

Startup Designs Firewall to Ensure RFID Network Security

NeoCatena's security appliance is designed to protect an RFID network from counterfeit RFID tags, and from attempts to use malware-encoded tags to introduce a virus to back-end systems—or to steal sensitive data.

By Mary Catherine O'Connor

May 8, 2008—[NeoCatena](#), a Sunnyvale, Calif., startup company, has emerged to address an issue its founders believe is of growing importance to end users of RFID technology: system security. The firm has created a security appliance designed to act as a firewall between RFID interrogators and the edge server of middleware an end user employs to collect and transmit RFID tag data upstream to its enterprise software.

The appliance, known as RF-Wall, runs software developed by NeoCatena to protect an RFID network from counterfeit RFID tags, and from attempts to use tags encoded with malware to introduce a virus to back-end systems, or to execute some type of breach to the security of sensitive data, according to the company's cofounders, Boris Wolf and Lukas Grunwald.

While there have been no publicized incidents involving the use of RFID-based network attacks or counterfeit RFID tags, Wolf and Grunwald believe the threats to be real, and say experiments performed by Grunwald dating back to 2004 have proven such things possible. At a data security conference that year, Grunwald introduced software he developed, dubbed RFDump, which reads RFID tags and shows how user data—a read-write field of data designed to carry information beyond the tag ID, as well as other read-only data encoded by the tag's manufacturer—can be modified using either a hex or ASCII editor.

Grunwald used RFDump to change data on the same tags utilized at [Metro Future Store](#) in Germany. In the future, he asserts, nefarious parties could employ interrogators to alter product data, including price, on RFID-tagged consumer goods. In addition, Grunwald has cloned an RFID proprietary access control card and an electronic passport.

Some in the RFID industry—including RFID Journal's editor and founder, Mark Roberti—have deemed Grunwald's assertions that RFID tags represent serious security risks to be far-fetched (see [Industry Group Says E-Passport Clone Poses Little Risk](#), [An RFID Hack Job](#) and [McAfee Report Hypes RFID Threat](#)). Still, there are some end users willing to take a closer look at what NeoCatena is offering. Wolf says his company is currently involved in beta-testing the RF-Wall product for two Fortune 500 companies, which he declines to name. One is a pharmaceutical company based outside the United States, he says, while the other, based in Asia, is in the supply chain industry.

The types of RFID tags that could pose dangers to an enterprise's back-end systems, Wolf and Grunwald claim, are those with user memory—data blocks intended to carry information supplemental to the tag ID—because that is where a nefarious party could execute known data attacks such as an SQL injection, designed to exploit an SQL database, or an attack using XML code.

Passive high-frequency tags, which have been widely manufactured and employed across numerous industries for years, tend to have larger amounts of user memory than EPC UHF tags do. However, there is a trend among makers of UHF tags to add an increasing amount of user memory (see [NXP Boosts EPC Gen 2 Tag Memory, Performance](#) and [Alien Technology Announces New EPC Gen 2 Chip](#)). Tag makers are targeting these tags to such applications as drug-tracking, in which pharmaceutical supply chain partners may add chain-of-custody data to the user memory on tags attached to drug packaging.

There are two main business risks associated with RFID networks, NeoCatena contends: that a tag's user data could be utilized to pass malware or viruses onto back-end systems, which could interrupt business processes or expose sensitive business data; and that RFID tags could be cloned, or their data manipulated, with the goal of defrauding an RFID-based transaction process. One example of the latter scenario would be if someone were to manipulate the data encoded to an RFID-based transit card to artificially add monetary value to the tag's data, then use the card to ride a transit system illegitimately.

To thwart that type of tag data manipulation, Grunwald says, the RF-Wall program would employ a digital signature to detect whether the information stored to a transit card's RFID tag was manipulated since it was last read. "The software calculates the signature when the ticket is handed out, and then again when it is being read [presented to a turnstile]," he says. "If the data on the card is not what it is supposed to be, then the signature won't match."

Most RFID tags used for transit applications contain the Mifare Classic chip, made by [NXP Semiconductors](#). While the Mifare protocol uses a proprietary data-encryption method to protect tag data, two separate research teams have recently shown the ability to break the encryption algorithm (see [NXP Announces New, More Secure Chip for Transport, Access Cards](#)).

If the RF-Wall software were to detect something indicative of a virus or malware, Wolf says, or if the digital signature on a tag read did not execute as expected, the business processes that would normally allow a tag to be accepted—such as a green light on a portal reader in a supply chain, or the unlocking of a turnstile to allow a commuter passage to a transit system—would not occur. What's more, a rules engine within the software would trigger appropriate alerts to business managers.

According to Wolf, NeoCatena is working on making the RF-Wall appliance scaleable to support multiple readers. The device currently supports reader protocols used by most off-the-shelf RFID interrogators, he says. It may eventually also support [EPCglobal's](#) ALE protocol, which would enable end users to install the RF-Wall behind their RFID server or reader networking device—though such an architecture would leave the server or networking device vulnerable to attacks or viruses.

RELATED ARTICLES In addition, NeoCatena offers a software product known as RF-Manager, which runs on a server and manages a distributed cluster of RF-Wall appliances. The firm also provides companies an RFID security auditing service through an add-on software module that can run on the RF-Wall appliance. This audit software is intended to act as an early-warning system for companies when it detects tag data that could represent a threat to back-end data security, or to legitimate business processes.

NeoCatena says its auditing service can also help companies comply with such regulations as the Sarbanes-Oxley Act in the United States, Germany's Control and Transparency Act (KonTraG) and Publication Transparency Act (TransPuG), and similar laws in Europe, by detecting business risks in RFID-enabled applications.