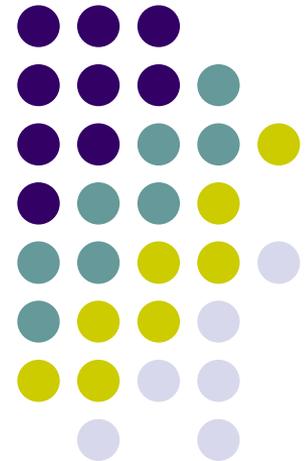
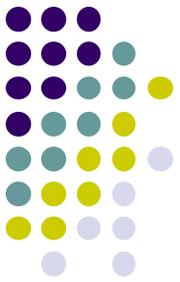


Telecom Testing and Security Certification

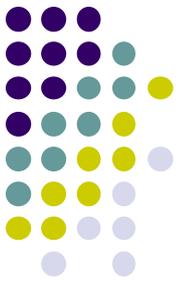
A.K.MITTAL
DDG (TTSC)
Department of Telecommunication
Ministry of Communication & IT



Need for Security Testing and Certification

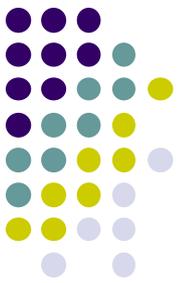


- Telecom is a vital infrastructure for the nation
- Equipments are procured from different sources/countries
- Need to develop our own capability to build and maintain a dependable and secure telecom infrastructure
- Need to develop frame work consisting of Standards, Processes and Procedures to identify safe to connect Telecom equipments



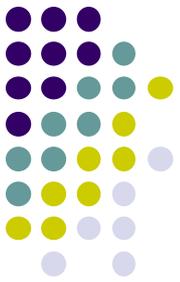
How to identify safe to connect equipments

- By measuring performance of equipments under cyber attacks
- By assessing the robustness in protocol implementations
- By detecting abnormal behavior of network under attacks
- By checking embedded malware during product's development stage or in transit



Threats to Network and Network elements

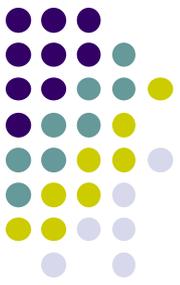
- Known DOS/ DDoS attacks (Network level and Application level) aim at Resource starvation, Hardware damage, Destruction of Network device/system configuration
- Known vulnerabilities (Published) as NVD /CVE Vulnerability Data bases maintained by NIST
- Unknown vulnerabilities (Zero day vulnerabilities) associated with newly published programs and web services
- Attacker attempts to exploit flaws in Network device protocol implementations
- Attacker attempts to exploit weak encryption crypto algorithms in Network device
- Attacker attempts to exploit flaws in Source Code implementations in Network device
- Attacker attempts to gather vulnerable information about network devices & with this information trying to penetrate into the network



Threats to Network and Network elements

Attacker attempts to

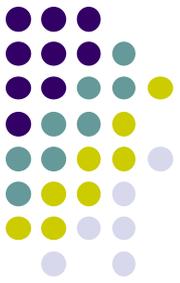
- attack unpatched software version of Network device
- install malicious code during software update process and take control on system and steal critical data in a system
- induct malicious code in Network device during supply chain process
- exploit poor passwords by way of Dictionary attacks/Brute force attacks



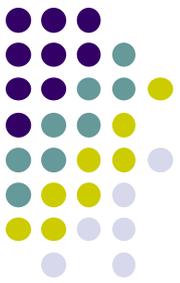
Regulatory Frame work

- Government of India had incorporated security conditions as a part of various service License agreements with TSP's
- TSP shall have organizational policy on security and security management of their networks including Network forensics, Network Hardening, Network penetration test, Risk assessment
- TSP shall induct only those network elements into its telecom network, which have been got tested as per relevant contemporary Indian or International Security Standards in labs located in India
- TSP should Keep a record of all the software updates and changes
- TSP should keep a record of supply chain of the products (hardware/ software). This should be taken from the manufacturer/ vendor/ supplier at the time of procurement of the products

Security Testing methodology-1 (Common Criteria) CEM



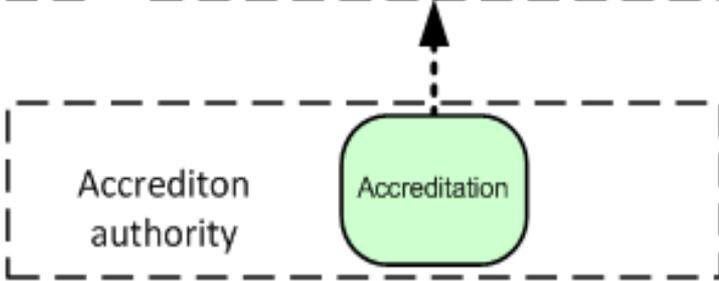
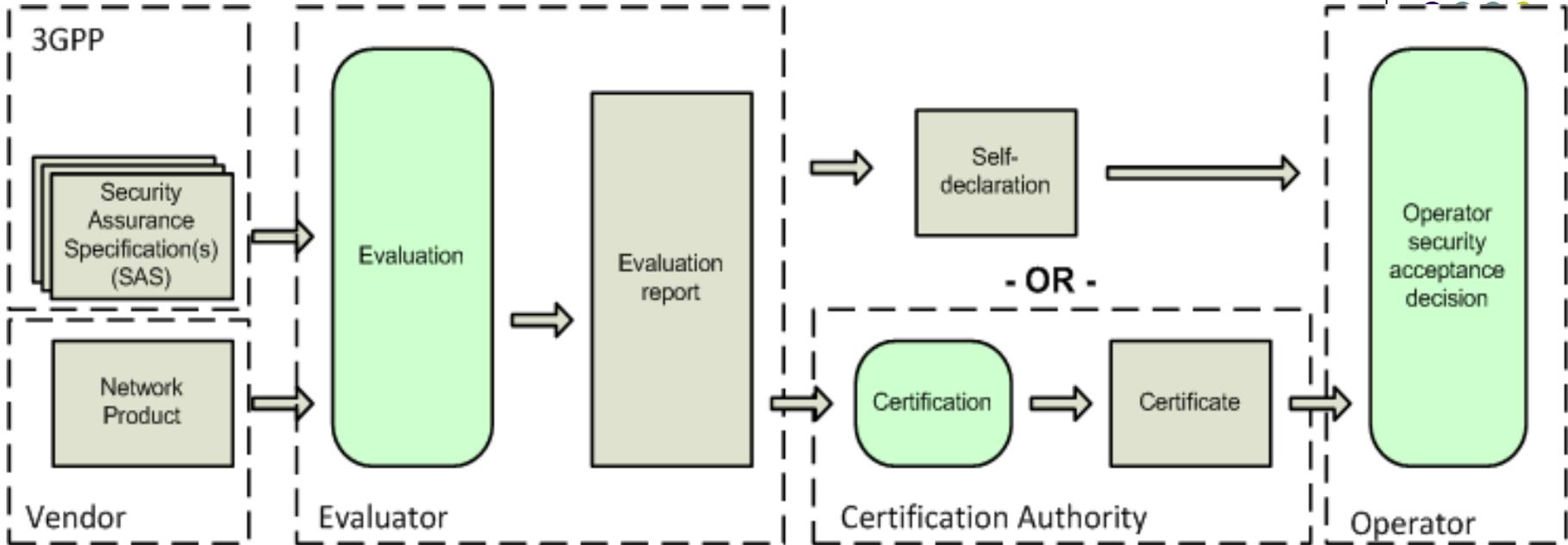
- Standards availability status - Readily available
- Generic and applicable for IT products (Hardware, Software and Firmware) originally and applicable for other areas
- More focus on Management traffic plane security than Data plane ,Control plane and Service plane security
- Detection of Intentional / Hidden Malware detection – Out of scope of evaluation
- Threat perception – Vendor driven
- Scope of evaluation
 - a) Network product evaluation (Product development process and Product Life cycle management process is done as a part of product's evaluation process
 - b) Security functional requirements compliance (positive testing)
- Opportunity to Buyer to express security requirements through Protection Profile



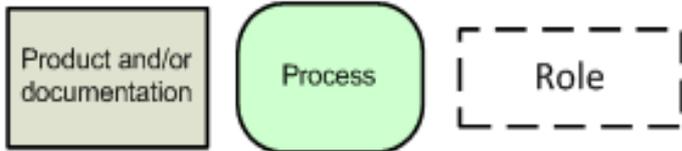
Security Testing methodology-2 (3gpp) SECAM

- Standards availability status - in evolving stage
- Focus on Management traffic plane, Data plane, Control plane and Service plane security- ITU-T X.805 Model
- Detection of Intentional / Hidden Malware detection – Out of scope of evaluation, now can be included as standards are in developing stage
- Threat perception – ITU-T X.800 Model
- Scope of evaluation
 - Network product evaluation (Product development process and Product Life cycle management process) is done as a part of vendor's accreditation process.
 - Security functional requirements compliance (both positive and negative testing) + Hardening (Both Hardware and Software)

3GPP Security Testing

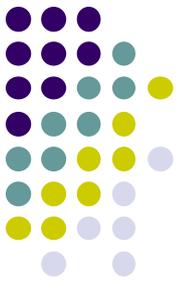


Legend:



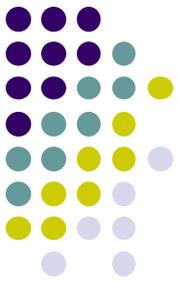
SECAM tasks	Accredited actor
Vendor network product development and network product lifecycle management process assurance compliance	Accredited vendor
Security compliance testing	Accredited vendor or accredited third-party evaluator
Basic Vulnerability Testing	Accredited vendor or accredited third-party evaluator
Enhanced Vulnerability Analysis	Accredited vendor or accredited third-party evaluator

Courtesy: 3GPP forum



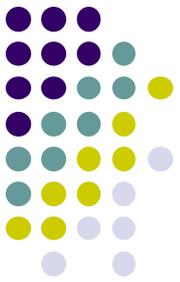
Types of Evaluation

- **Self declaration**
 - Declaration of security claims by Vendor
- **Self evaluation**
 - Assessment of product by vendor , vendor as accredited lab and performs product's evaluation
- **Third party evaluation**
 - Assessment of the product by an independent third-party, Third party has accredited evaluation lab performs evaluation
 - The evaluation lab assesses the product against defined criteria and produces an evaluation report
- **Certification**
 - Certification is the confirmation by an independent Certification Authority (CA) that the evaluation has been properly carried out



Methods of Security Testing

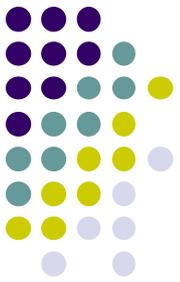
- **Black Box Testing**
 - No disclosure of Network diagrams, Source Code, IP addresses etc.
 - Pros (Less knowledge needed, tests system behavior)
 - Cons (Only identify symptoms not causes , High false negatives)
- **White Box Testing**
 - Disclosure of Source code etc.
 - Pros (More thorough, Evaluate system internals, Identify sources of potential vulnerabilities)
 - Cons (More skills required, High false positives)
- **Grey Box Testing**
 - Combines benefits of both methods



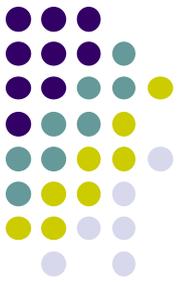
Roles in Security Assurance Process

- Evaluator
- Accreditation Body
- Certification Body
- Security specification /Standards making body
- Vendor
- Operator
- Licensor

Security Testing Lab Requirements – International Standards



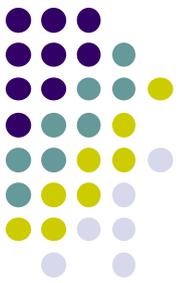
- ISO17025 (General requirements for the competence of testing and calibration laboratories)
- ISO 27001(Information Security Management System)
- ISO 17065 (Requirements for Bodies certifying products, processes and Services)
- ISO 15408
- 3GPP and 3GPP2
- ITU X.805
- FIPS 140-2 etc.



Scope of security Testing- Macro level

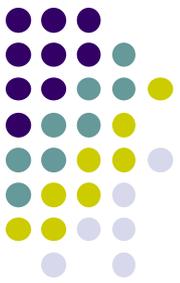
Testing aim to check

- Implementation errors (e.g., overflows)
- Design flaws (e.g., weak authentication)
- Configuration errors



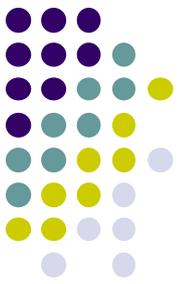
Scope of security Testing - Micro level

- Testing should address threats of Network and Network element
- Testing should ensure that Network elements should have inbuilt protection mechanism against DoS /DDoS attacks
- Testing should ensure that Network elements should be free from Reported /Published vulnerabilities in public domain
- Protocol fuzz testing assess the robustness of Protocols implementations of Network element and ensure that Network elements should be free from Zero day vulnerabilities
- Algorithm verification and its implementation robustness
- Software code analysis (static and dynamic) to check for coding related vulnerabilities i.e. Programming standards violations, Code review etc.



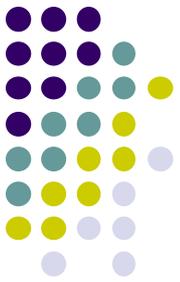
Scope of security Testing - Micro level view

- Testing should ensure that Firewall should be placed at the Network perimeter not to allow port scanning/ Vulnerability by attacker
- Testing should ensure that Network element must be up to date software patched
- Testing should ensure integrity of software image during transit
- Test to harden the Operating system / software applications to reduce the attack surface on network element
- Test the reverse engineering protocols / Binaries
- Testing should verify the Security Functional Requirements supported by Network element



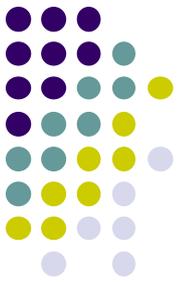
Security Testing Lab – Technical Man power

- Network administrators
- System administrators
- Penetration Testers
- Team member should have qualified network certifications
- Team member should be familiar with the network protocols
- Team member should be proficient in coding, reverse engineering, protocol analysis and exploit development
- Team member should be familiar with multiple languages such as C, C++, Python, Perl and assembler etc.
- Team members should be familiar with windows and non-Windows (such as Linux , Fedora) operating systems etc.



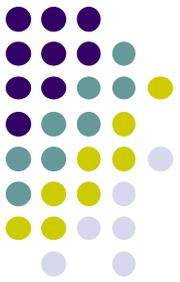
Tools required for Security Testing

- Network and Application Traffic generators
- Exploit Launching Programs
- Bad / Malware Traffic Generators
- DDOS(Distributed Denial of Service) Attack Traffic Generators
- Traffic Load Generators for TCP/IP, UDP etc
- Pass word cracking tools
- Random Password Generator



Tools required for Security Testing

- Network monitoring software
- Port Scanners
- Vulnerability Scanners
- Protocol fuzzer (Network and Application)
- Packet crafting tools
- Source Code Analyzers (Static and Dynamic)
- Reverse engineering protocol /binaries tool etc.



THANK YOU