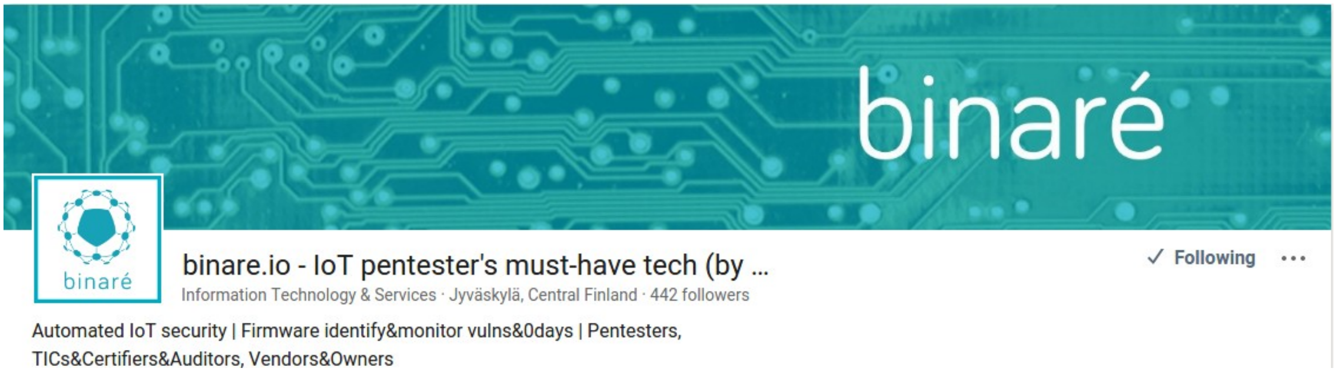


binare.io - IoT pentester's must-have tech (by ...

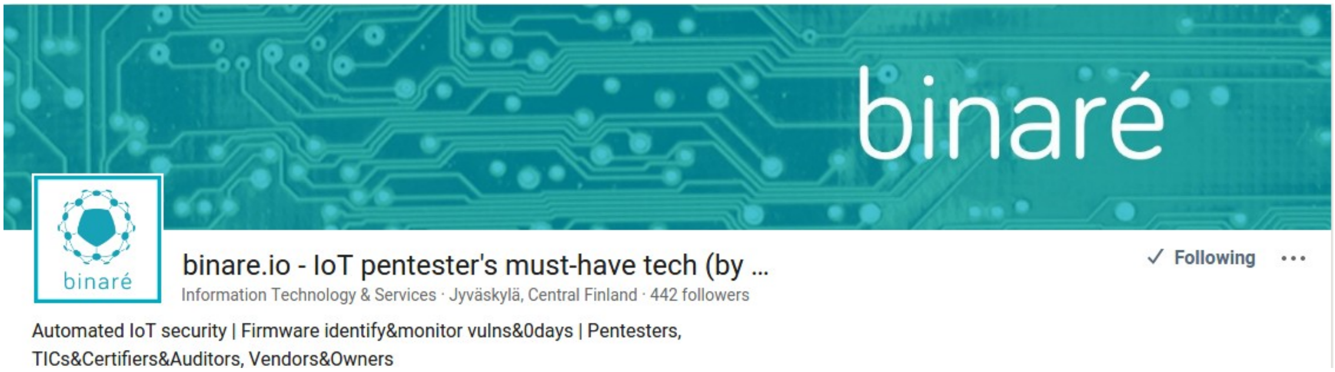
Information Technology & Services · Jyväskylä, Central Finland · 442 followers

Automated IoT security | Firmware identify&monitor vulns&0days | Pentesters, TICs&Certifiers&Auditors, Vendors&Owners

RE: **Binare.io**’s reply to request for public comments regarding *“DRAFT Baseline Security Criteria for Consumer IoT DevicesAugust 31, 2021Comments Due October 17, 2021 to labeling-eo@nist.gov”*

Comments:

1. Table 1, Asset Identification:
    1. A unique logical identifier, possibly generated by the product component host. **Ideally such identification to be as conveniently machine-readable as possible (e.g., JSON, XML) and obtainable via automated/API means as standardizes as possible (e.g., well-known URI IETF in RFC 8615, etc.).**
        1. *Comment: In bold, proposed addition (sample, could/should be rephrased/reworked).*
2. Table 1, Asset Identification:
    1. A unique physical identifier at an external or internal location on the device accessible to the consumer. **Ideally such identification to be as conveniently machine-readable as possible (e.g., QR-code and/or NFC tag, etc.) as to enable ease of automation of identification, tracking and onboarding/decomissioning, etc.**
        1. *Comment: In bold, proposed addition (sample, could/should be rephrased/reworked).*
3. Table 1, Product Configuration:
    1. Any security features should be enabled by default, **and such security features should adhere to minimal/basic security guidelines/requirements relevant to the said feature (e.g., passwords: no default/known/hardcoded passwords regardless if admin or non-admin; https: no self-signed and/or expired certificates, etc.)**
        1. *Comment: In bold, proposed addition (sample, could/should be rephrased/reworked).*
4. Table 1, Product Configuration:
    1. The ability for authorized individuals and other IoT product components to restore the product component to the default secure configuration, **using secure/proven protocols (as to avoid “IoT product components” to be abused for such actions, or “authorized individuals” to be socially-engineered to execute such actions without safeguards).**
        1. *Comment: For example, even if strong username/password credentials are being used, some sort of strong challenge-response protocols to be used to avoid trivial attacks such as automated brute-forcing and fully automated one-click/one-request attacks.*
        2. *Comment: In bold, proposed addition (sample, could/should be rephrased/reworked).*
5. Table 1, Data Protection:
    1. The ability for authorized individuals, other IoT product components, and/or systems to delete data at rest from the product component, **in a verifiable and demonstrable manner (e.g., unique, timestamped, digitally-verifiable proof receipt by the vendor/supplier**

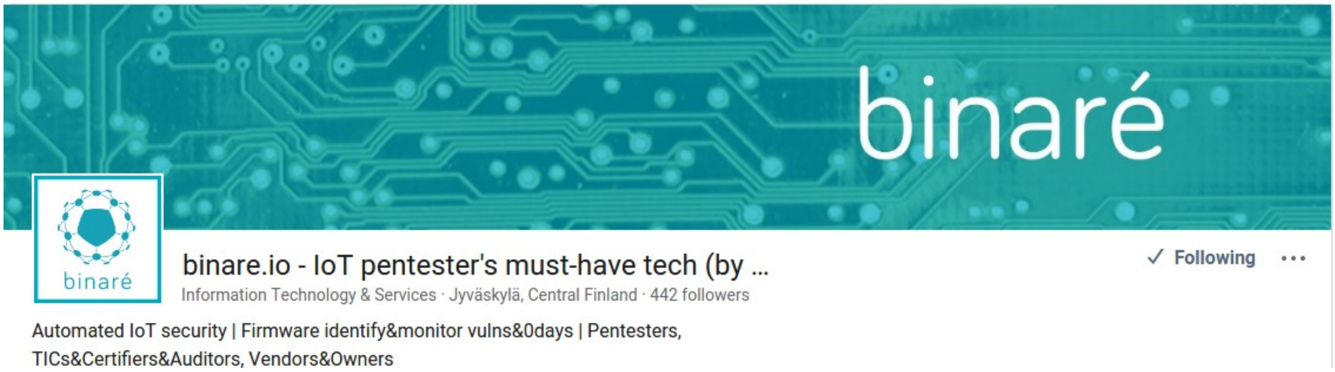


that the data has been erased – such proof could be used by the end customer in legal plane if the data was not actually deleted and found in data breach leaks).

1. *Comment: In bold, proposed addition (sample, could/should be rephrased/reworked).*

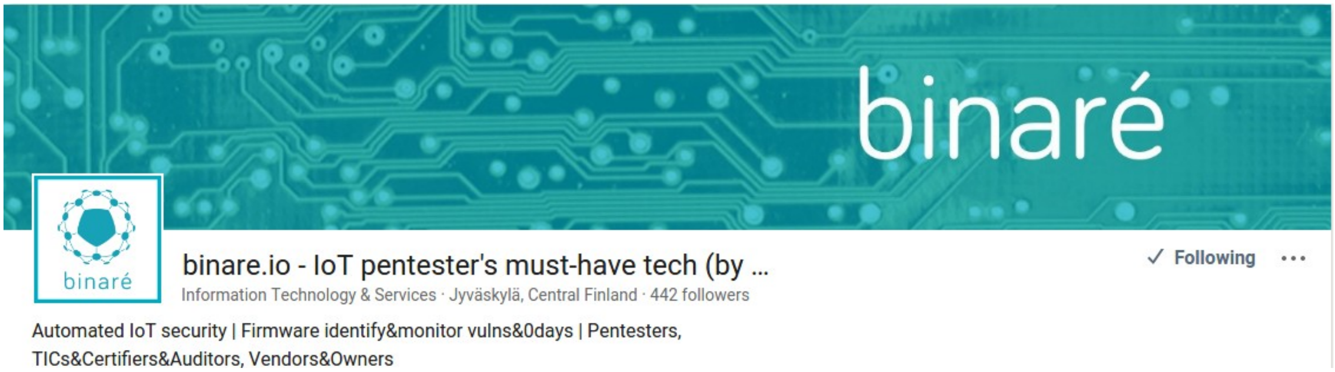
2. Add **5. Label indication (physical + digital) of the level of a) processing and b) storage of PII, with regards to various GDPR/CCPA/etc. “data privacy” directives**
    1. *Comment: Example scenario – fitness trackers many times need to pair with smartphone (Apple/Google account) and requires using some original vendor app (may require additional accounts such as samsung, huawei) or some third-party generic app. However, it is never clear whether any of the user information (such as account identification, etc.) is synced to the fitness tracker device itself, and if synced what exactly is stored on the fitness tracker and how it is dealt with/protected/erased/decommissioned.*
    2. *Comment: In bold, proposed addition (sample, could/should be rephrased/reworked).*

6. <u>Table 1, Logical Access to Interfaces</u>
    1. The ability of the product component to validate that the input received through its interfaces matches specified definitions of format and content.
        1. *Comment: Seems to be completely out of place here. Also, it is a HUGE “software security” topic – minimizing it to two-line text will basically render it useless (due to lacking concrete requirements and being too generic and open to interpretations).*
7. <u>Table 1, Software Update</u>
    1. updating of some product components by be dependent on or performed by
        1. *Comment: Sentence seems “broken”.*
8. <u>Table 1, Software Update</u>
    1. The ability for the product component to verify and authenticate any update before installing it.
        1. *Comment: Maybe instead of “ability” to be “necessity/MUST”.*
        2. *Comment: “any update” to also clarify that not just directly-functional, but rather any types of data/code that modifies the IoT component – classic example is Code Injection via “language packs”.*
9. <u>Table 1, Software Update</u>
    1. Add 1a: **“The ability to update the product component’s software in Internet-lacking situations (e.g., via USB/NFC as close-proximity, or Smartphone App pairing where the App SHOULD NOT require internet at the time of firmware update hence the App should be able to “cache” latest update for later use.)”**
        1. *Comment: Too many times we have seen that IoT products fail when Internet fails or provider’s servers are down. Moreover, there maybe users that may be faced with no-*



internet situations (by will or by circumstances), still such users SHOULD NOT be forced to have internet/connectivity in order to perform a software update.

10. Table 1, Cybersecurity State Awareness
    1. *Comment: Missing requirement about dealing/scrubbing any PII (e.g., owner/operator of the device, but can also be honest mistake "wrong device" type of failed login by users other than the owner/operator while introducing their username/password – there is the risk their PII is exposed without their consent and without them being even aware).*
11. Table 1, Cybersecurity State Awareness
    1. *Comment: Missing requirement that if such information is sent/copied/transferred to the vendor/provider (e.g., cloud, backend, etc.), the user must be notified (e.g., App alerts, or web-interface alerts if device exposes web-interface) when&what exactly was sent/copied/transferred, and such transfers should be also digitally/verifiably/traceably recorded in the logs IoT device/component/product logs (with unique global identifiers so that such identifiers can be used during support calls/emails and LE investigations), should be easily accessible for the end user for the lifetime and should lack ability to modify such logs by whatever entity (authorized/unauthorized).*
12. Table 1, Cybersecurity State Awareness
    1. *Comment: Missing requirement/ability for the end user to be offered end-to-end functionality to proactively indicate the suspicion of cybersecurity compromise (which would trigger some automated actions on the IoT product and/or some transfer of "cybersecurity state" data to the vendor's backend/cloud, however as above user awareness and user consent must be well and explicitly be taken into consideration before performing any such actions).*
13. Table 2, Documentation
    1. *Comment: All the data in the human-readable documentation, should be as much as possible encoded in machine-readable formats and specifications available/relevant for each type of document or documented information (NOTE: while PDF is a machine-readable format, it is not the best to ensure machine-to-machine data exchange and protocol communication) as to enable easier transition to SecOps in the future as well as to assist users who operate large fleets of devices and where it is impossible for humans to go over hundreds of PDFs containing each hundreds of pages.*
14. Table 2, Documentation
    1. *Comment: Missing documentation item related to "open specifications", "developer's guide", "reference implementation" - this is valid for the cases where end user want to move certain IoT device/product from "default backend/cloud" to some other non-default by implementing its own backend/cloud solution (or setting up some open-source, closed-source, free, paid service implementing a compatible backend/cloud for example).*



binare.io - IoT pentester's must-have tech (by ...

Information Technology & Services · Jyväskylä, Central Finland · 442 followers

Automated IoT security | Firmware identify&monitor vulns&0days | Pentesters, TICs&Certifiers&Auditors, Vendors&Owners

15. Table1??, Interoperability/Compatibility
    1. *Comment: Generally missing requirement to indicate/label how inter-compatible and cross-operation is a particular IoT device/component. This is crucial in case the end user wants to switch from a less secure backend/clowd/App, to a more secure backend/cloud/App. In order to give this options for an “informed buying decision”, it is important that the vendor labels and documents Interoperability/Compatibility support of each IoT device/component as follows:*
        1. *Open-specs - None, Partial, Full*
        2. *Open-source - None, Partial, Full*
        3. *Reference implementations provided by the vendor - None, Partial, Full*

       Having open-specs, open-source, reference implementations by the vendor (as opposed to individual experts performing “reverse engineering” efforts that seldom cover 100% of all functionality) will also enable and benefit the review and security testing/analysis of such IoT products, and hopefully will enable finding vulnerabilities sooner rather than later.

About Binare.io:

Binaré is a *visionary deep-tech spinoff* from the University of Jyväskylä, which boasts more than a decade of cybersecurity research vision and experience. Binaré is backed by UniFund investment and is supported by the Jyväskylän Yritystehdas incubator. Co-founded by Dr. Andrei Costin who provided visionary IoT/embedded security peer-reviewed research and has been a speaker at more than 45 top international cybersecurity events (such as USENIX Security, BlackHat, Chaos Computer Club CCC).

Binaré offers Software-as-a-Service (SaaS) and on-prem automated solutions for IoT cybersecurity, research, development and technology innovation services, as well as an extensive range of related consulting, training and advisory services. **Binaré’s unique IoT/IioT firmware analysis platform provides one-click cybersecurity reporting/pre-certification (and support during conformity certification) as well as SBoM generation and software component’s continuous monitoring for new vulnerabilities, without requiring any access to the source code!**

https://www.linkedin.com/company/binare/
https://twitter.com/binareio