



Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

1.1.3 Hardware supply chain Threats

Concepts (extracted from automatically generated subtitles):

Threat actor. Supply chain. Most obvious threat. Unintended actions. Much work. Potential threat. Impact of a threat actor. Outgoing device. Happy times. Person of authority. Subtle actions. Example. Competitors' technology. Ips. Last step.



[to video sequence search](#)

(within Understanding the digital supply chain and its stakes for humanitarian actors.)



[to video](#)

Center for Digital Education. More educational support material here:

<https://www.epfl.ch/education/educational-initiatives/cede/educational-technologies-gallery/boocs-en/>

page 1/20

THE HARDWARE AND SOFTWARE SUPPLY CHAINS

The Hardware Supply Chain: Threats

Shweta Shinde

Assistant Professor - Secure & Trustworthy Systems Group at ETH Zurich



...

notes

summary

0m 0s



Threats to Hardware Supply Chain



Now that you know how the supply chain is supposed to work in happy times, let's take a look at what can go wrong and why.

notes

summary

0m 4s



Threats to Hardware Supply Chain



Counterfeit IP Insertion: Threat actors can introduce fake or malicious intellectual property into chips.

IP Theft: Stealing intellectual property to avoid licensing fees or access competitor technology.

Tampering Sanctions: Producing chips without proper licenses or violating usage agreements.

Component Alteration: Replacing or misplacing components with subpar quality alternatives.

There are many things that can go wrong. If there is a threat actor, they can deliberately insert elements in each of the steps. Adding fake or counterfeit IPs to perform unintended actions is one example to backdoor a chip, and is perhaps the most obvious threat. But there are other subtle actions that a threat actor can perform. Let's look at a few possibilities.

notes

summary

0m 13s



Threats to Hardware Supply Chain



Counterfeit IP Insertion: Threat actors can introduce fake or malicious intellectual property into chips.

IP Theft: Stealing intellectual property to avoid licensing fees or access competitor technology.

Tampering Sanctions: Producing chips without proper licenses or violating usage agreements.

Component Alteration: Replacing or misplacing components with subpar quality alternatives.

Stealing IPs to avoid paying licensing fees,

notes

summary

0m 44s



Threats to Hardware Supply Chain



Counterfeit IP Insertion: Threat actors can introduce fake or malicious intellectual property into chips.

IP Theft: Stealing intellectual property to avoid licensing fees or access competitor technology.

Tampering Sanctions: Producing chips without proper licenses or violating usage agreements.

Component Alteration: Replacing or misplacing components with subpar quality alternatives.

or get access to competitors' technology, producing chips without buying licences, or violating sanctions or even usage agreements,

notes

summary

0m 49s



Threats to Hardware Supply Chain



Counterfeit IP Insertion: Threat actors can introduce fake or malicious intellectual property into chips.

IP Theft: Stealing intellectual property to avoid licensing fees or access competitor technology.

Tampering Sanctions: Producing chips without proper licenses or violating usage agreements.

Component Alteration: Replacing or misplacing components with subpar quality alternatives.

altering the components by misplacing them or replacing them with subpar quality.

notes

summary

1m 1s



Complex Chain



Design

IP (Intellectual Property)
in hardware language.



Fabrication

Physical layout design,
create mask for silicon
wafer, produce chips.



Assembly

Combine several chips,
integrate into building
blocks or products.



Distribution

Package in different form
factors, send to
manufacturers/consumers.

In other words, each step in the supply chain is a potential threat.

notes

summary

1m 6s



Threats to Hardware Supply Chain



Scale of impact: From targeting one batch of components to affecting all components...

Each person or entity that participates in the supply chain can alter the outcomes. The impact of a threat actor's actions

notes

summary

1m 13s



Threats to Hardware Supply Chain



Scale of impact: From targeting one batch of components to affecting all components...

can be as small as targeting one batch of components. For example, if they physically tamper with the outgoing device, or on the other hand, it can possibly impact all components. An example here would be implementing a weak encryption scheme.

notes

summary

1m 25s



Threats to Hardware Supply Chain



Nature of impact: From bad / non-functioning products to fully compromised ecosystems.

The outcomes of these threats can just be bad, or nonfunctional products. Or on the other extreme, it can be all the way to a fully compromised ecosystem. Imagine the threat actor has complete access to the infrastructure, and can observe or change all the data and communications. Detecting these threats is not always easy.

notes

summary

1m 44s





Seeding: An early-stage Manipulation

- Manipulate the manufacturing process directly.
- Add backdoor hardware directly into the component.
- Needs access to the factory.
- But difficult to detect.

Let's take a look at two approaches that a threat actor can use. Seeding is a method where a threat actor

notes

summary

2m 14s





Seeding: An early-stage Manipulation

- Manipulate the manufacturing process directly.
- Add backdoor hardware directly into the component.
- Needs access to the factory.
- But difficult to detect.

directly manipulates the manufacturing process. Their goal is to add hardware backdoors to the components. As the name suggests,

notes

summary

2m 25s





Seeding: An early-stage Manipulation

- Manipulate the manufacturing process directly.
- Add backdoor hardware directly into the component.
- Needs access to the factory.
- But difficult to detect.

the aim is to sow the bad seed as early as possible, and then reap the benefits when the component is deployed widely. Now, as you can imagine,

notes

summary

2m 37s





Seeding: An early-stage Manipulation

- Manipulate the manufacturing process directly.
- Add backdoor hardware directly into the component.
- Needs access to the factory.
- But difficult to detect.

this approach requires the threat actor to have high level of access to the factory facilities. While seemingly difficult, this is not impossible to achieve. A threat actor can impersonate a person of authority,

notes

summary

2m 49s





Seeding: An early-stage Manipulation

- Manipulate the manufacturing process directly.
- Add backdoor hardware directly into the component.
- Needs access to the factory.
- But difficult to detect.

or even bribe or threaten the factory employees to tamper with the process.

notes

summary

3m 1s





Interdiction

- Hijack a component while it is in transit.
- Modify the component, such as by adding extra hardware.
- Repackage the tampered and continue its delivery.

If you think seeding is too much work and risk, there is a low effort alternative.

notes

summary

3m 8s





Interdiction

- Hijack a component while it is in transit.
- Modify the component, such as by adding extra hardware.
- Repackage the tampered and continue its delivery.

It is called interdiction, and the idea is very simple. First, hijack the component when it is in transit,

notes

summary

3m 13s





Interdiction

- Hijack a component while it is in transit.
- Modify the component, such as by adding extra hardware.
- Repackage the tampered and continue its delivery.

say, from one factory to another or from manufacturer to end user. Then the threat actor can tamper with the component, say, by placing additional hardware on it.

notes

summary

3m 25s



Image reference



In order of appearance

PICTURE1 : Supply Chain concept by tippapatt from Adobe Stock

ICON1 : Created by Sharon Showalter from Noum Project

ICON2 : Created by Napisah from Noum Project

ICON3 : Created by Elsa from Noum Project

ICON4 : Created by Eko Pumomo from Noum Project

PICTURE3 : Image generated by gamma.ai

PICTURE4 : Image generated by gamma.ai

The last step is to repackage the component, and send it off on its way. The trick is to get access to the transport, and then tamper without getting detected, and there you have it.

notes

summary

3m 37s


