REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
APRIL 2008	Conference Paper Postprint	April 2008 – April 2009

4. TITLE AND SUBTITLE
SECURE WIRELESS KNOWLEDGE MANAGEMENT FOR INTELLIGENCE ANALYSIS

5a. CONTRACT NUMBER
FA8750-08-C-0107

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
65502F

6. AUTHOR(S)
Catherine H. Clark, John Spina, and Michael Corey

5d. PROJECT NUMBER
08SB

5e. TASK NUMBER
IR

5f. WORK UNIT NUMBER
35

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Vision Systems and Technology, Inc.
6021 University Boulevard
Ellicott City, MD 21043-6077

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFRL/RIEH
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TP-2009-47

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release; distribution unlimited PA# WPAFB-2008-1023 Date Cleared: 14-March-2008

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Although more information than ever before is available to support the intelligence analyst, the vast proliferation of types of data, devices, and protocols makes it increasingly difficult to ensure that the right information is received by the right people at the right time. Analysts struggle to balance information overload and an information vacuum depending on their location and available equipment. The ability to securely manage and deliver critical knowledge and actionable intelligence to the analyst regardless of device configuration, classification level or location in a reliable manner would provide the analyst 24/7 access to useable information. There are several important components to an intuitive system that can provide timely information in a user-preferred manner. Two of these components: information presentation based on the user's preference and requirements and the identification of solutions to the problem of secure information delivery across multiple security levels will be discussed in this paper.

15. SUBJECT TERMS
Information Delivery, Wireless Devices, Mobile Proxy

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			John Spina
U	U	U	UU	10	19b. TELEPHONE NUMBER (*Include area code*) N/A

Secure Wireless Knowledge Management for Intelligence Analysis

***Catherine H. Clark**, Vision Systems & Technology, Inc.*
***John Spina**, Air Force Research Laboratory*
***Michael Corey**, Air Force Research Laboratory*

***Abstract** - Although more information than ever before is available to support the intelligence analyst, the vast proliferation of types of data, devices, and protocols makes it increasingly difficult to ensure that the right information is received by the right people at the right time. Analysts can rapidly shift between information overload and an information vacuum depending on their location and available equipment. The ability to securely manage and deliver critical knowledge and actionable intelligence to the analyst regardless of device configuration (bandwidth, processing speed, etc.), classification level or location in a reliable manner, would provide the analyst 24/7 access to useable information. There are several important components to an intuitive system that can provide timely information in a user-preferred manner. Two of these components: formatting information to accommodate the user's profiles and the identification of solutions to the problem of secure information delivery across multiple security levels, will be discussed in this paper.*

1-Introduction

The Intelligence Community (IC) requires a secure method to provide information in many formats (text, images, video, etc.) to multiple users, using multiple devices (cell phones, Personal Digital Assistants (PDA), computers, etc.) over wireless and wired communications channels with varied bandwidths. One approach to meeting these requirements is to provide an innovative, domain-independent solution that is easily deployed and managed, extensible, will provide both push and pull of the information and/or notifications, and automatically modified in accordance with security requirements and the physical limitations of users' devices and connections. Information dissemination and management is device, connection, and protocol dependent. The currently available devices vary widely in size, hardware and software capabilities, and connection types. The modern analyst requires unified and secure methods to deliver and manage critical information flow that accommodate multiple devices, connections, and protocols; in addition, the system must be able to accommodate new devices rapidly and efficiently. The main concept that this paper explores is the development of an extensible, standards-based software application that can distribute secure, content-filtered information in differing formats to a wide variety of mobile devices, with a variety of connection bandwidths. In simple terms, the objective is to get the right information to the right people at the right time regardless of their device and location.

A difficult issue associated with implementing a system that leverages small hand-held devices is the ability to automatically massage the data being sent so that the device can receive and display the information in an intelligible format. For example, if an e-mail containing several image attachments is sent to a user utilizing a device that is incapable of displaying images, then bandwidth should not be wasted sending large image files.

The user should instead receives a textual description or metadata of the image. While capabilities and hardware profiles can vary tremendously across hand-held devices, users should not have to resolve these differences. An information dissemination platform must have an automatic, yet user-configurable, mechanism that supports adding new devices, specifying device capabilities, and defining of data transformation rules. The system must have built-in intelligence as to ensure that the user has access to critical information regardless of her profile. For purposes of this paper, the user's profile describes all of the various attributes of the user's device's capabilities (i.e. device, bandwidth, security clearances, and other limitations). Although more information than ever before is available to support decision making, the vast proliferation of types of data, devices and protocols makes it increasingly difficult to ensure that the right information is received by the right people at the right time. Too much information, not enough information, or information that is not properly formatted, can make decision-making more difficult.

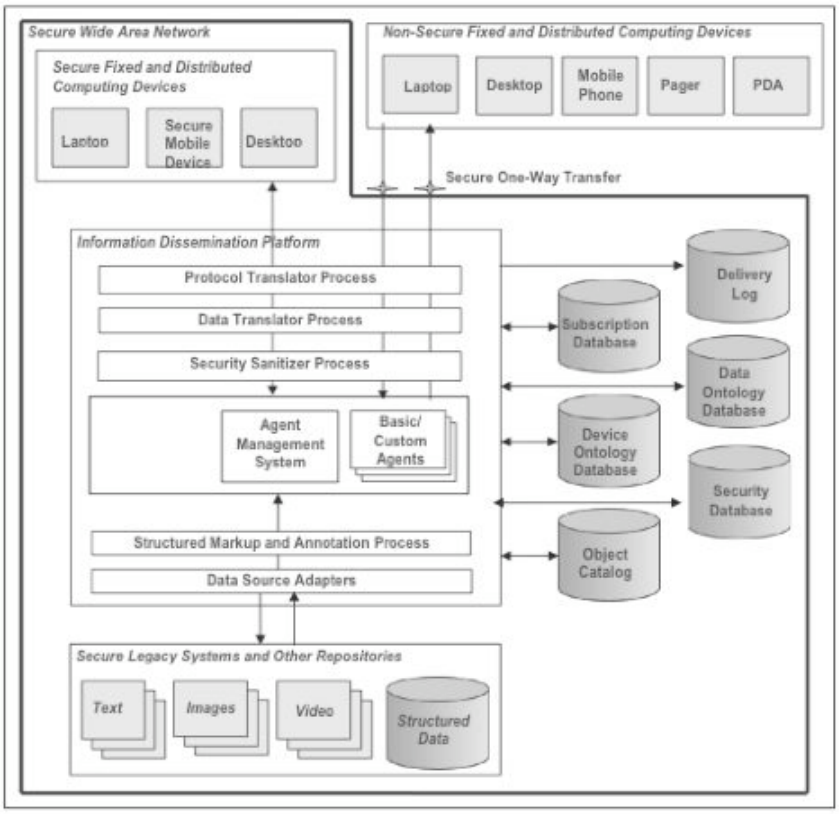

Figure 1: High-Level Architecture of the Information Dissemination Platform

2-Describing a User's Profile

Device, data and service provider descriptions are a vital part of an information dissemination platform. In order to optimize the delivery of information, characteristics of the user's environment must be captured. Is the user sitting at a high end desktop

computer in an office with a T1 internet capability or is the user traveling in a car with a cell phone? While that example offers the two extremes, several other scenarios in between are likely to occur. A system that can map the user's profile in order to determine the most user-preferred delivery method requires several databases or ontologies to perform. Aside from determining the optimal delivery method, the system might also consider allowing user-defined thresholds that weigh speed verses information quality. In other words, for a particular piece of information is it more important to get that information as fast as possible, regardless of the quality of the information, or take longer to push to the user, but provide a more complete information product? Where is that line and how do you approach the convergence of the right speed and ideal information? While exploring this concept is beyond the essence of this paper, it is important to build the foundation of the user's profile, particularly the device, data and connection descriptions.

As the convergence of telecommunications and computers has matured, there have been significant advancements. The pace of this convergence is only accelerating as new devices and technologies become available. Traditional computing depends heavily upon many known factors – known devices (e.g., workstations), known locations (e.g., desks in an office) and known capabilities (e.g., consistent network bandwidths and common software applications). The traditional computing environment has a relatively homogeneous infrastructure and very little thought needs to be given to the capabilities or availability of devices on the network. In contrast to traditional computing environments, the rapid evolution of the telecommunication, wireless, and mobile computing environments and the wide variety of available devices and protocols has created a very heterogeneous environment. This new environment has eliminated most of the known factors that were relied upon in traditional computing. A new type of computing infrastructure is needed to support this distributed, mobile computing paradigm. One of the more promising approaches for supporting this new type of computing infrastructure is the use of a distributed and mobile computing environment and the use of event-driven messaging systems that utilize a publish and subscribe paradigm [1]. Under this model, object interactions (e.g., the arrival of a new intelligence report, a user request for information, inventory stocks falling below a threshold) are treated as events and users identify the events in which they are interested. When an event of interest occurs, information about the event can be pushed to the user as an alert or added to an information queue to be downloaded when the user is online, based on the user's preferences and her device capabilities.

2.1-Device Ontology Database

One approach to managing the push and pull of information to a wide variety of smart devices is a device ontology. A device ontology is a database that contains the format, security, and protocol information about the devices that would be available to the system. The device ontology maps the specific protocols and requirements for a device to a common schema so intelligence products can be automatically reformatted,

reconfigured, and encoded in accordance with the device specifications. Smart mobile devices enable the opportunity for a user to leverage rapid information dissemination. They allow for the right information to be distributed to the right individuals at the right time. Unfortunately, devices operate in a heterogeneous environment. Manufacturers offer a wide array of devices to users with a vast set of features and capabilities. This creates a great strain on disseminating information. While simply distributing the lowest common denominator offers a solution to this problem, it is not an optimal one. Devices capable of receiving enhanced forms of media should receive the most comprehensive information object possible. While this information object could simply be a text message, it should extend to a video feed or similar means of multimedia providing the most relevant information whenever possible.

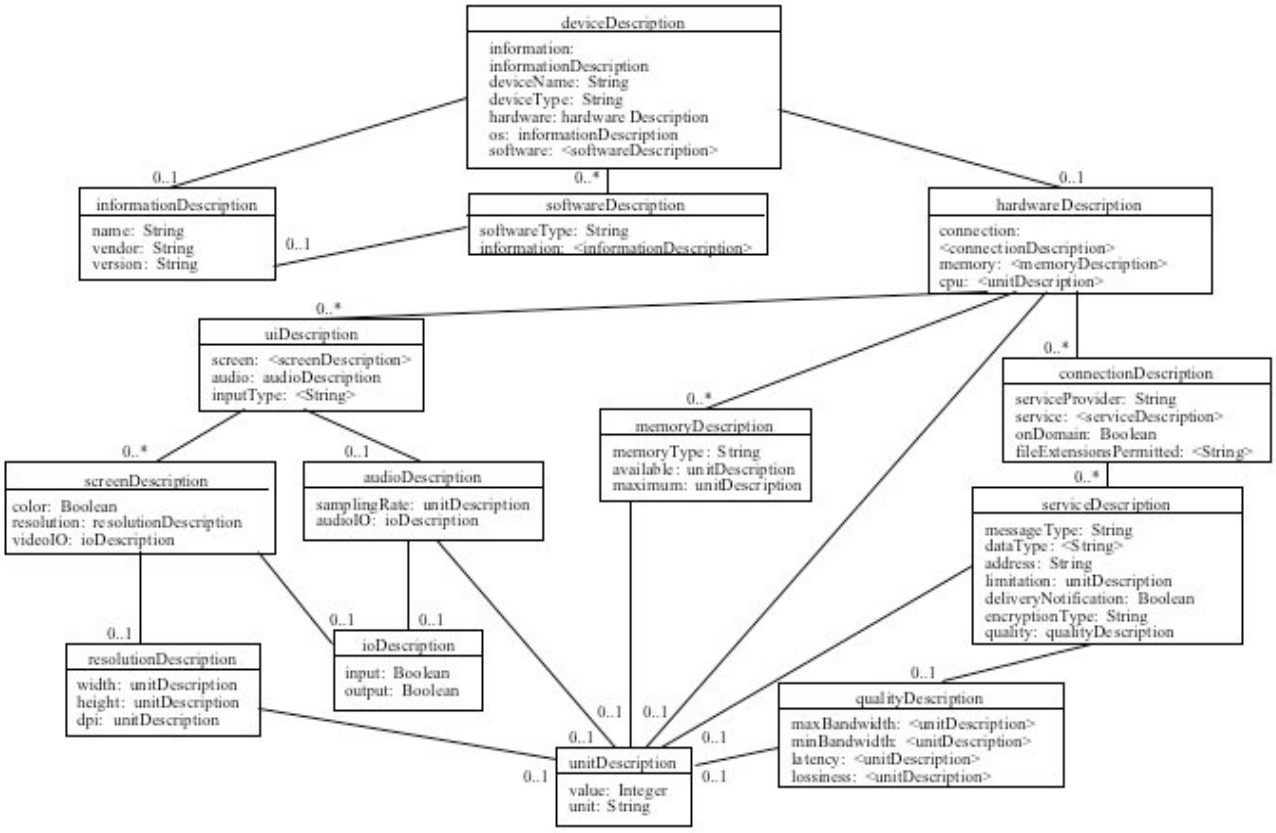

Figure 2: Example Device Ontology

2.2-Enhancing the Device Ontology

An ontology that has become somewhat of a standard is the Foundation for Intelligent Physical Agents (FIPA) device ontology. The FIPA device ontology addresses the problem of heterogeneous devices by providing a database of the specifications and capabilities of devices. This device ontology is a catalog of currently released mobile devices. It provides capabilities of many important areas of mobile devices. On the

hardware side, the device ontology contains slots for connection, memory and the user interface. Additionally, the device ontology addresses software versions briefly. While this ontology provides for basic dissemination, it can be improved upon for advanced reasoning in deciding what information can be delivered to a device. Proper extension allows for greater reasoning capability and flexibility. Specifically, a hardware description can be extended to better explain a devices reasoning capability. Additionally, multiple slots can be extended and better incorporated into the ontology through transitivity to allow for more generalized reasoning. [3]

It is envisioned that enhancements to the FIPA model will allow for advanced reasoning about a device's capability to both receive and transmit audio. This will prevent a device from unnecessarily sending a higher fidelity item than is necessary for an intended destination device. The hardware description is extended by adding slots for audio and video. Currently FIPA's device ontology only supports Boolean values for determining whether or not a device accepts input and output. This is simply not sufficient for a device that will publish information. The audioDescription frame will satisfy an audioInput and audioOutput slot of the uiDescription. Audio description has a value for sampling rate, buffer, and formats. Sampling rate will be a frequency value. Buffer represents the available time for recording. Finally, format is a one to many slot allowing for someone to define the formats the device can record or play (depending on whether the audioDescription instance satisfies the input or output slot). The videoDescription frame will satisfy two new slots under ui-description for videoInput and videoOutput. This frame is implemented similar to the audioDescription. Slots in this frame include format, an integer fps, and input and output audioDescriptions in case the audio cannot record with the same fidelity if the video is recording.

In its current form, FIPA's device ontology handles units poorly. It does not provide the flexibility or resources to state that two unit values are equivalent. The FIPA model can be improved by developing a unit frame with a literal, base unit, and multiple off the base unit. A unit frame can be sub-classed into similar appropriate units of measurement through a transitive subclassOf relationship. (e.g. FrequencyUnits, DistanceUnits, MemoryUnits). A description will now refer to a unit of measurement, by a value and an instance of a unit or subclass. This join is represented by the unitDescription frame. These additional capabilities will allow a user to extend an ontology to require specific types of units to satisfy a value. The value can then be reasoned over as described previously to allow comparison of values as well as calculations of requirements.

2.3-Data Ontology Database

The data ontology database contains the format and protocol information about all data used in this system. The data ontology maps fields, metadata, and other information describing the contents of the data to a common schema so individual components of the data can be extracted as necessary. This component allows only a subset of the original data fields to be sent to the device and avoids overwhelming devices that have limited

capabilities. Used in conjunction with the device ontology, the data ontology is a critical component in determining how the present the information to the user.

3-Information delivery across multiple security levels

Another main focus of this technology is the ability to navigate through different security levels. In order to handle varying security levels in an open environment, considering almost all mobile devices communicate on a non-secure network, the implementation of a secure one-way transfer capability is necessary. This will allow messages to be sent from a "high-security" network to a "low-security" network, and vice versa. As part of the system, a security database is required to store the user's security information as well as a security sanitizer process. In addition to incorporating a secure mobile device, several aspects of the application program should have the ability to communicate with several devices, and be able to send several different types of data. The system must be robust and flexible in order to work in many different scenarios. Incorporate multi-level security, will enable users to see only data that is within their security clearance level. Users that have access to a secure mobile device (e.g. SME-PED) will be able to send and receive secure transmissions in the field. Users who have non-secure devices will receive a filtered version of the secure message. This capability is extremely useful for the Intelligence Community, military and/or DoD organizations that inherently require access to multi-level security information, but still must get data to users in a timely manner.

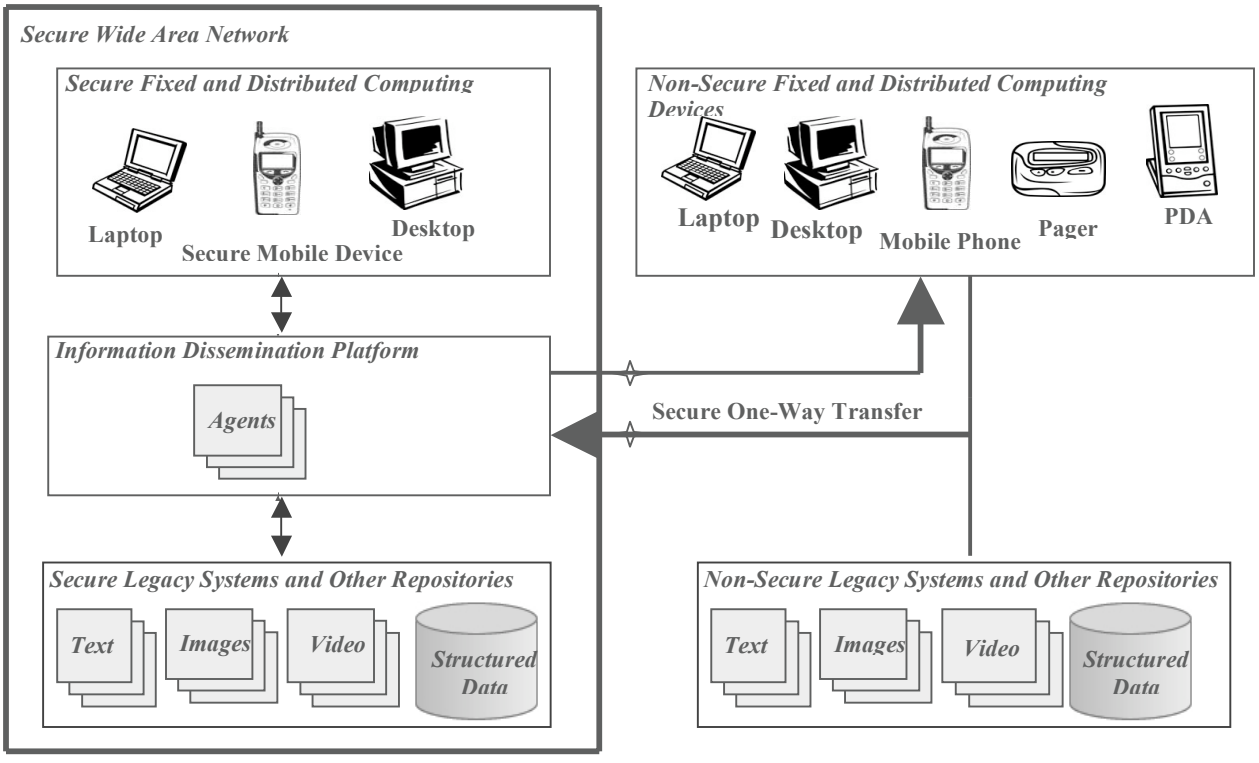

Figure 3: High-Level Architecture of a Secure System

The idea is to ensure that the system works in secure environments that have multi-level security associated with classified data, such as any of the agencies in the Intelligence Community (IC). It is essential that the system incorporate the ability to move across security domain both low to high and high back down to low. An ideal application would facilitate a one-way transfer across security domains, allowing email, web site content, and other open source information to be passed into secure networks. This allows for a one-way transfer of non-secure data to secure internal domains. The Low-to-High capability is currently being used in the IC and has been accredited at Protection Level 4. The Directory File Transfer System has been accredited at Evaluation Assurance Level 4. The significance of moving data from the "high" side to the "low" side may be more of a policy issue than a technical issue.

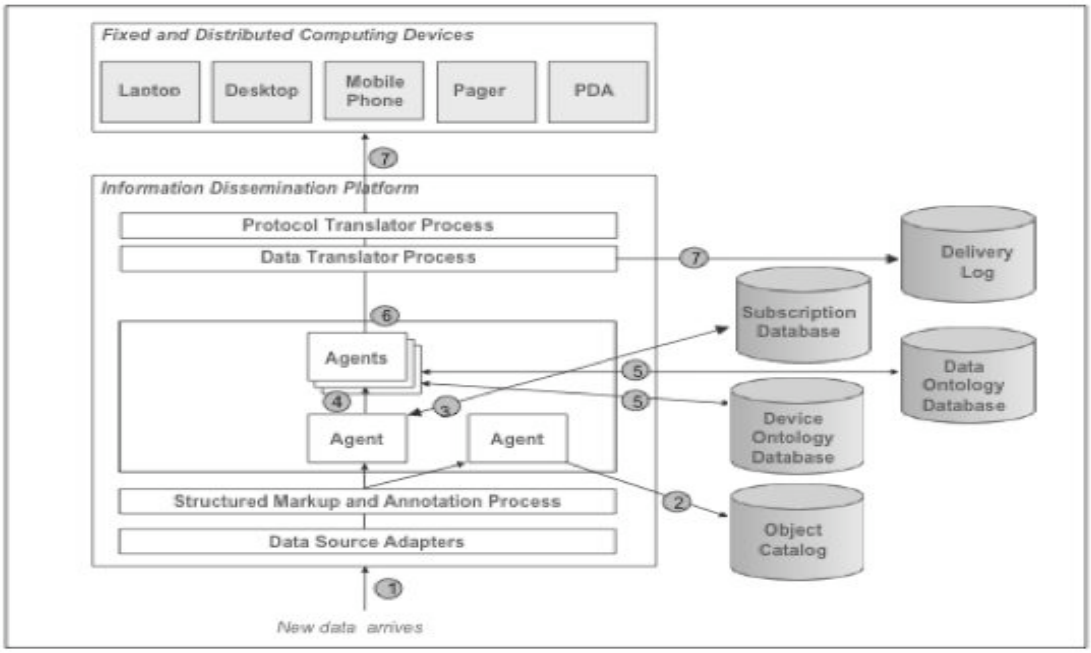

Figure 4: Example Scenario – Automatic Real-Time Alerting Scenario

Figure 4 illustrates an example of how an architecture such as this is utilized to perform real-time alerting. This capability can send data to every user in the system, or to a specified user.

1. The new data is annotated with a standard set of markup tags describing the information, origin, format, and summary of the data.
2. An agent registers the new report in the Object Catalog.
3. An agent compares the new report to the information needs identified by users in the Subscription Information Database to locate users who requested an alert be sent, and on which device.

4. An agent triggers other agents to begin delivery of the alerts.
5. An agent gathers device information for each user and communication information for the data.
6. An agent sends the alerts through the Data Translator Process, and Protocol Translator Process to adjust content, format, and protocol as specified.
7. The alert appears on the users' devices in the appropriate format. A notice of the delivery is sent to the Delivery Log.

4-Conclusions

In conclusion, it is possible to disseminate information to multiple devices using multiple service providers and implementing the device, data and connection ontologies. Most importantly, this can be done without adding any special software or hardware to the user's device. A user can log into the system and immediately add her devices to the system and begin sending and receiving information. This design allows for the system to be available immediately to any user with any device; no proprietary hardware and/or software restrictions placed on the device. This paradigm will not require users of the system to purchase specific devices in order to communicate with each other.

An important research finding was that when defining a device ontology, equal attention should be paid to the service provider and/or client's properties. Important device properties include available memory, sampling rate, and video resolution. Additionally, it is important to know the limitations of the service provider, for example encryption type, data size limitation, etc. Each service provider differs, regardless if the device is the same. Another finding is that it is possible to enhance the device ontologies that are available which will allow for advanced reasoning about a device's capability to both receive and transmit audio.

The ability to securely manage and deliver critical knowledge and actionable intelligence to the analyst regardless of device configuration (bandwidth, processing speed, etc.), classification level or location in a reliable manner, would provide the analyst 24/7 access to useable information.

References

[1] Capraro, Gerard T., "Publish and Subscribe Paradigm with Hand-held Computing Devices", proceedings of the 4th Annual Conference on Information Fusion, FrA2-19 (2004)

[2] P. Obendorf, D. Carney; "A Summary of DoD COTS-Related Policies", SEI Monographs on the Use of Commercial Software in Government Systems Carnegie Mellon Software Engineering Institute (1998)

[3] http://www.fipa.org/, “FIPA Device Ontology Specification” Foundation for Intelligence Physical Agents, Geneva, Switzerland (1996)