



INTRODUCTION

Protecting the integrity of the network and the privacy of sensitive data is of utmost concern to DataWind, making security an essential priority when extending Internet-based remote access to remote and mobile employees.

Critical to maintaining end-to-end security is managing authentication, authorization and encryption from the mobile device, over the transport medium, into the data-center.

DataWind's solution implements the two major features of mobile security: authentication and data protection (encryption).

CONTENTS:

Authenticated Access

- End-to-End Authentication
- Limited number of log-in attempts
- Inactivity time-outs

Data Protection

- Encryption: DataWind Server to Web Viewer Client Device
- Proprietary System & File Formats
- Cookie encryption
- Secure connections over the transport medium
 - GSM Networks
 - CDMA Networks
- Secure connections over bluetooth transport

Security Infrastructure

- Secure Facility
- Secure Firewall
- Secure Platform
- Scalable and Reliable Infrastructure

Privacy

- Protecting Customer Privacy
- Published Privacy Policy
- Disclosure of Customer Information
- Access to Customer Information



AUTHENTICATED ACCESS

End-to-End Authentication

Whenever the client device connects to the server, they authenticate each other, using a shared secret known only to machines, and not even known to the end user. This access code is never seen or stored by any machine, and is dynamically generated. The client device and host server each generate a very large random number and digitally sign that number with the access code. This challenge/response provides end-to-end authentication without transmitting the access code. Authentication mechanisms are used to properly identify users accessing corporate data. This is accomplished by a proprietary dynamic serial number identification (SNI) imbedded in the firmware of the DataWind web viewer. The SNI is a long and complex identifier which dynamically changes, based on pre-determined criteria, which is decrypted and verified at the start of each session by DataWind's database authentication servers. These are multiple, nested passwords, using cryptographic techniques to ensure that sensitive data - logins and passwords - are provided an additional level of protection. This dynamic authentication process is intended to prevent cloning and subscription fraud.

The DataWind server authenticates itself back to the Web Viewer client by supplying a digital certificate, and relying further on a DNS resolution of the server's hostname to reach the correct destination.

Once the identified user is granted access to a live session on DataWind's servers, additional measures are taken to insure that the data cannot be intercepted. Encryption is used to protect information not only in transit across the network, but also as it resides on the device or server.

The DataWind confidentiality between the browser client and server builds on the strong foundation provided by authentication. Authentication verifies the identity of every party from the Web Viewer Client and communication server to the database server. Access controls further ensure that only authenticated parties can gain access to authorized resources.

**Limited Number of Log-In Attempts**

DataWind limits the number of times any user can attempt to log in sequentially to one. This measure also helps to protect against dictionary attacks. By default, after one authentication failure, access to the user's session is temporarily deactivated for five minutes.

Inactivity Time-Outs

If the client device is left on, without logging out, DataWind addresses these threats by applying inactivity time-outs. Users are automatically logged out of the DataWind server site if their SSL connection is inactive for several minutes.



DATA PROTECTION

Encryption: DataWind Server to Web Viewer Client Device

Encryption algorithms safeguard data with end-to-end security. Data transferred between the server and client device are subject to encryption and authenticated digital signatures for decryption.

DataWind communication servers relay traffic between the client browser and web-server, by encrypting these packets. DataWind staff cannot decipher this traffic because they do not possess the access code used to generate encryption keys. Even if a hacker were to gain access to DataWind's servers, computer access codes are not stored there and individual session traffic is not recorded, so live-session traffic cannot be compromised. The access codes are generated dynamically for each session, and held in temporarily in the volatile memory of the respective session partner.

Proprietary System & File Formats

The content generated by DataWind's communication servers are of proprietary graphic file formats, further adding to the security of the session. Keyboard, mouse and display updates are transmitted over a highly compressed, encrypted stream.

Cookie encryption

DataWind servers also protects information stored within its database. Because the server actually provides the completing piece of the web browser functionality that is rendered by the Web Viewer Client, it is the server that is responsible for managing the web cookies that channels use to recognize users. To restrict access to cookie data, DataWind servers uses a 128-bit key for encryption. So this sensitive information is not stored in the clear. DataWind does not transmit or store cookies on the device.

Secure connections over the transport medium

Security over the Cellular Network is provided by the Network Operator. Proven industry standards and secure protocol provide the means for communicating over the cellular wide area wireless networks. Both GSM and CDMA networks



are recognized as highly secure, and add to the multiple layers of security between the DataWind servers and the Web Viewer. The noise-like signature of a cellular data signal over the air interface makes eavesdropping very difficult. This is due to the sequences, which are used to scramble voice and data transmissions.

Today's digital cellular networks further support the assignment of a Temporary Mobile Station Identifier to a mobile device to represent communications to and from a certain mobile device in over the air transmissions. This feature makes it more difficult to correlate a mobile user's transmission to a mobile user.

GSM Networks

Part of the enhanced security of GSM is due to the fact that it is a digital system utilizing a speech coding algorithm, Gaussian Minimum Shift Keying (GMSK) digital modulation, slow frequency hopping, and Time Division Multiple Access (TDMA) time slot architecture.

The subscriber's anonymity is ensured through the use of temporary identification numbers. The confidentiality of the communication itself on the radio link is performed by the application of encryption algorithms and frequency hopping which could only be realized using digital systems and signaling.

The security aspects of GSM are detailed in GSM Recommendations 02.09, "Security Aspects," 02.17, "Subscriber Identity Modules," 03.20, "Security Related Network Functions," and 03.21, "Security Related Algorithms". Security in GSM consists of the following aspects: subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. The subscriber is uniquely identified by the International Mobile Subscriber Identity (IMSI). This information, along with the individual subscriber authentication key (Ki), constitutes sensitive identification credentials analogous to the Electronic Serial Number (ESN) in analog systems such as AMPS and TACS. The design of the GSM authentication and encryption schemes is such that this sensitive information is never transmitted over the radio channel. Rather, a challenge-response mechanism is used to perform authentication. The actual conversations are encrypted using a temporary, randomly generated ciphering key (Kc). The MS identifies itself by means of the Temporary Mobile Subscriber Identity (TMSI),



which is issued by the network and may be changed periodically (i.e. during hand-offs) for additional security.

CDMA Networks

CDMA originated from military applications and cryptography, and to date there has never been a report of high-jacking or eavesdropping on a CDMA call in a commercially deployed network. The inherent security of CDMA's air interface comes from a combination of encryption and spread spectrum technology, which are used simultaneously to void any gaps in security. First, the CDMA signals of all calls are transmitted, or spread, over the entire bandwidth, rather than being tied to a specific time or element in the system. This results in the signal of all calls taking on white noise, a noise-like appearance that works as a disguise, making the signal of any one call difficult to distinguish and detect from background noise. If the signal could be detected, it would then have to be de-correlated for a fraudulent user to recover the information, or eavesdrop. But in order to de-correlate, the spreading code, also known as Walsh code, must be known to the interceptor. A spreading code is a sequence of binary values created in a pseudo-random manner that is multiplied to actual information bits before transmission. This use of spreading codes acts as a form of air interface encryption.

CDMA utilizes several spreading sequences whereby each CDMA spreading sequence is used for a specific purpose on the forward link (i.e., the path from the base station to the mobile) and a different purpose on the reverse link (i.e., the path from the mobile to the base station). These sequences are used to form code channels for users in both directions. These code channels act as a form of signal encryption on the air interface, which would require a long time to decode and to configure the interception. The interceptor must also know which chipset is in use in the base station equipment and must know specific information from the mobile device. However, the base station chipset required for listening to the reverse link signal is not available to the general public. So even if the interceptor were able to obtain access to the mobile device, the information needed to link to that device resides in the operator's network, and is unique for each base station. In essence, the interceptor could only eavesdrop on fragments of a conversation at best.



CDMA also has a unique soft handoff capability that allows a mobile to connect to as many as six radios in the network, each with its own Walsh code. This means that someone attempting to eavesdrop on a subscriber's call has to have several devices connected at exactly the same time in an attempt to synchronize with the intended signal. In addition, CDMA employs a fast power control, 800 times sampling per second, to maintain its radio link. It is difficult for a third party to have a stable link for interception of a CDMA voice channel, even with a full knowledge of a Walsh code. Without synchronization, the third-party listener only hears random noise.

Secure connections over bluetooth transport

Connection between the Web Viewer device and mobile-phone is further encrypted as provisioned by Bluetooth protocol V1.1. The current Bluetooth System specification defines security at the link level. During the pairing procedure both units calculate an initialisation key. The only secret input to the key calculation is the passkey (PIN). In the next step the combination or unit key is calculated. This calculation is protected using the initialisation key. Directly after the exchange of the link key, the authentication procedure is performed. The authentication uses the newly derived link key. All key derivation algorithms are symmetric algorithms that are implemented in hardware.

The Bluetooth wireless technology offers authentication and encryption mechanisms on the Baseband level (Baseband specification). They are used to protect Bluetooth point-to-point links. The Baseband security is based on the link keys that are determined for each particular Bluetooth device pair. The link key is derived during the pairing procedure.

In addition, the Web Viewer uses PPP authentication mechanisms used by the network access server. All connections between the Web Viewer device and phone are authenticated and encrypted. Fine grain access control in the Web Viewer is provided at higher layers, connected with the baseband authentication.

The range of signal strength on the mobile phone and Web Viewer for bluetooth connectivity is restricted by low power consumption, to approximately twelve feet. Thereby restricting any snooping or hacking effects to those within that radius.



SECURITY INFRASTRUCTURE

Secure Facility

DataWind's solution is delivered using an ASP model designed expressly to ensure robust and secure operation.

DataWind's, process and database servers are hosted in a highly secured data center. Physical access to servers is restricted. The entire site sits in a locked cage that is monitored by cameras. DataWind's network operations center (NOC) in Montreal, Canada, is similarly protected with strict security measures.

Secure Firewall

Perimeter security is provided by two layers of firewalls: one between the Internet and process servers, another between the client device and back-end databases. The Network Address Translation feature on the Internet connection port provides an effective Firewall, preventing any unwanted intrusion to the private network from the public Internet.

Secure Platform

DataWind back-end database and authentication servers employ Oracle and its encryption technologies, hardened with the latest security authorization procedures. We maintain system logs, which are regularly evaluated for suspicious activity.

Scalable and Reliable Infrastructure

DataWind's infrastructure is both robust and secure, incorporating Redundant routers, switches, server clusters and backup systems, which are used to ensure high availability. For scalability and reliability, switches transparently distribute incoming requests among DataWind process servers. For optimal performance, the authentication and database servers load balances the client/server sessions across geographically distributed process servers.



PRIVACY

Protecting Customer Privacy

DataWind has a strong privacy policy that prohibits unauthorized disclosure of personal or corporate information to any third party.

Published Privacy Policy

DataWind's published privacy policy is included in every service agreement. This policy identifies the information gathered, how it is used, with whom it is shared and the customer's ability to control the dissemination of information.

Disclosure of Customer Information

To deliver service, DataWind must collect certain user information, including first/last name, email address and account-level passwords. DataWind will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed services.

Access to Customer Information

DataWind NOC staff are the only individuals with access to DataWind servers – limited access is granted on a need-to-know basis for the express purpose of customer support. DataWind developers do not have access to DataWind's production servers. DataWind session logs are used by DataWind to maintain quality of service and assist in performance analysis. DataWind tracks domain names for traffic management. However, this data is gathered in the aggregate and is never correlated with an individual user or company account.