# Security Requirements for Wireless Networking

Developed by

RYSAVY RESEARCH

## Table of Contents

## Introduction

Organizations are deploying mobile computer applications over wide geographic areas, using an increasing number of private and public networks, many of which are wireless. Meanwhile, there are a growing number of regulatory requirements for the protection of communicated data, particularly in government, financial and medical areas. Even without regulations, nearly all enterprises and organizations want to ensure that their data communications are secure, and that their networks remain protected from external attacks.

To implement security policies and to most effectively design their security architectures, network managers must understand the security features of the networks they are using, as well as their limitations.

This white paper discusses security recommendations and regulations, reviews the security mechanisms available with public wireless networks, explains where they fall short, and concludes that only an end-to-end security approach such as a mobile VPN can fully address the security needs for most applications.

## Security Requirements

While any organization wants to protect its sensitive data, to detect tampering of data and to limit access to authorized individuals, various industries must also comply with an array of regulatory and industry requirements and guidelines. These include among others, the Sarbannes Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Criminal Justice Information Services Division (CJIS) Security Policy, and the PCI (Payment Card Industry) Data Security Standard.

One common requirement, especially for government organizations, is that sensitive data that is stored or communicated over public networks must be encrypted using certified algorithms. For instance, the Wireless Policy of the CJIS Security Policy[1] states “All new wireless upgrades contracted after the close of federal fiscal year 2002 (September 30, 2002), shall support a minimum of 128-bit encryption for all data.” The National Institute of Technology and Standards (NIST) FIPS 140-2 is a widely cited requirement.

Another common requirement is for users to authenticate themselves using two-authentication, generally achieved by a combination of something the user possesses such as a security token (e.g., USB dongle or security smart card), and something the user knows (e.g., password). Biometric approaches can also be used as one of the authentication factors.

[1] CJIS Security Policy, August 2003, Version 3.2

Regulations are becoming more stringent, both at the state and federal level. Organizations designing new mobile-access solutions need to plan accordingly to ensure they comply with both current and future requirements.

## Wireless Operator Security Limitations

Wireless operators have implemented a number of security mechanisms within their networks. While useful, the operator provisions have shortcomings, as explained in this section.

The typical security mechanisms that operators provide include device authentication, encryption of the radio link, optional encryption for Internet communications, private circuits and firewall rules.

In the case of user authentication, network operators are primarily concerned with fraudulent use of their network, and so the authentication mechanisms are designed to ensure that only legitimate devices connect to the network. With Global Systems for Mobile Communications (GSM) networks, for instance, the network validates the credentials in the Subscriber Identity Module (SIM) card. In 2G cellular networks, there are no provisions to authenticate the network to the user system. This allows man-in-the-middle attacks where an attacker could operate a low-power equipment that simulates a wireless network, and could acquire user credentials. While this is not a trivial undertaking, cellular technologists considered it a sufficient threat that 3G technologies such as Universal Mobile Telecommunications System (UMTS) employ bidirectional authentication.

The problem, however, is that users usually do not know whether they are on a 2G or 3G system, especially as operators have implemented seamless handover for both voice and data services between their 2G and 3G networks. The handover allows active data sessions to originate on one network, and then to carry across to the other network with the same IP address. For instance, the user could start their session on a 3G system but drive into a 2G-only coverage area. This problem of 2G vs. 3G systems is also an issue when we look at encryption.

With respect to user authentication, some mobile devices (e.g., GSM/UMTS), allow for devices to be configured so that a user must enter a PIN before using the device. However, a user can easily disable this mechanism. It also does not satisfy two-factor authentication requirements.

There is an additional concern with respect to authentication, particularly if the customer has arranged for a private connection between their network and the operator network. Typical arrangements include network VPNs and Frame Relay circuits. Often, these custom arrangements are made in conjunction with a specific pool of IP addresses that the network assigns to mobile systems, facilitating firewall rules at the customer site. The vulnerability is that access is based on the device's credentials, not the user's credentials. If the user's network card, laptop or smartphone is lost or stolen, then in many circumstances it will be possible for a third party to gain access to the enterprise network via the private connection.

The primary security mechanism promoted by operators is their encryption of the radio link. 3G systems have indeed implemented robust measures, with both UMTS[2] and CDMA2000 Evolved Data Optimized (EV-DO) technologies having implemented 128 bit encryption algorithms: Kasumi for UMTS and Advanced Encryption Standard (AES) for EV-DO. There are, however, various limitations to these schemes. One is that they are only available when in 3G mode. If connecting to a 2G system such as 1xRTT for CDMA 2000 or GPRS/EDGE with UMTS, the available encryption schemes are far weaker.

[2] Discussion of UMTS includes advanced data services such as High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA).

1xRTT employs a 32-bit shift register encryption scheme while most GSM/EDGE networks use a 64-bit key with an effective key length of 54 bits. Another concern is that cellular operators do not necessarily employ radio encryption even when it is available, as it is an optional feature of many wireless technologies, even 3G systems such as EV-DO. Your home operator could offer the encryption, but you might roam onto another carrier's network that does not have encryption. The bottom line is that it is problematic to reliably determine what kind of encryption the network is providing at any moment in time.

Even if you could restrict operation to wireless coverage areas that have strong encryption, there is yet another security concern. This is that the radio encryption terminates within the operator network. For EV-DO networks, the encryption end point is at the base-station controller (BSC), whereas for GSM/EDGE/UMTS networks it is at the Serving GPRS Support Node (SGSN). Beyond that, the data typically is in the clear as it traverses the operator network. Even if the operator re-encrypts user data within their network (e.g., using IPsec), the data will exist in an unencrypted form in a part of the network. Granted that the unencrypted data is on the operators private network and would likely be difficult to access from the outside, but relying on the operator safeguarding sensitive data represents a significant vulnerability, especially as it is completely out of the control of the organization using the network.

Then there is the matter of back-end connectivity, which refers to how organizations connect their networks to the operator network. The default connection method is via the Internet, which clearly is not a secure medium. To augment security of this link, some operators offer connectivity options such as Frame-Relay permanent virtual circuits (PVCs) and network VPN connections. Frame Relay circuits provide some measure of privacy, though they are not cryptologically protected, and hence vulnerable to attackers who may gain physical access to the local circuit that connects from the organization to the Frame Relay point of presence. Network VPN connections are generally based on IPsec protocols, and hence secure if configured correctly. However, both Frame Relay and network VPNs require custom arrangements with the operator, and will incur additional service charges. And they still do not address the problem that the data will pass through an unencrypted stage within the operator network.

Finally, users may be using a number of different access networks in addition to a cellular-operator wireless-data network. For instance, they may want to use their home high-speed Internet connections, hotel broadband connections or public hotspots. Clearly, the operator-based security mechanisms will provide no benefits in these alternative connection scenarios except in isolated instances where the operator operates both the wireless network and the alternate network.

The following table summarizes the limitations of operator-hosted security features.

**Table: Summary of Operator Security Mechanisms and Limitations**

| Operator Security Mechanism | How it Works | Limitations |
|---|---|---|
| Device Authentication | Network authenticates device to allow network access. | Only 3G networks employ bi-directional authentication. Seamless 2G/3G handover makes it difficult to know network type. |
| User Authentication | User must enter PIN to be able to use device. | Only available for GSM/UMTS networks.<br>User can disable feature, and does not satisfy two-factor authentication requirements. |

**Table: Summary of Operator Security Mechanisms and Limitations (continued)**

| **Operator Security Mechanism** | **How it Works** | **Limitations** |
|---|---|---|
| Encryption of Radio Link | Encryption of the radio link from user device to a node within the operator network. | Only 3G networks offer encryption using 128-bit keys and recognized algorithms, and not all operators necessarily implement the feature.<br>Seamless 2G/3G handover makes it difficult to know network type.<br>Data decrypted within operator network and may travel in the clear within operator network. |
| Back-end Connection Security Options | Private circuits and network VPNs to protect Internet traversal. | Requires custom arrangement with additional service charges. Private circuits such as Frame Relay do not encrypt data. |
| Protection for Alternate Network Access | Potential extension of encryption to other network types. | Only available in isolated cases for networks under the particular operator's control. |

Does this mean organizations should not take advantage of the operators' security options? Not necessarily. These security options may well augment an overall security architecture. For instance, some operators provide firewall configurations that prevent unsolicited IP packets from being sent to mobile devices, thus protecting against denial-of-service attacks. But by themselves, the operator provisions do not fully address the needs of secure applications.

## End-to-End Security

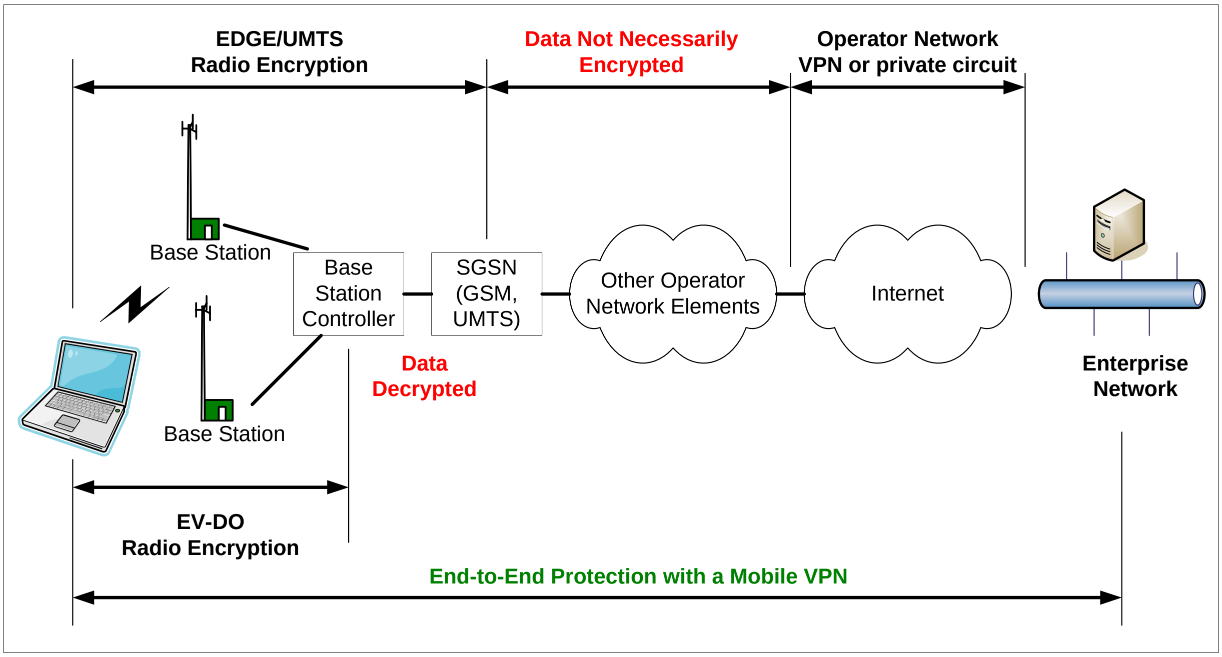
The only approach that provides security that addresses both regulatory requirements and guidelines, and that also overcomes the shortcomings of just using an operator's security provisions, is a virtual private network (VPN) that extends from the user device to a controlled node within the customer organization's network.

By using an end-to-end approach, organizations achieve the following security benefits:

- Two-factor authentication (which is supported by many VPNs)
- Mutual authentication
- Protection against lost or stolen devices
- Protection regardless of access network (operator network, Wi-Fi, home Internet, etc.)
- Privacy at every point of network traversal
- No need for customized back-end connectivity arrangements with operator

The following diagram illustrates the span of different security elements.

**Figure: Security Elements in Wireless Networks**



The wireless industry itself recognizes the limitations of their security provisions. For instance, Qualcomm, the company that was the primary inventor of CDMA2000 EV-DO technology, states in a white paper on security **"User data is best secured with a well tested end-to-end solution like a VPN regardless of airlink encryption"**[3]

## Conclusion

Enterprises are increasingly taking advantage of wireless networks for their mobile workers. However, these networks introduce significant security concerns, especially as enterprises must not only protect their data and networks, but must also address a growing number of regulatory requirements for data safeguarding.

Wireless operators have implemented various security mechanisms to mitigate security issues. For some relatively low-risk applications, these may be sufficient. But for sensitive data, these safeguards by themselves do not fully address user authentication and privacy, especially as encryption mechanisms extend only over a portion of the network. Another limitation is that the operator mechanisms only apply to their network and do not safeguard the user when using other types of networks.

The most effective solution for secure communication over wireless networks is to employ an end-to-end security approach such as a mobile VPN.

[3] Qualcomm white paper, 2003, "1xEV-DO Web Paper – Comparison of Airlink Encryptions."

Rysavy Research provides this document and the information contained herein to you for informational purposes only. Rysavy Research provides this information solely on the basis that you will take responsibility for making your own assessments of the information.

Although Rysavy Research has exercised reasonable care in providing this information to you, Rysavy Research does not warrant that the information is error-free. Rysavy Research disclaims and in no event shall be liable for any losses or damages of any kind, whether direct, indirect, incidental, consequential, or punitive arising out of or in any way related to the use of the information.