Vodafone Global Enterprise

Securing your business mobility with confidence

White Paper

power to you

Key concepts: Traditional 'behind the firewall' security measures are not practical or sufficient for the protection of corporate information in the wireless environment. Multiple security policy controls are now essential that cover network security, mobile devices, supporting IT systems and infrastructure, personnel and processes.

Who should read: CIO and IT and Telecoms Heads, Communication Consultants and Global and Regional Procurement Directors

Contents

This white paper outlines our security strategy and our recommendations on how to protect your corporate information in the wireless environment. It is one of a series of white papers available.

Vodafone has more than two decades' experience in wireless security management and fully understands how to protect corporate information in the wireless environment.

Executive Overview

In an increasingly competitive global environment businesses need to increase productivity and responsiveness in order to meet changing customer demands and expectations.

Mobilising the workforce and enabling workers to access enterprise applications, systems and processes wherever they are is key to unlocking productivity benefits and providing the flexibility to respond to these challenges.

However, organisations providing remote workers with real-time wireless access to corporate data must also consider new security challenges - traditional 'behind the firewall' security measures are not practical or sufficient for the protection of corporate information in the wireless environment.

In April 2006, Symantec reported:

Security concerns are the biggest obstacle to the widespread adoption of wireless and remote computing in businesses worldwide today, according to a globalsurvey by the Economist Intelligence Unit and sponsored by Symantec Corp. More than 60 percent of companies are holding back on deployment, citing security concerns.

Vodafone has gained over two decades' experience of wireless security management through its core voice and data operations, and understands the need to ensure customers' data remains secure when extending these operations to mobilising enterprise applications, systems and processes.

This white paper outlines our security strategy and our approach to securing such new services.

Defining security - one framework, many components

In order for businesses to safely mobilise their business applications, security controls need to address all the components shown and relate them to a Security Policy Framework. One of the most important features of which is the ability to identify and respond to new threats.

There are various interpretations of 'security' in a mobile context. Figure 1 describes some of the different components of security in an overall Security Strategy.

In this paper we will discuss the importance of establishing a robust Security Policy Framework, the different components involved, Vodafone's own global security strategy and processes and how you can mobilise your business applications safely.

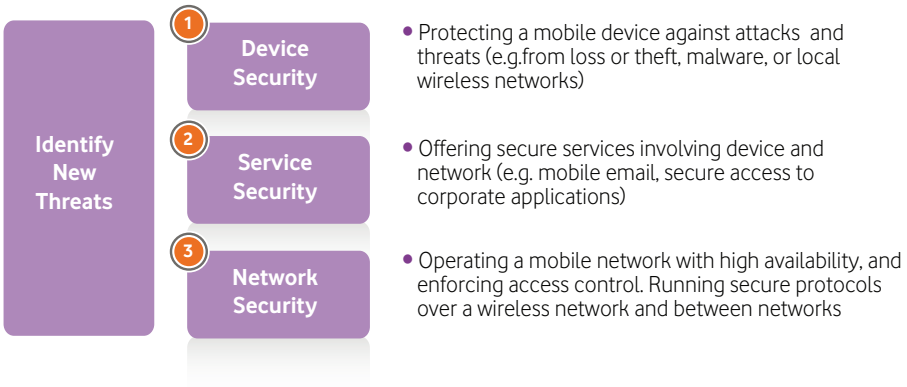

Figure 1: The different components of security in an overall Security Strategy.

Device security - protecting your mobile devices and corporate data

Data held on a mobile device is potentially at risk if the device is lost or stolen. This is essentially the same problem IT Managers experience when laptops are lost or stolen, and the security solutions are similar. It is therefore essential that data can be wiped remotely if the handset is lost or stolen.

Vodafone is currently testing file encryption software on mobile devices: such software stores sensitive data encrypted, and only decrypts it for the user to see on entry of a PIN or password.

Defending your devices from malware

In recent years there has been much publicity about viruses on mobile phones.

Malware on mobile phones is different to that on PCs, where it can propagate at high speed without user detection or interaction.

Most handsets are unaffected by malware because they either run a 'closed' Operating System (OS), which is unable to install new applications at all, or they can only install Java (J2ME) applications, running in a virtual machine 'sandbox' with strong protections against malware.

Some high-end smartphones are now built with PC-like functionality, with a flexible OS (such as Symbian or Microsoft Windows Mobile 6.0).

Where the OS is deliberately designed like a PC to allow any application to run, there is a consequent risk of "Trojan" malware.

The creation and spread of such malware is closely monitored by Vodafone, and to date does not show fast-spreading behaviour like PC viruses.

For instance, installation of Trojan malware can only occur if the device has been configured to allow unsigned applications, and the installation will provoke a series of security warnings and require user confirmation.

In addition, Vodafone offers the option for IT Managers to lock down phones, so that they can only install signed applications (which only become signed after passing through industry certification programmes offered variously by Java Verified, Symbian and Microsoft).

Vodafone is actively involved in driving the anti-malware activities of industry associations like the GSM-A and initiatives such as OMTP (Open Mobile Terminal Platform) and JCP (Java Community Process).

We are able to block known instances of malware from spreading over our networks (e.g. preventing propagation by MMS).

New features, new concerns?

Mobile phones are now being equipped with an increasing range of sophisticated features, beyond their core function as communication devices. Enhanced features such as Bluetooth and cameras can be useful, but are not always desirable in certain business environments.

Where Bluetooth is available on the phone there are a number of protections against its misuse. The Bluetooth feature needs to be actively switched on (it is off by default), then made 'discoverable', and then finally 'paired' with another device before information can be shared.

Even when paired, devices cannot automatically use each other's features without proper authorisation (either via a prompt, or via a general authorisation setting).

Vodafone works closely with phone manufacturers and Bluetooth-enabled products to continually enhance the security implementations of Bluetooth.

Our general policy is not to force unwanted features onto business devices and we offer a choice of mobile phones and communication devices with or without advanced features.

Service security - mobilising your business applications safely

Connecting Wirelessly to your Network
Using Vodafone data connectivity solutions, the security of the SIM or USIM can be leveraged to restrict data access to a company network.

In addition to IPSEC VPN tunnelling over the public internet, Vodafone can also offer Private APNs (Access Point Names) for exclusive use by a corporate customer if required. Authentication of the SIM card gates access through the APN, ensuring that only the company's own subscriptions can be used to send and receive data by that route. The remote user can also be authenticated via the corporate's own radius server if required.

Vodafone can also arrange for data traffic to travel only over private connections (e.g. GPRS/3G network, leased lines, leased DSL), keeping it away from the public Internet.

Vodafone's Secure Remote Access product offers the ability to seamlessly integrate all forms of connectivity (GPRS/3G, WiFi, fixed broadband, dial-up), and for an IT manager or administrator to set policy rules for access to different types of network. For example, the policy may prohibit use of unsecured WLAN networks, or allow only a campus WLAN to be used, or it may require a VPN connection. For further information on Vodafone Secure Remote Access solutions please contact your account manager.

Secure data connectivity and well-protected devices are of little use unless they can safely support business services and applications. Mobile email is an example with which many businesses are already familiar, but there are increasing needs to access multiple business systems, files and databases while on the move.

Securing the client end-point (the data and applications on the device) is extremely important, however it is equally important to secure the server end-point (in the company's network), together with the protocols used between the wireless client and server end-points.

Businesses can make one of two decisions on the protocol - either the protocol can be highly optimised for use on a mobile device or on a mobile network (this means that it is not exactly the same protocol at client and server end), or the protocol can run end-to-end from client to an existing applications server.

When using business applications on a laptop (e.g. with a mobile data card), an end-to-end solution is often preferred. For less powerful hand-held devices, an optimised solution may be necessary.

An example of the optimised solution is BlackBerry email. An example of the end-to-end approach is Windows Mobile email.

Optimised: The main feature of this solution is that it requires a conversion intermediary (e.g. the BlackBerry Enterprise Server - BES). This conversion intermediary is either hosted and managed by the business at additional expense, or outsourced.

It is often not possible to run end-to-end encryption through the intermediary: the intermediary has to break the encryption from the mobile client end (and possibly re-encrypt to the server end), creating an encryption 'gap' at the intermediary itself.

This requires use of a trusted intermediary, and if outsourced, must be hosted by a trusted third party.

End-to-End: The main characteristic of the end-to-end approach is the need for both ends to speak exactly the same protocol.

If it depends on a full Internet stack, the result is often a more complex mobile device, with higher expense, or slower time to market.

The protocol may not be well adapted to the characteristics of a mobile network, which means it is harder to deliver an acceptable service. In some cases there may be limited ability to utilise specific mobile features such as SIM card based authentication.

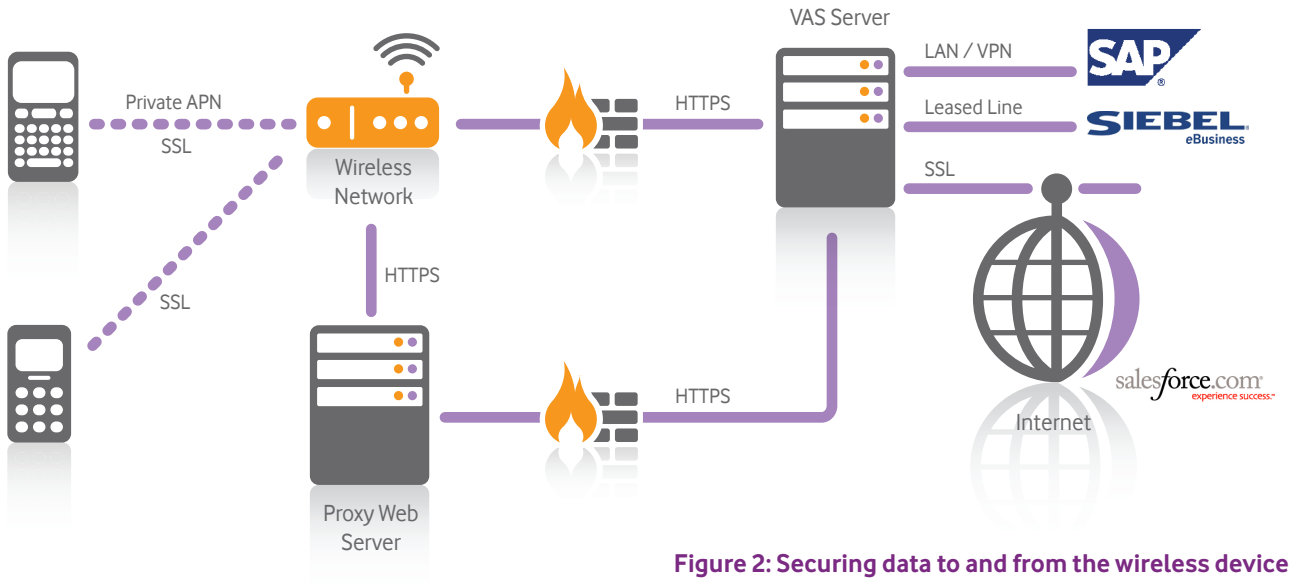

Figure 2: Securing data to and from the wireless device

End-to-end solutions do allow the option of end-to-end encryption (e.g. https), but that depends largely on how the original protocol works, and whether it can be tunnelled.

Again, if the encryption needs to be broken anywhere (which is typical for VPN solutions), a decision is required whether to host the 'gap' or outsource to a trusted third party.

Vodafone Applications Service

Vodafone has defined a generic product framework for mobilising business services and applications. The architecture and security aspects of this framework are described in detail in the Vodafone Applications Security Whitepaper, which is available on request from your Account Manager.

Whichever solution your organisation prefers, it is essential to work with a partner that has the experience and capability to help you deliver it.

For example, if trusted hosting forms part of the desired solution, the Vodafone Applications Service security framework addresses both physical security (hosting on a military base) and procedural security (a strict policy to prevent anyone from spying on the gap, audited to ensure compliance).

Network security - securing our own network

Providing network security, reliability and availability forms the very core of Vodafone's business, and this applies to the network elements themselves, their supporting IT systems and infrastructure, and the personnel and processes used to run them

Multiple policy controls are applied, and extend through to partners, contractors and out-sourcing operations.

Security controls for new systems and for enhancements to existing systems are incorporated into their business requirements. There is an established management authorisation process for new information processing facilities, and defined test and acceptance criteria for new information systems, upgrades and releases before introduction.

Prior to using any external facilities management services, security risks are identified and appropriate controls are agreed with the contractor and incorporated into the contract. This process applies at both Global and local Vodafone network levels.

Some examples of these detailed controls are listed below:

Availability and Resilience

Equipment is maintained in accordance with manufacturer's documented procedures in order to ensure its continued availability and integrity.

Business important and critical equipment is protected from power failures and other electrical anomalies, with backup power supplies being tested regularly.

Capacity demands are carefully monitored, and projections of future capacity requirements are made to ensure adequate processing power and storage is deployed in advance of demand.

Business Continuity

A managed process is in place for developing and maintaining business continuity throughout the organisation. Vodafone Group have an expert team dedicated to BCM (Business Continuity Management) to ensure that consistent BCM standards are applied across the group and provide consultancy advice on appropriate recovery strategies.

Providing network security, reliability and availability forms the very core of Vodafone's business

Following an interruption to, or failure of a critical business process, maintenance and restoration of business operations is carried out according to defined business continuity plans. Business continuity plans are tested regularly and maintained by regular reviews to ensure that they are up to date and effective.

Access Control Policy

Vodafone also maintains a strict Access Control Policy, where the allocation and use of privileges is restricted on a need only basis, with any requests for system access requiring senior management approval. Access to information services is controlled via a secure log-on process, with unique user IDs assigned for personal and sole use, together with audited security practices on password allocation and use.

In shared networks, controls segregate groups of information services, users and information systems. Sensitive systems have a dedicated and isolated computing environment. Connections to remote systems and diagnostic ports are authenticated and securely controlled, with inactive terminals serving high-risk systems being shut down after a defined period of inactivity. Active connection times are also restricted to provide additional security. The use of system utility programs and audit tools is restricted and tightly controlled.

Risks associated with access by third parties are assessed, and appropriate security controls implemented prior to entering into a contract with the relevant third party. A rigorous security review is conducted at any out-sourced site prior to signing a contract.

Vodafone's Access Control Policy also extends to physical network security. Security perimeters are used to protect areas which contain information-processing facilities, including appropriate entry controls, perimeter fences, security guards, CCTV, security lighting, motion sensors and intruder detection systems.

Delivery and loading areas are controlled and as a matter of policy isolated from information processing facilities to avoid unauthorised access. Security procedures and controls are used to secure equipment outside of Vodafone's premises, where external hosting proves necessary.

Malware and Denial of Service

Vodafone implements rigorous detection and prevention controls to defend against malicious software, denial of service (DoS) attacks, and related Internet threats.

Where networked systems do not need to be accessible from the public Internet, they are given only local IP addresses, and shielded using firewalls. Access to the Internet is denied, or granted via restrictive proxies only.

Internet facing services are fully hardened against external attacks such as DoS. Malware attacks are restricted by anti-virus and filtering software deployed at multiple points in the network (firewall, mail server, PC client). Links across internal networks exist only when necessary, and on secure channels (dedicated lines or VPNs).

Operating systems and critical software on networked systems is updated automatically, and employees have restricted installation privileges on company equipment.

Vodafone understands how vital it is for a mobile provider to safeguard customer data and implement strict controls to protect customer information

Unsolicited Messages

The ability of mobile terminals to send and receive messages also raises the question of unsolicited messages (spam), with the potential for social engineering attacks such as 'phishing'. Spam emails can of course be filtered out at your company's servers before they are even delivered to the mobile device.

Vodafone uses a variety of methods to deter messaging spam, not just technical solutions. These include early alert systems, applying termination charges to prevent high volume sending of free SMS, and withholding payment to premium rate operators in cases of abuse.

Confidentiality and Integrity of Customer Data

Vodafone understands how vital it is for a mobile provider to safeguard customer data. Leaked logs of business calls, data connections, usage and location movements can be as damaging to enterprise confidentiality as leaked emails and database transactions, as can lost or incorrect information.

Vodafone implements strict controls to protect customer information in accordance with relevant legislation and Vodafone's Information Classification policy as described earlier.

Important Vodafone records are protected from loss, destruction and falsification and a formal authorisation process occurs before information is made public, with mechanisms to ensure the integrity of such information.

Communications and Operations

Procedures for communications and operations management are also part of the Global Policy Framework. Information processing facilities and systems have recognised Change Control Processes in place, requiring approval from all impacted stakeholders before any changes are implemented.

Incident management teams are established within each Vodafone network to respond to security incidents. Separation between Development and Operational facilities is enforced locally by each network.

Information Classification Policy

Vodafone's Information Classification policy is a global standard that every Vodafone network must comply with.

The policy includes guidelines on how to classify information, the security controls to be implemented for such information (both physical and electronic), and defines the handling and storage of information in order to protect this information from unauthorised disclosure or misuse (including clear desk and clear screen policy).

Security controls include encryption and message authentication (or digital signatures), applied as appropriate in accordance with the sensitivity of information protected.

Personnel Controls

Staff's duties and areas of responsibility are segregated in order to reduce the opportunities for unauthorised modification or misuse of information or services.

Verification checks on staff are carried out at the time of job applications, and a confidentiality agreement is signed as part of the employee's terms and conditions of employment, defining their responsibilities for information security.

Security roles and responsibilities are documented in job definitions where appropriate and in the Employee Handbook. Dismissal as a result of a breach of security is included within terms and conditions of employment.

Users of information services are required to report any observed or suspected security weaknesses in or threats to systems or services as stated in Vodafone's policies. Staff activities are monitored by systems, and operational staff are required to log all activities.

Identifying new threats

Vodafone has for several years run an internal forum of security experts - the Global Security Forum. This forum ensures that there is clear communication of new security threats, with clear direction and visible management support for security initiatives.

Security experts from Vodafone Group and Vodafone networks, together with affiliates and partner networks, attend this Forum twice per year, with topic specific workgroup meetings taking place on a more frequent basis.

Rapid communication between forum members is facilitated by web-based information sharing systems and daily email updates.

Vodafone takes a proactive approach to ensuring that inherent security is designed into the technology from the outset. We are instrumental players in standards bodies such as 3GPP, ETSI, IETF and ITU-T in defining and subsequently implementing the highest levels of security for the core telecoms network.

We have over 100 staff working on standards, and security is one of the areas where we have strong - indeed industry leading - expertise and involvement.

Vodafone's global security strategy and solutions

Vodafone's overall security strategy is defined by a Global Security Policy Framework, which has been approved and published by Group management, and is binding on each local Vodafone company in the Vodafone Group.

Each Vodafone network is required to:

- Create and communicate a compatible local security policy
- Implement an Information Security Management System (ISMS)
- Select applicable controls from the Global Security Policy framework
- Apply appropriate measures to reduce security risks to an acceptable level.

Each Vodafone network's security policy is then approved and published by local management. It confirms management commitment and sets out the network's approach to managing information security.

As new companies join the Vodafone Group, their Security Policies are required to align with the Global Security Policy Framework.

Our role is to help our Global Enterprise customers to implement secure wireless mobility solutions with confidence so that they can create key competitive differentiation in their marketplace.

In conclusion

This paper discusses Vodafone's security strategy, both in overall framework terms and at different layers within that framework.

However, security is not a static field and we place great emphasis on keeping up to date with recent developments and emerging technologies in this area.

Vodafone's global forum of security experts shares threat information across operating companies, affiliates and partner networks, and can answer customers' questions on specific security concerns.

Vodafone can also run security workshops for your teams on specific products and services.

Vodafone will continue to offer the most secure service to global enterprise customers, giving your business the confidence to implement secure wireless mobility solutions and create key competitive differentiation in the marketplace.

For further details on our security strategy or to arrange a workshop please contact your Global Account Manager.

www.vodafone.com/globalenterprise

01.10.09

vodafone