

Why Over 90% of VoIP (Computer Phone) Services Are Vulnerable to Attack

Vulnerable to Attack

By Dee Scrip

© All rights reserved. Dee Scrip

You are in the crosshairs as a primary target of computer hackers if you own a computer or operate on un-secure VoIP (computer phone) services.

John Ashcroft, Attorney General, in remarks at the High Technology Crime Investigation Association 2004 International Training Conference held on September 13, 2004 stated, "We have seen worms and viruses attack...disrupting basic services...And with the increased use of the Internet and especially peer-to-peer networking, we have seen malicious code spread more quickly and infect more personal computers than ever before. The cost of these worms, viruses, and denial-of-service attacks...reaches into the billions of dollars."

In an article written by Daniel A. Morris, Assistant US Attorney, Computer and Telecommunications Coordinator with the District of Nebraska stated in "Tracking a Computer Hacker", that the "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

Ralph Echemendia, head of Intense School which trains executives regarding network security risks, stated that "Telecom providers are one of the main targets for malicious attackers because they control communications for everybody."

Sophisticated hackers have learned how to tap into sensitive information traveling on the Internet, and their focal point is communication.

How is this possible?

It is fairly simple. First, you should be aware that email services operate off of email servers, and web services operate off of web servers. Both email servers and web servers are built for data and not for voice.

Because VoIP has voice, it requires a system that will convert the voice into data packets to travel across the Internet, and then convert back to voice at destination. However, VoIP should not be considered just another application residing on a data network, as it necessitates a real time service due to performance expectations (e.g., quality of sound).

The majority of VoIP computer phones require a minimum of 20 kps (kilobytes per second) of bandwidth (information carrying capacity) for data packets to travel across the Internet, which is why most require a minimum high speed Internet connection in order to function without corrupting the quality of the voice.

Although in the minority, a few VoIP computer phone providers, some of which are reputable, require a minimum of less than 10 kps (kilobytes per second) of bandwidth (information carrying capacity), which is why their services can be used with dial-up connections or high speed (e.g., cable), satellite, and wireless connections.

Over 90% of VoIP services operate using industry standard codec (encryption codes) and industry standard protocols.

Computers are assigned a different numeric Internet Protocol (IP) address while on line, which is analogous to mail where you would have an identity location with your street number, city, state and zip code.

Relative to a protocol, the IP (Internet Protocol) address is a number that identifies the user and their computer. Industry standard codec and industry standard protocols are open and interpretable to the public. Unscrupulous hackers frequently launch their attacks against VoIP (Voice over Internet Protocol) services that operate on these publicly open and interpretable standards.

Peer-to-peer services, as well as over 90% of all VoIP computer phone services, operate on industry standard codec and industry standard protocols. In other words, their lines are not secure.

IM services also create targeted vulnerability to vicious hacker attacks by a simple monitoring program made available that enables electronic eavesdropping.

The above information is an excerpt taken from an in-depth and exclusive Report entitled "Why Hackers Love Computer Phones – A Shocking Report You Must Read!" by Dee Scrip available only at <http://www.whypay4calls.com/gtp/to.pl?l=ART-03>

****Attn Ezine editors / Site owners ****

Feel free to reprint this article in its entirety in your ezine or on your site so long as you leave all links in place, do not modify the content and include our resource box as listed above.

About the Author

The above information is an excerpt taken from an in-depth and exclusive Report entitled "Why Hackers Love Computer Phones – A Shocking Report You Must Read!" by Dee Scrip available only at <http://www.whypay4calls.com/gtp/to.pl?l=ART-03>

