



1710 Walnut Street / KANSAS CITY, MO 64108

toll-free: (888) 732.9406

Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access

Prepared by:

FishNet Security
Security Consulting Services Team

December 2nd-6th, 2004

Securely Enabling Business

The information transmitted in this document is intended only for the addressee and may contain confidential and/or privileged material. Any interception, review, retransmission, dissemination or other use of or taking of any action upon this information by persons or entities other than the intended recipient is prohibited by law and may subject them to criminal or civil liability.

FishNet Security has conducted work associated with this report as an independent, third party vendor, and maintains no ownership or interest in the Client.

Copyright © 2005 FishNet Security. All rights reserved. The FishNet Security logo is a registered trademark of FishNet Security. All other products and company names mentioned herein are trademarks or registered trademarks of their respective owners.

| | |
|----------------------------------------------------|-------------------------------------|
| General Information | 1 |
| Company Background | 1 |
| Corporate Profile..... | 2 |
| FishNet Security Vulnerability Research Team | 2 |
| Executive Summary..... | 10 |
| Purpose..... | 10 |
| Perspective..... | 10 |
| Issues | 11 |
| Findings and Recommendations | 11 |
| Findings..... | 11 |
| Threat Vectors | 14 |
| Recommendations | 14 |
| Securing Cisco Switches/Voice Networks | 15 |
| Glossary of Terms | <i>Error! Bookmark not defined.</i> |

General Information

Company Background

Founded in 1996, FishNet Security has become one of the country's leading and most respected innovators in the network security industry. FishNet Security is focused exclusively on network security. Our roots are grounded in the engineering and technical aspects of network security as opposed to consulting firms that have ventured resources into the network security arena. Our business foundations offer strength and stability that set us apart from the "dot-com" model.

Commitment to our Customers

Headquartered in Kansas City, Missouri, FishNet Security is committed to being the largest network security company in the Midwest. In order to provide superior customer service, FishNet has regional offices in St. Louis, Dallas, Minneapolis, and Boston. Our management team works to ensure a high level of service through frequent and direct contact with our customers.

Engineering Expertise

FishNet Security offers a technical staff with experience, training and industry certifications such as Check Point Certified Security Expert, Cisco Certified Internetwork Engineer (CCIE), Certified Information System Security Professional, Microsoft Certified System Engineer and more. Our engineers are certified in industry leading security product lines, and in the networking, operating system and routing foundations that underscore successful implementations.

Corporate Profile

FishNet Security Vulnerability Research Team

The FishNet Security Vulnerability Research Team is comprised of highly technical employees and is designed to be flexible to meet the varying needs of FishNet and our clients. The following individuals participated in the vulnerability research on this project:

Jake Reynolds – Initial vulnerability discovery, exploit development, and threat analysis

Senior Security Engineer

Office: 816-421-6611

Cell: 913-710-1986

Email: jake.reynolds@fishnetsecurity.com

Ed Welsh – In-depth vulnerability analysis, exploit and automated PoC (Proof of Concept Code) development

Security Engineer

Office: 816-421-6611

Cell: 816-686-4261

Email: ed.welsh@fishnetsecurity.com

Brandy Peterson – 802.1x expertise

Chief Technology Officer

Office: 816-421-6611

Toll Free: 888-732-9406

Cell: 913-710-6863

Email: brandy.peterson@fishnetsecurity.com

| If you are: | Please refer to: |
|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| An executive who desires a quick overview of the findings and recommendations of the security assessment. | The Executive Summary at the beginning of the document. (The executive summary in this document is technical in nature). |
| A manager tasked with interpreting the findings of the assessment and deciding what action to take based on the recommendations. | The Findings and Recommendations section to briefly recap the scope of the assessment and general results and for a summary of the most important issues discovered during the assessment. |
| A technical staff member tasked with understanding the issues presented in the assessment and implementing specific recommendations. | The Findings and Recommendations section contains the specific technical details needed to understand the security issues raised by the assessment. |

Executive Summary

Purpose

FishNet Security has performed a partial security assessment on versions of Cisco IOS and CatOS switching software that include 802.1x layer-2 port security functionality, along with full vulnerability research regarding discovered vulnerabilities. A security assessment is the process of identifying security risks and baselining the security posture of a specific device or application.

Due to the time and complexity of assessing an entire platform only a partial assessment has been performed on the Cisco switch software. FishNet Security's assessment team does offer comprehensive evaluation to identify threats, vulnerabilities, and suggesting solutions to specific security issues. In addition, FishNet Security's assessment services team performs vulnerability research on previously unknown vulnerabilities discovered during the course of assessment activities. With this information an organization can design and implement a strategy to reduce overall risk exposure to its infrastructure and application(s).

Cisco has *not* contracted FishNet Security to conduct an independent application security assessment of Cisco switching platforms. The vulnerability research contained in this report was stimulated by and is the byproduct of other unrelated vulnerability research.

The purpose of the Cisco switch vulnerability research was to identify the root cause of inappropriate behavior observed in the Cisco switch software and identify whether it represented a vulnerability to the platform. Once the vulnerability was confirmed, the further purpose was to test and document this vulnerability and assist Cisco Systems in securing the switch software, thus protecting their customer base from abuse.

FishNet Security follows the Full Disclosure Policy v2.0 responsible reporting guidelines which may be found at <http://www.wiretrip.net/rfp/policy.html>. Under this policy, Fishnet Security expects to receive response from Cisco Systems within five days of receipt via email of this document confirming the vulnerability, and expects to be updated by appropriate parties every five business days until the issue is resolved. Once the issue is resolved, and both Cisco Systems and FishNet Security are satisfied with the solution provided for Cisco switch users, FishNet Security encourages joint disclosure of the vulnerability information and suggests that Cisco Systems credit FishNet Security's research and "fair play", acknowledging the volunteer work taken to thoroughly test and document these issues.

Perspective

All exploitive testing of the Cisco switch software was done blind, e.g. – as an unauthenticated, unauthorized user attempting to subvert the platform, and in this case, gaining unauthorized access to the voice VLAN.

Confirmation of exploitation and further research into the exact method to exploit the platform was performed as a fully authenticated, administratively authorized user. This access is, however, in no way needed to obtain full voice VLAN access to an 802.1x voice-enabled Cisco switch.

Access to the voice VLAN is predicated upon the attacked 802.1x-enabled switch interface being configured with the voice VLAN command.

The application assessment testing was conducted by FishNet Security in Kansas City, MO.

Issues

Voice VLAN access abuse is possible by spoofing Cisco Discovery Protocol (CDP) on voice-enabled Cisco switch interfaces even if 802.1x port-level security is enabled.

“802.1x can be used for two purposes in this module. It can help to ensure that hosts (or telephones) logging on to the building access module have proper authentication credentials, and it can apply per-user access control lists (ACL’s) to limit the network resources that can be accessed. This can be especially helpful to give guests Internet-only access, if they need to work from inside an enterprise for a short period of time.”

-Cisco Systems SAFE Blueprint for Enterprise Networks

802.1x Voice VLAN Access Issue: 802.1x port security provides a means of authenticating users and devices at the layer-2 access level before network connectivity is granted. There are three entities to an 802.1x system: a supplicant, which represents the device or user, an authenticator, which represents the device being accessed, and the authentication server, which represents the RADIUS or TACACS server providing authentication, authorization, and accounting (AAA) services. Finer network access control can be achieved using 802.1x port security by configuring the authentication server to provide per-user access control lists (ACLs) or per-user VLAN information for dynamically mapping users to access control lists and VLANs.

FishNet Security has performed research on 802.1x-secured ports that are also voice-enabled and has determined that access to the voice VLAN of these ports can be gained trivially by spoofing a CDP message in a specific fashion. The crux of the issue is that there are few IP phones that currently support an 802.1x supplicant as a means to provide user credentials in order to authenticate. In fact Cisco Systems is going above and beyond the norm in that it requires a specific message from a Cisco IP phone before voice VLAN is granted. Unfortunately it is trivial to bypass this. Cisco Systems uses CDP messages to identify IP Phones in order to give them access to the voice VLAN independently of data VLAN access by users or devices that have authenticated via 802.1x. A false sense of security in enterprises that use 802.1x port-level authentication and IP telephony together may be the result of this.

Detailed threat vectors and a summary of attack trees will be documented under findings, but the high-level summary of threat vectors is as follows:

1. Attacker gains physical access to an 802.1x-secured, voice-enabled port and spoofs a CDP message to impersonate a phone.
2. Voice VLAN access is granted and the attacker begins reconnaissance for eventual attacks on voice (or data) infrastructure components or any reachable applications.

Once access to the voice VLAN is gained there is really no limit to the amount or severity of attacks that can be mounted. These include:

- Eavesdropping of voice calls: Address resolution protocol (ARP) spoofing on switched Ethernet can allow the attacker to perform a man-in-the-middle attack (MITM) on hosts participating on the voice VLAN.
- Spoofing of a trivial file transfer protocol (TFTP) server: By acting as the TFTP server an attacker can arbitrarily change the configuration of any dependent voice devices.
- Spoofing of Voice Control Software (SIP Proxy/CallManager/Gateways): The role of critical voice infrastructure devices can be assumed.

Many of these attacks can be mitigated by some of the recommendations mentioned in the [Securing Cisco Switches/Voice Networks](#) section below. However, they would be better mitigated at layer-2 where no connectivity would be granted without proper authentication.

Findings and Recommendations

Findings

Cisco Systems produces many different models of switches that are 802.1x capable. Many of these switches also provide the capability to recognize and participate in the configuration of Cisco IP Phones. Cisco IP phones are designed to accommodate connected workstations so that only one network drop is required per user workspace. There are three possible base configurations of Cisco IP phone-enabled switch ports, one of which applies to this issue. These phones do not contain an 802.1x supplicant, which means that user or device credentials cannot be entered and provided to an 802.1x authentication server. This obstacle is compounded by the fact that voice services are usually required even in situations where there are no user workstations connected to the phones, such as during non-business hours or on non-workstation community phones, etc. This means that enterprises requiring 802.1x port security and user workstations chained to Cisco IP phones cannot rely on the users attached to the Cisco IP phones to authenticate for both the user and the phone if voice services are required in the absence of the user. This has lead Cisco Systems to provide an alternative means of identifying Cisco IP phones on 802.1x-enabled switch interfaces so that they can function independently of data services.

This issue is dependent upon the following conditions:

- Cisco IP phones are being utilized with user workstations connected to the PC Port of the phones.
- The switch interfaces are configured to separate voice traffic from data traffic on different VLANs.
- 802.1x port security is enabled on the interfaces connected to the phones.

The following configuration was used on a Cisco Catalyst 3560G-24PS-24 switch to validate the vulnerability

```
aaa new-model
aaa group server radius RADIUS
  server 192.168.1.100 auth-port 1812 acct-port 1813
!
aaa authentication dot1x default group tacacs+
!
interface FastEthernet0/4
  switchport access vlan 100
  switchport trunk native vlan 100
  switchport mode access
  switchport voice vlan 200
  no ip address
  srr-queue bandwidth share 10 10 60 20
  srr-queue bandwidth shape 10 0 0 0
  mls qos trust device cisco-phone
```

```
mls qos trust cos
no mdix auto
dot1x port-control auto
auto qos voip cisco-phone
spanning-tree portfast
!
radius-server host 192.168.1.100 auth-port 1812 acct-port 1813 key RADk3y
```

Although not every Cisco switching platform has been tested due to lack of hardware, it is assumed that this vulnerability applies to any Cisco switch platform that supports 802.1x port security and IP phone functionality on the same port.

FishNet Security has determined that Cisco Systems is using CDP messages to identify Cisco IP phones and allow access to the voice VLAN independent of the workstation's access to the data VLAN on 802.1x-secured ports. Further testing indicated that the switches identify IP phones on 802.1x-secured ports by matching a string found in a particular field in the CDP message that the phones generate upon connection to the switch-port. When a Cisco switch receives a CDP message with this particular string in the correct CDP field on an 802.1x-secured port, it allows access to the voice VLAN even if a user has not authenticated. Publicly available tools can trivially subvert this means of identification by spoofing these CDP messages to cause the port to enable access to the voice VLAN. Once this is done network access is gained, and there are many attacks that can be waged on the voice system if proper controls have not been put into place. Although it is against Cisco SAFE recommendations it is common for data VLAN hosts to be reachable from voice VLAN hosts due to poorly configured access control. In these cases access of the voice VLAN versus the data VLAN may be irrelevant.

The concept for the following exploit was inspired directly from a couple of small mentions of 802.1x port security using voice-enabled ports on Cisco System's website. It should be noted that Cisco Systems never claims that the voice VLAN is 802.1x authenticated in its literature. However, it does not directly state how trivial it is to gain access to the voice VLAN, which could potentially leave system administrators with the false impression that any access to that port from any device other than an IP phone must be securely authenticated via 802.1x.

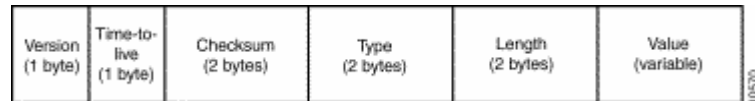
"Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port."

"A voice VLAN port becomes active when there is link, and the device MAC address appears after the first CDP message from the IP phone. Cisco IP phones do not relay CDP messages from other devices. As a result, if several Cisco IP phones are connected in series, the switch recognizes only the one directly connected to it. When 802.1X is enabled on a voice VLAN port, the switch drops packets from unrecognized Cisco IP phones more than one hop away."

-Configuring 802.1x Port-Based Authentication

http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00801a6c72.html

CDP Packet Format:



Exploiting this weakness in allowing access to voice VLANs on 802.1x-secured ports involves the following steps:

1. Gain physical access to an 802.1x-secured port that is also voice-enabled.
2. Plug a machine that supports 802.1q trunking directly into the switch-port.
3. Passively sniff traffic until an 802.1q encapsulated frame tagged with the VLAN ID of the voice VLAN arrives on the port.
4. Create an 802.1q subinterface to participate on this VLAN.
5. Inject two specially crafted CDP packets with the correct string placed in the correct field. Access to the voice VLAN is now granted.
6. Inject one CDP packet every minute or so such that the CDP entry does not time out of the connected switches CDP table.
7. Send a DHCP request on the voice VLAN in an attempt to get an address or statically assign one if DHCP fails.

If all of this is successful then attacks can be mounted on the network infrastructure and phone system. The TFTP server can be easily discovered by looking at the DHCP response and spoofed such that the configurations of all phones can be arbitrarily configured. Voice calls can be monitored by ARP spoofing or port stealing if proper switch configuration is not followed. The amount of attacks are virtually limitless.

Voice VLAN Access Proof of Concept Code: Proof of Concept script code has been written that trivializes the automated exploit of this vulnerability.

Threat Vectors

Attack against 802.1x-secured, voice-enabled Cisco switch interface:

- Physical access to the port either directly or through a patch, requirements: depends on environment, risk: LOW-HIGH
- 802.1q trunking support on the attacking host, requirements: trivial, risk: HIGH
- Employment of a CDP generator, requirements: trivial, risk: HIGH

Attack against non-802.1x-secured, voice-enabled, tagged Cisco switch interface:

- Physical access to the port either directly or through a patch, requirements: depends on environment, risk: LOW-HIGH
- 802.1q trunking support on the attacking host, requirements: trivial, risk: HIGH

Attack against non-802.1x-secured, voice-enabled, untagged Cisco switch interface:

- Physical access to the port either directly or through a patch, requirements: depends on environment, risk: LOW-HIGH

Recommendations

Workaround: There is no way to enforce 802.1x authentication of voice network access unless the voice devices used employ an 802.1x supplicant. Measures can be put into place such as 802.1x and MAC address-based port security but these are not effective against protecting voice VLAN access. Physical security of the premises could be increased to provide protection from unauthorized personnel attacking switch ports but these do nothing to stop attacks from employees.

A Better Means of Identifying Phones Must be Used: It is important to note that the 802.1x-secured voice-enabled interfaces provide the most protection out of all of the different configurations of voice-enabled interfaces. However, the method that Cisco switches use to identify Cisco IP phones allowing voice VLAN access on 802.1x-secured ports is not only insecure but trivially exploitable. Use of a Public Key Infrastructure (PKI) with x.509

certificates on each phone and 802.1x would allow cryptographically secure authentication of access to the voice VLAN by these devices without the need for a user to enter a username and password every time 802.1x authentication was required.

Cisco CallManager 4.0 provides station authentication via certificates if 7970 series Cisco IP phones are used. The other versions of phones that Cisco manufactures do not support this authentication method. Even still, this does not provide link-level authentication and leaves the rest of the network infrastructure to defend itself from attacks waged from unauthorized access of the voice VLAN.

"New industry-standard digital certificates in Cisco CallManager 4.0 confirm the identity of network devices to help protect against entry of rogue system users."

- Cisco Earns Top Rating in Challenging VoIP Security Test

http://newsroom.cisco.com/dlls/2004/prod_052604.html

Securing Cisco Switches/Voice Networks

This section describes techniques for locking down access to various Cisco devices that might be vulnerable to unauthorized access through voice VLAN access abuse. Additionally, certain security features that Cisco switches are capable of that can successfully mitigate certain attacks are mentioned. This is not intended to be a step-by-step implementation document; rather, it outlines high-level changes that can be implemented to help an organization minimize its risk in the event that an attacker gains unauthorized access to a voice VLAN.

There are two groups of changes, Standard and Advanced. The Standard set requires less effort, and the changes should be implemented by most administrators. The Advanced set is more complex in terms of implementation and ongoing management, and the changes should be evaluated and implemented if they are deemed necessary.

Standard

Separate Voice VLANs from Data VLANs: There are several reasons to do this. The first is that 802.1x port level security cannot be applied to interfaces on Cisco switches that do not split these VLANs. In addition, it is just good practice to separate the two networks by purpose so that inter-network access can be filtered by firewalls or access lists placed between them.

Enable 802.1x Port-Based Authentication: This will at least protect the data VLAN if it is properly filtered from voice networks. Improvements need to be made either to the phones, the authenticators, or both to ensure that the voice VLAN is treated similarly.

Disable Telnet Access on Phones: Telnet access to IP phones can be globally disabled to prevent the attacker from accessing them via this method.

Always Use Cryptographically Secure Management Protocols: Since access to the voice VLAN is so trivially gained as shown above, telnet and other clear-text management protocols that divulge sensitive information such as configurations, community strings, and passwords should be disabled and replaced by encrypted management protocols such as SSH, HTTP over TLS, and SNMP v3. ARP spoofing on the Voice VLAN could allow an attacker to capture administrative credentials or other sensitive information if it is sent in the clear.

Disable Administrative Access to Network Infrastructure From Voice VLAN: ACLs should be used to limit telnet, SSH, HTTP, and SNMP access to network infrastructure devices from the voice VLAN. This will prevent attackers from potentially gaining unauthorized access to these devices.

Configure Dynamic ARP Inspection: Dynamic ARP inspection should be configured to ensure that ARP spoofing/poisoning does not occur. Poisoning local hosts' and default gateways' ARP cache allows an attacker to perform a MITM attack. Dynamic ARP inspection configures the switch to inspect ARP traffic for valid IP to MAC mappings on untrusted ports.

Configured DHCP Snooping: DHCP snooping can help prevent DHCP server spoofing and other DHCP-related attacks including using a static address.

Configure Port Security: Limiting the number of MAC addresses that are allowed to appear behind a single interface prevents an attacker from overwhelming the switch CAM (content addressable memory) table and gaining access to other VLANs. This limit needs to be two or more on a port enabled for IP phones and users.

Configure Storm Control: Limiting the amount of multicast and broadcast traffic forwarded by a port is an easy way of ensuring that DOS attacks are not possible using non-unicast traffic. Best practices mandate that Cisco voice-enabled ports trust the COS value of incoming frames. This is because Cisco IP phones automatically mark time-sensitive voice traffic. If QOS is configured to allow these frames to be sent with priority then DOS attacks may be possible if an attacker floods a switch with traffic tagged with the correct COS values on the voice VLAN.

Configure Proper Filtering Between Networks: Many of the attacks described in this paper are dependent upon lack of proper filtering between the voice VLAN and other networks. Use of a firewall, access control lists, or VLAN access control lists can significantly reduce the risk posed by unauthorized voice VLAN access. See the [Cisco SAFE: IP Telephony Security in Depth](#) white paper for more details regarding this.

Advanced

Configure Ports as Protected: This functionality ensures that a switch port only communicates with non-protected ports, which isolates ports configured this way from each other. This can prevent eavesdropping and MITM attacks through ARP spoofing but also prevents users on the same switch from directly reaching each other.

