## Ke, Jessica - Intern

**From:** Ben McCarty <benmccarty0@gmail.com>
**Sent:** Thursday, June 17, 2021 11:21 AM
**To:** SBOM_RFC
**Cc:** Friedman, Allan
**Subject:** Minimum Elements of an SBOM
**Attachments:** threat-model.png

All Concerned,

An SBOM should include these 3 elements:

1. SBOM meta data

- CPE/SWID
- File Size (bytes)
- Timestamp - UTC (release or compilation)
- Output of Two different hash functions of the entire software package (i.e., SHA-3, BLAKE to make sure this thing is Post-Quantum)

2. SBOM ingredient list - merkle-hashed

- full file name, file size (bytes), hash (sha-3)

3. A publicly accessible authoritative digital record of Origin/Authorship and SBOM attestation

---

In terms of safeguarding the SBOM from compromise in a sophisticated supply-chain attack - I would like to draw your attention to this patent I co-invented and filed with the USPTO.
https://patents.google.com/patent/US20200235943A1/en

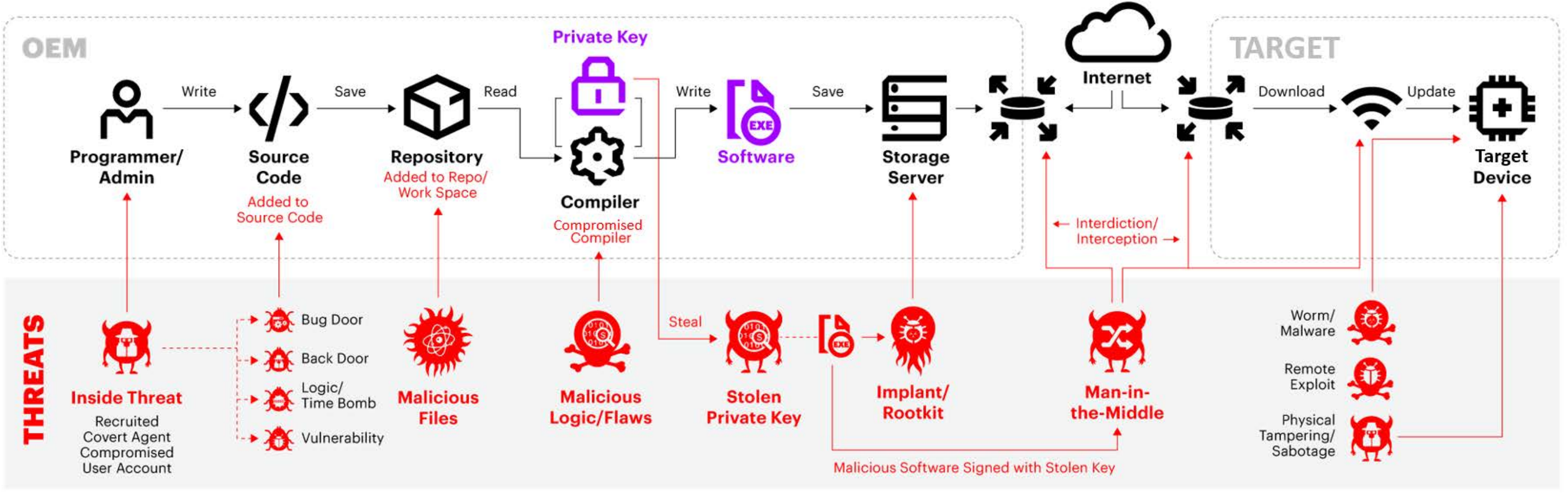
There are two additional defenses needed with an SBOM which we identified in our examination of the supply-chain attack threat model attached.

1. A digital-twin of the source code is logged and copied through one-way data-flow control into an isolated environment. A human process of validating every new file/line must be signed off as authorized changes. Then the digital-twin is compiled (ignoring a few header differences between different compilers) and is compared to its production counterpart in terms of file-size, hash, and static/dynamic malware analysis. Any significant changes should be investigated before authorizing a release of the software.

2. A separate segmented system with unique users maintains an authoritative record of Origin/Authorship and SBOM attestation. This is to mitigate an adversary with domain-admin/root access to an organization from forcibly pushing out compromised software-updates with matching SBOMs. The authoritative record could be many things - but we envisioned the authoritative digital record of SBOM attestation to be an encrypted decryption-key inside of a DNSSEC signed DNS TXT record. The digital ledger contains; the SBOM, a key to

decrypt the DNS TXT record, and an encrypted archive of the software. The novelty of our idea was to make the subdomains of the DNS record be the hashes of the SBOM. This method also allows organizations to delete DNS records to effectively revoke software from a blockchain/digital-ledger without editing the blockchain/digital-ledger. In this way, the SBOM and authoritative record cross-referenced each other and interlocked with each other to enhance security.

Thank you,
Ben McCarty
benmccarty0@gmail.com
https://www.linkedin.com/in/ben-mccarty/


OEM
Private Key
TARGET
Internet
Write
Save
Read
Write
Save
Download
Update
Programmer/
Admin
Source
Code
Added to
Source Code
Repository
Added to Repo/
Work Space
Compiler
Compromised
Compiler
Software
Storage
Server
Target
Device
Interdiction/
Interception
THREATS
Inside Threat
Recruited
Covert Agent
Compromised
User Account
Bug Door
Back Door
Logic/
Time Bomb
Vulnerability
Malicious
Files
Malicious
Logic/Flaws
Steal
Stolen
Private Key
Implant/
Rootkit
Man-in-
the-Middle
Worm/
Malware
Remote
Exploit
Physical
Tampering/
Sabotage
Malicious Software Signed with Stolen Key