



WHITE PAPER

WIRELESS SECURITY IS BROKEN AND IT DOESN'T MATTER

An information security white paper presenting a sensible and viable approach to securing wireless networks.



INTRODUCTION

It's hard to pick up an industry magazine or a newspaper without finding an article about the latest security flaw in one of the wireless protocols. Companies are scrambling to fix the problem by throwing money and resources at new standards and products. Organizations everywhere are wasting financial resources on technologies that prevent their users from taking advantage of wireless networks because of perceived security reasons.

Most of us accept that wireless networks are vulnerable, but we don't realize that the reality of the situation is that it just doesn't matter. We've been using technology to protect systems and secure sensitive information traversing untrusted networks, such as the Internet, for over 10 years. Attempts to fully secure the Internet or even encrypt all Internet traffic have all but died. We know the Internet is untrusted, yet we can still conduct business over it because we have security countermeasures at our disposal that can protect us in this environment.

Wireless networks should not be trusted now or even in the future. Acknowledging the fact that wireless networks are untrusted and deploying time-tested countermeasures to protect our communications and our data makes sound fiscal and technical sense.

THE FIRST LINE OF DEFENSE

The Internet was intended to be an open network that had virtually no access control or authorization. When you examine the TCP/IP (v4) protocol you will find very little in terms of real security controls. As computing evolved, we began to use the Internet to conduct business transactions. Vendors of all types tried to secure the Internet to allow e-commerce to proliferate. While other initiatives were trying to control the Internet, Virtual Private Networks (VPNs) emerged as good mechanisms to remotely access or join networks. Independently, firewalls separated internal networks and critical systems from the vast untrusted Internet and they started to control the data that could flow to and from it. Eventually, everyone gave up trying to tame the beast—satisfied that the measures that we put in place could, for the most part, allow us to use the Internet safely for business and more.

UNPLUGGING

After the onset of wireless technology, we became used to the fact that we could work from almost anywhere. We became enamored with not being tethered to a wall socket. There was freedom. We wanted to work from everywhere—in motion. Today, wireless network vulnerability announcements are commonplace. Headlines point to the fact that wireless networks can not be trusted and there are a myriad of vendors scrambling to propose solutions to fix the problem. Haven't we heard this before?

BACK TO THE FUTURE

We all know that even the most security-conscious organizations in the world use and trust VPNs to conduct business over the Internet. The only difference between the Internet and a wireless network, if both are viewed as untrusted networks, is the absence of wires. So, what aspects of today's strong high-security VPNs might be particularly applicable in a wireless scenario?

- State of the art VPNs require strong mutual authentication with digital certificates. Two-factor public key authentication requires something you have (usually some sort of ID) and something you know (a password) has become the standard for high security VPNs today.
- Once connected, secure VPNs put robust controls in place that "lock down" remote devices to the corporate network—enveloping it in the policies, rules, content filtering, and protections of the enterprise. This approach is much stronger than relying on the roaming device to secure itself. Administrators can now control peripheral devices in the same way as their internal systems.
- High-security VPNs not only encrypt normal packets traversing the network, but the packets that are sent to initialize the session are encrypted using asymmetric keys. They cannot be hijacked—ensuring confidentiality.
- Secure VPNs have the option of checking packet integrity to ensure that the data is not modified while in transit.

- Stealth mode. High-security VPNs should have the ability to ignore pinging from the outside while still being centrally managed. So, even if someone were able to attempt to break into a network over the air and through the VPN gateway, they would see nothing. You can't hack what you can't see.
- A state-of-the-art high-security VPN allows a user to move from one wireless access point to another with no perceived interruption in the connection to re-authenticate—saving time and enabling time-sensitive applications, such as Voice over IP.

CONCLUSION

Deploying high-security VPNs to simultaneously protect both wireless and wired communications makes more sense now than ever before. VPN technology has stood the test of time and is being used to lock-down the communications of the most security-conscious organizations on the planet. Information Technology departments, that are stretched for both time and money, can protect themselves from vulnerabilities while giving their organizations the flexibility they demand. In addition, options such as outsourcing high-security VPNs are being exercised by organizations who want to ensure tight security, reduce capital expenditures, and eliminate management headaches. Forget about the next wireless vulnerability or even listening to the cacophony of messages that you are bombarded with every day about the latest “band-aid” solution. You just might have a technically-solid, time-proven technology right at your fingertips.

ABOUT BLUE RIDGE NETWORKS

Blue Ridge Networks develops impenetrable remote access solutions for wireless and wired environments. Blue Ridge Networks was responsible for the industry's first commercial virtual private network and has since completed widespread deployments across commercial and government sectors. The Blue Ridge Networks BorderGuard product suite has been deployed globally and in demanding applications such as wireless LANs, extranets, site-to-site and remote access VPNs, and thin client computing—with no reported vulnerabilities in over 12 years. The company has earned numerous government agency certifications, including: JITC certification, FIPS 140-2 validation, Common Criteria certification, Army TIC approval, HIPAA compliance, and the Department of Defense SPOCK validation. Information about Blue Ridge Networks products and managed services can be found at www.blueridgenetworks.com.