INTERNET-DRAFT
Intended Status: Informational
Expires: January 21, 2016

C. Byrne
J. Kleberg

July 20, 2015

Advisory Guidelines for UDP Deployment
draft-byrne-opsec-udp-advisory-00

Abstract

User Datagram Protocol (UDP) is commonly used as a volumetric attack transport on the internet. Some network operators experience surges of UDP attack traffic that are multiple orders of magnitude above the baseline traffic rate for UDP. Application developers should be advised that UDP is being rate-limited on a bits-per-second and packet-per-second basis by network operators to enforce known good baseline traffic levels for UDP. UDP has been abused to such an extent that legitimate use may become collateral damage and application and protocol developers should avoid using UDP as a transport when possible.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Table of Contents

1 Introduction

The User Datagram Protocol (UDP) [RFC0768] provides a minimal, unreliable, best-effort, message-passing transport to applications and other protocols (such as tunnels) that desire to operate over UDP [I-D.draft-ietf-tsvwg-rfc5405bis]. Since UDP does not establish an end-to-end connection at the transport layer, it is possible to carry out a source IP address spoofed distributed reflective denial-of-service attack (DRDoS)[ROSSOW]. Large amplification attacks have happened for years on a daily basis and are having a widespread negative impact on the internet [US-CERT].

2 Threat from UDP

Simplicity is the strength of UDP. Simplicity is also UDP's weakness. UDP allows a single packet response from an application. TCP [RFC793] and SCTP [RFC4960] operate differently. TCP has a three-way handshake and SCTP has a four-way handshake, and thus they verify the reverse path will accept the communication within the transport layer prior to the application layer engaging. Since UDP does not do any of this handshaking in the transport layer, the applications are left to create their own procedure for responding to network communication initiation. In the case of SNMP, NTP, CHARGEN, and DNS, a single spoofed IP packet can generate a much larger response to an attack target in many deployments. The result is that several of these UDP deployments covering millions of internet nodes allow an attacker to hide the true source of the attack and amplify the magnitude of the attack by reflecting off of widely deployed UDP services on the internet [ROSSOW].

3 Recommendations for Application and Protocol Developers

1. Application and protocol developers should avoid using UDP. The abuse of UDP for DRDoS on the internet has made UDP subject to aggressive filtering at the transport protocol level.
2. If UDP must be used, encapsulate it in IPsec [RFC4303] to avoid matching IP protocol 17 filters.
3. In the case of WebRTC [I-D.draft-ietf-rtcweb-transports], TURN [RFC5766] should be used to concentrate and manage a known-good UDP flows. It is also recommended that WebRTC evolve to support native SCTP transport.
4. In the case of QUIC [I-D.draft-tsvwg-quic-protocol] and other transport innovations, a new IANA assigned protocol number should be used to meaningful differentiates traffic from commonly abused UDP services.

4 Recommendations for Network Operators

1. To prevent the spoofed reflection attacks, all network operators should implement anti-spoof address filtering [RFC2827]. This prevents the trigger of the DRDoS.
2. Network operators should govern the types of systems that offer UDP services. This stewardship of directly attached nodes limits the fleet of nodes offering UDP services that could be abused for DRDoS.
3. Network operators should baseline and rate-limit UDP for bits-per-second and packets-per-second. This effort acts as protection mechanism to prevent unexpected large UDP flows that are highly likely to be DRDoS from propagating across the internet.

3 Security Considerations

The continued abuse of UDP is a material security threat to the availability of the internet. While mitigating the threat at the node implementation level would be ideal, years of experience has demonstrated this is not broadly effective. While improving overall network availability by limiting UDP, it is likely that several important protocols will be negatively impacted including DNS, DNSSEC, DTLS, SRTP, UDP encapsulated IPsec and others.

4 IANA Considerations

None.

5 References

5.1 Normative References

[RFC768] Postel, J., "User Datagram Protocol", RFC768, August 1980.

[RFC2827] Ferguson, P., D Senie., "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC2827, BCP38, May 2000.

[RFC4303] Kent, S., "IP Encapsulating Security", RFC4303, December 2005.

[RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, April 2010.

[ROSSOW] Rossow, C., "Amplification Hell: Revisiting Network Protocols for DDoS Abuse", https://www.internetsociety.org/sites/default/files/01_5.pdf

, February 2014.

5.2 Informative References

[I-D.draft-ietf-rtcweb-transports] Alvestrand,H., "Transports for WebRTC", draft-ietf-rtcweb-transports-09 (work in progress), July 2015.

[I-D.draft-ietf-tsvwg-rfc5405bis] Eggert, C., G. Fairhurst., G. Shepherd, "UDP Usage Guidelines", draft-ietf-tsvwg-rfc5405bis-03 (work in progress), July 2015.

[I-D.draft-tsvwg-quic-protocol] Hamilton, R., J. Iyengar, I. Swett, A. Wilk., "QUIC: A UDP-Based Secure and Reliable Transport for HTTP/2", draft-tsvwg-quic-protocol-01 (work in progress), July 2015.

[RFC793] Postel, J., "Transport Control Protocol", RFC793, September 1981.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC4960, September 2007.

[US-CERT] US-CERT,"Alert (TA14-017A) UDP-Based Amplification Attacks", https://www.us-cert.gov/ncas/alerts/TA14-017A, 2015.

Authors' Addresses

Cameron Byrne
Bellevue, WA, USA
EMail: Cameron.Byrne@T-Mobile.com

Jason Kleberg
Bellevue, WA, USA
EMail: Jason.Kleberg@T-Mobile.com