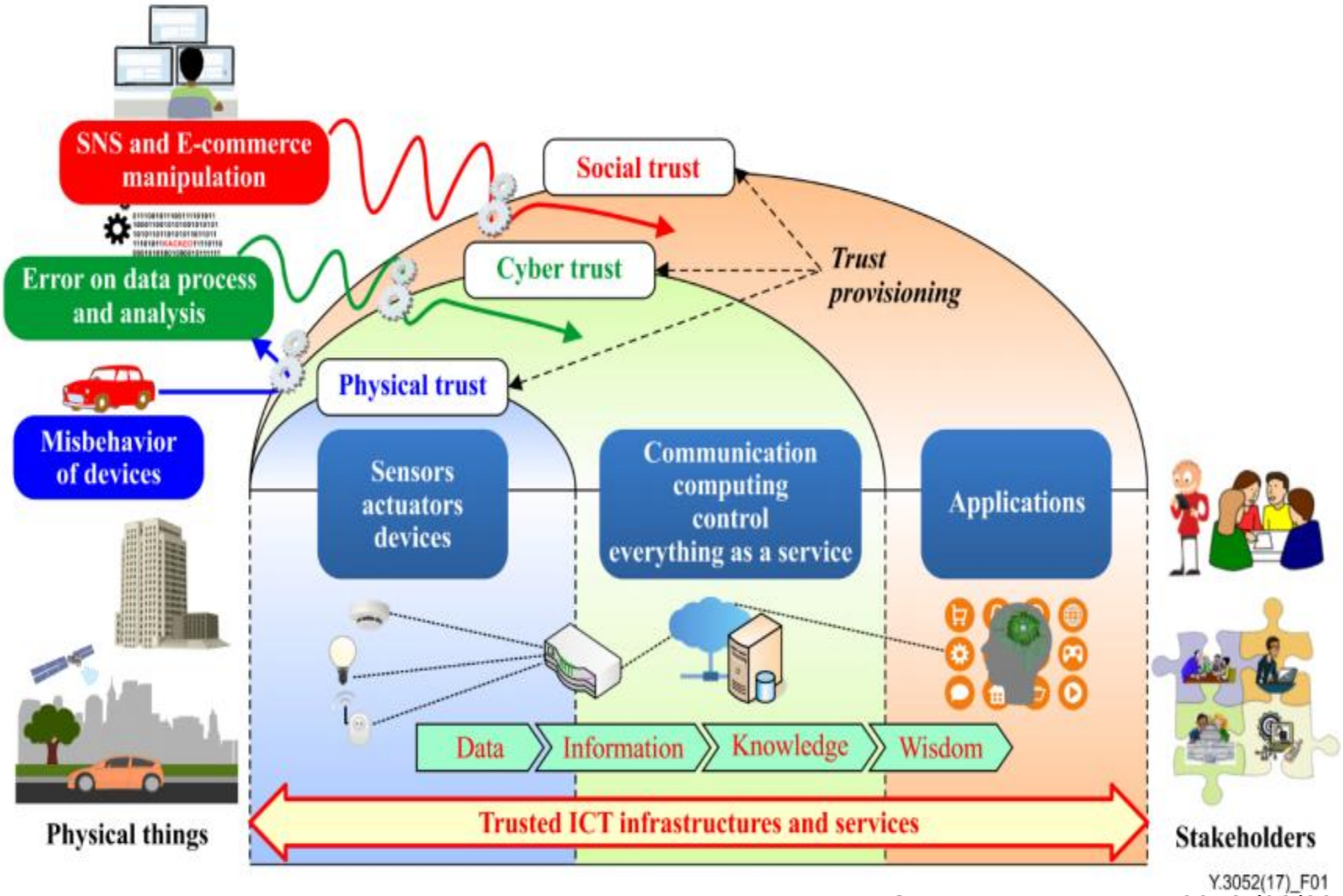
Security testing of Telecom equipment

P K Singh
DDG (TS), TEC, DoT

Transformation – Knowledge Society



Source: Rec. ITU-T Y.3052 (03/2017)

Pervasive ICT

- Digital India Program of GoI with vision around:
  - Digital Infrastructure as a Core Utility to Every Citizen
  - Governance and Services on Demand
  - Digital Empowerment of Citizens
- 1,183.04 million wireless subscribers, 407.88 million wireless & 21.35 internet subscribers
  - INR 1500 billion (approx.) investments
  - remaining 42300 villages to be provided universal mobile connection
  - All village panchayats to be connected through optical fibre, 2.6 lakh Km of fibre laid, 1.1 lakh panchayats already connected remaining 139000 panchayats to be connected by 2019
- Smartphone using population to be 530 million by 2018
- 38000 Wi-Fi hotspots under Bharatnet, proposed to add 700000 in next three years with 2-5 in each panchayat
- 48000 panchayats already having broadband services with 7000 to be added in 2018

Pervasive ICT

- Reserve Bank of India (RBI) data on (EPS), digital transactions in FY 17 was 1569.3 crore. 1512.6 crore for FY 16 targeted to make 2500 crore
- Demonetisation and subsequent development and launch of BHIM did increase the growth of digital transactions. Between November 2016 and January 2017, 545 crore digital transactions happened in India
- Linking of Aadhar, bank accounts, Gas connections, PAN, Mobile connection etc
- 20 mn registered users in GSTN, 60 mn taxpayer's information consisting of PAN, Bank Account, IT Details etc is available with Income Tax Department, 250 mn Passport information including personal details , 1.19 bn unique Aadhar IDs and 700 mn online service requests in 2017 like issuing caste certificate, driving licenses etc
- TSP generate and have access to call detail records, calling patterns, location data, data usage information, etc
- Growth in usage of social Media and OTT Services

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

A Brief History of the World

Security – Definition

- The protection against something bad that might happen in the future
  - Cybersecurity against potential danger
  - A danger or a threat is the possibility of something happening (attack, error, dysfunction, natural catastrophe, ...) that will injure, damage or destroy an ICT resource
  - The threat may/may not have a criminal origin, could be intentional or not
- The telecommunication infrastructures and the services are to be conceived, designed, set up and managed with security in mind
- Security is the cornerstone of any telecommunication activity; it should be viewed as a service that makes it possible to create other services and generate
- It is not a matter of technology alone

Source: ITU Cyber Security Guidelines for developing countries

Security Criteria

The Central theme of ICT security is the usability of the system

- The capability of a system to be utilized - availability
- The capability of a system to prevent unauthorized persons and processes from accessing data - access control procedures such as identification, authentication and authorization, preservation of data confidentiality and integrity
- The capability of a system to allow only authorized persons and processes to perform data modification
- The capability of a system to prove that actions and transactions have actually taken place - traceability, proof, administration, audit and non-repudiation
- The capability of a system to carry out actions and provide its expected services - continuity, reliability, user friendliness and operational soundness

Source: ITU Cyber Security Guidelines for developing countries

Security – Objectives

- Protecting values
- Reducing the likelihood that a threat materializes;
- Limiting the damage or malfunction resulting from an incident
- Ensuring that, following an incident, normal operations can be restored within an acceptable time-frame and at an acceptable cost.
- Providing support to the Lawful needs
- Close loop feedback for continuous improvement
- whether one calls it computer or telecom security, it touches on the security of the digital wealth of people, organizations and countries
- A strong response to the human, legal, economic and technological dimensions of information infrastructure security needs can build confidence and generate economic growth benefiting all of society - reinforcing trust

Why Security Testing

- Telecommunication networks are playing a critical role in the economic growth of the country
- Import of telecom equipment from other countries - embedded logic bombs and malware
- 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
- Online banking users in India to cover one & all by 2020 from 45 million active urban users
- Outlook and Expenditure towards Security

Why Security Testing ?

- In 2020, the average Indian will be 29 (lower than the average age in China and Japan). India's workforce will be the largest and youngest in the world
- More than 27,000 cybercrimes were reported in first half 2017, according to data released by the information and technology ministry. The figure was 50,362 for the entire 2016
- vulnerable to various risks such as phishing, identity theft, card skimming, vishing, SMSishing, viruses and Trojans, spyware and adware, social engineering, website cloning and cyber stalking
- privacy concerns also emanate from the activities of a variety of other stakeholders that process and control the personal data of users.
  - Cookies, Device fingerprinting, permissions by Applications
  - The devices and equipment used by individuals
  - the use of proprietary codes and systems
  - Growth in adoption of IoT

Why Security Testing ?

- Preserving data confidentiality is a fundamental motivator for ensuring the security of telecom infrastructure.
- Role of this sector as one of the key pillars of critical national infrastructure. Vulnerabilities in the telecommunication infrastructure can lead to disruption of basic services with a severe impact on citizens, businesses and the delivery of public services.
  - Customers/subscribers need confidence in the network and the services offered, including availability of services (especially emergency services) in case of major catastrophes.
  - Public authorities demand security by directives and legislation, in order to ensure availability of services, fair competition and privacy protection.
  - Network operators and service providers themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the public

Why Security Testing - Security incidences

- An advertisement on DarkNet announcing secret access to the servers and database dump of over 6000 Indian businesses - ISPs, Government and private organisations
- 3.2 million credit card and debit card details were stolen.Food and Civil Supplies Department of Chandigarh was reported to have published Aadhaar numbers of their public distribution system beneficiaries. Similar leak from Jharkhand
- As per incidents reported to CERT-In , 79 phishing incidents affecting 22 financial organisations, 13 incidents affecting ATMs, Point of Sales (POS) systems
- The RBI has registered a total of 13083, 16468, 13653 and 12520 cases of frauds involving credit cards in 2014-15, 2015 -16, 2016-17 and quarter April-September 2017
- Edward Snowden, from his asylum in Russia, and an Australian security expert Troy Hunt have raised questions on database security in India

Scope & Objective

- Deals with the testing the security features of all types of IP and telecom / ICT equipment in access, transport, control and application layers of wireless and wire line domain

- Various types of End User Devices such as mobile handsets, dongles, tablets, modems etc. and CPE devices such as Residential Gateways, LTE- CPE devices with Wi-Fi interfaces towards user etc.

- Proactive detection of vulnerabilities, which includes identification, understanding and verification of weaknesses, misconfigurations and vulnerabilities within all types of end user devices and nodes in a telecom network

- To test the resiliency of a system (network nodes and CPEs) against Distributed denial of service (DDoS) attacks, Botnets, Phishing, identity theft, Advanced Persistent Threats etc.

Security Testing - relevant standards

- ITU - T X.1520 defines the the use of the common vulnerabilities and exposures (CVE) , which provides a common nomenclature for publicly known problems in the com mercial or open source software used in communications networks, end-user devices ,etc
- ITU-T X.1524 defines the use of the common weakness enumeration (CWE), which provides a common nomenclature to exchange information regarding weaknesses in source code and operating systems
- ITU-T X.1521 provides common vulnerabilities scoring system (CVSS) as a standardized approach for communicating the characteristics and impacts of ICT vulnerabilities
- ITU-T X.1214 Security assessment techniques in telecommunication / ICT networks

Challenges in Security Testing

- No uniform testing methodology or parameters
- Each vulnerability is important and possess priority
- The tester should have knowledge and capability of detecting unknown attacks in addition to known attacks
- Knowledge and expertise of understanding the unknown vulnerabilities and attack scenarios
- Security tester must consider all the ways that a user might wilfully damage the application under test
- Access to Source code, binary code
- Support from the stakeholders

The way ahead

- By utilizing security and privacy mechanisms, trust can be realized in ICT infrastructures and services.
- Lack of trust, privacy, security, and reliability impedes information sharing
- Research is required for the creation of knowledge and learning in secure networking, systems, and applications
- Standardization for all elements constituting the ICT infrastructure is essential for transformation to a knowledge society

Thank You !