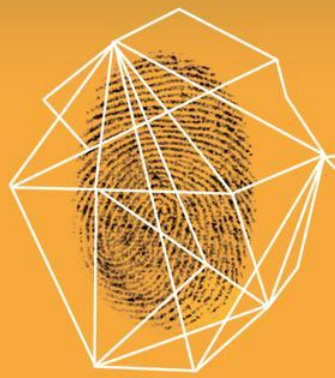


Security in knowledge

Rugged Identity Management - Avoiding Single Points Of Failure

Vernon Williams, CISSP ISSEP

The Patria Group

RSA CONFERENCE 2013

Session ID: IAM-R35A

Session Classification: Intermediate

Vern Williams

- CSO, The Patria Group
- CISSP ISSEP CBCP ISAM
- BS in Oceanography, US Naval Academy
- 20 Year US Navy Nuclear Submarines
- Masters of Science in Information Systems
- ISSA Fellow, IEEE Senior Member
- Disaster Relief Coordinator, ADRN

- VernWilliams@PatriaCorp.com
- Vern.Williams@IEEE.org
- 512-297-8798

THE PATRIA GROUP
Integrated Response Solutions

Environment / Tasking

- EM*ES Emergency Management Exercise System
  - Trained Nation's Emergency Operations Staff
    - Texas A&M Engineering Extension (TEEX), College Station, TX
  - Refined software in the classroom over 9 years of training classes
  - TPG Licensed to commercialize software
- Preparation for the real world requires:
  - Robust communications infrastructure
  - Hardened systems
  - Fault tolerant Identity management
  - Biometric authentication

Requirements

- Role Based Access Control / High Assurance Identity
  - Each responder is assigned a specific role in the recovery effort
  - Infrequent usage makes UID/PW based solutions impractical
  - Need a solution that ties an individual to their role with the option to substitute in case they are not available when the balloon goes up and the Fire Chief is on the beach in Hawaii.
- Eliminate single points of failure
  - Redundant data store
  - Fail over applications
  - Robust and secure DNS (DNSSEC)

Robust IdM: Not Optional

- Passwords are Insecure and Easily Broken
- Access control, the heart of security, is :
  - Allowing only authorized users, programs, or processes access to systems or resources;
  - Granting or denying, according to a particular security model, permission to access a resource;
  - Set of procedures--performed by hardware, software, and administrators--to monitor access, identify users requesting access, record access attempts, and grant or deny access based on pre-established rules
- Multifactor Authentication is key for critical systems or elevated privileges.

THE PATRIA GROUP
Integrated Response Solutions

IdM Solutions – Emerg. Management

- Infrequent use results in delays responding due to forgotten passwords or login IDs.
- Responders may need to authenticate from a variety of systems / mobile devices.
- Actions of responders need to be linked to their identities (life and death decisions and legal implications)
- If your data center is part of the casualty, you still need to be able to respond and manage the outcome.

THE PATRIA GROUP
Integrated Response Solutions

IdM Solutions – Emergency Mgt

- Level of authority needs to be associated with the level of assurance in the identity methods.
- Multiple USB connective methods support connection to a variety of systems / mobile devices.
- Responders can carry the Emergency Mgt application with the authentication device and provide a secure desktop even on untrusted systems.
- An alternative remote copy of the organizational and emergency response data means access and response from anywhere.

Identity Proofing

- Identity Proofing –The process by which the credential issuer validates sufficient information to uniquely identify a person applying for the credential. (NIST)
  - Prove that the identity exists
  - Prove the applicant is entitled to that identity
  - Address the potential for fraudulent issuance of credentials based on collusion
- Identity Source Documents: Need 2 I-9 Identity Sources
  - Must include a government-issued picture ID and fingerprints (10 for identification and two for verification)
- Background Checks: SF 85
  - Required Investigations based on the information provided in SF 85 and the Identity Source Documents

Applicable Technologies

- Biometrics
  - Facial Recognition
  - Dynamic Signature
  - Fingerprint Recognition
  - Hand Geometry
  - Iris Recognition
  - Palm Print Recognition
  - Speech Recognition
  - Vascular Pattern Recognition
- Automated Identity Proofing
  - Classic knowledge-based authentication (KBA)
  - Dynamic KBA
  - Out-of-band proofing

THE PATRIA GROUP
Integrated Response Solutions

Robust Identity Management

- Thorough Identity Proofing
- Granular Role Based Access Control (RBAC)
- Multi-Factor Biometric / Certificate Authentication
- Graceful failure modes
  - Both for Authentication Method and Remote Access to the control or response applications
- “Break Glass” with alerting and logging

THE PATRIA GROUP
Integrated Response Solutions

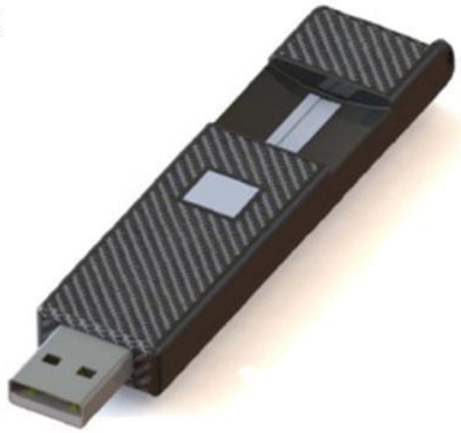
Product Selection

- M4S Authentication Gateway
  - The heart of the M4S solution
  - Brokers connection between endpoints
  - Enforces corporate security policies
  - Implements single sign on
  - Sets up the Secure Sync Channel
  - Provides secure management consoles
- Secure Sync Channel
  - Defeats common SSL/TLS attacks
    - Man In The Middle
    - Man In the Browser
    - Key logger
    - Replay

THE PATRIA GROUP
Integrated Response Solutions

Product Selection

- Personal Smart Key
  - Programmed by Me4Sure to Implement
  - Repudiation-proof fingerprint authentication
  - Virtual and remote desktop support
  - Secure storage for data, biometrics, softw
  - Corporate security policy enforcement
  - APIs for customization
- Demo



Security in knowledge