Security
May 7, 2009 3:59 PM PDT

Report: Hackers broke into FAA air traffic control systems

by Elinor Mills

Hackers have broken into the air traffic control mission-support systems of the U.S. Federal Aviation Administration several times in recent years, according to an Inspector General report sent to the FAA this week.

In February, hackers compromised an FAA public-facing computer and used it to gain access to personally identifiable information, such as Social Security numbers, on 48,000 current and former FAA employees, **the report said**.

Last year, hackers took control of FAA critical network servers and could have shut them down, which would have seriously disrupted the agency's mission-support network, the report said. Hackers took over FAA computers in Alaska, becoming "insiders," according to the report dated Monday.

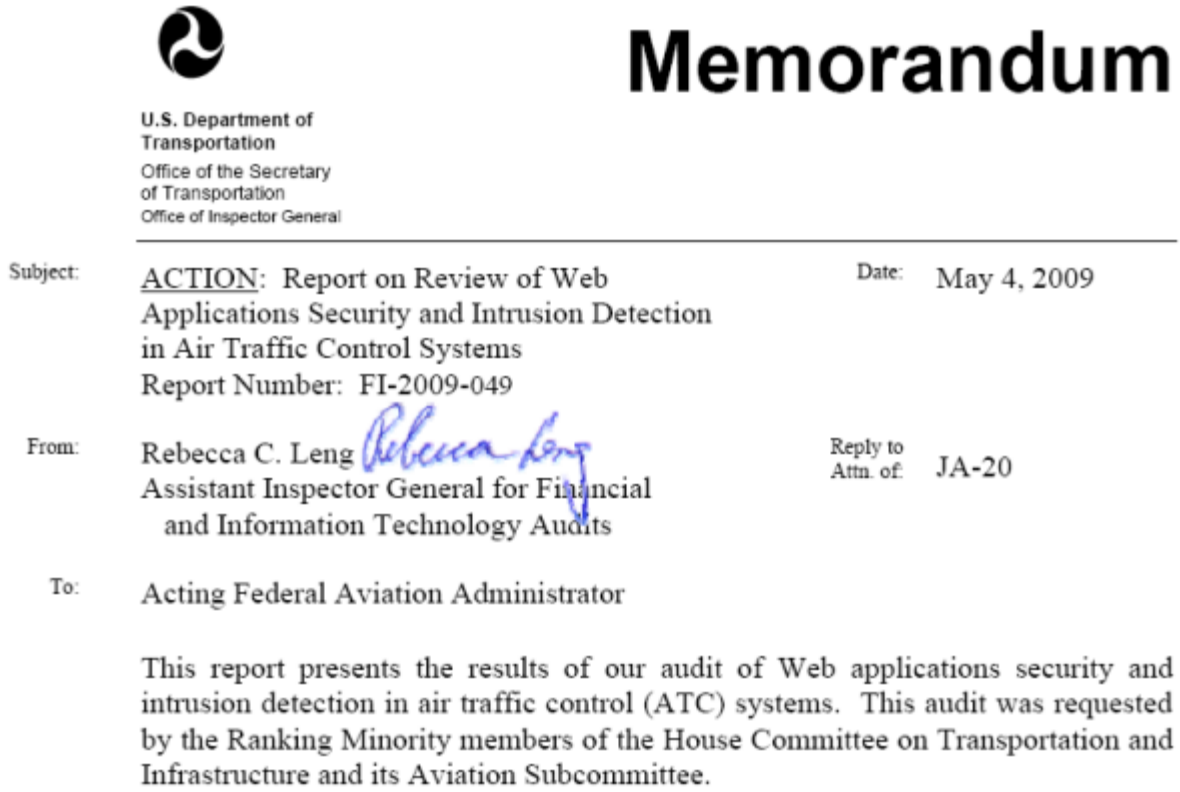
Then, taking advantage of interconnected networks, hackers later stole an administrator's password in Oklahoma, installed "malicious codes" with the stolen password and compromised the FAA domain controller in the Western Pacific Region, giving them the access to more than 40,000 FAA user IDs, passwords, and other data used to control a portion of the mission-support network, the report said.

And in 2006, a virus spread to the air traffic control (ATC) systems, forcing the FAA to shut down a portion of its systems in Alaska, according to the report.

The attacks so far have primarily disrupted mission-support functions, but attacks could spread over network connections from those areas to the operational networks where real-time surveillance, communications and flight information is processed, the

report warned.

"In our opinion, unless effective action is taken quickly, it is likely to be a matter of *when*, not *if*, ATC systems encounter attacks that do serious harm to ATC operations," the report concluded.



Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: ACTION: Report on Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems
Report Number: FI-2009-049

Date: May 4, 2009

From: Rebecca C. Leng
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Acting Federal Aviation Administrator

This report presents the results of our audit of Web applications security and intrusion detection in air traffic control (ATC) systems. This audit was requested by the Ranking Minority members of the House Committee on Transportation and Infrastructure and its Aviation Subcommittee.

An audit of the FAA's air traffic control cybersecurity protection measures finds them lacking and says there have been several breaches by hackers and a virus.
(Credit: U.S. Department of Transportation, Office of Inspector General)

The breaches were possible because Web applications that support the air traffic control system operations are not properly secured to prevent unauthorized access and network intrusion-detection software is not adequately being used to monitor and detect cyberattacks, the report concluded.

The FAA's increasing use of commercial software and Internet Protocol-based technologies as part of an effort to modernize the air traffic control systems poses a higher security risk to the systems than when they relied primarily on proprietary software, the report said.

"Now, attackers can take advantage of software vulnerabilities in commercial IP products to exploit ATC systems, which is especially worrisome at a time when the Nation is facing increased threats from sophisticated nation-state-sponsored cyber attacks," the report said.

In general, the nation's critical infrastructure is increasingly at risk as previously isolated and closed systems are moved to the Internet and commercial software, like Windows, is used, **security experts have said**.

The air traffic control system auditors said they discovered more than 760 high-risk vulnerabilities in the Web applications tested, including holes that provided "front-door access" to the systems and could allow attackers to inject malicious code onto FAA user computers. Web applications were not adequately configured and the applications with known vulnerabilities were not patched in a timely manner, auditors found.

Meanwhile, intrusion detection systems (IDS) are deployed at only 11 of hundreds of air traffic control facilities and none of the IDS sensors is installed to monitor operational systems at those sites, the report said. Cyber incidents are not effectively monitored or fixed quickly, the report concluded.

In 2008, more than 870 cyber incident alerts were issued to the organization responsible for air traffic control operations and by the end of the year 17 percent (more than 150 incidents) had not been remediated, "including critical incidents in which hackers may have taken over control" of operations computers, the report said.

The FAA is "identifying and fixing weaknesses," FAA spokeswoman Laura Brown **told The Wall Street Journal**. "We are working on developing security architecture for that whole system."

However, Brown dismissed the notion that hackers could get access to critical air traffic control operational systems.

The audit of the air traffic control systems was requested by the ranking minority members of the House Committee on Transportation and Infrastructure and its Aviation Subcommittee.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **News**, **Privacy & data protection**, **Vulnerabilities & attacks**

Tags: **critical infrastructure**, **air traffic control**, **FAA**, **hackers**, **breach**

Related

From CNET

EC wants software makers held liable for code

Google fixes severe Chrome security hole

Gates: Cyberattacks a constant threat

From around the web

Audit: air traffic systems vulnerable to... AOL News

FAA's Air-Traffic Networks Breached by H... Wall Street Journal