National Aeronautics and Space Administration

Informational Newsletter on Counterintelligence and Counterterrorism Issues Affecting NASA

All Eyes on NASA

April–June 2008

A Counterintelligence Perspective on NASA Technology Protection

This article presents the unclassified details of an actual counterintelligence investigation that I conducted while employed with another Federal agency. The case is representative of some of the methods foreign intelligence services use in order to exploit Government employees with access to information or technology they are seeking.

This case begins at an auditorium where I presented an espionage awareness briefing to an audience of 200 scientists and engineers. The purpose of the briefing was to educate the audience on how to recognize possible indicators that a foreign intelligence service was trying to exploit them for the purpose of illegally collecting information or technologies. The group was polite and even posed some interesting questions for clarification. But I left the auditorium with the general impression that they were mostly skeptical and did not necessarily accept the fact that foreign intelligence officers were active in the United States or that they could ever personally be targeted by one. After all, the Cold War was over, and the general impression was that all of the United States' enemies had since rejected spying against us. Right?

One week after my presentation, I received a telephone call from one of the engineers who had attended the briefing. He said that something had occurred over the weekend that seemed unusual, and that even though he thought it was probably nothing, one of his colleagues thought he ought to talk to me anyway. I went to his office right away. He was right to call me, because the events he related were hardly "nothing."

Over the weekend, the engineer received an unexpected telephone call from an unknown gentleman who happened to be in town and was eager to arrange a meeting. The caller explained that he was interested in the engineer's work, and that he had a business proposal for him. The engineer agreed to let him come to his home but realized shortly after he hung up that he had not given him his address. Surprisingly, the foreign businessman arrived at his home within a few minutes. He told our engineer that he represented a consulting group in a foreign country. He and his colleagues had read the engineer's papers and heard his presentations at various events throughout the world, and as a result, they were convinced that his work and talents would be a great contribution to their consulting firm. He asked the engineer to consider the proposal and said that he would contact him again. He left his business card with the engineer.

Using the information provided on the business card, we were able to confirm with our partners in the intelligence community that the "businessman" was actually a known foreign intelligence officer working under the cover of a businessman. We knew who he really was, but we did not yet know his true intentions. Our engineer was skeptical about what we had discovered but nevertheless agreed to work with us and continue to meet with the "businessman" to help us determine what he was really after. During the course of subsequent meetings and communications over the next few months, the foreign businessman asked our engineer to get copies of articles or papers that he said he was not able to get. Over the course of time, his requests became more suspicious in nature, asking for information and publications that, even though not classified, the engineer did not feel comfortable providing. Finally, after the foreign businessman believed that he had . . .
(continued on page 3)

Counterintelligence Quote of the Month

"The betrayal of trust carries a heavy taboo."
—Aldrich Ames, Soviet spy in the CIA

Counterintelligence Program Staff

Director
(b) (6), (b) (7)(C)

Operations
(b) (6), (b) (7)(C)

Office of Security and Program Protection

Interim Assistant Administrator
Jack Forsythe

NASA COUNTERINTELLIGENCE

A publication of the Office of Security and Program Protection
Counterintelligence Program

Counterintelligence News

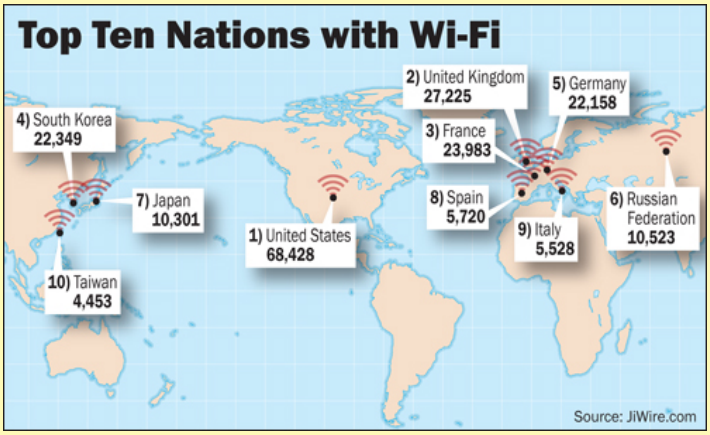
Wi-Fi Security
Some Advice from the FBI

You're at the airport waiting for your flight. With time to kill, you're thinking of connecting your laptop to the airport's Wi-Fi to check your office e-mail . . . do some personal banking . . . or shop for a gift for your spouse. But first, consider this: odds are there's a hacker nearby, with his own laptop, attempting to "eavesdrop" on your computer to obtain personal data that will provide access to your money or even to your company's sensitive information.

Here's something else to consider: there are **68,000 Wi-Fi "hot spots"** in the U.S. (see the graphic below for the top Wi-Fi countries)—at airports, coffee shops, hotels, bookstores, schools, and other locations where hundreds or thousands of people pass through every day. While many of these hot spots have secure networks, some do not, according to Supervisory Special Agent (b) (6), (b) (7)(C) of our Cyber Division. And connecting to an unsecure network can leave you vulnerable to attacks from hackers.

How do hackers grab your personal data out of thin air? Agent Peterson said one of the most common types of attack is this: a bogus but legitimate-looking Wi-Fi network with a strong signal is strategically set up in a known hot spot . . . and the hacker waits for nearby laptops to connect to it. At that point, your computer—including all your sensitive information, such as user ID, passwords, and credit card numbers—basically belongs to the hacker. The intruder can mine your computer for valuable data, direct you to phony Web pages that look like ones you frequent, and record your every keystroke.

"Another thing to remember," said Agent (b) (6), (b) (7)(C) "is that the connection between your laptop and the attacker's laptop runs both ways: while he's taking info from you, you may be unknowingly downloading viruses, worms, and other malware from him."



Businesses that offer free or ad hoc Wi-Fi often don't know their networks have been breached. Individual victims usually don't realize they've been targeted until it's too late. That's why, according to Agent Peterson, there aren't reliable stats on the number of these breaches, although the FBI does periodically receive reports on them. It's also very tough to trace a hack that orig an open, unsecure network.

Agent (b) (6), (b) (7)(C) explained that the criminal aspect comes into play once data taken by the hacker is used to commit a crime. If the hacker, armed with your personal or corporate information or access codes, tries to break into a secured network—whether it's a case of property or any other type of crime—then law enforcement gets involved.

What can you do to protect yourself? Agent Peterson's best advice is, don't connect to an unknown Wi-Fi network. But if you have to, there *are* some precautions you can take to decrease the threat:

- Make sure your laptop security is up to date, with current versions of your operating system, Web browser, firewalls, and antivirus and anti-spyware software.
- Don't conduct financial transactions or use applications like e-mail and instant messaging.
- Change the default setting on your laptop so you have to manually select the Wi-Fi network to which you are connecting.
- Turn off your laptop's Wi-Fi capabilities when you're not using them.

For more basic information on computer security, see our How To Protect Your Computer.

NASA OSPP PC/Laptop Security Tips

Cuba To Step Up Spying on U.S.

MIAMI (AFP)—Cuba's vast international spy network, considered among the best in the world, will remain intact under the leadership of the new president, Raul Castro, intelligence experts say . . . .

Read More

Main article, continued from page 1

sufficiently cultivated a trusted friendship with our engineer, he asked him to obtain a copy of a specific document that was export controlled and was not approved for foreign release. The engineer was promised several thousand dollars in return. Interestingly enough, it was during this meeting that the engineer finally believed what I already knew to be true: A foreign intelligence officer had indeed tried to exploit him, but in this case we were in the background keeping everything secure. Based on the information in the requested document, we also knew what the intelligence officer was actually seeking and what he was willing to pay for it. This also gave the intelligence community a better understanding of what one of our potential military adversaries was working on and how far they had progressed. The document remained properly secured, and the intelligence officer's efforts did not pay off.

To fully appreciate how the events in this case are applicable to NASA employees, it is important to review some of the facts briefly. The engineer was initially identified and targeted by foreign intelligence through his papers and presentations on unclassified, "public domain" sources. The foreign intelligence service was able to look at the details of his papers and presentations and combine that information with their knowledge of where he worked to determine what else he might have access to. The fictitious business approach was simply a ruse to try to gain some trust and develop a professional relationship with the engineer. Continuing to ask the engineer for other articles and publications, which gradually and subtly became more sensitive in nature, was simply a way to test the engineer's willingness to cooperate and to get him accustomed to providing the requested information. Once he thought everything about the relationship was firmly established, the intelligence officer requested an export controlled document in exchange for several thousand dollars.

NASA employees should take several lessons from this case study, as there are many obvious similarities upon which to draw. Even though the Cold War is over, foreign countries have never stopped conducting espionage against the United States; such activity occurs today at an ever-increasing rate. Dual-purpose technologies are particularly targeted, and, by default, so are the engineers that work with them. It is also particularly important to understand that even unclassified work performed by employees without security clearances is potentially valuable to foreign intelligence. It is recognized that much of what NASA accomplishes involves significant and legitimate foreign collaboration, for which necessary processes and procedures are in place to gain the necessary approvals and support. However, it should also be recognized that there are times when people and events might not actually be what they seem to be on the surface. While we should not be paranoid or cynical in our business and professional relationships, we should nonetheless be able to recognize anomalies for what they are and get the appropriate assistance. One thought-provoking principle sums up how each of us should approach this possibility: "Never assume that the other guy would never do something we would never do." Every NASA Center has a Counterintelligence Office with experienced special agents ready to assist in these matters, no matter how implausible something might seem. In the end, all suspicions or concerns reported to NASA Counterintelligence will be thoroughly and discreetly exam

Article by SA (b) (6), (b) (7)(C) **LaRC Counterintelligence Office**

NASA COUNTERINTELLIGENCE

NASA Center CI Offices

NASA Headquarters
(b) (6), (b) (7)(C)

Ames Research Center
(b) (6), (b) (7)(C)

Dryden Flight Research Center
(b) (6), (b) (7)(C)

Glenn Research Center
(b) (6), (b) (7)(C)

Goddard Space Flight Center
(b) (6), (b) (7)(C)

Jet Propulsion Laboratory
(b) (6), (b) (7)(C)

Johnson Space Center
(b) (6), (b) (7)(C)

Kennedy Space Center
(b) (6), (b) (7)(C)

Langley Research Center
(b) (6), (b) (7)(C)

Marshall Space Flight Center
(b) (6), (b) (7)(C)

Stennis Space Center
(b) (6), (b) (7)(C)