CYBER SECURITY CONNECTIONS

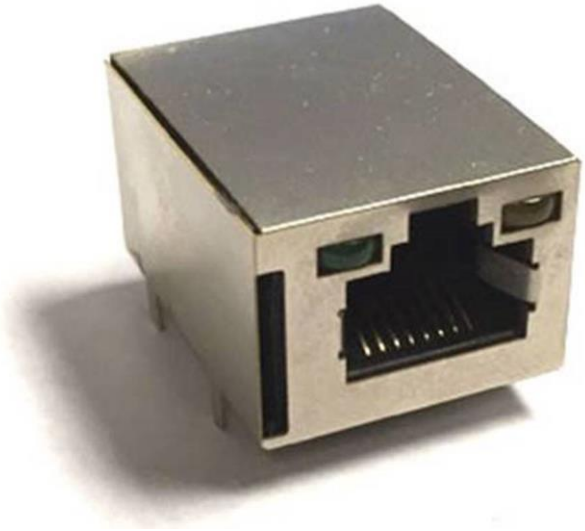
SMART®

New Approach to Networking and Computer Security

'Security On A Chip In A Connector'

Xmultiple announced a new approach to networking and computer security. Xmultiple was granted the #9,509,109 patent which embeds security into a microprocessor chip which integrates into a RJ connector's used for all connections to the Internet.

Putting "security on a chip integrated into a RJ connector" sounds like the right kind of approach to stop unauthorized access right at the connection source. As Mr. Alan Pocrass, CEO of Xmultiple Technologies, Inc., explains it, "security on a chip integrated into a connector" does not mean just stuffing antivirus into silicon, it is also about managing and securing computers, networking, and mobile devices right at the source of the connection.



The emerging Internet of Things (IoT) marketplace is radically changing our world. Estimates suggest that in the next 4-5 years, 30 billion to 50 billion "things" will be deployed. These devices will range from relatively simple sensors to complex data collectors and they will require security right at their source.

If you give a computer or mobile device to an employee that contains sensitive information on it, you want to make sure it does not fall into the wrong hand and more importantly you want to stop any unauthorized use on the device.

Security is a "device management" challenge that becomes more difficult when you have to do it across multiple platforms, such as Microsoft Windows, Apple's iOS and Google's Android. It's a headache not only the businesses who provide these devices, but the telecommunications companies that connect them.

How do these businesses manage computers and mobile devices? Currently, with software. Aside from some location features, most of these kinds of tasks – file virus scanning for example -- are done via applications and not baked into the device itself. All kinds of companies make money providing these features in applications for security. Our Xsmart can be capable of performing file virus scan on the connector and these files never leave the connector. The device with the Xsmart connector is protected before the security issues ever enter the CPU or memory of the device.

Security is currently handled at "the application level". With the Xmultiple "Xsmart" connector, it is moved into the hardware itself. In the marketplace, we call this "moving the functionality down the stack," which is an easier way of saying that the action is going to happen deeper inside the system levels, in this case "below" the operating system level.

"We deal with device reputation in different operating systems all the time. It would be great if all this was built into the connectors hardware and you didn't have to deal with software security vendors to perform this function," says Mr. Pocrass. **The key element of the Xsmart connector is that it has a high capacity Micro SD flash memory card to store mass amounts of data to keep unauthorized data from passing through the Xsmart connector until the integrated software chip checks that the data is authorized and virus free.**

Another benefit: enhanced trust and security. By moving security down the stack, Xmultiple can make devices safer. Packets of information could be checked as they are received by the device's connector, for example, rather than by some application running on top of the operating system. That means it'll likely be harder for hackers and other tinkerers to bypass a device's security mechanisms. For more information contact Robin Millard at robinm@xmultiple.com or call her at 805-579-1100.

Xmultiple Technologies, Inc., 1060 E. Los Angeles Avenue, Simi Valley, CA 93065, www.xmultiple.com, info@xmultiple.com