



GPRS / 3G Services: Security

An O2 White Paper

Page No.	Chapter No.
3	1. Executive summary
4	2. Abstract
5	3. What are GPRS and 3G?
6-7	4. GPRS components
8	5. 3G components
9	6. Inherent GPRS security
10-13	7. Attack scenarios
14	8. Summary
15	Appendix 1 – Glossary of terms
16	Appendix 2 – Accreditations

O2 has been at the forefront of mobile data since launching the world's first GPRS service in June 2000. O2 has worked with many companies assisting in the development of mobile data applications such as 'email on the move', field service engineering, sales order processing, parcels despatch and delivery, vehicle tracking, etc. There are many additional issues to be managed when companies install mobile data applications: sometimes business processes need to be re-engineered, sometimes employees contracts of employment need to be changed to home-based working, working practices may need to be changed so that field employees travel direct to their first job each day rather than travelling to a depot to pick up job sheets. One issue common to all mobile data applications is security. Business customers are rightly concerned to ensure their company data is secure as it is transmitted across the O2 network, and also to ensure that security of their LAN is not compromised by a connection to a mobile network.

O2 has reassured many business customers about the security of our data network, but we also accept some customers may still remain suspicious and express the view "Well they would say that, wouldn't they?" We therefore identified the need for an independent audit of the security of our GPRS and 3G services and infrastructure, together with a 'White Paper' describing the findings and the security features. The White Paper is aimed primarily at managers with responsibility for IT security.

IRM were selected by O2 to carry out the independent security audit because they are in a unique position to provide expertise not only in IP-based networks, but also in cellular networks. IRM are acknowledged as industry leaders in the vulnerability and penetration testing space. IRM Plc is proud of its customer base which – in recognition of its high level of expertise and experience – comprises national governments, international stock

exchanges, international law enforcement agencies, global financial institutions and Fortune 500 Global companies. IRM technical personnel hold a range of respected security-related certifications, including CESG CHECK and CLAS*, OPST* and OPSA*.

Eric Waters, O2 GPRS Bearer Service Product Manager

Cameron Black, O2 Network & Systems Technical Security Manager

* For explanation of accreditations, please see Appendix 2.

2. Abstract

This paper provides the results of an extensive security evaluation performed on the O2 GPRS and 3G network infrastructure by Information Risk Management Plc. The objective of the exercise was to evaluate the security of O2's GPRS/3G infrastructure in a series of scenario-based attacks using a combination of publicly available and in-house-created tools and techniques. IRM were provided with full details of the O2 infrastructure and all system components in both live and test environments.

3. What are GPRS and 3G?

GPRS (General Packet Radio Service) provides a network infrastructure to facilitate a range of data services that are provided by network operators worldwide. 3G is the common name for UMTS (Universal Mobile Telephony Service), which uses the same core network and protocols as GPRS to provide high speed data services. The main difference between a GPRS and 3G network infrastructure is the technology that handles the radio communication – in a 3G infrastructure, the equipment is capable of operating at much higher bandwidths; however, the core infrastructure components are identical.

Figure 1 shows an overview of the main elements within a typical GPRS and 3G network infrastructure along with the likely attack vectors into the network. This diagram will be referenced throughout the paper.

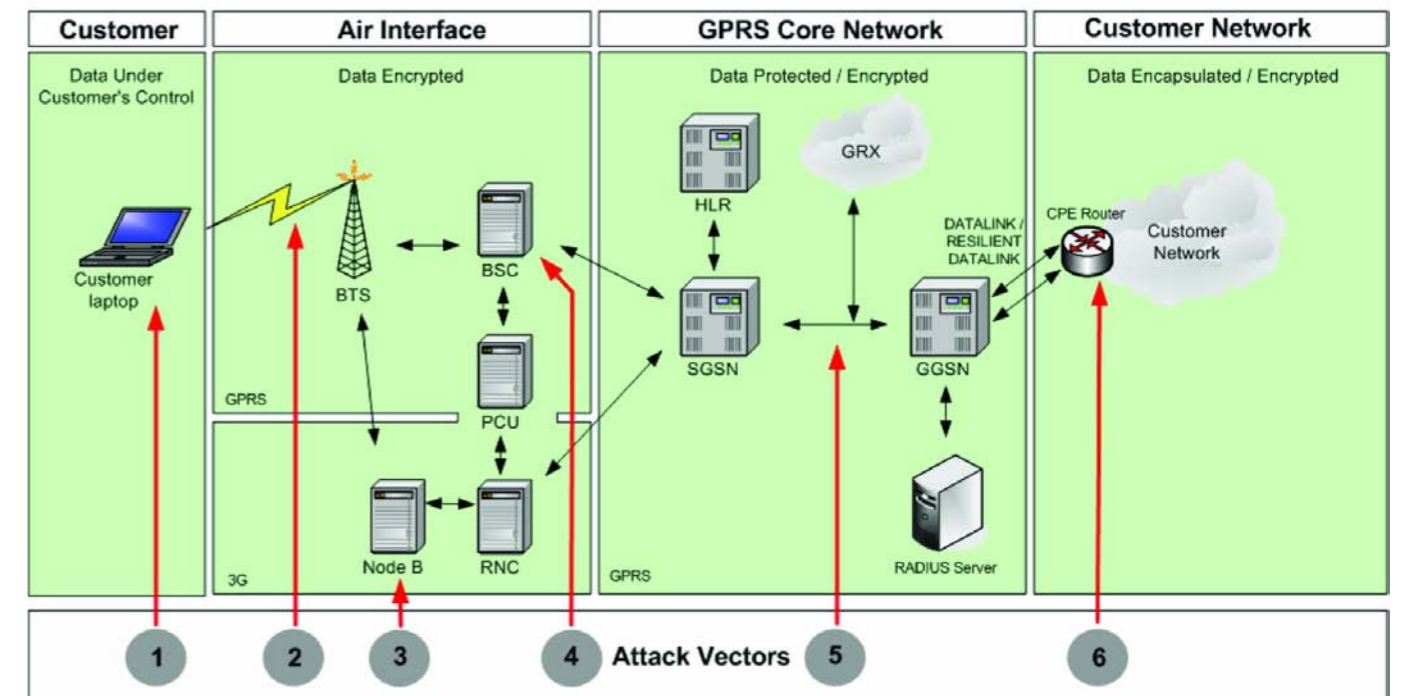


Figure 1 – Typical GPRS and 3G infrastructure and associated attack vectors.

4. GPRS components

An overview of the purpose and connectivity of each of the primary components within the infrastructure is discussed below.

Mobile device

This can be a phone, PDA (Personal Digital Assistant), or a datacard connected to a laptop PC that provides network connectivity to GPRS and/or 3G (as represented in the Figure 1).

Base Station System

The Base Station System consists of a BTS (Base Transceiver Station) and a BSC (Base Station Controller), which is shown in Figure 1.

- The BTS is the radio equipment that transmits and receives information over the air to provide GSM and GPRS communication with the mobile device
- The BSC manages the radio resource allocation and the handovers between several BTSs.

PCU (Packet Control Unit)

The Packet Control Unit is logically associated with a BSC (Base Station Controller). The PCU is responsible for controlling the radio related aspects of GPRS once the BSC has identified a data requirement, and lies between the BTS (Base Transceiver Station) and the SGSN (Serving GPRS Support Node).

HLR (Home Location Register) and VLR (Visitor Location Register)

These are the databases that hold information relating to the services associated with every SIM card on the mobile network. Information present in the HLR includes supplementary services, authentication credentials and APN (Access Point Names). For GPRS, subscription information is exchanged between the HLR and SGSN when required, e.g. when the mobile device attaches to the network, or requests connection to an APN. Similarly, the VLR contains

temporary subscription information needed to provide services for visiting subscribers roaming from overseas networks. In the same way, when O2 subscribers roam overseas, subscription information relating to the SIM card is temporarily transferred to the VLR of the overseas network.

It is important to note that no personal data, such as names, addresses and bank details, are held in the HLR, VLR or SGSN. Such information is only held in the billing and customer care systems, which are not accessible from the GPRS and 3G networks.

SGSN (Serving GPRS Support Node)

The SGSN forwards data to and from a mobile device within the SGSN service area, and it also provides data routing and transfer to and from the SGSN service area. It serves all GPRS subscribers that are physically located within the geographical SGSN service area. In addition, an SGSN provides encryption, authentication, session management, mobility management and billing data.

GGSN (Gateway GPRS Support Node)

The GGSN provides connectivity between the GPRS core network and the customer's corporate network or to the Internet. It also provides GPRS session management, and functionality for associating subscribers to the correct SGSN.

DataLink and CPE (Customer Premises Equipment) router

The network connectivity that enables a mobile user to communicate with his corporate systems is provided by the O2 DataLink (a leased line) and a CPE router, which is installed by O2 at the customer's premises. O2 uses GRE (Generic Routing Encapsulation) between the GGSN and the CPE router.

O2 also offer customers a Resilient DataLink, which consists of two CPE routers and two leased lines

connected to two GGSNs, both using the same APN and thereby protecting against failure of single components. From a security perspective, Resilient DataLinks are considered the same as DataLinks.

Customers do not have to connect their data network to O2 via a DataLink, they also have the option of connecting via the Internet, using Mobile Web (which provides mobile users with WWW access) or Mobile Web VPN (which supports recognised IPSEC VPN protocols, but has no access to the WWW ensuring all mobile devices can only be used for legitimate company business).

APN (Access Point Name)

An APN consists of a FQDN (Fully Qualified Domain Name) associated with a GPRS connection to an external data network, e.g. corporate1.operator.com. The IP address associated with this name is that of the GGSN that provides connectivity to the CPE router for that connection. The APN may be classed as either private or public. This determines whether O2 carries out a preliminary validation of the GPRS mobile device's subscription record before forwarding their access request to that data network.

Private APNs provide companies with 'closed user group' facilities. Any request for connection to a private access point will be validated by checking that the GPRS user's subscription record includes the Access Point Name (APN) requested. If the subscription record does not hold the APN, the request will be immediately rejected by O2, and not forwarded to the external data network.

Public APNs: O2 does not validate the subscription records of the GPRS user requesting access to a public access point, and may therefore forward requests for access from GPRS users unknown to the customer.

RADIUS (Remote Access Dial-In User Service) server

Customers may use RADIUS for authentication of the mobile devices connecting to their network. The RADIUS server may also be used to allocate an IP address to a mobile device connected to their APN. When a user makes a GPRS connection to a specific APN then an IP address within the address space of the associated corporate network must be allocated so that the mobile device can communicate with other devices residing on that network. O2 allows IP address pools to be hosted by either customer's RADIUS or DHCP (Dynamic Host Configuration Protocol), or by O2 on the GGSN.

5. 3G components

As mentioned earlier, 3G uses the same Core infrastructure and protocols as GPRS. The main changes are in the radio interface (or UTRAN – UMTS Terrestrial Radio Access Network – in 3G terminology) which uses the following components.

Node B

This is the radio element in a 3G network which interfaces with the mobile device. Node Bs consist of radio transmitters, receivers, antennas and feeders for one or more cells. Node B is analogous to the BTS in the GPRS network.

RNC (Radio Network Controller)

The RNC controls the radio resource, transmission and reception for Node Bs. It is analogous to the BSC in the GPRS network.

6. Inherent GPRS security

Although additional security enhancements can be adopted to further increase the security of customer data as it traverses a GPRS network, there are many security features inherent to the design of the system.

Mobile device security

Data sensitivity is a key issue when protecting intellectual rights, O2 take procedural steps to secure access to mobile devices that its subscribers use. Access control can be split into two areas:

- SIM (Subscriber Identity Module)
- Mobile device

Access control is implemented on all O2 SIMs. The SIM has a PIN lock function, which forces users to enter a PIN before allowing the mobile handset to authenticate to the O2 network. The SIM will only allow a maximum of three attempts before being locked out, preventing further attempts to authenticate.

Mobile devices are also provisioned with built-in access control. A variety of O2 devices provide the option to lock the handset via a 4 to 10 digit PIN, for example the Xda devices support such functionality. This provides an extra level of security which ensures only authorised subscribers can access the mobile device.

GPRS security vs 3G security

3G is based on GPRS standards. The internal core network elements of 3G replicate and re-use GPRS network elements and therefore there are no changes with regard to the internal network. The key difference from an architectural point between 3G and GPRS is the air interface. The mobile handset will now communicate to a Node B (a system installed in a street cabinet just like a BTS) instead of the BTS, this is because Node B's support the higher bandwidth provided by 3G networks. The Node B then communicates to a Radio Network

Controller (RNC). These communications replicate the air interface side of the GPRS network. 3G communication offers further security enhancements on the radio link, as it now supports integrity protection and mutual authentication.

Data confidentiality and VPNs

A GRE tunnel (note this is not encrypted) exists between the GGSN to the edge of the corporate network. If a VPN is not used in the transactions sent between the ultimate endpoints, then the communication is subject to interception. The key threat being the ability for an attacker to intercept information as it is transferred in plain text format. Because authentication and integrity protection will only be performed on a session basis (assuming TCP/IP is used), it will be possible for attackers to manipulate traffic in transit between the two end points. As with any telecoms networks, where highly sensitive information is being passed, the added security of a VPN to a corporate network is desirable. All data transferred from the GGSN to the mobile device still has the same level of security i.e. GPRS authentication, APN access controls etc. regardless of the existence of a VPN.

7. Attack scenarios

Table 1 provides a comparison of how different communication technologies offered by O2 are affected by a range of different attacks and how these are mitigated. Typical fixed line dial-up internet access is also included in the comparison.

The earlier Figure 1 shows the different attack vectors associated with GPRS security. These are detailed below along with the penetration testing results at each stage.

Attacks	O2 GPRS & 3G Bearer Service over DataLink and Resilient DataLink	O2 Mobile Web	O2 Mobile Web VPN	Typical PSTN dial-up Internet Access
Spoofting / impersonation	Mitigated by SIM authentication and APN access controls	Mitigated by SIM authentication	Mitigated by SIM authentication and APN access control A RADIUS server can be provided by O2 for various access control policies	Limited authentication provided by ISP provides some degree of mitigation
Data manipulation	Air interface controls prevent data manipulation	Air interface controls prevent data manipulation	Air interface controls prevent data manipulation	Security limitations enhances the risk of data manipulation
Data interception / unauthorised access to confidential data	Encryption mandated on all air interface traffic Uses leased line GRE tunnel provided for VPN CPE router managed by O2	Encryption mandated on all air interface traffic	Encryption mandated on all air interface traffic IPSec mandated	No guaranteed encryption policy over this link, any security has to be provided by the customer
Exposure to the internet	No exposure to the internet	Exposed to the internet, but protected by O2's firewall	Exposed to the internet, but only allows common IPSec products to work	Exposed to the internet

Table 1 – Comparison of O2-provided communication technologies and how they mitigate risks of attacks, compared with typical PSTN dial-up access.

Attack vector 1 – Customer’s laptop or mobile device

As mobile devices become more feature-rich in the network capabilities they offer and as the use of datacards in laptops increases, there is more scope for attacks being launched against a mobile operator’s network from this perspective. The most likely attacks to be launched by a mobile user are:

- Information leakage – can any information about the underlying infrastructure be enumerated?
- Access to core systems – can devices such as an SGSN, GGSN or HLR be accessed?
- Denial of Service attacks – can any attack degrade or deny service to other users?

O2 has configured the GPRS network to limit the amount of information leakage that can be obtained about the underlying infrastructure. In addition, rigorous network filtering and system patching prevented any access to core network components or the ability to perform Denial of Service attacks from a mobile user perspective.

Mobile devices have become more intelligent due to an open Operating System and more sophisticated applications. Although viruses have been released in the wild for Symbian-based devices, they have not made the impact so far that PC viruses have. O2 take the threat of mobile-based viruses extremely seriously and are researching techniques to protect subscribers from infection via the GPRS network infrastructure.

As well as the network level security policies of O2, it is also important for companies to have policies in place to protect their own laptops and devices (and the data held on them). IRM recommend that companies ensure that policies and protective measures are followed in order to secure the data in their end-user devices against theft and virus attacks.

Attack vector 2 – The air interface

The communication between the mobile device and the BSC or Node B is also known as the Air Interface, this is the radio link that enables subscribers to communicate with each other. Previous generations of mobile phones, based on the TACS technology, used an analogue radio signal to communicate with base stations; this signal could easily be intercepted using inexpensive radio scanners and conversations monitored. However, GPRS uses digital signalling between the handset and the GPRS network and provides encryption and authentication for all traffic communicated in this way. In addition, 3G provides further security enhancement of data integrity checking.

The authentication key that is used during communication with the GPRS network is embedded into the SIM (Subscriber Identity Module - which is installed in a phone) at manufacture time and cannot be retrieved by an external card reader, due to hardware reverse-engineering protection mechanisms. The value is also maintained by the Home Location Register (HLR). Unauthorised access to the GPRS network can only be achieved if an attacker can obtain the secret key stored on the SIM. Currently there are no known attacks to clone or to access this key.

The security implemented to protect GPRS radio transmissions is robust and adequate, as demonstrated by the standards. Currently, no known attacks exist that would enable a brute-force attack to break the authentication and encryption key associated with the GPRS encryption algorithms and therefore, it would be extremely difficult for attackers or O2 employees to gain access to data travelling over the air interface as the link is encrypted encrypted using GPRS Encryption Algorithm 1 (GEA1) up to the SGSN. All GPRS devices approved and sold by O2 in the UK support GEA1. The only circumstance in which data could be transmitted without



encryption would be if a GPRS device which does not support GEA1 (i.e. an unapproved device) connected to the O2 GPRS network.

Attack vectors 3 and 4 – Street furniture

The fundamental difference between a GPRS and 3G system is the bandwidth that is available. Typically the maximum bandwidth available over GPRS is 57kbps, whereas currently with 3G bandwidths of up to 384kbps are possible. This increase of bandwidth is achieved at the air interface. With GPRS the air interface is controlled by the BTS (Base Transceiver Station), whereas with 3G it is the combination of RNC (Radio Network Controller) and Node B that provide this functionality. RNCs are located in secured O2 premises, whereas both the BTS and Node B systems are located in street furniture, typically co-located with a mast and protected by a security fence.

Both BTS and Node B street cabinets used by O2 have physical anti-tamper devices installed so that if they are opened by unauthorised personnel an alarm is activated in an O2 Network Operations Centre. The BTS cabinets are also protected by the use of proprietary data connectors, protocols and software required to communicate with any of the devices. Furthermore, in the event of an O2 engineer's laptop being stolen along with appropriate cables and software, authentication credentials are required to access the systems and there is no IP connectivity to systems within the O2 core network from these devices.

The Node B cabinets have standard Ethernet ports on some of the enclosed devices that would be accessible to an intruder; however, by connecting to them, only limited status information could be obtained and rigorous network filtering prevented access to any other O2 systems.

Attack vector 5 – The GPRS core network

The GPRS core network contains components such as the SGSN and GGSN; due to a combination of multiple physical and network controls these are only accessible to a restricted number of authorised O2 employees. Therefore attacks performed from this perspective emulate the scenario of a 'malicious insider'. If an end-to-end VPN solution has not been implemented by the customer (where the VPN client software is running on the mobile device and the VPN server on the corporate network) then technically their data may be intercepted on the core network. However, due to the restricted access to the network this would only be available to a limited number of authorised O2 personnel.

The majority of traffic that traverses all GPRS core networks uses a protocol known as GTP (GPRS Tunnelling Protocol). Any security issues associated with the use of this protocol affect all mobile operators worldwide. IRM are of the opinion that O2 have mitigated the risks associated with these security issues in two ways: firstly by implementing both physical and network controls to protect access to the network and secondly, by working closely with the mobile standards bodies in order to constantly update and improve the security of communication protocols.

Attack vector 6 – The customer's corporate network

A common way for a company to ensure only its employees have access to their enterprise servers is via a VPN (Virtual Private Network) back to their internal network from their mobile devices. The allocation of IP addresses to a mobile device can be performed using a RADIUS (Remote Authentication Dial-In User Service) server located on the edge of the customer domain or within the O2 network; the RADIUS server is responsible for authenticating the employees and then allocating

internal IP addresses to the mobile devices (which the GGSN can supply on request of the RADIUS server). O2 accommodates the use of a VPN by providing a GRE tunnel from the GGSN to the customer's internal network and provide the following security measures to mitigate any risk of unauthorised access to corporate networks from users on other O2-provided networks:

- Separacy from the Internet
- SIM Authentication (which has already been discussed)
- Access to the APN
- RADIUS authentication (for IP allocation)

The O2 network is designed to ensure there is no connectivity between the links to customers' APNs and the Internet, nor with O2's Mobile Web APN which provides access to the Internet.

An APN (Access Point Name) appoints traffic from the SGSN to the GGSN that is responsible for routing the data to the correct destination. The overwhelming majority of corporate networks are accessed by private APNs, providing closed user group access. When a subscriber wants to connect to a corporate network with a private APN, the data connection is routed through the SGSN which checks if access is allowed to the requested APN. The Home Location Register (HLR) holds subscriber profile information, which is where APN access control is carried out. The SGSN queries the HLR to determine whether a subscriber accessing an APN has permission to do so. Without authorisation a subscriber cannot access a requested Private APN and if an attempt is made to do so, the request will be rejected at the SGSN. This prevents an arbitrary user attempting to access a private APN by simply modifying the APN details within the configuration of the mobile device.

All attempts to gain unauthorised access from one corporate network to another via the O2 GPRS infrastructure using inter-APN attack techniques failed. In summary, subscribers cannot access private APNs that are not provisioned in their HLR subscription profile, which is managed by O2 on behalf of the customer. There is no subscription checking for public APNs.

Customers can provide further security by means of RADIUS servers, which provide the ability to authenticate users to a particular domain. The objective of using a mechanism such as RADIUS is to ensure that only authenticated users can access a corporate network and be allocated an appropriate IP address for that network. Once the user has access to the correct APN, his connection is routed through to the RADIUS server on the edge of the corporate network. The user then has to authenticate himself to the RADIUS server before any access is granted.

With security being applied in different stages of the GPRS/3G transaction it ensures that only authorised employees can access their company's data. The APN access control only allows employees to access what has specifically been provisioned for them by O2; unauthorised attempts to access APNs not in the employees' profile will be rejected and logged.

GPRS and 3G network services are becoming more and more popular with companies wanting to enable their employees to become ever more mobile. The technology required to support that need therefore has to be sufficiently robust with respect to confidentiality, integrity and availability to justify its use for carrying out business.

Over a period of several months, with access to the extensive O2 testing facilities and technical expertise, IRM identified all the potential attack vectors associated with the GPRS and 3G infrastructure and developed scenarios whereby attacks could be mounted. During the project IRM were required to develop new tools and techniques in order to test for vulnerabilities in protocols and products for which there are no publicly available testing methodologies.

All areas of the infrastructure were evaluated, from the mobile user, through the air interface, core network, to the customer's corporate network. At each stage scenario-based attacks were mounted with the intention of gaining unauthorised access to any of the infrastructure components.

Throughout the entire investigation none of the discoveries by IRM were classified as 'high risk' and all findings were swiftly addressed and mitigated by O2. The GPRS and 3G services provided by O2 were considered to be extremely well configured and managed.

APN	Access Point Name
BSC	Base Station Controller
BTS	Base Transceiver Station
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
FQDN	Fully Qualified Domain Name
GEA	GPRS Encryption Algorithm
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
GTP	GPRS Tunnelling Protocol
HLR	Home Location Register
IP	Internet Protocol
IPSec	Internet Protocol Security
LAN	Local Area Network
PCU	Packet Control Unit
PIN	Personal Identity Number
PDA	Personal Digital Assistant
PSTN	Public Switched Telephone Network
RADIUS	Remote Access Dial-In User Service
RNC	Radio Network Controller
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
TACS	Total Access Communications System
TCP/IP	Transmission Control Protocol/Internet Protocol
UMTS	Universal Mobile Telephony Service
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register
VPN	Virtual Private Network

Appendix 2: Accreditations



Communications Electronics Security Group (CESG) Partnership – IT Health CHECK service providers approved to provide IT health check services and consulting in line with HMG policy and CESG / DERA (Defence Evaluation & Research Agency) guidelines.



CHECK approved company. All technical staff security vetted to Security Clearance (SC) level. All CESG Check Team Leader are passed through the GCHQ/CESG assault courses.



CLAS is the acronym for CESG Listed Advisor Scheme - started in 1998 by CESG for the purpose of vetting external consultants who could demonstrate relevant expertise in information security for the delivery of information security advice and assistance to government departments and clients. IRM's CLAS consultants provide best practice advice in line with HMG Infosec Standards and Procedures.



IRM Plc is the first accredited training partner for the Open Source Security Testing Methodology Manual (OSSTMM), which is a peer-reviewed methodology for performing security tests and metrics. OPST accreditation is the OSSTMM Professional Security Tester. OPSA is the OSSTMM Professional Security Analyst.