



White Paper

Rest Assured

Aaron Greenspan

Date: January 11, 2006
Topic Area: Security

Approximately one year ago, Think exposed security vulnerabilities in the South Station train terminal in Boston, Massachusetts, which led to the discovery of similar problems with Think's former web-based payroll vendor, who was exposing up to 100,000 social security numbers and salaries belonging to its clients nationwide. Meanwhile, Think's own Lampshade software programming toolkit had proven quite robust in the area of computer security, and security auditing services could always be sold alongside as a complementary good. Since the private sector didn't seem to be listening to the repeated dire warnings in the media about identity theft, I made an executive decision to try a new target market: the Government.

In late August, 2005, Think Computer Corporation began the process of applying for a General Services Administration (GSA) Federal Supply Schedule contract. The GSA is the federal Government's clearinghouse for volume purchases; its "GSA Advantage" web site is the Government's Sam's Club, where agencies shop for all kinds of products in bulk at substantial discounts. Consequently, for any business, a GSA

contract is a big deal, since it means the entire U.S. Government can come to them with terms pre-negotiated, and not *vice-versa*.

As one might expect, the process of applying is cumbersome. The GSA expects companies to read the given Schedule for their industry from

cover to cover, which is usually hundreds of pages long. "Refreshes" of the schedule, which are released on a sporadic basis throughout the year, make the process of understanding the process even more difficult. There are countless private seminars held across the country on an almost daily basis on ways to secure GSA contracts,

and despite the fact that most are scams, their existence alone reflects the fact that the process is unbelievably complicated.

In July, 2004, the GSA attempted to streamline its bureaucracy by introducing the eOffer system, which allowed Schedule 70 contractors, who specialize in Information Technology, to submit their offers to the GSA electronically. Though eOffer does not appear even once on the agency's home page (<http://www.gsa.gov>), I was eventually able to find it after inquiring with my regional branch office about a way to submit

The GSA's system, linked directly to the Pentagon and tens of thousands of confidential documents, had no user authentication at all, save a publicly-available DUNS identifier—and anyone on the system could change anyone else's data.





an application on-line. Today, eOffer and its counterpart system for existing contracts, eMods, cover five Schedules: Financial and Business Solutions, Advertising & Integrated Marketing Solutions, Professional Engineering Services, Mission Oriented Business Integrated Services, and Information Technology.

Companies who want to use eOffer must register with a vendor database operated by the Department of Defense, called the Central Contractor Registration (<http://www.ccr.gov>). In turn, the CCR depends on the company already having a Dun & Bradstreet Number (DUNS). Therefore, for a small business without a DUNS, “simply using eOffer” is not really that simple at all; there is a great deal of paperwork that has to be done first.

Fortunately, Think Computer Corporation already had its DUNS, and its CCR registration was complete, but it did not have eOffer’s third requirement: Access Certificates for Electronic Services (ACES), a special software-based encryption device designed to augment the typical SSL encryption that most web sites use to secure sensitive data in transit. ACES certificates restrict access to a web site to a single computer for a given user, which prompts the user for a password each time the certificate is used. The certificates also generate considerable revenues for the firms that issue them.

In order to obtain an ACES certificate, companies must register with one of these firms, send a notarized contract through the mail, and then wait for a special code to be e-mailed back so that the ACES certificate itself can be obtained over the World Wide Web. Installing the certificate does not take long at all, but requires some degree of technical ability.

By September, Think had its ACES certificate up and running, but could not sign onto the

eOffer system. A call to technical support revealed that the certificate will not work with the URL “<http://www.eoffer.gsa.gov>.” One had to remove the “www.” first in order to access the system. Of course, the site looked fine either way, but never stated the operating restriction anywhere in writing.

At long last, signing in with Think’s DUNS number worked. eOffer asked to verify Think’s DoD CCR MPIN, a plain-English password required by the CCR, in order to obtain Think’s address records from the Pentagon. For the next step, I typed in my own name and contact information as the lead negotiator. The following step asked me to answer questions about a number of legal clauses, most of which were irrelevant for my business. Then, the system asked for several documents about Think’s products, which had to be uploaded to the server.

It took a few weeks to come up with the exact kind of price list that the Government required. Uploading Think’s documents failed, however, because the system would not allow for file names with more than one period. (Think’s standard naming convention for documents requires two periods, in order to separate the date from the file description from the three-letter format extension.) Each of several files had to be renamed.

On September 29th, long after the eOffer application process had been completed, Think was assigned to an application examiner named Linda. Several weeks later, a request arrived via postal mail from the GSA. I was required to complete Form 527, asking for Think’s detailed financial data, including its bank account balance and its balance sheet for at least the prior fiscal year. The version of Form 527 included in the envelope was approximately ten years older than the version that I found buried in the GSA’s on-





line form archive in PDF format, but since even that file could not be filled in electronically, Adobe Illustrator and Photoshop had to be employed to make up for the GSA's deficiency. Eventually, the form had to be printed out and then scanned in again in order to fax it back with the bank's handwritten verification.

Several days after the GSA's financial department received Think's fax, a second request for Form 527 arrived via postal mail, again containing the same outdated form. I explained to Linda by e-mail that the information had already been sent. Finally, after repeated conversations with the financial department, I was told that I could have simply sent the company's IRS Form 1120S, which had been complete for months and could be filled out electronically in PDF format, as a substitute. Think's financial state was approved.

Next, Linda expressed confusion as to why I had not supplied a "Dun & Bradstreet" for Think. In response to her request, I had, in fact, sent a Dun & Bradstreet report for Think Computer Corporation, but it was not the "correct" one. In fact, the GSA required a report supplied only by Open Ratings, Inc., in affiliation with Dun & Bradstreet, which necessitated contacting up to twenty of Think's customers to have them complete an on-line survey about the company's past performance. After waiting for my clients to finish the survey, the final document was delivered, and it eventually made its way to Linda at the GSA. Open Ratings, Inc. had not been mentioned anywhere in the eOffer process, but collected a fee for the report. Its web site automatically revealed my account password in plain text in each e-mail that it sent to me, as well as in the URL of the survey administration page. When I called to point out that revealing passwords in such a manner was a bad idea since referring URLs are stored in log files, the person on the other end of

the line did not have enough technical knowledge to handle my complaint.

On November 4, 2005, Linda e-mailed three documents that needed to be completed in addition to the forms required by the eOffer system: a discount list, a cost chart, and GSA Form CSP-1. Attempts to explain that Think was a small business, without the capacity to issue standard discounts to large customers, were futile. Linda demanded that the form be completed with Think's "business practices." Further attempts to explain that as a software company Think had no non-labor costs for the majority of its goods were also pointless. The GSA could not conceive of such a company; I was told that my cost chart also had to be completed, including columns such as "Manufacturer Part Number."

Linda also wanted to know Think's markup on each product. Markup on software products is typically undefined, as markup is price divided by cost minus 100%, and cost is zero for software. When I was told that I was told that "undefined" was not an acceptable answer, I tried to explain the markup as 100%, which would technically mean double Think's "cost." At this high number, Linda balked that I would be drastically overcharging the Government.

Linda also repeatedly asked for an "internal pricing memo," referring to the phrase as if it were a standard document that every company had lying around. I explained to her that Think Computer Corporation had five employees when it was largest, so sending pricing memos would have been thought of as a joke.

On December 9, 2005, Linda requested for the second time a list of Think's three best customers, which were already listed on GSA Form 527. She also wanted a price list with detailed, paragraph-long descriptions for each product.





After I sent the descriptions, she further requested a list of products on GSA Advantage that were comparable to each, since she said that she still could not understand what my software actually did, even with the complete descriptions. Linda also wanted invoices for each product listed on the pricing spreadsheet. Some of the products, such as an web-based archaeology database system designed specifically for a government contract, had never been sold before, and thus had no prior invoices. Others had no comparable products on GSA Advantage since they filled niche markets.

To satisfy her requests, I sent Linda a link to several folders worth of compressed data on one of Think's servers, but she ignored the link, complaining that there were too many files, and that she could not be expected to read them all. Over the next few weeks, I sent her all of the same files individually, sometimes up to three times each, as she requested them again and again. Frustrated, I began drafting a letter to my Senator, when Linda's supervisor, Montrez, called. Montrez insisted that I was being impatient and difficult, and was clearly unhappy when I mentioned my incomplete letter to Congress. Eventually, I gave up writing my letter and sent Linda copies of all of my documents yet again, since Montrez indirectly threatened to terminate my application. For the "internal pricing memo," Montrez suggested writing a fake memo simply to satisfy the GSA's requirements.

"I don't feel comfortable concocting fake documents," I told her.

"This would be okay," she said. "It's just to meet our requirements." Grudgingly, I delivered a fake memo about Think's internal pricing policies, which contained vague statements about Think basing its rates on "market forces." The GSA found this acceptable.

On December 14, 2005, Linda finally rejected Think's offer due to a typo on the pricing spreadsheet that she had never mentioned before; it listed an hourly consulting rate as being \$2.05 higher than the same rate on an invoice. In the four full months from September through December, she never once asked for help reading Think's application from anyone with technical knowledge about computers, despite my urging her to do so.

Linda encouraged me to reapply, and she promised that she would push to have my application reassigned to her the second time around so that she would already be familiar with my situation. She remarked several times that I would have been better off using the paper application rather than eOffer, because it was "easier," but asked me to e-mail her all of my updated files yet again so that she would be prepared this time.

Without the time to read almost two hundred pages of legal jargon for my second application attempt, I opted to use eOffer one more time, counting on my computer savvy and better knowledge of the application process to carry me through. In the middle of uploading the Open Ratings report (now already complete) to the eOffer system, I noticed a spelling error after I had already pressed the "Upload" button, but there was no way to edit the entry. I had to delete it—which is when I noticed the uploaded file's unique ID, 10582. I clicked delete, and confirmed my action by clicking on a large "YES" button.

When I re-uploaded the same file, making sure to check my spelling, I noticed that its ID was now one number higher, 10583. Copying the URL into the web browser and changing the ID to 10582 revealed that my deleted file was actually still on the system, only hidden. Wondering if the GSA suffered from the same





type of sequential ID vulnerability as Think's former payroll company, in which case all of Think's sensitive financial data would have already been exposed for months, I changed the number once more to a different ID in the same general range. My web browser prompted me to download a file, which promptly appeared in Microsoft Excel. It was a price list, and it was not mine. The system was indeed vulnerable.

Signing into eOffer now displayed two offers in my main table: one that had been rejected, and one that was still in progress. The first column of the table was labeled "Offer Id." A quick look at the source code of the page revealed that the offer IDs were also present in hidden form input fields, which could be changed easily when the code was copied and pasted to a local file on a computer's hard drive. By changing the URL of the FORM ACTION parameter from a relative path to the absolute path on the GSA eOffer server and leaving my eOffer session active, it was possible to view, and then change, other companies' electronic offers. Since each offer's first page yielded the given company's DUNS information, the same number could then be pasted into the initial sign-in screen. Anyone with an ACES certificate tied to the eOffer system could sign in as any vendor they pleased.

In other words, the GSA's system, linked directly to the Pentagon and tens of thousands of confidential documents, had no user authentication at all, save a publicly-available DUNS identifier—and anyone on the system could change anyone else's data.

Further testing revealed that the eOffer system did not check a database at the GSA to determine the validity of the DUNS number. Rather, it checked the DoD CCR database directly. Any of the hundreds of thousands of companies registered with the CCR were vulner-

able. Any vendor could start a new offer "on their behalf," or use the parallel eMods system to modify an existing GSA schedule contract—even contracts granted by the GSA before the eOffer system came into existence. Theoretically, one could have started a bidding war between Boeing and Lockheed Martin, or Dell and Gateway, or changed the terms of their existing government contracts.

I notified the GSA of the problem immediately on December 22, 2005, finally reaching someone in the Inspector General's office. I also called the Washington, D.C. offices of four U.S. Senators. All four of their respective staffpeople declined to speak with me about the problem, since staff members were already on vacation. I left one voicemail, which was never returned.

On December 29, 2005, the GSA, which had decided to treat my complaint as a "hotline tip" (though I had never called any hotline), forwarded my e-mail to its IT group within the Inspector General's office. On vacation myself in New York, I offered to visit the GSA's New York branch to demonstrate the problem. My offer was declined. I also offered to rearrange my travel plans since my flight back was already routed through Washington, D.C. That offer, too, was declined. Instead, I was told, the GSA wanted to fly two agents to Dallas, round-trip.

Eventually, I was able to convince the GSA to save taxpayer money on unnecessary plane fares by creating a screen-capture video demonstrating the problems, at no cost to anyone at all. The Inspector General's office was easily convinced by the video that there was in fact a large problem, but no one at the GSA knew who had created the system in the first place, let alone how to fix it.

A quick search on the internet revealed that the eOffer system was designed by two compa-





nies: Unisys, and a subcontractor, Silanis. Silanis, a Canadian company that presented in tandem with the GSA at a conference on digital authentication systems in October, 2005, still boasts of its eOffer digital signature security technologies on its web site. (None of the files examined were digitally signed.) Unisys was just awarded a contract renewal worth \$750 million to create information technology systems similar to eOffer for the Department of Homeland Security.

Confronted with the possibility that virtually every major company in the United States (and thousands of small businesses, since the Small Business Administration is also linked to the CCR) could be affected by the numerous bugs in the GSA's systems, and unable to get through to Congress, I called the *Washington Post*.

"That position's been vacant for a month," I was told when I asked for a reporter who dealt with computer security. (One Senator's office had given me the same answer, aside from the timing of staffpeople's vacations.)

The eternal dilemma of security professionals is the best way to report a problem when the affected party refuses to listen or is too slow to act. In this case, the GSA Inspector General's office had been responsive, but could not convince the rest of the agency to move, and was fairly hampered by inefficiency itself. Consequently, it was imperative to find a reporter who would be willing to hold off on publishing the story until the problem was actually fixed.

Published too early, a story in the press would allow other vendors with ACES certificates to exploit the flaws (if they had not done so already, which the Inspector General's office admitted would be nearly impossible to determine). Yet, by contacting the press after the flaws had been fixed, news editors would wonder why a resolved situation was newsworthy.

"What if I call you after it's fixed, but tell you the details now?" I asked the *Post* reporter.

"We're not gonna run it," he said. CBS responded with the same tone, failing to understand, or even care to understand, the problem. Yet if the press failed to pick up the story, no one would ever know. With the ethical implications already murky, there was, and continues to be, a clear need for ethical reporting standards regarding computer security issues.

Luckily, *The New York Times* was more cooperative. In exchange for an exclusive story, I offered John Markoff the details of the problem ahead of time, on the condition that he investigate and then publish a story only when appropriate, based on my own determination of the timing. The GSA Inspector General's office saw no problem with going to the press, even if it would be detrimental to others in the agency, for which I was grateful.

Today, three weeks after being notified of the problem, and a year and a half after its launch, the GSA finally took down the eOffer system, replacing it with a message stating, "The eOffer system is down for maintenance. Please pardon the inconvenience, thank you." Coincidentally, Think Computer Corporation was also assigned a new analyst for its offer, which is no longer accessible electronically. The analyst is not Linda, after all, meaning that I will have to start the entire six-month-long application process at least one more time.

"Please let me assure you that your identity and privacy will be protected," my contact in the Inspector General's office wrote, referring to the event in which I would go to the press.

Somehow, I just can't rest assured.

Copyright © 2006 Think Computer Corporation. All Rights Reserved. Think Computer is a registered trademark of Think Computer Corporation. All other names may be trademarks or registered trademarks of their respective owners.

