GENERAL HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES
OFFICE OF THE DEPUTY CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, J6
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: 2016-04

Understanding Voice over Internet Protocol (VoIP)

Image from linkedin.com

What is VoIP?

Voice over Internet Protocol (VoIP) is a form of communication that allows you to make phone calls over a broadband internet connection instead of typical analog telephone lines. Basic VoIP access usually allows you to call others who are also receiving calls over the internet. Interconnected VoIP services also allow you to make and receive calls to and from traditional landline numbers, usually for a service fee. Some VoIP services require a computer or a dedicated VoIP phone, while others allow you to use your landline phone to place VoIP calls through a special adapter. VoIP is becoming an attractive communications option for consumers. Given the trend towards lower fees for basic broadband service and the brisk adoption of even faster internet offerings, VoIP usage should only gain popularity with time. However, as VoIP usage increases, so will the potential threats to the typical user. While VoIP vulnerabilities are typically similar to the ones users face on the internet, new threats, scams, and attacks unique to IP telephony are now emerging.

VoIP configurations

Dedicated routers

These devices allow you to use your traditional phone to place VoIP calls. They are connected to cable/DSL modems (or any high-speed internet source) and allow you to attach an ordinary telephone. Once configured, and with an appropriate VoIP provider and service plan, these devices require no special software or interaction with a computer. In fact, you only need to pick up your phone and dial a number at the dial tone. You also may bring your adapter with you when you travel and make calls wherever broadband internet access is available.

In case of any cyber-related incidents, report immediately to the AFP Computer Security Incidents Response Team (AFPCSIRT), Cyberspace Security Group, CEISSAFP, at AFPTSN 911-6001 local 5873.

Adapters (USB)

These devices also allow you to use a traditional phone to place VoIP calls. They usually come in the form of USB adapters that are slightly larger than the typical thumb drive. They feature a standard modular phone jack to which you can attach an ordinary phone line. Once connected, your phone behaves as if it were connected to standard phone service. Behind the scenes, however, the included software is actually setting up a VoIP call.

Software-controlled VoIP applications: "softphones"

There are many software applications ("softphones") that allow you to place VoIP phone calls directly from an ordinary computer with a headset, microphone, and sound card. Internet telephony service providers usually give away their softphones but require that you use their service. Together, these applications and services enable users to talk to other people using the same service at no cost, and to the rest of the world for a fee. Software-based VoIP applications are quite attractive to consumers because they often already have most of the components necessary to get started at little to no cost.

Dedicated VoIP phones

A VoIP phone looks like an ordinary corded or cordless telephone, but it connects directly to a computer network rather than a traditional phone line. A dedicated VoIP phone may consist of a phone and base station that connects to the

internet or it may also operate on a local wireless network. Like the VoIP adapters mentioned above, dedicated VoIP phones also require a provider and service plan.

Requirements, Availability, and Service Limitations

When considering VoIP service, you should not assume that its features, functionality, and options will equal those of traditional landlines; you should be familiar with the requirements, availability, and possible service limitations of VoIP service before switching to VoIP as either a primary means of communication or an enhancement to your current services.

Requirements

VoIP requires a connection to the Internet through an ISP, a VoIP service to extend the reach to traditional landlines, and VoIP software to actually place calls. Plain Old Telephone Service (POTS) requires none of these prerequisites. It is important to note that Digital Subscriber Line (DSL) internet service uses traditional phone lines for your internet connection; in this case, you already have telephone service to begin with. You may wish to weigh the expected benefits of VoIP against these costs given your current operating environment.

Availability due to power outages

During a typical power outage, VoIP becomes unavailable because VoIP devices (computers, routers, adapters) usually rely on a power source to function. Traditional phone lines are usually still available during such an outage, which is a major advantage in an emergency. Ultimately, it may be necessary to use an uninterruptible power supply (UPS) with a VoIP installation if connectivity is desired during a power outage or some other kind of emergency.

Availability due to bandwidth

VoIP communication nearly always requires a high-speed (broadband) internet connection for reliable functionality. Even given typical broadband connection speeds, though, service interruptions or degradation of quality is possible due to high internet traffic. For example, if you are trying to place a VoIP call while other people are using a lot of bandwidth on the same internet connection, the sound quality of your VoIP call or general VoIP availability may be affected.

Threats / Risks

Many of the threats associated with VoIP are similar to the threats inherent to any internet application. Internet users are already familiar with the nuisance of email abuse in the form of spam and phishing attempts. VoIP opens yet another pathway for these annoyances, which can lead to spam over internet

telephony (SPIT), spoofing, and identity theft. Additionally, the confidentiality of VoIP conversations themselves has come into question, depending on service type or VoIP configuration.

Spam over internet telephony (SPIT)

As VoIP usage increases, so will the pesky marketing strategies associated with it. Perennial annoyances like telemarketing and spam have been plaguing consumers and internet users for years. A new sort of hybrid of these two concepts is SPIT, or spam over internet telephony. Like email spamming, sending commercial messages via VoIP is fast and cheap. Unlike traditional telemarketing, though, VoIP offers the potential for large volumes of unsolicited calls, due to the wide array of tools already available to attackers on the internet. Telemarketers could easily send large amounts of messages to VoIP customers. Unlike traditional spam email messages, which average only 10–20 kilobytes in file size, unwanted VoIP voicemails can require megabytes of storage.

Spoofing

It is technically possible for an attacker to masquerade as another VoIP caller. For example, an attacker could possibly inject a bogus caller ID into an ordinary VoIP call so that the receiver believes the call to be coming from a known and trusted source (a bank, for example). The receiver, fooled by the electronic identification of the caller, may place unwarranted trust in the person at the other end. In such an exchange, the receiver may be tricked into disclosing personal information like account numbers, social security numbers, or secondary authentication factor: a mother's maiden name, for example. This scheme is essentially the VoIP version of traditional phishing, where a user follows links in an unsolicited email and is tricked into providing personal information on a bogus web site. Attackers may use these bits and pieces of personal information to complete partial identity records of victims of identity theft.

Confidentiality concerns

Many critics of VoIP question its confidentiality. The concern is that VoIP data sometimes travels unencrypted over the internet. Therefore, it is technically possible for someone to collect VoIP data and attempt to reconstruct a conversation. Although it is extremely difficult to achieve, some software programs are designed to piece together bits and pieces of VoIP data in an effort to reconstruct conversations. While such activity is currently rare, you should be aware of this possibility as it may increase as VoIP becomes more widespread.

How to Protect Against Risks

Many of the principles and practices for safe VoIP usage are the same as those you may already be practicing with other internet applications. Ignoring these general principles could allow attackers to gain control of your computer operating

system by means of an existing software flaw or a misconfiguration unrelated to your VoIP application. It may then be possible for them to exploit flaws in your VoIP configuration, thereby possibly gaining access to personal information you share when using VoIP. Here are some of the key practices of good personal computing:

- **Use and maintain anti-virus and anti-spyware programs.**
- **Be cautious about opening files attached to email messages or instant messages.**
- **Verify the authenticity and security of downloaded files and new software.**
- **Configure your web browser(s) securely.**
- **Use a firewall.**
- **Identify, back-up, and secure your personal or financial data.**
- **Create and use strong passwords.**
- **Patch and update your application software.**
- **Do not divulge personal information to people you don't know.**
- **If you are using a software VoIP application, consider using encryption software for both your installation and for those you wish to talk to.**

In case of any cyber-related incidents, report immediately to the AFP Computer Security Incidents Response Team (AFPCSIRT), Cyberspace Security Group, CEISSAFP, at AFPTSN 911-6001 local 5873.

Reference:

- This was cross-posted from https://www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf as referenced by CMB, G6 PA Cyber Security Bulletin #47 with minor additions/modifications