SAND2014-19127PE

Exceptional service in the national interest

Sandia National Laboratories

EMBERS:

EpheMeral Biometrically Enhanced Real-time location System

Sung Choi, Michael Bierma,
Yung Ryn (Elisha) Choe, David Zage

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2014-18652 C

Outline

Sandia National Laboratories

- Background
- Current Authentication Methods
- Real Time Location System (RTLS)
- Ephemeral Biometrics (EB)
- EMBERS = EB + RTLS
- Three Use Cases (Application Scenarios)
- Findings
- Limitations
- Conclusion

Background

- High Security Environment
  - Nuclear Facilities
- Accountability of critical assets, personnel, and activities
  - Essential for productive, safe, and secure operations
  - Manual procedure: inefficient and prone to human error
- Goal is to actively and continuously monitor
  - Reduce human reliability issues
  - Eliminate insider threat concerns
- Integrated Security Facility (ISF) in Sandia National Labs (SNL)
  - Functional testing ground
  - Physical Protection System (PPS) – Security camera, vibration sensors, IR sensors, and microwave motion detector are operational

Current Authentication Methods

What you know

What you have

What you are

--> Traditional two or three factor authentication

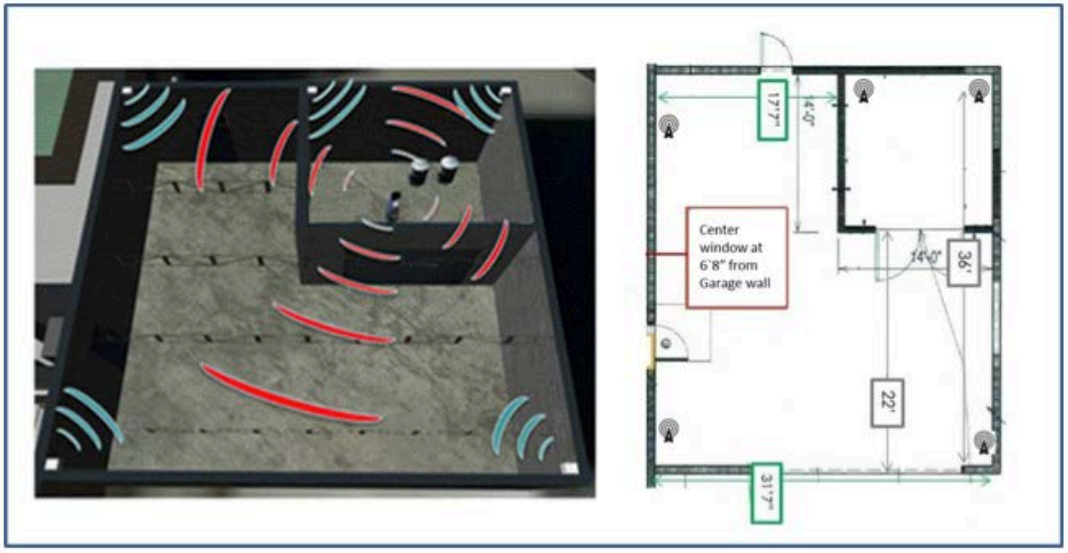
Flaws

Sandia National Laboratories

- Session hijacking
- Human error
- Violation of psychological acceptability
- Very easy to break
  - Especially vulnerable to insider attacks

Adding Real Time Location System

- Continuous id tracking and mediation of access to resources
- Requires remote threats to acquire physical presence
- Real time automated enforcement of cyber and physical security policies



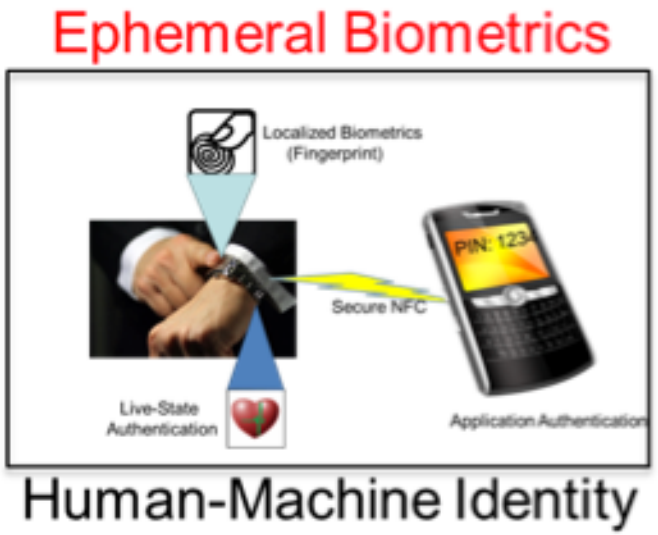
RTLS Weaknesses

Sandia National Laboratories

- Leaving Real Time Location System (RTLS) device behind
- Transfer to unauthorized party
- How can we mitigate these weaknesses to provide a better authentication method for protection against insider attacks?

Ephemeral Biometrics

- Unique human-to-machine identifier
- Distinctive id derived from merged traits of human factors (fingerprint, password) and the live state of user
- Continuously validates living state of individual
- Convenient form factors (watch) offer minimal impact to user



EMBERS

Sandia National Laboratories

- EpheMeral Biometrically Enhanced Real-time location System
- Combining Ephemeral Biometrics (EB) with RTLS
- Mitigate some of the weaknesses of both EB and RTLS
- Non invasive way of providing continuous authentication in high security environments
  - EMBERS uses the live state of the user to continuously authenticate a login session versus the traditional method of logging in once and being authenticated for the rest of the session
  - Creates a temporary unique identity, so only the actual user can be authenticated and malicious persons don't have access
  - Tracks the position of the user
- Heuristic Integration Study

Motivations

Sandia National Laboratories

- More accurate accountability of critical assets, personnel location, and activities
- Humans are error prone; EMBERS is automated
- Higher levels of security while also giving increased convenience to the user
- Harder to compromise due to dynamic nature of authentication

Use Cases – (1) Access Control

- Personnel (Facility Access)
  - Area Resident Personnel
  - Authorized Access Personnel
  - Visitors

- Material
  - Container D tagged with RTLS token
  - Manager A can take container out of the vault
  - Employee B can handle the container inside the vault
  - Employee C can only view the container

Use Cases – (2) Two-man Rule

- Used for high security applications
  - In government to mitigate insider threat
  - In Financial – large financial transaction
- Complex enforcement systems
  - Protocols and Procedures
  - Key lock combination and management
- EMBERS provides easy access and superior performance

Use Cases – (3) Safety

- Heart attack
  - Built-in inertial measurement unit
- Radiation zone dwell time
  - Track radiation exposure rate
  - Audible warning sign can be turned on
- Staff accounting
  - In case of emergency, track employee location
  - Whether employee is moving or last location

Findings

Sandia National Laboratories

- Ultra-wideband (UWB) tracks personnel indoors and outdoors
  - High tolerance for metals and electromagnetic interference
- Access to support and vendor APIs critical in order to develop custom solutions for varying use cases
- RTLS was able to read active tags of all personnel
  - Entry and Exit was tracked with master list in restricted area
- Difficulty in integrating RTLS with local access controls in place
  - Technically and politically challenging
- Challenge in logistics of distributing and managing RTLS tags
  - Visitor tag association with authorized personnel for accountability

Limitations

Sandia National Laboratories

- Inconsistent granular resolution (< 1ft) because of imprecise location measurement using RTLS UWB technology
- Sensor based RTLS not scalable, and vulnerable to DoS attacks
- Infrastructure deployment was not cost effective
- Reliable Ephemeral Biometric data stream required

Conclusion

Sandia National Laboratories

- EMBERS as 4th factor authentication
  - "Where you are" as 4th factor with Ephemeral Biometrics
- Integrates space/time/live-state of user
  - New form of Cyber-Physical identity: unique machine-to-human id
- Protocol for truly active and continuous authentication
- Further research and development needed to explore possible applications combining physical presence and persistent identity verification
  - To combat remote cyber threats and malicious insider threats

Questions?

Sandia National Laboratories

Future Work

Sandia National Laboratories

- Applications of this technology
- Two-man rule testing with vault doors
- Tracking flagged EMBERS users with on site cameras
- Doors locked/unlocked based on people in vicinity
- Automation of portable tools