New hardware should make it possible for all online data to be as secure as a credit card transaction.

By Tom Simonite

A new computer chip will help tackle one of the Web's weak spots—the fact that most data is exchanged without any protection against hackers or eavesdroppers.

For some communications, such as credit card payments and online banking transactions, it is standard to encrypt the information that users and websites send each other. But most online activity is completely unprotected, largely because encrypting communications requires extra work from Web servers and software, which is costly to implement.

Search queries and social media updates, for example, are almost exclusively sent in forms easily read by a third party snooping on Web traffic. Listening in to Web traffic can be as simple as using the same Wi-Fi network as the target, as Ashton Kutcher found when his Twitter account was hijacked at the TED conference earlier this year, by means of a Firefox add-on called Firesheep.

A microchip developed by semiconductor design company Cavium could allow much more—perhaps even all—Web traffic to be encrypted, by reducing the cost of implementing encryption. Cavium's Nitrox III chip is designed to be installed in data centers that serve up Web pages and manage Web apps. It's specialized design is extremely fast and efficient at the mathematical calculations underpinning the encryption that secures Web sites that use the protocol SSL. Sites secured this way have Web addresses that start with HTTPS, instead of HTTP.

When a person accesses an HTTPS site, the computer and the Web server exchange and mathematically verify cryptographic keys to establish a secure link. Any data exchanged over that link is then encrypted and is practically impossible for an attacker to decrypt.

Cavium's new chip can perform the necessary mathematical calculations much more quickly and efficiently than a general-purpose processor inside a Web server, making it cheaper to secure Web traffic, says Jeff Pangborn, the company's principal engineer for networking hardware. "The people operating data centers are very concerned about efficiency and how much power they use," he says.

Pangborn predicts that reducing the cost of securing Web traffic will encourage wider adoption of encryption. "There's going to be more development of applications that require encryption or just always use it," he says.

That may enable more Web providers to follow the lead of Google and Facebook, both of which have made it possible for people to use their services over a secure connection. Google's e-mail service, Gmail, always uses a secure link, and a secure version of Google's search engine is also available. Facebook allows users to set their accounts to always use HTTPS. The Electronic Frontier Foundation, a digital rights group, has begun a "HTTPS everywhere campaign to encourage more Web sites to make such security a default.

Cavium's new chip has 64 cores and is between 12 and 16 times faster than a previous, eight core, version. The new version can also process more than twice as much data using the same amount of energy. Such large increases in performance between generations are unusual, says Pangborn, but this one was necessary if encryption is to be used widely rather than just for specific cases like payments. In the next few months the first Nitrox III chips will be made available for testing by companies that make data-center hardware, with final versions expected to debut early next year.

Bob Wheeler, an analyst specializing in networking chips at the Linley Group, says that many data centers don't use special hardware for their encryption, because only a small percentage of their traffic is encrypted. "If secure connections become more common and a lot of data is encrypted, chips like this will be needed, because data centers are very sensitive to energy efficiency," says Wheeler.

The growth of cloud computing is dramatically increasing the demand for encrypted data, Wheeler says. When applications reside online instead of on a hard drive, all kinds of data become vulnerable, he notes.

Although Cavium's chip, when it launches, may offer the most powerful and efficient way to encrypt data, Wheeler says that less capable chips could still compete with it. Intel and other chip manufacturers are starting to add specialized encryption cores to general-purpose chips designed for use in Web servers. Some companies may consider it more practical to use regular chips with limited encryption functionality than to buy extra, dedicated processors.