Headquarters U.S. Air Force

Integrity - Service - Excellence

Technology Convergence

Mr. Konieczny
SAF/CIO CTO
Aug 2018

U.S. AIR FORCE

U.S. AIR FORCE

Discussion

- Technological convergence is the combination of two or more different technologies into a single capability
- Today's discussion topics
  - Use of biometrics information for personnel authentication
  - Extension of attribute based access control solution to content based management
  - Combination of Internet of Things (IoT) sensors to provide situational alerts
  - Combination of development tools into a unified environment to support automated Risk Management Framework (RMF) for Authority To Operate (ATO)

U.S. AIR FORCE

Personnel Authorization

- Smart devices have various embedded and auxiliary capabilities to provide personnel authentication
  - Auxiliary devices:
    - CAC reader
    - Security key fob
  - Embedded biometrics devices:
    - Retina scan
    - Fingerprint reader
    - Facial recognition
    - Voice recognition
    - Gait recognition
    - Selection/typing screen pressure recognition
  - Pattern of life detection
  - PIN meeting some alpha/number/symbol requirement

Authorization Access Controls

- How can these capabilities be combined to achieve the same or better assurance than the CAC?
  - Each capability has a maximum validation asurety value based on historical error rates/false reading
  - Also, each capability has certain criteria it must meet to provide its highest asurety value
  - Each type of data has an asurety requirement (e.g., a score associated with each impact level 2, 4, 5, and 6 as used in the cloud security designations)
  - So, to get access to a specific data set, the sum of the reported asurety values from each sensor capability should be equal or better than the asurety value of the data set
- Plan is to automatically gather random sensor data to meet the data asurety level; if the level cannot be achieved, then request user interaction
- Extension to the office environment with various sensor devices as a CAC replacement
- Experimenting with smart devices to be integrated with an access control system

U.S. AIR FORCE

Content Access Control

- An attribute-based access system provides role/claim based authorization access to application data dynamically based on user attributes; when attributes change, accesses also change
- A digital rights management system encrypts data, and provides decryption based on user registrations for that data, usually by group which a system admin maintains
- Goal is to use the automated generation of access with the digital rights system to provide automated access to content

Content Access Control

- Piloted this concept using Special Victims Counsel legal documents with success
  - Documents were classed based on content (e.g., evidence, client-lawyer info, lawyer notes)
  - Access to content was dynamically generated and changed when associated attributes were changed (e.g., paralegal reassigned to different case)
- Key to success was the ability to classify the documents and then determine the access requirements in terms of personnel attributes
- Further research is currently being done into the dynamic, semantic, analysis of content and using machine learning algorithms to classify the document for access

U.S. AIR FORCE

IoT Sensor Convergence

- IoT sensors are increasing in homes, as well as, on USAF bases
- The correlation of these, with additional information, can provide (1) Better situational awareness; (2) Potential alerts based on incident based machine learning

U.S. AIR FORCE

IoT Sensor Convergence Examples

- Camera motion detection + perimeter sensor + noise sensor ⟶ potential intrusion alert (machine learning would minimize false positives due to animals, etc.)
- Tire pressure sensor on tanker truck indicates very low pressure + location of truck + ambient temperature + current load → potential alert either intrusion or maintenance issue (machine learning would determine probability of each especially based on prior truck history)
- Fit bit results show person having heart attack + ambient temp + current location + last minutes of current activity → potential alert (machine learning to ascertain medical emergency or personnel attack emergency or normal for this person)

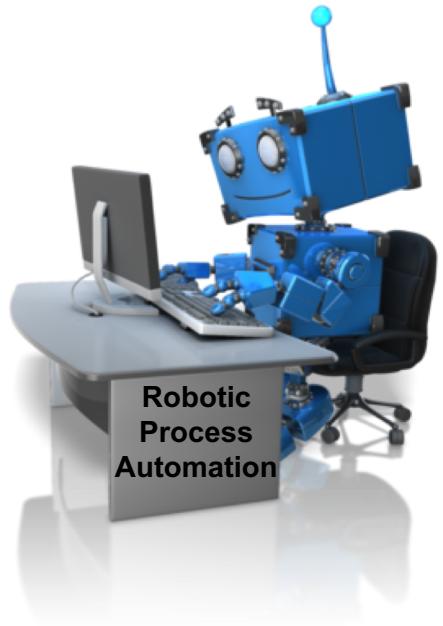
IoT Sensor Convergence

- Future activities:
  - Research a gateway that can effectively accumulate all types of IoT sensors at different rates and protocols
  - Establish potential convergence sensor combinations
  - Determine mission/personnel risk score based on correlated IoT sensor readings
  - Correlate risk incidents with mission threads to provide additional incident warning information

U.S. AIR FORCE

Automated Risk Management Framework (RMF)

- Goal: Build in and validate security during application development phases for "ATO in a Day"
  - Work with development community and users on an agile development process
  - Map the OWASP Application Security Verification Standard mapped to RMF controls
  - Based on the OWASP Application Security Verification Standard mapped to RMF controls
  - Select automated process/tools to satisfy the controls that satisfy the ATO criteria on the network
  - Support RMF continuous monitoring by performing update activities using the process/tools
  - Supply chain (software/hardware) analysis, as well as, test/pen test results stored and categorized in the RMF
- Results:
  - Used one application as a pilot (Air Tanker Refueling Scheduler)
  - Made changes based on lessons learns
  - Standardized the process for new application development in the Air Operations Center



U.S. AIR FORCE

Questions

- POC: Mr. Frank Konieczny
- Email: AFITC2018.AFCTO@gmail.com
- Comm Phone / DSN: 571-256-2524 / 260-2524