University of Geneva
Department Informatic

Backdoor

Information Systems Security

14X021

Michel Jean Joseph Donnet

October 9, 2025

Table of Contents

1 Theory

1.1 What is a backdoor

Backdoor is a mecanism that facilite access to

- service
- application
- ...

It can be created and used to maintain a software (with correct security measures !), but also for criminal purposes. However it's essentialy an entry point and not a kind of attack.

All backdoors are entry points for hackers !!!

Sources nexa.fr

1.2 Attack type

Attack	Target
Spoofing	Confidentiality
Tampering / Falsification	Integrity
Repudiation	Non repudiation
Information disclosure	Confidentiality
Denial of service	Disponibility
Exclanation of privileges	Authentification

Note Backdoor cover all this attacks !

1.3 Attack class

Attack class	Example
Hardware	Chips with exfiltration, reprogrammed FPGA chips
Firmware	Modification of firmware (disk, network device, …)
Software	Trojans, …
Supply-chain	Third party dependencies, software update, …
Network / Command & Control	Tunneling to another server, shell reverse, data extraction, …
Cryptographic / weak keys algorithm	Algorithm/key/RNG with vulnerabilities known by creator
Accounts	Hardcoded key in code, maintenance account not documented, …

1.4 Protection mecanism

- Check code and dependencies
- Log centralization and analysis
- Network trafic analysis
- Communication filtering
- Backup points
- …

2 Example 1

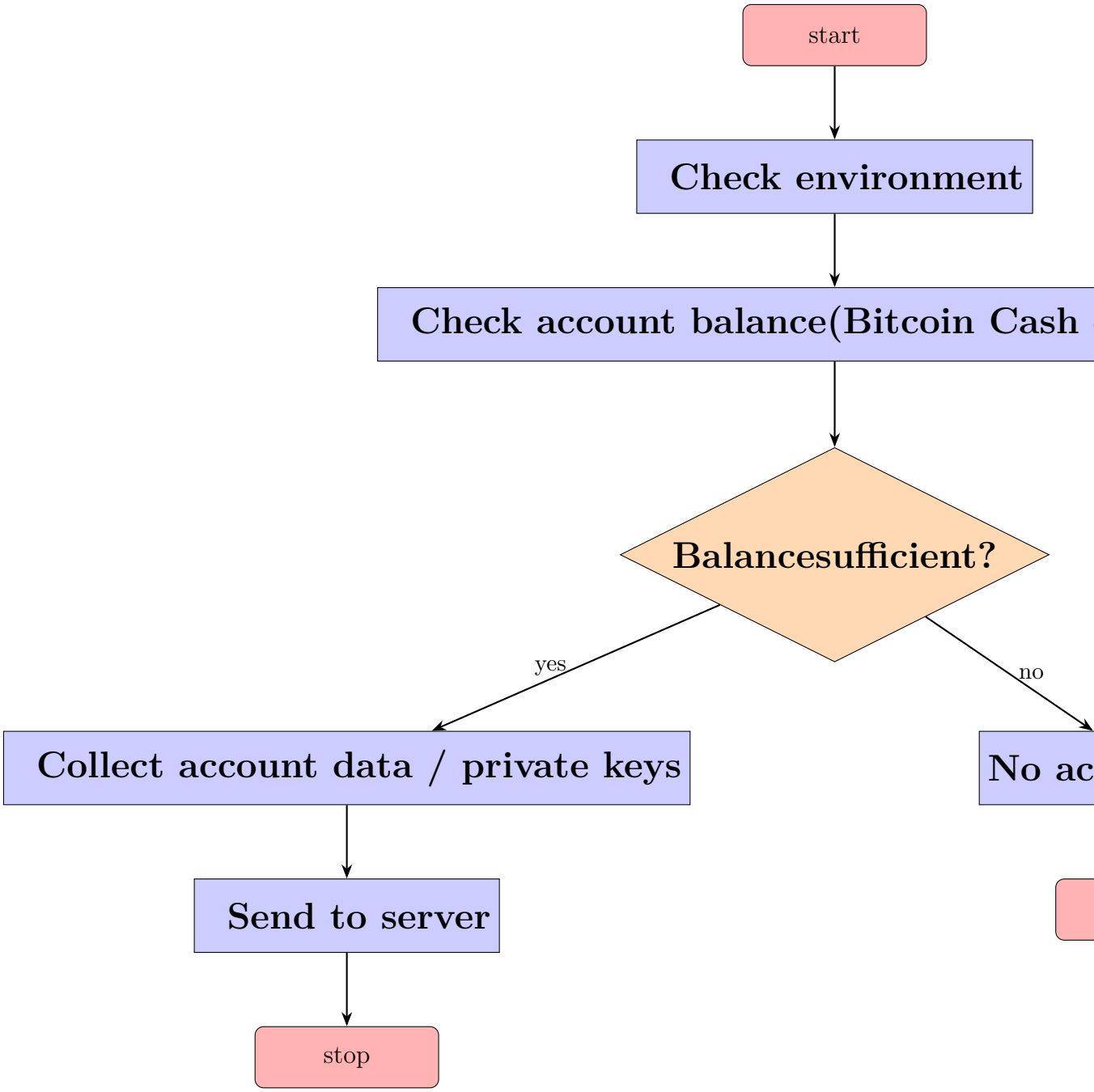
2.1 Flatmap-stream

"On the morning of November 26th, npm's security team was notified of a malicious package that had made its way into event-stream, a popular npm package. After triaging the malware, npm Security responded by removing flatmap-stream and event-stream@3.3.6 from the Registry and taking ownership of the event-stream package to prevent further abuse." from npm blog

2.2 Attack and target

Attacker earned confidence and take maintenance of `flatmap-stream`.

$$



$$

2.3 Note

It's a **social engineering attack** $\Longrightarrow$ Check the code delivered by others !!

3 Example 2

3.1 SolarWind attack (2020)

- Hackers infiltrated SolarWinds (Sep 2019)

- Spent month to test code injections in Orion, that manage metric performance (admin privileges !!)
- Backdoor "Sunburst" created in Orion
- SolarWind began to distribute update Orion with the backdoor (Mars 2020)
- Hackers wan access to network of victims
- criminal actions…

Sources: fortinet

3.2 Balance sheet

More than 18´000 clients are impacted

Pros:

- Companies share experience and good practices

Cons:

- Cost companies 11% of their annual revenue

4 Example 3

4.1 MIFARE backdoor

- Hardware backdoor on MIFARE contactless cards (cards from 2020)
- Enable to compromise all user-defined keys with knowledge of the backdoor by accessing the card in a few minutes
- Another hardware backdoor exist on older cards and is common to several manufacturers

Sources: Cryptology ePrint Archive, next, datasecuritybreach

4.2 Complementary informations

- Produced by **Shanghai Fudan Microelectronics Group**, one of China's leading chip manufacturers
- Over than 750 towns of more than 50 land use this system (contactless payment/access control, transport titles, …)
- Discovered by **Philippe Teuwen** from **Quarkslab** french compagny

5 Example 4

5.1 XZ Utils Backdoor

Discovered in 2024 by Andres Freund.

XZ utils (with liblzma) make the lzma compression and decompression (.tar.xz files)

It is often integrated to linux distribution as base package.

5.2 Social attack

A developer, Jia Tan, joined the project and make bug fixes, code improvement, pull requests, … He earns trust with his good work and began to receive repository permissions to commit.

Side by side, he (or they) used fake accounts to make lot of new feature requests and find a lot of bugs, so that the maintainer is overloaded.

Because of the work, the maintainer needed another maintainer to help him.

That's why Jia Tan receive maintainer permissions on the repository (release creation)

Source: akamai.com

5.3 Backdoor

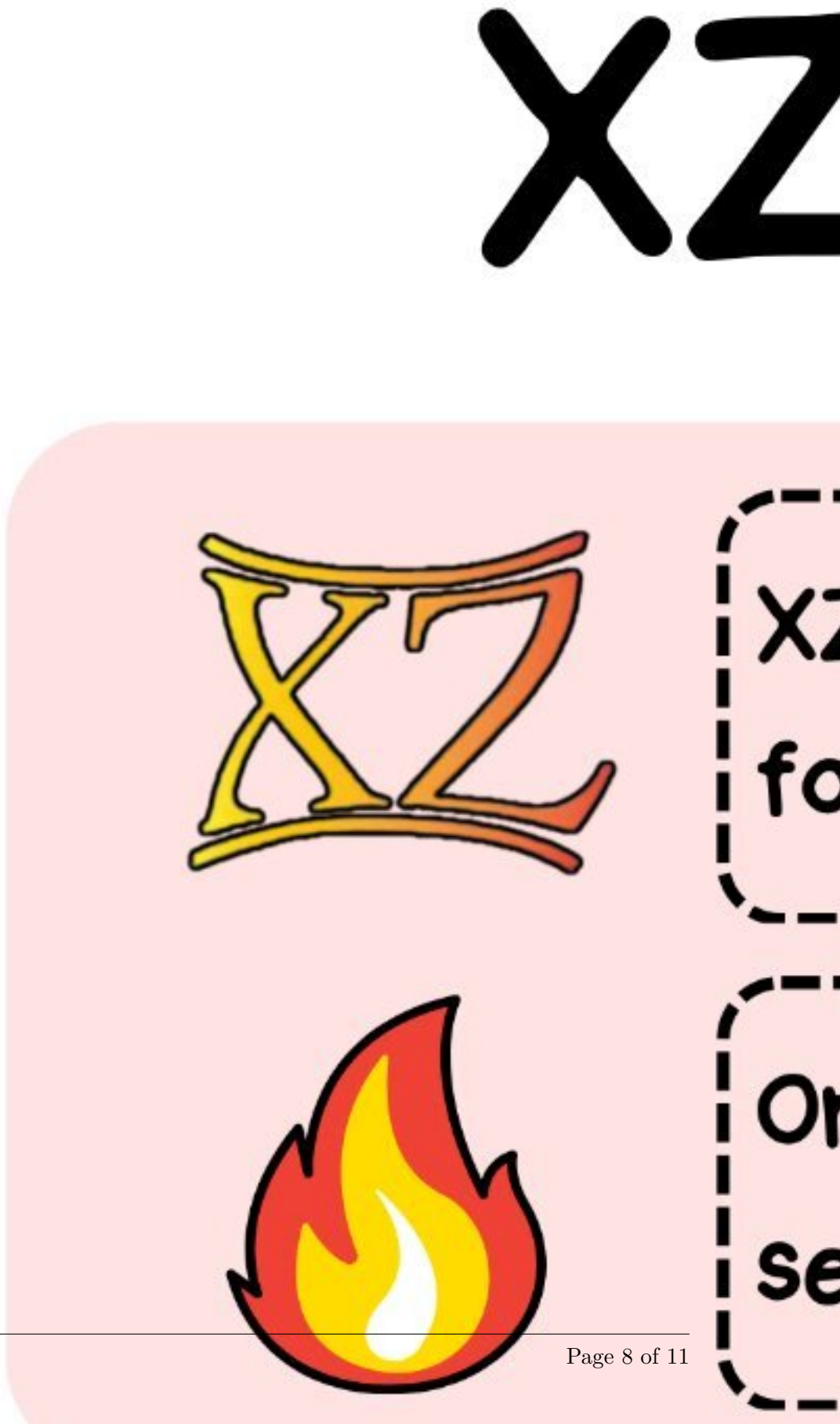
Backdoor introduced in a new release, only in source code tarball (compressed deliverable archive)

This backdoor is very complex.

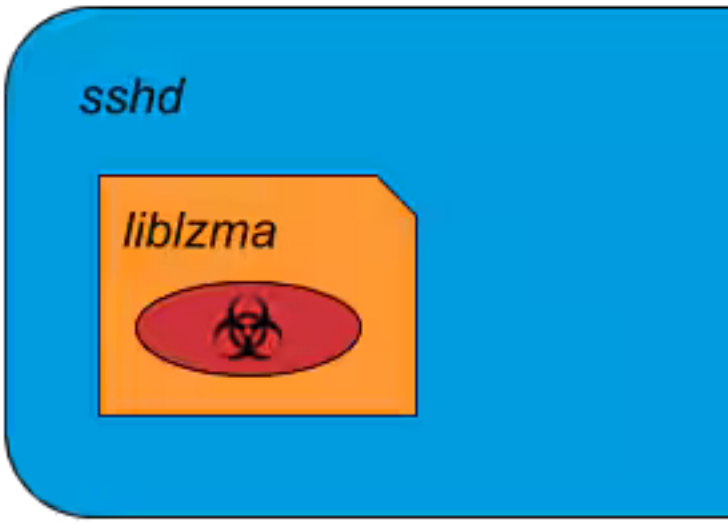
It infects ssh daemon, enabling attacker to execute arbitrary code on the remote machine.

It's the most intrusion made ever and have a critical score of 10/10 (CVSS)

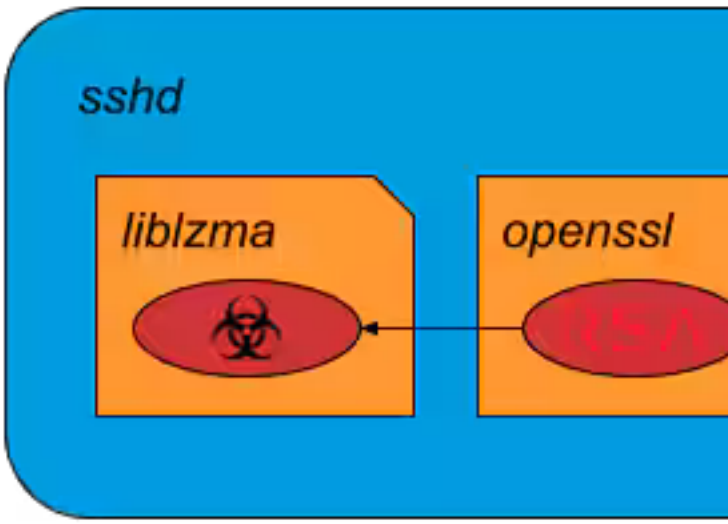
5.4 Backdoor attack graph



5.5 Backdoor attack graph 2



1. *liblzma* is loaded into
sshd during its startup



3. The hook interferes and
points the function symbo
a malicious implementati

6 Questions

- What is a backdoor ?
- What are the kinds of backdoors ?
- Give an example of backdoor