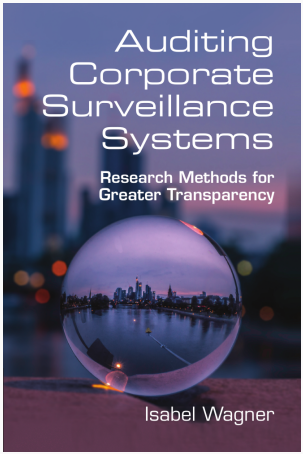
RESULTS FROM TRANSPARENCY RESEARCH

INTERNET OF THINGS

Isabel Wagner

De Montfort University



TRANSPARENCY FOR NEW TECHNOLOGIES: IOT

- New technologies drive demand for transparency
  - Smart doorbells
  - Smart fridges
  - Smart thermostats
- Internet of Things:
  - In-home placement: privileged position, access to sensitive information
  - Equipped with sensors and connectivity: lots of opportunity for corporate surveillance!
  - Security issues may allow adversarial surveillance by third parties
- Challenge: Cost of physical devices makes “1m IoT devices” study much harder than “1m websites”

OVERVIEW

- Communication protocols for IoT devices
- Detecting presence of IoT devices
- Detecting properties of IoT devices
- Results for IoT transparency
  - Voice assistants
  - Smart TVs

Communication protocols

COMMUNICATION PROTOCOLS FOR IOT: WI-FI, ZIGBEE

- Additional protocols for local communication of IoT devices: Wi-Fi, Zigbee, Bluetooth Low Energy
- Protocol determines which response variables can be sniffed on the wireless channel[1]
- Wi-Fi: internet connection through smart hub or access point
  - Identify devices by MAC and IP address
  - Protocol headers at internet layer and above are encrypted
- Zigbee:
  - Identify devices by MAC and network address (NwkAddr), not encrypted
  - Network coordinator (smart hub) has fixed address

[1] A. Acar, H. Fereidooni, T. Abera, *et al.*, "Peek-a-Boo: I see your smart home activities, even encrypted!" In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20)*, Linz, Austria: ACM, Jul. 2020. DOI: *10.1145/3395351.3399421*. arXiv: *1808.02741*.

- Device acts as “slave” node, broadcasts advertising packets to find “master” node
- “Master” node initiates connection
- Options for pairing protocol:
  - Just works
  - Passkey entry
  - Numeric comparison
  - Out of band
- Encryption keys negotiated possibly based on passkey
- After pairing, “master” device can read/write device properties
  - Hierarchical data structure, defined by device’s Generic Attribute Profile
  - Each service, service characteristic, and service characteristic descriptor has UUID

Detecting presence and properties

FINGERPRINTING OF BLE DEVICES

- Based on broadcast UUIDs[2]
  - BLE devices broadcast UUIDs of their services, can be sniffed
  - Sniffed UUIDs can be compared with UUIDs extracted from corresponding mobile app binaries (within calls to the Bluetooth API)
  - Set of UUIDs characterizes BLE device
  - Anyone within communication range can identify IoT devices
- Based on DNS traffic[3]
  - Web services contacted by IoT devices differ, depending on manufacturer and type
  - Set of web services characterizes IoT device
  - DNS traffic can be sniffed because protocol is not encrypted

[2] C. Zuo, H. Wen, Z. Lin, *et al.*, "Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19, London, United Kingdom: ACM, 2019, pp. 1469–1483. DOI: *10.1145/3319535.3354240*.

[3] R. Perdisci, T. Papastergiou, O. Alrawi, *et al.*, "IoTFinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis," in *IEEE European Symposium on Security and Privacy (Euro S&P)*, IEEE, 2020, pp. 474–489. DOI: *10.1109/EuroSP48549.2020.00037*.

DETECTING SMART SPEAKER ACTIVATION[4]

- Activation light?
- May not be accurate if smart speaker conducts secret surveillance
- Combination of methods:
  - Activation light: video recording of device, state of light can be matched against known *off* state
  - Companion app: contains list of activations, can be cross-referenced with video
  - Network traffic: traffic volume should be high when speaker is active
  - Empirically determined threshold to distinguish background traffic from activation traffic

[4] D. J. Dubois, R. Kolcun, A. M. Mandalari, *et al.*, "When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 4, pp. 255–276, 2020. DOI: 10.2478/popets-2020-0072.

Results for IoT transparency

SMART TVS

- Trackers present on 69% of Roku channels, 90% of Amazon Fire channels[5]
- 30% of channels leak device identifiers (MAC address, serial number)
  - Allows channels to relink user profiles if user changes advertising identifier
  - No effective opt-out possible!
- On-device options to limit tracking have nearly no effect
- Countermeasures for smart TVs[6]
  - DNS-based filter lists: block 27% of trackers on Amazon Fire, 22% on Roku

[5] H. M. Moghaddam, G. Acar, B. Burgess, *et al.*, "Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London, UK: ACM, Nov. 2019, pp. 131–147. DOI: *10.1145/3319535.3354198*.

[6] J. Varmarken, H. Le, A. Shuba, *et al.*, "The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 129–154, Apr. 2020. DOI: *10.2478/popets-2020-0021*.

VOICE ASSISTANTS

- Misactivation: voice assistant activates when wake word is not spoken
  - 0.95 misactivations per hour when playing sound from TV shows
  - 50% of misactivations longer than 1–4s, 25% longer than 2–7s
  - May allow capture of sensitive content
  - Remember that some voice assistants have humans review recordings[7]
- Voice assistant skills:
  - 5.5% of skills have sensitive commands (e.g., unlock door, get camera images)[8]
  - Certification of third-party skills: skills should meet voice assistant policies
  - But not applied consistently[9]: researchers succeeded in getting hundreds of policy-violating skills certified
  - Some skills continue eavesdropping even after user sends *stop* command[10]

[7] https://www.bbc.co.uk/news/technology-47893082

[8] F. H. Shezan, H. Hu, J. Wang, *et al.*, "Read Between the Lines: An Empirical Measurement of Sensitive Applications of Voice Personal Assistant Systems," in *Proceedings of The Web Conference 2020*, ser. WWW '20, Taipei, Taiwan: ACM, Apr. 2020, pp. 1006–1017. DOI: *10.1145/3366423.3380179*.

[9] L. Cheng, C. Wilson, S. Liao, *et al.*, "Dangerous Skills Got Certified: Measuring the Trustworthiness of Skill Certification in Voice Personal Assistant Platforms," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20, online: Association for Computing Machinery, Oct. 2020, pp. 1699–1716. DOI: *10.1145/3372297.3423339*.

[10] Z. Guo, Z. Lin, P. Li, *et al.*, "SkillExplorer: Understanding the Behavior of Skills in Large Scale," in *29th {USENIX} Security Symposium ({USENIX} Security*

Summary

CHALLENGES FOR IOT TRANSPARENCY

- IoT devices are embedded devices, often closed platforms
- How to automate user interaction?
  - Interaction via voice commands: speech recognition and speech synthesis?[11]
  - Data-driven dialogue systems?[12]
- TLS with certificate pinning prevents retrieval of cleartext traffic with mitmproxy
- Cost of physical devices (+laboratory setup) limits scale of studies

[11] G. Celosia and M. Cunche, "Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 1, pp. 26–46, Jan. 2020. DOI: 10.2478/popets-2020-0003.

[12] L. Cheng, C. Wilson, S. Liao, *et al.*, "Dangerous Skills Got Certified: Measuring the Trustworthiness of Skill Certification in Voice Personal Assistant Platforms," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20, online: Association for Computing Machinery, Oct. 2020, pp. 1699–1716. DOI: 10.1145/3372297.3423339.

ABOUT THIS SLIDE DECK

- These slides are designed to accompany a lecture based on the textbook “Auditing Corporate Surveillance Systems: Research Methods for Greater Transparency” by Isabel Wagner, published in 2022 by Cambridge University Press.
-
-
- Please leave this slide intact, but indicate modifications below.
  - Version 2022-04
  - Improved version for release on book website (Isabel Wagner)
- Updated versions of the original slide deck are available online: corporatesurveillance.org