Dept of Computer Science, P B SIDDHARTHA COLLEGE OF ARTS & SCIENCE, VIJAYAWADA.
UGC SPONSORED NATIONAL SEMINAR ON "CYBER SECURITY WITH SPECIAL FOCUS ON CYBER CRIMES & CYBER LAWS (NSCS 2014)" on
15th & 16th November 2014-IJDCST SPECIAL ISSUE, PAPER –ID: IJDCST-21
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Today's Mobile Cybersecurity

K.Suneetha[1], D.V. Chandra Sekhar[2]

[1] P.G Department of Computer science, TJPS college,Guntur, sunitha680.poluri@gmail.com

[2]Department of Computer science, TJPS college,Guntur, chand.info@gmail.com

ABSTRACT: Delivering advanced Cyber-Security in mobile communications may sound simple, but the reality is a complex, constantly evolving undertaking. The Cyber-threat landscape changes literally by the hour and requires constant vigilance and innovation throughout the entire mobile industry - an industry that provides 3.8 million direct and indirect jobs across the nation. It is a constant risk to be managed, where opposing forces must constantly adapt their strategies and tactics to keep the advantage. Today's mobile Cyber-Security protections must be flexible and adaptable in the face of increasingly sophisticated and persistent global threats. Staying ahead of Cyber-threats is far too big of a job for a go-it-alone approach, so the company members of CTIA-The Wireless Association are working together to deliver real-world solutions driven by these market forces.

Keywords: Cyber-Network, Security, threat, Firewall

INTRODUCTION

Wireless communications players invest hundreds of millions of dollars to enhance the security of their networks, software, hardware and devices. This means carriers, manufacturers, applications providers, operating system and platform providers, among others, pursue unified efforts in addition to independent investments. All share an economic interest in delivering effective Cyber-Security and ensuring the entire interdependent mobile ecosystem delivers sustained, high-value security for all users.

Work Focused on :

- A brief overview of the Cyber-Security landscape of the mobile communications industry,
- The extent of its interdependence in responding to an environment of rapidly changing threats,
- A summary of the many Cyber-Security features and solutions at work today, and
- A sampling of the many advanced protections available for device users.

Security is only as good as the weakest link. In addition to the efforts of the mobile industry, Cyber-Security depends on the awareness and daily security practices of consumers and end users across business and government enterprises. Policymakers also play a vital role in working collaboratively with the industry to encourage and maintain a flexible framework that balances the needs of stakeholders while preserving the industry's

ability to stay ahead of cybercriminals and hackers. Everyone has a stake in maintaining effective Cyber-Security across the nation's mobile communications system. There is great value in policymakers, government entities and the wireless industry working collaboratively on maintaining the strongest and most resilient. The wireless industry looks to policymakers for a flexible and collaborative framework, where industry provides policymakers a "view from the trenches" from the individuals and entities that are fighting the battle every day. The ability to share information about

Cyber-Threats and effective countermeasures among industry.The mobile industry is in the best position to respond to the changing threats as demonstrated by the set of mobile Cyber-Security solutions available today and outlined in this paper. Continued flexibility, dynamic and responsive countermeasures from the industry are essential going forward to stay one step ahead of the cybercriminals, hackers and hacktivists that target mobile communications .

Goal of Cyber-Security

Security is only as good as the weakest link. In addition to the efforts of the mobile industry, Cyber-Security depends on the awareness and daily security practices of consumers and end users across business and government enterprises. Policymakers also play a vital role in working collaboratively with the industry to encourage and maintain a flexible framework that balances the needs of stakeholders while preserving the industry's

ability to stay ahead of cybercriminals and hackers. Everyone has a stake in aintaining effective Cyber-Security across the nation's mobile communications system. There is great value in policymakers, government entities and the wireless industry working collaboratively on maintaining the strongest and most resilient Cyber-Security posture possible. The wireless industry looks to policymakers for a flexible and collaborative framework, where industry provides policymakers a "view from the trenches" from the individuals and entities that are fighting the battle every day. The ability to share information about Cyber-Threats and effective countermeasures among industry players and between industry and government is crucial, as is promoting such information sharing with effective industry liability protections. The mobile industry is in the best position to respond to the changing threats as demonstrated by the set of mobile Cyber-Security solutions available today and outlined in this paper. Continued flexibility, dynamic and responsive countermeasures from the industry are essential going forward to stay one step ahead of the cybercriminals, hackers and hacktivists that target mobile Communications.

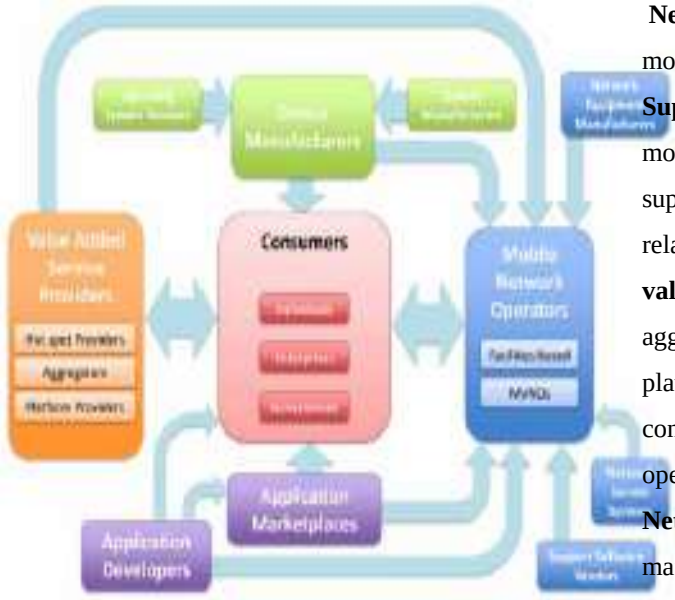
Components of Wireless Technolgy

Although mobile communications have changed our world in so many ways, most of us take it for granted. Mobile communications and computing for most of us means a cellphone, smartphone or tablet, and it just "works." It is a convenient tool for personal and business communications that is as indispensible as it is ubiquitous.

However, there is one critical element of this magic where a lack of basic understanding of how mobile networks work is a problem —Cyber-Security. Indeed online privacy and Cyber-Security go hand-in-hand since one cannot have privacy without security. Though not well understood by the public, mobile network operators (MNOs) have been focused on Cyber-Security since the earliest days of cellular communications. As a result, the key components for protecting cellular networks are well established, and form the backbone of the communications systems we rely on today. The central idea behind protecting networks is to safeguard the elements that transport information and services, including the voice, data and video transmissions that are translated into packets of information. This Cyber-Security backbone that MNOs provide, including network protection as well as security policies .

Frame Work of Proposed System

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)



Cconsumers – Generally individuals drawn from the public and employees of enterprises or government agencies that use mobile devices.

Mobile Network Operators – Both facilities based and virtual network operators that render mobile services to consumers.

Device manufacturers – Entities that develop and manufacture mobile devices that have the ability to access networks that are provided by mobile network operators.

applications marketplaces – Generally available virtual marketplace that provides for the download of applications to mobile devices, including Web applications and native applications.

application Developers – Entities that develop applications and make them available through the applications marketplace or through the mobile network operators, often in an over-the-top (OTT) scenario.

Operating System vendors – Entities that offer mobile operating systems on mobile devices.

chipset manufacturers – Entities that develop and manufacture mobile device integrated circuits.

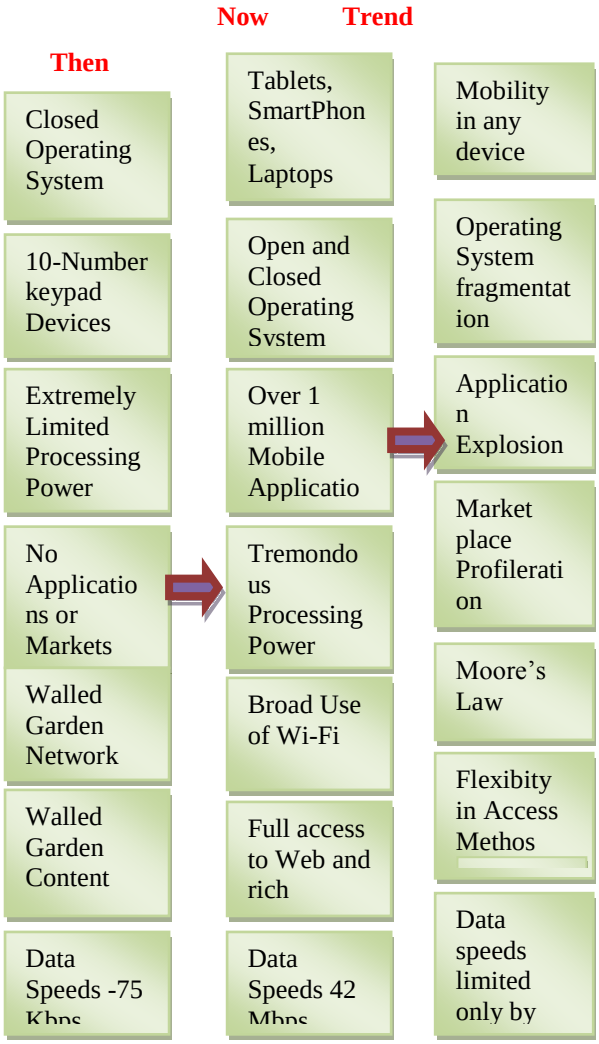
Network Service Systems – Entities that render mobile network related services to mobile operators.

Support Software vendors – Entities that provide mobile network support software such as operational support systems, back-office systems and other related software.

value added Service Providers – Service aggregators, Wi-Fi hot spot providers and other platform providers that can render services to consumers directly or through the mobile network operator, often in an OTT scenario.

Network Equipment manufacturers – Entities that manufacture network equipment such as mobile base stations, network routers, switching center infrastructure, transmission infrastructure and other network While growing more complex and remaining a relatively open technology ecosystem, mobile communication are becoming an increasingly attractive target for attackers. As a result, there can be no single fix or single point for delivering Cyber-Security. It is not possible to say, "If only the carriers could do X, or the equipment makers would do Y or the applications providers would do Z, we would be safe and be 100 percent secure." There is no "silver bullet" solution, regardless of how much money, expertise or effort is dedicated to the Cyber-Security challenge. The futility of a single fix is illustrated in the diagram below, depicting just a few of the major changes in the mobile environment within the last five years. Today, cyber risks can only be successfully managed via constantly evolving collaboration, innovation and partnerships between the many players in the mobile ecosystem, including consumers.

New Trends in Mobile Environment



The mobile ecosystem is important, it is also necessary to understand the players and how they interact within the ecosystem.

These players include all of the organizations that bring together the chain of technology assets or "system of systems" that make mobile communications possible.

Five Stones of Mobile Cyber-Security

we explore each of the five segments, the threat landscape and the proactive steps the mobile industry is taking to address the threats through solutions available

today. Following this, we outline the Cyber-Security industry solutions available today in the section on Solutions from Industry.

1.Consumers and End Users

Industry is working hard, and with growing success, to educate users on how to reduce their Cyber-Security risks. Best practices that the industry recommends for consumers to become security savvy include:

configure Devices to Be more Secure – Smartphones and other mobile devices have password features that lock the devices on a scheduled basis. After a predetermined period of time of inactivity (e.g., one minute, two minutes, etc.) the device requires the correct PIN or password to be entered. Encryption, remote-wipe capabilities and - depending on the operating system - anti-virus software may also serve to improve security.

check Permissions – Check the access (i.e., access to which segments of your mobile device) that an application requires, including Web-based applications, browsers and native applications

2.Devices

Today's mobile devices are miniature computers. In addition to these truly "smart" phones, there is a growing variety of devices such as tablets and netbook computers that include wireless connectivity. These new mobile devices are more

advanced than those sold even five years ago. All computers, including mobile devices, need to be secured to prevent intrusion. Applications downloaded from questionable, or even legitimate sites, can record information typed onto the device (e.g., bank account numbers, passwords and PINs), read data stored on the device (including emails, attachments, text messages, credit card numbers and login/password combinations to corporate intranets); and record conversations (not only telephone calls) within earshot of the phone.

3. Network based policies

From a consumer perspective, network operators provide a wealth of tools that can be used to provide improved security and data protection for information that resides on the smart phone or tablet. Such tools include device management capabilities, firewalls and

other network-based functionality. These tools give consumers the power to protect their information but network service providers cannot dictate security policies for consumers to follow. However, service providers provide a wealth of consumer educational materials of security problem

4.Authentication and control

Authentication is the mechanism that requires the user to enter credentials based on such things as a password or PIN, and, in the case of an enterprise, based on the organization's policy settings and active directory database. In some instances, multi-factor

authentication is used to protect very Sensitive data, comprising two or more of the following classic requirements:

- Something the user knows (PIN, password, secret)
- Something the user has (physical token, smartcard, mobile device)
- Something the user is (biometric data such as a fingerprint, retina

  scan or photo recognition)

As an example, this is especially helpful for anyone who wants to access banking information on a website using an unsecured terminal location, such as at a coffee shop with a Wi-Fi hot spot.

5. The cloud Networks and Services

The Cloud allows public and private sector consumers to use applications and information in a remote data center, where large clusters of systems work in parallel to process and store data. Consumers directly access cloud services over the Internet.

The complex security solutions that the industry provides in the figure shown on page 10 (Five Cornerstones of Mobile Cybersecurity) encompass multiple types of network hosting and transmission points, including data centers. Data centers are a core element of the Internet backbone, as they host the web pages and web-enabled software/applications that consumers utilize when they access the Internet through the multitude of network options available in the marketplace. Data center operators are responsible for the management and security of both physical and virtual assets, as well as the implementation of organizational security and compliance policies.

internet Backbone — The Internet backbone is comprised of the principal data routes between large telecommunications networks and core routers. These data routes are operated by a mix of primarily commercial (i.e., private sector) operators, and for certain purposes, government agencies and academic institutions. In the private sector, Internet services providers (ISPs) deliver Internet exchange traffic (i.e., email and Web content) via privately negotiated interconnection agreements.

core Network — The core network forms a "bridge" between the Internet backbone and the next step in the chain, access networks. One of the main functions of core networks is to route phone calls across the public switched telephone network (PSTN). Among the technologies used in core and backbone facilities are data link layer and network layer technologies.

access Network — The access network connects users to their immediate service provider. The access network refers to the series of wires, cables and equipment lying between the point at which telephoneconnection reaches the customer and the local telephone exchange

Cyber-Security for Various Organisations

While the industry has done a great deal to secure its services, it has also heavily invested in solutions that offer protection and security for consumers and enterprises. These solutions are generally available throughout the mobile ecosystem and, as described below, offer a more complete picture of what is available today. The industry also works to educate consumers about the available solutions as evidenced by the CTIA Cyber -Safety Tips in the Appendix. The solutions offer protections that consumers can avail themselves of based on their unique needs and requirements

- **Lost or Stolen Smartphone Database**
- **Password Mobile Device Lock**
- **Remote lock of Mobile Device**
- **Remote Wipe of Mobile Device**
- **Anti-Malware/Anti-Virus Software**
- **MDM Policy Management**
- **Encryption Data at Rest**
- **Encription Data in Transit**
- **VPNs**
- **Secure Email Solutions**
- **Parental Controls**
- **Secure Applications**
- **Cloud Based Services and Secure**
- **BYOD Solutions**
- **Authentication and Identity**
- **Management**

Conclusion

Effective Cyber-Security, whether for a nation, business, organization or individual is the result of a partnership between the entity being protected and those in the industry that makes mobile communications possible. All of the participants, from the consumer to the manufacturers, carriers, applications developers, software providers, etc. have a role to play. At every step of the process, there is a shared responsibility for making

Cyber-Security a priority. While achieving political consensus is always a challenge, there appears to be a widespread understanding among policymakers that a single legislative "fix" for Cyber-Security does not exist; therefore, a flexible approach to legislation in the wireless arena is necessary. The threat landscape is, by definition, a non-static one. Enabling Cyber-Security, as a result, cannot be achieved by following a set list of mandated criteria. Cyber-Security threats and vulnerabilities can change from day to day, and even hour to hour. The effective steps for managing cyber risks today are unlikely to suffice for very long. Maintaining security in a wireless environment is a constantly evolving dynamic.

However, policymakers play an important role in Cyber-Security. Policy efforts that are informed by the realities of the Cyber-Security atmosphere — no silver bullet, no single fix, many moving parts and all of them interdependent — are a must. Similarly, policies that seek quick-fixes, one-size-fits-all outcomes or so-called solutions that restrict the

flexibility that the wireless industry requires to respond quickly to new and emerging security challenges can cause unintended harm to the very businesses, consumers and institutions it seeks to assist. Cyber-Security posture in a fashion that is flexible and adaptive to the changing threat environment.

References

1. http:// csrc.nist.gov/publications (NIST, Computer Security Resource Center)

2.http://www.drizzle.com/~aboba/IEEE/ (Unofficial 802.11 security Web site)

3.http://its.med.yale.edu/computing_services.html (Yale University School of Medicine provides information on wireless applications and future uses)

4.http://xforce.iss.net (X-Force Web site provides information on leading computer threats and vulnerabilities)

5.http:/whttpww.cisco.com (Cisco Web site provides information on securing wireless networks)

6.http://computeruser.com/resources/dictionary/dictionary.html (reference for technical terms)

7.http://www.computerworld.com (provides white papers, surveys, and reports related to security of wireless networks)

8. http:// www.eet.com (technical Web site that serves as a primer for different technologies and applications)

9.http://www.gcn.com (Government Computer News provides up-to-date information on wireless and mobile devices and their related security issues)

10.http://www.informationweek.com (provides information on wireless networks, wireless communications, and security solutions in the form of articles and other documents)

11. http://www.infosecuritymagazine.com (provides white papers, surveys, and reports on wireless network security)

12.http://.isaac.cs.berkeley.edu/isaac/wep-faq.html (University of California at Berkeley provides "frequently asked questions" on WEP setup, problems, and attacks)

13.http://www.networkcomputing.com (provides white papers, surveys, and reports on wireless network security)

14.http://www.nwfusion.com (Network World Fusion Web site provides white papers, surveys, and reports on wireless network security)

15.http://www.scmagazine.com(SCMagazine Web site, an information security online magazine provides information on wireless security issues)

16.http://www.zdnetindia.com (ZDNet India Magazine Web site provides white papers, surveys, and reports on wireless network security)