TELECOM FRONTLINE
LATEST INFORMATION ON TELECOM INDIA

Telecom: The Next Step!

By: Govind Rammurthy MD & CEO eScan

The Indian telecom industry has witnessed significant growth comparable to global standards. With wireless telephony a little over a decade, old India has grown from a subscriber base of zero to becoming the second largest network provider in the world. More so, the Indian telecommunication industry continues to be one of the biggest success stories in the business world. With the overall growth mainly succeeding on the wireless revolution, this sector has been adding to the overall revenue generation by roping in close to 10 million subscribers per month.

Moreover, the Indian broadband is yet another sector that has been effectively growing over the years. With the growing demand of fixed broadband services among small and medium businesses and home users, the fixed line base is said to grow to approximately 40 million users by 2012. With that, the number of mobile internet subscribers is also said to grow from 76 million to 196 million.

The figures itself speak volumes of the trend at which the telecom industry is growing. Moreover, with the growing number of users, we are going to see a sharp increase in the number of wireless hotspots.

All said and done, there is always the risk of data theft especially when users connect to random access points or hotspots. The issue here lies in the security measures implemented by the providers – which could be in shopping malls, offices, etc. More often than not, the need for securing wireless hotspots is overlooked – thus leaving users open to a variety of web-based attacks. Man-in-the-Middle attacks are the most used in such scenarios.

Even with a secured Wi-Fi connection, what most fail to understand is the security level that is required. WPA and WPA-PSK based security is the most sort after security protocols used to secure ones connection. What people do not realize is the fact that this level of security can easily be hacked using brute force attack. Anything below WPA2-PSK is considered weak and insecure. This along with a 10-digit alphanumeric pass phrase is what needs to be used to prevent snoopers from gaining access to privilege data.

Data theft has almost become a routine affair amongst small and large companies. Take the instance of BPO companies – every second month we hear about employees selling user data for a fee.

The need to secure endpoints is something most companies need to look into; which could be anything from blocking of USB ports to Bluetooth to securing various other interconnected devices. It is these vital points that provide access to critical data. Overlooking security at these points can not only lead to a breach in data but can also help in spreading malware across the network; both equally potent in shutting down large and small companies (Telecom in this case).
While this has not hit the Indian telecom industry, yet there is always a chance for perpetrators to get their hands on user data. Now, imagine the damage telecom industry would face if even one percent of all listed data got into the wrong hands. It could be in the form of a hack or could be taken from any of the service provider outlets in the country. The question to ask is – are we taking the right steps to ensure user security? Or are we just playing it easy waiting for an incident to occur?

Take the instance of recent events (April 8, 2012) where the hacker group Anonymous claimed responsibility for leading denial-of-service attacks on USTelecom and TechAmerica. The companies affected include AT&T, Verizon, and CenturyLink, while members for TechAmerica include tech companies such as IBM, Microsoft and Apple. While both organizations denied breach of sensitive data, the attack itself should come as a wakeup call for most Telecoms.

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.

Firmware is the heart of the system for any Telecommunication Network to function at its optimum level. Any vulnerability discovered in these equipments need to be patched. In addition, due to the

sheer number of equipments, it is imperative for companies to ensure speedy updates and that the Firmware update files are verified before being applied.

With rising incidents of data breaches coupled with telecommunication equipments being targeted, it is imperative to ensure that the critical elements of the network are not vulnerable to these attacks.

Patch management for computers / mobile devices have reached a level, wherein patches for discovered vulnerabilities are applied in an automated manner and threat is mitigated. However, the same does not hold true for Consumer Premise Equipments (CPEs) / Telecommunications Equipments. Most of the CPEs are never patched due to lack of information to the concerned administrators and they are blissfully unaware about the flaws existing within their Telecom Equipments.

Very recently, we have seen instances about Wi-Fi devices being vulnerable to a specific flaw but due to non-existence of patch-download-apply and auto-notification features to the concerned end-users, these devices are at the mercy of hackers.

Firmware is the heart of the system for any Telecommunication Network to function at its optimum level