Report – Software and Hardware Supply Chain Security

Co-Leads: Navid Asadi (University of Florida), Akond Rahman (Tennessee Tech University), and Laurie Williams (NC State University)

Description: Attackers are increasingly using the software and hardware supply chain as an attack vector. This breakout group focused on identifying similarities and differences between software and hardware supply chain security so the security community can share a common vocabulary, leverage the research in overlapping areas, and consider the convergence of software/hardware supply chain into a joint threat model. Additionally, a convergence can enable communications between government agencies on research in hardware and software supply chain security (e.g. NSF, DoD, DHS, NIST).

1. Is there an existing body of research and/or practice? What are some highlights or pointers to it?
    - CHIP Act, SHIP (State-of-the-art Heterogeneous Integrated Packaging)
    - Advanced Packaging and heterogeneous integration. How the new packaging will impact the hardware supply chain
    - Executive Order 14028 (EO 14028) Section 4 and associated standards and regulations
    - Industry has responded to EO 14028 through a number of industry-wide initiatives: Linux Foundation/Open Source Security Foundation (OpenSSF; https://openssf.org/), Supply chain Levels for Software Artifacts (SLSA; https://slsa.dev/), and others
2. What are important challenges that remain? Are there new challenges that have arisen based on new models, new knowledge, new technologies, new uses, etc?
    - Agree on a common
        i. Threat model: who is the victim and who is the attacker
        ii. Attack phase: at what phase through the supply chain the attack is exploited
        iii. Standards: can we define similar language for standards between hardware and software
        iv. Impact on:
            1. Human lives: how critical the impact can be on human lives
            2. Cost: Loss of intellectual property, privacy-related costs due to breaches
    - Quantify the risk and come up with different levels for associated risk
    - Unknown unknowns: providing the assurance at time zero
    - Software automation pipelines
    - Evolving technology stack for hardware and software

3. Are there promising directions to addressing them? What kinds of expertise and collaboration is needed (disciplines and subdisciplines)?
    - Forensic and provenance analysis
    - Interdisciplinary research in SW/HW (electronics, computer science, materials, fabrication)
    - Verification (H/W, S/W)
    - Human factors: intent vs lack of knowledge, nature of contributions
    - Policy making and enforcement: cybersecurity, political science, software, hardware
    - Internet of things (low-powered devices that send data to cloud-based infrastructures)

4. What are important terminologies/vocabulary used in software and/or hardware supply chain security that should be used and defined in common (e.g. hardware having defensive focus [e.g. countermeasure], software having offensive focus [e.g. attack]; attack vector)
    - Malicious clones: In hardware, the clone will have duplicate functionality through unauthorized access to the “design”; the designer loses their intellectual property but the user is not harmed. In software, clones are duplicated packages often copied and re-deployed via typosquatting, forking, etc.; and the user is deceived and does not receive an authentic, supported product/package and may receive a version containing intentionally-injected vulnerabilities.
    - Age: Older hardware can be resold as new with a shorter life-span than expected. In the case of software, age is related to the use of an unsupported version of a package. In both hardware and software, defects and vulnerabilities may not be fixed.
    - Credentials: In the case of hardware, keys and secrets that are distributed post deployment. In the case of PUFs, benign manufacturing variation can be used for device identifiers. For software, secrets refer to hard-coded passwords and SSH keys in source code, container build environments, version control history etc.
    - Counterfeiting: A counterfeit piece of hardware may be known as an explicit substitution for the desired/authentic product made for monetary benefits. In software, the term counterfeit is not generally used (see malicious clone) Trojaned build environment.
    - Build infrastructure: In hardware, electronics production involves tools and methods used to design, fabricate, and test electronics components and systems. In software, build infrastructure includes tools and scripts to compile, build, and deploy a product. Nefarious instructions can be injected into these tools/methods/scripts to result in a malicious artifact.
    - Third-party components. A component produced by a trusted or untrusted outside organization integrated into a product.

Trends: Software supply chain attacks historically have been attackers finding and exploiting unintentionally-injected vulnerabilities and is moving to include intentionally-injecting and exploiting vulnerabilities.   Hardware supply chain attacks historically have been attackers intentionally-injecting and exploiting vulnerabilities and is moving to include finding and exploiting unintentionally-injected vulnerabilities (a.k.a Spectre/Meltdown).

5. How can we build better synergies between SW/HW supply chain security?
    - Allocate more resources: workshops, share infrastructure, lab equipment, workforce, etc.