CANADIAN CENTRE FOR CYBER SECURITY

Learning Hub

Short Presentation – 155

Strengthening Authentication

Presentation Outline

- Part 1 – Identification and authentication
- Part 2 – Threats to authentication
- Part 3 – Methods of authentication
- Part 4 – Attributes of authentication
- Part 5 – Using typical types of authentication

Part 1 – Authentication

- What are identification and authentication?
- What do we authenticate?

What Are Identification and Authentication?

- **Identification** means providing a unique identification to an entity:
  - Username
  - Role
  - Device ID Number
- **Authentication** means providing a level of assurance to the accuracy of the identification
- Different schemes of authentication provide different **levels of assurance**
- The level of assurance needed is in relation to the **sensitivity of the information system** being accessed

What Do We Authenticate?

- Objectives defined in the Directive on Identity Management:
  - To manage identity in a manner that mitigates risks to personnel and organizational and national security, while protecting program **integrity** and enabling trusted citizen-centered service delivery
  - To manage identity consistently and collaboratively within the Government of Canada and with other jurisdictions and industry sectors, where identity of **employees**, **organizations**, **devices** and **individuals** is required
  - To manage **credentials**, **authenticate users** or **accept trusted digital identities** for the purposes of administering a program or delivering an internal or external service

Reference: Directive on Identity Management (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577)

Part 2 – Threats to Authentication

- What is the role of authentication?
- What happens when authentication cannot be trusted?

Fraud Committed by Deepfake Voice

- First machine-learning deepfake used in a scam
- A CEO was fooled into believing he was talking to the CEO of the parent company
- Following orders, a transfer of funds was immediately initiated

Source: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=7c2bf38c2241

DeepVoice Example

- Joe Rogan's voice was "deepfaked"
- The audio clips demonstrate machine-learning capabilities

Source: https://youtu.be/DWK_iYBl8cA

Authentication

- Authentication is critical operation for interactions:
  - Between users
  - Between systems and users
  - Between users and systems
- Authentication protects:
  - Privacy
  - Confidentiality
  - Integrity
  - Authenticity
  - Availability
  - Non-repudiation

Challenges to Authentication

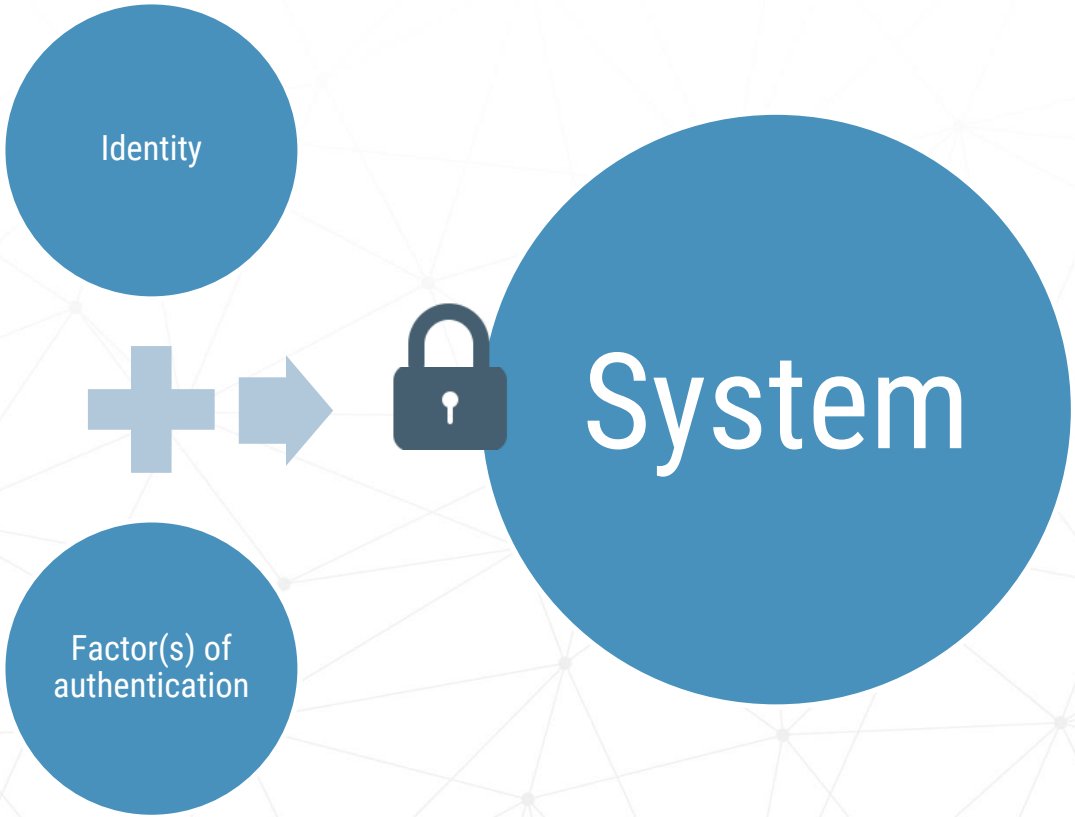
- Online services are expanding faster than we can secure them
- Authentication methods are not up to the level of sophistication of attackers
- Older methods still used are very inadequate:
  - Social Insurance Numbers
  - Photo ID
  - Printed invoice

Part 3 – Methods of Authentication

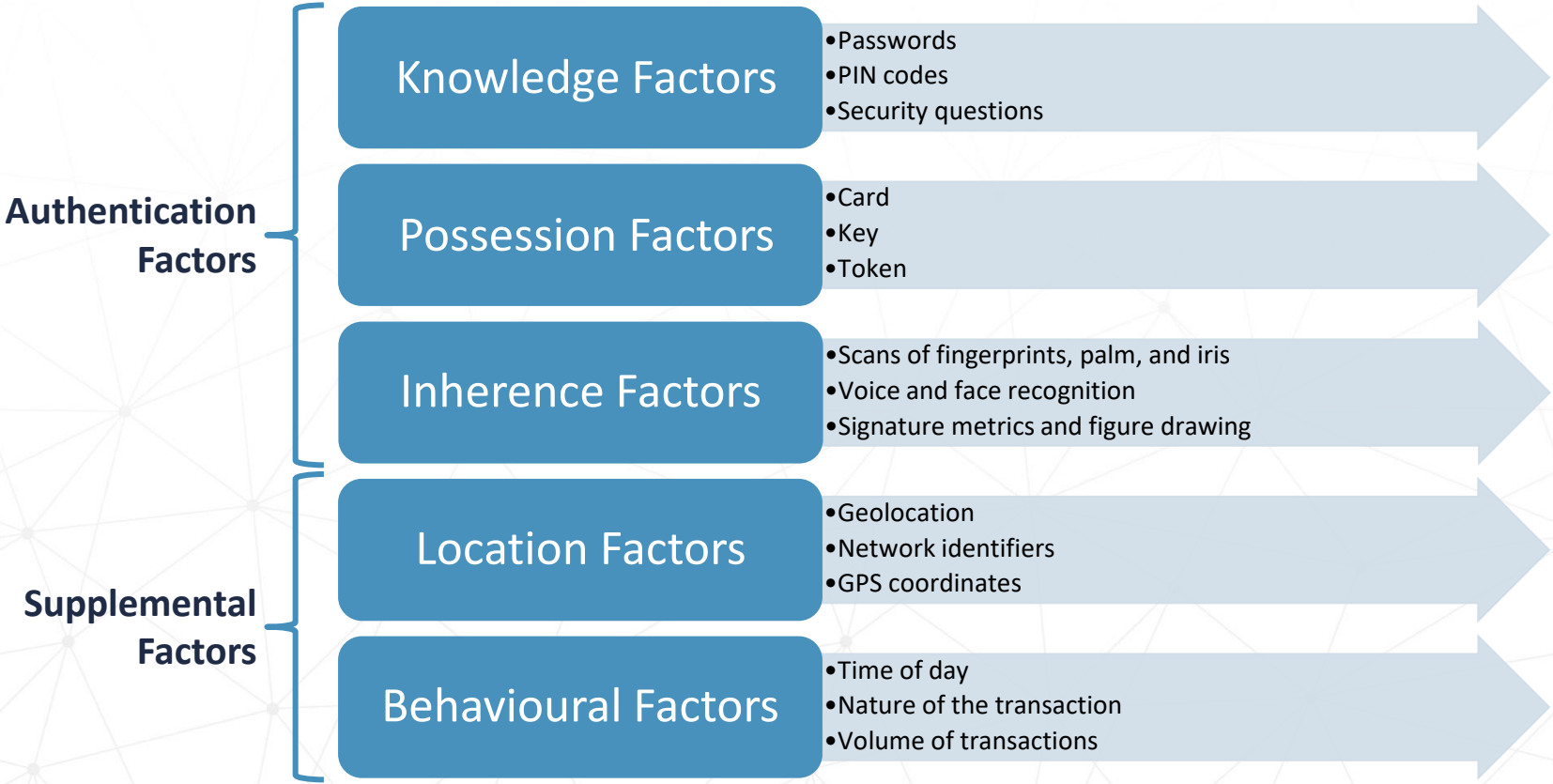
In this module the learner will explore:

- Identification and authentication
- Factors of authentication
- Pathways to authentication

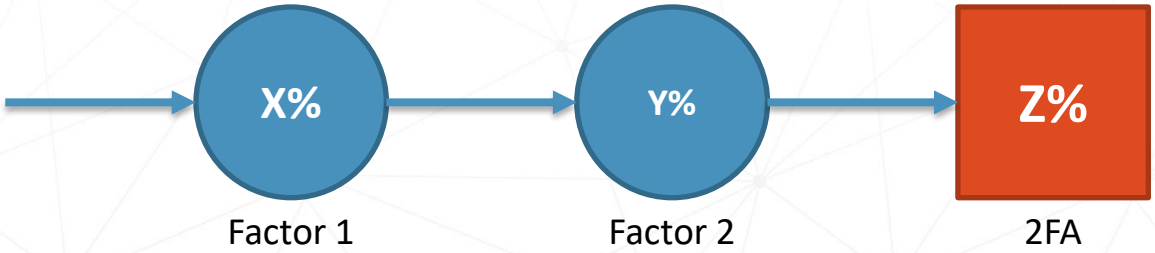
Identification and Authentication Methods



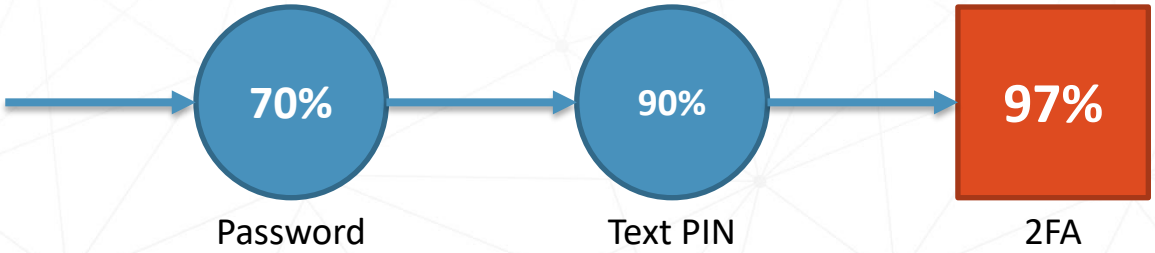
Authentication Scheme Components



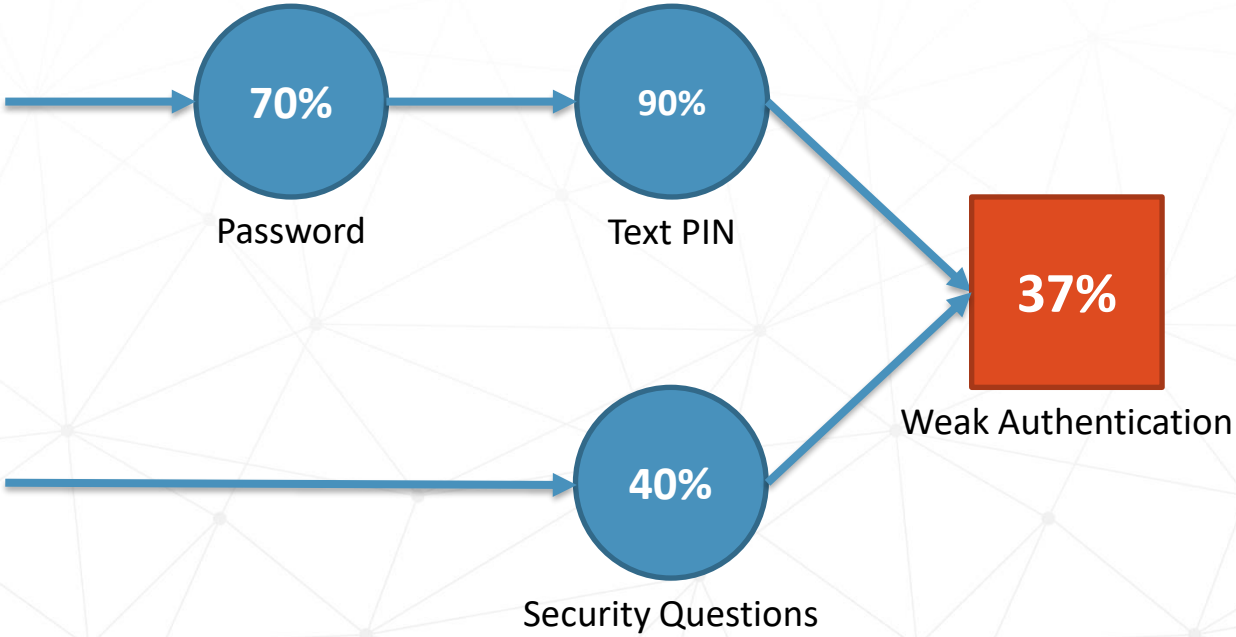
Multiple-Factor Authentication



Multiple-Factor Authentication



Multiple-Factor Authentication



Multi-Factor Authentication

- Can increase the assurance level – when done right
  - One path, multiple authentication – stronger than the best authentication
  - Multiple paths, multiple authentication – weaker than the worst authentication

Part 4 – Attributes of Authentication

- Which attributes should be considered for authentication?
- Which authentication methods implement the attributes?

Attributes of Authentication

- Strength and assurance (robustness)
  - Unforgeable
  - Not exposed to outsiders
  - Protected from insiders
  - Protected from interception
  - Protected from storage breach
  - Protected from replay attack
  - Protected from social engineering
  - Industry-recognized and adopted
- Deployment
  - Low cost
  - No special equipment
- Accuracy and reliability
  - Low false acceptance rate (FAR)
  - Low false rejection rate (FRR)
- User-friendliness
  - Low user effort
  - Convenient
  - Enrollment time
  - Possibility of modification
  - Remote use
  - No privacy impacts

Attributes of Authentication – Signature

- Strength and assurance (robustness)
  - ✗ Unforgeable
  - ✗ Not exposed to outsiders
  - ✗ Protected from insiders
  - N/A Protected from interception
  - ✓ Protected from storage breach
  - ✗ Protected from replay attack
  - ⚠ Protected from social engineering
  - ⚠ Industry-recognized and adopted
- Deployment
  - ✓ Low cost
  - ✓ No special equipment
- Accuracy and reliability
  - ✗ Low false acceptance rate (FAR)
  - ✓ Low false rejection rate (FRR)
- User-friendliness
  - ⚠ Low user effort
  - ⚠ Convenient
  - ⚠ Enrollment time
  - ✓ Possibility of modification
  - ⚠ Remote use
  - ⚠ No privacy impacts

Note: This documentation is not official and for discussion purposes only

Attributes of Authentication – Chip and PIN

- Strength and assurance (robustness)
  - ✓ Unforgeable
  - ⚠ Not exposed to outsiders
  - ⚠ Protected from insiders
  - ✗ Protected from interception
  - ✓ Protected from storage breach
  - ✓ Protected from replay attack
  - ✓ Protected from social engineering
  - ✓ Industry-recognized and adopted
- Deployment
  - ✗ Low cost
  - ✗ No special equipment
- Accuracy and reliability
  - ✓ Low false acceptance rate (FAR)
  - ✓ Low false rejection rate (FRR)
- User-friendliness
  - ⚠ Low user effort
  - ⚠ Convenient
  - ⚠ Enrollment time
  - ✓ Possibility of modification
  - ⚠ Remote use
  - ✓ No privacy impacts

Note: This documentation is not official and for discussion purposes only

Attributes of Authentication – Iris Scan

- Strength and assurance (robustness)
  - ⚠ Unforgeable
  - ✗ Not exposed to outsiders
  - ⚠ Protected from insiders
  - ⚠ Protected from interception
  - ⚠ Protected from storage breach
  - ✗ Protected from replay attack
  - ✓ Protected from social engineering
  - ✓ Industry-recognized and adopted
- Deployment
  - ✗ Low cost
  - ✗ No special equipment
- Accuracy and reliability
  - ✓ Low false acceptance rate (FAR)
  - ✓ Low false rejection rate (FRR)
- User-friendliness
  - ✓ Low user effort
  - ✓ Convenient
  - ⚠ Enrollment time
  - ✗ Possibility of modification
  - ⚠ Remote use
  - ✗ No privacy impacts

Note: This documentation is not official and for discussion purposes only

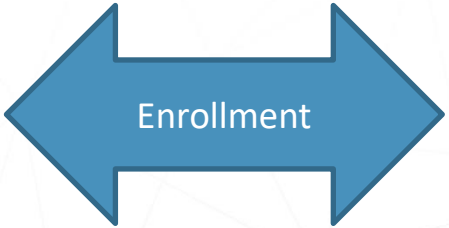
Attributes of Authentication - Password

- Strength and assurance (robustness)
  - ✓ Unforgeable
  - ⚠ Not exposed to outsiders
  - ⚠ Protected from insiders
  - ✗ Protected from interception
  - ⚠ Protected from storage breach
  - ⚠ Protected from replay attack
  - ✗ Protected from social engineering
  - ✓ Industry-recognized and adopted
- Deployment
  - ✓ Low cost
  - ✓ No special equipment
- Accuracy and reliability
  - ✓ Low false acceptance rate (FAR)
  - ✓ Low false rejection rate (FRR)
- User-friendliness
  - ✗ Low user effort
  - ✓ Convenient
  - ✓ Enrollment time
  - ✓ Possibility of modification
  - ✓ Remote use
  - ✓ No privacy impacts

Note: This documentation is not official and for discussion purposes only

One-Time Password

Website with OTP Capability



Laptop Registering Account

Cell with OTP App Synchronizing

Current OTP Expected

2FA Authentication

Cell with OTP App

Attributes of Authentication – One-Time-Password

- Strength and assurance (robustness)
  - ✓ Unforgeable
  - ✓ Not exposed to outsiders
  - ⚠ Protected from insiders
  - ✓ Protected from interception
  - ⚠ Protected from storage breach
  - ✓ Protected from replay attack
  - ✓ Protected from social engineering
  - ✗ Industry-recognized and adopted
- Deployment
  - ⚠ Low cost
  - ⚠ No special equipment
- Accuracy and reliability
  - ✓ Low false acceptance rate (FAR)
  - ⚠ Low false rejection rate (FRR)
- User-friendliness
  - ⚠ Low user effort
  - ⚠ Convenient
  - ⚠ Enrollment time
  - ⚠ Possibility of modification
  - ✓ Remote use
  - ✓ No privacy impacts

Note: This documentation is not official and for discussion purposes only

Part 5 – Tips to Use Authentication

- Best practices for password use
- Best practices for biometrics
- Best practices for one-time-password use

Best Practices for Password Use

- Minimize user effort and password fatigue:
  - Do not generate your own passwords
  - Do not memorize your passwords
- Use a trusted password manager:
  - To generate pseudo-random robust and unique passwords
  - To protect the passwords in one or more encrypted vaults
  - Safeguard access to vaults with strong authentication

Best Practices for Password Use

- Do not log into services from unmanaged devices
- Leverage your trusted devices for authentication

Full Disk Encryption:
Biometric + PIN access

Password Manager:
Biometric

Website: Password +
Second Factor

Best Practices for Biometrics Use

- Convenient for repeated use:
  - Unlock phone or laptop
  - Access security area in workplace
- Use with local encrypted storage
- Use as a second factor

Best Practices for Software OTP

- Use as a second factor for authentication
- Use from a trusted device
- Implement recovery methods

GoogleOTP

FreeOTP

Best Practices for Hardware OTP

- Use as a second factor of authentication
- Use devices compatible with Fast ID Online (FIDO) security standard
- Use two devices to have a backup if you lose one
- Implement a handling strategy, as you would a security badge

Google Titan Key Bundle

Yubikey

Conclusion

Summary:

- Authentication
- Threats to authentication
- Methods of authentication
- Attributes of authentication
- Tips to use authentication methods

Questions