AFCEA Global Identity Summit 2014
Engagement Theater

Tuesday, September 16th

2:00 p.m. - 3:50 p.m.

Confirmation of the Biometric Identity of an ePassport Holder and Atomic Authorization for Devices (AKA Secure Attribute Management for the Cloud)

Prequalified for one CompTIA CEU: Security+, Cloud+, and CASP and one GIAC CPE

Presenters (ePassport Validation):
Bill Russell
Chief Technology Officer
Mount Airey Group, Inc.

Phil Stevens
Director, Government Sales
WidePoint Corporation

Presenters (Attribute-based Access Control):
Paul Townsend
Director of Cybersecurity
Mount Airey Group, Inc.

Paul Nowacek
Director, Federal Sales
WidePoint Corporation

This session will prepare the attendee with the Best Practices review technology and processes necessary for the the PKI processing necessary to validate an e-Passport, its issuer, and its contents. The discussion will include:

- RECOMMENDED FIPS 201-2 Strong identity vetting on the front-end of the credentialing processes
- REQUIRED back-end process for Automated Border Control to confirm that the biometric(s) stored on the chip are genuine, the document is authentic, and that the identity of the traveler can be proven via a 1:1 biometric match against the chip data
- Recommended for confirmation of identity in support of Large Financial transactions and the issuance of travel VISAs/e-VISAs
- Advice and best practices for the integration into existing business processes (including PV-as-a-Service)

The session will also address Atomic Authorization for Devices (AKA Secure Attribute Management for the Cloud) that will prepare the attendee with the Best Practices to:

- Leverage Derived/Device Credentials while cryptographically controlling access to protected resources
- Securely manage authorizations/attributes/permissions and cryptographically bind them to the credential
- Securely deliver the authorizations/attributes/permissions via the cloud to the relying party without privacy concerns

Tuesday, September 16th

3:50 p.m. - 5:00 p.m.

Creating an IPSec Trusted Mobile Enterprise with Digital Signature Accountability. Always-on Security for the Always-on Mobile World

Prequalified for one CompTIA CEU: Security+, Network+, Mobility+, and CASP and one GIAC CPE

Moderator:
Eric S. Green
Director
Mobile Active Defense, Inc.

Panelists:
Larry Whiteside, Jr.
Chief Information Security Officer
Lower Colorado River Authority
Brian Murphy
President and CEO
ReliaQuest
Spencer Cobb
CEO and Co-founder
Mobile Active Defense
Phil Lambert
Associate Director, Network Security Architecture
Starwood Hotels & Resorts Worldwide, Inc.
Andy Swenson
Chief Information Officer
UPC Insurance

This session will address the challenges enterprises are being force to embrace with respect to mobility, particularly that the newest smart devices are increasingly exposed to more access to sensitive data. The session will identify the security aspects of today's mobility deployments and the need for better solutions to determine: which users on what devices are accessing what resources on enterprise networks. The attendee will be exposed to how a BYOD program can be incrementally deployed to effectively enhance your organization's security posture:

- How can we protect mobile data from snoopers and hackers?
- What best practices can be adopted for implementing secure communications for mobile devices including certificate authenticated on-demand IPSec VPN to enable mobile business?

Wednesday, September 17th

10:40 a.m. - 12:00 p.m.

An Innovative Approach to Building Federation across Diverse Groups of Relying Parties and End Users

Prequalified for one CompTIA CEU: Security+ and CASP and one GIAC CPE

Speaker:
Matthew Thompson
Founder and COO
ID.me

Deployment integration of Identity Federations can be a challenge, but through standards setting and innovative approaches to Identity Access Management that process can move much faster and bring benefits to all parties growing their respective markets. Industry based development and application of standards helps set the industry levels for operating while testing and trust marks help support rapid on boarding of Relying Partners. Customer-centric online identity models improve conversions for end users and increases trust creating a win-win on both sides of the transaction.

In this session attendees will learn:

- Lesson concerning the Integration and Deployment of Federations
- How to develop compelling services built on top of Open Standards
- The importance of Verification of Services for "Trust" as a driver and supporter of market growth
- Lessons learned from
    - Case Studies with Under Armour and KISS that support the business value created from IAM solutions
    - Retail Federation and scaling new identity solutions

Wednesday, September 17th

2:00 p.m. - 3:40 p.m.

Identity as the New Perimeter – Privileged User Management and Trust in Identity

Prequalified for one CompTIA CEU: Cloud+ and CASP and one GIAC CPE

Presenters:
Ken Ammon
Chief Strategy Officer
Xceedium, Inc.

Patty Arcano
Vice President, Government Sales
Xceedium, Inc.

The last decade has given rise to the daily report of nation-state attacks targeting information systems of US government, critical infrastructure, and business. And, as the attacks continue to increase the success rate has become a national crisis. Traditional approaches to information security continue to focus great resources on network and device monitoring while the majority of attacks are taking advantage of hijacking user accounts followed by escalating privilege. IT defenses must shift the investment from detection to protection and adopt a security foundation to separate authentication from authorization and enforce least privilege.

Mobility, cloud, and virtualization are central themes contributing to the erosion of current methods to secure a perimeter. In fact, this perimeter has eroded and now presents IT operators and security professionals with the challenge of treating identity as the new perimeter. The attendees to this session will learn how to address recent policy and technology advancements in Trusted Identity and Privileged Management and place them within the context of managing logical access controls for traditional, virtual, and cloud IT platforms. This will include instruction for a kill chain analysis of the recent Target Inc. breach as an example of the urgent need to adopt Trusted Identity and Privileged User Management. Finally, the attendee will be provided with recommendations for best practice in privileged user management for cloud and virtualized platforms and a recommendation for utilizing insider threat programs, NIST continuous monitoring and HSPD-12-ICAM as the framework for achieving least privilege and infrastructure integrity.

Wednesday, September 17th

3:40 p.m. - 5:00 p.m.

Case Study/Lessons Learned: Cross Sector Digital Identity Initiative (CSDII) Trust Framework

Prequalified for one CompTIA CEU: CASP and one GIAC CPE

Moderator:
Mike Farnsworth
Vice President
Binary Structures Corporation

Panelists:

Jennifer Behrens, MSW, Ph.D.
Vice President and Chief Operations Officer
Binary Structures Corporation

Joseph W. Grubbs, Ph.D.
Vice President and Chief Information Architect
Binary Structures Corporation

Making a vision a reality takes hard work from many different perspectives. In this session the panel will delve into the business, technical, legal, political, economic, and privacy related considerations that were put into the creation of a robust trust framework that is adoptable by both private and public sector organizations. The panel will share lessons learned, offer their perspectives on trust frameworks and their creation, and provide tools for attendees to incorporate into their own efforts.

Thursday, September 18th

9:00 a.m. - 10:40 p.m.

The Importance of Strong Identity, Credential, and Access Management Practices to Safeguard and Share Government Sensitive Data

Prequalified for one CompTIA CEU: Security+, Cloud+, and CASP and one GIAC CPE

Speaker:
Reid Carlisle
Director
SPYRUS, Inc.

The rapid evolution of high density, cost effective flash memory, its associated controllers, and complementary technologies including USB 3.0 compliant Windows-to-Go and LINUX based architectures has presented the mobile force with a confluence of features making a portable platform-independent user environment and “personal cloud” a demonstrable reality. Moreover, the personal cloud, which today can consist of up to ½ Terabyte or more of high performance SSD quality flash memory in a USB “stick” form factor, can be linked to “big data” in the “big cloud” to create a hybrid cloud architecture. The high performance localized storage and execution environment can not only provide a schema for personal "in-memory" data analytics, but facilitate the collaboration of a widely distributed user base without the requirement for persistent connectivity or reachback to a central site.

The convenience of a portable user environment has its own challenges, not the least of which are information security, particularly when gigabytes of highly confidential or sensitive data are stored in a mobile device. SPYRUS, Inc., will briefly describe some leading edge scenarios for information assurance in distributed computing applications, including merging biometric authentication with N-Factor authentication and hybrid cloud security. We will touch on the benefits and challenges of built in encryption mechanisms coupled with internal biometric authentication and secure signed templates. A robust authentication environment will also mitigate the challenges or security for authentication between personal datastores and the “back office” cloud. Additional leading edge concepts will include the use of the distributed environment for real time analytics tailored to particular operational scenarios, secure non-repudiable information sharing between members of today’s in transient, highly mobile workforce.

Thursday, September 18th

10:40 a.m. - 12:00 p.m.

Case Study/Lessons Learned: Noteworthy Risks of Not Using NIST-Compliant Solutions in Health IT

Prequalified for one CompTIA CEU: CASP and one GIAC CPE

Presenters:
John Odden
Co-founder and Director
Collaboration for Universal Health, Inc.

Dan Turissini
Executive Vice President and Chief Technology Officer
WidePoint Corporation

Whether for reasons of market advantage, funding limitations, or simply the long history of User ID/Password as the accepted "Identity Management Standard" across Health IT, many current practices fall short of presenting a fully federal vetted and compliant solution. Some stakeholders are voicing concerns that may augur for a rapid return to full Federal Bridge compliance as a necessary standard of practice. Attendees will learn:

- The importance of the Digital ID topic given the impact on health care providers and their need to practice with proper information privacy and security
- The rapidly developing expectations of patients and other stakeholders to avoid solving this issue with unique a silo'd solutions.
- An understanding of the feasibility of operating with fully Federal Bridge compliant solutions
- And, participate in an open, inclusive and effective dialog about the concerns, risks and costs of doing otherwise.