Miercom

Lab Testing Summary Report

December 2005
Report 051120

Product Category:
Remote Access Security and Control

Vendor Tested:
Cranite Systems

Product Tested:
SafeConnect™ v 1.0

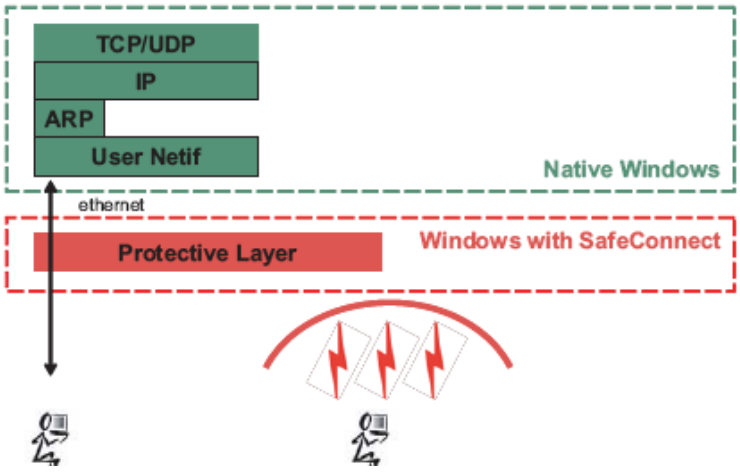
Miercom CERTIFIED SECURE™

Key findings and conclusions:

- **Cranite Systems' SafeConnect™ was the first remote security product tested to pass all vulnerability tests and withstand complex attacks**
- **SafeConnect employs broader use of authentication and encryption, compared to IPsec VPN clients**
- **SafeConnect provides better remote access security and administration than most VPN products**
- **Secure multicast and peer file sharing work as if clients are local, unlike VPN products tested**

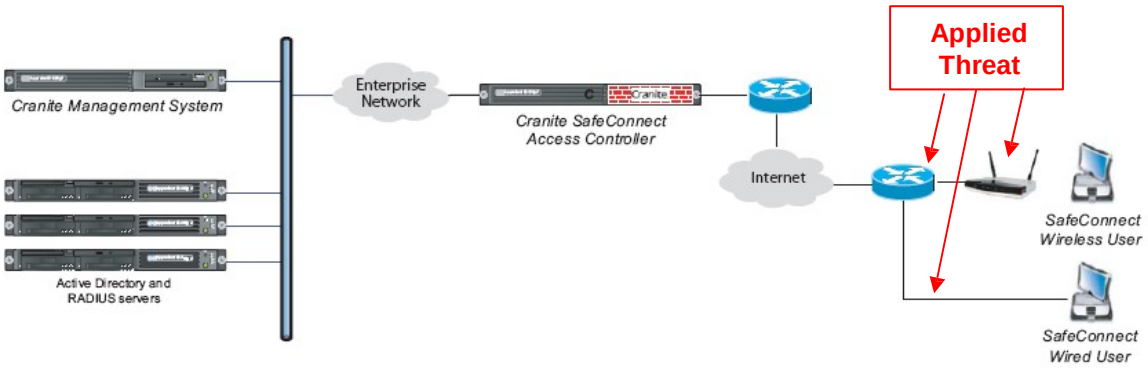
Cranite Systems SafeConnect 1.0 was independently evaluated, under Miercom's Certified Secure™ security and vulnerability test certification program. Summary test results documenting the certification of this product are included in this report. Cranite's role in providing high-end security products previously restricted to the government market positions the vendor well as a security product provider for other markets.

Cranite's SafeConnect PC client was evaluated by Miercom labs and found to be a very effective remote access solution for wireless and other remote users. We found SafeConnect to offer superior security to commercial IPsec VPN products. We also found that SafeConnect provided remote users more functionality, such as secure multicast and remote resource sharing, both of which are typically not available with legacy VPN technology. SafeConnect's unique ability to encrypt information including IP header, port addresses and connection negotiation allow SafeConnect to provide a more secure remote access solution when compared to legacy IPsec VPNs. Using IPsec VPN technologies we demonstrated that we could fairly easily disrupt



Cranite Systems SafeConnect offers better protection from would be hackers by encrypting more of the IP Packet than legacy IPsec VPN products. Encrypting additional IP header information makes it much harder for would be hackers to exploit.

Test Bed Setup



The test bed network included Windows 2003/Exchange 2003-based Domain Controller, DNS server and DHCP server. For authentication of wireless clients we used Funk Software's Steel Belted RADIUS server v5.0, running on a Windows 2000 server. The RADIUS server worked in conjunction with Windows' Active Directory.

We reviewed each VPN and security package using a mix of laptops running Microsoft XP Pro and Windows 2000. We intentionally used a different wireless adapter in each laptop, including units from Broadcom, Proxim Orinoco, D-Link AirPlus, and Linksys.

Veriwave's AP Management Performance Test Suite v2.5 package running on an IBM platform was used to test AP performance. Test traffic passed between Veriwave's wireless traffic generator/performance analyzers and the APs under test. Each laptop client was required to be RADIUS-authenticated, and then all traffic was encrypted using "WPA TKIP."

AP recovery time -- the time it took a "mistakenly unplugged" access point to "re-insert" in the network, and begin passing wireless traffic again -- was measured by a continuous ping stream as well as the Veriwave test system.

SafeConnect Access Controller (SAC) was installed at our simulated "Corporate Network" for remote clients to authenticate. We used SafeConnect version 1.0 client installed on client computers to access from remote LAN and wireless locations.

SafeConnect continues to be monitored in Miercom's ReliabilityAssured™ and CertifiedSecure™ programs, which will provide other reviewers, customers and developers the latest available information on SafeConnect's performance and functionality as a network security and reliability enhancing product.

connections, capture key session negotiation information, and insert ourselves in the "secure" VPN connection without alerting the user or corporate gateway to the intrusion. We did not employ other security measures on the network that would normally be present, firewall, IPS etc. as we were testing the inherent security that these technologies provide. However, it is very possible that many of these advanced countermeasures will be either missing or disabled (for remote administration, i.e.,) for remote users connecting through hot spots and other unsecured networks.

Vulnerability Assessment

We submitted SafeConnect and the IPsec VPN alternatives through a battery of vulnerability test scenarios divided into six categories:

1) Surveillance and reconnaissance - under this category of tests we explored different means to eavesdrop on sessions and decipher message content and collect information on the supporting network including counter measures that might be employed. We observed that the IPsec VPN client allowed IP header, port destinations, and VPN connection negotiation to be captured and read in the clear with little difficulty by our hacker team. Whereas by using the Cranite SafeConnect client we could monitor the connection negotiation but information we needed to identify to launch our attacks was encrypted. Although this encryption is not unbreakable, it would be extremely difficult to decipher.

2) IP Header Exploits - The next set of vulnerability tests focused on IP Header exploits. Both IPsec VPN clients were found to allow unencrypted surveillance of the IP header information and were susceptible to a wide range of both commonly known attacks and advanced attacks. Again with SafeConnect we could not attempt these attacks without knowing the IP header information that is encrypted with Cranite SafeConnect. We attempted the attacks nonetheless using a previously known default gateway and other common addresses but SafeConnect could not be cracked.

3) Directed and distributed denial of service attacks (DDOS) - IPsec VPN products tested allowed us to execute and exploit with ease using a series of denial of service attacks against the authenticating device, the gateways, as well as

the VPN clients themselves. We could easily interrupt VPN sessions, or prevent other VPN sessions from initiating. With Cranite's SafeConnect we could not penetrate the client PC's ARP cache or routing table, we also could not identify some of the key information hackers need to attack those specific resources for the DOS attacks

4) Payload monitoring and associated attacks - We attempted to monitor and use information from the data - payload section of the packets. All products tested satisfactorily and employed encryption so no payload content information could be exploited.

5) ARP Cache - The ARP cache in both IPsec VPN clients could be manipulated. Further entries to the routing tables on the clients could be manipulated. The gates were then left wide open for our hackers to exploit the IPsec VPN clients. However, SafeConnect could not be exploited.

6) Man-in-the-middle - Once the ARP and routing tables of the IPsec VPN clients were compromised in the previous test, we conducted the "man-in-the-middle" complex attack. This attack simulates an attack that could be conducted at a wireless or other unsecured Internet hot spot. We intercepted IP Header information and VPN authentication details from the remote user and inserted our hacking tool virtually in the middle. Once inserting our intrusion tool, we could terminate the IPsec VPN connections (how quickly depends on the client's timeout setting, which was 90 seconds during our testing) and then capture the IKE handshake when the user tries to re-establish another connection. A passive dictionary attack was launched against the PSK (group password) in IKE Aggressive Mode PSK authentication. We also inserted other rogue addresses in the local ARP cache to further exploit the network and the IPsec VPN clients.

Vulnerability Assessment Summary		
TESTED ATTACKS	Cranite SafeConnect	IPsec VPN Client
Surveillance	√-	**FAIL**
IP Header	√	**FAIL**
DDOS	√	**FAIL**
Payload Monitor	√	√
ARP Cache	√	**FAIL**
Man-in-the-middle	√	**FAIL**
Alleviated Threats	**92%**	**17%**

Cranite SafeConnect passed *all vulnerability tests, while legacy IPsec VPNs were found inherently vulnerable*

Cranite Systems Solution Overview	
Product tested, version	SafeConnect Access Controller 1.0 and SafeConnect Client 1.0 Cranite Management System 1.0
Description	Linux based servers and standard PC clients
AP support	Works with any 3rd party APs; tested with Cisco Aironet 1100/1200 and Buffalo AirStation G54 APs
Main functions performed	• Client authentication • Enhanced encryption & message integrity • Seamless directory integration • Policy management • Rogue AP detection and mitigation via third party product
Price, US list	Software license based on number of concurrent users

Source: Miercom Independent Security Evaluation, November 2005

We could not exploit the SafeConnect client with this type of attack as all the necessary information from IP headers and port numbers were encrypted. We found the ARP cache of a SafeConnect client cannot be modified while the client has a SafeConnect connection — the hacking tool cannot insert itself "in the middle".

The chart on the left summarizes the six levels of attacks and surveillance conducted on the systems under test. Cranite Systems' SafeConnect passed all tests for security and vulnerability assessment evaluation. Some points were deducted as encrypted information could be surveyed although it was found unusable by our hackers. A perfect score would imply the client communications was completely obscured from monitoring.

Miercom will continue to monitor SafeConnect 1.0 and watch for further product enhancements in subsequent releases. The current release is shipping and immediately ready for deployment.

Miercom Certified Secure™ Certification

Based on Miercom's thorough testing of Cranite's SafeConnect and validation of capabilities, operation, and features, as described herein, Miercom proudly attests the Cranite SafeConnect 1.0 is Certified Secure™ in accordance with the Certified Secure Testing Program of *Miercom* and partnering labs, effective for one year from test certification or until next product release.

- The system features excellent client ease of use and increased functionality beyond IPsec and SSL VPN clients
- SafeConnect client is well suited for any remote locations including hotels, transient work sites, SoHos and regional offices.
- Client software features AES encryption
- SafeConnect works using both wired and wireless access
- SafeConnect is application agnostic, no plug-in required
- SafeConnect enables remote users to securely access all enterprise applications

About Miercom's Product Testing Services…

With hundreds of its product-comparison analyses published over the years in such leading network trade periodicals as *Business Communications Review*, *Network World and VoIP Magazine*, Miercom's reputation as the leading, independent product test center is unquestioned. Founded in 1988, the company has pioneered the comparative assessment of networking hardware and software, having developed methodologies for testing products from enterprise class VoIP gateways and IP PBX's to carrier grade switching equipment and gateway products. Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs for VoIP, Security and Reliability: Certified SIP™, Certified Reliable™ and Certified Secure™. Products may also be evaluated under the NetWORKS As Advertised™ program, in which networking-related products must endure a comprehensive, independent assessment of the products' usability and performance.

379 Princeton-Hightstown Rd., East Windsor, NJ 08512
609-490-0200 z fax 609-490-0610 z www.miercom.com

Report 051120