White Paper

Telecommunication Networks: Security Management

Telecommunication networks are today an inseparable part of social interaction and critical national infrastructure. Protecting these networks from malicious attacks, that could lead to unavailability or loss of integrity and confidentiality of network services, is thus an important aspect that cannot be ignored. An effective and robust security programme should be implemented to protect telecommunication networks from such attacks.

This white paper presents some of the important security challenges to current telecommunication networks, the need for security management and an approach to manage security for these networks.

General Terms

Telecommunication, Network Security, Security Standards, Next Generation Networks, Circuit-switching, Packet-switching, Vulnerability Assessment, Fuzz Testing

Keywords

Telecommunication Networks, Security Management, Network Security, Next Generation Networks, Vulnerability Management, Fuzz Testing

About the Authors

Colonel Rajmohan, CISSP

Colonel Rajmohan heads the Security CoE practice of TCS' Niche Technology Delivery Group (NTDG). He has led several security initiatives in emerging areas and has been the architect for end-to-end security solutions for strategic consulting engagements in many industry verticals.

Ganesh Subramanya

Ganesh is a Security Architect with the Security CoE practice of TCS' Niche Technology Delivery Group (NTDG). He has worked extensively on ISO 27001 implementations and on information security management. He has also conducted several security audits across industry verticals.

Navneet Sharma

Navneet is a Security Analyst with the Security CoE practice of TCS' Niche Technology Delivery Group (NTDG). He has experience in information security management and network security. He has conducted several vulnerability assessments for applications and networks across various platforms.

Table of Contents

Introduction

Traditionally, the Public Switched Telephone Network (PSTN) has been the dominant type of public telecommunications (also referred to as "telecom" in this paper) network worldwide, and consists of telephone lines, fibre optic cables, microwave transmission links, communication satellites and undersea telephone cables.

The advent of cellular technologies led to the interconnection of the mobile phone (cellular) networks with PSTN. The PSTN was based on circuit-switched technology, which had been primarily developed for voice traffic. Technologies developed for data transmission like PSDN, ISDN, Dial-up, DSL and others also leverage the existing PSTN infrastructure.

Due to the growing demand for data and video services and the limitations of the circuit-switched technology, telecom operators find it economically prohibitive to expand their circuit-switched networks to meet demand. This has led to a gradual move towards the adoption of packet-based switching technology. Newer 2G and 3G mobile phone systems like GPRS, EDGE and HSPA that are designed for data transmissions are also based on packet-based switching technology.

The term, Next Generation Network (NGN), is generally used to refer to these packet-based networks that transport all information and services – data, voice and media like videos. NGNs are most commonly based on the Internet Protocol (IP). NGN is expected to reshape the current structure of the telecommunication system and access to the Internet [1].

Telecommunications Network Components

Today's telecom networks are a combination of several technologies – PSTN, 2G, 3G – that have evolved over a period of time. Generally speaking, the current telecom network comprises the following parts:

- Access Network – This is the part of the network that connects the telecommunication equipment – fixed or mobile – to the core network for provision of services. This includes the local loop (telephone cables/fibre optic) of the fixed networks and the radio links in a mobile network, the radio towers, base stations and controllers.
- Core Network – This consists of the network elements responsible for service delivery and setting up of the end-to-end connection and handovers, and may be classified into circuit-switched and packet-switched domains. The core network includes components such as switches, the Mobile Switching Centre (MSC), the Host Location Register (HLR), the Visitor Location Register, and the Authentication Centre.
- Application and Management Network – This consists of end-user application servers, and systems and services that support the operation, administration and maintenance functions of the network.
- Internal Network – This is the telecom operator's internal network. This includes systems used by the operator's employees.
- External Network – This is the externally visible network, typically deployed in the De-Militarized Zone (DMZ). This includes the Web servers, application servers and mail servers that are hosted by the telecom operator.

Security Challenges to the Telecom Networks

The structure and functioning of circuit-switched PSTN networks, traditionally controlled by the telecom operators, ensured fewer possibilities for misuse of the network, as compared to a packet-switched network based on an open protocol like the Internet Protocol (IP). However, the PSTN networks are increasingly being controlled and are dependent on software and on the operations networks. As a result, users now have greater access to functions that were previously restricted to telecom employees. This exposes the network to intruders and increases the potential for attacks caused by virus, worms and malicious software.

GSM, which is a widely used mobile phone system, implements several security mechanisms designed to protect confidentiality over radio interfaces, subscriber authentication, subscriber anonymity to external parties, and prevent the use of stolen terminals[2]. However, a speech call made between two GSM operator networks or between a GSM phone and a fixed phone traverses the fixed network, and is subject to the same security considerations in speech and signalling as for a fixed network. CDMA mobile networks are also exposed to the same threats and attack vectors as a GSM network.

Packet-based switching technology used in Next Generation Networks is usually implemented through the use of the Internet Protocol (IP) suite. The IP was based on open standards and not originally designed for security implementations. The weaknesses in the IP have been exploited since long, and add to the risks of adopting an IP-based network.

Both the traditional circuit-switched networks and the packet-based next generation networks are exposed to different threats and attacks – both from external and internal sources – that target the various parts of the telecommunications network. These attacks may be targeted at any part of the telecom network, including the radio path of the access network. Attacks on one telecom operator's network could also spread to multiple networks over the interconnection interfaces. Some of the threats to the telecom networks are listed in Table 1.

Threat	Can Result in
Unauthorised physical access to switching infrastructure, underground and local loop cable infrastructure and other critical telecom network equipment, for example, AuC, HLR and VLR	Tampering, destruction or theft of information and equipment, illegal tapping and interception of the network traffic
Interception of voice traffic or signalling system in PSTN networks due to absence of encryption for speech channels and inadequate authentication, integrity and confidentiality for the messages transmitted over the signalling system (which is based on the ITU-T SS7 specification)	Unauthorised access to telecom network traffic
Use of modified mobile stations to exploit weaknesses in the authentication of messages received over the radio interface	Spoofing of user de-registration and location update requests, leading to unreliable service/disruption
Use of modified base stations to entice users to attach to it	Denial of service, interception of traffic
Misuse of the lawful interception mechanism	Illegal tapping/interception of telecom network traffic

Threat	Can Result in
Compromise of the AuC or SIM used for storing the shared secret for the challenge-response mechanism	Identity theft (intruders masquerading as legitimate users)
Deployment of malicious applications on devices with always-on capabilities like smart phones and tablets	Use of these compromised devices target the operator's network (for example, by setting up botnets to carry out DDoS attacks)
Intrusions into the operations networks	Unauthorised changes to the users' service profiles, billing and routing systems, resulting in toll fraud and unreliable service
Compromises of network databases containing customer information	Unauthorised access to personal and confidential data
Masquerading as authorised users, by gaining access to their credentials by means of malware, hacking tools, social engineering tools or other means	Gain unauthorised access or greater privileges to the network systems, which can then be used to launch other attacks
Traffic analysis – observing the calling and called numbers, and the frequency and length of the calls	Inference of activities that can be used against the
Social engineering attacks on operator employees	Unauthorised access to confidential information

Table 1: Threats to Telecom Networks [3] [4]

Consequences for operators who fail to adequately protect their networks include:

- Financial loss
- Loss of reputation for the operators in the industry
- Loss of customer confidence
- Legal action and fines from regulatory bodies for failure to provide secure services

Apart from these, the weaknesses in the telecommunication networks may also be exploited by anti-national and terrorist organisations for their own benefit by intercepting communications, causing denial of service during terror strikes and also using it as a platform to launch attacks.

Need for Security Management in Telecom Networks

The import of telecom equipment from other countries that are antagonistic to a state's strategic interests may lead to supply chain contamination by means of embedded logic bombs and malware. The dependence on telecommunication networks and the critical role that they play in the economic growth of a country has led to government regulations in the telecom industry, which include requirements for ensuring the security of the telecom equipment and networks.

The interconnection of the PSTN networks of fixed and mobile phone systems and the next generation network has increased the attack surface of the telecom networks. The wide range of end-user devices that can now connect to the telecom networks has added to the complexity of the networks, thereby increasing the risks and vulnerabilities as well.

The security threats and challenges to the telecom network listed in the Section 3 are indicative of the risks to these networks. As noted, the consequences of not implementing adequate security measures to deal with these could be heavy.

Several international standard development organisations like ITU, ISO/IEC, 3GPP, 3GPP2 and ETSI have prescribed standards that are applicable to telecom networks. Some of the most prominent standards that include requirements/guidelines for the security of telecom networks are listed in Table 2. Also, many countries have legislations and regulations that the telecom operators must comply with, which may require the adoption of specific security standards.

Telecom operators should adopt a robust, managed security programme to ensure that their networks are protected against malicious attacks, both external and internal, while also ensuring compliance to the local regulatory environment. This requires a holistic approach to implementing security measures, based on globally accepted security standards and best practices.

Organisation	Standard/Specifications	Description
ISO/IEC	27001:2005	Specifies requirements for an Information Security Management System
	27002:2005	Specifies a code of practice for information security management based on ISO 27001
	27011:2008	ISO 27002 tailored specifically for application to telecommunications organisations, developed as a joint effort with ITU-T
	15408 (The Common Criteria)	A common set of security requirements for evaluation of computer security products and systems, including telecom network components
3GPP	33-Series	Provides specifications for security standards for GSM (including GPRS and EDGE), W-CDMA and LTE (including advanced LTE) mobile systems
3GPP2	S.S0086 and others	Provides specifications for security standards for GSM (including GPRS and EDGE), W-CDMA and LTE (including advanced LTE) mobile systems

Organisation	Standard/Specifications	Description
ITU-T[5]	E.408	Provides an overview of security requirements, threat identification frameworks and guidelines for risk mitigation
	E.409	Incident organisation and security incident handling
	X.805	Security architecture for systems providing end-to-end communications
	X.1051	ISMS guidelines for telecommunications, which is also referred to as ISO 27011:2008

Table 2 : Security Standards for Telecom Operators

Telecom Network Security Management

A multi-pronged approach to security should be adopted by telecom operators to address the current and future security challenges. Industry-recognised standards, best practices and technologies must be adopted to build a robust security programme. In addition, all applicable legal and regulatory requirements should also be considered.

Adopting a Security Framework

Organisations develop and implement security policies and procedures to address the security requirements for their environment. However, to be effective, these policies and procedures should be tightly coupled, and supported by industry-accepted guidelines, standards and best practices. There also should be a risk-based approach while developing these policies to ensure that the security measures are adequate to the address the perceived business risks.

Several IT Frameworks available today, like COSO, COBIT, ITIL, ISO27001 and others, can be adopted to formulate a security programme. The ISO 27001:2005 standard is one of the most widely accepted security standards across industries. This provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). For the telecom industry, this is further supported by ISO 27011:2008, which provides guidelines on information security management for telecommunication networks (jointly developed along with ITU-T).

The ISO 27001 standard is based on the Plan-Do-Check-Act (PDCA) model, which is applied to all ISMS processes, as illustrated in Figure 1. This PDCA model ensures that there is a continued focus on the security programme, and that it is not a one-time activity.

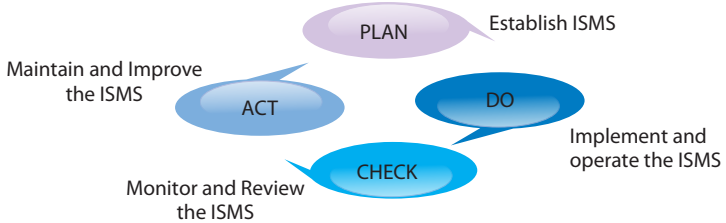

Figure 1: The PDCA Model

The ISO standard spans 11 security domains, and prescribes a total of 133 controls across these domains. Among others, this covers areas of Security Governance, Physical Security, System and Network Security, Business Continuity, Incident Management and Compliance, all of which are critical for the security of the telecommunication networks.

Managing telecommunication security without cognisance of risk exposure creates the possibility of inappropriate or inadequate security measures, the consequences of which include resource wastage and unchecked exposure to harm. So, risk assessments play a vital role in any information security programme, ensuring that resources are being allocated in the most effective way to support the business. The ISMS framework requires that controls be identified on the basis of a thorough risk assessment, and documented as the Statement of Applicability (SoA). Figure 2 illustrates a possible risk management process for telecom networks.

The ISMS framework also provides flexibility in adopting controls so as to meet the regulatory and legal requirements of the telecom operator. Post-implementation, the ISMS is reviewed on a periodic basis by means of internal audits to check the effectiveness of the implementation. The standard also requires organisations to continuously improve their ISMS based on inputs from monitoring and maintenance activities, internal audits, reviews and industry best practices.

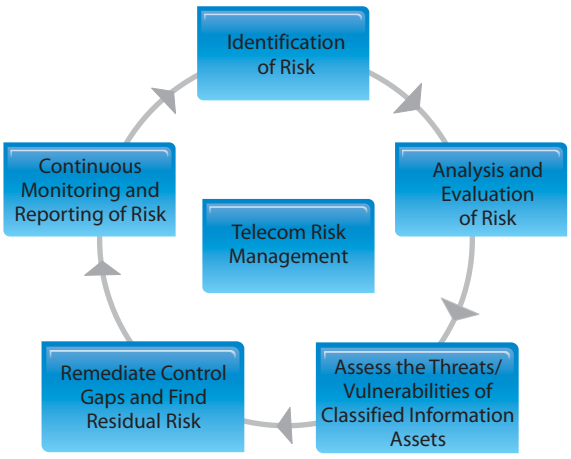

Figure 2: Telecom Risk Management Process

Organisations can also choose to undertake ISO 27001 certification based on assessments by external independent certified bodies. The certification will not only validate the implementation on a periodic basis, but also underscore management's commitment towards a strong security programme.

Implementing a Security Infrastructure

The implementation of ISMS policies and processes should be supported by a security infrastructure that includes multiple security layers. This "Defence in Depth" approach ensures that the compromise of one security layer alone does not expose the network to attacks.

Some of the security measures that can be deployed across the various layers are:

- Interference and tamper-proof cabling infrastructure
- Security guards and CCTV monitoring for operator premise perimeters
- Physical access control mechanisms like smartcard and biometric readers
- Firewalls at the network perimeter and DMZ for publicly accessible systems
- Host- and network-based Intrusion Detection/Protection Systems
- Security Information and Event Management (SIEM) systems to handle security events and logs generated by multiple systems
- Malware management by deployment of antivirus, antispyware technologies on internal systems and mail servers
- Secure application development practices
- Security testing of the telecom equipment, perimeters, critical network components and applications
- Encryption and data masking techniques for both data at rest and transit
- Security awareness

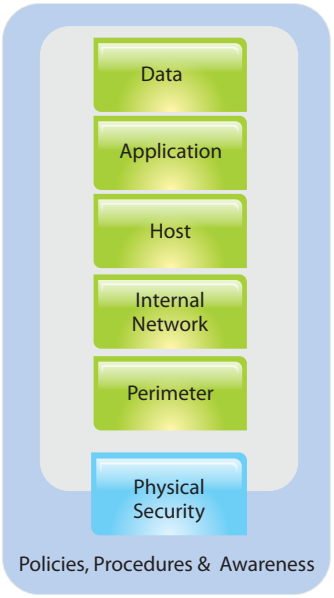

Figure 3: Defense in Depth

Conducting Security Testing

Maintaining a consistent security posture across an organisation's network in the face of the ever-changing nature of IT security is a complex and time consuming task. Periodic security testing plays a vital role in assessing and enhancing the security of networks.

Telecom Equipment Testing

Telecommunication networks are likely to have a heterogeneous mix of equipment from various suppliers. A highly credible, trusted third party certification programme must be in place to conduct an assessment to identify and evaluate security weaknesses and vulnerabilities contained in equipment software, firmware and hardware implementations. Certification of the supplier products against the Common Criteria Specifications (ISO 15408) ensures this at the component level.

IT and Telecom Network Vulnerability Assessment

With a large number of vulnerabilities and an increasing number of attacks exploiting them being reported across technology platforms, it is becoming difficult to ensure that the critical elements of a telecommunications network are not vulnerable to these attacks.

Vulnerability assessment can be used to:

- Identify vulnerabilities
- Report and assess the vulnerability and its overall consequence
- Recommend mitigation strategies (safeguards or workarounds)
- Ensure that organisational security policies are met by auditing the system configurations
- Provide input into the incident handling process

A five-phase approach to vulnerability assessment is illustrated in Figure 4.

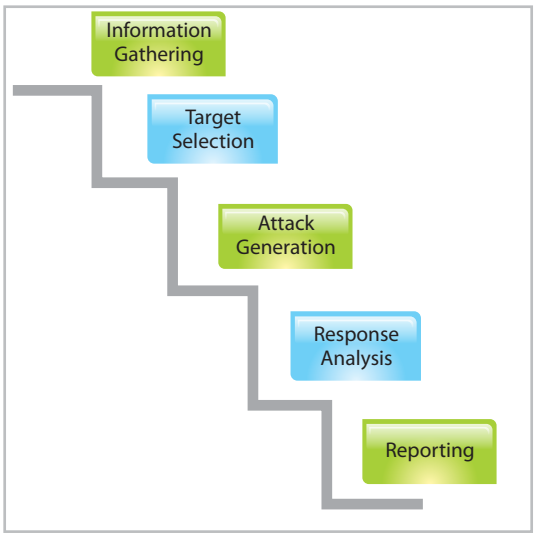

Figure 4: Vulnerability Assessment Approach

Fuzz Testing

While vulnerability assessments can help identify and mitigate known vulnerabilities, it cannot be used to protect against exploitation of unknown vulnerabilities that are likely in complex networks like telecom networks. A methodology that is now being used to address these unknown vulnerabilities is Fuzz Testing, which is a form of attack simulation where abnormal inputs are used to trigger vulnerabilities [6]. One approach is model-based fuzzing, which uses protocol specifications to target tests at protocol areas most susceptible to vulnerabilities. Another approach, traffic capture fuzzing, uses traffic captures to create the fuzzers used for testing.

Radio Access Path Security Testing

An aspect of security testing that is unique to a telecommunications network is the testing of the radio access network. By and large, the approach to testing radio nodes is based on custom test scenarios that are in turn based on the characteristics of individual radio nodes. The primary tools in use are a modified Mobile Station (MS) and the custom radio traffic injection scripts. In order to protect the privacy of subscribers' information during the security tests, it is recommended that a second test device (an unmodified MS) is used as the primary target for the attacks where possible. The tests should be designed to prevent legitimate subscribers from associating with the modified equipment being used, and also to ensure that there is no service disruption.

Penetration Testing

Penetration testing supplements the vulnerability assessment activities by taking "the last step" and actually exploiting these vulnerabilities to compromise and gain access to the target systems, and not just report potential vulnerabilities. Penetration testing provides the "hacker's" perspective inside and outside the network perimeter. Security testing specialists attempt to infiltrate the client's network, systems and applications using not only common technologies and techniques, but also specialised tools and some unexpected methods, such as combined techniques ("multi-vector" attacks). The result is a detailed report identifying key vulnerabilities and suggested protection tactics – an action plan to improve the organisation's security posture.

Conducting Network Security Audits

Network security audits can be conducted to discover, assess, test and report the existing security infrastructure implementations. Network security audits should be based on internationally accepted standards and frameworks like ISO 27001 and COBIT.

Figure 5 illustrates a methodology for network security audits, consisting of four distinct phases:

1. Scope and Plan - This involves defining the audit objective, determining the audit scope, understanding the business risks and defining the project plan.
2. Information Gathering – This is gathering the information about the security policies, processes and security controls that have been implemented, and also the industry best practices, standards and guidelines that are applicable.

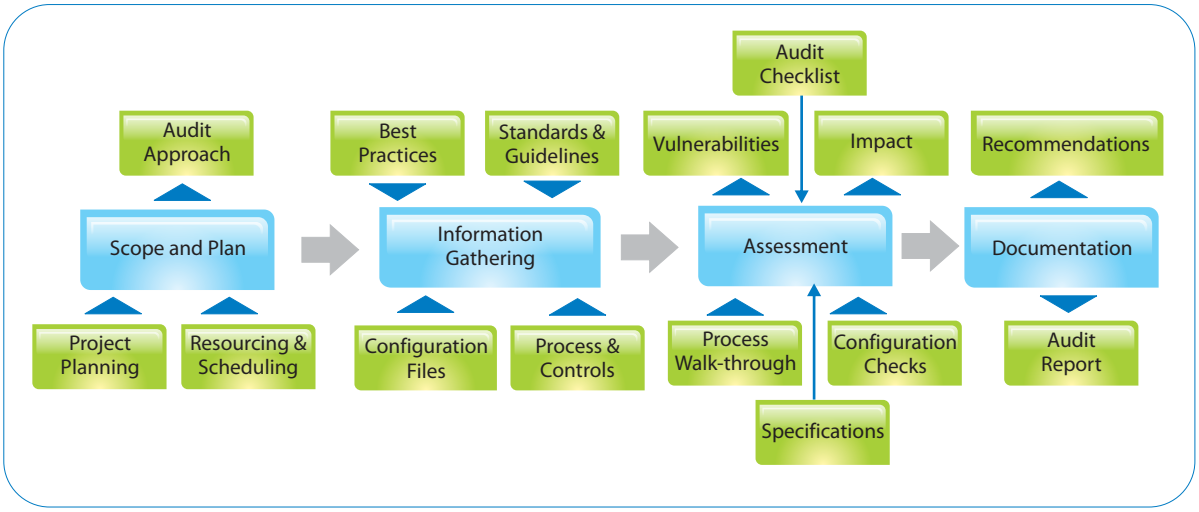

Figure 5: Security Audit Methodology

3. Assessment – This is performed to discover the vulnerabilities existing in the system. The impact of any discovered vulnerability on the telecom operator business is used to determine a risk rating.
4. Documentation – This includes the analysis and reporting of data and test results. The report documents the results and findings of the security assessment and includes a discussion of the risk analysis arising from the assessment, implications to the telecom operator's systems and networks and recommendations for improving the security position of the operator's applications, systems and networks.

Conclusion

As telecom technologies advance, and NGNs are more widely deployed, it is essential that telecom operators put their best foot forward to secure their networks and services. It is alo critical that they conduct periodic risk assessments of their networks and tweak their security programmes to adapt to the ever-changing security environment. As new vulnerabilities are discovered, new threats emerge, and security products evolve, operators need to take judicious decisions to choose the right security solutions and methodologies, in line with their risk appetite.

References

[1] Convergence and Next Generation Networks, Ministerial Background Report (OECD), 2007

[2] "Security in the Traditional Telecommunications Networks and in the Internet", Markus Isomäki, November 1999

[3] NIST Special Publication 800-13, Telecommunications Security Guidelines for TMN, October 1995

[4] "A Guide to 3rd Generation Security", 3GPP TR 33.900 version 1.4.0

[5] Security in Telecommunications and Information Technology, An overview of issues and the deployment of existing ITU-T recommendations for secure telecommunications, ITU-T, June 2006

[6] Unknown Vulnerability Management for Telecommunications, Anna-Maija Juuso and Ari Takanen,Codenomicon, February 2011

List of Abbreviations

Abbreviation	Expansion
2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AuC	Authentication Centre
CCTV	Closed Circuit Television
CDMA	Code-Division Multiple Access
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSL	Digital Subscriber Line
DMZ	De-Militarized Zone
EDGE	Enhanced Data for Global Evolution
ETSI	European Telecommunications Standards Institute
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HLR	Home Location Registry
HSPA	High Speed Packet Access
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LTE	Long Term Evolution (3GPP)
MS	Mobile Station
MSC	Mobile Switching Centre
NGN	Next Generation Network
PDCA	Plan-Do-Check-Act

Abbreviation	Expansion
PSDN	Public Switched Data Network
PSTN	Public Switched Telephone Network
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SoA	Statement of Applicability
SS7	Signalling System 7
TSG	Technical Specification Group
VLR	Visitor Location Registry
W-CDMA	Wideband Code Division Multiple Access

TATA CONSULTANCY SERVICES

Experience certainty.

Contact

For more information about TCS' consulting services, contact at **ntdg.scan@tcs.com**

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w

Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at **www.tcs.com**

IT Services
Business Solutions
Outsourcing

TCS Design Services | M | 01 | 12