

THE CREDIT UNION JOURNAL

www.cujournal.com

THE NATION'S LEADING INDEPENDENT CREDIT UNION NEWSWEEKLY October 18, 2004

IP-Based ATMs Popular, But Security Vulnerabilities Lead CU To Take Action

By Kevin Jepson, *Technology Writer*

EUREKA, Calif.—New ATMs running on Internet Protocol (IP) are all the rage for credit unions looking for speed and regulatory compliance—but the IP-based machines may be vulnerable to security risks not associated with their legacy predecessors, according to Glenn Powell, vice president of Information Systems at Coast Central CU.

“When we converted to IP-based ATMs, it occurred to me that we suddenly had Windows-based terminals,” said Powell. “Now I had to worry about viruses and worms. In addition, our ATMs are a bit more vulnerable because they’re off-site and out of my control.”

Security for IP-based ATMs is still maturing, Powell continued. “I spent time talking to other IP users, and a lot of people hadn’t thought about ATM security.”

Powell said that Diebold, Inc., which supplies Coast Central’s IP-based ATMs, responded to his concern with the suggestion that he put a firewall behind each new ATM. “I wasn’t satisfied with the suggestion because configuring the firewalls and keeping them updated with patches is difficult. And firewalls are only one layer of protection.”

Diebold declined to elaborate on network security for its IP-based ATMs.

For a while, Powell “lay awake at night worrying.” His first IP-based ATM went up one year ago, and now Coast Central’s entire fleet of 18 ATMs are communicating via IP, he said. “General paranoia led me to take action,” Powell continued.

In July, he realized he could apply the same “layered” security that

General paranoia led me
to take action.

—Glen Powell

protects Coast Central’s Internet banking server to the new IP-based ATM fleet.

That “layered” security is provided by VaultIT, Simplere-Webb,

Inc.’s collection of Managed Security Services, including Firewall Management and Intrusion Detection and Prevention.

Since 2002, Coast Central has used the VaultIT solution, which includes control of Cisco Security Agent (CSA) software that detects malicious behavior.

VaultIT compiles real-time information from the individual CSA host agents on each device in Coast Central’s network. The solution also tracks the internal and external network sensors that monitor IP traffic across Coast Central’s 10 branches and retail outlets.

“The firewall will permit traffic based on port and protocol, whereas the CSA software will look for a greater variety of behavioral-based vulnerabilities hidden within the allowed network traffic,” added Sean Martin, consultant for Simplere-Webb. “In addition, the VaultIT solution provides enhanced

reporting capabilities.

“Based on our alarm policies and Coast Central’s security profile, we can deploy a variety of defenses including blocking an IP address or shutting down a switch port at the credit union when we encounter malicious traffic,” Martin explained.

“But even when we manage the solution, Coast Central retains control,” said Chris Cobb, chief financial officer at Simplere-Webb. Cobb referred to the Client Portal, from which Coast Central manages the CSA and can lock and unlock the agent for network changes without Simplere-Webb’s intervention.

Austin, Texas-based Simplere-Webb provides 24X7 network monitoring and network consulting services.

The \$540-million Coast Central CU migrated its ATM network to IP Communications in response to Triple DES (Data Encryption Standard) regulations, Powell said. MasterCard International Inc., VISA U.S.A. Inc. and associated network providers have mandated that all hosts and processors make ATMs compliant by December 2005.

Triple DES is an encryption method that is designed to improve PIN security.

CUJ Resources



For more info on this story:
* Coast Central CU at
www.coastccu.org
* Simplere-Webb at
www.swinc.com

SIMPLERE WEBB

512.322.0071 • info@swinc.com