Lotus

White Paper

Secure Wireless Communication with Domino Everyplace Access Server

November 2001

Connected communities that shrink the world
Access to ideas that expand the world

A Lotus Software White Paper

IBM®

Contents

Overview

Wireless devices and wireless security standards are still evolving rapidly. This creates special challenges for corporate data security.

Wireless devices, like all technologies that provide external access to corporate networks, present security challenges. With wireless standards and practices still rapidly evolving, it is important to understand the strengths and limitations of available technologies in order to implement a secure solution.

Extending your current security policies to encompass wireless devices requires an understanding of the security features of both wireless devices and wireless networks.

Critical security questions include:

- *How will individual wireless devices be authenticated?*
- *How can you verify that the device being used is actually in the hands of an authorized user?*
- *What can you do if a user's device is lost or stolen?*
- *How can you validate that each requested connection comes from a Wireless Service Provider with whom you are currently doing business?*
- *How can you ensure that outgoing data is encrypted from your network to the device?*

Lotus® Software currently addresses enterprise requirements for wireless messaging and wireless application support with Domino™ Everyplace Access 2.1 (DEA). DEA is an end-to-end solution that extends the reach of the Domino infrastructure to encompass hand-held, wireless devices such as Web-ready phones and PDAs. With DEA, wireless users can securely exchange messages with other e-mail clients like Web browsers and Lotus Notes® clients. DEA gives wireless users access to their e-mail, personal calendar and the Domino Directory. DEA also provides a full complement of wireless administrative capabilities.

Lotus Notes and Domino provide one of the most reliable and secure data networking environments in existence. Domino Everyplace Access server builds on these proven capabilities to address the unique challenges presented by wireless devices and the wireless networks that support them.

Wireless Security Challenges

Each mobile device is a unique platform. Wireless networks also vary widely in terms of how they operate. There are currently no universal security standards analogous to X.509 and SSL in the PC world.

Mobile devices and wireless networks rely on a broad spectrum of technology, much of it cutting-edge. Unlike with PCs, each class of mobile device currently represents a unique hardware and software platform. Mobile phones and PDAs, for example, have varying capabilities and limitations both as computing devices and as client devices accessing corporate networks. The wireless networks that support mobile devices are similarly diverse.

By relying on industry standard protocols like TCP/IP, HTTP, SMTP and TAP, Domino Everyplace Access supports many of the major wireless networks currently in operation. This standards-based approach also provides DEA with a common security model that can operate across wireless networks, while at the same time taking some of the complexity out of doing business with different wireless network providers.

However, it is important to understand that there is currently no industry-wide security standard that will work on every mobile device and on every wireless network, in the way that X.509 and SSL span the PC universe. DEA bridges this gap wherever possible by adding its own security features.

This section discusses the following security areas:

- Onboard security to protect unauthorized use of wireless devices, or misappropriation of the data stored on them.
- Over-the-air security between the corporate network and wireless devices.
- Security features of the DEA server.
- Security between DEA and the Domino network.

Onboard Security for Mobile Devices

Wireless devices generally provide little or no onboard security.

Most mobile devices currently provide only a simple username/password combination to block use of the device (a few also offer local data encryption). And since most users do not employ even this rudimentary level of security, mobile devices like, mobile phones and PDAs are essentially unsecured.

Existing PC-based security mechanisms, such as client certificates, are being utilized, now that wireless devices have the ability to store a client certificate on the device. The ISO standard for the certificate is known as X.509. Due to the substantial size of the X.509 certificate and the limited capabilities of wireless devices, they now use a standard called Wireless Transport Layer Security (WTLS), also called light-weight certificates. This provides certificate-based authentication of the WAP gateway to the handset, and 128-bit data encryption of all communications from the device. This means that the first time the mobile user authenticates itself to the WAP Gateway by a valid username and password, a certificate is downloaded and stored on the handset. This certificate is used by the WAP gateway to identify that particular user for future connections to the gateway. This has now become the standard security that works across all wireless technologies.

Security, moreover, has only recently become a major concern of device vendors. This is because wireless devices have traditionally been targeted at individual users for access to their personal data — not corporate data. But as mobile device usage among corporate customers increases, improved security has become a paramount requirement. As vendors address this growing need, more and more security solutions and proposed standards will emerge.

How Domino Everyplace Access Enhances Device Security

DEA supports the full spectrum of wireless devices: from complex PDAs; to the latest generation of Web-ready phones equipped with micro-browsers, from which users can access their Notes® mail, calendar, corporate directory and other additional wireless applications.

Because of the great diversity of device capabilities, as well as their inherent security limitations, DEA cannot provide security for data stored locally across every device. Instead, DEA provides security for corporate data inside the firewall by securing it against unauthorized access by wireless devices.

In particular, DEA provides administrators with the ability to:

- Associate a specific, authorized user with each mobile device (see "Trusted Devices")
- Specify what wireless networks can communicate with DEA (see "Trusted IP Addresses")
- Specify number of failed login attempts ("Login Attempts Allowed")
- Specify time period you are unable to log in ("Login lockout Duration")
- Logout of device and login as a different user
- Automatic logout after 'x' minutes

Trusted Devices

The Trusted Device feature enables administrators both to know what employee is authorized to use each device, and to control the ability of each user or device to access Domino via DEA. For example, if an employee loses his or her mobile device, an administrator can immediately disable the use of that device with DEA, thus eliminating the risk that an impostor can access the network. This feature assumes network support for device ids.

Trusted IP Addresses

DEA enables administrators to register the IP addresses of the WAP gateways they use with DEA. Only HTTP requests from these IP addresses are permitted to use the DEA application. This effectively restricts the proxies that can access an organizational network. To add to this you are able to also specify which WAP gateways you should block by adding their IP address to the 'Permitted/Restricted WAP gateway IP addresses' fields located on the Mobile tab of the DEA server document located in the Domino Directory.

Lockout - Failed Login Attempts

DEA allows you to specify the number of failed wireless logons. If this number is reached then the wireless user must wait a specified time before they are able to login again. Only after the lockout duration has been reached, will you be able to login.

Login Lockout Duration

The Lockout feature is enabled only after the maximum number of failed login attempts has occurred. This field will specify the amount of time you must wait before you will be allowed to login. This feature compliments the failed login attempts which will reduce any unauthorized external threats. Both the failed login attempts and the lockout duration features restrict any threats of so called "Dictionary Attacks" to obtain access to your corporate infrastructure.

Logout of Device

New to DEA is the ability to log out of your current wireless session. When selecting this link from the mobile notes home page, DEA will end your wireless session and take you back to the login page. Only entering a valid username and password will allow access to your Domino information. This feature will ensure that your wireless device does not cache any username or password information. Also, if your handset is lost or stolen, this feature will prevent any unauthorized access to your Domino infrastructure.

Over-the-Air Security

All wireless providers offer secure communication of data transmitted between the device, cell tower and WAP gateway.

In today's wireless world, organizations may have little control over which wireless network its data travels over between the firewall and employees' mobile devices. And while the Internet offers security standards for authentication and encryption between a remote user's laptop-based Web browser and a corporate intranet, wireless networks have no analogous universal security mechanisms. However, today's standards have come a long way in the wireless world; you are now able to ensure that you use the industry standard WTLS with all wireless communications from your handset to the WAP gateway. WTLS is based on the industry standard of TLS (Transport Layer Security) which is the wireless equivalent to what we call Secure Socket Layer (SSL). Using this protocol ensures session-based encryption between the phone, base station and WAP gateway.

Security features common to many wireless networks include the following:

1. WTLS in all "over-the-air" transmissions between the device and the wireless network.
2. As requests from the micro-browser reach the WAP gateway over the wireless network, they are converted and passed along to the HTTP server. This transformation takes place in real time, in the local memory of the WAP gateway. The possibility of unauthorized access to data during this process is therefore limited.
3. The WAP gateway can also support HTTPS connections, along with various kinds of certificates. By ensuring the use of the secure certificate from a trusted root certificate of authority, this provides the highest level of security between the WAP gateway and application servers like Domino Everyplace Access server.

This multi-layer approach, illustrated in Figure 1, provides a secure foundation for over-the-air connections.

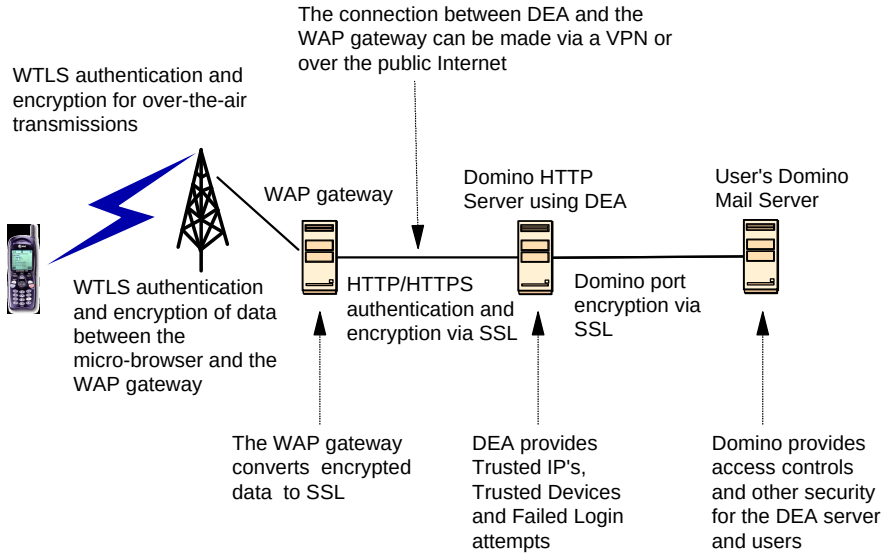

Figure 1: Over-the-air security in a wireless network.

Domino Everyplace Access Server Security

As illustrated above, the foundation for all of DEA security capabilities is Domino's integrated security services. Because DEA is a fully integrated, Domino-based solution, applicable Domino security services are available for use on the DEA server itself. For example, Domino supports encrypting data on specific ports to prevent network eavesdropping. Therefore, the network communication between DEA and the rest of the Domino environment can be encrypted, providing an excellent way to increase security for corporate data.

Because it is fully integrated with Domino, applicable Domino security services are automatically available to DEA.

Not only is the DEA server as secure as any Domino server, but it also enables organizations to administer DEA server security the same way all other Domino servers in the environment are managed for security purposes.

Moreover, all additional security capabilities that DEA provides for mobile devices and wireless networks are managed via the Domino Directory. This greatly simplifies administrative control over access to the network infrastructure.

Security between the DEA and the WAP Gateway

Connections between WAP gateways and DEA take place over IP, using HTTP/HTTPS.

Connections between a WAP gateway and the DEA server take place over TCP/IP, using HTTP or HTTPS as the transport. This makes it possible to use industry standard mechanisms such as SSL for authentication and encryption of the Internet connection.[1] Because DEA relies on Domino's native TCP/IP and HTTP support, these connections can be administered through Domino's administration facilities.

There are two ways to encrypt data in transit between the DEA and the WAP gateway using HTTPS:

- Organizations can use Domino's port encryption feature to encrypt network data on the specific ports used by DEA to communicate with the WAP gateway. This will result in the automatic encryption of all data both to and from DEA.
- Mobile users can append an 'S' to the protocol portion (e.g. "HTTP") of the URL when they initially create a bookmark to the DEA server on their mobile device. This will force the WAP gateway to use SSL between itself and the DEA server.

Trusted Devices

Using Trusted Devices, administrators can control which mobile devices they will allow to use the DEA server, simply by entering the unique address assigned to each device into the Trusted Devices sections of the Wireless Security in the Domino directory. DEA compares this unique address, from what is received as part of each HTTP request from the WAP gateway.

Security between DEA and Domino

DEA acts as a proxy between mobile devices and the Domino network, greatly simplifying security and management concerns.

Because the DEA server acts as a proxy for mobile device users, there is no end-to-end networking session between the mobile device and whatever Domino mail and application servers users need to access. Thus, no software or security changes are required for DEA to work with any given Domino server to access users' mail files. For example, there is no need to copy users' mail files to the DEA server.

The DEA server uses Notes Remote Procedure Calls (RPC) which are part of Domino's extensive set of API's, to collect the requested data on behalf of users. DEA then converts the Domino-format data into the format required by the micro-browser on the mobile device, and delivers it back to the WAP gateway via HTTP. The WAP gateway, in turn, encrypts the HTTP-format data into the data format required by the micro-browser.

Because DEA is fully integrated with Domino, the Domino security infrastructure can be used to control which Domino servers and applications the DEA server can access. And because Domino and DEA communicate via Notes RPC API, sensitive data like e-mail remains in the Domino network, and is not exposed via HTTP. This is obviously not the case with typical HTTP-based solutions.

---

[1] Other approaches might include a Virtual Private Network over an Internet connection, or a leased line T1 type connection directly between the wireless service provider's network and the organization's network. It is also possible to establish a Frame Relay or ATM network connection between the company and the wireless provider. Each of these approaches provide additional levels of security, along with reliability, performance and cost tradeoffs.

Moreover, only specified Domino servers in your network environment are accessible to the controlled list of mobile users and devices, primarily because HTTP support is not required for Domino servers to communicate with the DEA server. This additional security can be implemented by configuring specific Domino servers to grant network access privileges to the DEA server, and listing these accessible Domino servers on the DEA server. This greatly reduces the network's security exposure to the Internet and HTTP.

Robust Domino authentication and encryption is automatically in use between the DEA server and all the other Domino servers from which mobile users can request data. This gives organizations total control over whether the DEA server is certified and how it gains access to other Domino servers in the network.

In addition to TCP/IP, organizations can use any of Domino's supported protocols for connections between DEA and other Domino servers. Whatever protocol(s) are used, Domino/DEA server-to-server security is controlled in the same way that all other Domino security mechanisms are managed.

Anatomy of a Wireless Access Session

This section presents a typical example of how wireless access works, and what security features can be enforced at various points in the session:

1. Picture yourself standing in a parking lot holding a Web-enabled cell phone. You want to check your Notes mail using your phone.
2. From your device menus (configurations may vary) choose Mobile Notes™; i.e., the shortcut to the URL you use to access DEA. At this point, the phone connects for the first time with the Domino Everyplace Access server.
3. First and foremost, DEA checks to ensure that the IP address of the WAP gateway is a permitted IP address. If this check fails, access to the Domino network is denied.
4. Next, DEA checks the IP address of your device to ensure it is a trusted device. If not, access to the Domino network is denied.
5. If DEA trusts your device, it next attempts to authenticate you, the user. You will be prompted for your Notes username or short name, and your Internet (HTTP) password.
6. If the username and password are valid, you can choose from the following Mobile Notes menu: *Mail*, *Calendar*, *To Do, Address Book, User Preferences, Help* and *Logout*. If the username and/or password is invalid, DEA returns you to the Mobile Notes Login page. Figure 2 shows the menu choices.
7. To check your Mail, select *Mail* from the menu. The WAP gateway will then render the first four unread messages in your mailbox in HDML, and pass them to the micro-browser in your phone. Assuming SSL is enabled, each message is encrypted in transmission from the DEA server to the WAP gateway (and vice versa) and WTLS encryption between the WAP gateway and your wireless device. DEA will display your unread messages which are marked with a * before the memo information. Click on the *New Memo* button to create a new memo. Your request will go out from the device to the WAP gateway, and then to DEA, before reaching your inbox on the Domino server.

Note that, DEA will not be able to access your mail file if it is not listed as a manager in the Access Control List, either listed explicitly, or in the group LocalDomainServers. You also require manager access to your mail file, otherwise you will not be able to browse your mail file.

8. The phone decrypts and then displays each chunk of data (also called a "deck"), as it arrives. You select which messages to read by clicking on them one at a time. To receive more documents, select *Next Messages*. Select *Previous Messages* to review the messages you've already received. (Note that, since the micro-browser caches the data it receives for the session, unauthorized access is possible if the phone is lost or stolen while the session is in progress.) Mobile access is a browser-centric experience, in the sense that nothing resides on the phone itself once the session is terminated. Messages sent to your phone are marked as read in your Notes mailbox. When you choose Delete, and subsequently empty the trash, the message is deleted on your Domino mail server.

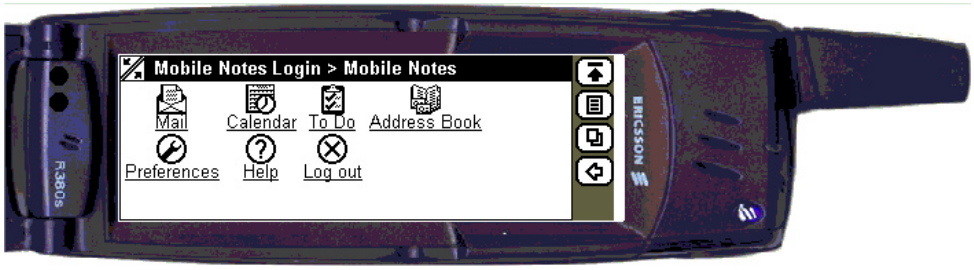

Figure 2: Mobile Notes menu options on a Web-ready cell phone.

Additional DEA Security Tips

Because Domino Everyplace Access server relies on TCP/IP and HTTP connections in order to communicate with each wireless service provider's WAP gateway, it is important to carefully evaluate the location of the DEA server in a network topology.

This section illustrates three scenarios that can help make network connections between DEA and the WAP gateway more secure. Note that these considerations are valid not only when deploying DEA, but with respect to any TCP/IP and HTTP server that may be exposed outside of the corporate firewall.

Figure 3 shows a network configuration that employs all of these security features.

DEA on the Public Internet

In this scenario, an Internet connection is used, for example, from an ISP of choice. The DEA server could be available on port 80 (the default for Domino HTTP); or port 443, which is the default Domino HTTP/SSL port.

Disabling unused Domino ports on the DEA server will further ensure a secure environment.

Disabling all other (unused) Domino ports on the DEA server will further protect the server from unauthorized parties. Only those ports needed for processes like Domino replication and access to other Domino servers should be enabled between the DEA sever and the rest of a Domino network.

In addition, you can use a third party Certificate Authority to validate the credentials of the Internet Service Provider and their WAP gateway, and require the use of SSL for communication between the service provider and their gateway.

DEA behind a Firewall

Placing the DEA server between two firewalls will restrict traffic from both the Internet and the Domino network.

Most extranet networks today that are based on Web standards employ some form of DMZ, or Demilitarized Zone (also referred to as a "double firewall"). In this configuration, the DEA server is positioned between two corporate firewalls. One firewall, on the Internet side, should only allow traffic from specific, trusted IP addresses to the DEA server. The other, on the Domino network side, should only allow the DEA server to communicate with specific Domino servers, via specific (and optionally encrypted) ports.

DEA in a VPN

A Virtual Private Network provides a private tunnel that bypasses the public Internet.

In a virtual private network (VPN) environment, a leased-line T1 circuit, Frame Relay or ATM-type connection is installed directly between the Wireless Server Provider and the corporate network. This provides a more secure connection, by virtue of creating a private "tunnel" that bypasses the public Internet altogether. A VPN also provides a much more reliable transport because it is not dependent on the Internet for connectivity. Another benefit of private networks, such as those implemented via frame relay, is that they can be much faster than some Internet connections.

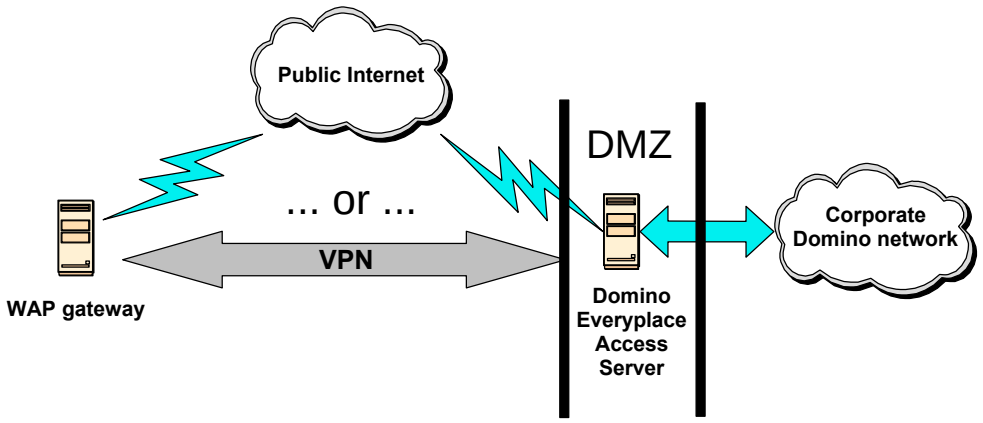

Figure 3: Extra security between DEA and a WAP gateway.

Conclusion

Wireless access to corporate data from mobile devices such as Web-enabled cell phones and PDAs has become a fact of corporate life. Organizations must fully understand the security implications of this type of access to keep their proprietary data secure. Domino Everyplace Access Server, along with the Domino Server itself, provide one of the most secure wireless access solutions available today.

In today's world, the need for end-to-end authentication and encryption is mandatory not only for the PC world but also for wireless data access. DEA addresses many of the most critical security concerns that are inherent when users access corporate and personal data from mobile devices. Key DEA security features include:

- **Trusted IP addresses,** enabling the DEA server to accept connections only from the IP addresses of approved wireless service providers as well as restricting IP addresses from unwanted WAP gateways.
- **Trusted devices**, enabling DEA to associate a specific wireless device with a specific user.
- **HTTP username/password authentication**, enabling DEA to authenticate each user for each session.
- **Access Control List verification**, which ensures that an authenticated user has the correct access permissions to access his or her Notes mailbox, before DEA sends any data.

As wireless security standards emerge, Lotus will embrace these as well, ensuring that Domino Everyplace Access continues to deliver the most secure wireless communications possible.