U.S. International Trade Commission

Audit of Perimeter Network Security

OIG-AR-11-01

October 19, 2010

UNITED STATES INTERNATIONAL TRADE COMMISSION

Office of Inspector General

The U.S. International Trade Commission is an independent, nonpartisan, quasi-judicial federal agency that provides trade expertise to both the legislative and executive branches of government, determines the impact of imports on U.S. industries, and directs actions against certain unfair trade practices, such as patent, trademark, and copyright infringement. USITC analysts and economists investigate and publish reports on U.S. industries and the global trends that affect them. The agency also maintains and publishes the Harmonized Tariff Schedule of the United States.

Commissioners

Deanna Tanner Okun, Chairman
Charlotte R. Lane
Daniel R. Pearson
Shara L. Aranoff
Irving A. Williamson
Dean A. Pinkert

OFFICE OF INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

October 19, 2010 OIG-HH-028

Chairman Okun:

This memorandum transmits the Office of Inspector General's final report Audit of Perimeter Network Security, *OIG-AR-11-01*. In finalizing the report, we analyzed management's comments on our draft report and have included those comments in their entirety in Appendix A.

This report contains two recommendations for corrective action. The Commission has already implemented these recommended changes. As a result, we consider that final action has been completed for all recommendations in this report.

Thank you for the courtesies extended to my staff during this audit, and for quickly addressing our recommendations.

Sincerely,

Philip M. Heneghan
Inspector General

Table of Contents

Results of Audit **1**

Area for Improvement **2**

Web servers should use current security protocols and a minimum 112-bit cipher key strength 2

Recommendation 1: *That the Commission discontinue use of SSLv2 (Secure Socket Layer version 2).* *4*

Recommendation 2: *That the Commission require a minimum 112-bit key strength for its ciphers.* *4*

Management Comments and Our Analysis **4**

Objective, Scope, and Methodology **5**

Appendix A: Management Comments on Draft Report

Results of Audit

The objective of this audit was to determine: "Is ITCNet's perimeter defense effective?"

ITCNet's perimeter defense is effective.

A penetration test is an attempt to breach a network and gain unauthorized access to its resources. On July 28-29, 2010, we conducted a penetration test of ITCNet using public information. Our Google search for information on ITCNet servers identified 22 potential targets. The IP (Internet Protocol) addresses of the identified servers indicated a network range of 256 addresses where ITCNet hosts its servers. We used software to discover listening service ports, and then we scanned the servers for known vulnerabilities.

The USITC's computer network, ITCNet, has over 500 systems, consisting of servers, desktops, laptops, printers, phones, and network infrastructure devices. Every computer is connected to the network with a unique IP (Internet Protocol) address. For example, a desktop PC on ITCNet will have an address like 192.168.50.40. A typical Windows XP PC can have more than 20 listening ports. Each port serves a function; for instance, an Internet browser connects to port 80 to request web pages from a server, and email servers use port 25 to transfer messages. It would be normal for a network of 500 systems to present 10,000 listening ports, all potential targets for attack.

The goal of perimeter defense is to minimize the number of exposed ports, known as the "attack surface." A network with no open ports is not a network: open ports are required to communicate. Devices such as firewalls are configured to limit the number of ports exposed to the Internet, and newer technologies such as Intrusion Detection and Protection Systems (IDPS) can provide additional protection.

Several effective characteristics of ITCNet's perimeter defense include the following:

- ITCNet's firewalls effectively limit the exposure of internal systems to the Internet. Inside ITCNet, 10,000 or more service ports might be actively listening and responding to requests. From the Internet, only 51 ports were discovered in our scan of the ITC network.
- Not all of these 51 ports were real ITCNet services, after communicating with certain ports; we lost all communications with ITCNet. This indicated that these ports were intentional decoys presented by the IDPS to identify attackers.
- ITCNet uses IDPS. This software quickly detected our scans and blocked further scanning attempts.

- The listening services we identified all seemed to be functions necessary for the USITC to conduct business. We did not find any instances of services that should not have been exposed to the Internet.
- ITCNet's remote access services require two-factor authentication. Without knowledge of a user name, password, PIN, and RSA token (with a one-time code that changes every sixty seconds), it is not possible to login to ITCNet from the Internet.
- DNS zone transfers are not allowed. The Commission is following a best practice of not publishing this information. If allowed, this would effectively provide a potential hacker with an official map of ITC's network, much as a phone book would tell an outsider about every employee and their phone number. In the effort to secure a network, the less technical information published, the better.

In summary, ITCNet's perimeter defense effectively prevented our intrusion attempts.

An effective perimeter defense is a significant component of a complete network security program. An attacker can exploit a network in a number of ways. In general, she can attack the network perimeter as we did, or she can bypass the perimeter by tricking a user into letting her in. Means of accomplishing this could be as simple as having a user open a malicious email or visit an infected website, or by leaving an infected USB drive to be found by an employee near the front door of the building. While ITCNet's current perimeter defense is effective, continuous attention and improvement are required to ensure that it remains effective in the future.

Our penetration testing did reveal a potential area for improvement: Commission web servers should use current security protocols and a minimum 112-bit cipher key strength. This potential area for improvement is detailed below.

Area for Improvement

Web servers should use current security protocols and a minimum 112-bit cipher key strength.

We identified eight servers used by the Commission to publish information on the web. Of these eight servers, we identified four that provide sensitive information and use encryption. Encryption involves many components; two that are configured on our servers are the security protocol and the length of the cipher key. One server uses current

security protocols and 112-bit cipher key strength. The other three use older protocols and allow weaker 40- and 56-bit encryption.

Why Are Protocols Important?

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are used to secure network communications. These protocols are designed to encrypt sensitive information, such as health, financial, or confidential business data. When a user accesses a website to transmit or receive sensitive information, the website should be configured to communicate in a secure, encrypted manner. SSL version 2 was the original method used to secure this network traffic. This protocol contains security flaws, and was superseded by SSL v3 in 1996. TLS was introduced in 1999 as an upgrade to SSL.

Three USITC websites allow use of the outdated SSLv2 protocol.

Why are Cipher Strings Important?

The strength of encryption can be described by the number of bits in the cipher key. A 1-bit key is analogous to a coin: just as a coin can only be heads or tails, a bit is either 0 or 1. A 1-bit key would only require two tries to get it right. A 2-bit key would have 4 possibilities: 00, 01, 10, and 11. A 3-bit key would present 8 possibilities: 000, 001, 010, 011, 100, 101, 110, and 111. Other cipher key strengths:

- 40-bit: 1,099,511,627,776 possibilities
- 56-bit: 72,057,594,037,927,936 possibilities
- 112-bit: 5,192,296,858,534,827,628,530,496,329,220,100 possibilities

Today's computing power makes it feasible for individuals to crack weaker encryption. Commodity hardware available today for $400 can test 1.8 billion passwords per second. This hardware could crack a 40-bit cipher key, containing over 1 trillion combinations, in 10 minutes or less. More sophisticated and better funded hacking efforts would employ much higher performance systems, greatly reducing the time required to break encryption. Requiring web servers to deploy a minimum 112-bit cipher key strength would provide a high degree of protection for all sensitive Commission data.

Maximum time required to crack selected ciphers using inexpensive commodity hardware:

- 40-bit: 10 minutes
- 56-bit: 1.27 years
- 112-bit: 91,470,362,945,607,600 years

Three USITC websites allow the use of Low strength (40-bit) or Medium strength (56-bit) ciphers, placing the traffic at risk of being intercepted and decrypted.

Recommendation 1:

That the Commission discontinue use of SSLv2 (Secure Socket Layer version 2).

Recommendation 2:

That the Commission require a minimum 112-bit key strength for its ciphers.

Management Comments and Our Analysis

On October 15, 2010, Chairman Deanna Tanner Okun provided management comments to the draft audit report. The Chairman agreed that the Commission's perimeter defense is effective.

Based on the recommendations we made in our draft report, the Office of the CIO has reconfigured its Internet-facing web servers to remove the SSL v2 protocol and require a minimum 112-bit cipher key strength.

Objective, Scope, and Methodology

Objective:
Is ITCNet's perimeter defense effective?

Scope:
This audit focused on performing a penetration test of all public, Internet-accessible USITC services, including DNS, Web, and Email servers as well as any other discoverable services on July 28-29, 2010. The scope was restricted to the use of only two IP source addresses, involved only external probes of logical network security, and was time restricted to only two days of attacks. This audit involved specific testing, and is not to be interpreted as an audit of compliance. The following techniques were not used in our testing, but would be used by motivated attackers that had little concern about the health of ITCNet:

- Potentially destructive activities
- Denial of Service
- Social Engineering
- Spearphishing
- Malware-infected USB drives
- Distributed scans
- Wi-Fi scans
- Wardialing
- Spoofing
- Brute Force Attack
- Physical Security testing

Methodology:
We used publicly available information to discover USITC's Internet-accessible assets. The information gathered provided us with a map of the Commission's Internet services, which we used as a starting point for our discovery scans. We used NMap with multiple source addresses and with delayed timing to perform discovery, Nessus 4.2.2 to perform general vulnerability scanning, and Cenzic Hailstorm Pro 6.5 to perform website-specific vulnerability scanning.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A: Management Comments on Draft Report

Chairman

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

CO76-HH-019

October 15, 2010

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Deanna Tanner Okun, Chairman

SUBJECT: Management Response to the Inspector General's Draft Audit Report, "Audit of Perimeter Network Security"

I am in receipt of the Inspector General's draft report, *Audit of Perimeter Network Security*, dated September 15, 2010. I appreciate the opportunity to review the draft report and to provide a response to the findings.

The Inspector General's draft report found that the ITCNet's perimeter defense is effective. The report, however, did reveal one area for improvement: Commission web servers should use current security protocols and a minimum 112-bit cipher key strength. We agree that a few of our servers had used older security protocols and allowed weaker 40- and 56-bit encryption.

I am pleased to report that the Commission has instituted corrective actions and has implemented both of the recommendations in your draft report. In order to implement the recommendations related to weak cipher strength, the Office of the Chief Information Officer made a number of changes on the hosts identified to disable SSL v2 as well as any low or medium strength cipher keys. In addition, all internet-facing SSL websites hosted by the Commission now require a minimum of 128-bit key strength cipher and use only current security protocols.

The Commission is dedicated to ensuring that ITCNet has an effective perimeter defense. Thank you for reviewing the ITCNet's external defenses and making the recommendations to strengthen its effectiveness.

"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

To Promote and Preserve the Efficiency, Effectiveness, and Integrity of the U.S. International Trade Commission

U.S. International Trade Commission
Office of Inspector General
500 E Street, SW
Washington, DC 20436

Office: 202-205-2210
Fax: 202-205-1859
Hotline: 877-358-8530
OIGHotline@USITC.gov