Overview of Security Issues and Architectures

Dr. John Campbell, President, Bion Biometrics Inc.

Panel on Security Issues and Architectures for Biometric Integration in E-Authentication Systems

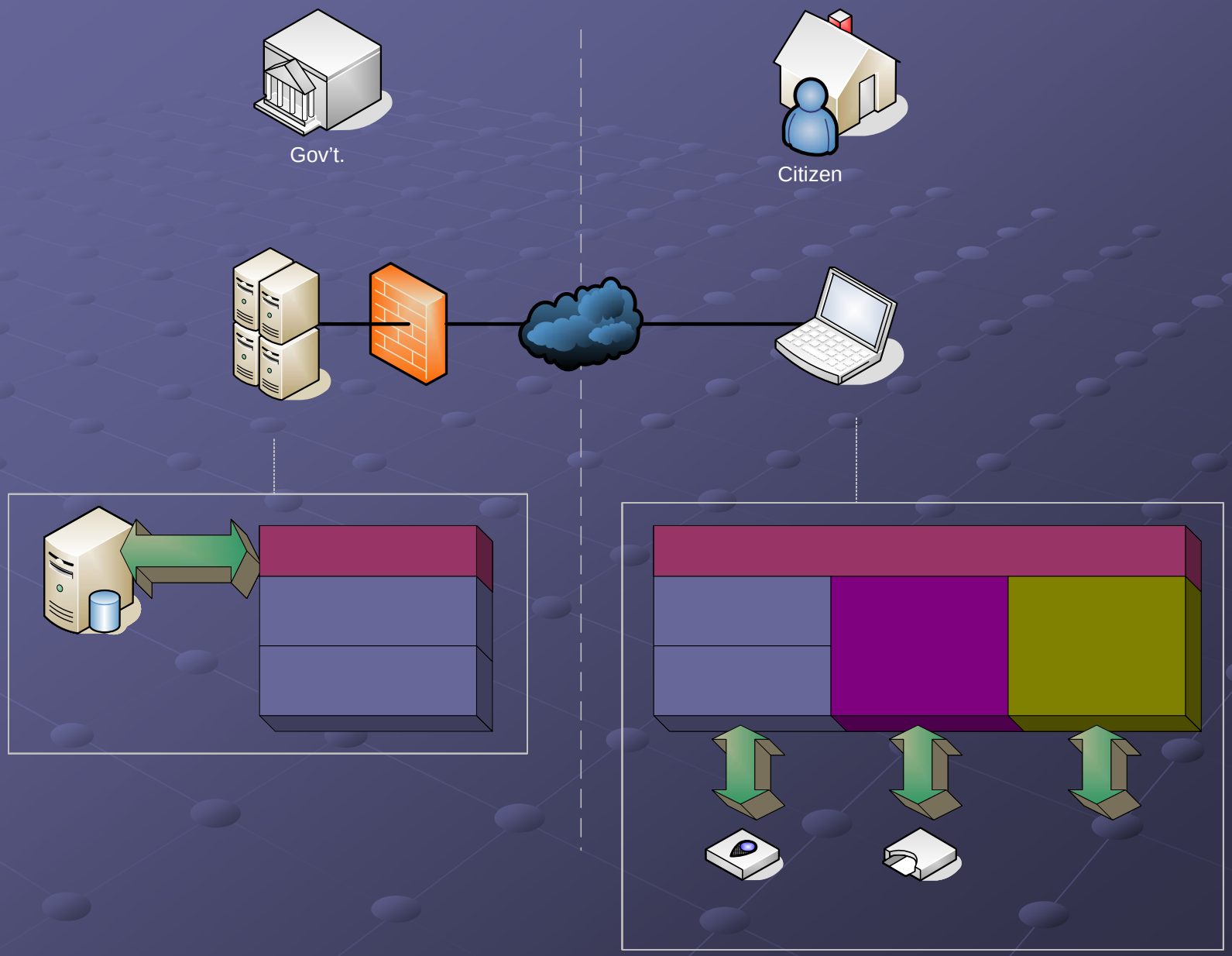
NIST Workshop on Biometrics and E-Authentication Over Open Networks

Wednesday, March 30, 2005

E-Authentication Over Open Networks

- Authenticate user identity to (Government) IT System
- Information passes over untrusted network (e.g. internet)
- Four levels of authentication
- Level 1 and 2 require only one factor authentication
- Levels 3 and 4 require two factor authentication
- Three factors are:
  1. Something you know (e.g. password)
  2. Something you have (e.g. smartcard)
  3. Something you are (e.g. biometric trait)

Generic Architecture Diagram



Security Issues in Generic Diagram

- Protocol Attacks (Eavesdropping, Replay, Man-in-the-Middle, etc.)
  - Mainly in the open network (internet)
  - Can be in the local stack from client to application to device, if client or device are compromised (trojans, keyboard sniffers, etc.)
  - Solutions are the same regardless of whether password, token or biometric are involved (digital signing, encryption, etc.)

Security Issues in Generic Diagram

- System Compromise (with or without insider assistance)
  - Strong network security and physical controls must be in place to limit risk on Gov't side
  - Citizen side may be a public kiosk or an individual's PC and can't be properly secured
  - This is why higher authentication levels require FIPS certified tokens and appropriate protocols, so authentication relies only on the token and the server

Security Issues in Generic Diagram

- Brute Force Attacks
  - Try to guess password or cryptographic key from token or find matching biometric
  - Requires appropriate password complexity, key length of biometric false accept rate
- Out of Band (Social Engineering)
  - Password written down
  - Attacker poses as technical support
  - Steal or borrow physical token
  - These are TOUGH issues
  - Banking example!

Biometrics in E-Authentication

- Level 1 and Level 2 E-Authentication allow password alone or token alone, but not biometric alone.
- Level 3 and Level 4 allow password and token or biometric and token, but not password and biometric.
- Why?

Biometrics in E-Authentication

- Is biometric authentication inherently less secure than other methods?
- What security techniques currently exist for use with biometrics authentication and how do they fit in the authentication architecture?
- These panelists will discuss these issues.