The Deployment Of A Secure 'Outside-In' Enterprise Mobile Solution

Psion Teklogix is a manufacturer of mobile devices and has deployed many mobile solutions worldwide. Appgate Network Security supplies advanced VPN solutions that extend e-security from the mobile device to within a company's network.

Customers need to be convinced that the broadside of challenges presented by the increasingly widespread availability of mobile devices and data services has been successfully addressed by the industry as a whole. As suppliers of the technology which enables the deployment of a secure end to end enterprise mobile solutions, Psion Teklogix and Appgate have been working jointly on a solution designed to give customers the proof they need to move their own businesses forward into the mobile age.

This solution is not simply a paper exercise – we have built a real mobile application. We have gone through the pain of the development and integration process and now have a solution which leads the way for forward looking enterprises.

The typical solution the enterprise is faced with requires the connection of a mobile task centric (blue collar) worker to the enterprise in order to unlock the huge productivity gains achievable. A very different challenge is to connect the enterprise to a mobile office (white collar) worker. Some typical considerations are shown below:

- Device type – physically and electrically different from a PDA.
- Environmental – indoor, outdoor, at sea.
- Services – will require mainly vertical market apps not PIM apps.
- Connectivity – is a must have, as they are not office based.
- Transaction – high value / secure (inclusing credit card transactions).
- Skill – often limited so functionality has to be simple.
- Who – may not be company employees (security risk).

In the case of the solution Psion Teklogix and Appgate have built, our target mobile worker was the sales teams. These guys are normally considered white collar so we concentrated on giving them a demonstration environment appropriate to their needs to sell mobile solutions, as opposed to mobilising their white collar requirements.

This process of building a secure end to end enterprise mobile solution has helped in the understanding of the issues relating to all aspects of the deployment of a mobile solution, including security. Given the context of this paper we will ignore the commercial considerations which are vital to any successful enterprise mobile deployment. What remaining considerations there are tend to fall into the two categories:

1. What are the business issues to be overcome?
2. What are the technical problems to be overcome?

And the remainder of this paper will examine these categories in more detail, hopefully addressing some of the challenges of designing a secure environment. We tried to focus on the business and technical issues that relate to security because the focus of this paper *is security.* Our objective is to provide an informative check-list which should help you tread this path.

However before we do that it is worth introducing the concept of outside-in thinking as this approach tends to lead to a better result as far as the overall business is concerned.

Outside-in Thinking

What is outside-in thinking?

Many of the disparate systems within an enterprise are increasingly being integrated either by the availability of one-does-all solutions like SAP or through web/XML implementations.

At the same time businesses are increasingly using a proliferation of mobile devices from the mobile phone to a laptop. Historically, task-centric workers with mobile devices used to interface to one PC or to one business system sometimes in semi-isolation from other unrelated business systems. Meanwhile white-collar workers tend to be connected by VPN or modem and expect to have normal access to all the business systems.

The issue that needs to be addressed here is that for a white-collar (office) worker, companies connect the office environment out to the mobile world. This solution may also work for the task-centric worker but just using it by default may not be optimal. In the task centric case you are connecting the mobile environment into the office which some might argue is the exact opposite. Has your IT manager met the contractor trying to use RSA's SecureID authentication on a touch screen device up a telegraph pole using a heavily trafficed GPRS network when it is -6C and he only has one hand free?

So outside-in thinking looks at the task to be done and designs the solution to meet the exact needs of the mobile worker. The complications and complexity are handled by the IT infrastructure, not the mobile worker.

PSION TEKLOGIX
www.psionteklogix.com

What are the business issues to be overcome?

1. Security of the hosting network

Inside-out thinking:

This is the URL of the gateway and here is the WinXP VPN software you need to run on your PC.

Outside-in thinking:

What hardware/software/connectivity combination is best suited to the task-centric worker's role

Any application that an enterprise uses needs to be hosted. Typically this is done by the company themselves (although the ASP model is now a credible alternative). Most IT managers are very protective of the networks that host their applications and rightly so. So far it has been relatively easy to manage these when used by employees on trusted sites maybe with VPN access through the firewall.

But now you have task-centric workers using a non PC platform, and just to make life a bit more interesting they need to use the internet, GPRS via the internet APN, satellite comms, 802 etc as the 'transport' for your data. Just because your existing VPN solution does work with the optimal 'transport' choice that should not mean you can not use it or that you have to move your application servers outside the firewall, as is often done in demo environments.

Imaginative solutions are required which meet the needs of this *new* community by providing appropriate access.

2. Security of hosted applications

Inside-out thinking:

I am king of the castle and nobody enters without my say so.

Outside-in thinking:

You are allowed in but your access is strictly limited to the areas you need to get your job done.

The software in your enterprise may have cost many K$ to develop and you do not want it to be copied or pirated as has happened recently where a whole web site was 'copied'. So any solution should not compromise having the application servers well protected (behind the firewall).

But a company's task-centric workers are often less trustworthy and more transient than white-collar employees. Also many companies now outsource some of their 'mobile' operations, commonly Sales and Field Service. And these teams may even spend their days criss-crossing your firewall. (One company who is looking at using mobile devices for their sales teams at the moment is restricting the programme to employees only – even though this represents less than 50% of the field based sales heads!)

So a different mindset is required which offers sufficient flexibility to meet the varied requirements of the task-centric worker within the existing network configurations. The solution therefore needs to move away from the full-access rights office-worker model towards providing pinpoint access to applications with the access rights strictly controlled to the minimum set required to get the job done.

3. Management of the mobile workforce

Inside-out thinking:
LDAP is king.

Outside-in thinking:
I have a 1000 new (very transient) users to connect – I wonder what is the best way?

It is not uncommon for your mobile workers to be using paper today so they are unknown to your IT systems (apart from maybe payroll!). Some businesses who focus on task-centric work may have a mobile workforce which vastly outnumbers the office based workforce (Courier/Delivery companies). These circumstances may make it unsuitable to include the task-centric worker into the legacy office systems.

So any security model needs to have simple tools to manage the access rights to the hosting network and the hosted applications. There needs to be the ability for different types of mobile workers (sales vs service or employed vs contract) to be attached to a defined set of applications to do their job. These management tools need to be able to remove users and application accesses just as easily, thus reducing the possibility of leaving back doors open.

4. User and/or device authentication

Inside-out thinking:
This is how we do it round here.

Outside-in thinking:
Let's minimise the security risk and so simplify the task-workers interface as much as is possible

Mobile workers are very widely spread and carry devices which are easy to forget, lose or have stolen. Authentication should be appropriate to the security risk relating to the data and the network access. Any model should therefore be 'scalable' to allow for simple authentication where the company' data and network is at minimal risk from an errant device or more comprehensive authentication where the risk is higher.

5. Security of data

Inside-out thinking:
We only use 128bit encryption now what's the problem?

Outside-in thinking:
What security risk does the data records being sent represent?

Even if the data is of minimal security risk (such as pallet numbers) because the media are increasingly focused on security and because technology allows data to be easily encrypted it is becoming an automatic requirement. However any solution should be appropriate to the devices being used and expecting a 16 bit

CPU to handle 128 bit encryption is probably not sensible. Encryption will cost time and this should be married up to the type of role the mobile worker is being asked to do.

6. Task to be done

Inside-out thinking:
It's not in our control – it's the way x's software works

Outside-in thinking:
The task is to get each transaction down to 45 seconds to hit our ROI target.

And while considering the business issues above we can not forget that for the task centric worker the task is king. Such workers can not be expected to wait for 4 or 5 minutes for their 'tool' (a mobile device in this instance) to be available for use. Security can often get in the way of the task; but in the case of the task centric worker the security solution must deliver adequate security while not compromising the task.

What are the technical problems to be overcome?

1. Use of GPRS and fixed line connectivity

The problem:

The network performance can vary a lot

Mobile devices may be connected in a number of different ways. Examples are GPRS, infrared or cable. All of these methods have different characteristics. The most important ones are: Bandwidth, Latency, MTU (packet size) and packet loss. The security solution should be capable of handling all these different environments.

Big variations in latency on a network happen, for example, when roaming in a radio-based network. Packet loss is also always an issue, it is usually more prevalent in a radio-based network but may occur on all other types as well.

Mobile devices may also experience disconnects every now and then (such as in a tunnel), so sessions should ideally be easy to reestablish.

Our solution:

Make sure the application places as small a requirement on the network performance as possible. In effect, conserve bandwidth.

2. Network topology and functionality

The problem:

The packets you send may not be the ones which are received

There are many different ways to build a network topology. The mobile device may find itself located in any of them. This means that it may find itself behind a NAT-bridge, or behind an IPv6-to-IPv4 gateway. These devices all modify the packet to some extent. This is often a big problem for standard IPsec-based solutions.

Our solution:

Open a single TCP connection to the server and apply the encryption to the actual data. This has many advantages, but the biggest one is that it works over almost any network. The packets may be chopped, sliced, diced and mixed in any way. As long as the data arrives in the right order, which is handled by TCP, we are fine.

3. Multiple OS choices – use of Java

The problem:

There are many different devices, and most of them are incompatible

Mobile devices comes in all different form-factors, colours, brands and most importantly, use different platforms / operating systems. This poses a problem for all application developers. These problems are usually more severe for the security solution since this often has to be tightly integrated with the platform, which makes it very sensitive to even minor differences in implementation.

One commonly used solution to the problem with multiple platforms is to use a cross platform language, like Java. However the more abstract and platform-neutral the language becomes the more impossible it becomes to do tight integration with the OS.

Normally there are two different ways to cope with these problems. One is to write platform-specific code and accept the fact that there is going to be a high cost for each additional platform/OS supported. The other is to write a security toolkit in a cross platform language and expect those applications that care about security to use it.

Our solution:

The AppGate client software is written in Java and is thus pretty platform neutral. The way it works is that we configure the applications to contact the local host instead of the server directly. The AppGate client then accepts the connections and encrypts the data before inserting it into the tunnel to the server.

This gives us the best of both worlds. We are pretty platform neutral and we do not require modification of the applications.

4. Multiple hardware – User Interfaces

The problem:

Most mobile devices have small screens

Different devices have different screens. Most of them are small. This places limitations on the UI of any software. This does not matter much for the task-centric worker since we usually want a very limited and easy-to-use GUI with no room for mistakes anyway. But you still need good feedback on the current status of the connection, device and application.

Different users also require different levels of functionality. The task-centric worker may use a very simple GUI but the IT manager trying to find operating problems may need more information. And the IT engineer trying to develop new services needs even more functionality. Ideally they should all use the same client or client family so that there are no nasty surprises on deployment.

Our solution:

Have a very small UI with just enough functionality for the task-centric worker. More advanced functionality is controlled by configuration files.

5. Limitations of mobile hardware – processing power

The problem:

Mobile devices usually have limited performance

Small devices have historically meant devices with very limited memory. And Java is not really known for being a light language. But modern mobile devices present less of a problem, often having a fair amount of memory, which is the most critical resource for Java applications.

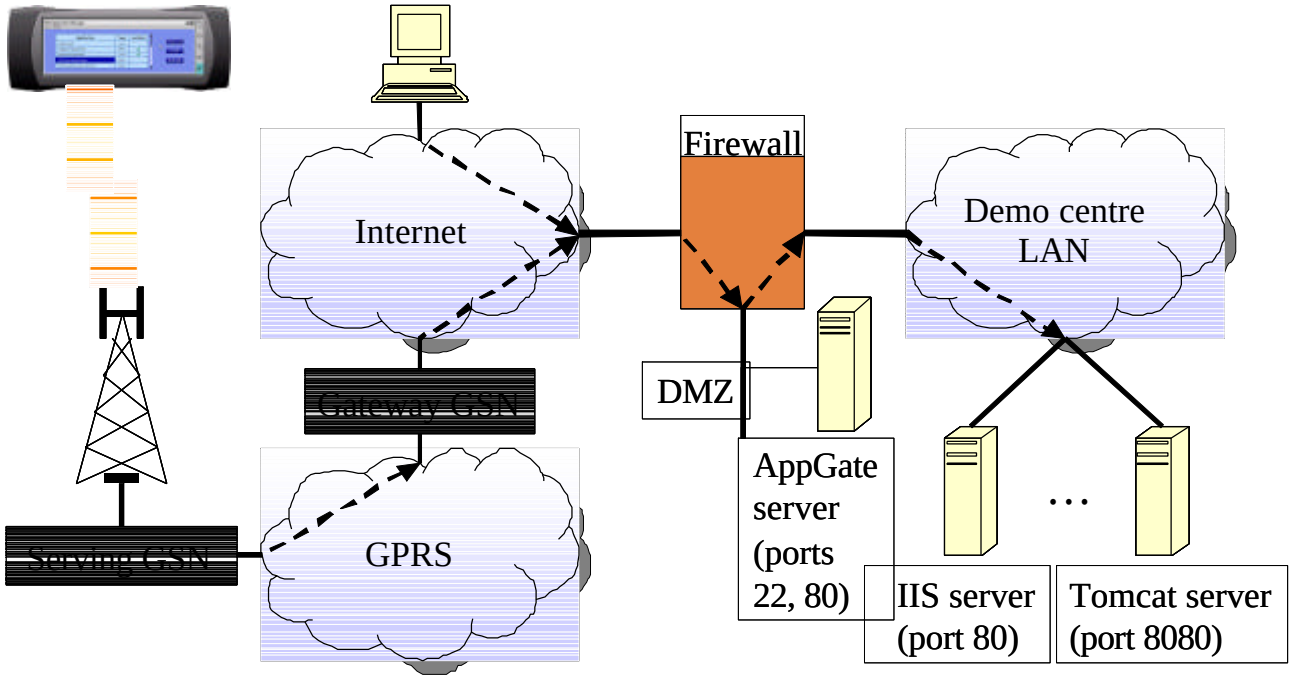
A harder problem is the processor speed. Mobile devices often have relatively slow processors, often to save on power consumption. Cryptography is normally assumed to be heavy on the CPU, but that is not completely true. There are two main classes of encryption algorithms; symmetric and asymmetric. Symmetric algorithms do not require much CPU-power at all while asymmetric algorithms use heavy maths which places quite a strain on smaller CPUs.

Our solution:

We use asymmetric algorithms while setting up the encrypted session and then symmetric algorithms to encrypt the bulk data.

A secure enterprise mobile solution

The drawing below shows the topology of the solution deployed. The Psion Teklogix netpad or a fixed PC are used to connect (via the internet) to the AppGate server located in the DMZ. The netpad uses the AppGate lite client and the PC uses either the AppGate applet or the full client.



The solution is capable of hosting a wide range of applications, all of which are running on one of two servers located inside the firewall. The AppGate server authenticates the user, secures the connection to the 'external' device and then effectively extends the security inside the network by only allowing a given user access from the AppGate box to a specific port on a specific box using a specific protocol at specific times.

Jamie Bodley-Scott

Has a degree in electronic engineering and a career which has mixed electronics/software and marketing. Works for Psion Teklogix in the UK (3 years) as Business Development Manager. Has been working in the area of Mobile Computing.

Martin Forssen

Has a Masters degree in Computer Science & Engineering and has worked in the computer security field for more than 5 years. Works for AppGate Network Security where he manages the development of the AppGate VPN product range.