Achieving Truly Secure Cloud Communications

How to navigate evolving security threats

NetFortris

Security is quickly becoming the primary concern of many businesses, and protecting VoIP vulnerabilities is critical. Organizations must fully understand the different types of threats in order to combat them effectively.

Common VoIP Security Threats:

Call Fraud
Eavesdropping
Phreaking
Malware and Viruses
Denial of Service Attacks
Call Hijacking

VoIP Call Fraud

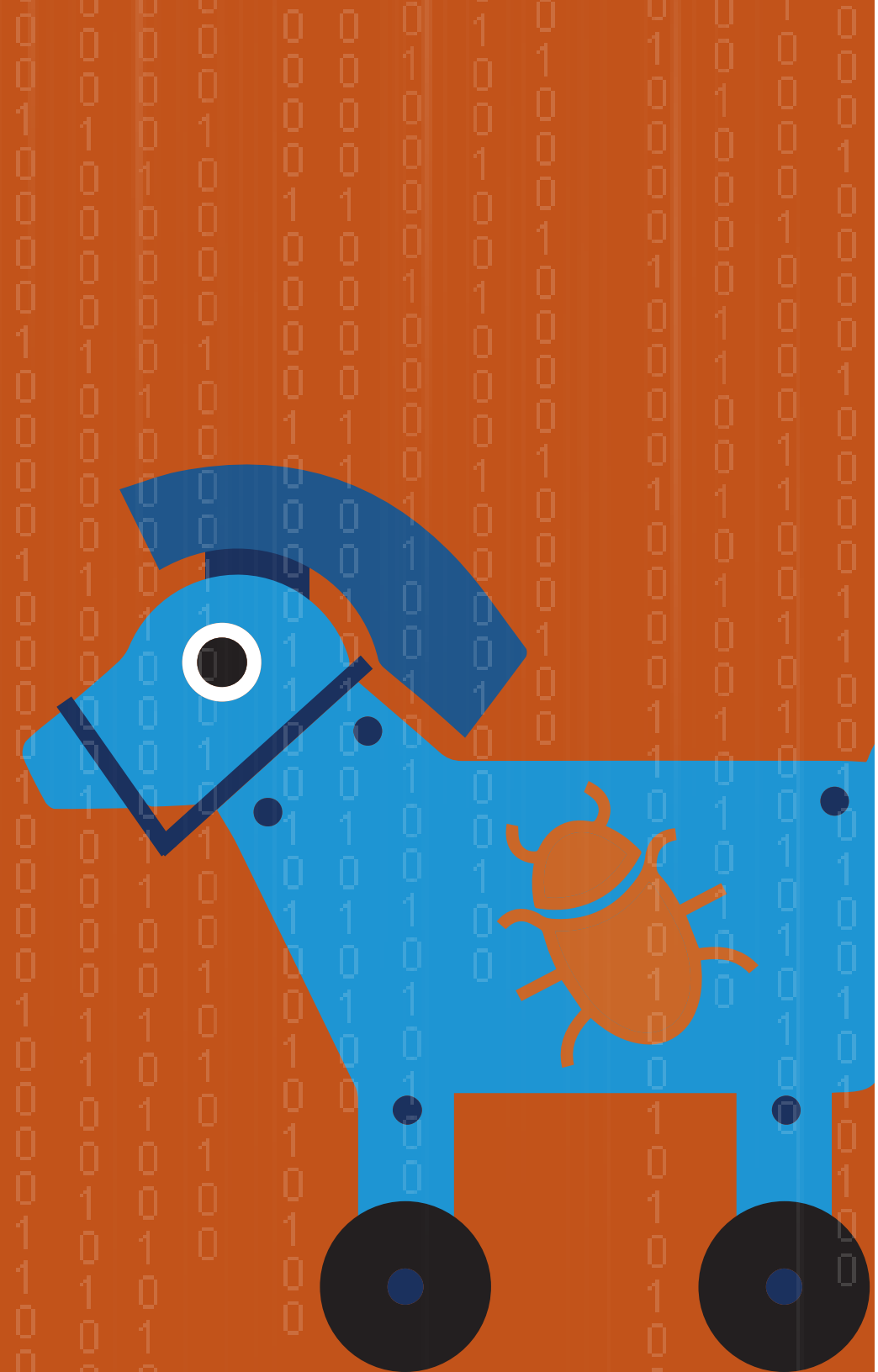
Call fraud involves tapping into a VoIP line and commandeering it to make unauthorized calls. The two main types are eavesdropping and phreaking.

Eavesdropping

Eavesdropping on VoIP calls is a tool used in identity theft, VoIP service threat (also called VoIP fraud), and corporate sabotage. Hackers tap into VoIP phone calls, listening to steal employee names, passwords, phone numbers, and other information that can give them access to voice mail, billing information, and other sensitive business or customer information.

Phreaking

In contrast to eavesdropping, phreaking is when hackers gain illegitimate access to a business's VoIP service provider information, stealing account numbers, access codes, and other proprietary information. They use this to either add unauthorized phone lines, or make calls on existing VoIP lines. Both result in excessive charges that are most often discovered when businesses receive an unpleasant provider bill.



Malware, Worms, and Viruses

Cloud communication services utilize software and soft phones and as a result, are vulnerable to attack by malware, malicious software worms, and other computer network viruses. These viruses often take a computer system hostage and allow hackers to send spam or other types of malicious data. Some worms can specifically target information, destroying it without the possibility of recovery. They can also trace key strokes or data entry, allowing remote access of a business's computer or phone system. Hackers can then copy sensitive files and obtain credit card information. This is especially worrisome for businesses who handle customers' financial data such as credit cards or account numbers.

Denial of Service Attack

Denial of Service (DoS) attacks occur when a network or server is flooded with information, consuming all available bandwidth and preventing incoming and outgoing VoIP calls. When a system is hijacked by a DoS attack, hackers can gain remote control of administrative servers to steal sensitive business or customer information and abuse VoIP services, making expensive phone calls on a business's service account.

VoIP Tampering and Call Hijacking

With VoIP call tampering, noise packets are sent over the network to interrupt the communication stream, causing poor call quality, dropped calls, and delays in voice signal. VoIP call signals are vulnerable and can be intercepted by a malicious third party who changes the encryption key of the call's digital signature. This change tricks VoIP servers into thinking that the two original parties are still in communication and gives the hacker the opportunity to cause serious communication problems.

VoIP Security Measures

Encryption

Most cloud communication solution providers give customers guidelines for encryption and authentication protocols, and many offer encryption as an additional service. While all businesses should work to ensure ultimate customer protection, several specific industries must take extra measures. Retailers and other businesses that deal with sensitive customer data, as well as financial services firms and similarly regulated organizations, must ensure that all network data is encrypted, or else face serious penalties and consequences. Encrypted sensitive data that flows over an end-to-end VPN or MPLS network secure.

Authentication Protocols

VoIP authentication protocols vary based on the type of data being transported. They range from a typical password authentication procedure, to a complex three-way authentication process that protects servers and business VoIP from malicious attacks.

Password Authentication, also called the two-way handshake, sends a password across an Internet , VPN or MPLS network link. It tells the server the user name and password entered by the end user. Users gain access and the ability to place VoIP phone calls only when the password entered matches the one on file with the server. If the password does not match, the server rejects the request and denies VoIP access.

Password Authentication is highly vulnerable to attack and can be easily exploited. Many times the user name and password are not sufficiently disguised or encrypted before they are sent across the link. This risk is reduced significantly by utilizing a VPN or a secure MPLS network rather than the open Internet.

Challenge, Handshake Authentication Protocol (CHAP)

When the calling client (computer or soft phone that sends data and initializes a VoIP call) links with the authenticator application located in the VoIP server, the authenticator uses a three-step process to determine legitimacy. Also called a three-way handshake, this protocol grants or denies access.

Step 1. Challenge

The authenticating server creates a simple text message or data packet and sends it back to the calling client.

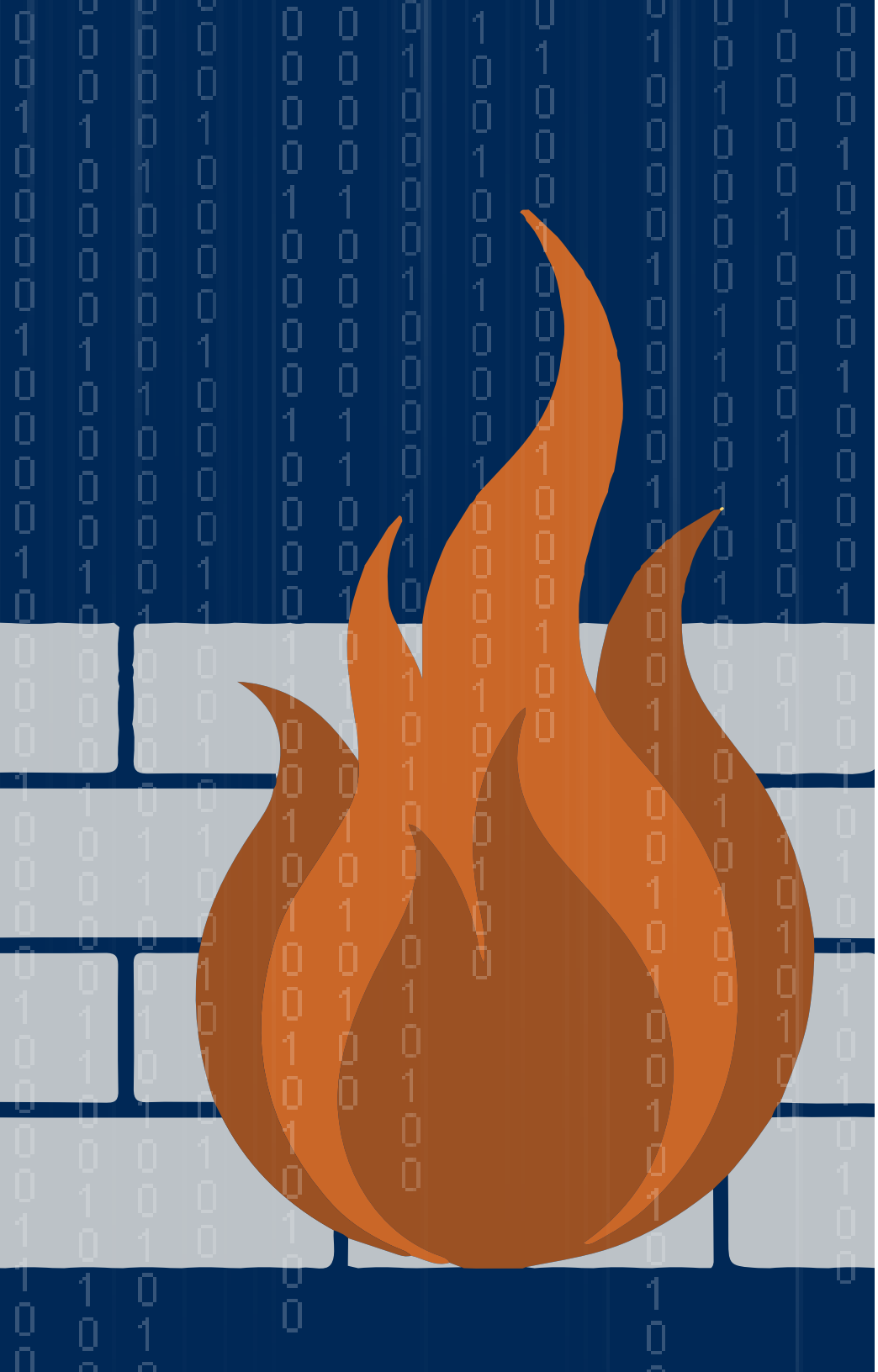
Step 2. Response

The calling client sends a password or code that is known to the authenticator. It encrypts the message sent during the challenge phase and then sends it back to the server authenticator.

Step 3. Success or Failure

The server authenticator encrypts the challenge text to see if the results match the calling client message. If the calling client has the correct password (or encryption key), the authenticator sends a "success" message and grants access. An NCP link can then be established and the server can host VoIP phone calls.

If the encrypted messages do not match, a failure message is sent, and access is denied to prevent VoIP calls from being made. While there are other ways of implementing CHAP, this is one of the most effective and commonly used methods.



Anti-Virus Software

VoIP softphones are a part of office computer systems. As a result, it is critical to protect them from viruses and other dangerous third-party programs. These viruses often enter an organization's VoIP system through email and then attack existing security protocols to interrupt or suspend VoIP network services entirely. Installation and maintenance of anti-virus and anti-malware software programs like firewalls are critical first steps in protecting VoIP hardware from third-party attack.

Often, VoIP vendors or network providers offer anti-virus software, also known as unified threat management software, as part of their service offering. Be sure to check with your provider for available options.

Deep Packet Inspection

Deep Packet Inspection (DPI) locates, identifies, and classifies data packets through packet filtering. It can reroute, or even block, incoming packets with unidentified code or forbidden data, deterring unauthorized use of your wide area, local area, or VoIP network. DPI protocols monitor all incoming media and signaling streams, as well as all outgoing media streams, for altered or inserted data packets and then flags them for review.

VoIP service providers maintain protocols that classify flagged data packets with priority ratings from high to low. This allows them to route data accordingly. High priority flags can be rerouted or completely blocked by the client caller. VoIP providers also use DPI to improve network performance and stopping peer-to-peer abuse that may result from VoIP fraud.

Session Border Controllers (SBC)

Session border controllers are devices used in VoIP networks to control media streams and protocol signals. Functionally, they start, conduct, and stop VoIP voice calls. SBCs adhere to quality of service protocols (QoS) and ensure the safety and best possible voice quality of all VoIP calls.

Stringent Authorization Policies

In addition to these practices, businesses can secure VoIP lines by performing audits and creating call restrictions. By auditing administrative accounts and employee user sessions, organizations can keep track of VoIP activity and monitor accordingly. They can ensure that none of the lines are being tapped or accessed by unauthorized entities for malicious purposes.

Restrict VoIP Calls to Prevent Abuse

Businesses should also secure the configuration of VoIP apps by creating white lists of approved country codes for employee usage. This type of list prevents toll fraud and the occurrence of other types of unauthorized activity. Network administrators should configure VoIP settings to establish call restrictions with only approved country codes in order to keep VoIP services and networks as secure as possible

Utilizing VoIP security tools and current control protocols is the best defense against network attack. These measures ensure the continuity of a business's Internet-based telecommunications and protect sensitive, proprietary information from abuse.

Partnering with the right provider enhances an organization's ability to counteract these evolving network threats. To learn more about NetFortris Cloud Communications solutions, please visit our website.

www.netfortris.com/cloud-communications

NetFortris