Enable your Research with Cybersecurity!
Day 2

Prepared by:
Raphaelle Gauriau
Information Security Strategic Execution Manager, University of Toronto

Assignment 1 - Review

Questions?

Findings?

Agenda – Day 2

Review assignment 1

Best practices (suite)

Cryptography Concepts

SSH keys usage

Assignment 2

Best Practices (suite)

End-Users

Anonymous Survey –

Do you use the same password to access different resources?

Twitter users told to change passwords after internal leak

4 May 2018 · Comments

Passwords that

Twitter's 330 million users are being urged to change their passwords after some were exposed in plain text on its internal network.

An error in the way the passwords were handled meant some were stored in easily readable form, said Twitter.

The passwords should have been put through a procedure called "hashing" making them very difficult to read.

Security experts said the way Twitter handled the potential breach was "encouraging".

Yahoo 2013 data breach hit 'all three billion accounts'

3 October 2017

Yahoo has said that all of its three billion user accounts were affected in a hacking attack dating back to 2013.

The company, which was taken over by Verizon earlier this year, **said an investigation had shown the breach went much further** than originally thought.

ZDNET

tomorrow belongs to those who embrace it today

trending innovation home & office business finance education

/ innovation

Home / Innovation / Security

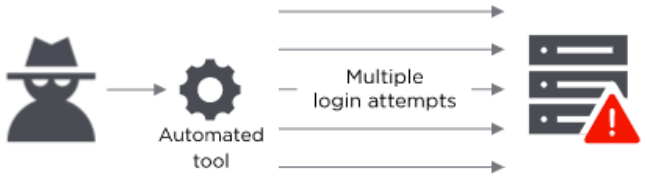
MySpace hack puts another 427 million passwords up for sale

Password theft should lead victims to change credentials they re-used for other sites.

Written by **John Fontana,** Contributor on May 31, 2016

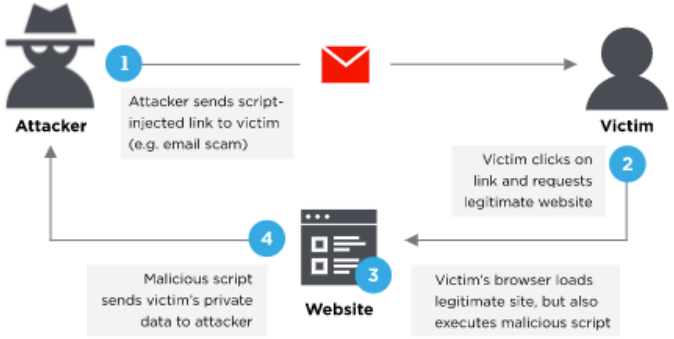
Passwords attacks (1/2)

- Brute force attacks



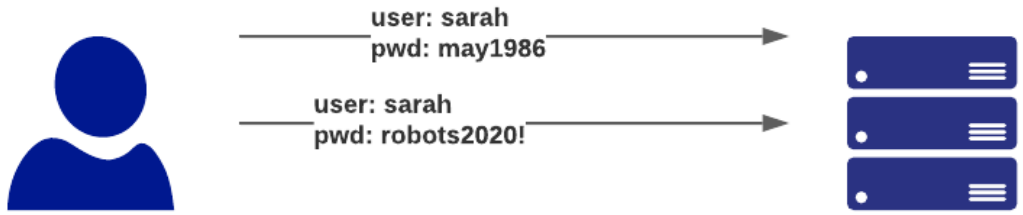
- Dictionary attacks

- Keyloggers

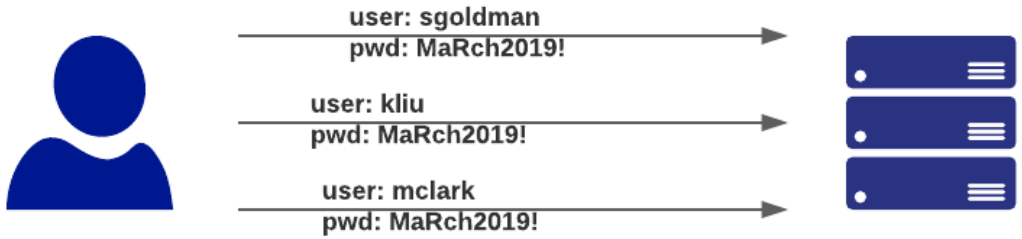


Passwords attacks (2/2)

- Password guessing



- Password spraying



- Phishing

Best practice #4 - Password usage (1/2)

DO NOT

- Do not use the same password everywhere
- Do not use simple passwords (example: Summer2018)
- Do not store passwords in clear text
- Do not share your password
- Do not transmit password via email or text

Anonymous Survey –

Do you use a password vault?

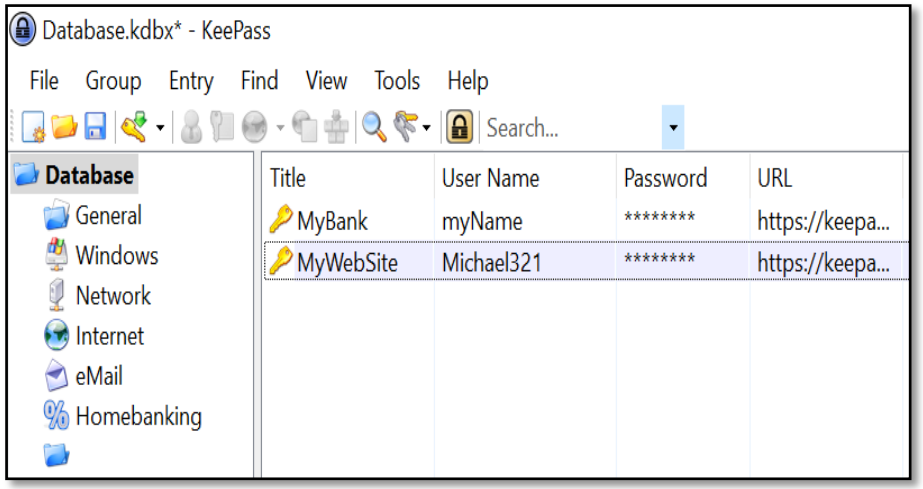
Best practice #4 - Password usage (2/2)

DO

- Use a different password for each account
- Use a password vault, such as
  - Bitwarden
  - Keypass

  Note 1: Dedicated password manager is usually more secure than storing your password in the browser

  Note 2: Ensure the master password is strong!
- Long passphrase (15 characters or more)
- Transmit securely
- Use MFA (multi-factor authentication) when possible



Tips

Do you want to know if your personal information or password has been leaked?

Check this website:
https://haveibeenpwned.com/

Exercise 1

Install a password vault of your choice on your workstation and create one secret.

Please find below two options:

- Keypass

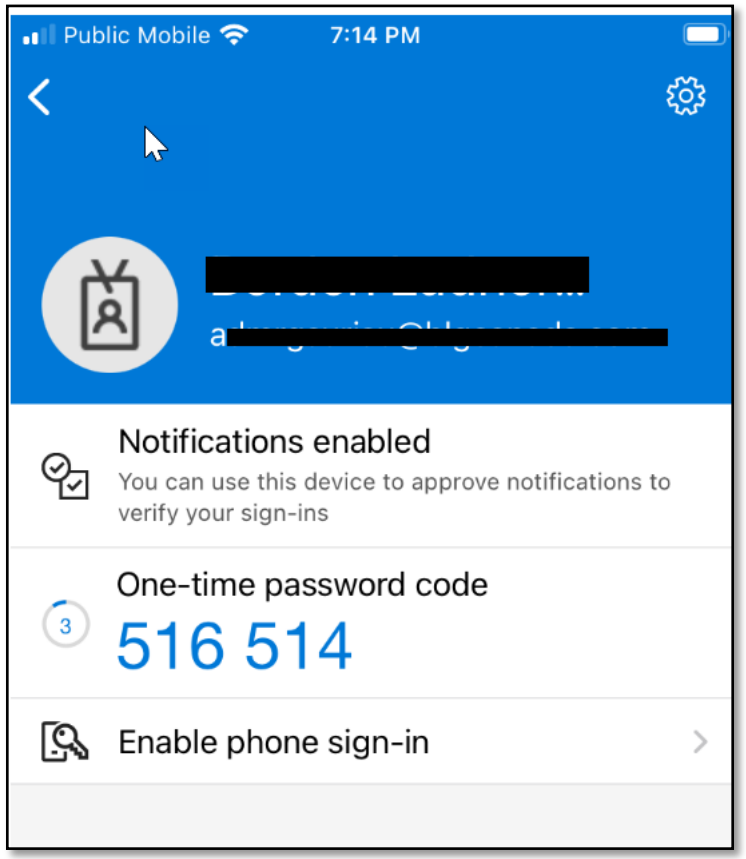
https://keepass.info/ (stored locally)

- Bitwarden

https://bitwarden.com (stored in the Cloud)

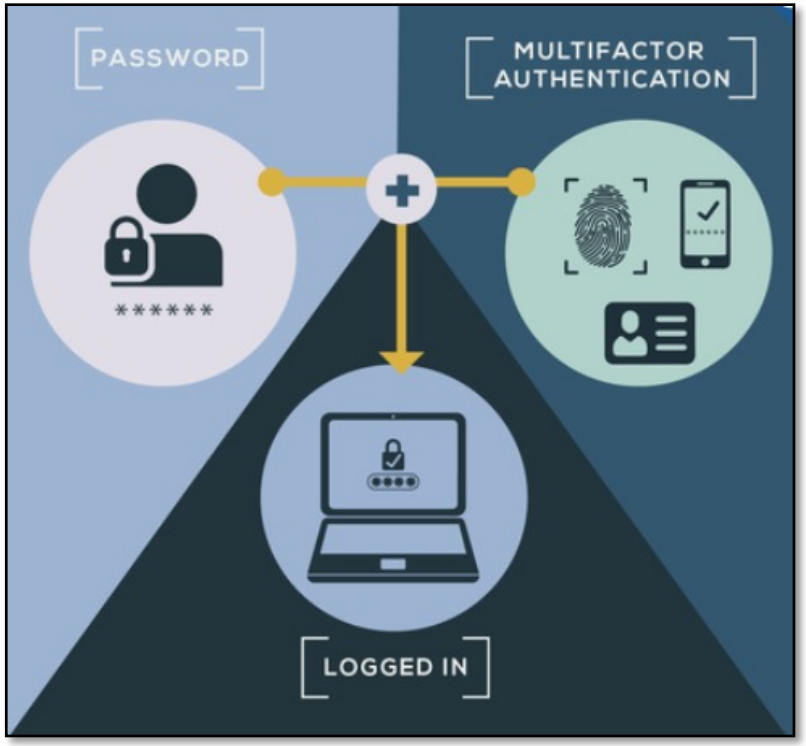
Best practice #5 - Use MFA (1/2)

- **Multi-Factor Authentication**: provide several pieces of evidence from different factors to prove your identity
- Factors:
  - **Something you know**
  - **Something you have**
  - **Something you are**
- Be careful when using your phone number as a second factor (ex: text message)
  - Phone number recycling
  - SMS is not the most secure way!



Best practice #5 - Use MFA (2/2)

- Protection against **phishing, social engineering** and **password brute-force attacks** and **stolen credentials**
- MFA project at the Digital Research Alliance of Canada
- Note: entering two different passwords is NOT considered as multi-factor



Source: https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

MFA Circumvention

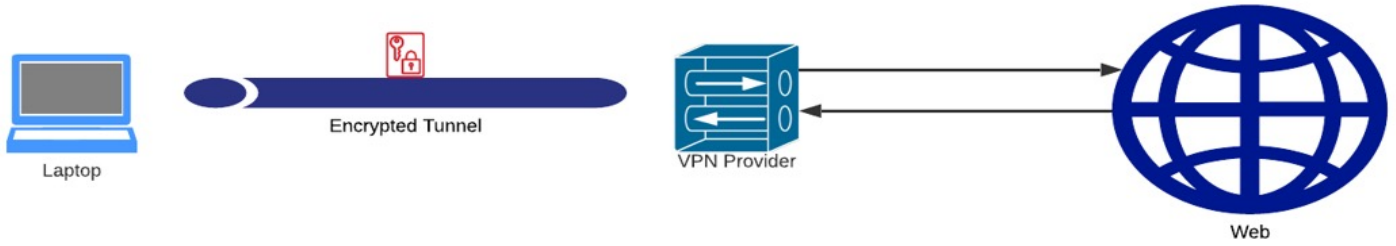
Stealing cookies is one method to circumvent MFA.

Some MFA factors are more robust than others.

While MFA is one efficient and additional way to protect your research, adopting the **principle of defense in depth is essentia**l (regular patching, have an anti-virus, being careful of phishing etc…): **if one control fails, another control protects your systems/data.**

Virtual Private Network (VPN)

- **Encrypted connection** between the user's device and the Internet
- Provides online **privacy and anonymity** by masking the user's IP address
- Minimizes two main risks:
  - Privacy risk, as a VPN provides anonymity
  - Someone eavesdropping your connection
- Available **via your host institution**, or often included as part of anti-malware vendor service
- **Regulations** in some countries

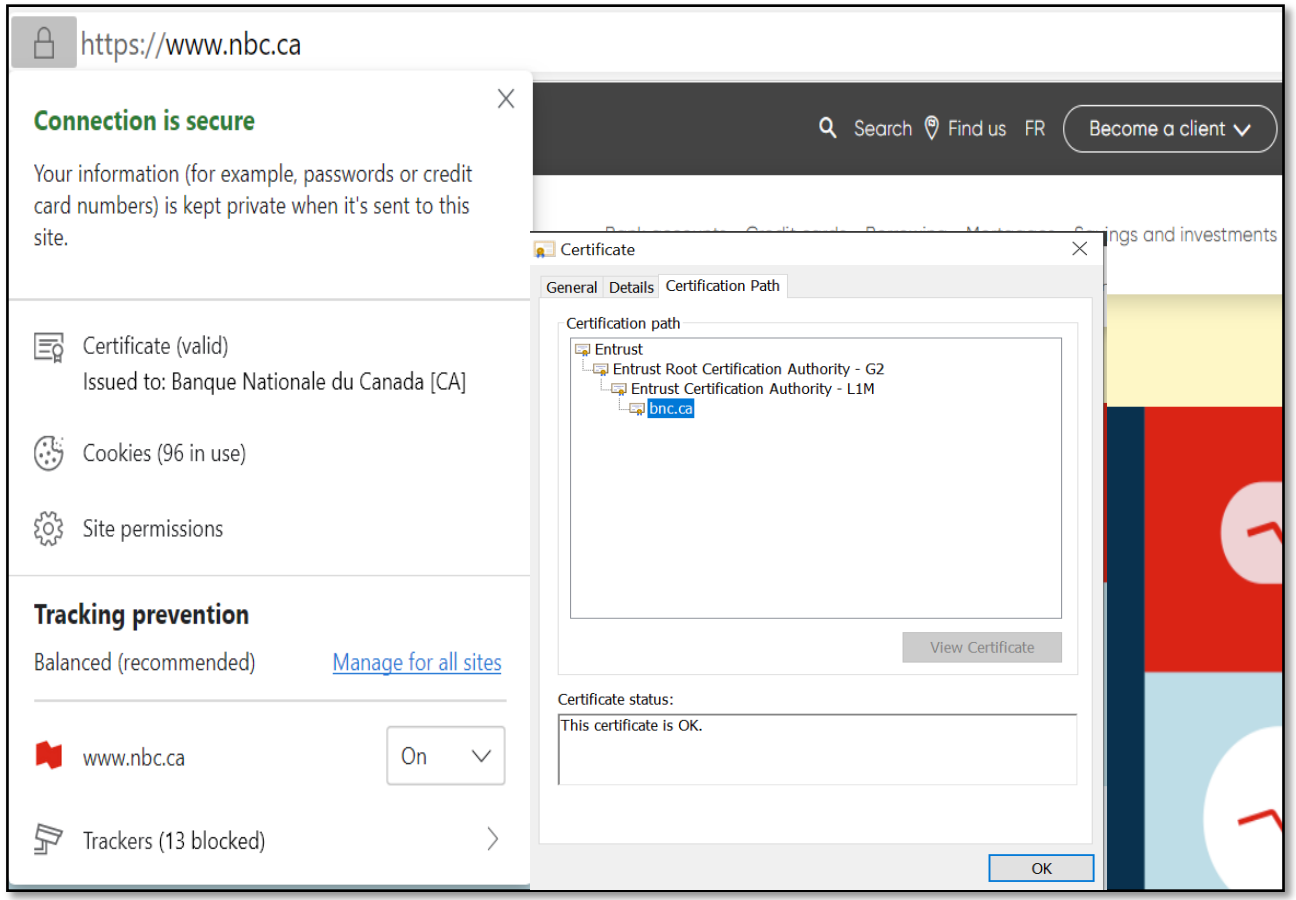


Best practice #6 - Safe Internet Browsing (1/2)

- **Public-WIFI**: **avoid** it as much as possible

- If you absolutely need to access a public WIFI:
  - Ensure that the WIFI name is known
  - Consider using a VPN (Virtual Private Network)
  - Stick to https websites and check certificates

- **Personal information**: be mindful of what you provide
  - Name, address, phone number, date of birth…



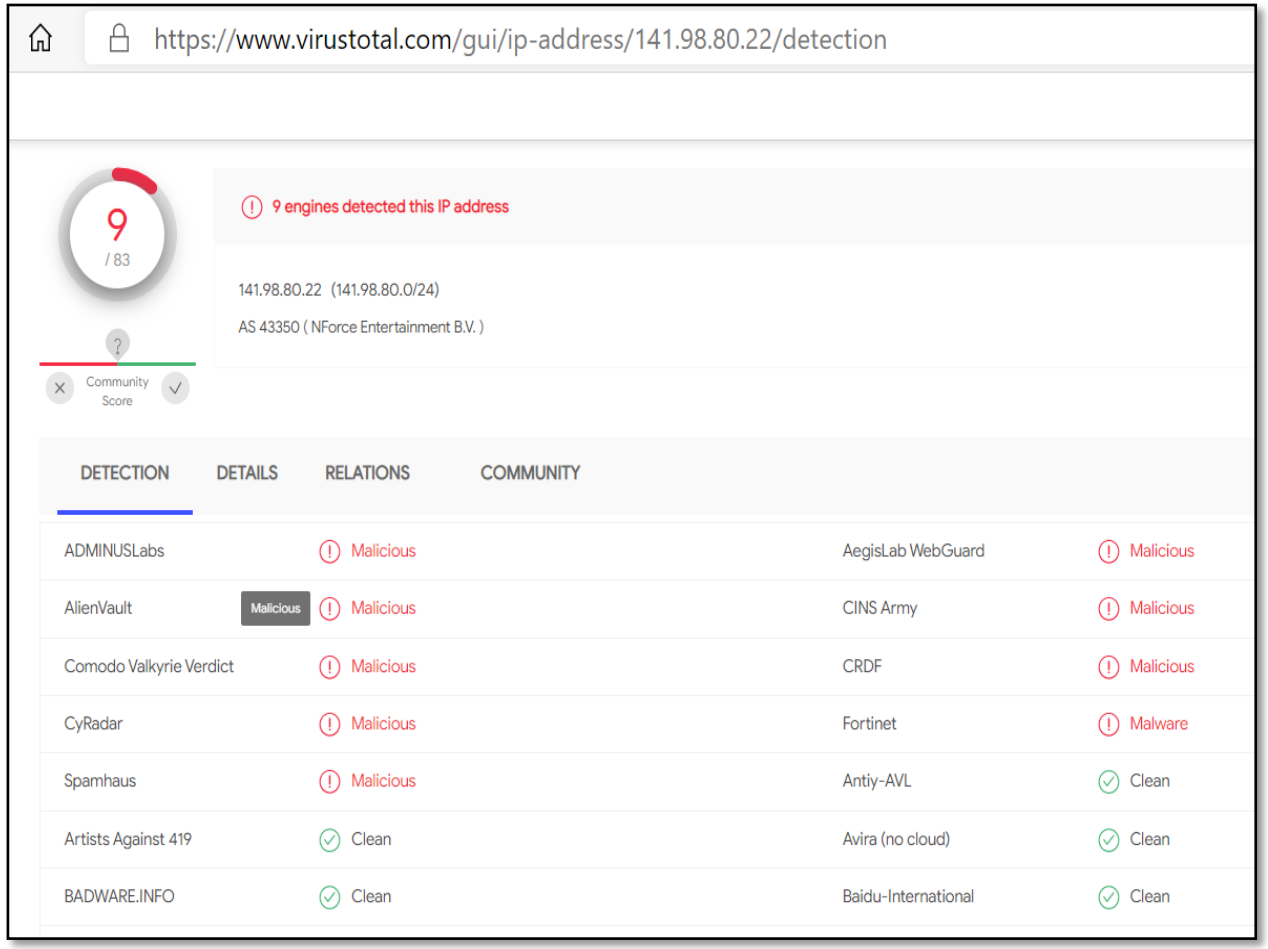
Best practice #6 - Safe Internet Browsing (2/2)

- Be careful with **browser extensions**
- Not sure about the **legitimacy** of a website?

https://www.virustotal.com

- Use **Cira Canadian Shield** at home

https://www.cira.ca/cybersecurity-services/canadian-shield



Best practice #7 - Backup your data (1/3)

- **Data loss** can occur due to incidents like **power surge, cyberattacks like ransomware, physical theft**
- **Backup** your important data **on a regular basis**
- Keep your backups in **a safe, different location**
- Cloud vs on-premise
- **Test** your backups!

Best practice #7 - Backup your data (2/3)

Different types of backups

- ***Full backups***: most applicable in the context of a user
- ***Incremental backups***: store only those files that have been modified since the time of the most recent full or incremental backup. Saves time and space. Applicable in the context of an organization.
- ***Differential backups***: store all files that have been modified since the time of the most recent full backup. Saves time and space. Applicable in the context of an organization.

Best practice #7 - Backup your data (3/3)

On **CC** systems (**non cloud**):

- $HOME and $PROJECT are backed up

On **CC** systems (**cloud**):

- Your responsibility

https://docs.alliancecan.ca/wiki/Backing_up_your_VM/en

Cryptography

& SSH keys

Cryptography Definitions

Encryption: The process of converting the message from its plaintext to ciphertext

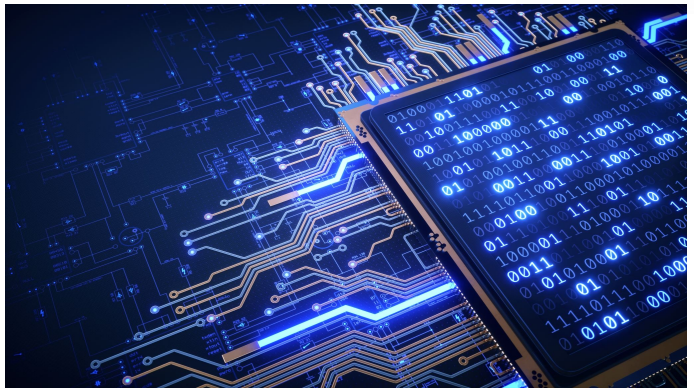
Plaintext: The message in its natural format has not been turned into a secret.

Ciphertext: The altered form of a plaintext message, so as to be unreadable for anyone except the intended recipients. Something that has been turned into a secret.

Hash function: Accepts an input message of any length and generates, through a one-way operation, a fixed-length output called a message digest or hash (ex: SHA-256).
Example of use case: data integrity

Source: https://www.isc2.org/Certifications/CISSP/CISSP-Student-Glossary

Encryption – Why? Where?



Why:

- Protect sensitive data

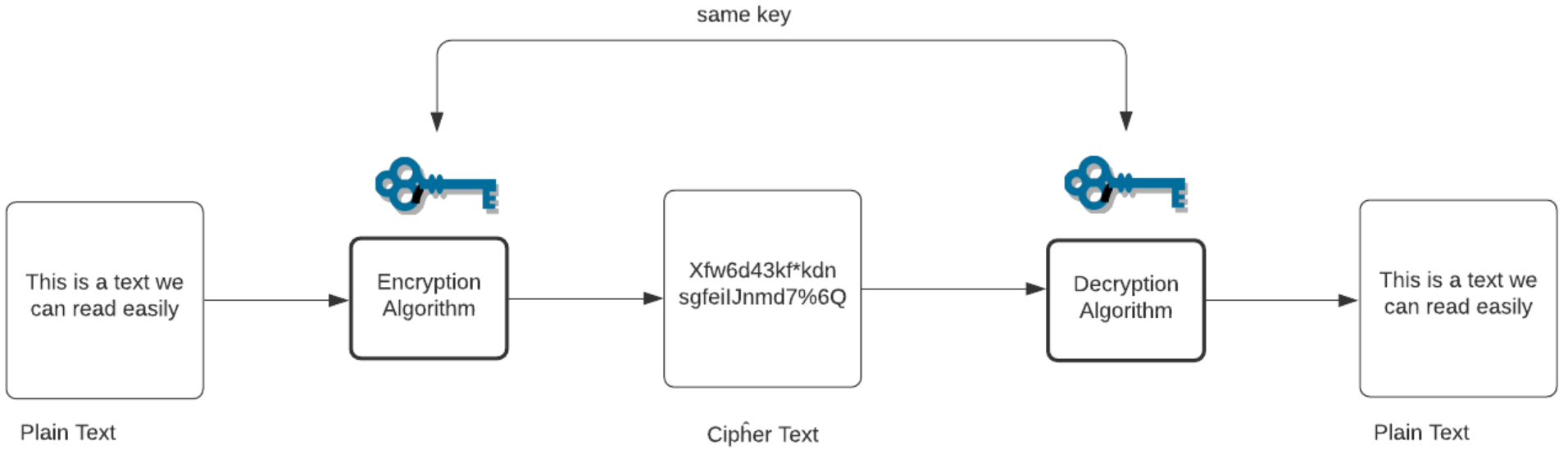
What :

- **In transit**
  - Data moving from one location to another (HTTPS, SSL, TLS, FTPS, etc)
  - Attacks against data in transit include man-in-the-middle attacks, wired tapping

- **At rest**
  - Data stored on a hard drive, laptop, flash drive, or archived/stored in some other way
  - Attacks against data at-rest include attempts to obtain physical access to the hardware on which the data is stored, and then compromise the contained data.
  - Requirement by some regulations: HIPAA, PCI

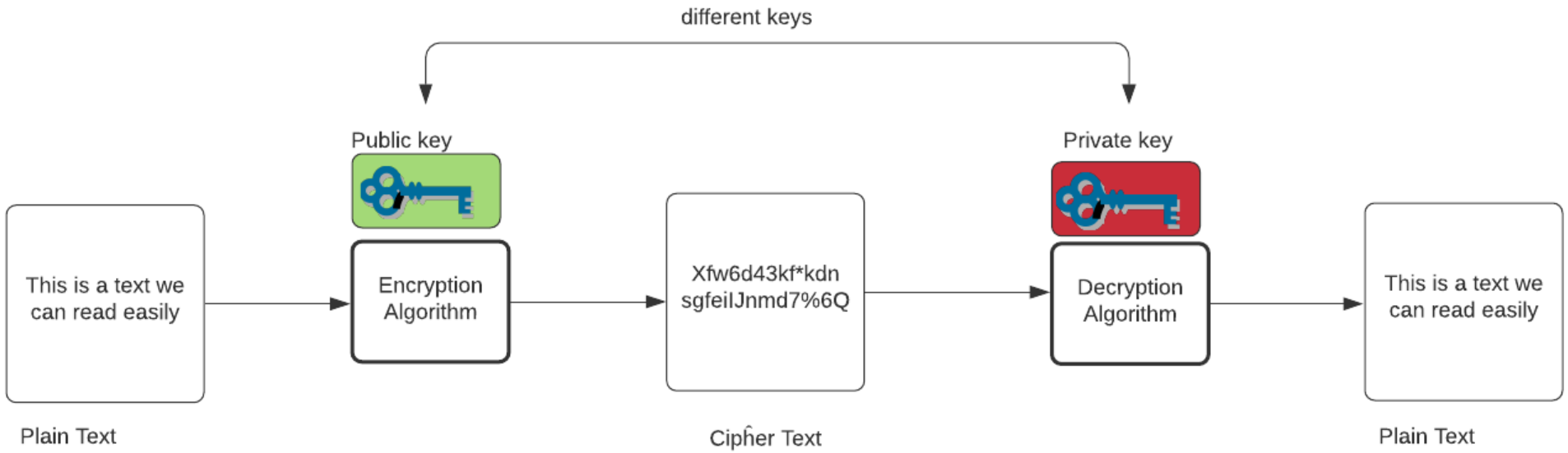
Symmetric vs Asymmetric Encryption (1/3)

Symmetric



Symmetric vs Asymmetric Encryption (2/3)

Asymmetric



Symmetric vs Asymmetric Encryption (3/3)

Symmetric encryption

One secret key to encrypt and decrypt

Very efficient

How do you exchange the secret key?

Algorithms:
RC4*, AES, DES*, 3DES, QUAD, Blowfish

Asymmetric encryption

One key to encrypt, another key to decrypt

Public key vs Private key

Public key: available to everyone

Private key: keep in a secure location

Algorithms:
RSA, Diffie-Hellman, ECC

*: weak algorithms

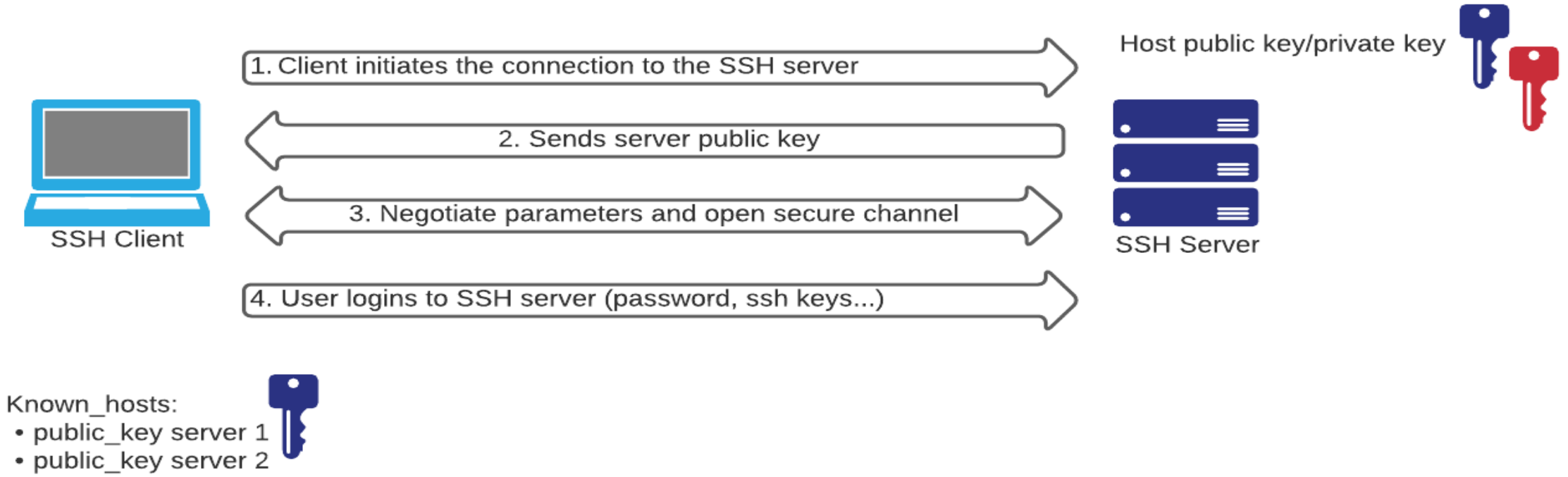
Quantum Computing

- **Threat** to cybersecurity and in particular cryptography, timeframe horizon of one decade
- **Harvest** encrypted content now to decrypt it later
- In July, NIST announced **First Four Quantum-Resistant Cryptographic Algorithms**
- The industry will need to align itself with the new algorithms. Organizations will need to transition to quantum-resistant algorithms.

Source: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Real-Life Scenario: SSH

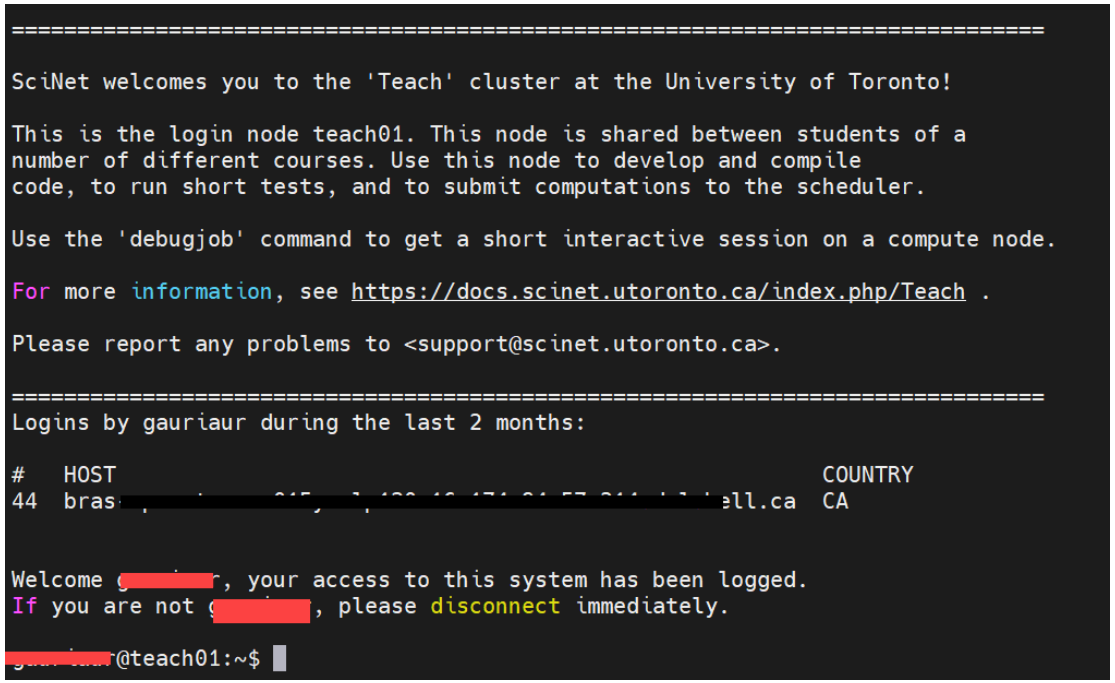
SSH (Secure Shell): a method for secure remote login



Exercise 2

Authenticate to SciNet Teach cluster via a password

teach.scinet.utoronto.ca



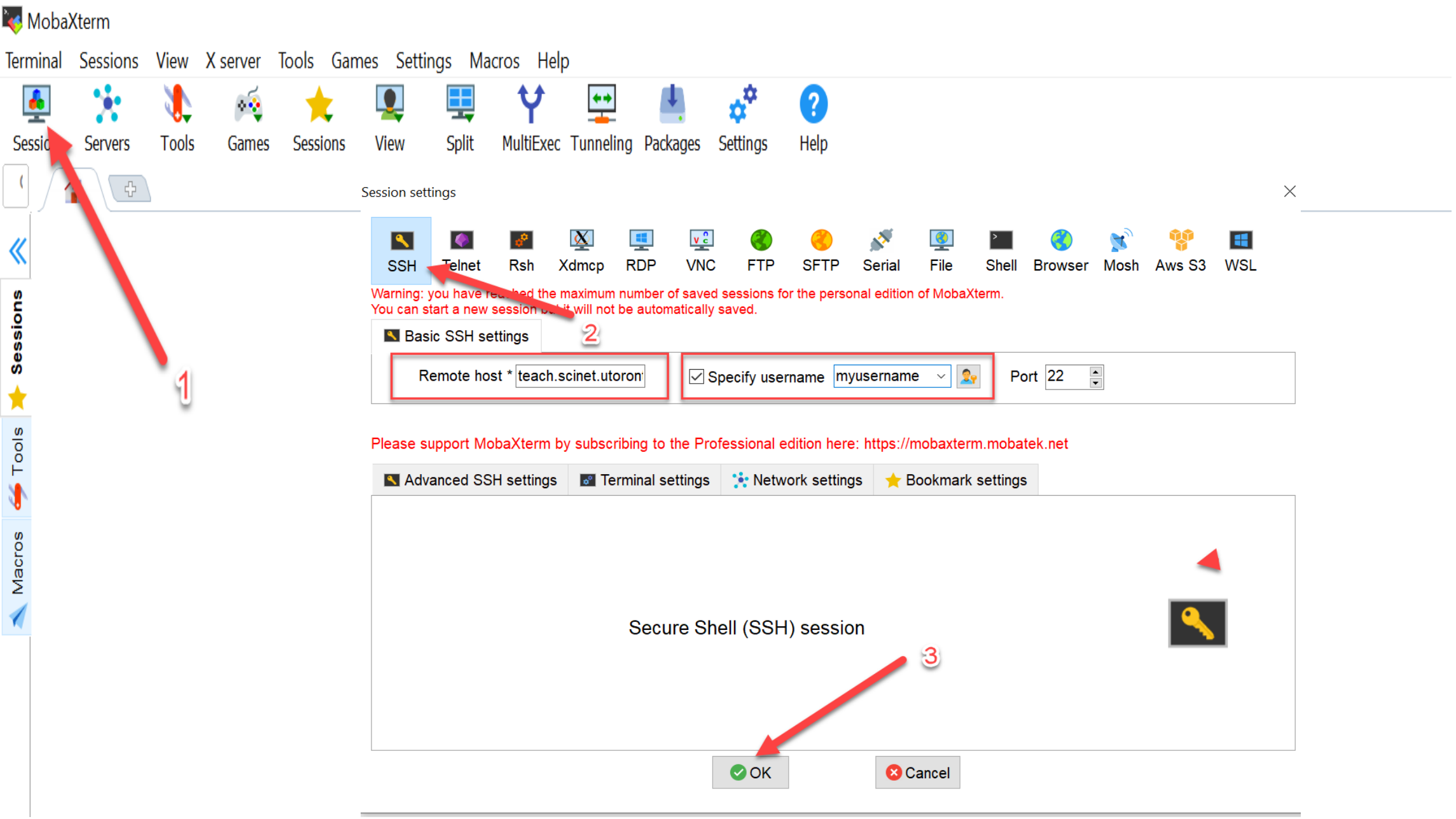
Windows:

Use MobaXterm or another tool

MacOS/Linux:

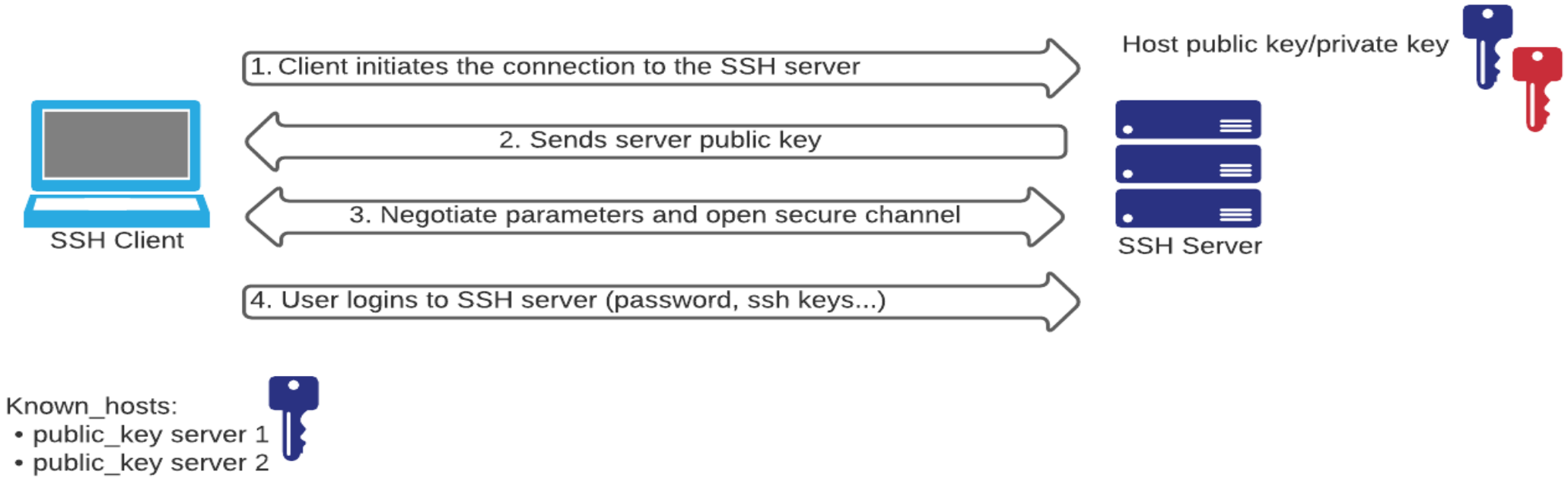
Via a terminal, type:

ssh username@teach.scinet.utoronto.ca


MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Sessio Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL
Warning: you have reached the maximum number of saved sessions for the personal edition of MobaXterm.
You can start a new session but it will not be automatically saved.
Basic SSH settings
Remote host * teach.scinet.utoron
Specify username myusername
Port 22
Please support MobaXterm by subscribing to the Professional edition here: https://mobaxterm.mobatek.net
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
Secure Shell (SSH) session
OK
Cancel
1
2
3
Sessions
Tools
Macros

Real-Life Scenario: SSH

SSH (Secure Shell): a method for secure remote login



SSH keys for authentication

- SSH keys: an alternative to passwords to authenticate
- Harder to crack than passwords
- Private key vs public key
- Protect your **private key in a safe location**
- **Do not share your private key!**
- Add a **passphrase** to the private key

Strength	RSA	ECDSA, EdDSA, DH, MQV
NOT RECOMMENDED ANYMORE	k = 1024	f = 160-223
RECOMMENDED	k = 2048 (and above)	f = 224-255 (and above)

Note: k and f above are commonly considered as key size

Asymmetric Algorithms and Corresponding Keys

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

Anonymous Survey –

Have you created an SSH key pair before?

Exercise 3

Goal: Create an SSH key pair on your workstation, then authenticate to SciNet Teach cluster via SSH key.

STEP 1 – On your workstation, create your SSH key pair.

STEP 2 – Make the public key available on Teach cluster.

Option a – Upload the SSH **public** key to CCDB (Compute Canada account needed):

https://ccdb.computecanada.ca/ssh_authorized_keys

Option b - Copy the SSH public key to Teach, under .ssh/authorized_keys file

STEP 3 – From your workstation, try to authenticate to Teach with your SSH key.

Source: https://docs.alliancecan.ca/wiki/SSH_Keys

STEP 1 – Create your SSH Key pair

Steps for **Linux/MacOS**:
https://docs.alliancecan.ca/wiki/Using_SSH_keys_in_Linux

Steps for **Windows**:
https://docs.alliancecan.ca/wiki/Generating_SSH_keys_in_Windows

Recommendations:

- Add a passphrase to encrypt the private key; 15 characters or more.
- Name the SSH key as you may create SSH keys for other systems. Ex: LaptopName_SciNet
- If you have several laptops, create dedicated SSH key pairs for each of them.

STEP 2 – Make the public key available on Teach cluster

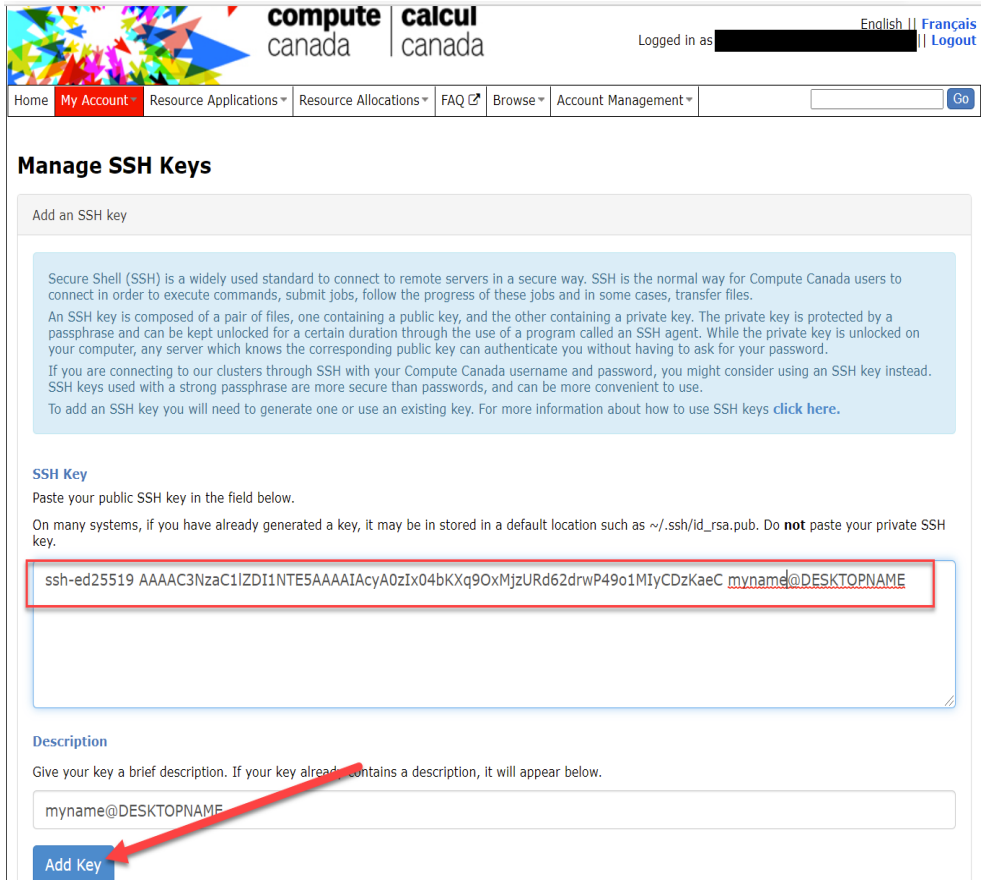
Option a - Upload the SSH **public** key to CCDB (Alliance account needed):

https://ccdb.computecanada.ca/ssh_authorized_keys

Option b - Copy the SSH **public** key to Teach, under .ssh/authorized_keys file

https://docs.alliancecan.ca/wiki/Using_SSH_keys_in_Linux#Installing_locally

https://docs.alliancecan.ca/wiki/Generating_SSH_keys_in_Windows#Installing_locally



Option a – Upload public key to CCDB

STEP 3 – Authenticate with your SSH Key pair

From your workstation:

On Linux/MacOS:

$ ssh -i ~/.ssh/private_key_name myusername@teach.scinet.utoronto.ca

On Windows:

https://docs.alliancecan.ca/wiki/Connecting_with_PuTTY#Using_a_Key_Pair

https://docs.alliancecan.ca/wiki/Connecting_with_MobaXTerm#Using_a_Key_Pair

Key Take-Aways – Day 2

- Use a **password vault**, combined with **MFA** whenever possible
- **Consider encryption** at rest and in transit to secure your data
- **Use SSH keys** and protect your SSH private key (location, passphrase)

Pick one thing to change!

Source: https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

Assignment – Day 2

1. What did you learn in today's session (1-2 items)?
2. Install a password vault and create some secrets (see Exercise 1).
3. Create an SSH key pair, then add your public key to Teach cluster and try to authenticate via SSH key (see Exercise 3).

Other resources

- https://securitymatters.utoronto.ca/resources/students/
- https://securityplanner.org/#/
- https://www.ic.gc.ca/eic/site/063.nsf/eng/h_97955.html

Sources and Images (day 1 and day 2)

- https://resources.infosecinstitute.com/certification/the-cissp-domains-an-overview/
- https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors
- https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary
- https://www.avast.com/en-ca/business/resources/defence-in-depth
- https://securitymatters.utoronto.ca/resources/it-professionals/ - (image)
- https://securitymatters.utoronto.ca/phish-got-a-moment/
- https://unsplash.com/s/photos/email - (image)
- https://unsplash.com/s/photos/castle - (image)
- https://www.sentinelone.com/blog/are-we-done-with-wannacry/
- https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
- Palo Alto Unit 42 Incident Response Report 2022
- https://cofense.com/knowledge-center/signs-of-a-phishing-email/
- https://www.pexels.com/photo/man-in-red-shirt-wearing-black-framed-eyeglasses-3965246 – (image)
- https://www.av-test.org/en/
- https://www.forcepoint.com/cyber-edu/heuristic-analysis
- https://www.zdnet.com/article/flashback-trojan-wake-up-call-for-mac-users/
- https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
- CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition by Darril Gibson; James M. Stewart; Mike Chapple ; Backups Chapter
- https://www.ssh.com/academy/ssh/protocol
- https://docs.alliancecan.ca/wiki/SSH_Keys

Thank You!
Questions?