1.2, , available from http://www.trustedcomputinggroup.org/resources/tpm_main_specification , last access April 2016

[21] Trusted Computing Group, "Trusted Platform Module Library Specification, Family 2.0", 2014, available from http://www.trustedcomputinggroup.org/resources/tpm_library_specification , last access April 2016

[22] K. Pahlavan, et al., "Taking Positioning Indoors, Wi-Fi Localization and GNSS", InsideGNSS, pp. 40-47, May 2010, available from http://www.insidegnss.com/auto/may10-Pahlavan.pdf , last access April 2016

[23] B. Parno, " Bootstrapping Trust in a Trusted Platform", 3rd USENIX Workshop on Hot Topics in Security, July 2008, available from http://www.usenix.org/event/hotsec08/tech/full_papers/parno/parno_html/ , last access: April 2016

[24] M. Braun, E. Hess, and B. Meyer, "Using Elliptic Curves on RFID Tags," International Journal of Computer Science and Network Security, vol. 2, pp. 1-9, February 2008

[25] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, Aug. 2008, available from http://tools.ietf.org/html/rfc5246 , last access: April 2016

[26] H. Xu, Y. Zhou, and M. R. Lyu: Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones, Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11, 2014, Menlo Park, CA, available from: https://www.usenix.org/system/files/conference/soups2014/soups14-paper-xu.pdf , last access: April 2016

[27] K. Niinuma and A. K. Jain, "Continuous User Authentication Using Temporal Information", available from http://biometrics.cse.msu.edu/Publications/Face/NiinumaJain_ContinuousAuth_SPIE10.pdf , last access: April 2016

[28] N. Costigan and I. Deutschmann, DARPA's Active Authentication program, RSA Conference Asia Pacific 2013 available from https://www.rsaconference.com/writable/presentations/file_upload/sec-t05_final.pdf , last access: April 2016

[29] U. Gupta, "Application of Multi factor authentication in Internet of Things domain: multi-factor authentication of users towards IoT devices, Cornell university arXiv:1506.03753, 2015, available from: http://arxiv.org/ftp/arxiv/papers/1506/1506.03753.pdf , last access: April 2016

[30] A. Mordeno and B. Russel, "Identity and Access Management for the Internet of Things - Summary Guidance", Cloud Security Alliance, 2015, available from: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf , last access: April 2016

[31] J. Ajit and M.C. Suni, "Security considerations for Internet of Things", L&T Technology Services, 2014, http://www.lnttechservices.com/media/30090/whitepaper_security-considerations-for-internet-of-things.pdf

[32] T. Borgohain, A. Borgohain, U. Kumar, and S. Sanyal, "Authentication Systems in Internet of Things", Int. J. Advanced Networking and Applications, vol. 6, issue 4, pp. 2422-2426, 2015, available from http://www.ijana.in/papers/V6I4-11.pdf , last access: April 2016

[33] O. Al Ibrahim and S. Nair, "Cyber-Physical Security Using System-Level PUFs", 7th International Wireless Communications and Mobile Computing Conference (IWCMC), 2011, available from http://lyle.smu.edu/~nair/ftp/research_papers_nair/CyPhy11.pdf , last access: April 2016

[34] Trusted Computing Group, "TCG TPM 2.0 Automotive Thin Profile", level 00, version 1.0, 2015, available from http://www.trustedcomputinggroup.org/resources/tcg_tpm_20_library_profile_for_automotivethin , last access: April 2016

[35] A. C-F. Chan and J. Zhou, "Cyber-Physical Device Authentication for Smart Grid Electric Vehicle Ecosystem", IEEE Journal on Selected Areas in Communications, vol. 32, issue 7, pp. 1509 – 1517, 2014

[36] R. Wichmann, "The Samhain HIDS", fact sheet, 2011, available from http://la-samhna.de/samhain/samhain_leaf.pdf, last access April 2016

[37] OSSEC, "Open Source HIDS SECurity", web site, 2010 - 2015, available from http://ossec.github.io/ , last access April 2016

[38] Letsencrypt, letsencrypt.org, last access April 2016