International Journal of Information Technology and Management

Vol. VI, Issue No. II, May-2014, ISSN 2249-4510

THE USE OF WI-FI NETWORK SECURITY KEYS

International Journal of Information Technology and Management
Vol. VI, Issue No. II, May-2014, ISSN 2249-4510

The Use of Wi-Fi Network Security Keys

Pushkar Raj[1] Rashmi Kumari[2]

[1]Assistant Professor, N.S.I.T. Bihta Patna Bihar

[2]Assistant Professor, S. Sinha College Aurangabad Bihar

Abstract – There are a few steps involved in configuring security on a Wi-Fi network, the management of wireless keys turns out to be the most important. These keys are digital passwords (sequences of letters and/or digits, technically called a "string") that all devices on a network need to know in order to connect with each other. In particular, all devices on a local Wi-Fi network share a common key.

Keywords: Wi-Fi, Network, Security, Encryption, Keys

---------------------------♦-----------------------------

INTRODUCTION

A consideration on any computer network, security is especially important on Wi-Fi wireless networks. Hackers can easily intercept wireless network traffic over open air connections and extract information like passwords and credit card numbers. Several Wi-Fi network security technologies have been developed to combat hackers, of course, although some of these technologies can be defeated relatively easily.

Computer system security has become a major concern over the past few years. Attack, threat or intrusions, against computer system and network have become commonplace events, many system device and other tools are available to help counter the threat of these attack. Analyzed from proposal [1] and [2] highlighted currently countermeasure against from security violation.

NETWORK DATA ENCRYPTION

Network security protocols usually use encryption technology. Encryption scrambles data sent over network connections to hide information from humans while still allowing computers to properly decipher the messages. Many forms of encryption technology exist in the industry.

RULES FOR MAKING WI-FI KEYS

Setting up security on a Wi-Fi network router , wireless hotspot or client device involves choosing from among a list of security options and then entering a key string that the device stores away. Wi-Fi keys exist in two basic forms:

- ASCII – a sequence of letters and/or decimal numbers
- hex – a sequence of hexadecimal numbers
- Hex keys (strings like '0FA76401DB', without the quotes) are the standard format that Wi-Fi devices understand. ASCII keys are also called pass phrases because people often choose easy-to-remember words and phrases for their keys, like 'ilovewifi' or 'hispeed1234'. Note that some Wi-Fi devices support only hex keys and will either disallow entering passphrase characters or report an error when trying to save a passphrase. Wi-Fi devices convert both ASCII and hex keys into binary numbers that become the actual key value used by the Wi-Fi hardware to encrypt data sent over the wireless link.
- The most common security options used for home networking include 64-bit or 128-bit WEP (not recommended due to its inferior level of protection), WPA andWPA2). Some restrictions on the choice of Wi-Fi key depend on the option chosen as follows:
- 64-bit WEP - passphrases must be exactly 5 ASCII characters; keys must be exactly 10 hexadecimal digits
- 128-bit WEP - passphrases must be exactly 13 ASCII characters; keys must be exactly 26 hexadecimal digits

- WPA and WPA2 – passphrases must be between 8 and 63 ASCII characters; keys must be 64 hex digits

SYNCHRONIZING KEYS ACROSS LOCAL DEVICES

The simplest method to ensure all devices on a home or local network are correctly configured with the same Wi-Fi key is to first set a key for the router (or other access point) and then systematically update each client one by one to use the matching string. Exact steps for applying a Wi-Fi key to a router or other device vary slightly depending on the specific hardware involved, but as a general rule:

- enter keys into the router’s administration pages for wireless settings

- enter keys into a client device through its Settings app or operating system control panel

ETHERNET IP ENCRYPTION APPLIANCE WITH KEYNET IP MANAGER

Cipher X 7211 IP encryption provides strategic-level secure communications and network encryption for global IP networks — voice, data, and video. It integrates seamlessly into existing or new networks without degrading network performance, while the unique combination of flexibility, scalable 1 Gb/s performance, and KEYNET IP Manager delivers a robust, cost-effective solution that is easy to deploy, monitor and manage. Some applications include secure voice over IP/VoIP, secure satellite communications, secure video conferencing, secure video surveillance, and secure data for LAN to LAN, LAN to WAN and multisite networks. We assume in this approach that accuracy alarm, risk rating and event response allow increasing accuracy. In the other hands, we identified some instances [3], [14], [5], [6], conducted to proposed composite and associate between accuracy and event response or contrary.

BENEFITS

- Strategic-level data protection

- Scalable, interoperable wire speed performance

- Flexible network configurations and security policies

- AES 256-bit; easily integrates national algorithms

- Multi-layer key and device management

- Cost-effective IP encryption solution

- No network architecture changes or performance degradation

- Easy to deploy, monitor and manage

IP ENCRYPTION SOLUTION SEAMLESSLY OVERLAYS ON NETWORKS

Cipher X 7211 IP encryption enables data to securely transit networks over fiber, satellite or microwave, including multicast applications such as secure video conferencing. Wire-speed Cipher X 7211 IP encryption is a tuneless, Layer 3 or 4 solution, which overlays on top of existing or new networks — no network architecture changes or performance degradation.

IP ENCRYPTION WITH SUPERIOR-GRADE SECURITY

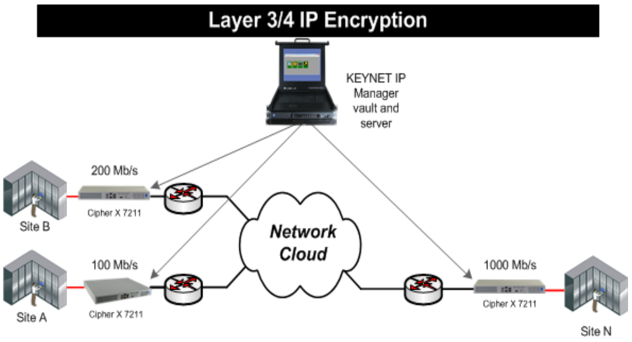
Cipher X 7211 IP encryption is a FIPS 140-2 Level 3 designed, hardware-based encryption solution with multiple layers of protection. It comes in a 1RU anti-tamper rack-mountable enclosure. The AES 256-bit algorithm in Galois Counter Mode provides superior-grade IP encryption and authentication. Optionally, national algorithms can be easily integrated without hardware modification.

A three-tier symmetric key management architecture integrating Cipher X 7211 IP encryption and KEYNET IP Manager maximizes network security. The Cipher X 7211's embedded key vault processor securely manages system parameters, generates local data encryption keys and ensures cryptographic integrity, while KEYNET IP Manager provides secure management communications and key delivery.

KEYNET IP MANAGER EASILY MANAGES AND DEPLOYS CIPHER X 7211 IP ENCRYPTION

Centralized and automated key and device management of a Cipher X 7211 IP encryption secure network is provided by KEYNET IP Manager. KEYNET consists of a Windows 7 rack mount server and 1RU tamper-proof security vault. Multiple layers of protection secure keys at every point in their life cycle with limited human intervention.

KEYNET has user-authenticated, role-based security and it simplifies the provisioning and management of the wide-range of network configurations and security requirements supported by the Cipher X 7211 IP encryption security policy engine. With KEYNET's intuitive user interface and automated polling of device alarms and logs, a network expert is not required to manage network security.



CONCLUSIONS

An essential in network security is to monitor and analyzed network traffic for profiling user behavior. A robust defense system has to hold parameters representing both normal and abnormal user behavior patterns, and such parameters require to be recalibrated consistently to adjust for changes in network and user behavior over time.

We found that the Intrusion Detection, which proactive technique is, prevent the attacks from entering the network by examining various data record and detection demeanor of pattern recognition sensor, when an attack is identified, intrusion prevention block and log the offending data. Ghorbani [3], IDS and IPS, currently IDS can be seen as a traditional second line of defense system, it is becoming more difficult to apply security access control [4].

REFERENCES:

[1] E. Guillen, D. Padilla, and Y. Colorado, “based Intrusion Detection and Prevention Systems,” Latin-American Conference Communications, 2009, pp. 0-4.

[2] B. Cao, Z. Zhihong, L. Tie, Y. Zhongde, and L. Jiren, “A Study on Performance Improvement of Gateway Anti-Virus System Based on File Scanning,” Control and Decision Conference 09, 2009, pp. 2293-2295.

[3] T. Ghorbani, A.A., Lu, W., Network Intrusion Detection and Prevention : Concepts and Technique, Springer, 2009.

[4] S.H. Oh and W.K. Lee, “An anomaly intrusion detection method by clustering normal user behavior,” Computers & Security, vol. 22, 2003, pp. 596-612.

[5] F.G. Marmol and G.M. Perez, “Security threats scenarios in trust and reputation models for distributed systems,” Computers & Security, vol. 28, 2009, pp. 545-556.

[6] T. Walker, “Practical management of malicious insider threat – An enterprise CSIRT perspective,” Information Security Technical Report, vol. 13, 2008, pp. 225-234.

[7] http://www.tccsecure.com/products/network encryption /cipherx7211 detail.aspx?_vsrefdom=gppc&gclid=CIbwxYH40sACFQiTjgodAJQA-A

[8] http://compnetworking.about.com/od/wirelesssecurity/a/mastering-the-use-of-wifi-network-security-keys.htm