Authentication Based Attacks

Objectives

- Discuss what authentication is and how it’s performed
- Understand what points in the authentication process are vulnerable to attack
- Discuss how users habits can introduce risk in the way they authenticate

Authentication

- RFC 4949 defines user authentication as “The process of verifying an identity claimed by or for a system entity”
- This could be a user or system
- We also call this a “security principal”
- It’s really an object
- Can the object authenticate?

Authentication Steps

- Identification Step
  - Presents an identifier to the system
  - Could be a security principal
- Verification Step
  - Is there something that validates or verifies the identity presented or security principal presented

Authentication Systems

- There are many authentication systems in existence
- Think about how many devices you own
- Think about how many times you log into something
- Windows
  - Credential providers, Windows 10
- Linux
  - PAM
- CAS, SSO, AUTH, ETC

E-Authentication Architectural Model

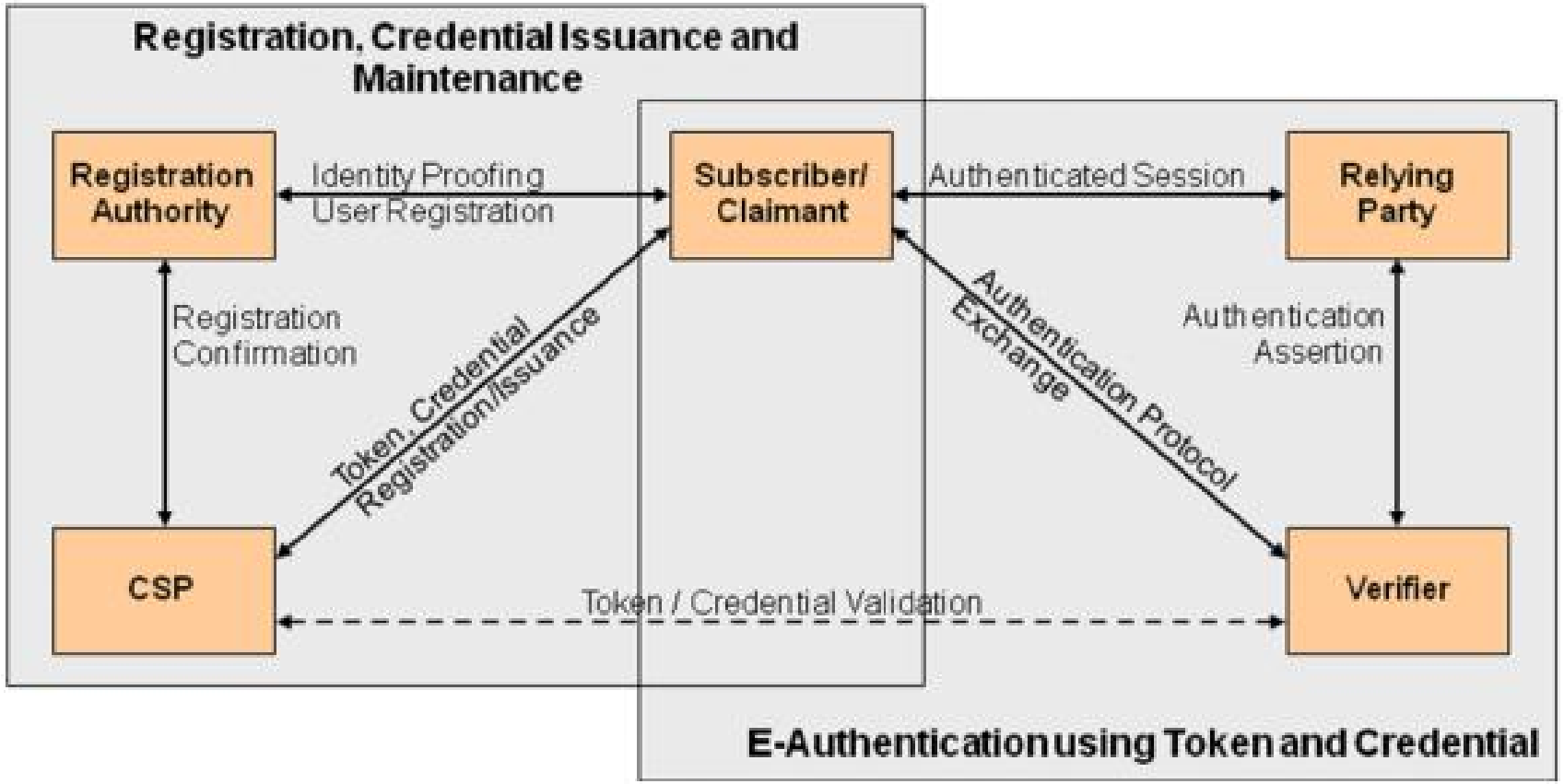

Figure 1 - *The NIST SP 800-63-1 E-Authentication Architectural Model*

Factors of Identification

- Something you know
  - Password
  - PIN
  - Security Questions
- Something you have
  - Smartcard
  - Physical Token
- Something you are
  - Fingerprint
  - Iris
- Something you do
  - Voice pattern
  - Handwriting

Threats to something you know

- Password authentication
  - Phishing
  - Poor password management techniques
  - Key logging
  - Other eavesdropping
- Password based attacks
  - Password cracking
  - Rainbow tables
  - Password storage attacks
- Secret questions
  - Easy to obtain answers

Threats to something you have

- Very few
- Usually protected with a chip
- However, RFID copying
- Magnetic copying

Threats to something you are

- Some say the industry just isn’t there yet
- Many “facial recognition” systems are fooled with a print out of your face
- False positives or false negatives are issues with this

Overall security issues

- Eavesdropping
- Replay
- Malware
- Denial of Service
- Host and client based attacks
- Really depends on the how clever you are