Network Working Group
Request for Comments: 3689
Category: Informational

K. Carlberg
UCL
R. Atkinson
Extreme Networks

February 2004

General Requirements for Emergency Telecommunication Service (ETS)

Status of this Memo

Copyright Notice

Abstract

This document presents a list of general requirements in support of Emergency Telecommunications Service (ETS). Solutions to these requirements are not presented in this document. Additional requirements pertaining to specific applications, or types of applications, are to be specified in separate document(s).

1. Introduction

Effective telecommunications capabilities can be imperative to facilitate immediate recovery operations for serious disaster events, such as, hurricanes, floods, earthquakes, and terrorist attacks. Disasters can happen any time, any place, unexpectedly. Quick response for recovery operations requires immediate access to any public telecommunications capabilities at hand. These capabilities include: conventional telephone, cellular phones, and Internet access via online terminals, IP telephones, and wireless PDAs. The commercial telecommunications infrastructure is rapidly evolving to Internet-based technology. Therefore, the Internet community needs to consider how it can best support emergency management and recovery operations.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [1].

1.1. Terminology

Label:
The term label has been used for a number of years in various IETF protocols. It is simply an identifier. It can be manifested in the form of a numeric, alphanumeric value, or a specific bit pattern, within a field of a packet header. The exact form is dependent on the protocol in which it is used.

An example of a label can be found in RFC 3031; the Multiprotocol Label Switching Architecture. Another example can be found in RFC 2597 (and updated by RFC 3260); a bit pattern for the Assured Forwarding PHB group. This latter case is a type of label that does not involve routing. Note that specification of labels is outside the scope of this document. Further comments on labels are discussed below in section 3.

1.2. Existing Emergency Related Standards

The following are standards from other organizations that are specifically aimed at supporting emergency communications. Most of these standards specify telephony mechanisms or define telephony related labels.

Standard	/ Organization
1) T1.631	/ ANSI
2) E.106	/ ITU
3) F.706	/ ITU
4) H.460.4	/ ITU
5) I.255.3	/ ITU

The first specifies an indicator for SS7 networks that signals the need for a High Probability of Completion (HPC) service. This indicator is termed National Security / Emergency Preparedness (NS/EP) The T1.631 standard [2] is the basis for the U.S. Government Emergency Telecommunications Service (GETS) [7].

The second standard describes functional capabilities for the Public Switched Telephone Network (PSTN) to support International Emergency Preparedness System (IEPS) [3]. From the PSTN perspective, one can view NS/EP as a standard with national boundaries, while IEPS is an extension to international boundaries for telephony.

The third standard extends IEPS beyond the scope of telephony into other forms that encompass multimedia [4].

The fourth and fifth standard focuses on a multi-level labeling mechanism distinguishing emergency type traffic from that which is not. The former case focuses on call signaling for H.323 networks [5], while the latter has been applied for both SS7 [6] and data networks.

While the above standards are outside the scope of the IETF, they do represent existing efforts in the area of emergency communications, as opposed to conceptual of potential possibilities. They act as example manifestations of Emergency Telecommunications Service (ETS).

1.3. Problem

One problem faced by the IEPREP working group entails how, and to what degree, support for these standards are to be realized within the Internet architecture and the existing suite of IETF standards and associated working groups. This support could be in the form of interoperability with corresponding IETF protocols.

A subsequent problem is to ensure that requirements associated with potential support is not focused just on IP telephony applications. The I-Am-Alive (IAA) database system is an example of an ETS type application used in Japan that supports both signaled and non-signaled access by users [10]. It is a distributed database system that provides registration, querying, and reply primitives to participants during times of an emergency (e.g., an earthquake) so that others can make an after-the-event determination about the status of a person. In this case, a separate signaling protocol like SIP is not always required to establish or maintain a connection.

Given the case where signaling is optional, requirements and subsequent solutions that address these problems must not assume the existence of signaling and must be able to support applications that only have labels in data packets. These label(s) may be in various places, such as the application or IP header.

2. Scope

This document defines a set of general system requirements to achieve support for ETS and addressing the problem space presented in Section 1.3. In defining these requirements, we consider known systems such as GETS and IAA that represent existing manifestations of emergency related systems. These two examples also represent a broad spectrum of characteristics that range from signaling & interactive non-elastic applications to non-signaled & elastic applications.

We stress that ETS, and its associated requirements, is not the only means of supporting authorized emergency communications. It is simply an approach influenced by existing systems and standards.

Solutions to requirements are not defined. This document does not specify protocol enhancements or specifications. Requirements for specific types of applications that go beyond the general set stated in section 3 are to be specified in other document(s). At the current writing of this document, [9] has been written for the case of IP telephony.

The current IEPREP charter stipulates that any proposed solution to support ETS that responds to the requirements of this document are to be developed in other working groups. We note that other specific requirements (like that of IP telephony) may be defined as an extension of the general requirements presented in section 3 below.

2.1. Out of Scope

While the problem space stated in section 1.3 includes standards related to telephony, this document is meant to be broader in scope. Hence, emulation of specific architectures, like the PSTN, or focus on a specific application is out of scope. Further, the specifications of requirements that are aimed at adhering to regulations or laws of governments is also out of the scope of this document. The focus of the IETF and its working groups is technical positions that follow the architecture of the Internet.

Another item that is not in scope of this document is mandating acceptance and support of the requirements presented in this document. There is an expectation that business contracts, (e.g., Service Level Agreements), will be used to satisfy those requirements that apply to service providers. Absence of an SLA implies best effort service is provided.

3. General Requirements

These are general requirements that apply to authorized emergency telecommunications service. The first requirement is presented as a conditional one since not all applications use or are reliant on signaling.

1) Signaling

   IF signaling is to be used to convey the state or existence of emergency, then signaling mechanism(s) MUST exist to carry applicable labels.

2) Labels

Labels may exist in various forms at different layers. They might be carried as part of signaling, and/or as part of the header of a data packet. Labels from different layers are NOT required to be the same, but MAY be related to each other.

3) Policy

Policy MUST be kept separate from label(s). This topic has generated a fair amount of debate, and so we provide additional guidance from the following:

A set of labels may be defined as being related to each other. Characteristics (e.g., drop precedence) may also be attributed to these labels. [11] is an example of a related set of labels based on a specific characteristic.

However, the mechanisms used to achieve a stated characteristic MUST NOT be stated in the definition of a label. Local policy determines mechanism(s) used to achieve or support a specific characteristic. This allows for the possibility of different mechanisms to achieve the same stated characteristic.

The interaction between unrelated labels MUST NOT be embedded within the definition of a label. Local policy states the actions (if any) to be taken if unrelated labeled traffic merges at a node.

Finally, labels may have additional characteristics added to them as a result of local policy.

4) Network Functionality

Functionality to support a better than best effort SHOULD focus on probability versus guarantees. Probability can be realized in terms of reduced probability of packet loss, and/or minimal jitter, and/or minimal end-to-end delay. There is NO requirement that a better than best effort functionality MUST exist. There is NO requirement that if a better than best effort functionality exists then it must be ubiquitous between end users.

3.1. General Security Related Requirements

The following are security related requirements that emerge given the requirements 1 through 4 above.

5) Authorization

Authorization is a method of validating that a user or some traffic is allowed by policy to use a particular service offering.

Mechanisms must be implemented so that only authorized users have access to emergency telecommunications services. Any mechanism for providing such authorization beyond closed private networks SHOULD meet IETF Security Area criterion (e.g., clear-text passwords would not generally be acceptable). Authorization protects network resources from excessive use, from abuse, and might also support billing and accounting for the offered service.

Such authorization mechanisms SHOULD be flexible enough to provide various levels of restriction and authorization depending on the expectations of a particular service or customer.

6) Integrity & Authentication

In practice, authentication and integrity for IP based communications are generally bound within a single mechanism, even though conceptually they are different. Authentication ensures that the user or traffic is who it claims to be. Integrity offers assurance that unauthorized modifications to objects can be detected.

Authorized emergency traffic needs to have reduced risk of adverse impact from denial of service. This implies a need to ensure integrity of the authorized emergency network traffic. It should be noted, though, that mechanisms used to ensure integrity can also be subject to Denial of Service attacks.

Users of emergency network services SHOULD consider deploying end-to-end integrity and authentication, rather than relying on services that might be offered by any single provider of emergency network services. Users SHOULD also carefully consider which application-layer security services might be appropriate to use.

7) Confidentiality

Some emergency communications might have a requirement that they not be susceptible to interception or viewing by others, due to the sensitive and urgent nature of emergency response activities. An emergency telecommunications service MAY offer options to provide confidentiality for certain authorized user traffic.

Consistent with other IETF standards and the Internet Architecture, this document recommends that IEPREP users SHOULD deploy end-to-end security mechanisms, rather than rely on security services that might be offered by a single network operator. IEPREP users SHOULD carefully consider security alternatives (e.g., PGP, TLS, IPsec transport-mode) at different layers (e.g., Application Layer, Session Layer, Transport Layer) of the Internet Architecture before deployment.

4. Issues

This section presents issues that arise in considering solutions for the requirements that have been defined for ETS. This section does not specify solutions nor is it to be confused with requirements. Subsequent documents that articulate a more specific set of requirements for a particular service may make a statement about the following issues.

1) Accounting

Accounting represents a method of tracking actual usage of a service. We assume that the usage of any service better than best effort will be tracked and subsequently billed to the user. Accounting is not addressed as a general requirement for ETS. However, solutions used to realize ETS should not preclude an accounting mechanism.

2) Admission Control

The requirements of section 3 discuss labels and security. Those developing solutions should understand that the ability labels provide to distinguish emergency flows does not create an ability to selectively admit flows. Admission control as it is commonly understood in circuit-switched networks is not present in IP-based networks, and schemes which presume the ability to selectively admit flows when resources are scarce will fail outside of very controlled environments. In cases where emergency related flows occur outside of controlled environments, the development of technologies based on admission control is not recommended as the foundation of emergency services.

3) Digital Signatures

Verification of digital signatures is computationally expensive. If an operator acts upon a label and hence needs to verify the authenticity of the label, then there is a potential denial-of-service attack on the entity performing the authentication. The DoS attack works by flooding the entity performing the

authentication with invalid (i.e., not authentic) labelled information, causing the victim to spend excessive amounts of computing resources on signature validation. Even though the invalid information might get discarded after the signature validation fails, the adversary has already forced the victim to expend significant amounts of computing resource. Accordingly, any system requiring such validation SHOULD define operational and protocol measures to reduce the vulnerability to such a DoS attack.

5. Related Work

RFC 3487 describes requirements for resource priority mechanisms for the Session Initiation Protocol [8]. The requirements specified in that RFC pertain to a specific application level protocol. In contrast, the requirements of this document are a generalization that are not application specific. From this blueprint (acting as a guideline), more specific requirements may be described in future documents.

6. Security Considerations

Security in terms of requirements is discussed sections 3.1 and 4.

7. References

7.1. Normative Reference

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7.2. Informative References

[2] ANSI, "Signaling System No. 7(SS7) "High Probability of Completion (HPC) Network Capability" , ANSI T1.631-1993 (R1999).

[3] "Description of an International Emergency Preference Scheme (IEPS)", ITU-T Recommendation E.106 March, 2000.

[4] "Description for an International Emergency Multimedia Service", ITU Draft Recommendation F.706, February, 2002.

[5] "Call Priority Designation for H.323 Calls", ITU Recommendation H.460.4, November, 2002.

[6] ITU, "Multi-Level Precedence and Preemption Service, ITU, Recommendation, I.255.3, July, 1990.

[7] U.S. National Communications System: http://www.ncs.gov

[8] Schulzrinne, H., "Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP)", RFC 3487, February 2003.

[9] Carlberg, K. and R. Atkinson, "IP Telephony Requirements for Emergency Telecommunications Service", RFC 3690, February 2004.

[10] Tada, N., et. al., "IAA System (I Am Alive): The Experiences of the Internet Disaster Drills", Proceedings of INET-2000, June.

[11] Heinanen, J., Baker, F., Weiss, W. and J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, June 1999.

8. Authors' Addresses

Ken Carlberg
University College London
Department of Computer Science
Gower Street
London, WC1E 6BT
United Kingdom

EMail: k.carlberg@cs.ucl.ac.uk

Ran Atkinson
Extreme Networks
3585 Monroe Street
Santa Clara, CA
95051 USA

EMail: rja@extremenetworks.com

9. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.