Hacking Capitalism

by Andy Greenberg via Kismo - Forbes *Monday, Aug 6 2007, 10:28pm*
international / social/political / other press

> LAS VEGAS -- Lost seconds mean lost dollars on Wall Street. But the race for faster transactions risks security disaster.
>
> Employees of banks could shut down computers that make quick arbitrage trades across markets, using denial-of-service attacks to overwhelm servers and potentially cause millions in losses. Ultra-fast electronic trades may be especially vulnerable to sabotage. And the need for speed has made things worse -- with financial institutions avoiding software security features that might cause crucial millisecond delays.

So say Jeremy Rauch and David Goldsmith, researchers at the IT security firm Matasano. In a Thursday afternoon presentation titled "Hacking Capitalism" at the Black Hat conference, a gathering of computer security experts, they detailed weaknesses in applications using Financial Information eXchange Protocol, or FIX, a common language used in communications between banks and commercial markets.

FIX's flaws, including a lack of encryption on passwords and usernames, aren't new. But Rauch says that the demand for speed increases the risk of hacking.

"You've got computers taking advantage of the sheer quantity of information available, and they can make enormous amounts of money if they buy and sell quickly enough," says Rauch. "In the name of bigger financial transactions, speed takes precedence over security."

Goldsmith and Rauch say that FIX is just one of several protocols in use with exploitable vulnerabilities known to software developers and banks. But because bank transactions take place on private networks rather than the public Internet, they've long been assumed to be safe.

But as banks become more aware of the potential for cyber-attacks by their own employees, Rauch and Goldsmith say some have contacted them, hoping to resolve the conflict between speed and security.

There are no easy solutions. "The worry is that adding any encryption would hit performance, and performance is everything," said one security director of a financial institution attending the talk, who asked not to have his name or employer revealed. "Even testing is a problem. If a test adds 10 milliseconds, we can't live with that."

There are no documented cases of bank employees using FIX vulnerabilities to block financial transactions. But the unnamed financial institution's security chief warned that if the exploit had been used, it most likely wouldn't have been reported. "And even if it's something that hasn't happened, it's still a risk," he said. "This is financial information flowing over shared networks."

Given the sensitivity of the vulnerabilities highlighted by Matasano's researchers, he had mixed feelings about the public airing of his industry's weak points. "Talks like this are good and bad," he said. "They increase awareness of the risk. But they also give people ideas."

http://www.forbes.com/2007/08/03/banks-fix-security-tech-ebiz-cx_ag_0803techbank.html

---