



Systems and Network Analysis Center
Information Assurance Directorate

Cisco Unified Presence Server (CUPS)

What is CUPS?

The CUPS is a major component of Cisco's Unified Communications (CUC) solution. It provides a standards-based platform that collects information from multiple sources about user availability and communications capabilities to provide presence status and facilitate presence-enabled communications with the CUC and other critical business applications.

CUPS Functions

The main function of the CUPS is to provide presence information about each user. Presence information includes the logical location, availability, and methods of communication for each user. The methods of communications include phone, video call, IM, or email. Before presence information for a user is disseminated, the CUPS verifies that only an authenticated user receives this information.

Cisco uses a standardized protocol known as SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) to distribute presence information and communicate with Cisco's Unified Presence Client (CUPC). SIMPLE is also used to communicate with Microsoft's Office Communicator (MOC) or any other client that supports SIMPLE. By using a standard based protocol, the CUPS can easily communicate with other organizations via a function Cisco calls federation. A federation is defined as any distribution of presence information that crosses a trust boundary, for example, when two companies wish to share presence information with each other.

Once a federation link is configured all users from one company will have the ability to add users from the other company to their buddy list.

Risks of Using CUPS

Introducing the CUPS to a network presents several security risks. The most obvious risk is that the CUPS will automatically pull information from MS Outlook calendar and any information that the user posts on their client. This information will then be disseminated to anyone who wants to know the location of a user. Also, external users may gain access to this information if a federation link or the network perimeter is improperly secured.


Securing CUPS

Most of the security risks presented by the CUPS can be mitigated. Proper configuration of user groups and access permissions on the CUPS can control which users can view the presence information of other users. Also, if proper perimeter security techniques are used, then only connections to the CUPS from "trusted" Internet Protocol (IP) addresses will be permitted. Given the use of SIP trunks to communicate with other CUPS, a Session Border Controller (SBC) is also an effective perimeter device to defend against outside attacks.

The CUPS also provides the option of using encryption to communicate with clients and other CUPS. Using encryption will provide confidentiality and integrity of user traffic, preventing an insider from sniffing the



The Information Assurance Mission at NSA



wire for information. Encryption will also prevent external attacks, because the CUPS and clients will only accept properly encrypted traffic.

Instant Messaging

Support for Instant Messaging (IM) is one of the primary functions of the CUPS. All IM messages are sent to the CUPS, and the CUPS forwards these messages to the end user. IM uses SIMPLE, which is an unauthenticated client/server protocol used to pass the IM messages. Given this lack of authentication, IM may be vulnerable to message spoofing, social engineering, and sniffing of messages. Enabling encryption mitigates most of these attacks. Also, proper measures should be taken to protect the network perimeter from outside attacks.

Computer Telephony Integration (CTI)

Cisco uses CTI to manage and control a desktop phone from a computer. This feature allows Cisco to provide presence information about a user based on the phone's state. These states include "On hook", "Off hook", "Incoming Call", and "Outgoing call". Also Cisco uses CTI to control the phone through CUPC or MOC. This provides a method for the user to click on another user's name in CUPC and place a call while directing the audio to the phone sitting on the user's desk.

Impact to Network Security

If a Cisco VoIP solution is already in place and the recommendations in the SNAC's "Recommended IPT Architecture" document were followed, then it is a properly secured telephony system. The "Recommended IPT Architecture" document is available on NSA.gov. Introducing the CUPS into this IPT architecture will require relaxing some of those defenses and replacing some others.

The largest restriction that must be relaxed is the separation of the voice and data networks. A secured voice and data network would only allow the phones to communicate with the Cisco Unified Communications Manager (CUCM) and prevent any computer from accessing these servers. With the addition of IM, CTI, and softphones, the computers now must be able to communicate with the CUCM and the CUPS.

By allowing a computer to communicate with the CUCM and the CUPS it opens up a new avenue of attack for an insider. An insider may use this additional access to attack the CUCM and the CUPS, or to sniff phone calls on the network.

Also, in most enterprise networks the VoIP network does not communicate with the business servers. By adding the CUPS and implementing the CUC, the CUPS and the CUCM will need to communicate with the Active Directory (AD) server and the email server. This means that exploiting the CUCM or the CUPS could lead to a compromise of the email and AD servers.

Relaxing the lines of separation requires additional measures be taken to properly secure the network. The encryption provided by the CUPS and the CUCM should be implemented wherever possible to prevent attacks. Access Control Lists (ACLs) or firewalls should also be put into place to ensure that only necessary traffic is being passed between the different security zones. Generally, the only types of traffic that should be allowed between desktops and the CUPS are signaling, IM, presence updates, and logon information. Finally, only media sessions should traverse between a desktop and a phone for conversations.



Systems and Network Analysis Center

410 854-6632 • DSN: 244-6632 • FAX: 410-854-6604

SNAC DoD, 9800 Savage Rd. Ft. Meade, MD 20755-6704

www.nsa.gov/snac

SNAC@radium.ncsc.mil