OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

IoT Device Identific***A***tion and Reco***G***nition (***IoTAG***)

Lukas Hinterberger **(OTH Regensburg, lukas.hinterberger@st.oth-regensburg.de)**
Bernhard Weber (OTH Regensburg, bernhard1.weber@st.oth-regensburg.de)
Sebastian Fischer (Fraunhofer AISEC, sebastian.fischer@aisec.fraunhofer.de)
Katrin Neubauer (OTH Regensburg, katrin1.neubauer@oth-regensburg.de)
Prof. Dr. Rudolf Hackenberg (OTH Regensburg, rudolf.hackenberg@oth-regensburg.de)

Cloud Computing 2020 - October 25, 2020 to October 29, 2020 - Nice, France

Presenter

- Name: Lukas Hinterberger
- Date of birth: July 27, 1995
- Education:
  - 2006 – 2014: Werner von Siemens Gymnasium Regensburg (Abitur)
  - 2014 – 2018: OTH Regensburg (B.Sc. Technical Computer Science)
  - 2018 – 2020: OTH Regensburg (M.Sc. Applied Research)

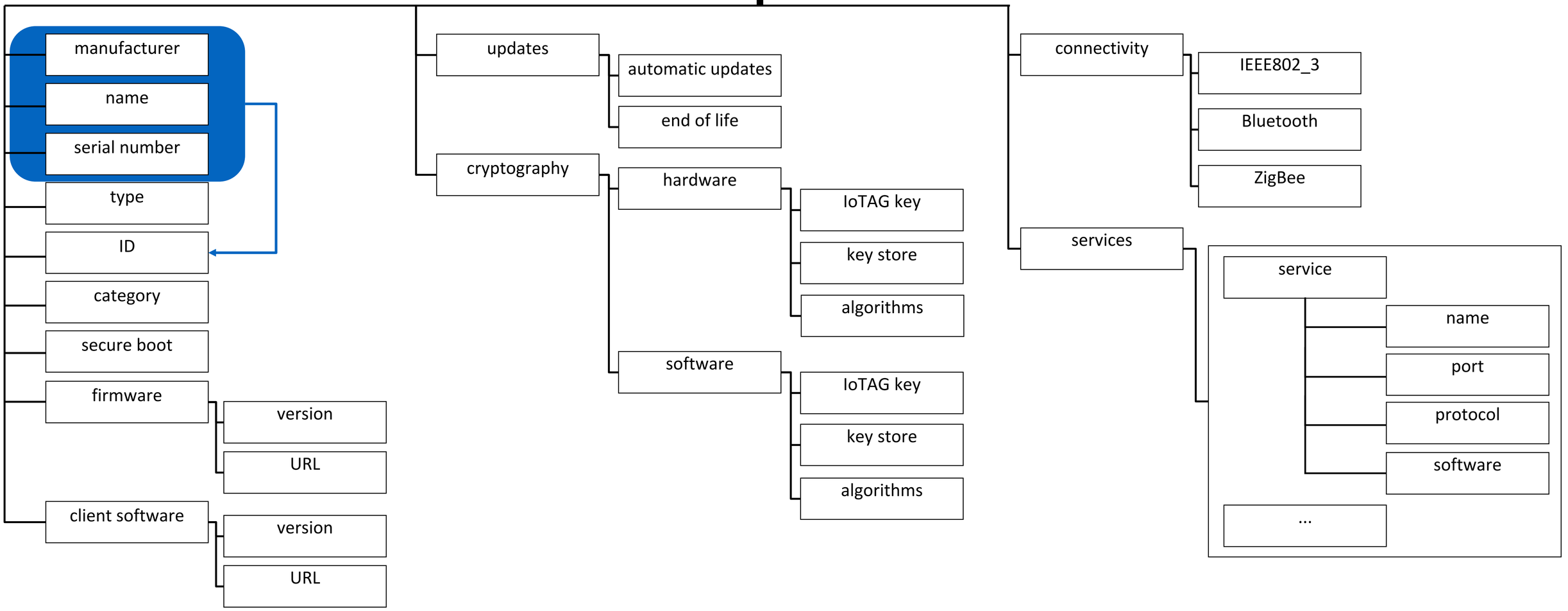
What is IoTAG

- Open Standard for **IoT** Device Identific**A**tion and Reco**G**nition
- Provision of security relevant information by IoT devices themselves
- Predefined communication channels
- Data protection against manipulation
- Easy implementation through the use of existing standards

Why IoTAG?

- IoT devices ARE insecure (most of them) -> see botnets
- Increasing complexity of IoT networks
- Security indicator for devices is necessary
  - Information about devices needed
  - Existing device scanning methods (e.g. Nmap) are too inaccurate
  - ➢ Devices have to provide information themselves

IoTAG Dataset



IoTAG Serialization

- JSON (UTF-8)
  - Expandable
  - Human readable
  - Standardized
  - Broadly supported

```
{
  "Manufacturer": "Beispiel GmbH",
   "Name": "PoC-Device",
   "SerialNumber": "D1.0",
   "Type": "weather station",
   "ID": "67c8acf906269aecd5e3fa85f5be1042b6712adfc529e727534332edb8cef66e",
   "Category": "infrastructure",
   "SecureBoot": false,
   "Firmware": {
      "Version": "1.0",
      "URL": "https://192.168.102.94:10000/FirmwareInfo"
   },
   "Updates": {
      "AutomaticUpdates": false,
      "EndOfLife": "2021-01-01T00:00:00"
   },
   "Connectivity": {
      "IEEE802_3": [“WPA2”, "b", "g", "n", "ac"],
   }, …
}
```

IoTAG Data Integrity

- Without integrity check:
  - Every device can send false data
  - An attacker could use IoTAG to masquerade himself as a harmless IoT device
  - ➢ **It's necessary to sign this information to ensure their authenticity and correctness**

IoTAG Signature

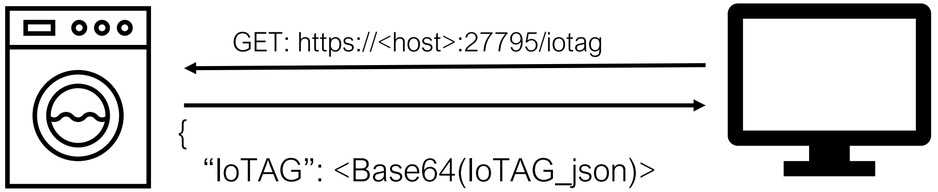
- RSASSA-PSS
  - Asymmetrical
- Certificates for key exchange
  - According to ITU-T X.509 and RFC 2459
- Key size: at least 2048 bits (as recommended by NIST)
- Application to SHA256 hash of the serialized record

IoTAG Communication

- General
  - HTTPS (HTTP/2 + TLS)
  - GET-Request
  - JSON formatted data

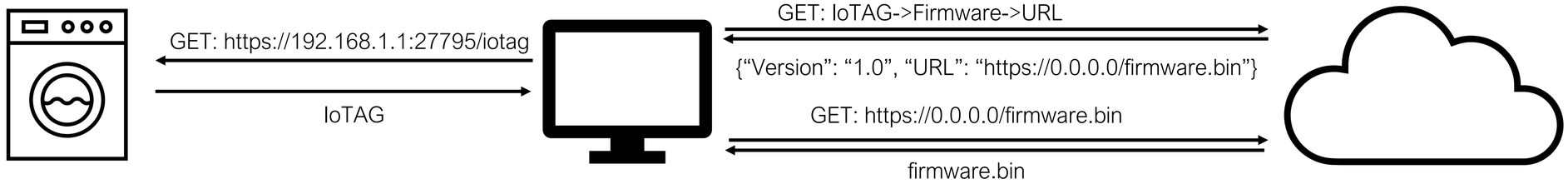
IoTAG Communication

- Retrieving IoTAG
  - JSON object containing “IoTAG”, “Signature” and “Certificates”
  - Base64 encoded data to prevent errors due to different formatting
  - URL: https://<host>:27795/iotag



IoTAG Communication

- Retrieving Software Resources
  - URL contained in IoTAG inside “firmware” or “client software”
  - Software not downloaded directly
  - JSON object containing “URL” and “Version”



IoTAG Conclusion

- Detailed information about devices available
- A central gateway (e.g., the router) can periodically check all devices
- New services for automated scanning for new vulnerabilities (CVE) are possible
- In case of an outdated service or missing software updates:
  - Display security warning
  - Temporarily disable the communication with the insecure device

Pending Issues And Further Work

- How to prevent an attacker who has access to the network to use the provided information from IoTAG to scan for insecure or unpatched devices?
- Add support for multiple signature procedures (e.g. elliptic curve cryptography)
- Add new entries to the dataset (e.g. required cloud resources)
- Development of a security rating system based on the IoTAG dataset

References

[1] Federal Office for Information Security (Germany), “SYS.4.4: Allgemeines IoT-Gerät,” IT-Grundschutz-Kompendium 2. Version 2019, Cologne, Bundesanzeiger Verlag GmbH, 2019, p. 3.
[2] European Telecommunications Standards Institute, “Draft ETSI EN 303 645 V2.0.0 (2019-11),” 2019.
[3] S. Fischer, K. Neubauer, L. Hinterberger, B. Weber, and R. Hackenberg, “IoTAG: An Open Standard for IoT Device IdentificAtion and RecoGnition,” The Thirteenth International Conference on Emerging Security Information, Systems and Technologies, IARIA, 2019, pp. 107-113.
[4] World Wide Web Consortium, “Web of Things (WoT) Thing Description,” Apr. 2018. [Online]. Available from: https://www.w3.org/TR/wot-thing-description/ [accessed: 2020-07-20].
[5] A. E. Khaled, A. Helal, W. Lindquist, and C. Lee, “IoT-DDL—Device Description Language for the “T” in IoT,” IEEE Access, Nr. 6, pp. 24048-24063, Apr. 2018.
[6] U.S. Department of Commerce und National Institute of Standards and Technology, “Secure Hash Standard (SHS),” 2015.
[7] Internet Engineering Task Force, “RFC 4648 - The Base16, Base32, and Base64 Data Encodings,” Oct. 2006. [Online]. Available from: https://tools.ietf.org/html/rfc4648. [accessed: 2020-07-20].
[8] National Institute of Standards and Technology, “NIST Policy on Hash Functions - Hash Functions — CSRC,” May 2019. [Online]. Available from: https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions. [accessed: 2020-07-20].
[9] R. K. Dahal, J. Bhatta, and T. N. Dhamala, “Performance Analysis of SHA-2 and SHA-3 Finalists,” International Journal on Cryptography and Information Security (IJCIS), Sept. 2013, pp.720-730.
[10] U.S. Department of Commerce und National Institute of Standards and Technology, “SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions,” 2015.
[11] J. Vermillard, “Sicherheit für IoT-Geräte,” Linux Magazin, Oct. 2015.
[12] A. S. Tanenbaum, “Moderne Betriebssysteme,” Hallbergmoos: Pearson Deutschland GmbH, 2009, pp. 720-721.
[13] Internet Engineering Task Force, “RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax,” Jan. 2005. [Online]. Available from: https://tools.ietf.org/html/rfc3986. [accessed: 2020-07-20].
[14] International Organization for Standardization, “ISO 8601:2004: Data elements and interchange formats — Information interchange — Representation of dates and times,” 2004.
[15] Internet Engineering Task Force, “RFC 5656 - Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer,” Dec. 2009. [Online]. Available from: https://tools.ietf.org/html/rfc5656. [accessed: 2020-07-20].
[16] A.Healey,“GET 802(R) Standards,” [Online]. Available from: https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68. [accessed: 2020-07-20].
[17] Bluetooth SIG, Inc., “Bluetooth Core Specification, Revision 5.2,” 2019.
[18] ZigBee Alliance, “ZigBee Specification,” 2015.
[19] P. Kraft and A. Weyert, “Network Hacking,” Franzis Verlag GmbH, 2015, pp. 345-360.
[20] J. Erickson, “Hacking,” dpunkt.verlag GmbH, 2009, pp. 472-488.
[21] ECMA International, “The JSON Data Interchange Syntax,” 2017.
[22] Internet Engineering Task Force, “RFC 8259 - The JavaScript Object Notation (JSON) Data Interchange Format,” Dec. 2017. [Online]. Available from: https://tools.ietf.org/html/rfc8259. [accessed: 2020-07-20].
[23] N. Nurseitov, M. Paulson, R. Reynolds, and C. Izurieta, “Comparison of JSON and XML data interchange formats: A case study,” International Conference on Computer Applications in Industry and Engineering, CAINE, 2009, pp.157-162.
[24] U.S. Department of Commerce and National Institute of Standards and Technology, “Recommendation for Key Management,” 2015.
[25] Internet Engineering Task Force, “RFC 8017 - PKCS #1: RSA Cryptography Specifications Version 2.2,” Nov. 2016. [Online]. Available from: https://tools.ietf.org/html/rfc8017. [accessed: 2020-07-20].
[26] International Telecommunication Union, “Recommendation ITU-T X.509,” 2016.
[27] Internet Engineering Task Force, “RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” Jan. 1999. [Online]. Available from: https://tools.ietf.org/html/rfc2459. [accessed: 2020-07-20].
[28] National Institute of Standards and Technology, “NIST Policy on Hash Functions - Hash Functions — CSRC,” May 2019. [Online]. Available from: https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions. [accessed: 2020-07-20].
[29] Internet Engineering Task Force, “RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2,” Aug. 2008. [Online]. Available from: https://tools.ietf.org/html/rfc5246. [accessed: 2020-07-20].
[30] Internet Engineering Task Force, “RFC 7540 - Hypertext Transfer Protocol Version 2 (HTTP/2),” May 2015. [Online]. Available from: https://tools.ietf.org/html/rfc7540. [accessed: 2020-07-20].
[31] Internet Engineering Task Force, “RFC 2616 - Hypertext Transfer Protocol – HTTP/1.1,” June 1999. [Online]. Available from: https://tools.ietf.org/html/rfc2616. [accessed: 2020-07-20].
[32] Internet Engineering Task Force, “RFC 7468 - Textual Encodings of PKIX, PKCS, and CMS Structures,” Apr. 2015. [Online]. Available from: https://tools.ietf.org/html/rfc7468. [accessed: 2020-07-20].
[33] International Telecommunication Union, “Recommendation ITU-T X.690,” 2015.