Network Working Group
Internet-Draft
April 1, 2005

M. Schulze
Matthew.Schulze@mapics.com
W. Lohsen
William.Lohsen@GTRI.gatech.edu

IP over Burrito Carriers

draft-lohsen-ip-burrito-00

Status of this Memo

Copyright Notice

Abstract

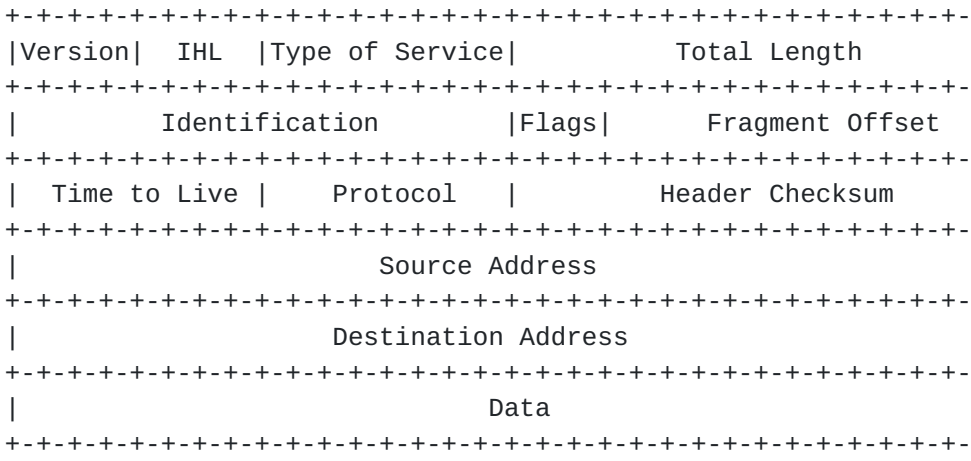
IP over Burrito Carriers describes an experimental method for the creation of edible data packets. This standard is intended to be implemented in metropolitan area networks due to the preexisting burrito delivery infrastructure. While currently only flour tortillas have been found acceptable for encapsulating the data contained in the packet, tests are underway to determine the viability of using corn tortillas. One must be wary of disreputable IP over Burrito service providers as packet corruption and bad data handling can result in damage to the receiving unit and may result in an extremely messy packet rejection. Conveniently, there is a rating system already in place. While the rating by the health department doesn't ensure proper data encapsulation, it does allow the end user to determine if the service provider's quality to cost ratio is adequate. This is an experimental standard, not a recommended standard.

Introduction

In today's wireless hotspot, WAP enabled, WiFi zoned world of dining there exists a discrimination against diners who prefer to eat outside the established confines of the restaurant. The IP over Burrito standard was developed to create an edible solution to the growing rift in the availability of free internet access between sit-down and delivery/carry out diners. While considerable research has yet to be performed on the IP over Burrito standard, multiple simulations in a controlled environment have proven to be both successful and filling. Some concerns that must be addressed in the future include the ability of the hosts buffer to accommodate a large number of packets while they are processed. Also the fact that a buffer overflow would cause a catastrophic system failure resulting in a purging of all previously processed datagrams is of major concern. Currently datagrams are encapsulated in a flour tortilla. Future projects will determine the viability of using corn tortillas but for now the standard requires the use of a flour tortilla for all datagram encapsulation.

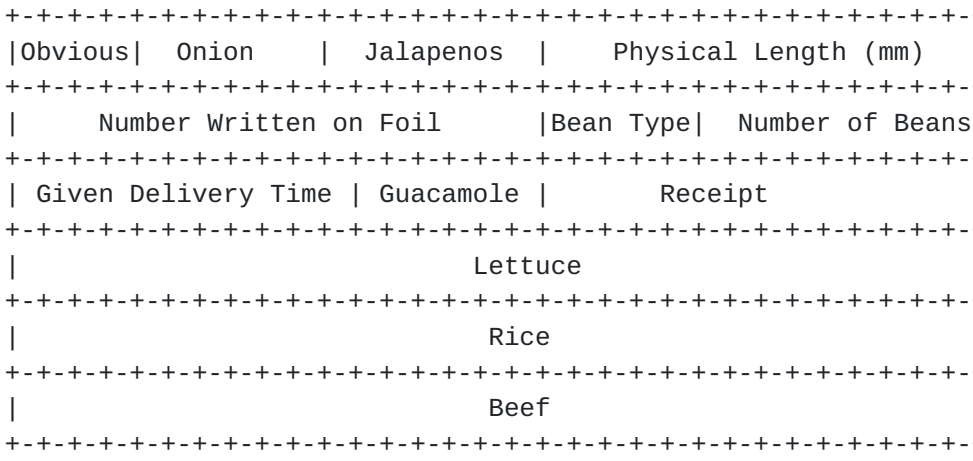
Packet Format

Packets will follow the standard Internet Header Format [RFC-791] (Figure 1). Each field (Figure 1) has been sublimated with a tangible equivalent (Figure 2) to binary representation that is both tasty and filling.



The Internet Header Format [RFC-791]

Figure 1.



The Burrito Internet Header Format

Figure 2.

Version: Obvious

The Version field is indicated by the obvious. It is a burrito. As the IP over Burrito standard is designed to work solely with modern equipment, it supports only IPv4 packets.

IHL: Onion

Internet Header Length is specified by the number of onions placed in the burrito.

Type of Service: Jalapenos

The 8 bits of this header are specified by 8 jalapeno slices. A half slice indicates a zero and a whole slice indicates a one.

Total Length: Physical Burrito Length

The length of the burrito in centimeters multiplied by 4096 gives the total length of the datagram, in octets.

Identification: Number written on foil wrapper.

Flags: Type of Beans

Black Beans = Don't Fragment
Red Beans = Fragment
Pinto Beans = Last Fragment
Kidney Beans = More Fragments

Fragment Offset: Total Number of Beans.

Time to Live: Specified by source host in minutes.

Commonly in the range of 35-45 minutes, given traffic conditions.

Protocol: Guacamole

The chunkiness, quality, and amount of Guacamole determine this data.

Header Checksum: Receipt

The data on the receipt should match the specifications of the burrito datagram.

Source Address: Lettuce

Given the size of this field it is necessary to break it down into subsections. The lettuce is placed in 4 discrete groups. Also, the lettuce is colored with food coloring to be either red, green, or blue. Red lettuce indicates the most significant digit, green the middle digit, and blue the least significant digit. Thus limiting the amount of lettuce on the burrito to a manageable level in respect to determining the data and fitting in the tortilla.

Destination Address: Rice

Given the size of this field it is necessary to break it down into subsections. The rice is placed in 4 discrete groups. Also, the rice is colored with food coloring to be either red, green, or blue. Red rice indicates the most significant digit, green the middle digit, and blue the least significant digit. Thus limiting the amount of rice on the burrito to a manageable level in respect to determining the data and fitting in the tortilla.

Data: Beef

The data will be transmitted in a beef representation of hexadecimal. Each beef cluster will be counted as a decimal representation of a hexadecimal digit. Each beef field will be separated by a slice of chicken. There will be a maximum of 15 chunks of beef and a minimum of 0 chunks of beef per unit chicken. Approximately 16 bytes of data can be stored per burrito packet.

Packet Routing

Should a node become damaged or congested (i.e. traffic jam, construction, etc) and be unable to accommodate Burrito encapsulated packets in a timely fashion then the packet will be routed by the delivery boy around any obstructions in an attempt to make a delivery inside of the packets given TTL.

Security Considerations

The IP over Burrito service can be considered secure for almost any non-tactical use. Before transmission, the data contents of the packet are sterilized, killing most viruses that might be transmitted via the packet. Unfortunately, due to the nature of the packet, this uninfected state is only temporary. Unlike the current IP transmission standard, packets created by the IP over Burrito Carrier service are vulnerable to infection during transmission. Infected packets will usually be detected two to four hours after the packet is destroyed.

As every packet is encapsulated in an opaque wrapper, the data inside the packet is impossible to access via standard packet sniffing procedures. Attempts to breach the encapsulation of the package in transit will likely cause permanent damage to the encapsulation, thereby signaling to the original recipients of the packet that data interception was attempted. Re-encapsulation of the original data is impossible, as the packet data is tightly integrated with the encapsulation. Due to the long delay between packet transmission and packet reception, however, there is sufficient time for a third party to duplicate the packet data and forward it to the original recipient. The detection of this interception is likely only if the recipient should follow the standard packet disposal process and be well acquainted with the peculiarities of packets created by a given server.

Packet transportation uses a highly advanced algorithm to prevent damage to the packet and to prevent its reception by third parties. As the packet transportation system is highly vulnerable to social engineering, however, the use of encryption is recommended for the transmission of any secure data.

Although the packets decay naturally over time, the slow rate of natural packet decay will likely make user-induced destruction mandatory to prevent third parties from examining the packet data after the packet has been received. Unfortunately, the packet delivery system works poorly in a tactical environment, as the packet can be easily waylaid by hostile forces.

Due to the extended time that packet creation requires, servers will be highly vulnerable to message flooding. and responses will be delayed greatly; however, the likeliness of a IP over Burrito DOS attack can be considered negligible, as the clients are charged for each packet that the server sends to them.

Of more concern is the extended time that packet processing requires on the receiving hosts end. Should a host attempt to process more than 5 packets a in a one hour period a buffer overflow could occur and data might be lost, or worse: it could be disseminated in a disorganized and partially processed state all over any nearby objects. This could result in damage to secondary systems and the server storage facility. Unfortunately a buffer overflow on one host can cause hosts in the immediate vicinity to suffer similar buffer overflows.

Also a matter of great concern is the ability of viruses to spread by IP over Burrito. Should the server or packet itself be infected then infection of the host is highly likely. When dealing with an unknown server it is advisable to carefully examine the packet for any sign of damage or infection (i.e. rotten smell, slick covering to the meat, etc).

IANA Considerations

This document has no actions for IANA.

Normative References

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

Authors' Addresses

Matthew Schulze
Paragon Systems International
1000 Windward Concourse Parkway, suite 140
Alpharetta, GA, 30005

EMail: Matthew.Schulze@mapics.com

William Lohsen
Georgia Tech Research Institute
347 Ferst Drive
Atlanta, Georgia 30332-0821

EMail: William.Lohsen@GTRI.gatech.edu

Full Copyright Statement

Disclaimer of Validity

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.