Task 1:

Containers are used to package applications in an isolated user space, sharing the same kernel. This makes them lightweight and easy to deploy. However, the use of a shared kernel brings with it some security risks. Since all containers run on the same Operating System, a vulnerability in the kernel can affect all containers as well as the host. Systems like namespaces and cgroups can be used to help isolated resources used by the containers, they are not as secure as a hypervisor.

Virtualisation is used to create a virtual representation of a computing environment compared to a physical environment. This allows several VMs to run on a single physical computer or server. Each VM can then run independently from each other while sharing the resources of the physical machine. Since each VM has it’s own kernel, one VM being compromised doesn’t affect the other VMs or the host. This is done by the use of a hypervisor. However, hypervisors themselves can be the target of attacks. Vulnerabilities in the hypervisor can allow an attacker to “escape” the VM and compromise the host or other VMs. While running VMs can be more secure than using containerisation, it also comes at a performance cost.

- https://www.redhat.com/en/topics/containers
- https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-virtualization
- https://aws.amazon.com/what-is/virtualization/

Task 2:

Upholding a secure supply chain is crucial for any company to prevent any tampering with the products, limiting customer or company data breaches, and upholding the integrity of the company and the products it produces.

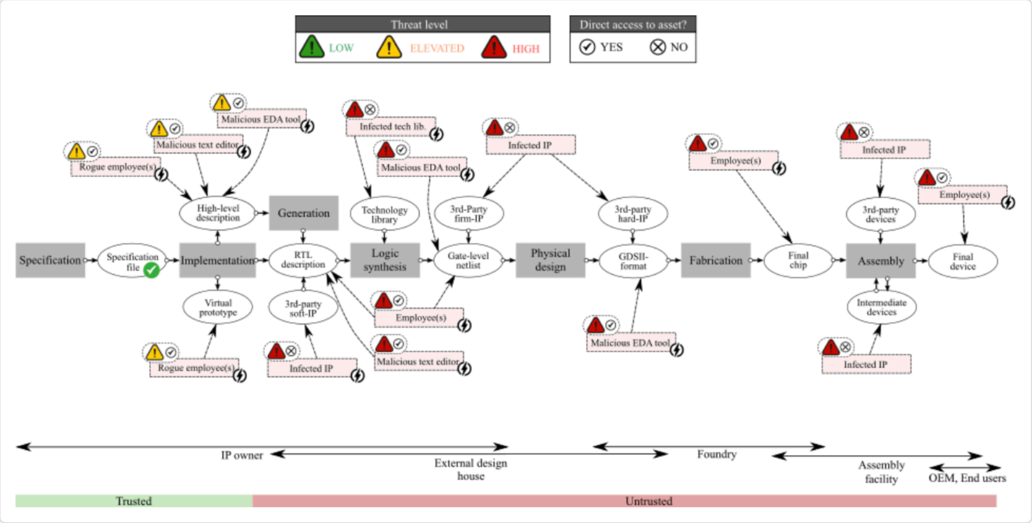
1. Hardware Supply Chain

Actors:
- Company X: Manufactures the parts for the router
- Transport Company Y: Transports the parts
- Factory Z: Assembles the parts into the full router
- Retailer A: Sells the routers

To prevent tampering of company products during transportation, Company X must implement tamper-evident seals for any parts created. Trucks driven by Transport Company Y must further be equipped with GPS tracking for any deliveries done for Company X.

Any third-party supplier (Company X) must be certified by a trusted authority and be subjected to regular security audits by a trusted auditing company. This includes evaluating facilities and making sure proper access control is maintained for employees of the companies.

An example of many possible vulnerabilities within the Hardware Supply Chain (https://vision.hipeac.net/cybersecurity--integrity-of-hardware-supply-chains.html):



2. Software Supply Chain

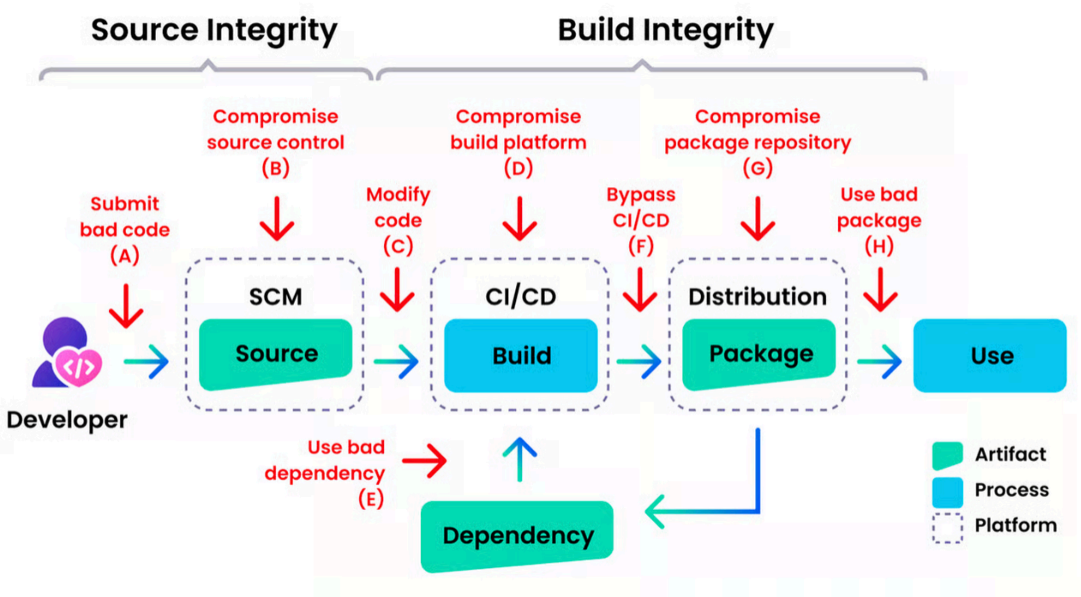
Actors:
- In-house employees
- Company B: Software Auditors

For any software deployed by in-house developers, a strict source code management policy that includes multi-layered version control should be implemented. Further, regular third-party code audits should be conducted by Company B.

All development tools should be hosted on a secure cloud platform with zero-trust architectural rules. This means that no single actor has unmonitored or unrestricted access to software repositories within the cloud. All users must use a secure password along with MFA to best secure the environment.

To prevent bad code from affecting the system, all software updates should be cryptographically signed to ensure integrity. Implementing Endpoint Detection and Response systems to monitor deployment of software is also crucial.

An example of possible vulnerabilities within the Software Supply Chain (https://tldrsec.com/p/supply-chain-security-overview):



3. Employee and Insider Threat Management:

Use User Behavioral Analytics to monitor in-house employees for any unusual activity. UBA tools could detect off patterns such as large or unusually common downloads, strange login times and login attempts. It is important, however, to make sure privacy concerns of the employees is addressed and properly deal with.

Another important step is regular security training for all employees within the supply chain. This includes but is not limited to: phishing tests (ex: emails), secure handling of company property (both hardware and software), and data protection protocols.

Types of insider threats (https://www.ekransystem.com/en/blog/insider-threat-definition):

Types of insider threats according to Verizon

Careless employees

who thoughtlessly click on links in phishing emails

Regular employees

who don't follow cyber security best practices

Malicious insiders

who use their access to steal and sell sensitive corporate and consumer data

Disgruntled employees

who seek to disrupt business operations or access information for personal gain

Third parties

who compromise your security by misusing your assets