The Common Alerting Protocol: An Open Standard for Alerting, Warning and Notification

Art Botterell
incident.com
acb@incident.com

ABSTRACT

This document describes the OASIS Common Alerting Protocol (CAP) standard, review its history and current status, and propose some directions for its future application and development. This XML content standard specifies a canonical data model for alerting, warning and notification messages. By abstracting the essential elements of effective warning messages from the underlying delivery technologies, CAP simplifies the integration of diverse warning delivery systems and provides a simple template for the creation of alerts and warnings. CAP is being used in a variety of warning systems and applications, but its full potential has yet to be exploited.

Keywords

Common Alerting Protocol, XML, data standards, alerting, warning, emergency, disaster.

INTRODUCTION

The effectiveness of public warning systems can be evaluated in a variety of ways. From one perspective warning is strictly an information-transfer activity; once the basic facts about a hazard are made available, this view holds, it is up to each recipient to evaluate, plan and act upon them (or not) as that recipient sees fit. Another point of view sees warning as a tool of community or national self-preservation; according to this model, warning is only effective to the extent it improves (or degrades) net outcomes for the community as a whole. A third viewpoint considers warning to be a tool of authority; from this perspective the measure of warning system effectiveness is the extent of compliance with the recommendations or instructions of the issuing authority.

The common denominator of these perspectives is the psychological and interpersonal dynamics of and among warning recipients. Considerable research has been conducted into how people evaluate the credibility and relevance of warning messages. In November, 2000 a report by the U.S. National Science and Technology Council reviewed this body of research and recommended that:

> "A standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally, and nationally for input into a wide variety of dissemination systems." (NSTC 2000)

This recommendation was based in large part on the need to allow a wide range of official agencies at various levels of government to access an increasingly diverse collection of warning delivery systems. At the same time, the NSTC study noted that coordinated use of multiple delivery systems is required to maximize the reach of warning messages. Other studies have stressed the value of multiple delivery channels in corroborating the authenticity and factual content of an alert (FCC 2004).

The many-to-many nature of the warning system integration challenge suggests the use of a canonical data model pattern (Hohpe and Woolf 2004) to connect multiple warning producers to multiple consumer channels without allowing existing origination or dissemination technologies to become barriers to future improvements in warning technology. Such a model may serve to enhance the effectiveness of warning activities by whatever measure is applied. While helping standardize a complete model of warning information, it also can instantiate various recommendations drawn from the social sciences based on real-world warning experience.

HISTORY AND DESIGN

The initial requirements for a Common Alerting Protocol were drafted by an international Internet-based ad-hoc working group of more than 130 emergency managers and information technology and telecommunications experts convened in early 2001. The CAP Working Group developed a requirements document and initial draft specification based on specific recommendations from Chapter Six of the NSTC report and the professional experiences of Working Group participants.

The CAP requirements described an open, non-proprietary data standard that would provide:

- Compatibility with the data models of existing public warning systems such as the U.S. Emergency Alert System (EAS) and Weather Radio systems;
- Flexible message targeting using geospatial representations in three dimensions;
- Multilingual and multi-audience messaging;
- Phased and delayed effective times and expirations;
- Enhanced message update and cancellation features;
- Template support for framing complete and effective warning messages;
- Digital encryption and signature capability; and,
- Facilities for referencing or inclusion of digital images, audio and video (EM-TC 2003).

The CAP project was endorsed by the non-profit Partnership for Public Warning, and the draft went though several cycles of revision and testing in implementations and field trials in Virginia and California during 2002 and 2003. The CAP draft was formalized as the OASIS CAP 1.0 specification in April, 2004. An updated specification, CAP 1.1, was adopted in October, 2005 (OASIS 2005).

The CAP data model is specified in terms of the eXtensible Markup Language (XML) for communication compatibility with current technologies. However, the same data model can be represented directly in various other formats. A generalized object model for a CAP message is illustrated in Figure 1.

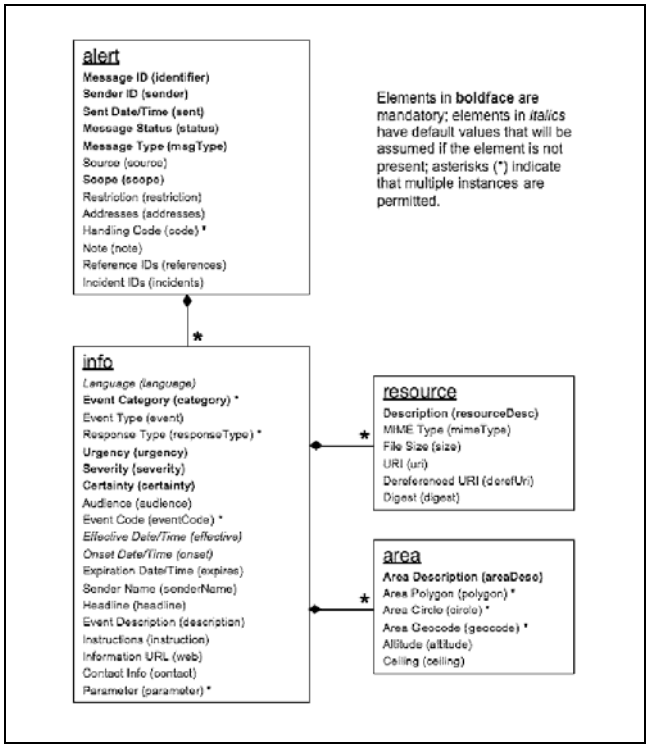

Figure 1. CAP Message Data Model (OASIS 2005)

CURRENT STATUS AND CHALLENGES

The CAP specification was released at an opportune time. In early 2004 the U.S. federal government and many state and local governments had adopted enterprise architectures that encouraged open interface standards, and the tragic events of September 11, 2001 had raised interest in warning and public protection systems. "Interoperability" had become a mantra, and although most uses of that word referred to two-way radios, it nonetheless offered a powerful metaphor for concerns that had until then been seen as somewhat abstract and rarified.

Those factors, in combination with the iterative, prototype-driven design process that preceded formalization of the CAP specification, led to rapid adoption of CAP in a number of contexts. These implementations, in turn, raised issues for future development.

Early Implementations

Early U.S. adopters of CAP included the Department of Homeland Security (DHS), the National Weather Service, the U.S. Geological Survey and the Centers for Disease Control. The CAP data format was utilized in "Digital EAS" trials in and around Washington D.C. in 2005 as a joint venture between DHS and the Association of Public Television Stations. The Federal Communications Commission requested comment on CAP in a Notice of Proposed Rulemaking process in 2004-2005, and received endorsements of CAP from, among others, the U.S. Society of Broadcast Engineers.

CAP-based alerting systems have been deployed by the State of California and the Contra Costa County (California) Sheriff's department. A number of states, including California, Florida and Washington, have announced that they will require CAP compatibility in all future warning system procurements. CAP implementations have also been reported in Australia, Canada, Czechoslovakia and Italy. Numerous warning system and messaging system vendors have claimed various degrees of CAP capability (CAP Cookbook 2006).

An open-source Java implementation of classes for parsing, modifying and originating CAP messages has been published (caplib 2006) and is the base of a number of current CAP "channel adapter" modules for warning devices and emergency management software packages.

Early Challenges

Although the Common Alerting Protocol provides a data model for alerting system, it by no means answers all the challenges and issues surrounding public warning. The rapid adoption of CAP has led to equally rapid identification of additional warning system challenges which previously might have been masked by a lack of an agreed content definition. These include:

Transport Mechanisms

The CAP data model was designed to be agnostic as to data transport facilities. CAP messages can be used in synchronous, asynchronous, multicast, publish/subscribe and other messaging systems. This flexibility is also a shortcoming in some contexts; an integrated warning framework requires definition of transport arrangements as well as of message payload.

Definition of transport infrastructure is only partly a technical problem. Issues of organizational responsibility, budgetary priority, agency and unit autonomy, local control, and commercial factors all interact with functional requirements in the design of actual deployments. The availability of a common data model that is not constrained by any particular transportation agreement has made negotiation and bridging of diverse systems both possible and necessary.

In the short time CAP has been available, four primary approaches to CAP transport have emerged:

- RSS-style "feeds" (using either the RSS 2.0 or Atom formats) scale well for the publication of current and recent alerts to a large number of recipients. They can provide the equivalent of a "durable subscriber" publish/subscribe mechanism for automated clients while also being "web-browser friendly" by means of eXtensible Stylesheet Language (XSL) formatting.
- Web Services can be used effectively to accept CAP messages from a variety of senders, generally with some form of authentication, and to pass messages among servers. They also can be used to access databases of CAP messages.

- Multicasting has limited viability on wired networks due to routing and performance constraints, but has proven effective over wireless broadcast networks such as digital television and satellite.
- A profile for transporting CAP messages over the XMPP ("Jabber") messaging protocol has been published, which may offer an efficient "push" mechanism for publish/subscribe patterns (JEP-0127 2004).

Other transport arrangements are possible, and a period of experimentation and evolution (both in technology and in organizational arrangements for alerting and public warning) seems to be underway. It remains to be seen which transports and patterns will be adopted widely.

Identity and Authority

The authenticity of warning messages is of great concern both to dissemination system operators and to the receiving public. At present most CAP implementations employ a trusted-server authentication model, wherein message originators authenticate themselves to the server, and consumers trust that server to have verified the identity and authority of the sender. This "one hop" trust model is readily implemented using conventional Secure Sockets Layer (SSL) encryption of transactions with a web server, and can be enhanced on the input side by the use of two-factor authentication methods such as password tokens. However, such single-hub architectures are subject to various reliability, scalability and political critiques.

The CAP standard specifies how the World Wide Web Consortium (W3C) XML-Signature and XML-Encryption standards can be applied to CAP messages. XML Signature (XMLSIG 2002) in particular provides a mechanism for persistent end-to-end authentication of individual messages without relying on the security of the links and nodes those messages traverse. XML signatures provide a means of detecting modifications of messages in transit ("man in the middle" attacks) and also of verifying the authenticity of the message.

However, such XML signatures require a public key infrastructure (PKI) to maintain the binding between the digital identity of a message originator and the "real world" roles, attributes and authority of the individual wielding that digital identity. Such PKIs are required for a number of public-safety and emergency management information technologies, but they have been slow to develop. Possible reasons for this delay include the complexity (or at least, perceived complexity) of PKI implementation, and the persistent labor costs entailed in verifying and updating identities, delivering digital identity certificates and maintaining certificate revocation lists.

Other approaches to digital signatures that might not require a large-scale PKI are being investigated in the research community and might come into application soon enough to mitigate the current obstacles.

Geospatial Referencing

One of the major technical advances embodied in the CAP data model is the use of flexible geospatial (latitude, longitude and altitude) descriptions of locations and areas in preference over the multitude of pre-determined targeting zone codes in use by various existing warning systems. Whether such pre-existing codes were derived from planning scenarios (as is typical around nuclear power plants and other potentially hazardous facilities) or drawn along administrative boundaries (as with the county boundaries used as the Emergency Alert System), actual events tend not to conform to them.

However, many officials are long familiar with such static zones and view their replacement with some anxiety. In addition, some of these boundaries have been memorialized in procedures or regulations and are required to be referenced in warning messages. While practitioners versed in geographic information systems (GIS) understand that any predetermined geographic zone designator is simply shorthand for a geospatial point or polygon, there remains a sizeable cognitive gap between many emergency managers (and even many information technology professionals) and the specialist GIS community.

For "backward compatibility" with existing coding schemes, CAP provides for the use of such "geocodes." However, their use is deprecated because they rely on all clients having knowledge of all the possible alert-zone systems they might encounter; particularly for mobile clients, that poses a serious challenge to interoperability.

As GIS emerges from specialty departments and becomes more generally familiar (through the agency of popular geospatial services like Google Earth and Yahoo! Maps) user anxieties about drawing custom alert target zones directly on a map may be salved somewhat. At the same time, geospatial "thesaurus" services may smooth the conversion from static zones to flexible geospatial representations of hazard areas and message distribution targets.

Uncertainty

One of the most unsetting aspects of any emergency is the uncertainty induced by sudden or unexpected events. An undesirable side effect of this is a temptation of individuals, particularly those in positions of authority, to assert a greater degree of certainty then the available facts justify. This human tendency is compounded by the all-or-nothing nature of many existing warning systems; this frequently results in warnings being withheld until additional information is obtained, by which time they may be too late to help their audience.

In addition to codifying the urgency (in terms of time) and severity of a hazard, the CAP message format allows the sender to assert a level of certainty associated with the warning information. Regrettably, some warning originators may perceive any confession of uncertainty as either evidence of poor performance on their part or as a weakening of the impact of their warning message. A great deal of research and education in the area of communicating probabilistic information to mass audiences may be required before the uncertainty barrier can be removed.

POTENTIAL FUTURE APPLICATIONS

In this document we have used the terms "alert," "warning" and "notification" interchangeably, while defining none of them. We are aware of no general convention (and a wide diversity of local ones) for the specific usages of these terms; however, it may be worth noting that each of them, and particularly "warning," tends to have connotations of special knowledge or authority on the part of the source. While this conventional sense may be reflected in specialized domains like meteorology or military defense, there are a number of potential applications of the Common Alerting Protocol that do not entail formal authority relationships.

CAP for Disclosure of System State

One application of an RSS-style CAP "feed" might be to characterize the state of a system, facility or community by exposing a collection of current CAP documents representing any excursions from or exceptions to the "normal" state. These notices would be visible using a web browser and would also be well-suited to automatic monitoring. This might be a simple way to address community notification requirements around potentially hazardous facilities, volcanoes, flood zones and so on.

CAP as Request for Service

Just as a CAP message can be used to encode information and instructions from an authoritative source to individual citizens, the same data format might be used to implement a "digital 9-1-1" request for assistance from an individual, household or office to local authorities. The same message, shared locally, might also summon life-saving assistance from other nearby homes, offices or even passers-by. This same concept could be applied to larger-scale requests for assistance, especially from isolated facilities, ships, island communities and the like.

CAP in Attention Management

Although we make no attempt to define the terms "warning" or "alerting," we will observe that they have strong connotations of attempts to redirect the attention of the recipient. It seems possible that the CAP data format might be used as input to personal attention-management applications to provide information about less dire events and situations than we normally associate with the words "alert" or "warning."

Obviously this raises questions of who has control of whose attention. The specter of "attention spam" is enough to give any serious implementer pause. One way to guard against intrusive or unwanted "notifications" would be to implement a strict sender-authentication function into the application; this would not in itself prevent misuse but would provide accountability and enforceability of laws, policies and personal preferences.

CAP as Event-Driven Messaging

Perhaps by virtue of its early availability and its built-in facilities for correlation, cancellation, updates, error handling and the inclusion of specialized parameter data values and binary assets, CAP has been applied in ways many of its designers have found surprising. For example, one web-server monitoring firm uses CAP messages to notify its subscribers when their servers malfunction (SiteRecon 2005). This suggests that CAP may have potential for use as a general-purpose "eventing" message format; what it lacks in specialization it may make up in ready availability.

OPEN SOURCE IN PUBLIC SAFETY

Leaving aside the particulars of CAP for a moment, it may be worthwhile briefly to consider the process by which CAP was developed and then brought into use, particularly by government agencies. It has been said, "Free is the one price government doesn't know how to pay." Certainly when it comes to sophisticated technology, government procurements (in the U.S. at least) have a strong tendency to be vendor-driven. The technical possibilities perceived by government officials tend to be the ones suggested by known vendors. Innovative suggestions from outside the existing vendor community have difficulty getting a hearing, and it is not unknown for vendors to deliberately cast doubt on "disruptive" technologies in a bureaucratic maneuver so familiar it has a name: "Defending the rice bowl."

Doubtless this mechanism has filtered out an enormous number of bad proposals. However, it also has raised barriers to legitimate innovators, especially in the academic sector, many of whom feel their attempts to bring new technologies from the laboratory to the field have hit a "glass ceiling." In particular, innovations that do not fit neatly into existing governmental programs (or commercial product categories) frequently are relegated to an "orphan" status wherein they languish for lack of attention and resources. This certainly was the case for CAP. A number of participants in the original, ad-hoc CAP Working Group were current or former government officials who reported frustration with trying to address warning problems through official challenges. It was the introduction of processes drawn from the "open source" movement of skilled volunteerism that enabled these professionals to achieve outside both government and commerce what neither of those institutions seemed capable of accomplishing separately or in concert. Its very lack of pre-existing priorities or commitments allowed the Working Group to take a fresh approach to what had hitherto been intractable technical and operational problems, while the collaborative processes pioneered by the open source software community provided the necessary balance between individual initiative and the wisdom of an inclusive and experienced team.

The protocols of open-source teamwork might lead the author to understate the crucial role of strong individual visions in this process. The open-source community has refined a collection of norms and techniques for harnessing the creative energy of individuals in support of shared goals without distorting the individuals' personal contributions or creating undue organizational stresses. This style of organizational design for creativity appears to be a very fruitful area for future research. Many of its roots may be found in the creative and communication arts as well as in computer science. The success of CAP in making the transition from an unofficial, non-commercial open-source effort into successful adoption by business and government also may be worthy of further study as a successful method of incorporating innovation into our collective response to the hazards and uncertainties of our modern world.

CONCLUSION

The Common Alerting Protocol is an attempt to inject an appropriate and useful layer of abstraction into the only-too-concrete business of public safety, emergency management and homeland security. Recognition of the value of such abstractions in the formulation of business processes and the information environment is one of the key contributions of the computer sciences to modern society. CAP is one small application of that principle to the protection and promotion of the common good.

ACKNOWLEDGMENTS

It is impossible to acknowledge the literally hundreds of individuals and institutions that have contributed to the development and deployment of CAP. Suffice it to say that CAP continues to be the product of the collective creativity, idealism and optimism of a global community that includes each of you who have taken time to read these words.

REFERENCES

1. CAP Cookbook 2006 - (2006) Who's Using CAP?, http://www.incident.com/cookbook/index.php/Who_Is_Using_CAP?
2. caplib 2006 - Botterell, A. (2006) caplib - An Open-Source Library for the Common Alerting Protocol, http://www.incident.com/caplib/
3. EM-TC 2003 - OASIS Emergency Management Technical Committee (2003) Requirements for a Common Alerting Protocol,
4. FCC 2004 - Media Safety and Reliability Council (2004) Public Communications and Safety Working Group: Final Report, Federal Communications Commission, Washington, D.C.

5. Hohpe, G. and Woolf, B. (2004) Enterprise Integration Patterns : designing, building, and deploying messaging solutions, Addison-Wesley, Boston.
6. JEP-0127 2004 - Saint-Andre, P. and Fletcher, B. (2004) JEP-0127: Common Alerting Protocol (CAP) Over XMPP, http://www.jabber.org/jeps/jep-0127.html
7. NSTC 2000 - U.S. National Science and Technology Council (2000) Effective Disaster Warnings, U.S. National Science and Technology Council, City
8. OASIS 2005 - OASIS Emergency Management Technical Committee (2005) Common Alerting Protocol, v. 1.1, Organization for the Advancement of Structured Information Standards (OASIS), http://www.oasis-open.org/committees/download.php/14759/emergency-CAPv1.1.pdf
9. SiteRecon 2005 - Integration Solutions, I. (2005) Common Alerting Protocol (CAP) Monitoring Feed, http://www.siterecon.com/CAPFeed.aspx
10. XMLSIG 2002 - Eastlake, D., Reagle, J. and Solo, D. (2002) XML-Signature Syntax andProcessing, W3C, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/