Network Working Group
Internet Draft
Intended status: Experimental
Expires: February 21, 2009

S. Guthery
HID Global

August 21, 2008

IP and ARP over Wiegand
draft-guthery-wiegand-ip-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes the transport of IP datagrams over the Security Industry Association standard [3] five-conductor cable called the Wiegand interface used for communication between card readers and control panels in physical access control systems.

Conventions used in this document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

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 RFC-2119 [1].

Table of Contents

1. Introduction

This document describes the transport of IP datagrams including ARP and ICMP messages over the five-conductor cable called the Wiegand reader interface that is used for communication between card readers and control panels in physical access control systems.

2. Wiegand Physical Layer

The physical and electrical properties of the five conductors on the Wiegand reader interface are described in the Security Industry Association standard AC-01, Access Control Standard Protocol for the 26-BIT Wiegand Reader Interface, dated October 17, 1996 [3].

Two of the five conductors on the Wiegand reader interface, power (from panel to reader) and ground, do not carry communication signals. Two of the remaining three conductors, called DATA0 and DATA1, carry digital data from the reader to the panel using what is known in the trade as the Wiegand Protocol. The remaining conductor, LEDCTL, carries a high-or-low indicator from the panel to the reader. It is used to provide access control feedback to the person, for example turning the color of a light-emitting diode on the reader to green to indicate that access has been granted.

Unlike most IP channels including birds and semaphores, the Wiegand channel is asymmetric at the physical layer. Typical implementations of the Wiegand standard block the transmission of any signal from the panel to the reader on DATA0/DATA1 and from the reader to the panel on LEDCTL.

The DATA0 conductor carries the 0's of a bit stream and the DATA1 conductor carries the 1's of the bit stream. DATA0 and DATA1 are half-duplex in the sense that there is never a signal on both of these conductors at the same time. The datalink protocol for transmitting bit streams from the reader to the panel on DATA0 and DATA1 is defined by AC-01.

LEDCTL is a 2-way switch. In the example usages described in AC-01, when voltage is low a red/green LED on the reader is to be green or a red LED is to be red. When voltage is high a red/green LED on the reader is to be red or a red LED is to be off. Because these light indications are intended to be observable by a human observer, the hold times for both levels are supraliminal and thus of 10ms or more.

The use of the LEDCTL line can therefore extended by saying that any signal from the panel to the reader on LEDCTL with a hold time of less than 10ms SHALL interpreted a data link signal in an asynchronous transmission protocol and not as a signal to change the state of the LED. Further details of this protocol are described in

the following sections.

3. Wiegand Data Link Layer

TTY ("mark-and-space") bit encoding on LEDCTL with one START bit, 8 character bits and one STOP bit and no parity bit (8N1) SHALL be used on LEDCTL.

All datalink frames SHALL be the same size.

SLIP packet framing within the Wiegand data link frame SHALL be used on DATA0/DATA1 and LEDCTL.

4. IP over Wiegand

IP datagrams over Wiegand SHALL be wholly contained within one datalink frame. IP over Wiegand does not support IP datagram fragmentation across multiple datalink frames.

The Version field SHALL be set to 4.

The Internet Header Length field SHALL be set to 5. No IP datagram options are supported by IP over Wiegand.

The Type of Service field SHALL be set to 0.

The Flags and Fragment Offset fields SHALL be set to 0.

The Protocol field SHALL be set to 61 ("any host internal protocol") in the case that the data field contains a proprietary or vendor-specific protocol packet; i.e. the packet of a protocol other than one with an IANA Assigned Internet Protocol Number.

5. ICMP Messages

The card reader SHOULD support ECHO REQUEST.

The card reader MAY support TIMESTAMP and TIMSTAMP REPLY.

The card reader and the control panel MAY support ICMP security failure messages (type=40) with the proviso that the message need not be restricted to the failure of a Photuris session key management protocol execution but rather to the execution of any security protocol known implicitly to both the card reader and the control panel.

6. ARP and RARP Message Format

A Wiegand network consists of a control panel together with all the card readers that are physically connected to it. Each physical connection is through an interface that has a 16-bit address on the control panel. A Wiegand network is structurally similar to the Logical IP Subnetwork (LIS) of ATM networks [9] since each of the card readers can communicate directly with the control panel but not with each other.

The Wiegand ARP/RARP protocol uses the same packet format as ARP for Ethernet. ARP packets shall be transmitted with the assigned Wiegand hardware type code, XX. ARP packets SHALL be accepted by a card reader only if received with this hardware type.

ar$hrd (16 bits) SHALL contain the Wiegand specified hardware type value, XX (decimal).

ar$pro (16 bits) SHALL contain the IP protocol code 2048 (decimal).

ar$hln (8 bits) SHALL contain 2.

ar$pln (8 bits) SHALL contain 4.

ar$op (16 bits) SHALL contain 1 for requests, 2 for responses.

ar$sha (16 bits) in requests SHALL contain the requester's interface address. In replies it SHALL contain the target node's interface address.

ar$spa (32 bits) in requests SHALL contain the requester's IP address if known, otherwise zero. In replies it shall contain the target node's IP address.

ar$tpa (32 bits) in requests SHALL contain the target's IP address if known, otherwise zero. In replies it SHALL contain the requester's IP address.

ar$atn (8 bits) is the octet length of following ar$uid.

ar$uid (n octets) in requests SHALL contain the requester's unique identifier. In replies it shall contain the target node's unique identifier.

Support for ARP and RARP by both card readers and control panels is OPTIONAL.

7. Card Reader Cache

The default entry in the route cache of card reader contains SHOULD be the control panel. A card reader MAY maintain a route cache that consists of solely of this entry.

8. Maximum Transmission Unit

The effective upper bound on the size of a Wiegand IP datagram is not determined by the properties of the link layer protocol but rather by the computational capabilities of card readers. Card readers considered in this document include those that use interrupts-off, software UART ("bit banging") techniques for low-level input and output. Since a card reader's primary responsibility is to respond to the presentation of a card, time intervals during which this is not possible SHOULD be minimized. Therefore the MTU for IP over Wiegand is set to the maximum datagram that all hosts must be prepared to accept, namely 576 octets.

9. IPv6 Considerations

It is desirable to be able to give each card reader and each control panel its own static IP address in the IT infrastructure within which the card readers and control panels are installed. Therefore it is expected that IPv6 will be more attractive than IPv4 for physical access control systems.

IPv6 requires that the MTU be at least 1280 octets. This requirement exceeds the design capabilities of today's Wiegand wire infrastructure. Therefore, this document does not foresee the use of IPv6 in the context it has considered.

10. Security Considerations

Security issues are not discussed in this document.

11. IANA Considerations

12. Conclusions

This document describes a realization of the Internet Protocol on the physical, electrical and logical characteristics of the Wiegand reader interface as described the Security Industry Association standard AC-01, Access Control Standard Protocol for the 26-BIT Wiegand Reader Interface, dated October 17, 1996. The realization is backward compatible with and maintains conformance to that standard.

13. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

References

13.1. Normative References

[1] Bradner, S., "The Internet Standards Process -- Revision 3", BCP9, RFC 2026, October 1996

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

[3] Security Industry Association, AC-01, Access Control Standard Protocol for the 26-BIT Wiegand Reader Interface, October 17, 1996

[4] Braden, R. "Requirements for Internet Hosts - Communication Layers", RFC 1122, October 1989

[5] Postel, J., "Internet Protocol", RFC 791, USC/Information Sciences Institute, September 1981

[6] Finlayson, R., Mann, T., Mogul, J., and M. Theimer, "A Reverse Address Resolution Protocol", STD 38, RFC 903, Stanford, June 1984

[7] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, USC/Information Sciences Institute, October 1994

[8] Postel, J., "Internet Control Message Protocol", RFC-792, STD 5, USC/Information Sciences Institute, September 1981

[9] Laubach, M. and J. Halpern, "Classical IP and ARP over ATM," RFC 2225, April 1998

[10] Karn, P., "ICMP Security Failures Messages," RCF 2521, March 1999

13.2. Informative References

Author's Addresses

Scott Guthery
HID Global
1320 Centre Street #201A
Newton Center, MA 02459-2497

Phone: +1 617 365 3059
Email: sguthery@hidcorp.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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