Security for Wireless Java

June 27, 2002 — NTRU, a Burlington, Mass., company that offers security software, has released of Java version of its NTRU encryption algorithm. The company says NTRU Neo Java is the first security system designed for all wireless Java devices and applications, including smart cards.

Back in March, NTRU introduced GenuID, a security system for

encrypting data transmitted between RFID tags and readers. Now, the company wants to reach the market for mobile phones, PDAs and other smart consumer devices that may hit the market soon.

Java has its own security functions built into it. But Ed Kountz, senior wireless analyst for the Tower Group, says both customers and financial institutions will want more security as mobile commerce catches on.

“If you are transmitting payment information over a wireless network, strong end-to-end security is essential,” he says. “NTRU is example of companies introducing products to meet the need.”

More powerful encryption has been a problem for Java devices because sophisticated encryption schemes are slow and tend to take up too much of the limited storage space for applications on low-end devices. NTRU was founded six years ago by four mathematicians who had figured out an encryption algorithm that requires far less processing power than public key infrastructure (PKI).

NTRU’s basic operation involves adding 7-bit numbers, a function that is typically very fast. NTRU also breaks the encrypted number into chunks, so it requires less processing power. The company claims that the smallest version of Neo Java takes up just 5 KB of storage space is more than 100 times faster than existing Java security solutions.

“Neo Java has two strong characteristics,” says Guy Singh, NTRU’s director of wireless. “It’s incredibly fast and it is outrageously small, which means you can integrate a strong form of security into any Java application in a mobile device or contactless smart card with no degradation in performance or compromise in your footprint.”

The company is licensing a Java library of encryption tools that will enable application developers, device manufacturers

and Java platform vendors to build advance encryption technology into their products. NTRU says its systems are interoperable, so provided the communications protocols are compatible, an RFID tag using NTRU could be read by a Java smart card reader using NTRU Neo Java.

The company's long-term goal is to have Neo Java adopted as the de facto encryption standard for wireless Java devices. The company points out that Cahners In-Stat/MDR predicts that the wireless Java market will grow at a rate of over eighty percent a year through 2005.

NTRU envisions a world where smart devices with wireless capabilities and RFID tags might be used to pay for content downloaded from the Web and for gasoline and French fries. Singh sees NTRU's technology playing an important role in securing these transactions.

For that to happen, the company will have to win over the Java developer community. So far one outfit, the Tao Group, has signed on to use Neo Java.

"Developers have to be convinced that this is something they need and can afford," says Tower Group's Kountz. "NTRU's product makes sense, but it's hard to say how widely it will adopted at this point."

- Follow
- Follow