Authorization, Authentication and Audit—

AAA Technology Support

for

“Communities of Trust”

ISCRAM 2008

Communities of Trust

- Crisis response and management can be supported by information sharing within Internet-based “Communities of Trust”, which *link people and information for better decision making*, in a trusted network environment.
- Authorization, Authentication and Audit (AAA) are the technology cornerstones needed to create a trusted environment.

Communities of Trust (CoT)

- People with a common concern or interest, or who need to share information.
- Often in heterogeneous organizations, e.g.:
  - Government agencies, NGOs, private organizations all need to communicate in a crisis
  - Hurricane example: FEMA, local authorities, Red Cross, National Guard, big-box retailers, industries that can contribute needed goods, personnel or capabilities (e.g. WalMart, Home Depot)
  - Other examples: Cross-agency team of port security stakeholders; regional public safety authorities and private critical infrastructure security managers, etc.

Internet Communications for CoT

- Reach stakeholder CoT members with authenticated information, notifications and alerts quickly, *automatically.*
- Multi-media; video, audio, maps, text, etc.
- Aggregate information for analysis; deliver common operating picture.
- Segment data to a fine-grained level:
  - Segment by community
  - Segment within communities; discrete information can be delivered to certain members of a community and blocked from others, based on rules applied by information owner
  - Segment and protect personally identifiable information (PII) for privacy policy compliance.

CoT Members Must Trust the Environment Before They Will Share Information

- Swan Island has been evolving a new trust model for sharing sensitive information across organizations, especially for emergency, security and operational continuity management.
- This model's first principle is: Focus on letting only "known good guys" in, rather than on just keeping "unknown bad guys" out.
- By creating high-assurance environments that (unlike email and Web portals, for example) are dedicated to particular mission-critical operations, and which inspire high levels of trust and confidence among participants, new forms of information sharing and cross-organizational "mash ups" can sprout and grow.

Lessons Learned, 1

- Security systems should be *as simple as possible, but no simpler*. The balance is between trust and security, on one hand, and ease-of-use on the other. Both must be achieved for trusted computing systems to be effective.
- *Close the open window first*. In cyber security circles, this is known as the "Hundredth Window" principle. If you have a mansion with 100 doors and windows, with one of them wide open, what's the point of adding more bars, chains and locks to the other 99? Better to locate the open window, and work on securing it first.

Lessons Learned, 2

- *Deliver needles, not haystacks*. Too much information can be as bad as too little.
- *Not merely a network of networks, but a community of trusted communities.* It's easy to overlook critical cultural, political and basic human elements of a trust environment—the qualities that bind communities in the real world.
  - The most successful online communities will increasingly learn how to emulate the best features of real-world communities.

How Authorization, Authentication and Audit (AAA) Fits In

- The goal of our security model is to create *trust*: the ability to reasonably and reliably predict how the system—and the humans in it—will behave. Policies and rules established in the system are enforced throughout to support this.
- System behavior is the result of thousands of individual transactions: Web service-to-Web service; server-to-server; network-to-human; and human-to-human, etc. The key to making these transactions *trusted* is for each side to be able to authenticate, and ultimately depend upon, the other.
- Authorization, Authentication and Audit (AAA) elements function together to—
  - create a comprehensive trust framework
  - provide a contextually appropriate level of
    - information assurance
    - data protection
    - dissemination control

Authorization, 1

- Establish a Community of Trust Champion—a leader who sets the rules for community membership, and determines who can join. Champions should be highly trustworthy people in positions of some authority, passionate about their particular mission and well-connected.
- Champions set authorization policies and manage usage rights for members, such as what information sources they can view.
- Ways a Champion can add members:
  - Leverage association or group membership ranks, or personal contacts.
  - Establish a set of membership guidelines and policies, and have others apply these guidelines.
    - Example: A federal intelligence agency set up membership guidelines for port security stakeholders at the state/local level across America, and Swan Island identified, recruited and signed up appropriate local subscribers.

Authorization, 2

- Community membership is the single attribute in the run-time environment determining access to the network and information.
- Subscriber attributes such as job, location, security level and various credentials are managed by Champions rather than being part of a system-wide profile vetted for each user in each session. This reduces system complexity, increases the speed of access processes, and generates greater system flexibility.
- The net effect of the authorization system is to create an interlocking network of communities that consist of members trusted by that community's Champion.

Authentication

- Once a A CoT member is authorized to connect to the trusted environment, the system must authenticate this subscriber in each online session.
- Multi-factor authentication: Software tokens are downloaded as part of the sign up process. These tokens then function as the "something you have" factor in a multi-factor authentication model. Thus, a particular user account can be accessed only from machines that have appropriate tokens.
- In the case of browser access to the trusted environment, a "strong passphrase" model of authentication is recommended. While not as strong as a multi-factor approach, strong passphrase does provide greater security than normal user-name/password schemes.

Audit

- All system activity involving a member's access to the trusted system is captured in a set of system logs. These logs can be used to generate highly detailed reports, based on a particular member's activity, a particular content feed's usage, or overall community behavior.
- These logs become a "trusted third party" record of system events—including chronologies of incident notifications and response.
- Immutable audit logs are best – nobody can change, only add correcting transactions.

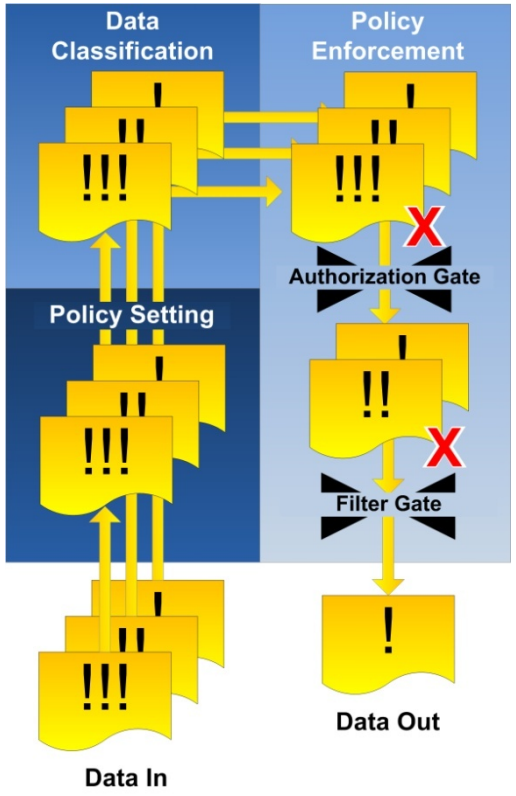
Additional Access Control Features, 1

- **Locked Community Dashboards.** A Champion configures the dashboard (selects information sources, filtering attributes, etc.) and distributes it to all the members of the Champion's community, exactly as he/she has constructed it. Locked dashboards cannot be altered by members.
- **User-Configurable Dashboards.** This kind of dashboard is entirely configurable by individual members, allowing them to fully customize the dashboard's operational picture to fit his/her job or interests.
- **Hybrid Dashboards** are Locked Dashboards that can be supplemented with configurable elements, while the core locked elements remain unalterable.

Additional Access Control Features, 2

The Double-Gated Targeting™ system makes it possible for both providers and consumers of information to share information, across organizations, under system-wide rules.

- Think of a water reservoir with secure pipes going to a number of local farms. The reservoir (the content source) has a gate at the head of each pipe, and each farm has another gate at the point the pipe enters the farm. For water to flow from the reservoir into the fields of each farm, both gates need to be open.
- The Authorization Gate (at the information reservoir) is controlled by the content source. This source can set various policies about eligibility to receive its information—and these policies result in the opening or close of the Authorization Gate for each particular farm (i.e., member).
- Each member also controls a unique gate, known as the Filtering Gate. The member sets personal policies (using filtering attributes such as incident location, information type, severity level, etc.) that determine whether his/her Filtering Gate is open to receive each kind of available information.
- Between these two gates, all information is encrypted using standard SSL technology, in order to ensure safe transport.



Additional Access Control Features, 3

- Individuals can be members of multiple communities, yet view information from all communities on a single set of integrated dashboards. Participation in each community is managed through AAA controls.
- The highest purpose of the information controls, somewhat paradoxically, is to increase information sharing—both within and across organizations.

TIES: High Level Overview

Demonstration – Trusted Information Exchange Model

www.swanisland.net

Questions?

Pete O'Dell

Swan Island Networks

pete.odell@swanisland.net

Office: 703-519-0188 | Cell: 202-460-9207

ISCRAM 2008