Cybersecurity Training for Users of Remote Computing

SEHET'23 @ PEARC'23

Marcelo Ponce[†] and *Ramses van Zon*[‡]

July 24, 2023

[†] Department of Computer and Mathematical Sciences, University of Toronto Scarborough
[‡] SciNet HPC Consortium, University of Toronto

Content

Motivation

Security Incident Example 1

2011 - Running bitcoin on a cluster's compute nodes

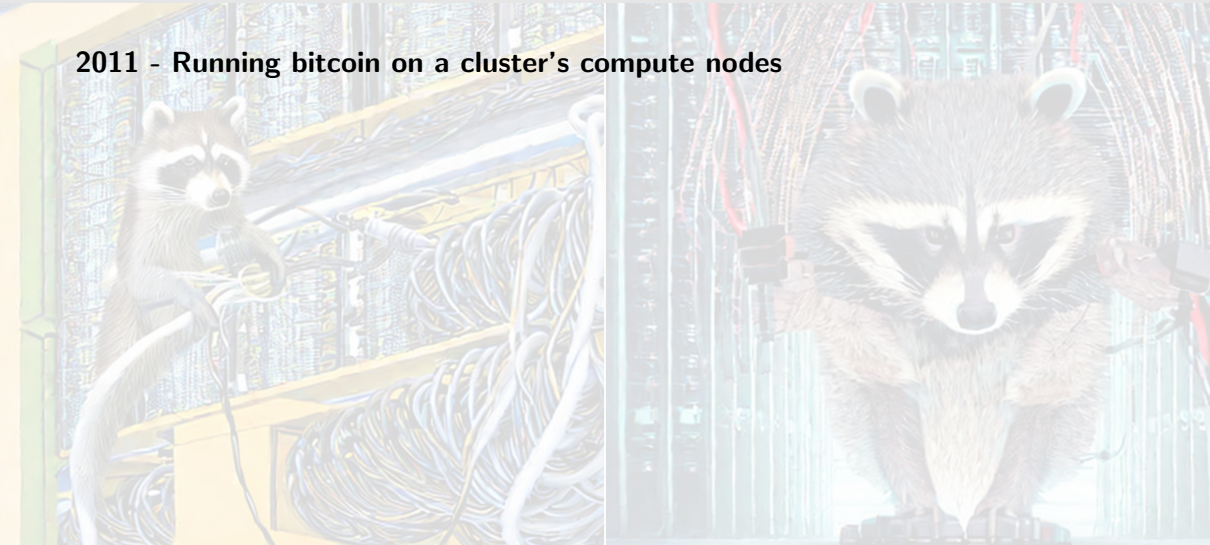
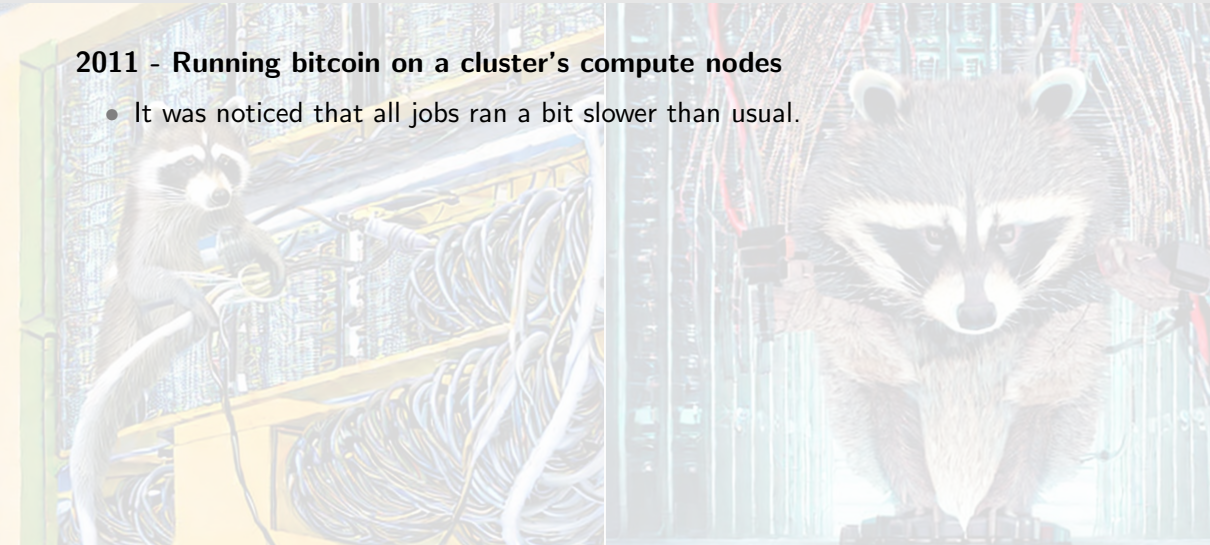


Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"raccoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Security Incident Example 1

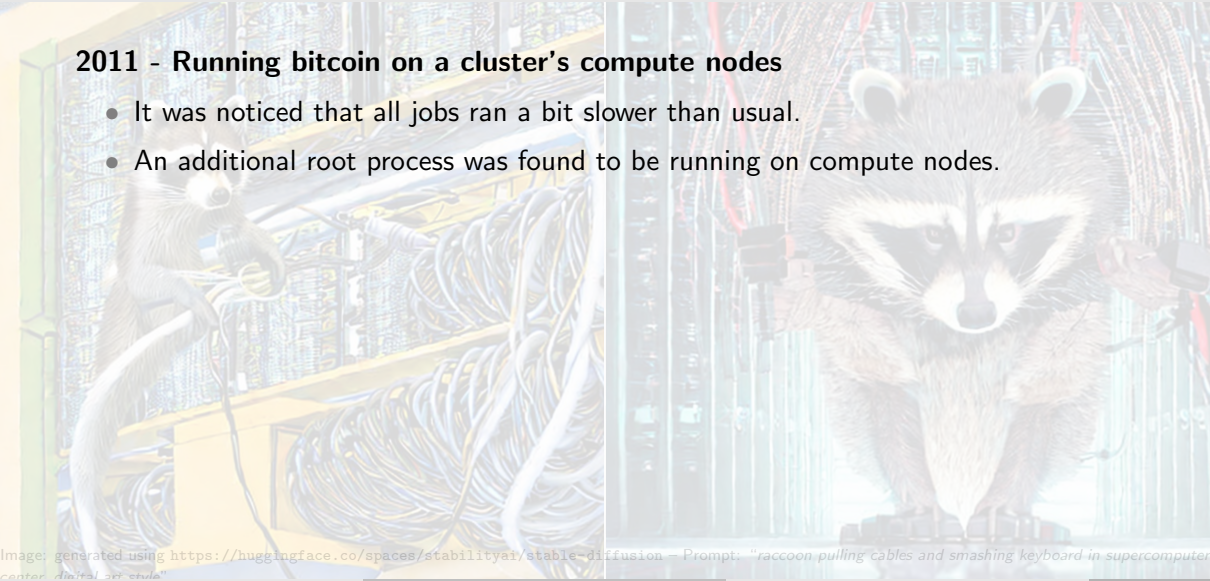


2011 - Running bitcoin on a cluster's compute nodes

- It was noticed that all jobs ran a bit slower than usual.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"raccoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Security Incident Example 1

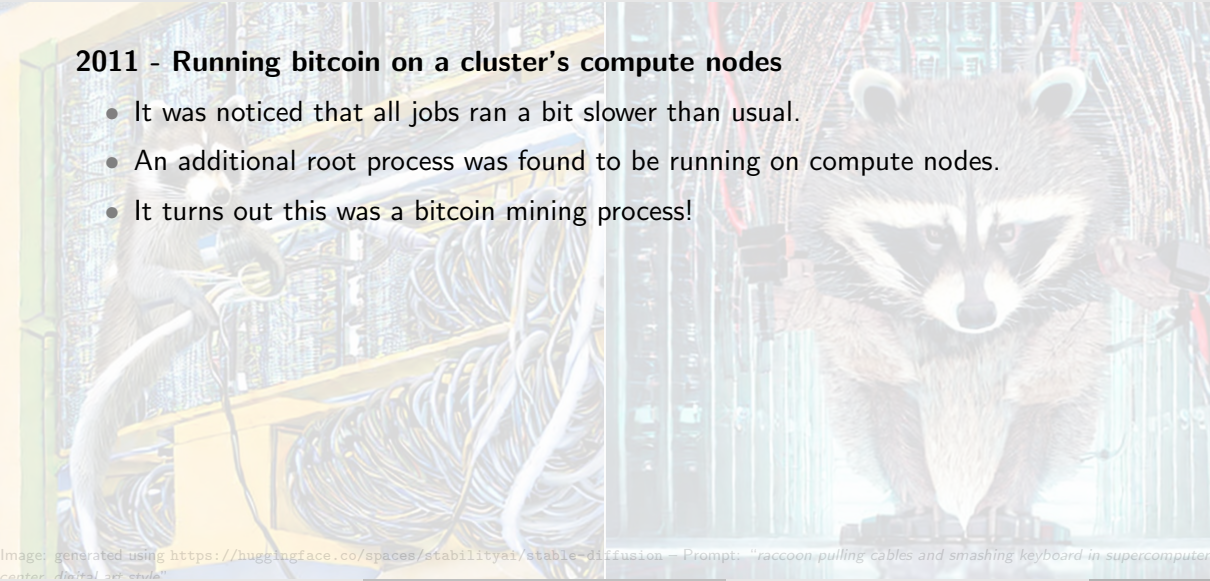


2011 - Running bitcoin on a cluster's compute nodes

- It was noticed that all jobs ran a bit slower than usual.
- An additional root process was found to be running on compute nodes.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"raccoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Security Incident Example 1

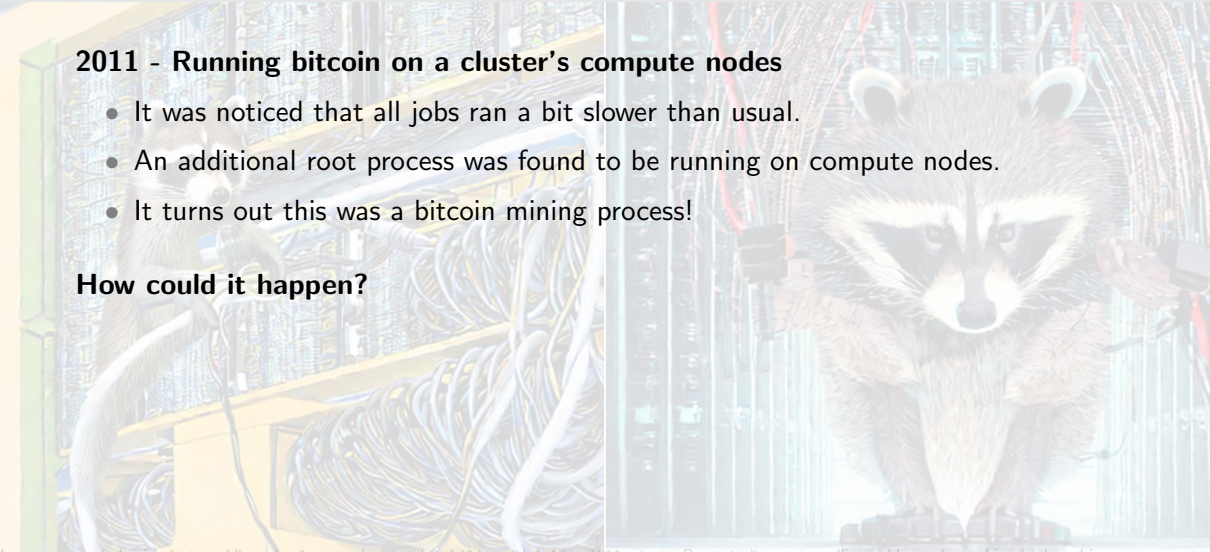


2011 - Running bitcoin on a cluster's compute nodes

- It was noticed that all jobs ran a bit slower than usual.
- An additional root process was found to be running on compute nodes.
- It turns out this was a bitcoin mining process!

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"raccoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Security Incident Example 1



2011 - Running bitcoin on a cluster's compute nodes

- It was noticed that all jobs ran a bit slower than usual.
- An additional root process was found to be running on compute nodes.
- It turns out this was a bitcoin mining process!

How could it happen?

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"raccoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Security Incident Example 1

2011 - Running bitcoin on a cluster's compute nodes

- It was noticed that all jobs ran a bit slower than usual.
- An additional root process was found to be running on compute nodes.
- It turns out this was a bitcoin mining process!

How could it happen?

- A user's password was compromised on a cluster.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"raccoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Security Incident Example 1

2011 - Running bitcoin on a cluster's compute nodes

- It was noticed that all jobs ran a bit slower than usual.
- An additional root process was found to be running on compute nodes.
- It turns out this was a bitcoin mining process!

How could it happen?

- A user's password was compromised on a cluster.
- With their account, a glibc bug was exploited on another cluster to get root access.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"raccoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Security Incident Example 1

2011 - Running bitcoin on a cluster's compute nodes

- It was noticed that all jobs ran a bit slower than usual.
- An additional root process was found to be running on compute nodes.
- It turns out this was a bitcoin mining process!

How could it happen?

- A user's password was compromised on a cluster.
- With their account, a glibc bug was exploited on another cluster to get root access.
- Sshd was replaced, and passwords sniffed.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"raccoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Security Incident Example 1

2011 - Running bitcoin on a cluster's compute nodes

- It was noticed that all jobs ran a bit slower than usual.
- An additional root process was found to be running on compute nodes.
- It turns out this was a bitcoin mining process!

How could it happen?

- A user's password was compromised on a cluster.
- With their account, a glibc bug was exploited on another cluster to get root access.
- Sshd was replaced, and passwords sniffed.
- With root access, started bitcoin processes on all nodes.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"raccoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Security Incident Example 2

2020 - High loads on compute nodes of a cluster 12-6am

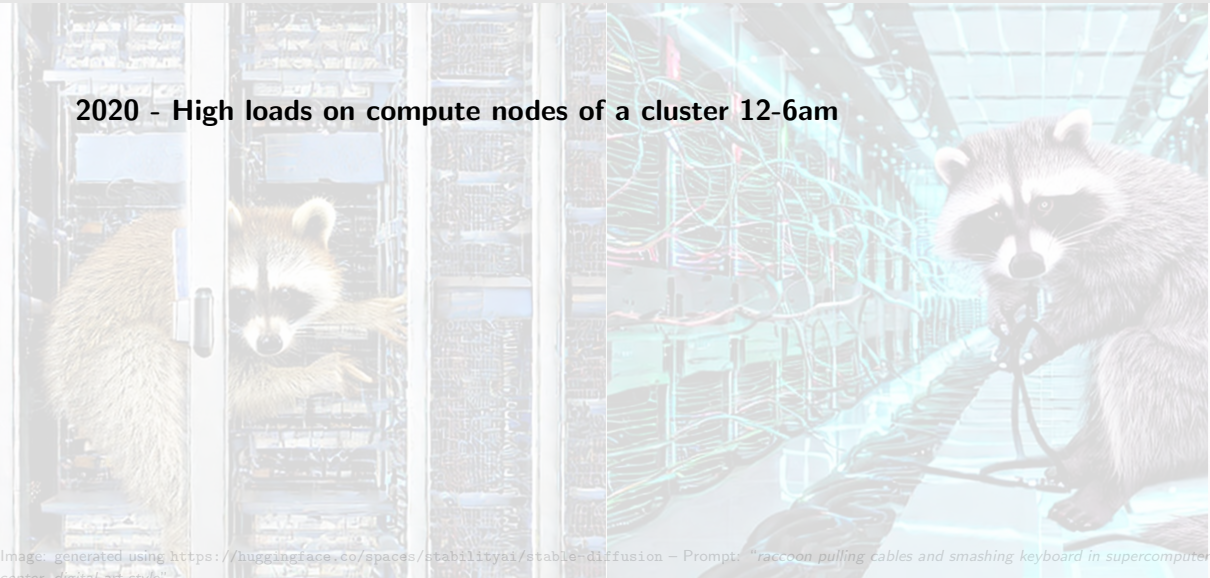
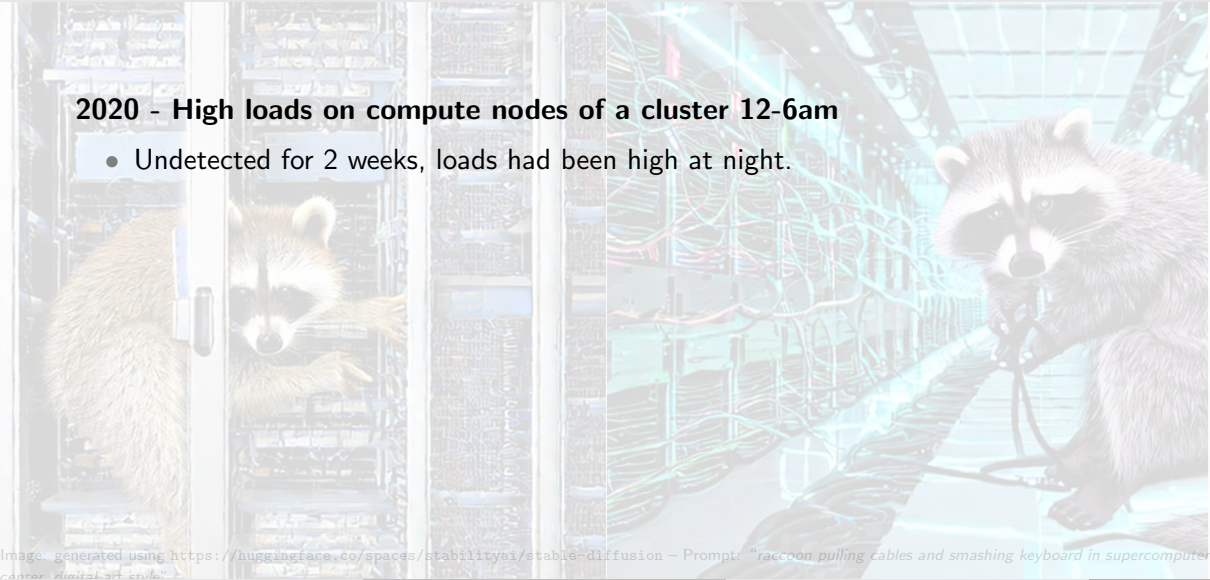


Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"racoon pulling cables and smashing keyboard in supercomputer center digital art style"*

Security Incident Example 2

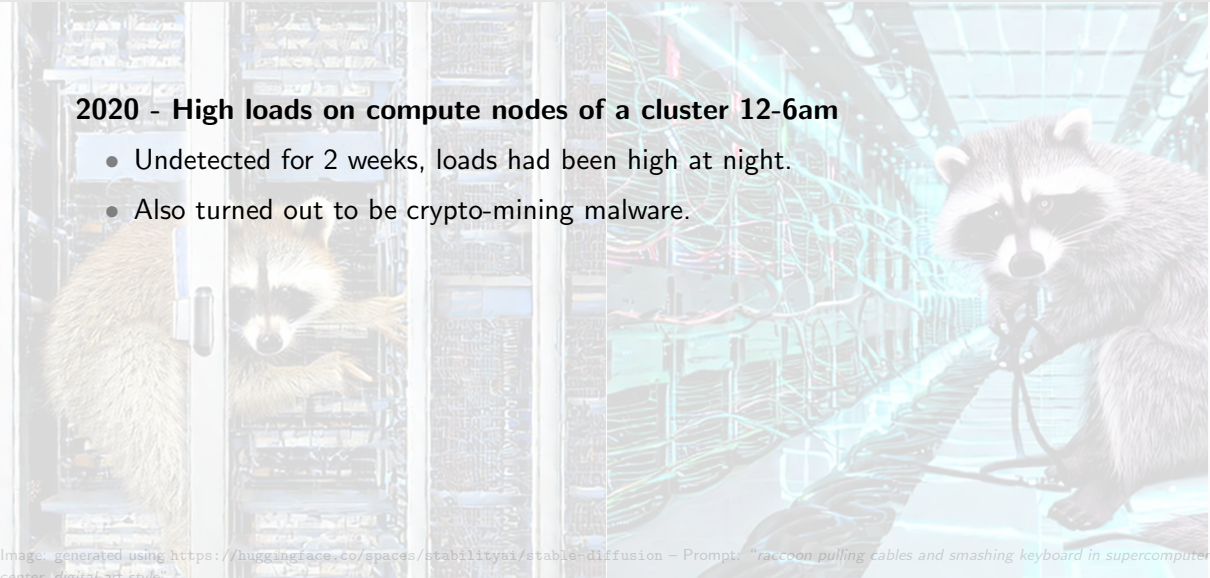


2020 - High loads on compute nodes of a cluster 12-6am

- Undetected for 2 weeks, loads had been high at night.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"racoon pulling cables and smashing keyboard in supercomputer center digital art style"*

Security Incident Example 2



2020 - High loads on compute nodes of a cluster 12-6am

- Undetected for 2 weeks, loads had been high at night.
- Also turned out to be crypto-mining malware.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"racoon pulling cables and smashing keyboard in supercomputer center digital art style"*

Security Incident Example 2

2020 - High loads on compute nodes of a cluster 12-6am

- Undetected for 2 weeks, loads had been high at night.
- Also turned out to be crypto-mining malware.
- Much better hidden exploit.

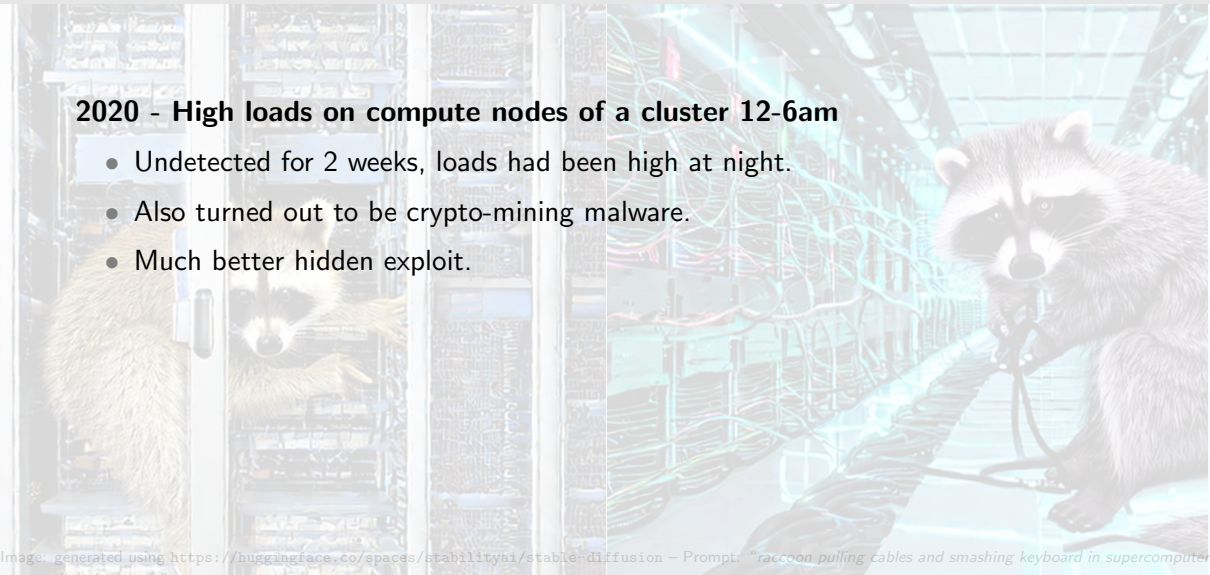


Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"racoon pulling cables and smashing keyboard in supercomputer center digital art style"*

Security Incident Example 2

2020 - High loads on compute nodes of a cluster 12-6am

- Undetected for 2 weeks, loads had been high at night.
- Also turned out to be crypto-mining malware.
- Much better hidden exploit.

How could it happen?

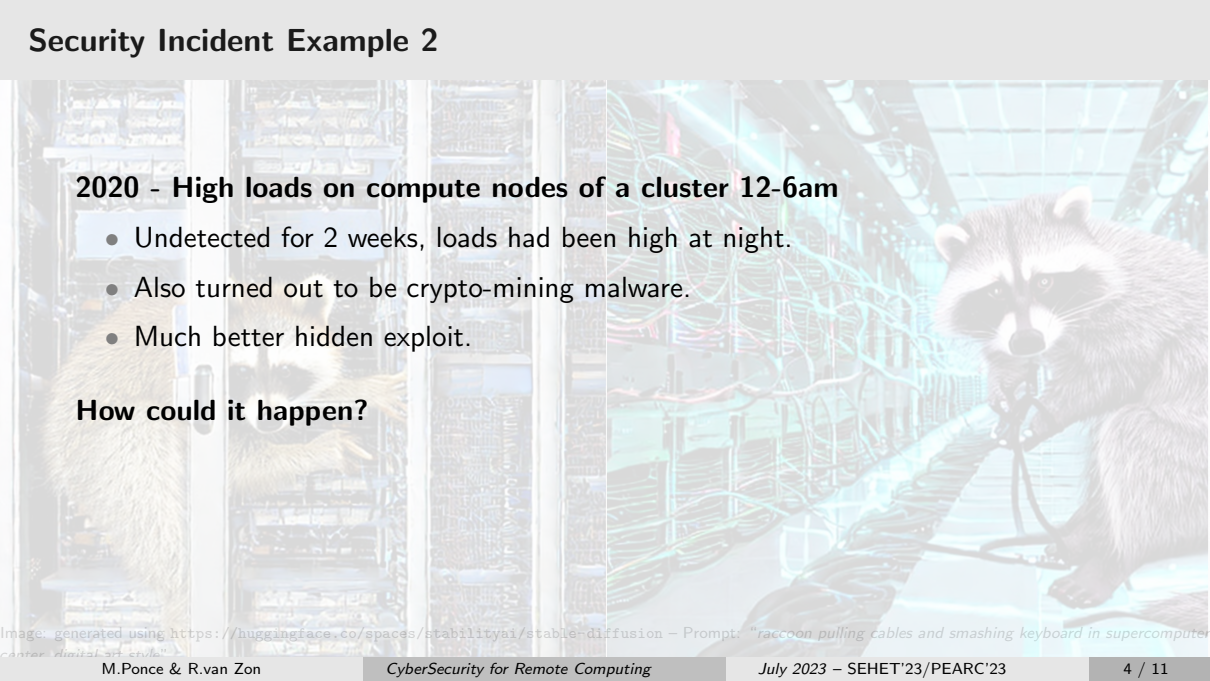


Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"racoon pulling cables and smashing keyboard in supercomputer center digital art style"*

Security Incident Example 2

2020 - High loads on compute nodes of a cluster 12-6am

- Undetected for 2 weeks, loads had been high at night.
- Also turned out to be crypto-mining malware.
- Much better hidden exploit.

How could it happen?

- A sysadmin's password was compromised.

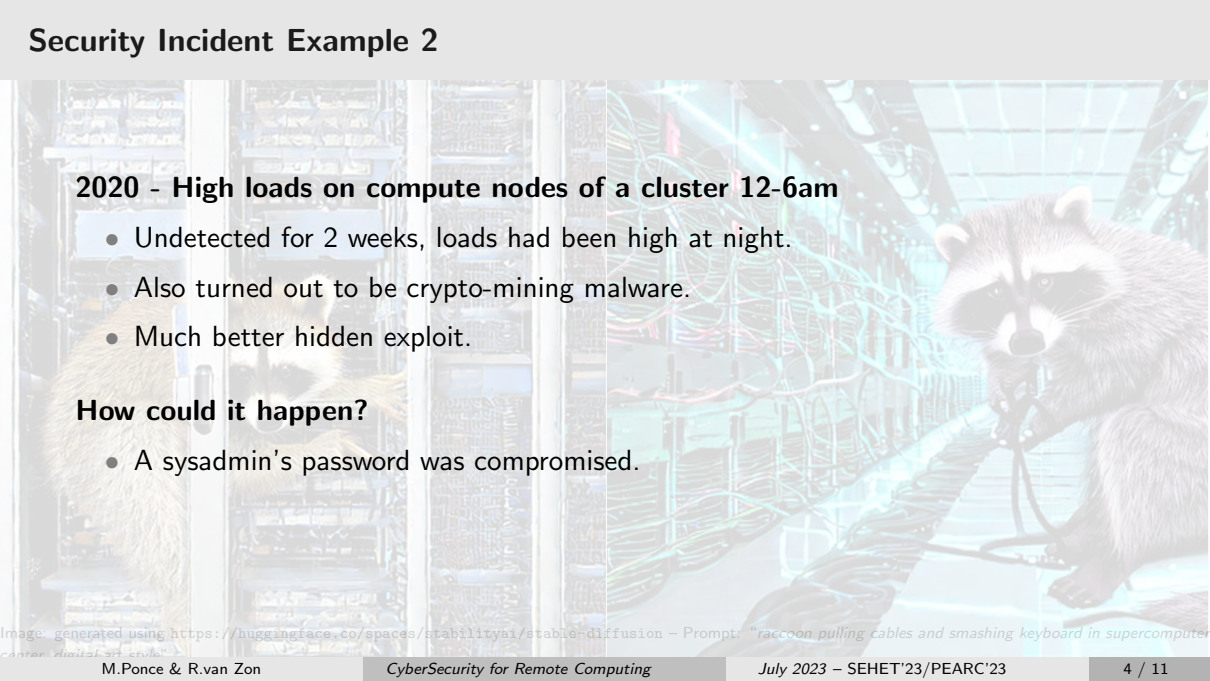


Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"racoon pulling cables and smashing keyboard in supercomputer center digital art style"*

Security Incident Example 2

2020 - High loads on compute nodes of a cluster 12-6am

- Undetected for 2 weeks, loads had been high at night.
- Also turned out to be crypto-mining malware.
- Much better hidden exploit.

How could it happen?

- A sysadmin's password was compromised.
- A few systems hadn't yet enforced multi-factor authentication for staff.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"racoon pulling cables and smashing keyboard in supercomputer center digital art style"*

Security Incident Example 2

2020 - High loads on compute nodes of a cluster 12-6am

- Undetected for 2 weeks, loads had been high at night.
- Also turned out to be crypto-mining malware.
- Much better hidden exploit.

How could it happen?

- A sysadmin's password was compromised.
- A few systems hadn't yet enforced multi-factor authentication for staff.
- The attacker used a "rootkit" to hide their activities.

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: *"racoon pulling cables and smashing keyboard in supercomputer center, digital art style"*

Lessons?

Many current best practices would've prevented such an attack.

Lessons?

Many current best practices would've prevented such an attack.

E.g.:

- Users and staff's own computers must be up-to-date.
- Root access should restricted and logged on user-facing servers
- Root on user-facing servers cannot connect to other servers.
- Use ssh keys to avoid password sniffing.
- Multi-factor authentication.
- Increase user's cybersecurity awareness.

Lessons?

Many current best practices would've prevented such an attack.

E.g.:

- Users and staff's own computers must be up-to-date.
- Root access should restricted and logged on user-facing servers
- Root on user-facing servers cannot connect to other servers.
- Use ssh keys to avoid password sniffing.
- Multi-factor authentication.
- Increase user's cybersecurity awareness.

Many of these require the cooperation of users, who need **cybersecurity training**.

Typical Cybersecurity Threats of which to be Aware

- DoS, DDoS
- Sniffing, IP/DNS spoofing, Man-in-the-Middle
- Phishing
- Malware, Ransomware
- Social engineering

This is an incomplete list!

- Steal credentials, 0-day exploits
- Disable a service
- Steal secure information
- Install unauthorized software
- Abuse resources
- ...

Cybersecurity Awareness and Training

End-Users Training Program

Introductory Courses

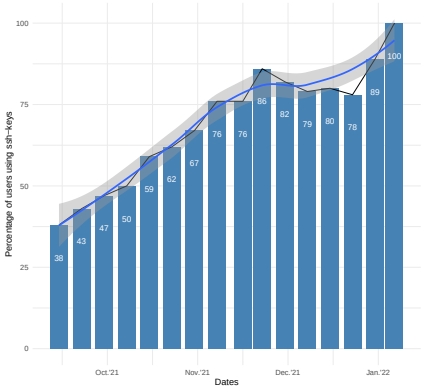
- Introduction to Supercomputing (HPC101)
- Intro to SciNet, Niagara, and Mist (HPC105)

Operational Courses

- Intro to the Linux Shell (SCMP101)
- Advanced Linux Command Line (SCMP271)
- Bash command line with common idioms (SCMP281)
- Introduction to Apptainer (SCMP161)

Specialized Courses

- Securing File Access Permissions on Linux (SCMP283)
- Enable Your Research with Cybersecurity (SCMP183)
- SSH Keys Drop-in Session (SCMP110)



Courses materials available at

`httts://education.scinet`

End-Users Training Program

Introductory Courses

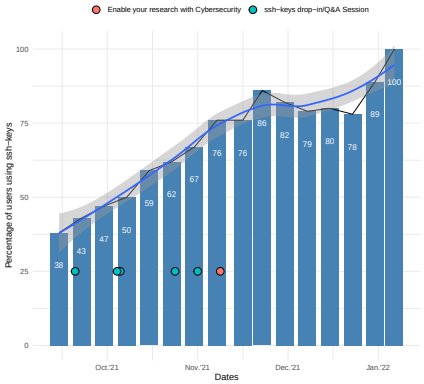
- Introduction to Supercomputing (HPC101)
- Intro to SciNet, Niagara, and Mist (HPC105)

Operational Courses

- Intro to the Linux Shell (SCMP101)
- Advanced Linux Command Line (SCMP271)
- Bash command line with common idioms (SCMP281)
- Introduction to Apptainer (SCMP161)

Specialized Courses

- Securing File Access Permissions on Linux (SCMP283)
- Enable Your Research with Cybersecurity (SCMP183)
- SSH Keys Drop-in Session (SCMP110)



Courses materials available at

`httts://education.scinet`

End-Users Training Program

Introductory Courses

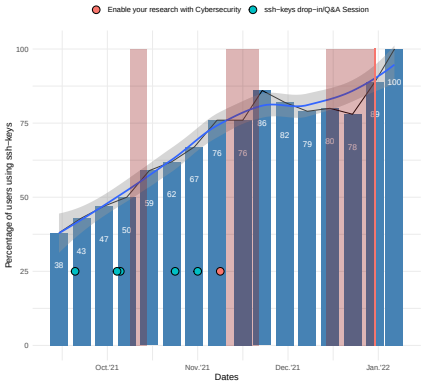
- Introduction to Supercomputing (HPC101)
- Intro to SciNet, Niagara, and Mist (HPC105)

Operational Courses

- Intro to the Linux Shell (SCMP101)
- Advanced Linux Command Line (SCMP271)
- Bash command line with common idioms (SCMP281)
- Introduction to Apptainer (SCMP161)

Specialized Courses

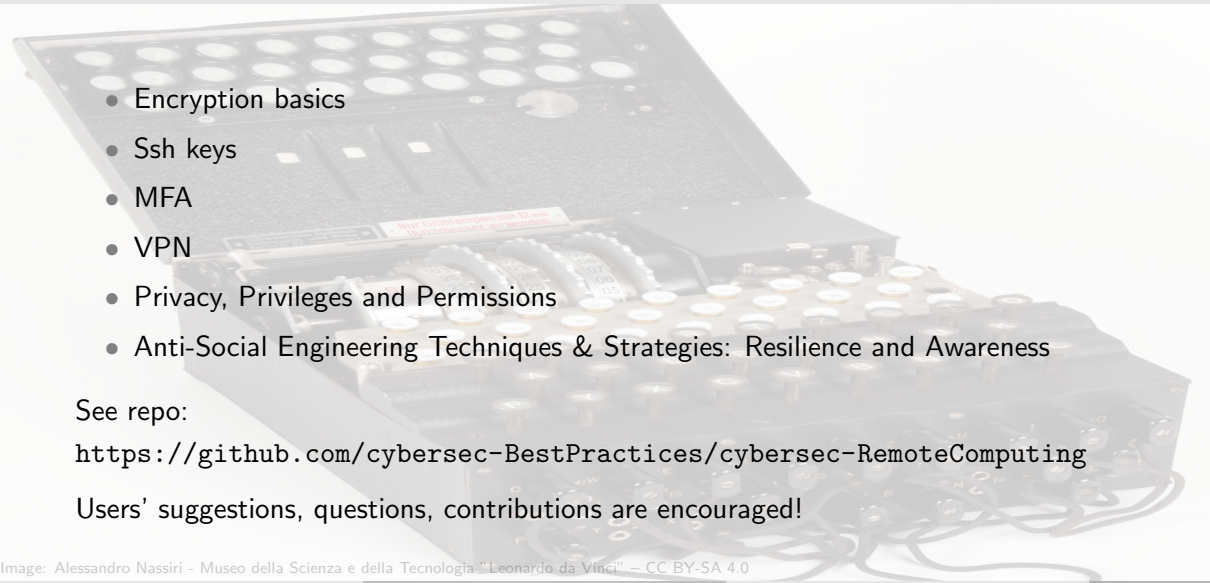
- Securing File Access Permissions on Linux (SCMP283)
- Enable Your Research with Cybersecurity (SCMP183)
- SSH Keys Drop-in Session (SCMP110)



Courses materials available at

`httts://education.scinet`

Teachable Topics in Remote Computing Cybersecurity



- Encryption basics
- Ssh keys
- MFA
- VPN
- Privacy, Privileges and Permissions
- Anti-Social Engineering Techniques & Strategies: Resilience and Awareness

See repo:

`https://github.com/cybersec-BestPractices/cybersec-RemoteComputing`

Users' suggestions, questions, contributions are encouraged!

Cybersecurity Best Practices & Checklist

connecting to remote systems

- use ssh keys, with passphrases
- use MFA
- use VPN
- check the information provided by the remote system
- avoid public wifi unsecure connections
- consider using "private browsing" and set restrictions on cookies policies

Image: generated using stablediffusionweb.com/#demo – Prompt: *"merge machine alethiometer an enigma machine and a Caesar cipher"*

Cybersecurity Best Practices & Checklist

connecting to remote systems

- use ssh keys, with passphrases
- use MFA
- use VPN
- check the information provided by the remote system
- avoid public wifi unsecure connections
- consider using "private browsing" and set restrictions on cookies policies

in local systems

- use an anti-virus
- keep software up-to-date, OS & Apps
- be mindful of emails, malicious attachments and links:
  do not enter sensitive data in unknown sites, verify for https connections and SSL certificates
- do not plug any type of device of unknown origin or source, e.g. USB sticks, etc.
- use a password manager, do not store passwords in plain-text
- encrypt sensitive data

Image: generated using stablediffusionweb.com/#demo – Prompt: *"merge machine alethiometer an enigma machine and a Caesar cipher"*

Conclusions

Summary / Overview

- Increase awareness and improve cybersecurity posture in *remote computing* (HPC/ARC) users
- **Critical: training and education!** (recall usually the weakest element is the "human factor")
- One source of reference to point to users for recommending best practices
- Keep it updated with latest trends and updates

References & Resources

Resources

- Cybersecurity Best Practices repository,
  `https://github.com/cybersec-BestPractices/cybersec-RemoteComputing`
- Wiki,
  `https://github.com/cybersec-BestPractices/cybersec-RemoteComputing/wiki`
- Users' suggestions, questions, contributions are encouraged and welcome!

Image: generated using https://huggingface.co/spaces/stabilityai/stable-diffusion – Prompt: "merge machine alethiometer an enigma machine and a Caesar cipher"