
# DEFENSE OF ACCOUNTS

## ADOPTION OF CYBERSECURITY TECHNOLOGY WORKSHOP 2016

### Protecting Critical Infrastructure and Accounts from Adversaries

**Sponsor: Arthur R. Friedman**
Program Director Strategic Mission Integration
Information Assurance Mission, NSA
arfried@nsa.gov

**Early Detection & Reaction**

**User Participation**

**Proactive Defense Construct**

**Multi-Factor Authentication & Dynamic Authorization**

**Identity, Device, and Environment**

**Dynamic Deception and Notification**

**Prevent Escalation & Lateral Movement**

**Sandia National Laboratories**
Albuquerque, NM

http://cps-vo.org/group/sos/act

## Overview

Defense of Accounts (DoA) addresses the protection of applications and data against adversaries who have compromised an account or credential. The assumption is that at some point in time an account or credential *will* be compromised, and therefore the next layer of defense is preventing escalation of privileges or lateral movement by the adversary.

DoA goes beyond standard Role or Attribute Based Access Control (RBAC & ABAC) by implementing Context Based Access Control (CBAC). CBAC moves beyond statically defined roles and attributes to enable access with unlimited virtual security overlays for resource access. In addition to CBAC, Defense of Accounts incorporates Multi-Factor Authentication (MFA), spearphishing defense, and real-time threat detection to provide a solid foundation for enhancing security.

## Defense of Accounts – History

Defense of Accounts is one of four use cases at the Adoption of Cybersecurity Technology (ACT) workshop, an invite-only event sponsored by the Special Cyber Operations Research and Engineering (SCORE) subcommittee. The intention of these use cases is to enhance the adoption of currently available technology solutions to address cyber issues affecting the Department of Defense (DoD) and civilian federal government. The ACT workshop is hosted and lead by representatives from the Department of Homeland Security (DHS), the National Security Agency (NSA), and Sandia National Laboratories. The ACT-2 workshop concludes in March 2017 with a full use case briefing and demo at Sandia to the full ACT-2 community.

## Early Detection and Reaction

The speed at which a compromised credential or account is identified is a major factor in controlling the amount of damage that can be inflicted by an adversary. Incorporating administrators into the process of defining digital access policy with CBAC greatly increases the capability to detect and restrict anomalous activity. DoA incorporates an automated feedback cycle to both users and system owners that can be modified, duplicated, and quickly (re)deployed to ensure the latest detection and preventive mechanisms are in place.

## User Participation

In order to facilitate early attempts to compromise credentials using malicious email, the user is provided with Identification, Friend or Foe (IFF) email visual discriminators. Simply stated, authentic emails are shown with a "Trust Indicator" icon. Emails without this "Trust Indicator" quickly tell the user that investigation is warranted on what is a potential spearphishing attack.

The wide variability of individual users and individuals' usage patterns makes it difficult for analytics to distinguish normal variations in activity from unauthorized activity over short periods of time. In order to help disambiguate abnormal access indications, the user's knowledge of one's own activities is leveraged by providing the user with audit reports and reporting tools.

## Proactive Defense Construct

As DoA is a foundational solution to cyber defense, additional security solutions form layers in the overall security stack. Integration, not replacement, is a key feature of DoA. Enabling early detection and defensive reaction provides the ability to govern the rules/parameters for digital policy access.

DoA is not a static, but an evolving solution which expands as security or mission requirements are identified or refined. Any available attributes possessed by an account holder can be used to grant or deny access, and any available attribute can be monitored to detect activity outside normal parameters. The ability to see a holistic view of activity highlights abnormal access patterns that can be further investigated.

## Multi-Factor Authentication and Dynamic Authorization

Strong authentication can be achieved using MFA with any combination of hard tokens, soft tokens, OTP, and of course PIV/CAC cards. The challenge is often determining *which* set of MFA options makes the most sense for any one environment. For DoA, a hard token that supports the PIV/CAC data model in a USB form

factor along with support for OTP, U2F, and optionally NFC proved the best MFA credential. This hard token provides an excellent alternative for environments where PIV/CAC cannot meet the needs of the user population.

The challenge of *which* MFA solution to apply is resolved by the use of CBAC. This allows for an environment to select MFA options that meet its security profile, while not impacting other environments. Each environment has its own virtual security profile, consisting of MFA options plus user identity and attributes to determine appropriate authorization. Virtualizing these profiles means that changes can be made quickly – allowing for a truly dynamic authentication and authorization policy. As security needs change, so can the virtual security profiles that overlay environments.

## Identity, Device, and Environment

Expanding the richness to DoA is the ability to incorporate information about identities from associated devices and environments. User location, device, threat conditions, and sensitivity attributes can all be leveraged for access and reporting. DoA incorporates additional sources of information without custom development.

## Dynamic Deception & Notification

Dynamic deception technology creates a distributed decoy system to lure in attackers. Once attackers engage with the Defense of Accounts solution, infected endpoints are immediately identified and the notification process begins. To understand the intent of the attack, a port can also be opened to connect to the hacker's command and control (C&C) to collect additional information. Notification of such an attack can be done on multiple levels, from dashboard alerts for security admins to individual notification that their workstations are potentially part of an abusive attack.

## Goal: Prevent Escalation and Lateral Movement

A compromised account provides a pathway for an attacker to escalate privileges and move laterally movement. Detecting such a compromise is crucial to resource protection. With Defense of Accounts, outliers in account activity can be detected through monitored attributes, such as access location, physical access control usage, GPS coordinates, or even time of day, to determine if further investigation is necessary.

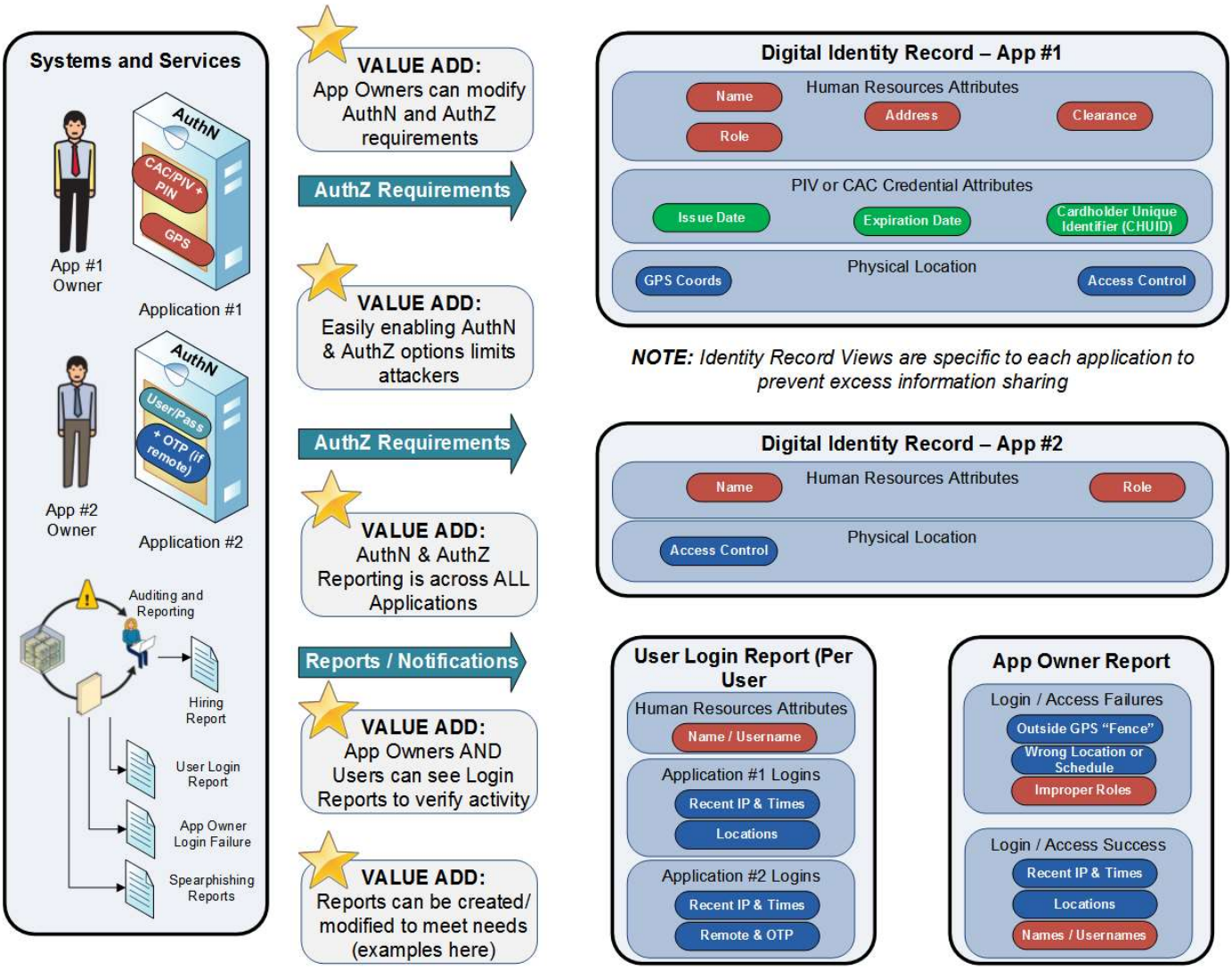
Initial protection of accounts can be provided by disrupting email-based attacks (e.g. spearphishing) and by making multi-factor authentication practical to implement for both individuals and administrators. This creates a larger hurdle to overcome for attackers and eliminates the "low-hanging fruit" which is the cause of many compromised accounts. For accounts compromised by other means, detection mechanisms are established to act as sinks for malicious activity. Such activity is detected with zero false-positive alerts and therefore provides notifications of high-value and include extensive forensic data. Dummy user accounts can also be created to assist in detection of lateral movement and escalation.

Detection with analytic toolsets and reporting mechanisms provides end-users and administrators the ability to contribute to the process. Both machine and human analysis together is an effective tool to identify compromised accounts, which can be immediately revoked to disable access.

## *Defense of Accounts - Solution Benefits:*

- **Virtualization of identity/attribute contexts**
- **Spearphishing defense & reporting**
- **Practical MFA tokens alongside PIV/CAC**
- **Reporting and analytics in near-realtime**
- **Detection of adversary attacks on resources**
- **Modular deployment and integration**

## Solution Architecture: Use Case Overview




## Defense of Accounts: Solution Partners

# Defense of Accounts - Pilot Description

For a functional pilot, Defense of Accounts will showcase the interaction of users, strong authentication, dynamic authorization, and a reporting/auditing framework. This pilot represents a foundational infrastructure that can be expanded to include any number of users, devices, attributes, applications, and reports. This flexibility and scalability is paramount to the Defense of Accounts use case, and is a key differentiator from existing solutions available today.

## Milestone 1 - Infrastructure

The first major milestone for the pilot is to build the initial user identity, user participation, and attribute store for a small set of individuals and associated attributes, and a set of sample applications that can leverage any of the available attributes to make authorization decisions after a successful authentication. This beginning framework of identities, attributes, and applications will then be incorporated into a set of real-time reports that can be shown on a set of configurable dashboards or alerts.

This completes the initial infrastructure framework and shows the full lifecycle of identity, authentication, authorization, and feedback.

## Milestone 2 – Strong Authentication & Dynamic Authorization

With the initial infrastructure in place, the need to provide System/Data Owners with an increased set of strong authentication and authorization tools is the next milestone. A selection of available authentication factors for applications will be provided to an Application/Data Owner, such as username/password, OTP, and Smart Card/PIN. Owners can cross-map these factors in combination with identity attributes to determine what Authentication and Authorization parameters are necessary to access an application and what data is accessible.

A crucial differentiator at this stage versus other solutions is the ability for a System/Data Owner to define multiple cross-mappings of authentication factors and authorization parameters. This means, for example, a “high” side and a “low” side cross-map can be used simultaneously. Initially a small set of cross-mappings will be used for demonstration, but it is important to note that the Defense of Accounts framework has no limitation on the final number defined and utilized.

## Milestone 3 – Activity Simulation and Reporting

To demonstrate the full capability of the infrastructure, activity generation tools will be used to simulate user creation, attribute definition, user participation, and application/data access. These events and actions will be used to generate reports and alerts that would be seen by end-users and application/data owners, such as anomalous access attempts, monitored attribute notifications, incongruous emails, and related reports that would be representative of real-life scenarios that could detect adversary actions.

These reports and alerts are intended to provide the feedback back into the environment as to what additional actions must be taken to secure the environment. Actions such as revoking a credential, flagging a suspect account, or increasing the attributes of identities being monitored are all valid and expected to meet operational needs. The actions can be unique to every application and authentication/authorization cross-map to ensure that the best possible security solution is found.

## Milestone 4 – Expansion and Usability Refinement

As the core infrastructure and functions are developed and deployed, the final milestone is to ensure that expansion of the solution is feasible. This means that as the number of identities, credentials, applications, and reports grows performance is maintained across the framework. Additionally, usability of the solution must be maintained so that end-users are capable of identifying and implementing necessary changes quickly and predictably from within the framework that improve the security of both applications and accounts.