Think Computer®

White Paper

Identity Crisis

Aaron Greenspan

Date: February 19, 2005
Topic Area: Security

A little more than two weeks ago, Think Computer Corporation released a White Paper describing how a few small technical problems at South Station in Boston could have caused disproportionately large problems for thousands of people. Breaking into the network at South Station required nothing but "common mistakes and guesswork," as one critic put it, but the simple nature of all the flaws involved was precisely the point of the paper. We trust software vendors far too much when it comes to our sensitive personal data. When combined with the faulty assumption that serious damage can only be caused by sophisticated hacking, and the fact that vendors have overwhelming incentives to deny the existence of errors in their products, the foundation for a technological disaster is complete.

Based on the IDs for each year's W-2 system, the problem definitely exposed more than 25,468 (but probably fewer than 100,000) Social Security numbers with other associated information.

PayMaxx, Inc. is a Tennessee-based payroll company that boasts a few thousand clients. PayMaxx differs from some of its more traditional competitors in that its operations are entirely web-based, making it an especially attractive option for companies in high-technology industries who may have already automated related accounting systems. PayMaxx has clients across the United States, from California to Maine. Their model is a good one, for it alleviates much of the frustration of using cumbersome client-side payroll software (with limited internet connectivity support), or worse yet, paper forms. The password-protected PayMaxx web site allows authorized personnel to input payroll information from practically anywhere over an encrypted HTTP connection.

Each one of PayMaxx's customers is assigned a customer ID, and each customer ID allows for multiple user accounts, with which people can sign into the PayMaxx system in order to update payroll information. The system runs on a Windows-based server and a combination of scripting languages, including ColdFusion, sold by Macromedia, Inc., and Microsoft VBScript, which is coincidentally a favorite of virus authors.

Aside from the convenience of being able to input data from anywhere, web-based systems also offer the additional benefit of making data output easier (and cheaper). In theory, you could print out your IRS form W-2 at home instead of paying an extra fee to have the same form shipped to you. As it so happens, PayMaxx still requires its customers to pay a shipping fee to receive paper copies of forms, but it also provides the ability to view the forms on-line in Adobe Acrobat PDF format, which is designed to preserve typefaces and layout, so that copies of documents are indistinguishable from their originals.

It is this feature of the PayMaxx system that is gravely flawed. While PayMaxx's programmers took care to ensure that their system's authentication software worked well, they took less care to protect the code that dynamically generated form W-2, and each form includes a person's home address, aggregate payroll, and Social Security number. Perhaps the team that created it lost sight of the sensitivity of this information; as a programmer, it is easy to become focused on the detailed mechanisms that make your program work and forget about the "big picture," but in any event, it is still not a very good excuse.

The result of this mistake was that when PayMaxx announced the availability of 2004 W-2s on-line, the home address, aggregate payroll, and Social Security number of each and every one of PayMaxx's customers became available to us here at Think. By simply changing one number in a hyperlink on PayMaxx's "secure" web site, it was possible to scan through PayMaxx's entire W-2 database for the year 2004. PayMaxx stored each employee's data record sequentially in a table—a perfectly normal and acceptable practice, and one that Think uses frequently in its own software, but also one which made it possible to always guess the ID of the next record by simply adding 1. In software based on the Think Lampshade platform, each HTTP request is checked against a security array to verify that the user signed in actually has access to the data being requested. In PayMaxx's software, this process simply didn't exist. Anyone with access to the system could view the W-2s of employees with whom they had had no connection whatsoever. Furthermore, by simply subtracting the first ID from the last ID that allowed this behavior, it was possible to ascertain the number of W-2 forms that PayMaxx had printed for the 2004 tax year: 25,468. In other words, a glitch on a single web page made it possible to access the Social Security numbers and salaries of 25,468 individuals nationwide.

Shockingly, the exact same bug applied not only to the 2004 W-2 system, but to the 2003, 2002, 2001, and 2000 systems, and possibly even systems for earlier years. If one assumes that PayMaxx's customer list changed from year to year, then each year's system would include new employees relative to years previous. Based on the IDs for each year's W-2 system, the problem definitely exposed more than 25,468 (but probably fewer than 100,000) Social Security numbers with other associated information.

That the glitch made each employee's W-2 available not in a raw data format only readable by machines, but in a human-readable, perfectly printable, high-quality format (identical to that of the original form), raises another concern: anyone can press a "Print" button. If a disgruntled employee wanted to blackmail his or her superior by threatening to reveal confidential salary information, it would only take a few seconds to post that person's W-2 in a location visible to the public, whether electronically or on a physical bulletin board. If a criminal with plans to commit identity fraud wanted to convince a bank that he or she was really the owner of someone else's bank account, a completely accurate printout of form W-2 might just be good enough evidence to "prove" identity.

PayMaxx was at one point Think Computer Corporation's payroll processor, until Think gave the company notice that we would no longer require its services for reasons unrelated to the problems described in this paper. Yet it was only when we notified PayMaxx of the vulnerabilities in their system that the company chose to actually disable Think’s customer ID and all of its associated user accounts. This should have rendered the vulnerable web site inaccessible.

Yet the bug remained. On every one of the thousands of check stubs that PayMaxx prints, there is a reminder to the recipient, “For Check/Earnings detail visit our secure website...” followed by a “secret PIN number.” The paystub site then provides links for earnings history, reports, and a feature called “InstantW2.”

Signing into the paystub site revealed that, in fact, InstantW2 was really just the same buggy code from the protected PayMaxx site, except in a different location accessible to all employees, instead of only those with management privileges. Any employee, whether terminated, presently working, on leave, or even affiliated with a company that was no longer a PayMaxx customer, could therefore look up the supposedly confidential W-2 of any other onetime PayMaxx customer.

Identity theft that involves Social Security numbers is harder to rectify than other forms of identity theft. You cannot simply cut up your Social Security card as you would a credit card when you think someone else has the number, and then call the Social Security Administration for a replacement. The SSA has stringent criteria—most of which necessitate the involvement of a life-or-death situation—for triggering the issue of a new number. (For more information, see http://www.ssa.gov/pubs/10093.html.) Payroll data cannot be used for identification purposes as easily, but it is typically private, and once it is out in the public domain there is no way to reel it back in.

Unfortunately, it is not inconceivable that PayMaxx’s client database is already in the public domain, due to another unrelated oversight by its programmers. PayMaxx left a record in its employee table set aside either for testing, or for disabled records, that made the W-2 systems available essentially to anyone with internet access and a sticky keyboard. With the Social Security number 000-00-0000, and the PIN 000000, one could sign into any of a number of corporate accounts, conveniently listed in a menu. From there, it was only a click away to the vulnerable InstantW2 generator.

Upon discovering the vulnerabilities in PayMaxx’s system and their extent on February 7, 2005, Think immediately notified PayMaxx that the problems were of a serious nature, and recommended that the company hire a security consultant to remedy them if it was unable to fix them on its own. After more than two weeks, PayMaxx issued no formal response and took no action, leaving the security holes wide open. Meanwhile, statements remained on its corporate site such as, “At PayMaxx, we are committed to maintaining your privacy and data security.” Interestingly enough, as recently as February 18, 2005, Attorneys General in thirty-eight states signed an open letter to ChoicePoint, Inc. protesting that company’s inaction after it was notified of a remarkably similar problem.

PayMaxx has unwittingly created a perfect example of how a security breach is possible over a connection that is technically secure. While there are plenty of standards for data encryption, web-based software vendors rarely if ever conform to standards for secure data storage once a transmission has been received. Yet even if data *is* stored with appropriate safeguards, such as hashing for passwords or encryption for credit card numbers, information can still be vulnerable. Secure data transmission and storage are meaningless if anyone can guess legitimate credentials.

Indeed, the glowing lock icon that appears in most popular web browsers when a valid SSL certificate is in use is one of the largest hoaxes of all, since it implies to naive consumers that everything about the transaction at hand is indeed "secure." Ben Edelman, a Ph.D. candidate at Harvard, has done interesting research into the market for these certificates, linking the indiscriminate practices of certificate vendors to the annoying pop-up advertisements that most World Wide Web users face on a daily basis. He makes the observation that, "If VeriSign revoked the digital certificates used by clear wrongdoers—those with invalid purported company names, or with outrageously deceptive installation practices—users wouldn't face the misleading popups" (http://www.benedelman.org).

VeriSign is not the only one to blame for a false sense of security, however. GeoTrust, formerly a division of EquiFax, and one of VeriSign's small handful of competitors, actually issues its "QuickSSL" line of certificates to web site *addresses*, as opposed to proven legal entities, in order to lure in those customers only willing to pay a lower price for encryption technology that is otherwise identical to its normal certificates. While this probably boosts GeoTrust's revenue (and profit, since there is approximately zero cost to producing a virtual certificate based on a publicly-available algorithm), it also completely defeats the point of issuing certificates in the first place. Imagine if Harvard or Yale were to start issuing diplomas to anyone, for half the price of normal tuition, that read "Your Name Here."

Microsoft, too, has come under scrutiny of late for its handling of vulnerabilities in its Windows operating system, but it has largely escaped the spotlight for its role in the market for SSL certificates. Its Internet Explorer web browser will only properly recognize (which is to say that it does not display an error message for) certificates that stem from large companies, such as VeriSign, with which Microsoft likely has large contracts for the express purpose of limiting competition in the SSL market. We as a society have therefore trusted our data security to a monopoly that props up a cartel. Surely competitive market forces could do a better job.

The solution to the problem of verifying trustworthiness is clearly not letting just anyone generate their own SSL certificate (again, think "printing your own diploma"), but then, the solution is also not the current system, which is for all intents and purposes broken. Microsoft, not to mention the Mozilla Foundation, which is gaining market share with its Firefox browser and is supposedly founded on principles of openness, could at least open the field to companies whose verification processes for those requesting SSL certificates actually meet some sort of standards. If such standards for authenticating companies do not yet exist, they should.

The flaws in security technology and politics already make it difficult to make systems that are reasonably secure. In the meantime, what is really necessary is an attitude on behalf of technology companies (and PayMaxx should not escape this statement by calling itself a "payroll company") that does more than pay lip service to security. Indeed, payroll companies, banks, government institutions, and other financial brokerages are entrusted with huge amounts of highly confidential data. It would be comforting to think that they do everything in their power to protect that information, but sadly, in many cases, it would also be wrong.