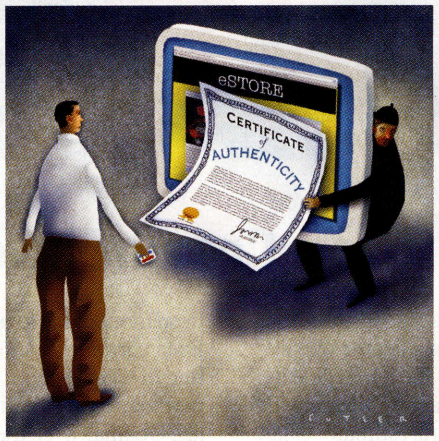
Christopher Werth

Attack of the Vigilante Cryptos

DESPITE SLUGGISH SPENDING ACROSS THE GLOBE, ONLINE RETAIL SALES REMAIN A glimmer of hope in the United States and Europe. More and more people do their banking and even grocery shopping from their laptops. But for e-commerce to work, it has to be secure. To that end, retailers and financial institutions turn to private firms to issue digital certificates verifying the legitimacy of Web sites. The system protects online shoppers from counterfeit sites that trick users into revealing passwords and credit-card numbers. As long as all three parties—the retailer, the certification authority and the software company that makes the browser—have done their due diligence, a little common sense on the part of users can keep most online transactions from going awry. That's the theory, anyway.

This trio played in harmony until a few weeks ago, when a loose group of international researchers cast doubt on the whole arrangement. The group, unofficially known as MD5 Collision Inc., demonstrated that they'd discovered a way to fabricate rogue certificates copied from the legitimate one they had bought from VeriSign, the world's biggest issuer. A cybercriminal holding a rogue certificate could convince any browser that a fake Web site is authentic. Secure networks would easily crumble under some of the most common tricks of the trade, such as man-in-the-middle attacks, which allow hackers to redirect users from a genuine site to a malicious one, and phishing, which uses disingenuous e-mails with links to bogus sites. As far as we know, there are no rogue certificates in the wild—MD5 Collision refrained from providing a blueprint of their attack—but for the first time, they've proved it's possible.

At its most basic, maintaining the Web as a safe place to do business comes down to staying several steps ahead of Moore's Law, which holds that computing power doubles every two years or so. Faster computers mean that encryption measures considered strong and reliable a few years ago eventually fall under the brute force of new, more powerful processors. In this case, the chink in the electronic armor lay in VeriSign's continued use of MD5, an encryption algorithm developed at MIT in the 1990s to generate unique and secure digital signatures. MD5 has been considered too weak for important security applications at least since 2004, when Xiaoyun Wang, a professor at Shandong University in China, revealed that she had broken the algorithm at a conference in Santa Barbara, California—receiving a standing ovation from her cryptography colleagues. That laid the groundwork for MD5 Collision, which wired together more than 200 Sony PlayStation 3s to create one supercomputer. (It turns out the chip that Sony developed is perfect for hacking code—one PlayStation is equivalent to about 40 average PCs.) In only three days the group had produced a rogue certificate. Fearing legal action from VeriSign would prevent them from going public, the researchers contacted Microsoft and Mozilla, whose browsers have to work with VeriSign certificates, who then notified VeriSign that something was about to happen.



A cybercriminal holding a rogue certificate could convince any browser that a fake Web site is authentic.

When the news hit the blogs, security analysts weren't as shocked by the rogue certificate as they were to learn that VeriSign was still issuing MD5 certificates at all. Most certification authorities have moved on to a more robust family of algorithms created by the U.S. National Security Agency, known as SHA-1. "Using MD5 is basically wrong," says William Burr, a cryptologist at the U.S. National Institute of Standards and Technology. "They should be embarrassed." To its credit, VeriSign discontinued its use in a matter of hours, claiming they had planned to make the switch to SHA-1 by the end of January anyway.

MD5 is still out there, however. About 9,000 Web sites use MD5 certificates, estimates MD5 Collision, almost all of them with certificates from VeriSign. Getting rid of it for good will be not be easy. Setting browsers to reject MD5 certificates would effectively shut down a multitude of Web sites and applications. But, ultimately, that's the plan. "Once we're confident that it's not going to hurt a lot of businesses," says Jonathan Nightingale, who works as Mozilla's human security shield, "we want to move the state of the Internet to the algorithms that do the best job of protecting commerce out there."

If the industry doesn't hurry, it will be two steps behind. Wang has already made some headway in breaking SHA-1. It's only a matter of time before it succumbs to a barrage of videogame boxes. The U.S. government, which sets the de facto industry standard, will retire SHA-1 and move exclusively to its more capable sibling, SHA-2, by the end of next year, and plans to develop SHA-3 by 2012. Most new browsers are prepared for the changeover to SHA-2, but with so many outdated versions of Internet Explorer and Windows XP out there, it could take years to develop the necessary patches and software updates.

Should consumers worry? The optimistic view is that vigilante researchers like MD5 Collision are keeping the Internet security industry on its toes. "If [we] weren't hacking this stuff, someone else would be," says Benne Weger, a computer scientist at Eindhoven University of Technology in the Netherlands and a member of MD5 Collision. Is that reassuring?

ILLUSTRATION BY DAVE CUTLER FOR NEWSWEEK