

Event Notification for Homeland Security

Phillip J. Windley
phil@windley.com



Emergency Broadcast System

- Emergency Broadcast System
 - ◆ Effective
 - ◆ Crude
- Homeland security needs a national network to serve as an EBS network outside traditional media.
- Internet offers no owners to impose burden upon.

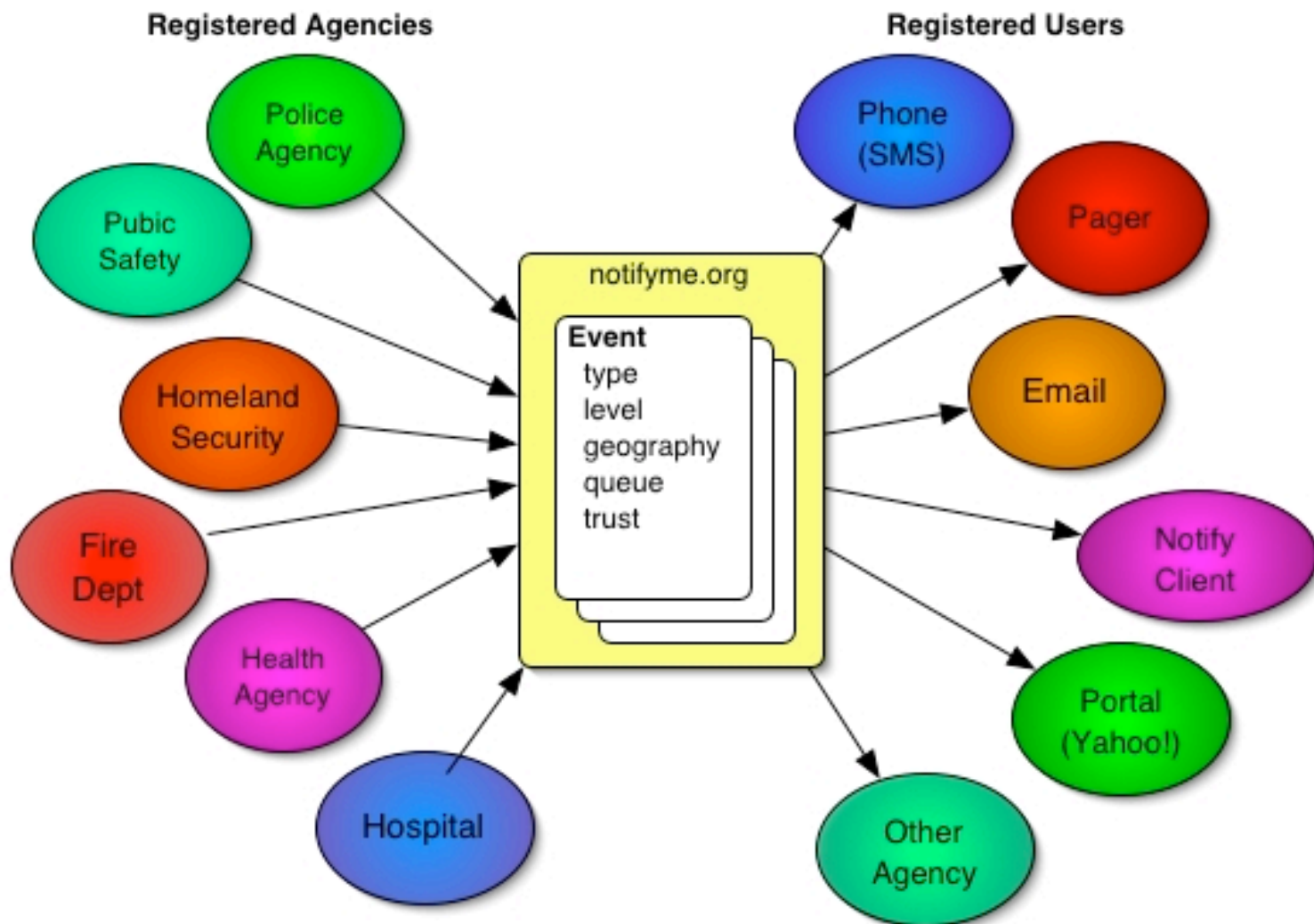
Part I: Uses of Event Network

- An emergency broadcast system for the 21st century.
 - ◆ Homeland security alerts
 - ◆ Amber alerts
 - ◆ Severe weather alerts
 - ◆ Traffic alerts
 - ◆ Health alerts
 - ◆ Air quality alerts
 - ◆ Sharing information among public safety agencies.

Alerts

- Type of alert
- Level of urgency
- Geography
 - ◆ Zip code
 - ◆ Political boundaries
 - ◆ Latitude/longitude with radius
 - ◆ Defined using GIS tool
- Trust based on insertion
- Targeted
- Issuing agency
- Defined using industry standards

Logical Architecture



Targeted Alerts

- Target by
 - ◆ Geography
 - ◆ Occupation or skills
 - ◆ Memberships
 - ◆ Assets
 - ◆ Specific situations
 - E.g. Asthma sufferers
- Multiple profiles
 - ◆ Home
 - ◆ Work
 - ◆ Vacation property
 - ◆ Schools
- Managed Groups
 - ◆ E.g Families, employee groups, etc.
 - ◆ Managed with a single profile
 - ◆ Emergency workers and first responders

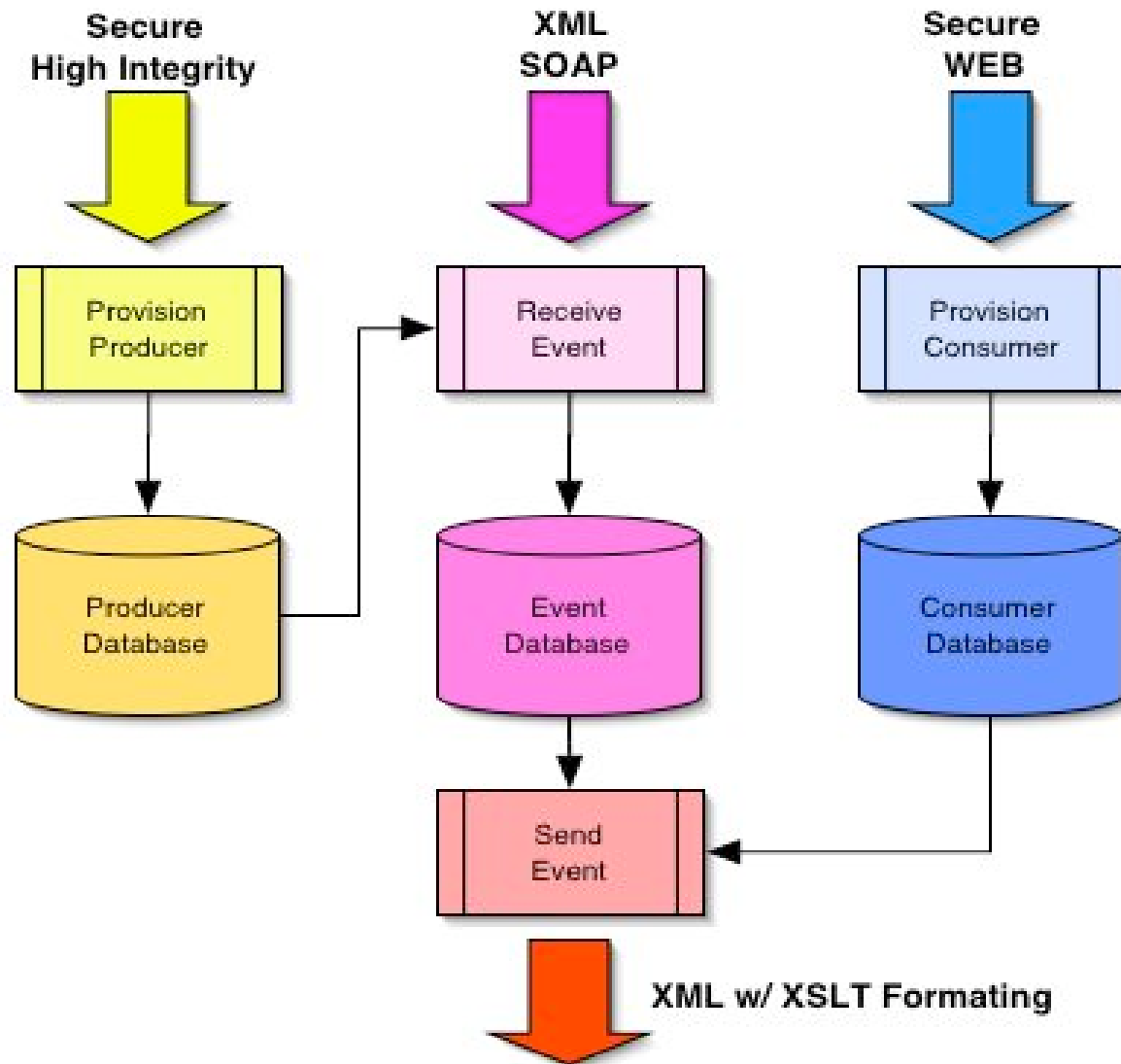
Types of Alerts

- Actionable
- Informative
- Safety
- Health
- Property damage

XML Standards

- Common Alerting Protocol - standard method to collect and relay instantaneously and automatically all types of hazard warnings.
- Emergency XML - an open XML-based standard for emergency management data exchange.
- These are not yet fully baked.

Process Architecture



Provisioning Producers

- High integrity process vets producer
 - ◆ Similar to PKI checks by certificate authorities
 - ◆ Multiple tests
- Multiple levels of trust
 - ◆ No authentication
 - ◆ UID/Password
 - ◆ Digital signature
 - ◆ Collaborated/Approved

Provisioning Consumers

- Web page based, free-form sign-up.
- Chooses how to receive notifications
- Chooses conditions:
 - ◆ Geography
 - ◆ Trust
 - ◆ Level
 - ◆ Type
 - ◆ Agency
 - ◆ Etc.
- Multiple profiles allowed

Alert Insertion

- Multiple insertion methods
 - ◆ Web form based
 - ◆ Polling by URL over HTTPS
 - ◆ SOAP-based insertion
- XML event format fixed
- Trust level varied by insertion mechanism and authentication requirements

Alert Broadcast

- Alerts are produced in XML
- Device independent: multiple formats produced through XSLT translation
- Filtered by
 - ◆ Type
 - ◆ Level
 - ◆ Geography
 - ◆ Trust

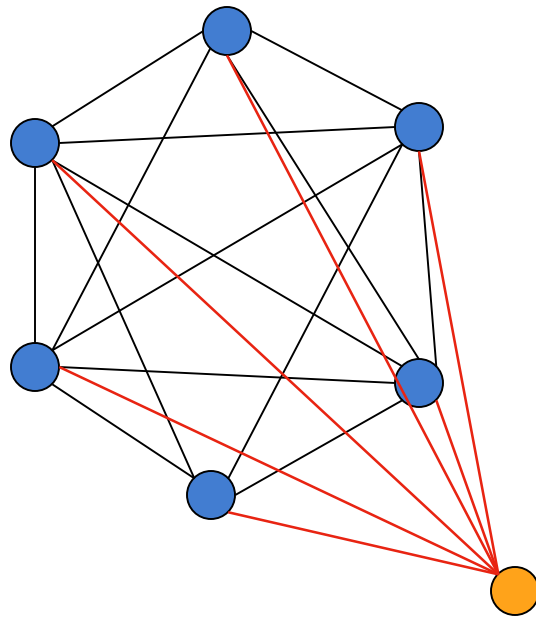
Security Issues

- Properly authenticate alert producers
- Securely retrieve and process alerts
- Reliable delivery
- Physical security
- Network security
- System reliability and guarantees
- Background checks of all employees
- Self replicating architecture ensures message/alert integrity

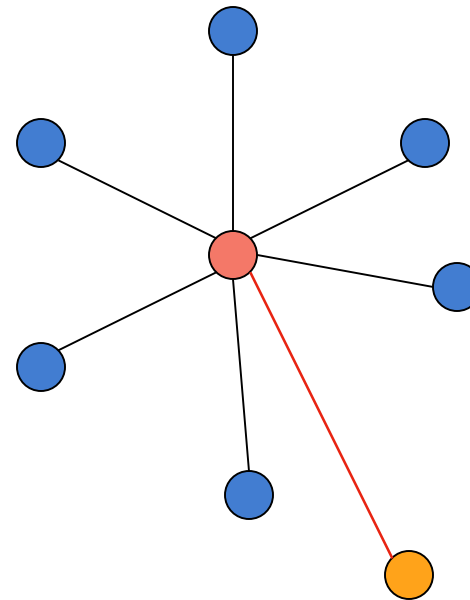
Part II: Event Broker

- Exchanging events between public safety related agencies
- Key piece of national homeland security infrastructure
- Who will build it?
- The infrastructure necessary to build the alert system gives you an message broker for free.

Need for a Broker



Without Broker:
 N^2 connections



With Broker:
 N connections

Value-Added Network

- Built for SOAP/XML messages
- Message store and forward
- Identification, Authentication, and Authorization
- Logging
- Audit trails
- Event and message filtering
- Possibility to do traffic analysis

Event Network

- Reliable
- Guaranteed (certain transactions)
 - ◆ One and only one notification
- Secure

Existing HS Related Networks

- RISS
 - ◆ Regional Information Sharing Program
 - ◆ used for exchanging information about drug trafficking, gang activity and violent crime
 - ◆ Federally funded non-profit
- Matrix – used for exchanging general public safety intelligence
- Neither currently being used for purposes outlined here

Business Model I

- Run as Non-Profit
- Event insertion is a free, public service
- Personal subscriptions to event notification are free
- Supported by donations and grants

Business Model II

- Operate for profit
- Event insertion is still a free, public service
- Personal subscriptions to event notification are still free
- But, charge for:
 - ◆ Commercial subscriptions
 - ◆ Commercial notifications
 - ◆ P2P notification and special queues
 - Warrants
 - Arrests
 - Guaranteed communications

Business Model III

- Alternate ideas:
 - ◆ Member owned network?
 - ◆ Privately owned network with member affiliate on a board?

Demo

- Producer and consumer registries in OpenLDAP
- Event store in MySQL
- Messaging system from jBOSS?
- jBOSS for middleware
- Functionality
 - ◆ Accept and store event via SOAP and web
 - ◆ Queue XML event and demo translation
 - ◆ Process queue based on consumer profiles and translate to multiple formats

Notes

- RISS
- Matrix
- E911 data
- Voice XML
- Randy Fisher/Roland Squires