ICT Security and Security Testing Aspects

Mayur Dave[1] and Anand R. Prasad[2]

[1] *mayur215in@yahoo.co.in*
[2]*NEC Corporation, Japan; email: anand@bq.jp.nec.com*

Received July 2013; Accepted August 2013

Abstract

This paper provides an overview of the activities of Security & Privacy Working Group (S&P WG) of the Global ICT Standardisation Forum of India (GISFI). Today telecommunications has become "the utility" of human society and thus is the life-line for not only citizens of India but also for the economy. Therefore there has been serious consideration for security and privacy in and of Indian telecommunication systems and networks. Therefore it was found essential to create a security and privacy working group (S&P WG) in GISFI that would develop solutions for ICT security issues in India as well as provide security solutions for activities in other WG. This paper presents details of the scope, current work accomplishments and future strategy and plans of the S&P WG [1].

Keywords: Telecom Security, Network Element testing, Network testing, methods.

1 Introduction

Since there have been incidents of security breaches in network systems around the world in recent times, the topic of security and consequently the effort of securing network systems has gained momentum.

Journal of ICT Standardization, Vol. 1, 175–186.
doi:10.13052/jicts2245-800X.12a4
© 2013 *River Publishers. All rights reserved.*

Considering this eventuality, as a safety precaution, the Department of Telecom (DoT), Government of India (GoI), has mandated network equipment manufacturers to comply with their latest regulation of having network equipment products tested and certified for security, in Indian labs accredited by the Government [2]. At the same time, the Government has mandated Telecom Licensees (Service Providers) to have their networks tested and certified for security, through periodic network security audits [2]. GISFI S&P WG has undertaken the activity to assist the Indian Telecom industry stakeholders (the Government, the Telecom Service Providers and Network Equipment Manufacturers) by means of preparing and proposing the Telecom Security Framework Proposal, and also Security Testing Methods for Information and Communication Technology (ICT) products and Systems. GISFI S&P WG with its security expertise is analyzing DoT requirements [2] to help in defining and resolving the gaps in the guidelines to enable timely and appropriate implementation of security guidelines.

The paper starts with a section on background and scope to the S&P WG in Section 2 followed by achievements of the group in Section 3. In Section 4 we briefly discuss future plans of the WG and in Section 5 we conclude the paper.

2 Background and Scope

2.1 Background Information

The Security & Privacy Working Group (S&P WG) started as a topic within the Special Interest Group (SIG) and matured with time as a WG. In its short life-span the S&P WG of GISFI has clearly described its role and is working with standardization bodies worldwide. Currently the prime topic that the S&P WG is working on is regarding the Indian network testing requirements. So far, the organizations that have contributed to this WG are NEC, Niksun, TCS, Tata Teleservices, Ericsson, Huawei and I2TB. The working group also had workshops and meetings with participants from DoT, IISc, Tata Teleservices, Airtel, Aircel, MTS and Uninor.

2.2 Scope and Objectives

In this section we present the scope of S&P WG as given in [1].

Security and privacy is of utmost importance in today's industry particularly for Information and Communication Technology (ICT). Work on security must be started from the beginning with complete system

consideration otherwise the result is a system full of security holes requiring patch-work. Thus work on security and privacy is required for all technical activities of GISFI. Working on security as a side topic will not suffice therefore a separate technical committee that focuses on security and privacy aspects and has expertise in the field is necessary.

The security and privacy working group performs the following tasks:

1. Study security and privacy including legal intercept requirements regarding ICT for the India.
2. Develop recommendations regarding security and privacy including legal intercept in/for India. This can also include recommendation on algorithms to be used.
3. Perform threat analysis on systems under consideration and technologies being developed by GISFI.
4. Develop security and privacy solutions in collaboration with other committees.
5. Develop legal intercept solutions.
6. Bring Indian requirements on security and privacy including legal intercept to international standardization bodies.

3 Achievements

In this section we give an overview of each of the S&P WG deliverables. These deliverables are the outcome of exhaustive study that we at GISFI S&P WG have performed towards the DoT requirements for security testing mandate to Indian Telecom Network equipment vendors and Network Operators.

The Technical Reports and Specifications have been based on the study of existing Global Wireless Standards and Industry best practices. Recent industry trends and advancements have also been tracked and relevant requirements designed and incorporated while preparing the reports and TSes so as to ensure that the work being done achieves compatibility. These documents have been presented in the GISFI Standardization series meetings and stand approved after review from GISFI members.

A workshop on Indian security requirements between GISFI and DoT was also organized.

GISFI S&P WG is in continuous communication with the Department of Telecom (DoT) and Telecommunications Engineering Center (TEC) of the Government of India. All deliverables of GISFI are submitted to both security section of DoT and TEC.

Table 1 GISFI Security and Privacy WG list of achievements.

Technical Specifications	***Significance***	***Status***
Network (and Equipment) Security Requirements and Element Selection Guideline for Security Testing	A comprehensive list of Standards-based Telecom network (element) security requirements, along-with a guideline for assisting on priority-based, selection of network elements to be considered for security testing.	Completed
Telecom Security Framework Proposal for India	Shall present definitions and descriptions for various security testing-related terms, along-with a methodology specified for the each of those terms.	In progress
Technical Reports	***Significance***	***Status***
Telecom Security Framework Proposal for India [3]	Presents definitions and descriptions for various security testing-related terms and information on available methodologies (Standards and Industry Best practices).	Completed
Security in mobile communication systems; Comparison and proposals for India [4]	Presents information on security implementation and/or architecture in the various Cellular technology generations, along-with (potential) security threats in each.	Completed
Security Testing Methods for ICT products [5]	Presents a proposal for security testing methods for security testing for network elements and network (as an entity).	Completed
Element Selection Guideline for Network Equipment Security Testing [6]	A guideline proposal for assisting on priority-based, selection of network elements to be considered for security testing.	Completed
Requirements Study on Circular titled "10-15/2011-AS.III/(21)" [8]	Presents an understanding of the DoT's requirements towards security testing mandate, as mentioned in the said DoT Circular.	In progress
Telecom Security Policy Study and Proposals	Presents an understanding of the DoT's Telecom Security Policy and GISFI proposals towards refining or enhancing the same.	In progress

Considering it as a sign of being appreciated, the work done by the S&P WG has been well accepted by the DoT and parts of it are being used to develop the regulations on security testing in the Indian context.

Our achievements, in terms of documents, are summarized in Table 1.

3.1 Telecom Security Framework Proposal for India [3]

We have presented a technical report outlining the definition and description of ICT security related terminologies as "Network Forensics", "Network Hardening", "Penetration Testing" and "Risk Assessment". The report also presents few standardized methodologies and best practices designed by various organizations for each of the above-listed aspects related to security testing.

Conclusively, we present the topic of "Network Forensics" as the capture, storage and analysis of network events, "Network hardening" as involving the steps taken to secure a network and the devices on it, "Network Penetration Testing" as a test of a network's vulnerabilities by having an authorized individual actually attempt to break into the network in disguise of a hacker and "Risk Assessment" as a process used to identify and evaluate risk and its potential effects, one of the phases of the generic risk management effort.

The report performs such a study on these ICT security related testing procedures, processes and related terminologies which have also been mentioned in the Department of Telecommunications (DoT) (vide Circular "10-15/2011-AS.III/ (21)", dated 31/05/2011) [2]. As a future activity, the report proposes to design a framework, including the same, that will find applicability for testing Mobile Communication Network Equipment's and Systems. Also, we propose on working on solutions leading to actions to fix and prevent recurrence of security problems, as required by the DoT.

A Technical Specification document based on the completed, available Technical Report is in the making.

3.2 Security in mobile communication systems: Comparison and proposals for India [4]

We have presented a technical report on the subject of "Security in Mobile Communication Systems" that is of paramount importance in the times of evolving technologies which is challenged by threats and attacks on them. It provides an overview of the security implementations or architectures provided in the various generations of wireless/mobile communication technologies. The report also provides a brief description of the various security issues in the various phases of technology evolutions in the various generations of wireless/mobile communication technologies. These security issues are in the form of False Base Transceiver Station (BTS) attacks, Interception, Denial of Service (DoS), Distributed Denial of Service (DDoS), Cryptanalysis of algorithms, etc.

As a future activity, we propose a gap analysis between the security mechanisms or architectures in each of the wireless technology generation, for the 3GPP and 3GPP2 technology Standards family, and the weaknesses or security flaws in the same. This would enable network equipment vendors and operators to address existing known issues through firmware or software patch fixes and upgrades.

Further, in this report we have enlisted the Mandatory and Optional requirements (including those for Lawful Interception), regarding the implementation and/or use of security features, as specified in the 3GPP 33-series Technical Specifications (TSs).

This list provides an overview to the concerned Indian Government departments on the 3GPP Standards-based security features, both mandatory and optional, that are to be considered by vendors and operators as part of the Indian Network Security requirements.

Further, this report assists network equipment vendors, network equipment (security) test labs and related stake-holders to select network elements, based on assigned (perceived) priority levels labelled by GISFI, to conduct security testing for network elements according to the DoT's Circular [2] to the TSP's.

The list of network elements, along-with network interfaces and reference points, are derived from the 3rd Generation Partnership Project (3GPP) and 3rd Generation Partnership Project–2 (3GPP2) Wireless Communications Standards.

A Technical Specification document based on the available Technical Report, with the Mandatory and Optional requirements (including those for Lawful Interception) has been presented at the GISFI Standardization Series Meeting #14 and is currently under review by GISFI members.

3.3 Security Testing Methods for ICT products [5]

We have presented a report capturing information about already available security test methods being employed by product/system certification bodies. Examples of such product/system certification schemes are Common Criteria (CC) (testing), and those based on the National Institute of Standards and Technology (NIST) Special Publication Guideline (SP800-115), Open Web Application Security Project (OWASP) Testing Guide (Ver. 3), etc.

The report presents a proposal on 'Network Element Testing' steps in regards to performing security tests on network elements and to certifying them as 'approved/tested/etc. for security' before they are integrated into

the mobile network. The proposal outlines a phase-wise testing of network elements, first against Wireless Standards by the 3GPP or 3GPP2 and then against developed Security Targets (STs) and Protection Profiles (PPs) for CC testing. The network elements to be tested for security compliance are listed and assigned a perceived priority as documented in [6].

The report also details a proposal on 'Network Testing' in regards to performing security tests on entire mobile networks deployed by Cellular Operators and to certifying them as 'approved/tested/etc. for security'. It proposes testing of three distinctly identifiable sub-systems (Access Network sub-system, Core Network sub-system and Internet Sub-system), first against Wireless Standards by the 3GPP or 3GPP2 and then against the NIST SP800-115 Guidelines. After successful rounds of testing on the sub-systems, a complete network test, first against Wireless Standards by the 3GPP or 3GPP2 and then against the NIST SP800-115 Guidelines is proposed.

In this report, we have listed the technical and policy gaps between the DoT requirements [2] and the actual (detailed) requirements needed to meet those set by the DoT. This shall help GISFI in working towards providing recommendations with an aim to fill those gaps and assist network operators within the country to practically realize the DoT requirements.

A Technical Specification document based on the completed, available Technical Report is in the making.

3.4 Study on the Common Criteria (CC) [7] in the Indian context

We have presented an input document [7] that introduces the Common Criteria that is a popularly adapted standard for evaluating Information and Communications Technology (ICT) products. This report presents the various technical and procedural aspects related to CC testing and certification. It describes how the various parts (Standards) that collectively make up the Common Criteria have been designed and organized and provides an overview of the contents of each of those Standards. Precisely, the CC has been adopted and standardized by the ISO/IEC into three parts under the ISO/IEC 15408 family (as Part 1, Part 2 and Part 3). Along-with the ISO/IEC 18045 Standard (known as the Common Evaluation Methodology), the ISO/IEC specifies the actions to carry out in the process of evaluation of an ICT product as required by ISO/IEC 15408.

The Common Criteria (CC) is a standardized framework for evaluating ICT products against two types of requirements:

- Security Functional Requirements
- Security Assurance requirements

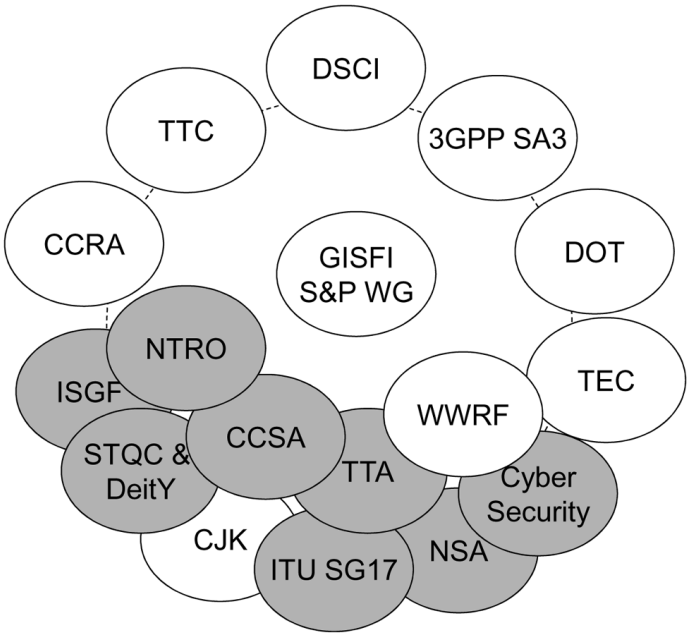

Figure 1 GISFI S&P WG liaison (gray: planned to send liaison).

This report also discusses about the Common Criteria Recognition Agreement (CCRA) and various aspects of certification tasks that the CCRA carries out in co-ordination with various nations of the world.

As mentioned in Section 3.3 and as depicted in Sections 4 and 5, GISFI is actively seeking to engage in and develop towards CC testing and certification for ICT products in the Indian context.

4 WG Plan

Goal of the S&P WG is to have its specifications accepted by the Indian government. For this purpose, strengthening the relation with DoT and, if needed, with other government agencies will be necessary. The TRs of S&P WG is now completed or close to completion therefore activity on technical specifications (TSes) is on-going.

Planned topics, till date, towards developing TSes for assisting TSP's to fulfil the DoT mandate of Security Testing are as follows:

- TS on Network Element Security Testing
- TS on Network Security Testing

- TS on Tools for (Network Element/ Network) Security Testing
- TS on Security Requirements

The WG also plans to develop relationship with several international organizations working on security, some of this is shown in Figure 1.

5 Conclusions

The GISFI security & privacy working group has already produced 1 technical Specification and 5 technical reports towards Indian security requirements. These reports are communicated to the Indian government department of telecommunications. The WG works with Indian mobile operators, vendors and the government thus giving results that balance all needs while fulfilling the security requirements. In the short span of its activity, the S&P WG has also developed relationship with international bodies, for example, 3GPP, CJK, TTC etc. Several new topics are also being developed by GISFI members thus many more results should be accepted from the WG in nea future.

References

[1] GISFI_SIG_201109129, "Security WG Proposal", September 2011.
[2] DoT Circular "10-15/2011-AS.III/(21)", 31 May 2011. URL: www.dot.gov.in/AS-III/2011/as-iii.pdf.
[3] GISFI TR SP.101, "Telecom Security Framework Proposal for India"; December 2012.
[4] GISFI TR SP.103, "Security in mobile communication systems: Comparison and proposals for India"; January 2013.
[5] GISFI TR SP.105, "Security Testing Methods for ICT products"; January 2013.
[6] GISFI TR SP.106, "Element Selection Guideline for Network Equipment Security Testing"; January 2013.
[7] GISFI_SP_201206260, "Report on Common Criteria (CC) in the Indian context"; June 2012.
[8] GISFI TR SP.100, "Requirements Study on Circular titled "10-15/2011-AS.III/(21)", dated 31/05/2011"; January 2013.

Biographies

Mayur R. Dave, MBA- Marketing (Amity University), preceded by a Bachelor of Engineering (B.E.) degree in the field of Electronics and Telecommunications (Mumbai University), is a Senior Manager with an Indian Telecom Operator and has a rich experience working with globally, leading telecommunication product companies in their Research and Development (R&D) divisions for their respective India centers. His expertise is built on testing and validation of telecommunication (end-user) devices to ensure quality and thereby to assist in building and maintaining brand equity for companies as Nokia Mobiles and LG Mobiles that he has worked with. For over a decade, Mayur has played a vital role in formulating quality R&D test processes for organizations and has also contributed to integrating technical superiority into the same through his understanding of global wireless Standards. In his current stint with an Indian Telecom Operator, he is responsible for leading the validation of, and enabling the launch of, quality telecommunication end-user devices for the Operator. As an independent Telecom professional, he also contributes towards GISFI Work Group (WG) research activities in the form of numerous input documents and Technical Reports/Specifications (TR's/TS's), for the 'Security and Privacy' and 'Future Radio Networks' WGs, under the proficient guidance of Dr. Anand R. Prasad.

Vision: Telecommunications and its services will become a part of life as is breathing to humankind.

http://www.prasad.bz

Anand R. Prasad, Dr. & Ir. (MScEngg), Delft University of Technology, The Netherlands, Certified Information Systems Security Professional (CISSP), Fellow IETE and Senior Member IEEE, is a NEC Certified Professional (NCP) and works as a Senior Expert at NEC Corporation, Japan, where he leads the mobile communications related security activity. Anand is a vice-chairman of 3GPP SA3 (mobile communications security standardization group). He is a Member of the Governing Body of Global ICT Standardisation Forum for India (GISFI) where he is founder chairman of the Security & Privacy working group and

was chairman of the Green ICT working group. Before joining NEC, Anand led the network security team in DoCoMo Euro-Labs, Munich, Germany, as a manager. He started his career at Uniden Corporation, Tokyo, Japan, as a researcher developing embedded solutions, such as medium access control (MAC) and automatic repeat request (ARQ) schemes for wireless local area network (WLAN) product, and later he was a project leader of the software modem team. Subsequently, he was a systems architect (as distinguished member of technical staff) for IEEE 802.11 based WLANs (WaveLAN and ORiNOCO) in Lucent Technologies, Nieuwegein, The Netherlands, during which period he was also a voting member of IEEE 802.11. After Lucent, Anand joined Genista Corporation, Tokyo, Japan, as a technical director with focus on perceptual QoS. Anand has provided business and technical consultancy to start-ups, started an offshore development center based on his concept of cost effective outsourcing models and is involved in business development.

Anand has applied for more than 50 patents, has published 6 books and authored more than 50 peer reviewed papers in international journals and conferences. His latest book is on "Security in Next Generation Mobile Networks: SAE/LTE and WiMAX", published by River Publishers, August 2011. He is a series editor for standardization book series and editor-in-chief of the Journal of ICT Standardisation published by River Publishers, an Associate Editor of IEEK (Institute of Electronics Engineers of Korea) Transactions on Smart Processing & Computing (SPC), advisor to Journal of Cyber Security and Mobility, and chair / committee member of several international activities. He is a recipient of the 2012 (ISC)² Asia Pacific Information Security Leadership Achievements (ISLA) Award as a Senior Information Security Professional.