Cybersecurity Essentials for Smart Manufacturing Professionals

Module 2: User Accounts and Access Control

ESL Global Cybersecurity Institute

Rochester Institute of Technology

September 2023

Learning Outcomes

By the end of this class, you will be able to:

- Understand the importance of access control
- Identify common types of access control mechanisms
- Exercise best practices for managing user accounts
- Understand the importance of cloud-based access control solutions

Access Control Principles

Access Control in Manufacturing

- What comes to your mind when one says, ‘access control’?
- Why is important in manufacturing?

https://www.haascnc.com/service/troubleshooting-and-how-to/how-to/software-available-for-download-from-haas-portal.html

Access Control – Definition

- Access control enables only authorized personnel to access physical and online data (or resources)
- Importance of access control mechanisms
  - Ensures consistent high productivity through remote access capabilities
  - Reduces security risk to the company
  - Facilitates maintenance, management and monitoring

Access Control Mechanisms

- User authentication – verifying identity of a user
- Authentication mechanisms
  - Passwords (something you know)
  - Biometrics (something you are)
  - Multi-factor Authentication (something you have)

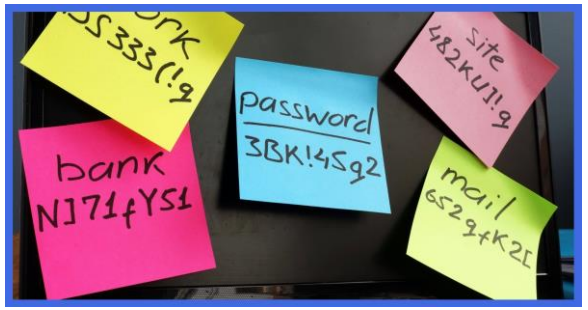
Potential Attacks on Access Control

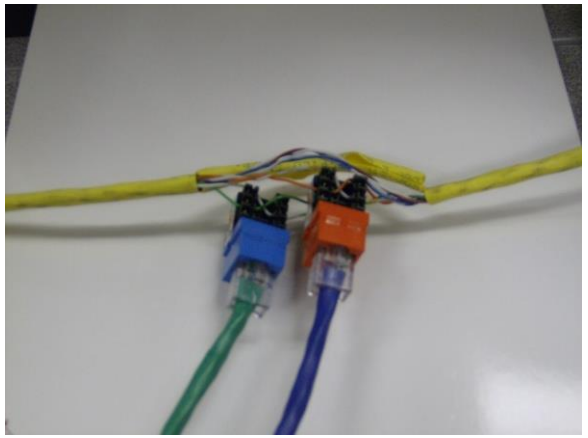
Internal Threats

- Individuals with malicious intent who possess legitimate access
  - Disgruntled employees, contractors
- Insiders can perform attacks such as
  - Compromise user accounts
  - Perform phishing attacks
  - Leak trade secrets
  - Implement insecure security configurations

External Threats

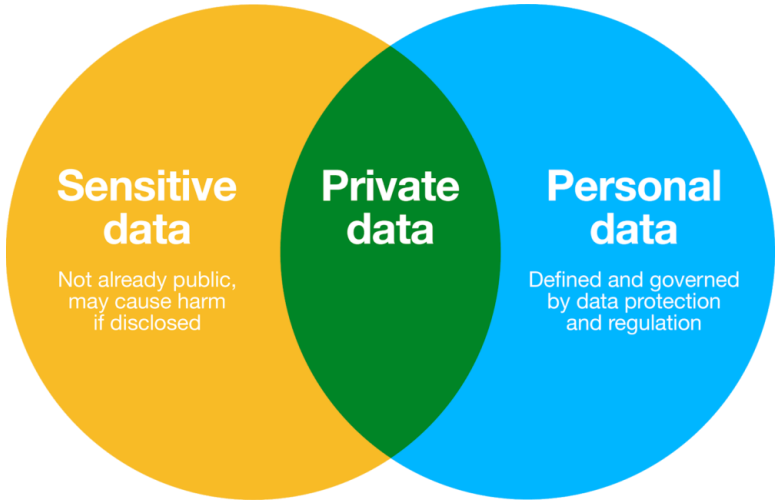
- Hackers, saboteurs, thieves that attack from outside the company
- They can use the following techniques
  - Password theft – sticky notes, password cracking
  - Wiretapping network traffic
  - Spoofing / faking Wi-Fi networks
  - Social engineering / phishing / scam emails





Risks to the Company

- Unauthorized disclosure of information
  - Trade secrets, user / customer data
- Computer service availability issues
  - Downtime due to cyber attacks
- Legal implications
  - Lawsuits due to privacy breaches
- Extortion
  - Demands for ransom



Protecting Access Control

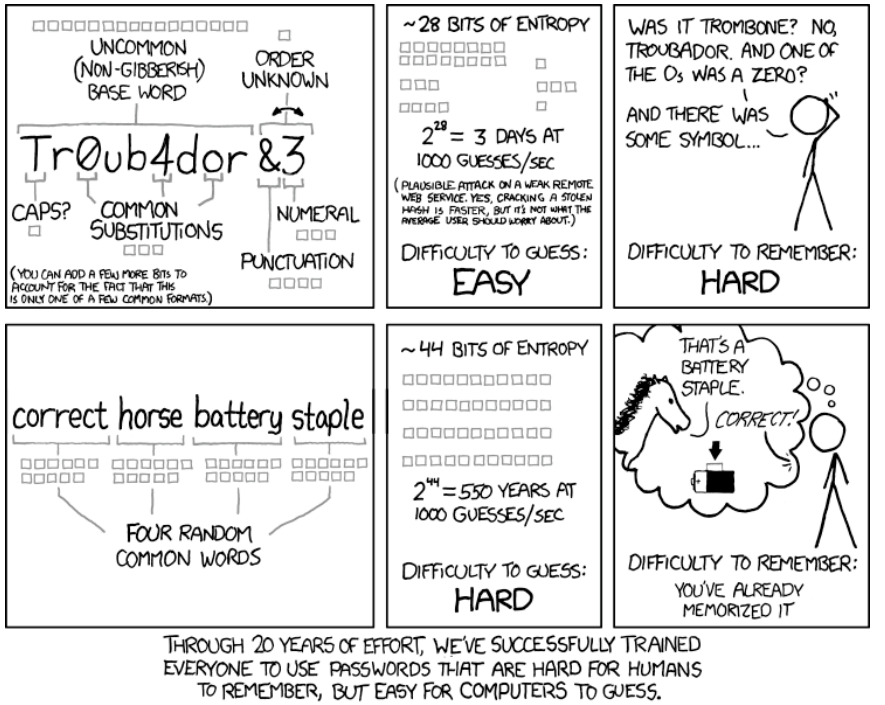
- It is very easy to compromise a user account!
  - A simple sticky note is all it takes
  - An attacker on a tour / simply walking by can easily see such a note
- Consequences of improper access control
  - Tampering of machining data
  - Theft of confidential data
- Principle of Least Privilege
  - Users should have minimum level of access
  - Allow access only to necessary resources

Post-it note with passwords

Best Practices for Managing User Accounts

Password Hygiene

- Use best practices for password security
  - Don’t reveal passwords in the open – no sticky notes!
  - Use long phrases that are easy to remember
  - Password managers can be used company-wide
- Always change default passwords
- Multi-factor authentication
  - Biometric data – fingerprints, retina scan
- Password Strength Exercise!
  - Can you create a short but strong password?



User Provisioning

- Assign ***roles*** to perform access control
  - Apprentice < supervisor < shop floor boss, etc.
- Configure roles to have appropriate access to necessary resources
  - Apprentices can only operate machines, but not modify machining data
  - Supervisors can modify machining data
  - Machines can only be accessed from 9am to 5pm
- Access should be least privilege
- Inactive accounts should be automatically terminated

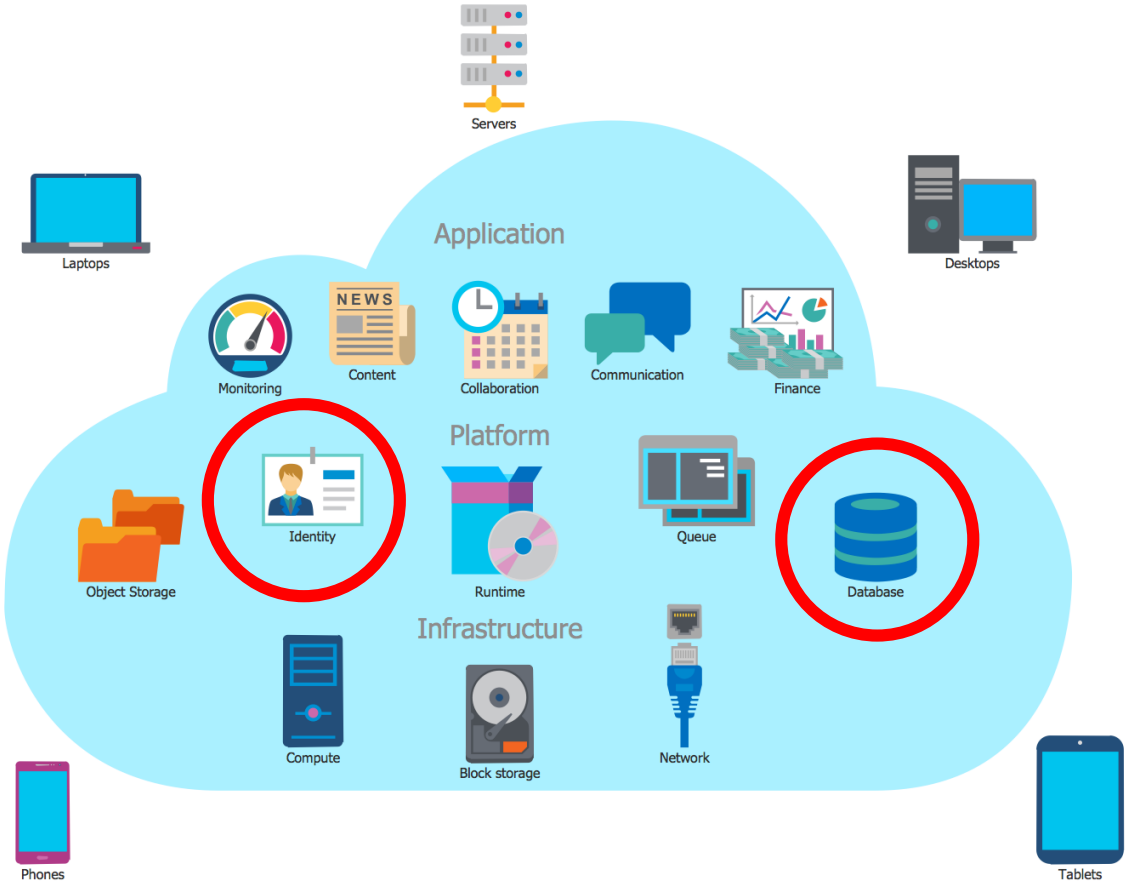
Regular Updates

- Regularly check for software updates
  - Should be don't at least once a month
- Create a schedule for periodically updating software
  - Updates should be made only when machines are not in use
- Update hardware!
  - Update at least once every 5-10 years

Access Control for Cloud-based Smart Manufacturing

Overview of Cloud Computing

- Cloud-based solutions provide services via a remote server
  - Services such as data storage, access control, etc.
  - Remotely accessible – useful during extreme cases, such as a pandemic
  - Does not require regular maintenance



Overview of Cloud Computing

- Cloud Service Examples
  - Data storage – Dropbox, Google Drive, Microsoft OneDrive
  - Access control – Lenel BlueDiamond, Brivo, Prodatakey, Openpath
  - Password Management – Bitwarden, 1Password

bitwarden 1Password

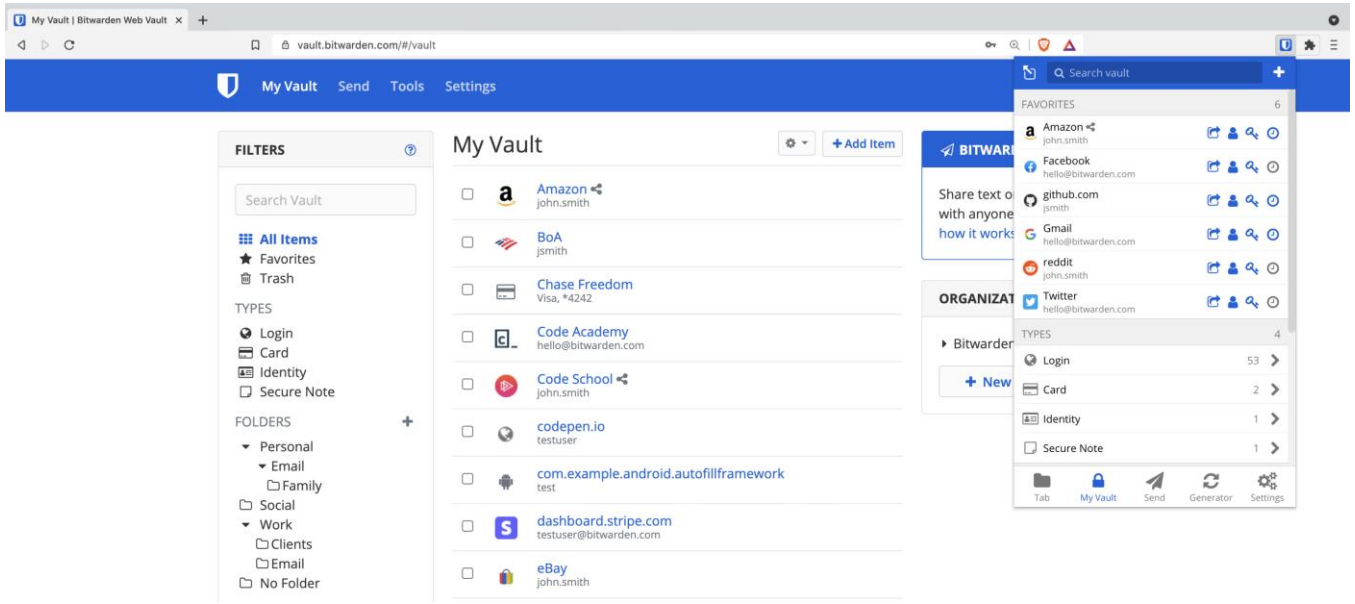
Cloud-based Access Control

- Access control via cloud-connected applications and devices
- Cloud-based physical access control
  - Access physical resources without the need of a key/keycard.
  - For example, unlocking a door to a room full of CNC machines using your phone

Unlock using phone app

Cloud-based Access Control

- Cloud-based online access control
  - Remotely controlling access to online user accounts
  - Allows random passwords that don't need to be remembered
  - For example, using password managers to store CNC machine user account credentials



Importance of Cloud-based Solutions

- Control access from anywhere
- Easily update/revoke credentials to access physical/online resources
- Easy to scale, operate and maintain
- Requires cloud-connectivity – no internet = no access!
- Password managers – master password becomes single point of failure
  - If master password is compromised, all accounts are vulnerable!

Best practices of Cloud-based Solutions

- Regularly update/revoke access control permissions
  - For example, employees changing teams, leaving company
- Password manager – allows random passwords
- Update critical credentials regularly
  - For example, update master password at least once a month
  - Ideally, master password should be updated after every use
- Keep physical backups
  - During emergencies, cloud services may not always be accessible
  - For example, backup physical keycards

Thank you!

Contact: hanif.rahbari@rit.edu
Wireless and IoT Privacy (WISP) Lab (rit.edu/wisplab)
ESL Global Cybersecurity Institute
Rochester Institute of Technology

Hanif Rahbari

Sid Dongre