



Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

1.2.2 Supply Chain Overview

Concepts (extracted from automatically generated subtitles):

Software supply chain attacks. External components. Today's software. App developers. Software development. Source code perspective. Build environments. Larger software development ecosystem. Mobile phone apps. Application code. Download software. Jigsaw puzzle. Functional components. Software libraries. Developer perspective.



[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 1/32

THE HARDWARE AND SOFTWARE SUPPLY CHAINS



The Software Supply Chain Overview

Mathias Payer

Associate Professor - HexHive Laboratory at EPFL



...

notes

summary

0m 0s



The Software Supply Chain Overview



Android messaging app

Developers **Software is Modular**

Relies on external libraries for functions like image processing, cryptography, and audio encoding, enabling developers to save time by reusing code.

Security Risks

Attackers can exploit weaknesses in any point in this chain, from dependencies to libraries or tools.



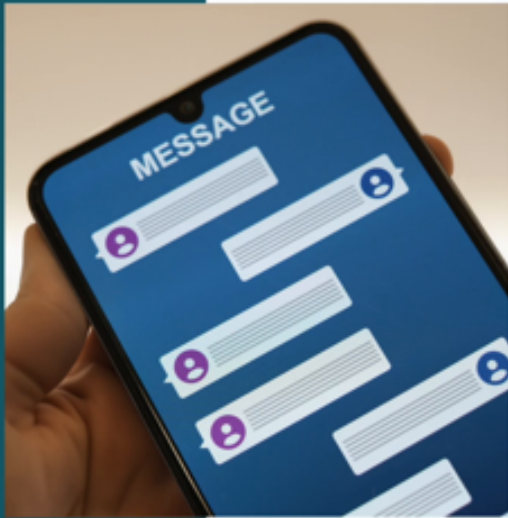
Let me introduce software supply chain attacks through the overview figure that you have already seen at the beginning of this module. Today's software is highly modular and extremely complex. Like a jigsaw puzzle, software is modular and built out of many diverse blocks.

notes

summary

0m 2s





Android messaging app

Development Ecosystem

Relies on external libraries for functions like image processing, cryptography, and audio encoding, enabling developers to save time by reusing code.

Security Risks

Attackers can exploit vulnerabilities at any point in this chain, targeting libraries or tools to compromise the app.

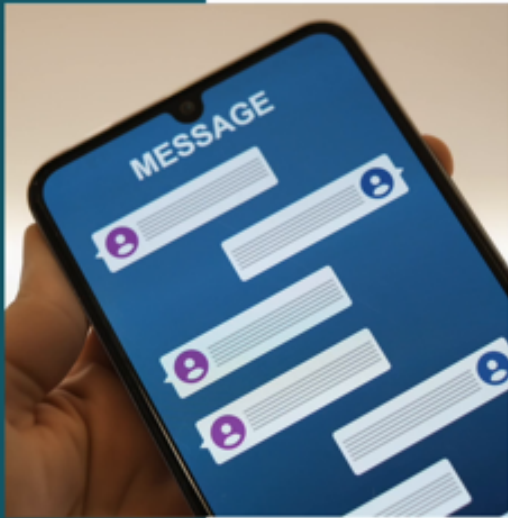
For example, an Android messaging application contains

notes

summary

0m 23s





Android messaging app

Development Ecosystem

Relies on external libraries for functions like image processing, cryptography, and audio encoding, enabling developers to save time by reusing code.

Security Risks

Attackers can exploit vulnerabilities at any point in this chain, targeting libraries or tools to compromise the app.

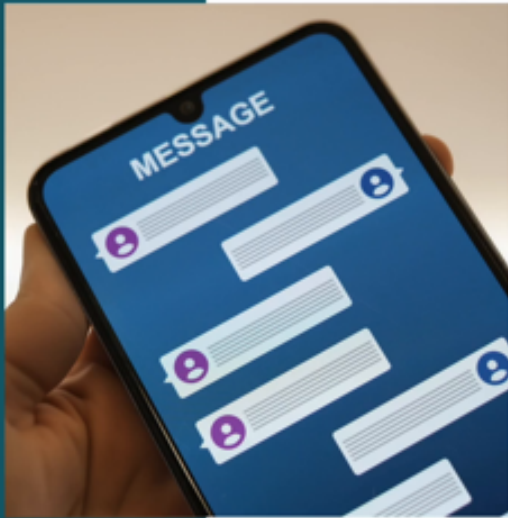
libraries for image processing, audio encoding, emojis, cryptography, text input or guest recognition and many more.

notes

summary

0m 25s





Android messaging app

Development Ecosystem

Relies on external libraries for functions like image processing, cryptography, and audio encoding, enabling developers to save time by reusing code.

Security Risks

Attackers can exploit vulnerabilities at any point in this chain, targeting libraries or tools to compromise the app.

App developers rely on external components for these libraries and heavily reuse existing code to reduce the implementation cost.

notes

summary

0m 37s



Two Perspectives on Software



There are two perspectives, the source code perspective and the developer perspective.

notes

summary

0m 45s



Two Perspectives on Software



The Source Code Perspective

Software consists of:

- Functional components
- Access to libraries

The application code integrates functionalities.

From the source code perspective, software consists of functional components that each provide some functionality. In addition, software libraries provide access

notes

summary

0m 50s



Two Perspectives on Software



The Source Code Perspective

Software consists of:

- Functional components
- Access to libraries

The application code integrates functionalities.

Developer Perspective

Software development follows standardized process and best practices.

to frameworks and other larger grouped functionalities. The application code then glues together the necessary functionalities to assemble the desired app.

notes

summary

1m 1s



Two Perspectives on Software



The Source Code Perspective

Software consists of:

- Functional components
- Access to libraries

The application code integrates functionalities.

Developer Perspective

Software development follows standardized process and best practices.

Now from the developer perspective, software development follows standardised processes

notes

summary

1m 13s



Two Perspectives on Software



Developer Perspective

Software development follows standardized process and best practices.

and best practises rely on diverse tools such as build environments, integrated developer environments, compilers, or testing frameworks. Together they formed a larger software development ecosystem.

notes

summary

1m 18s



Two Perspectives on Software



Security Risks

Attackers can exploit vulnerabilities at any point in this chain, targeting libraries or tools to compromise the app.

An attacker may plant vulnerabilities anywhere in this ecosystem

notes

summary

1m 34s



The Software Supply Chain Overview



along the chain of included libraries or tools to exploit some target software. Let's now break the software supply chain into individual steps.

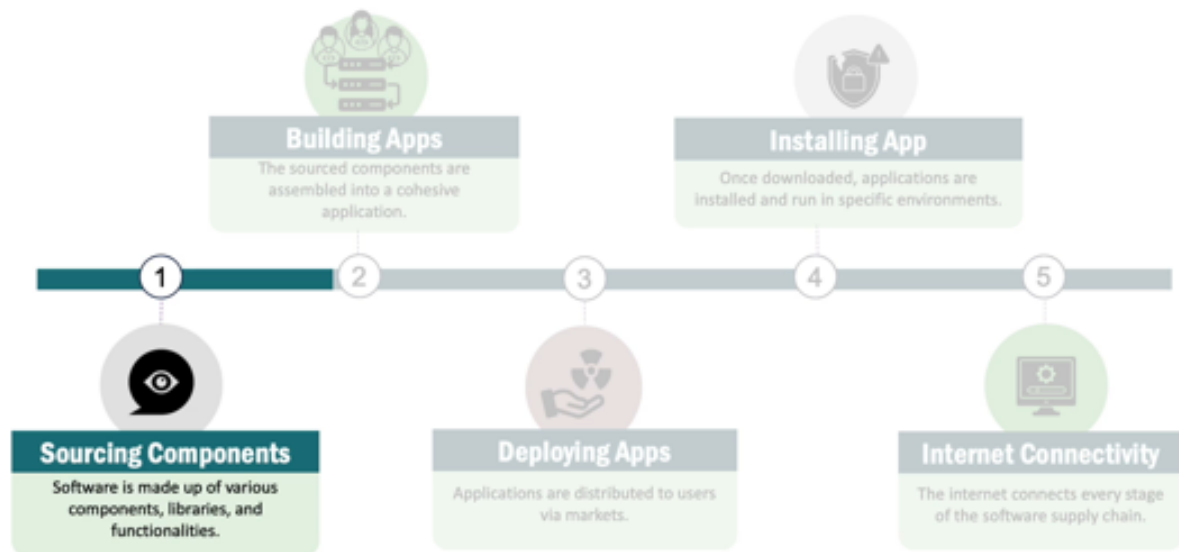
notes

summary

1m 37s



The Software Supply Chain Overview



Software consists of diverse components, libraries, and functionalities

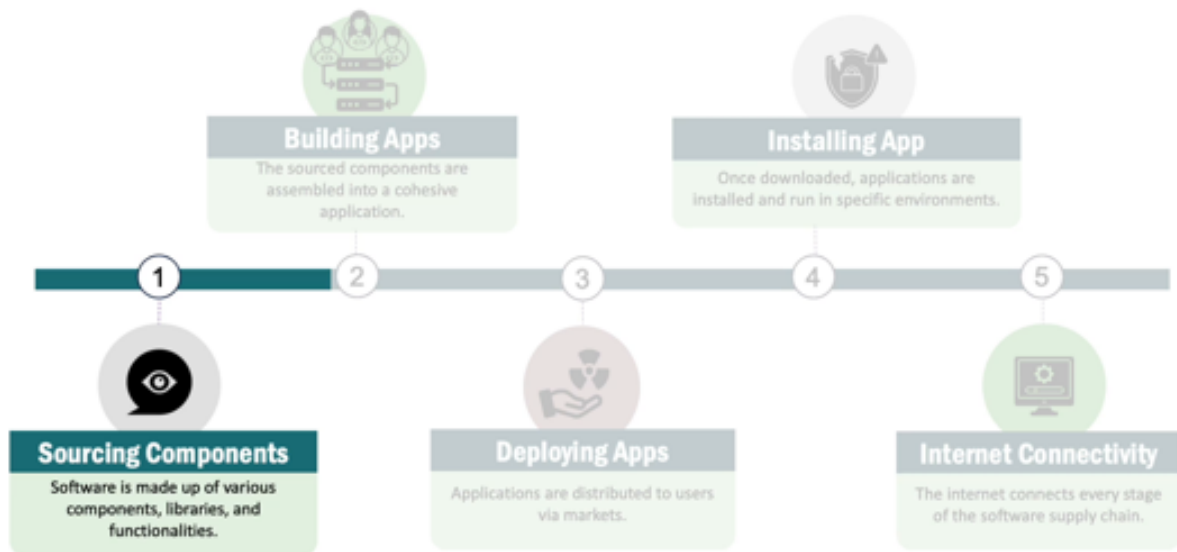
notes

summary

1m 49s



The Software Supply Chain Overview



that are bought from a vendor or downloaded from an open source platform like GitHub.

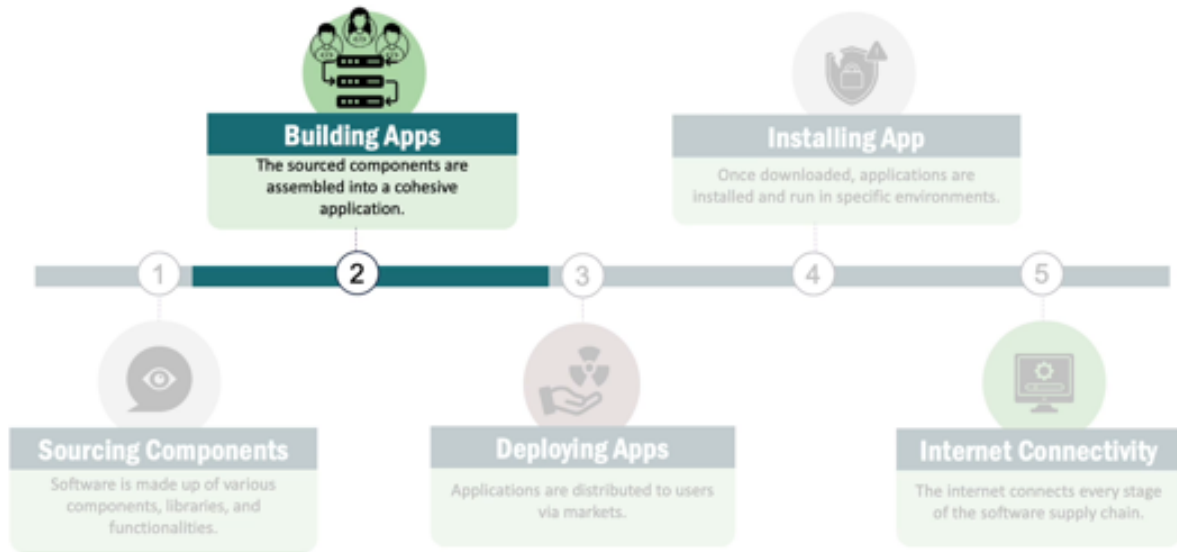
notes

summary

1m 53s



The Software Supply Chain Overview



Components may contain bugs or may even be maliciously compromised. To build an application, these components are connected and glued together using build systems that validate and check for functionality. Due to the complexity of all components, it is challenging for any developer or team to oversee the system end to end.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

2m 1s



.....

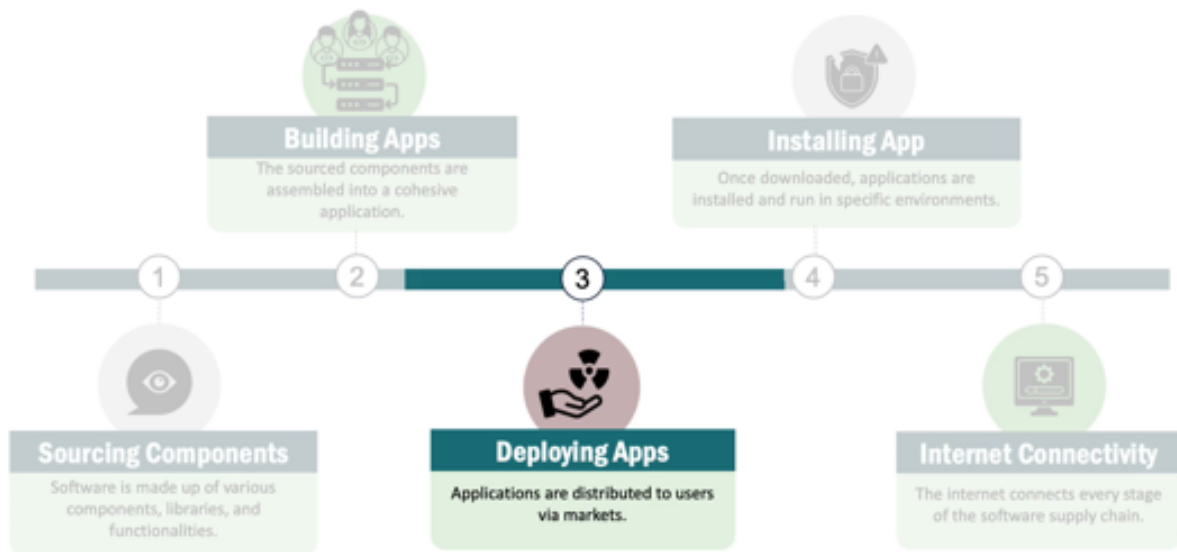
.....

.....

.....

.....

The Software Supply Chain Overview



Applications are deployed into a market such as those for mobile phone apps

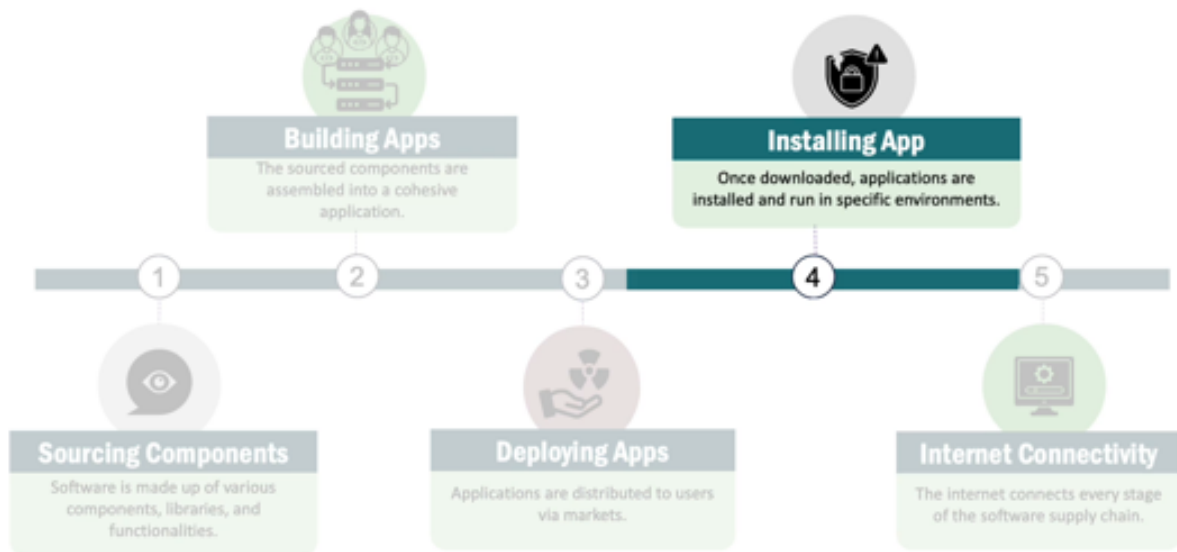
notes

summary

2m 22s



The Software Supply Chain Overview



where users can download applications and install them. Similar markets exist for server applications.

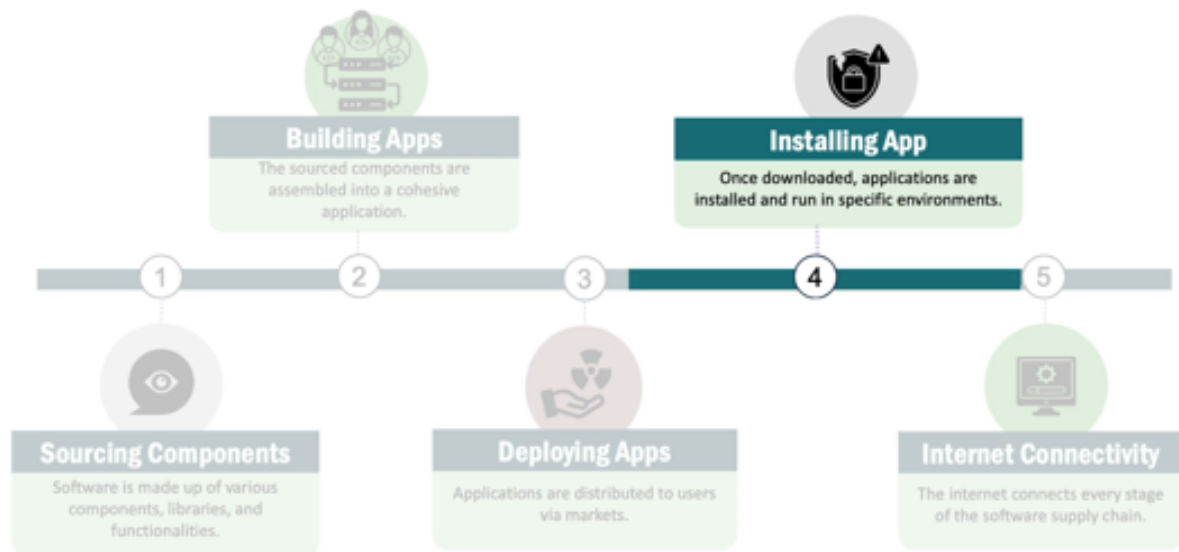
notes

summary

2m 25s



The Software Supply Chain Overview



After software is downloaded on devices, it is installed and deployed

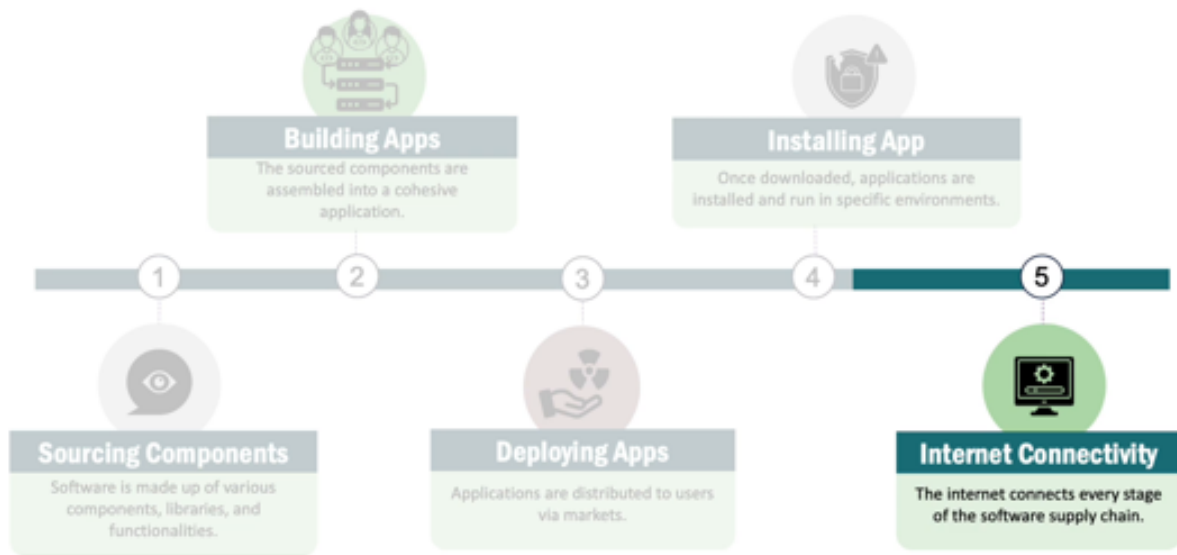
notes

summary

2m 37s



The Software Supply Chain Overview



with a concrete configuration to serve its purpose. Apps are used on phones in particular settings with private user data while server applications may process the sensitive data of millions of users. The internet is ubiquitously used to download packages, libraries,

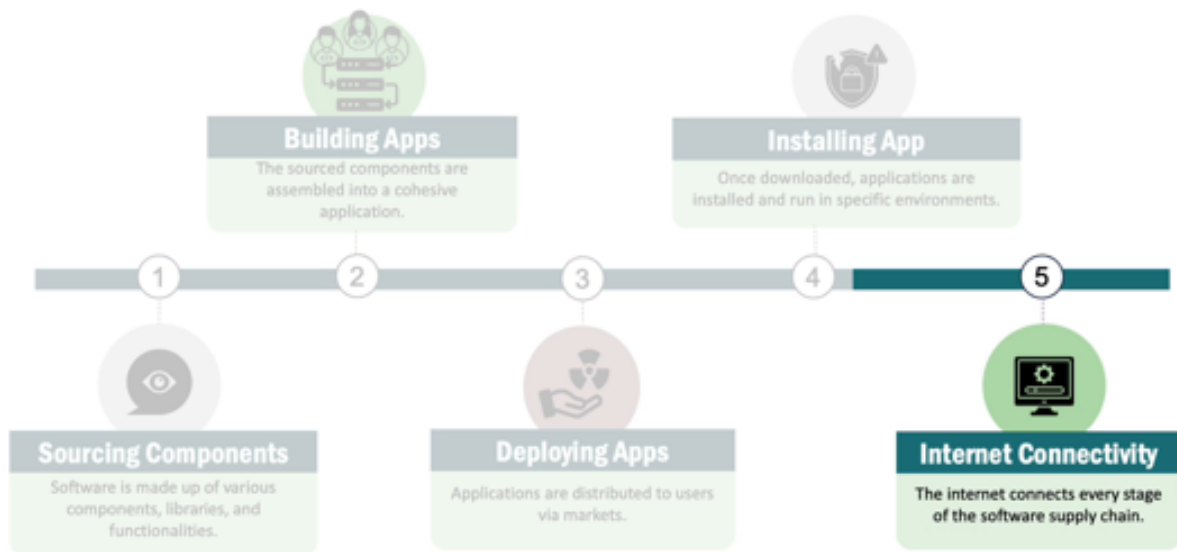
notes

summary

2m 38s



The Software Supply Chain Overview



upload software to markets, or download software to servers.

notes

summary

3m 0s



Software Development



Software Development is built on:

- Extensive frameworks
- Diverse external libraries

Which are selected according to requirements and functionalities.

All of these connections must be protected against adversaries. Software development captures two of the key phases of the software supply chain.

notes

summary

3m 1s



Software Development



Software Development is built on:

- Extensive frameworks
- Diverse external libraries

Which are selected according to requirements and functionalities.

Today's applications are built using extensive frameworks and diverse libraries from varying provinces. Following software development practise processes and best practises,

notes

summary

3m 13s



Software Development



Software Development is built on:

- Extensive frameworks
- Diverse external libraries

Which are selected according to requirements and functionalities.

developers create requirements and select the best framework and environment to develop their application along with searching for libraries that cover required functionalities.

notes

summary

3m 25s





Need to accept and integrate risks related with external frameworks and libraries as:

- They have the same rights and privileges as in-house code.
- Might be buggy, or even compromised and malicious.
- They are controlled externally (for patches).

When using external frameworks and libraries, developers integrate and accept the risk for these components. It is very important to understand that any included component has the same rights and privileges as the code developed in house.

notes

summary

3m 37s





Need to accept and integrate risks related with external frameworks and libraries as:

- They have the same rights and privileges as in-house code.
- Might be buggy, or even compromised and malicious.
- They are controlled externally (for patches).

Included components may be buggy or even compromised and malicious.

notes

summary

3m 49s



Software Development



Need to accept and integrate risks related with external frameworks and libraries as:

- They have the same rights and privileges as in-house code.
- Might be buggy, or even compromised and malicious.
- They are controlled externally (for patches).

Compared to in house developed components, any external dependencies are controlled externally. Discovered bugs must be patched by the original developers and the company depends on timely patches.

notes

summary

3m 52s



The Software Supply Chain Overview



Deploying apps

Deployment via Markets:

Software is uploaded to markets (e.g., app stores or open-source platforms) for users to discover and install on their devices.

Security Risks

Adversaries may compromise the market or the user's device, altering the software's configuration, settings, or binaries.

After software is built by a company, it needs to be deployed to

notes

summary

4m 7s



The Software Supply Chain Overview



Deploying apps

Deployment via Markets:

Software is uploaded to markets (e.g., app stores or open-source platforms) for users to discover and install on their devices.

Security Risks

Adversaries may compromise the market or the user's device, altering the software's configuration, settings, or binaries.

and installed on an end device through a market. Markets have become commonly known with the rise of mobile phones and our app ecosystem, but they have existed long before in the open source ecosystems

notes

summary

4m 13s



The Software Supply Chain Overview



Deploying apps

Deployment via Markets:

Software is uploaded to markets (e.g., app stores or open-source platforms) for users to discover and install on their devices.

Security Risks

Adversaries may compromise the market or the user's device, altering the software's configuration, settings, or binaries.

where distributors distribute for example Linux applications.

notes

summary

4m 25s



The Software Supply Chain Overview



Deploying apps

Deployment via Markets:

Software is uploaded to markets (e.g., app stores or open-source platforms) for users to discover and install on their devices.

Security Risks

Adversaries may compromise the market or the user's device, altering the software's configuration, settings, or binaries.

The software vendor uploads their application to the market, where it can then be discovered by the users and installed on their devices such as mobile phones, tablets, laptops, or servers. Adversaries may compromise the market itself

notes

summary

4m 30s





which stores the application binaries or the running application on the user's end by modifying the configuration, settings, or compromising the binary itself.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

4m 44s



.....

.....

.....

.....

.....