RC24115 (W0611-157) November 27, 2006
Computer Science

IBM Research Report

Pushing Emergency Management into Usable SPACE: Securing and Personalizing the Voice Channel

Dimitri Kanevsky
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

Dawn Jutla
Sobey School of Business
Saint Mary's University
Nova Scotia, Canada

Nabil Adam
CIMIC
Rutgers University
New Jersey

Research Division
Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich

Pushing Emergency Management into Usable SPACE: Securing and Personalizing the Voice Channel

Dimitri Kanevsky
Human Language Technologies
IBM T.J. Watson Research Centre
New York, USA

Dawn N. Jutla
Sobey School of Business
Saint Mary's University
Nova Scotia, Canada

Nabil Adam
CIMIC
Rutgers University
New Jersey, USA

Abstract

Human error compromises the security of information systems in government and business organizations in the best of times. In an emergency situation, users are apt to give out more, rather than less information, over the voice channel, in the hope that any extra information may be helpful. Social engineering schemes to gain unauthorized information access are more likely to succeed as human expediency, to access information to inform decision makers and emergency operations, wins the tradeoff over seemingly pedantic security management. We propose an architectural design, specifically for the voice channel, consisting of the coupling of security and context mechanisms with query processing for *secure and relevant information retrieval* in emergency situations. Security and context mechanisms are expected to enhance the utility of information dissemination, via voice, to the emergency worker while ensuring procedural and fine-grain levels of security in emergency management situations.

Introduction

In emergency management, one of the key challenges is achieving effective, timely and systematic collaboration and information sharing among various government agencies at the federal/national, state/provincial, and municipal or local levels. Given the sensitive nature of the information and the emergency environment, it is critical that information sharing be based on user relevance, timeliness, and security. A majority of the agencies are using the Web and voice channels as a means for sharing related information, that exists in different forms – structured and unstructured. Since a person can speak much more quickly than type, voice interaction with information systems matches the urgent nature of emergency management. However, the voice channel, for information access and dissemination, requires further formalization of procedures and control processes than are currently deployed.

In crises, virtual response team(s) needs to be formed in an ad-hoc manner. To add to the complexity, members of a virtual response team may come from various government agencies and private organizations. Depending on several factors, including the location and nature of the crisis, the composition of this virtual multi-agency response team may change from one crisis to another. Furthermore, during the course of a given crisis the membership of this virtual multi-agency response team (VMART) may change dynamically to accommodate various needs (e.g., public health versus fire) and to conform to certain constraints, such as jurisdictions, e.g., the crisis extends, initially from New York to New Jersey. Members of the VMART are both information providers and consumers. As an information provider, an agency will send information, e.g., situation report, to the rest of the team as soon as it is created; members of a team will also share information with others on their team as well as with other team' members. As this information is "pushed" to the various agencies and team members, there is a need to be concerned about access to and distribution of this sensitive information both at the agency level (inter-agency) as well as within a given agency (intra-agency).

This subset of user requirements for the emergency management system motivates us to focus on design, and implementation technologies, to secure voice interaction with emergency management information systems. We design to make secure voice interaction more useful by considering context. However due to space constraints, we do not detail associated context implementation technologies in this paper but do make reference to them.

Fast Authentication and Access

Access to information systems for various purposes, for example for medical help, evacuation plans, or traffic status maps etc. must be as fast as possible. The fact that some infrastructure may be down, such as power (and hence Web servers), telephone lines etc., must be incorporated in a technological response to maintain information availability in crises. Such a response would obviously leverage rapid deployment technologies, e.g. satellite with global coverage and point to multipoint transmission capabilities, mobile vehicles with hardened servers (against movement and other physical trauma) and antennae for supporting wireless network rebuilding, and portable personal devices.

Consider a user querying a "system" in an emergency with "get me all info in the last two hours about xyz". The ideal information retrieval situation would be for the system to automatically and seamlessly compose all the relevant or criti-

cal media to which the user has authorization and send it back to him/her. Such automated retrieval means that objects are retrieved irrespective of where they are stored and without the user issuing individual queries for each document or media object. In such situations, the output delivery model may have to cater for "as info become available" as in when Amazon delivers partially-filled book orders. For further illustration, consider a scenario where there several explosions in various parts of New York and assume that the following agencies constitute the initial VMART.

(1) JIC (Joint Information Center), (2) FBI (Federal Bureau of Investigation), (3) HHS (Health & Human Services), (4) NYPD (New York Police Department), (5) NYFD (New York Fire Department), (6) NYDOT (New York Department of Transportation), (7) FEMA (Federal Emergency Management Agency), and (8) PANYN (Port Authority of New York and New Jersey). Based on its responsibilities, a given agency may generate a set of situation reports. Table 1 lists the different types of situation reports shared among different agencies. Once a situation report is generated by a given agency, certain portions of the report need to be shared with various members of the team.

Based on its responsibilities, a given agency may generate a set of situation reports. Table 1 lists the different types of situation reports shared among different agencies. Once a situation report is generated by a given agency, certain portions of the report are shared with various members of the team.

Table 1. Agencies, responsibilities, and situation reports

Agency	Situation Report	Shared Agency Responsibilities
JIC	Inform the public	Communication transcripts (FBI, NYPD)
FBI	Investigation	Profile records (NYPD) Intelligence reports (NYPD)
HHS	Medical services, syndromic surveillance	Data for disease trends (FEMA) Hospital data (FEMA, NYPD)
NYPD	Evacuation, first response	Crime records/profiles (FBI) First response (HHS, FBI, NYFD, JIC)
NYFD	Firefighting, evacuation	Fire fighting resources status (FEMA)
NYDOT	Security of transportation	Traffic status (NYPD, NYFD, FEMA) Construction status (NYPD, NYFD, FEMA)
FEMA	Reducing loss of life and property	Emergency relief supplies status (NYFD)
PANYNJ	Managing critical infrastructure	Infrastructure details (NYDOT) Surveillance records (FBI)

We propose to augment the user information retrieval task in such a way that information to which the user is authorized to access is retrieved from multiple situation reports (registered sources) and pushed to the user device in response to the query "get me all info in the last two hours about xyz". First, the biometric security process authenticates the user. Once the user passes the authentication test, context is then used to determine which objects, i.e. situation reports, would be relevant to produce results for the user. The situation reports or multiple registered sources may belong to a named group(s) relating to emergency contexts. The attribute types of emergency contexts include, and are not limited to, emergency type (e.g. values are hurricane, tornado, pandemic, earthquake, ice storm), user physical conditions (e.g. light, noise, and temperature levels, crowded), temporal conditions (time, threats from emerging environmental conditions in close future time), user tasks (e.g. task details, status), situation tasks (e.g. completion status), and location. The contexts are intended to provide auxiliary and useful knowledge and information in addition to the content in the situation reports. Contexts will group all the situation reports that are pertinent to a situation or similar situation.

Once the query processing and emergency context units determine which objects or situation reports should help the user, the query processing unit generates a plan to access the remote servers containing the objects. Each of these servers possesses a local biometric security processing system. The user's partial biometric [7] is passed to each remote server, for a second authentication step, and for application of the user's access control role rights to determine and retrieve the portions of objects the user can access. Each local biometric security system maintains biometric prototypes as well as access control rights for each user to the objects that the server manages. The biometric prototype is the pre-enrolled user partial biometric to which a receiving user biometric is matched and considered equivalent above a computed threshold value.

There are two key advantages for the distribution of the partial biometric security units. Firstly, if the central biometric security server is compromised in some way, the various agencies' remote security biometric systems present a further line of defense to protect sensitive data. Alerts can be generated by these remote servers to signal that a central server compromise may have occurred. The governance models then will be accessed and invalidation of the system may occur. Secondly, the distribution of the user' access rights to objects spreads out the index size among various agencies. A disadvantage to the distribution is that if two or more users' access rights to objects are the same, then caching query results at the query processing unit is not possible for response-time speed-up. However, if the user was part of a group, which can be managed and detected at the central biometric unit, then such caching is possible and the user will quickly receive composed delivery objects without incurring traffic to the remote servers.

A main advantage of the integrated architecture, shown in Figure 1, is the user customization due to maintenance of user models - e.g. sending content back to a hearing-or-visually challenged user rather than to a role (e.g. in role-based access control) which cannot be customized at this level. Without our proposal, during usual systems' access, a user may have to directly access various remote systems multiple times in multiple roles to get at various pieces of information to then compose the picture s(he) needs. Our alternative secure IR proposal can provide some enhanced degree of systems' seamlessness, ease of use, and perceived usefulness - while still

ness, ease of use, and perceived usefulness - while still providing strong security.

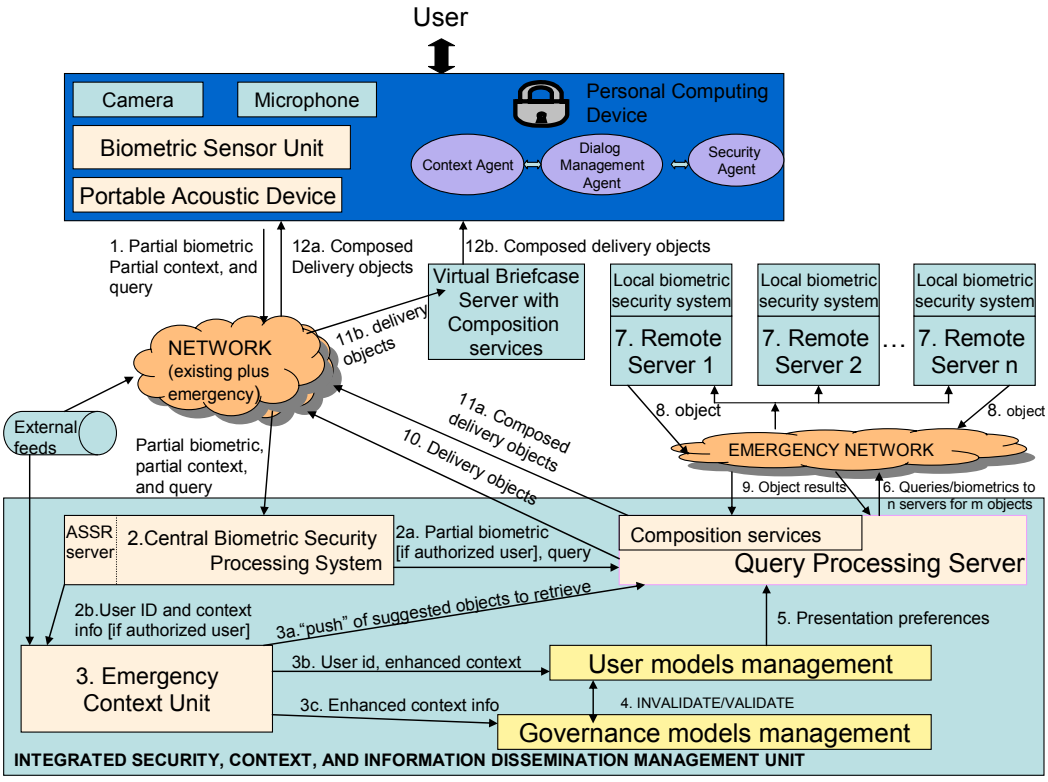

Figure 1. ForSURE (For SecUre Information Retrieval Everywhere) Architecture. (1) User Logan, aviation emergency specialist for NavCAN, sends his partial biometric and a query to get access to key situation data about a plane in an emergency situation in Canadian airspace at 9:00 p.m. He is in his car on the way to command central. (2) The central biometric security (CBS) system ascertains that the user is Logan through its authentication routines, including matching the received partial biometrics with Logan's biometric prototype. (2a) The CBS system forwards the partial biometric and query to the query processing server. (2b) The CBS system sends Logan's user ID and contextual information that he is driving in his car (this context is detected with techniques as described in [11, 13]) to the emergency context unit (ECU). (3) The ECU has previous knowledge that an aviation emergency situation is occurring and based on this temporal context, knowledge of Logan's role as an aviation emergency specialist given his user ID, and new knowledge of what the query is and where the query was issued from, it ranks the objects he should have access to and also sends suggestions to composition services as to the placement of the objects in its final user presentation. (3a) The ECU sends suggested objects to be retrieved to augment and/or confirm those identified by the query processor. (3b) The ECU sends Logan's User ID and summarized context info to the user model management unit. (3c) The ECU sends context info to the Governance Models Management (GMM) unit for audit purposes later. (4) If Logan had issued a command to invalidate one of his partial biometric passwords, the GMM would record this request, and pass on the info to the UMM. (5) The UMM sends presentation instructions to the composition services. These composition services can be simple or sophisticated in terms of converting texts to tables and graphs [e.g. 14] and converting text to audio as in [15]. (6) The Query processing unit decomposes Logan's high level query into a number of smaller separate queries during generating and optimizing its query plan stage; each subquery and (7) Logan's partial biometric is sent to the relevant resources containing the information to be retrieved. Each of these resources has its own local biometric security system whereby Logan is re-authenticated and his access rights to objects on the server are applied to the queried objects. (8) The resources send back the information over the network to (9) the query processor and composition services are possibly invoked and composed objects are delivered as shown in (11a). 10. Composition services are not invoked at the central security, context, and information dissemination unit. Rather, the query results are sent to the virtual briefcase server in (11b). (12a) Personalized and useful information is presented to Logan. (12b) The virtual briefcase server applies Logan's presentation preferences for travel in his car and delivers personalized and useful information to him.

Partial Biometric Security System

Consider our VMART scenario. At the inter-agency level, each agency that is member of the VMART fulfils a certain role and, accordingly, gains access to certain information that is necessary to discharge its duties and fulfill its responsibilities within the overall efforts. For example, the public health agency would need to have access only to the information in the shared reports related to public health, whereas FBI may need access to other related information that is different from the information needed by the public health agency.

At the intra-agency level, each of the agencies, in the VMART, has its own complex security policy and attendant implementation. In addition, within each of these agencies there are individuals who perform a certain role (e.g., chief, first responder), possess different credentials and have different levels of access permissions that match their duties, tasks at hand, and their roles within the agency. Adherence and enforcement of these distributed policies that determine, who can access and/or distribute what information and at what level of granularity to which users, (e.g., the entire situation report, or only the part of the report that pertains to public health to an authorized person) are essential in order to ensure effective inter-agency and inter-governmental response. In Figure 1, we illustrate the distribution of partial biometric security units to the remote servers containing the situation reports and per agency information. These partial biometric units, along with their maintenance of lists of objects and access rights per user, implement and enforce the required policies at each agency' servers. The central biometric security unit forms the first line of defense around the situation reports.

Figure 1 illustrates the network environment in which the random partial biometric security system can operate. The proposed solution associates a set of random partial biometrics [7] with a user who has access rights to portions of documents, conversations, or images. Random partial biometrics are lightweight and appropriate for an environment where power and transmission bandwidth may have become scarce resources. In essence, partial biometrics use allow for *multiple passwords per user for any given system* thereby allowing a user to maintain several identities. As emergencies are temporal in nature, a biometric scheme that allows for password "change" over time is attractive. Biometric-based identification is relevant as they do not have the limitations of having the user carry and manipulate a computer-readable card or pocket token and separately handle a portable or personal device assistant.

Multiple passwords are useful in various scenarios. Imagine a user gets access to a classified portion of a situation report. Assume the content has been tagged with the user partial biometric, to prevent unauthorized content dissemination, and that a user has to input a matching biometric on his PDA to read the content. Now a user wants to transmit the content to an authorized peer's PDA who has been unable to get a strong enough signal to access the information himself. The user sends the content to his peer. He also separately sends the partial biometric which allows the peer to access the content. The original partial biometric owner sends an invalidate command to the central biometric security, context, and IR unit to remove the partial biometric as a future password. This means that there are situations where partial biometrics can be transferred in a similar manner to a user telling a trusted person a password for temporary use. Thus, a user can transfer a partial biometric to another person without worrying about compromising the security of all systems.

Since different user partial biometric sets could be associated with other portions of the same document, conversation, image etc. in a multimedia base, then a user can also self-regulate his/her access to a remote server depending on which biometric piece she chooses to transmit. In other words, an implementation could associate different pieces of a user's biometrics with different access rights to parts of the document (conversation, image) depending on content and need for security. A system can have security, or a user can reveal more or less about himself/herself, on a sliding scale or on an as-needed basis. The systems would also ensure that the user is prevented from revealing his/her full biometric set.

It is possible to compose and enroll a biometric key with several partial (other or self) user biometrics to then require many persons' presence for access (the physical analog is two persons inserting their keys in a safe deposit box before getting access to its contents). Users who wish to escalate their access privileges can use alternative biometric passwords to get at the resources, if necessary. Emergency management workers however may be trained to abide to the principle of least privileged.

Of course with multiple partial biometrics in use, in a conventional situation, it would be possible over time for an eavesdropper to capture a full biometric. In a crisis, this is less likely as it is dubious that hundreds of accesses per user will occur, as well as some access may be to mobile servers on trucks as ad hoc emergency networks are set up. Malicious users would not have the luxury of time to install sniffers etc. even if they had access due to expected gaps due to damage to network infrastructure. However, if necessary, a cryptographic hash function can be implemented, where the central biometric security system sends a random challenge, C, to the biometric sensor unit. The challenge C gets appended to the image pin. Both sides compute a cryptographic hash of the result. The biometric sensor unit sends its hash value to the central biometric security system which compares for equality.

A better alternative for reducing the threat of eavesdroppers capturing full user biometric information is the use of a scheme [10] whereby the user security agent is confirmed with data about its location. This means that if eavesdropper copies, say, partial biometrics data and tries to use it at another location - this can be detected if one finds that the same partial biometrics travels at a different location (there cannot be two identical agents in different locations at the same time period and one can require that travelling agents have a short lifespan - therefore an eavesdropper cannot keep copies of security agents for a long time.

In random partial biometric security, only a portion of biometric data is used to validate the identity of the user. The user biometric data can include fingerprints, voice characteristics, handwriting characteristics, tissue characteristics, gestures, and any other known biometric data. Upon a user request to access secure data, a portion of the digitized user biometric data is sent to a central biometric security system to identify the user. The portion of the digitized user biometric data can include a portion of the digitized image, for example, when the biometric data consists of a fingerprint, facial characteristic or handwriting characteristic, or a portion of speech segments when the biometric data consists of voice characteristics. Since only a random portion of the potentially confidential biometric is being transmitted, the system allows the biometric portions to be transmitted over unsecured communication lines, and even if captured by an eavesdropper, the full biometric image is not obtained.

Figure 2 illustrate various representative biometric portions. A Fingerprint can include coordinates labeled 201-203 which is a set of small rectangular portions within the larger fingerprint. Partial biometrics can also be composed of sound sub-units such as represented as areas OE 205 and PH 206 in the spectogram in Figure 2, for a sequence of phones OE, L, IE, and PH. In addition, biometric portions can include sound sub-units of a given speech phone, such as PH 206. For example, a sub-unit of phone can include portions of a given phone or the whole cepstral feature vector within a phone. Alternatively, biometric portions can be parts of a face picture such as around the eyes (210), the nostrils (209), or part of the ear (208). Parts of a written phrase may also form a partial biometric. More complex composition of one or more of these biometric examples is also possible for higher security needs.

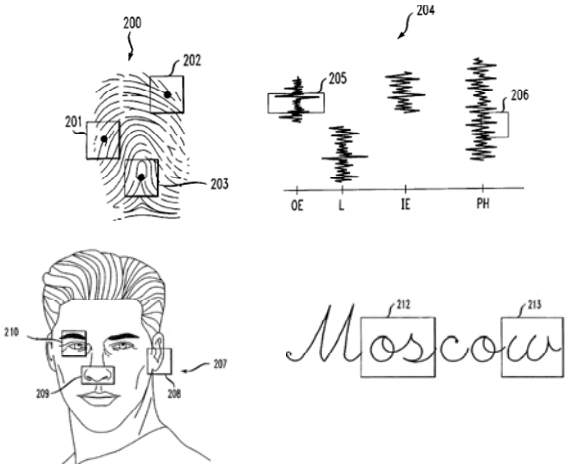

Figure 2. Partial Biometric Examples

There are several possible design implementations for a biometric security system. In one implementation, the biometric security system transmits a security agent to the user's computing device upon a user request to access a remote device. The security agent serves to extract user biometric portions in accordance with the sampling request from the central biometric security system. For illustration, consider that the partial biometric is a voice sample. The security agent then uses the microphone to extract a sampling of speech data from the voice phrase spoken by the user. The security agent then decodes the voice samples and obtains a string of phones. The decoded string of phones is compared to the string of phones received over the network from the central biometric security unit. If the comparison exceeds a predefined threshold, the user is granted access to the requested remote server.

Since only a random portion of the potentially confidential biometric info is being transmitted, the partial biometric portion can be transmitted over unsecured communication channels. The latter is an important consideration when it is uncertain as to which transmission channels are available in a crisis.

The Portable Voice Channel

The voice channel rises in importance in an emergency due to the rapidity in which voice communications can be cheaply restored, its wide area coverage, lower power consumption, and productivity value proposition to name a few. It is safe to assume that emergency management workers will have personal computing devices equipped with voice transaction capability. These days, most of these devices also come equipped with cameras and Internet access-readiness.

Here we describe the need for the portable acoustic unit [9] shown on the personal computing device in Figure 1. First, any system having this unit consisting of a speech signal preprocessing (SSP) device and depending on a remote automatic speech/speaker recognition (ASSR) server, can be used to remotely activate, reset, or change passwords. Second, there are operational difficulties associated with telephonic ASSR systems which need to be ameliorated, including (1) loss of accuracy due to degradation of voice data when it is sent over telephone lines, and (2) the varied background noise characteristics at the user end. Both situations can result in either data or signal integrity loss and thus severe reduction in the accuracy in recognition of the speech/speaker. In an emergency, we expect the quality of transmission to be degraded.

In general, local recognition or validation of a user biometric, via this portable acoustic unit, before performing a remote recognition would reduce the risk of failed server side recognition due to poor biometrics feature. In addition, the overall accuracy is improved while reducing network traffic. Incorrect samples are rejected locally before interacting with the central security system to transmit partial biometrics. The local recognition implementation can, at low cost, require multiple acquisitions of biometric features. Until a verification/identification is positive, the central biometric security system will work with an acceptable set of biometric features (the features stored in the database).

Figure 3 shows one implementation of the acoustic portable device, comprising a microphone for converting sound including speech, silence, and background noise signals to analog signals; a digital signal processor (DSP) for generating from digital signals feature vector data representing the speech and characterization data denoting the silence and background noise signals; a coupler for coupling to an acoustic or data communication device for communicating the feature vector data over a communication channel for recognition of the speech by an ASSR server at a remote location. The coupler can be acoustic for transmission of signals over telephone lines (land line or cellular) and also including an interface (e.g. connector, ports, and protocols, for coupling to a digital transmission device for transmission over a data communication channel.

The portable SSP device may include an encryption device for encrypting the feature vector data, and a data compression device for compressing the feature vector data, and decompressing and decrypting return data. The portable SSP includes characterizing the acoustic features of the transmitting device, environment, speaker, and the communication channel. The SSP information is processed by the ASSR server to set refer-

ences, select appropriate decode models and algorithms to recognize the speaker or decode the speech by modeling the channel transfer function and the background noise to reduce error rate of the speech or to accurately perform speaker recognition.

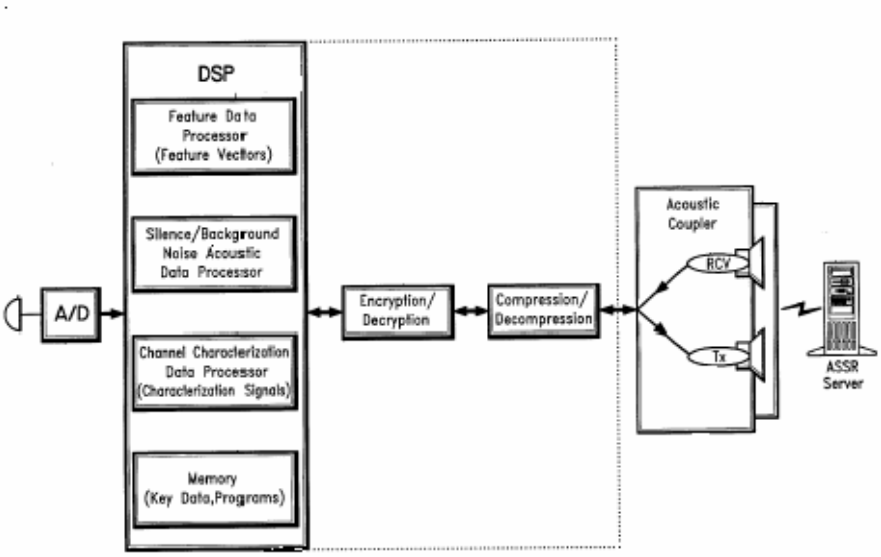

Figure 3. Portable Acoustic Device. (1) A microphone is used to receive sound including speech spoken by the user, silence, and background noise and convert the sound to analog electrical signals (2) The analog to digital converter digitizes the signal (3) The Digital Signal Processor includes a processor and associated memory and stored programs for processing data and controlling data flow in the portable SSP device. (4) The functions (feature, silence/background noise, and channel characterization processors' functions) of the DSP are standard and are commercially available in Texas Instrument's TMS 32010 model for example. The encryption/decryption and compression/decompression devices are optional components and may be separate or attached modules to the DSP. (5) The data processed by the DSP is output to an acoustic coupler.(6) The ASSR system stores models of user enrollment data in memory. ASSR server performs speaker identification and verification.

The ASSR server in the system includes stored models of enrollment or authentication data. The models are built during subscriber or client enrollment. The ASSR server also stores a set of vocabularies and other models, such as language models, and Hidden Markov Models (HMM), for speech recognition. The ASSR server processes the signals received from the portable SSP device and compares the processed signals with the stored models. In summary, the unit shown in Figure 3, enhances the quality of the security management for controlled dissemination of information to users.

Dynamic Information Dissemination: Personalized and Contextualized

Context is any information that can be used to characterize an entity in the environment, which could be location, time, capabilities, lighting, noise levels, services offered and sought, activities and tasks engaged, roles, beliefs, and preferences [5, 6]. As shown in Figure 1, the emergency context management unit has multiple external feeds on the specialized topic of emergency management, from several stakeholders, including previously stored expert knowledge and new user-provided information.

Our system uses two distinct capture and storage points for context management – at the client and server side. At the client side, user context is captured in user models stored in a virtual briefcase [4]. The virtual briefcase may be stored on a nearby server and presentation preferences can be applied to content pushed to it from the central servers. The use of a virtual client briefcase allows a mobile user to travel with his/her virtual portfolio "following" or "shadowing" him/her everywhere and accessible via any local server computer near the user [8]. In particular, users with a PDA (e.g. Blackberry Pearl, PalmPilot) can be connected to any computer at any participating building (e.g. a local coordination site, hospital, mobile truck) and immediately get at an emergency management services computer interface and data in their virtual briefcase related to them.

The virtual client briefcase contains items as personal user data (e.g. user biometrics, client's presentation preference data), general data that is often used by the client (e.g. dictionaries), software packages for office-type applications (e.g. database, spreadsheet, personal time management) and for multimedia and security (e.g. supporting speech, handwriting and user verification recognition systems), and specialized emergency management services applications. Maintenance of the briefcase contents can occur before predicted events (e.g. hurricane, airline crash, tidal wave), with key agency service providers pushing updates to emergency workers' service

applications. Thus such a secure, portable, and ad hoc infrastructure is particularly suitable for the emergency management situation.

Contexts may be implemented with various knowledge representations (e.g. semantic web technologies, such as OWL SWRL, RuleML or web services protocols, or for speed, implemented with a mixture of simple declarative representations in any tag-based markup language. Context traversal could be through a hybrid of reasoning and/or fast program logic with prescriptive data structure lookups, or finite state machines-based. Case-based reasoning [e.g. 2], based on the concept of finding and using past experiences (cases) most similar to the current situation, use of a global access control policy for predefined contexts [1], or simply a table look-up may be used to determine or recommend which large-grain objects (e.g. situation reports) should be part of a retrieval instance for a given user query and context.

Indeed, partial biometrics may be used to support context as well as the additional security it provides. The user security agent can determine what portion of the biometrics to send depending on user-stated context. There are pre-classified contexts, context models, or cases which can be associated with users and their biometric prototypes on enrollment, and one can enhance what information the security agent has to work with. It is possible for the receiving system to get a clue of context also depending of what type of partial biometric, the information content of the biometric, and/or how much of the user biometric it receives. Mechanisms can tie access control with context, such as purpose, (important for privacy or privileged access control) or emergency level status. Such ties make post activities easier, such as security/regulatory auditing, and support risk management. We further propose dynamic Bayesian networks (DBNs) [12] to help manage temporalities in contexts. DBNs are extended from BNs for probabilistic inference in dynamic domains. Compared to BNs, DBNs can capture richer and more realistic domain dependencies and have been applied to manage context-based inferencing in context-aware systems in [3, 4]. Application to emergency management appears straightforward.

Thus if the emergency worker incurs a disability during the emergency, or are in low-lit conditions, or in noisy or low-audio conditions, then existing methods applied to personalization/presentation of information services can help automate adaptation to such situations.

ICE: In Case of Emergency

The ForSURE architectural design facilitates tasks critical to successful emergency management, such as, secure, voice-based information access, and communications. It may facilitate voice channel coordination among a number of agencies. For example, context information, such as "I can see smoke on the 7th floor" can be supplied to the system and be pushed to other related emergency VMART members (firemen, police, ambulance, hospital emergency workers) for tactical coordination.

We anticipate the ForSURE architectural design and associated technologies can both augment and enforce compliance to organizational policies and procedures for secure information retrieval and update over the voice channel.

In case of emergency, ordinary citizens may call the Next Generation (NG) 9-1-1, the US Department of Transportation's initiative for rolling out 9-1-1 with video, voice, and data. Emergency workers, if you see something strange in your neighborhood, who you gonna call? ForSURE?

References

[1] Adam N, Kozanoglu, A., Paliwal, A., Youssef, M., Mutual Trust in Open Environment for Cascaded Web Services, 15 pages, to appear.

[2] Agnar Aamodt and Enric Plaza, "Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches," Artificial Intelligence Communications 7 (1994): 1, 39-52.

[3] An X., Jutla D.N, Cercone N. (2006), Temporal Context Lie Detection and Generation, in Secure Data Management, Very Large Databases VLDB'06, Seoul, Korea, Sept. 2006, 30-47.

[4] An X., Jutla D.N, Cercone N.(2006), Auditing and Inference Control for Privacy Preservation in Uncertain Environments, *First European Conference on Smart Sensing and Context*, Enschede, Netherlands, Oct. 2006, 159-173.

[5] Chen, H., Finin, T., Joshi, A.: An ontology for context-aware pervasive computing environments., Knowledge Engineering Review, Special Issue on Ontologies for Distributed Systems, 18(3) (2004)

[6] Dey, A.: Understanding and using context. Personal and Ubiquitous Computing 5(1) (2001)

[7] Gopalakrishnan, P.S., Kanevsky D., Maes, US Patent No. 6,735, 695 B1, *Methods and Apparatus for Restricting Access of a User Using Random Partial Biometrics*, 2004

[8] Kanevsky D. and Zadrozny, W.W., US Patent No 6,912,580 B1, Virtual Shadow Briefcase in Servers Supporting Moving Embedded Clients, 2005.

[9] Kanevsky, D. and Maes, S.H., Poon, P.S., Prochillo, C., US Patent No. 6,615,171 B1, Portable Acoustic Interface for Remote Access to Automatic Speech/Speaker Recognition Software, 2003

[10] Kanevsky D., US Patent No 6, 988, 279 B1, Intelligent Agent Authentication via Position Locator System, 2006.

[11] Kanevsky, D., Maes, S.H., Sorenson, J.S., US Patent No. 6,665,644 B1, *Conversational Data Mining*, 2003

[12] Li, X., Ji, Q.: Active affective state detection and user assistance with dynamic Bayesian networks. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 35(1) (2005), 93-105

[13] Smith, D., Ma, L., Ryan, N., Acoustic Environment as an indicator of social and physical context, Personal Ubiquitous Computing, 2006, 10:251-254.

[14] Subramaniam C, Kerpedjiev S. Dissemination of Weather Information to Emergency Managers: A Decision Support Tool, IEEE Transactions on Engineering Management, 45 (2), 1998, 106-114.

[15] Viascribe, http://www.liberatedlearning.com/technology/index.html

Dr. Dimitri Kanevsky is an IBM T. J Watson researcher, master inventor, and project manager. His areas of expertise span human language technologies, mathematics, communication technologies for accessibility, and speech recognition for embedded devices and transcription. He holds 89 US issued patents and more than 100 worldwide. Between 2002 and 2006 at least 9 of his patents were classified in the top 10% for major impact on IBM's business.

Dr. Dawn Jutla is a Professor of Information Systems and Computer Science in the Department of Finance, Information Systems, and Management Science at Saint Mary's University in Halifax, Nova Scotia, Canada. She has authored over 70 papers in e-commerce and e-government. She is co-author of the 2001 book entitled *e-Business Readiness: A Customer-Focused Framework* in the Addison Wesley Information Technology Professional Series

Dr. Nabil Adam is a Professor in the Department of Management Science and Information Systems, the Founding Director of the Center for Information Management, Integration and Connectivity (CIMIC), Director of the Meadowlands Environmental Research Institute, and the Director of the Laboratory for Water Security at Rutgers University, Newark, New Jersey. He co-authored/co-edited ten books in areas, such as, Electronic Commerce and Databases Issues in GIS. He serves as the Editor-in-Chief of the International Journal on Digital Libraries. His research work has been supported by various federal, state agencies including the National Science Foundation (NSF), the National Security Agency (NSA), NOAA, US Environmental Protection Agency, the Defense Logistics Agency (DLA), the NJ Meadowlands Commission, and NASA.