ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

A Survey on Current Cyber Threats, Their Issues and Solutions

Lakshmi Shree K, N Ankit Kumar, Aayushi Sharma

Asst. Professor, Dept. of Computer Science and Engineering, Jain University, Kanakapura , Bangalore , India

Student, Dept. of Computer Science and Engineering, Jain University, Kanakapura , Bangalore , India

Student, Dept. of Computer Science and Engineering, Jain University, Kanakapura , Bangalore , India

ABSTRACT: In the era of high end application ,communication among people across the world to acquire instant data at any point and any where is a huge achievement . With these facilities users are also facing problems with the threats in all the application. In this paper we attempt to review various issues of cyber threats which users face in the applications and also suggest various solutions to these threats. We also guide the users with techniques and commercial solutions to each threat.

KEYWORDS*:* Malware ; Virus; Online threat ; Security ; hacking

I. INTRODUCTION

Cyber security is a domain which consists ofvarious practices designed to enhance the protection of programs and data from attack. The area enhances to check on unauthorised access and operates on a systematic basis where users, services providers and commercial or social outlets come together and share a virtual interaction within a platform in order to execute transactions. The major loophole of this virtual interaction is that there is no formal policing and no common laws of cyber space. As a result the norms and conducts are easily deceived and exploited making the cyber world more susceptible to socio-technical vulnerabilities.

Online network has become an essential platform for social interactions and virtual transaction. Social networking sites such as Facebook,LinkedIn, MySpace,whatsapp have threat issues like privacy violations,identity theft ,social bots and sexual harassments etc.Virtual transactions such as online shopping, online bill payments have become associated with people's day-to-day life. Unfortunately, a large fraction of these users are uninformed about the various threats such as online scams, phishing, password theft,session hijacking etc. that exists in these types of transactions. Our aim in this paper is to highlight the threats , create a awareness about all these areas to users who use the current technology in their day to day lives.
In this survey paper we highlight about various categories of cyber threats such as social networking, online transactions ,Wi-Fi threats, cloud computing threats ,mobile malware ,vehicle hacking, software cracking in the section II, in section III we identify the solutions and in section IV the commercial recommendations for the threats. This paper also provides an interesting insights to some very rare and new emerging technologies: vehicle hacking

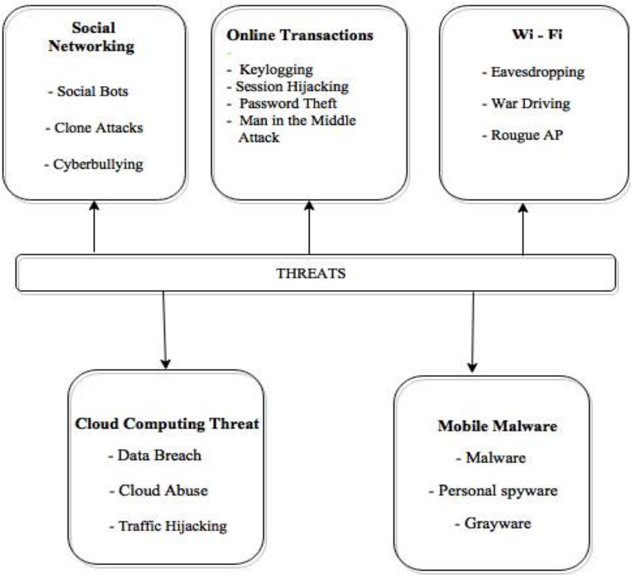
Wi-Fi has become a fundamental part of our lives. Irrespective of the locations like office, home or any other institution we are connected to a Wi-Fi network. The major underlying problem is users are not aware of the security & their potential implications when they connect to new networks.The common threats in using Wi-Fi networks are data interception,war driving,rouge app,eavesdropping,denial of service, wireless intruders and the list continues with many more such harms. Cloud computing is a kind of internet based computing that provides shared processing resources to computer and other devices on demand. This is one of the most recent emerging trend. Some major threats in cloud computing: data breaches,service traffic hijacking, insecure API's,session riding etc.

DOI: 10.15680/IJIRCCE.2016. 0408127

II. CYBER THREATS

With the growing usage of cyber technologies many users are still unaware of the threats and risks that they are being exposed to on account of their security and privacy.

We have discussed briefly 5 categories of threats as shown in the figure 1.



.

Figure 1: Various Threats and its categories

III. THREATS CLASSIFICATION

A.Social networking threats

With the growing and expanding usage of online social networking day-by-day ,users have become more vulnerable to various threats .We have addressed four sub categories of social networking threats .

a. Social Bots

Also known as fake profiles or sybils which gathers user's personal data by watching users interactions with peers in networks sites such as facebook and twitter. On monitoring users fake profiles are created , friend requests are initiated , spam messages are published , can also manipulate victim's statistics can create damage to his/her profile.

b. Clickjacking

Users become victim's of clickjacking when users clicks certain links/buttons user assumes to navigate to genuine page but the user would have executed the embedded code or a script without user's knowledge and thereby victimised . The victim's system and confidential information is captured. Some common examples of clickjacking are i) clicking goggle adsense ads to generate pay per click revenue ii) downloading and running a malware unknowingly.

c. Identity clone attacks

User identity is cloned / duplicated in social networking site and further can send friend requests ,deceive victim's friends to gain their trust and collect victims details. Identity cloning is a rare form of identity theft. using this technique ,the attackers duplicate (clone) the victim's online presence and use it to deceive victim's friends to gain their trust. The attackers further use this trust to collect personal info about the user or to perform various types of online frauds.

d. Cyberbullying / Cyber abuse

A user becomes a victim by receiving repeated harassing messages, sexual remarks, publish embarrassing pictures via emails , chats, phone conversations. Usually victims are children rather than adults. Adults should play a role to make their kids aware and educate them rightly.

Classic Threats	**Modern Threats**	**Threats Targeting Children**
□ Malware □ Phishing Attacks □ Spammers □ Cross-Site Scripting □ Internet Fraud	□ Click Jacking □ De-anonymization □ Face Recognition □ Fake Profiles □ Identity Clone Attacks □ Information Leakage □ Location Leakage □ Socware	□ Online predators □ Risky Behaviour □ Cyber bullying

Table 1 : Types of social networking Threats

B. Online transaction threats

Users across the world rely on online for processing any of the tasks instantly. With the number of user's usage attackers are exploring to attack and take benefits. Some threats encountered in online transaction processing are:

a. Password Theft

For every transaction user will have to create login user name and a password as a preliminary step, after which the respective transaction gets processed. Attackers capture passwords and user data from one site , attempt to hack other sites also. This attack becomes harmful to users especially when bank related data / personal information is stolen.

b. Man-in-the-middle attacks (MiM)

As the name suggests here the attacker attempts to gain the data which is sent between two users. To illustrate this attacker 'B' participate in a conversation between two other machines 'A' & 'C' ensures all the IP packets to pass through B's interface once the attacker is successful attacker inject messages, alter the messages, distributing malware between these users, redirect users to fake sites and so on.

c. Session hijacking/ cookie hijacking

When users communicate with each other a session is created. During that particular session users exchange packets , a hacker attempts to hijack such session and attempts to gain unauthorized access to information or services in a computer system using source-routed IP packets method.

d. Key logging/ keystroke logging

A attacker records all the actions performed by the keyboards on a system by installing Key loggers.

C. Wireless security

With the evolution of internet from wired to wireless to support user’s mobility wireless networks has become increasingly popular .The medium for transferring data is via radio waves spreading throughout the space thereby information exchanged between users has higher chances of reaching the unauthorized .Some common threats in wireless transmission mechanism are

a. Eavesdropping

A process where in a intruder attempts to intrude a private communication. The types of eavesdropping can be either passive or active.

- Passive eavesdropping the intruder just gathers all the information exchanged between the users and later this information is being used for some dangerous activities.
- Active eavesdropping the attackeris able to modify the information exchanged and may also inject his own data into the conversion.

b. War driving

Is an exploitation method wherein special hardware and software is utilized for mapping approximate locations of discovered wireless APs within a specific geographic area.

Defined as the act of moving around a specific area and mapping the population of wireless access points for statistical purposes. Vistumbler is a well known open source program for War Driving.

c. Rougue AP

Attackers install accesspoints called as a *rougue access point in a* secure network without the knowledge of users and local network administrator. Later attackers can check for vulnerable points by running vulnerability scanners.

C1) Wi-Fi Security Threats

A wireless local area network is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. In 1997, IEEE 802.11 was implemented as the first WLAN standard based on radio technology. *Wlan Security Threats-*

a.   Information Disclosure (Attack on WEP)

Wired Equivalent Privacy (WEP) is an encryption algorithm called "RC4" which generates a key which is XORed with the plaintext to form cipher text. And is said to be easily vulnerable to attacks due to this usage of XOR operation, small IV and short RC4 encryption key.

b .Signalinterference

When the wireless router is next to an operating device and wireless Access Point and the base station is over the same channel communications gets affected when may receive a signal because of the confusion. If there are more obstacles between the wireless base station and AP, it can lead to reduced access rate or disconnected. Also, when there are multiple wireless routers working simultaneously in the same frequency transmit the signal, then also it causes interference.

D. Mobile Malware

Mobiles have been evolved drastically especially the smart phones which provides all applications browsing, social networking, online banking and many more. With this improvement in the technology they have also been a target for malicious activities.

a. Malware

Various malware that affects the systems can classified as

- Virus – A piece of code that can replicate itself.

- Worm – A program that makes copies of itself and consumes the bandwidth, damages the phone.
- Rootkits – Infects the phone OS and also hide malicious user-space processes and files.
- Botnet – An attacker takes the control of the systems and controls them remotely

Few mobiles threats identified are Malware, personal spyware & gray ware.

Malware is a distributing as a spam which is a kind of hostile, intrusive, or annoying software or program code whose main intention is to use to affect the users system. Without the owner’s consent it is present within a malicious attachment or when a user clicks on some link in an infected websites.

- Wireless Attacks: eavesdropping on wireless transmissions to extract confidential information, such as usernames and passwords.
- Break-in Attacks: Attacker exploits the device and controls the system and cause programming errors.
- Infrastructure-based – Attackers attack sensitive areas such mobile stations , internet , the interface between the mobile and SGSN (Serving GPRS Support Node) of the service providers like GPRS , UMTS.
- Botnets – Attackers create botnet to gain the control.
- User as an Attack Vector - A user are being if when are not having technical knowledge of the security.

Detecting malware on Android smart phones system metrics, such as CPU consumption, number of sent packets, number of running processes. *Virusmeter* performs malware detection to monitor the power consumption under normal mode with calls ,SMS.

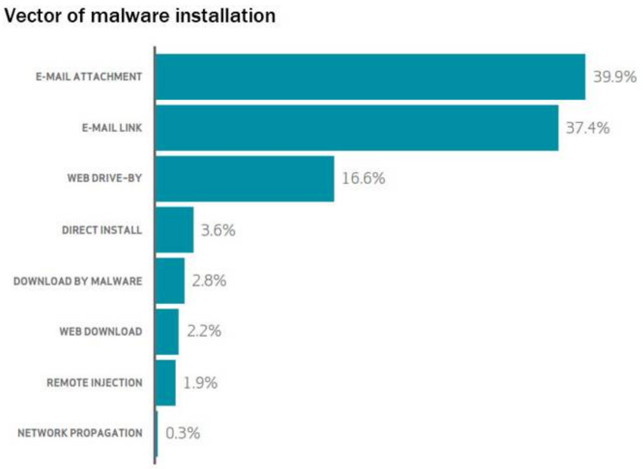


Figure 2: Shows a survey of various malware installed

a. *Personal spyware*

Every phone has personal data like the calls/messages histories, photos, contacts which is personal and users would not like to share with others. Attackers can install malicious software such as personal spyware and the user is victimized and all the phone activities are being monitored.

b. *Grayware*

As Users browse for products , sites visited , the transactions , search in the search tab is captures to analyze the users functionality , likes, dislikes and so on. The gray-ware spy ‘s on all these activities and utilizes all these data and distributes among firms which require it for marketing or analysis for their product rates.

c. *Headless worms*

One of the biggest threats of 2016. Worms are define as standalone malware programs that replicates itself to other systems. These worms are headless, said to be more dangerous and causes more damage than the normal worms . The malicious codes will target headless devices like smart watches , Smartphone’s and medical hardware. The damage caused by headless worms is more than caused by the normal worms.

d. keystroke logging /key logging techniques to detect anomalies to track the keys struck on a keyboard to monitor the actions of the user.

E. Cloud Computing Security

To increase data storage and decrease the resources usage firms have transferred their data to cloud and with this the challenge to provide security has also increased .The security concerns associated with cloud computing can be categorized as issues faced by the cloud providers and security issue faced by the customers.

Some of the cloud security threats are

a. Data Breach

As users import/ export/ store the data like credit cards , bank details ,personal information , trade secrets of corporations there might be few cases where these data are intentionally or unintentionally released to un trusted environment is done.

b. Cloud Abuse

A cloud computing environment has relatively weak registration systems welcoming spammers, hackers and other criminals to use the cloud services and also launch cloud services. Example of such attacks includes: password and key cracking, DDOS, malicious data hosting, building rainbow tables etc.

c. Traffic Hijacking

Attackers pretends to be genuine customers of the cloud and hijack the traffic performing illegal activities such as eavesdropping other clients data and further manipulate, gain access clients credentials , return falsified information, redirect the users to illegitimate sites and so on.

F. *Some Emerging Threats*

Vehicle hacking-Vehicles in the highways is progressing to the next level by connecting to other vehicles , to the local server and to the built in sub modules which holds variety of driving functions and other enhanced features. Numerous control systems present internally exchange data among themselves, to the drivers display screen and among other moving vehicles and objects like (street lights, hoardings). Vehicle hacking is a process of manipulation of code in car’s electronic control unit (ECU) to exploit the vulnerabilities and gain access of other ECUs as well. Hackers focus to gain control of various sub components such as speedo meter, air bags, accelerometers etc.

Threats for vehicles are

- Online automotive apps and services being accessed also for user’s names and passwords.
- Obtaining the details such as insurance, tax data, License numbers which is useful for thefts can be misused.
- Vehicle location information which may be used to identify patterns of use or driver behaviour in anticipation of offensive action against a vehicle.
- Data theft - Physical data exchanged between sub modules with congestion free.
- Extortion / denial-of-service threat
- Fraud and deception (altering or deleting schedule logs and records)
- Freight and goods theft (activating false alarms that cause goods to be left unattended)
- Automotive ‘Hacktivism’ – cyber infiltration of a vehicle’s systems that is politically or ideologically motivated.
- Immobilisation - Mischief and malevolence – individual hackers testing defences and their skills; or wanting to inflict damage and/or disruption out of spite.

IV. SOLUTIONS AND RECOMMENDATIONS FOR THE THREATS

A. Social Networking Solutions

Few identified are solutions[1,2] are

- CloneSpotter which can be deployed into the OSN infrastructure and can detect cloning attacks by using users’ data records, such as a user’s login IP records that are available to the OSN operator.

□ Sybil Infer defence algorithm which can distinguish between “honest” and “dishonest” users - Cloned Profile Detection

□ Using of Different types machine learning algorithms , honey pots for Spammer Detection:

□ Improving Privacy Setting Interfaces: Users of social networking must be aware and privacy setting with the flexibility to change the visibility of details such as personal, official, restrict unknown users to check profiles.

□ Facebook Immune System (FIS) – Is a learning system of Face book which performs realtime checks by protecting users from malicious attacks and collecting information

□ Use various configurable user privacy settings that enable users to protect their personal data from other users or applications

□ Use Authentication Mechanisms: such as CAPTCHA, photos-of-friends identification , multi-factor authentication like government issued ID ‘s .

B . Solutions Online Transactions

From [3][4] we were able to brief few of the recommendations for the online transactions as shown in the list below. i) Shop at Secure Web Sites ensures users use encryption technology to transfer information from your computer to the online merchant's computer. ii) Research the Web Site before You Order – Enquire with business address, phone numbers by calling. Increase awareness in employee and customers conduct awareness by training sessions, educating about security policy[5].

OPERATOR SOLUTIONS	COMMERCIAL SOLUTIONS	ACADEMIC SOLUTIONS
- Authentication Mechanisms - Security and Privacy Settings - Internal Protection Mechanism - Report Users	- Internet Security Solutions - AVG PrivacyFix - FB Phishing Protector - Norton Safe Web - McAfee Social Protection - MyPermissions - NoScript	- Improving Privacy Settings - Phishing Detection - Spammer Detection - Cloned Profile Detection - Fake Profile Detection

Table 2 - Solution and Recommendations for the threats

Shop at Secure Web Sites
□ Research the Web Site before You Order
□ Read the Web Site's Privacy and Security Policies
□ Be Aware of Cookies and Behavioral Marketing
□ Use of credit card for shopping its the safest way
□ Disclose Only the Bare Facts When You Order
□ Don't Fall for "Phishing" Messages
□ Always Print or Save Copies of Your Order
□ Learn the Merchant's Cancellation, Return and Complaint-Handling Policies
□ Understand Your Responsibility for Sales and Use Taxes Online

Table 3 - List of Recommendations for Online Transactions[4]

E-Commerce security tools [4]

□ Firewalls – Software and Hardware
□ Public Key infrastructure
□ Encryption software
□ Digital certificates
□ Digital Signatures
□ Biometrics – retinal scan, fingerprints, voice etc
□ Passwords
□ Locks and bars – network operations centers

TRANSACTION PHASE	SECURITY MEASURES
Information Phase	□ confidentiality □ integrity check □ access control
Negotiation Phase	□ secure contract □ identification □ digital signatures
Payment Phase	□ encryption
Delivery Phase	□ securedelivery □ integrity checks

Table 4: Security measures in different phases of Ecommerce Transaction.

Keyloggers can be detected in following ways:

□ Antivirus can scan and detect a key logger on your system.
□ Hard discs should be scanned regularly for any recent logs.
□ Programs like spybot search should be run on your system to check key logging of certain types.
□User's awareness is required whenever a file is downloaded from unknown sources.

C.Solutions for Wireless Security

In [8] authors discuss that the usage of user authentication and data encryption solutions results in high latency and overhead. There must be the upper-layer security algorithms, including the identity authentication, key generation and so on. Artificial noise generation techniques provide security at physical-layer against eavesdropping attacks. In this method only the eavesdropping attackers will be affected by the artificial noise, while the legitimate receiver is unaffected. The authors have demonstrated war driving in 3 cities in rural, suburban and urban environments and a compare both residential and commercial wireless security. The results show that the wireless security is enforced more in commercial environments rather residential environments. And the solution is to have encryption enabled in open networks.

Few Other Solutions are:

- Beamforming approach – When a legitimate transmitter sends data/ information signal in a particular direction to a legitimate receiver the receiver obtains constructive interference if an eavesdropper attempts to receive the signal a destructive interference is obtained.
- Usage of CSIs of the main channel and/or the wiretap channel ensures protection against the attacks performed by a eavesdropper in wireless physical-layer security.
- There should some technique to have random key generations instead of having the fixed keys at the Physical-layer and also support the agreement related details.
- Use techniques which combine FHSS with physical-layer security.
- Organizations should install wireless intrusion prevention systems to monitor radio spectrum for unauthorized access points in order to prevent the installation of rougue AP’s.

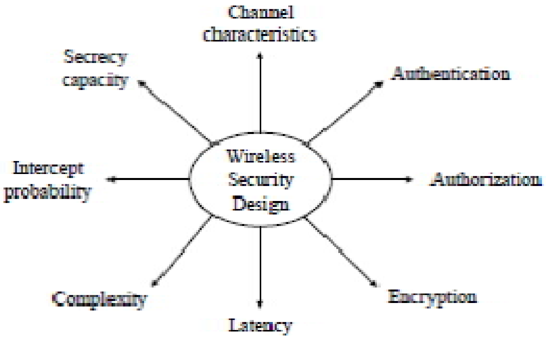


Figure 3 - Wireless security methodologies and design factors

In figure (4) authors of [6] have highlighted the attacks affected at each layer of the OSI model.

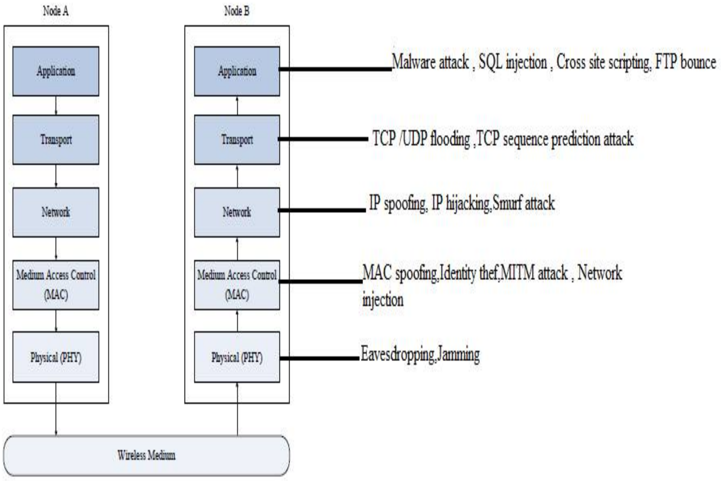

Node A
Node B
Application
Transport
Network
Medium Access Control (MAC)
Physical (PHY)
Application
Transport
Network
Medium Access Control (MAC)
Physical (PHY)
Malware attack , SQL injection , Cross site scripting, FTP bounce
TCP /UDP flooding ,TCP sequence prediction attack
IP spoofing, IP hijacking,Smurf attack
MAC spoofing,Identity thef,MITM attack , Network injection
Eavesdropping,Jamming
Wireless Medium

Figure 4 – The types of wireless attacks at various layers of OSI

C1. Solution for WLAN

In order to prevent and protect against these attacks, several security techniques and protocols have been introduced in [7].

WEP protocol – WEP (wired equivalent privacy) protocol standard for the protection of WLAN networks provide data security in wireless networks using shared secret key.

The key factors in a wireless security network

a. Authentication **-** It is the procedure used to confirm identity of the participants in the channel.

As per IEEE 802.11 specification, there are 2 types of authentications:

i) Open System Authentication - Allows unauthorized
access as its sensitive. Enables mobile stations to access the access point without confirmation of the station's identity.

ii) Shared-key Authentication - It is based on encryption
and decryption technique on the sender and receiver side respectively. Users will have to answer few query's if successful the access point is enabled also the access point should decrypt the station's answer by shared key.

b. Confidentiality and Integrity is supported WEP protocol.

Wi-Fi Protected Access

WPA security protocol operates in two modes -

a. Personal mode - use of pre-shared key (PSK) for authentication uses an encryption method called as Temporal Key Integrity Protocol - a WEP patch with three new elements: message integrity code (MIC) ,packet sequencing procedure and per packet key mixing function.
b. Enterprise mode - works on IEEE 802.1x protocol and EAP for mutual authentication.

Some of the Practical Solutions to WLan Security [9]

1. Never set SSID to default .
2. Utilize VPN - authenticates users coming from an untrusted space and encrypts their communication. A wireless Access Point is very secure behind a VPN server without any overloads.
3.Use static IP address and disable Dynamic Host Configuration Protocol (DHCP) as it does not differentiate a legitimate user from a hacker. Place the WLAN access point outside the firewall to protect from intruders.
4. Minimize radio wave propagation for non-user areas such as parking lots, lobbies thus restrict intruder in participating in wireless LAN.
5. Set and Enforce WLAN Policies forbid unauthorized access points, ad hoc networks and reconfiguration of access points/WLAN cards.
6. Monitor the network and network resources techniques such as protocol analysis, statistical anomaly for timely intrusion detection and for prevention methods.
7. Use of Encryption and Decryption Technology.
8. Use of Firewall Technology.
9. Don't Access Public Hot Spots.

D. Solutions for Mobiles

In mobiles to overcome the threats approaches[11] such as intrusion detection system(IDS) is employed. (IDS) constitutes of two complementary approaches such as

a. Prevention-based approaches: such as digital signatures,
hash functions.

b. Detection-based approaches: A defensive act to identify
malicious activities.

This approach includes

i) Anomaly Detection - An anomaly detection compares the "normal" behavior with the real one. The solutions included in this section are either monitor distinct activities on the mobile, e.g. SMS or MMS services or Bluetooth connections, or analyze the power consumption model of the phone to detect anomalies. Moreover, we detail frameworks that adopt run-time monitoring of the activities. We can split the architecture of a generic Smartphone in the layers such as user, application, virtual machine or guest OS, hypervisor, physical. For each functional layer, the authors propose several distinct features that should be collected for measuring the phone's behavior and used by an anomaly detection IDS. Anomaly-based approaches for smartphones are either based upon machine learning techniques or upon monitoring power consumption. ii) Signature-Based - A knowledge based detection based upon patterns of well-known attacks such in mobile phones detects anomaly on smart phones using signatures. The signature-based approach checks if each signature derived from an application matches any signature in a malware database. The database of malware signature can be automatically or manually defined.

In [12] authors identify solutions for mobile which include
Usage and install anti-virus and anti-malware solutions from trusted sources to protect the device against malware and viruses. All the APP developers should use HTTPS/ TLS networks to transfer the data in encrypted form. Ensure to minimize the use of built-in permissions in their applications.

Users install various Apps from playstores to install games and other Apps. Service providers should build the applications to free from malicious codes, and offensive material. Illegal grayware can be punished with corporate fines .Or such activities can be objected by the users if they discover anything illegal.

E. Solution for cloud computing

To overcome the threats of cloud computing [10] -

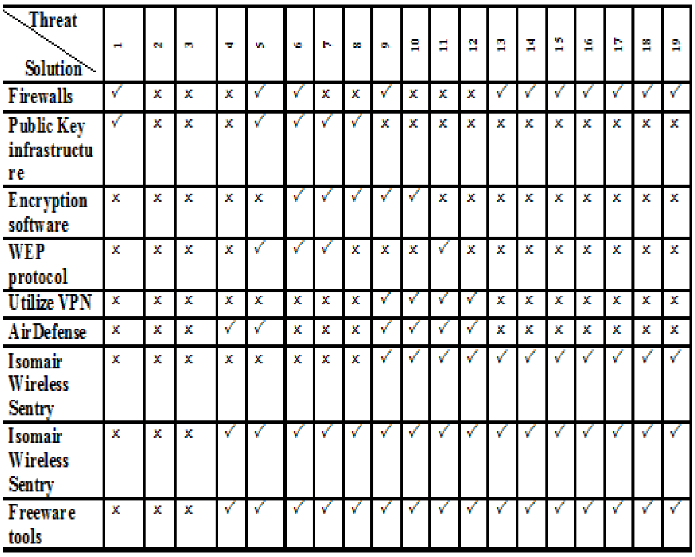
1. Find the best cloud provider based his requirements and on different data security and data management and select the right cloud provider.
2. Clients should have basic knowledge about standards, regulation ensure for a secure channel for data transmission
3. Enhance access control and restrict access to unauthorized persons
4. Systematic auditing with logging and monitoring events for analyzing events.
5. Test software patches before software patches to install.
6. Provide secure keys for encryption and procedures to recover keys.
7. Data breaches can be eliminated by encrypting all of the clients data provided a backup is create to avoid the loss in case
the encryption key is lost, the client would have a complete data loss. Thus, the client should have a backup copy of the
data.
8. The first mitigation technique is to increase the awareness. Keeping all systems up-to-date and always patching an updating operating systems and protection software is also vital.

F. Vehicle Hacking solutions

To prevent Vehicle Hacking threat few measures [15] are suggested .

1. Vehicles need regular up-to-dates to system to avoid expensive and lengthy recalls every time a security vulnerability is found .
2. Manufacturers should separate infotainment systems and critical drive units, strictly controlling the communication between them.
3. The manufacturers should secure each individual software subcomponent since a breach to one component means breach to the entire system.

DOI: 10.15680/IJIRCCE.2016. 0408127



Threat Solution	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Firewalls	✓	x	x	x	✓	✓	x	x	✓	x	x	x	✓	✓	✓	✓	✓	✓	✓
Public Key infrastructure	✓	x	x	x	✓	✓	✓	✓	x	x	x	x	x	x	x	x	x	x	x
Encryption software	x	x	x	x	x	✓	✓	✓	✓	✓	x	x	x	x	x	x	x	x	x
WEP protocol	x	x	x	x	✓	✓	✓	x	x	x	✓	x	x	x	x	x	x	x	x
Utilize VPN	x	x	x	x	x	x	x	x	✓	✓	✓	✓	x	x	x	x	x	x	x
AirDefense	x	x	x	✓	✓	x	x	x	✓	✓	✓	✓	x	x	x	x	x	x	x
Isomair Wireless Sentry	x	x	x	x	x	x	x	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Isomair Wireless Sentry	x	x	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Freeware tools	x	x	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

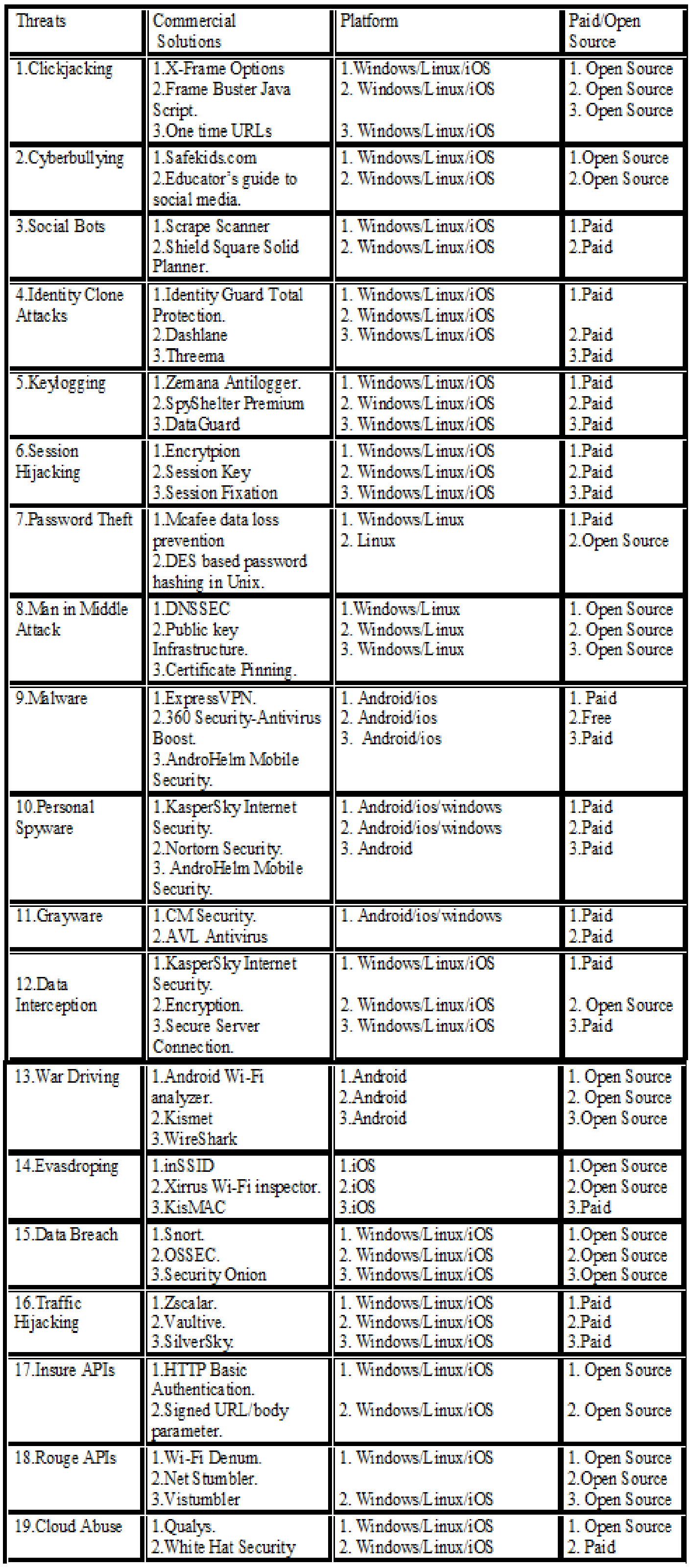
1 - Click jacking 2 - Cyber bullying
3 - Socialbots 4 - Identity clone attack
5- Key logging 6 - Session Hijacking
7 - Password Theft 8 - Man in The Middle
9 - Data Interception 10 - War Driving
11- Rouge AP's 12 - Eavesdropping
13 - Data Breaches 14 - Traffic Hijacking
15 - Insecure API's -15 16 - Cloud Abuse
17 - Malware 18 - Personal Spyware
19- Grayware

✓ - Solution supports the threats

✗ - Solution does not support the threat

Table 6 – Tools for the threats discussed and the features whichthe tools support

DOI: 10.15680/IJIRCCE.2016. 0408127



Threats	Commercial Solutions	Platform	Paid/Open Source
1.Clickjacking	1.X-Frame Options 2.Frame Buster Java Script. 3.One time URLs	1.Windows/Linux/iOS 2. Windows/Linux/iOS 3. Windows/Linux/iOS	1. Open Source 2. Open Source 3. Open Source
2.Cyberbullying	1.Safekids.com 2.Educator's guide to social media.	1. Windows/Linux/iOS 2. Windows/Linux/iOS	1.Open Source 2.Open Source
3.Social Bots	1.Scrape Scanner 2.Shield Square Solid Planner.	1. Windows/Linux/iOS 2. Windows/Linux/iOS	1.Paid 2.Paid
4.Identity Clone Attacks	1.Identity Guard Total Protection. 2.Dashlane 3.Threema	1. Windows/Linux/iOS 2. Windows/Linux/iOS 3. Windows/Linux/iOS	1.Paid 2.Paid 3.Paid
5.Keylogging	1.Zemana Antilogger. 2.SpyShelter Premium 3.DataGuard	1. Windows/Linux/iOS 2. Windows/Linux/iOS 3. Windows/Linux/iOS	1.Paid 2.Paid 3.Paid
6.Session Hijacking	1.Encrytpion 2.Session Key 3.Session Fixation	1. Windows/Linux/iOS 2. Windows/Linux/iOS 3. Windows/Linux/iOS	1.Paid 2.Paid 3.Paid
7.Password Theft	1.Mcafee data loss prevention 2.DES based password hashing in Unix.	1. Windows/Linux 2. Linux	1.Paid 2.Open Source
8.Man in Middle Attack	1.DNSSEC 2.Public key Infrastructure. 3.Certificate Pinning.	1.Windows/Linux 2. Windows/Linux 3. Windows/Linux	1. Open Source 2. Open Source 3. Open Source
9.Malware	1.ExpressVPN. 2.360 Security-Antivirus Boost. 3.AndroHelm Mobile Security.	1. Android/ios 2. Android/ios 3. Android/ios	1. Paid 2.Free 3.Paid
10.Personal Spyware	1.KasperSky Internet Security. 2.Nortorn Security. 3. AndroHelm Mobile Security.	1. Android/ios/windows 2. Android/ios/windows 3. Android	1.Paid 2.Paid 3.Paid
11.Grayware	1.CM Security. 2.AVL Antivirus	1. Android/ios/windows	1.Paid 2.Paid
12.Data Interception	1.KasperSky Internet Security. 2.Encryption. 3.Secure Server Connection.	1. Windows/Linux/iOS 2. Windows/Linux/iOS 3. Windows/Linux/iOS	1.Paid 2. Open Source 3.Paid
13.War Driving	1.Android Wi-Fi analyzer. 2.Kismet 3.WireShark	1.Android 2.Android 3.Android	1. Open Source 2. Open Source 3.Open Source
14.Evasdroping	1.inSSID 2.Xirrus Wi-Fi inspector. 3.KisMAC	1.iOS 2.iOS 3.iOS	1.Open Source 2.Open Source 3.Paid
15.Data Breach	1.Snort. 2.OSSEC. 3.Security Onion	1. Windows/Linux/iOS 2. Windows/Linux/iOS 3. Windows/Linux/iOS	1.Open Source 2.Open Source 3.Open Source
16.Traffic Hijacking	1.Zscalar. 2.Vaultive. 3.SilverSky.	1. Windows/Linux/iOS 2. Windows/Linux/iOS 3. Windows/Linux/iOS	1.Paid 2.Paid 3.Paid
17.Insure APIs	1.HTTP Basic Authentication. 2.Signed URL/body parameter.	1. Windows/Linux/iOS 2. Windows/Linux/iOS	1. Open Source 2. Open Source
18.Rouge APIs	1.Wi-Fi Denum. 2.Net Stumbler. 3.Vistumbler	1. Windows/Linux/iOS 2. Windows/Linux/iOS	1. Open Source 2.Open Source 3. Open Source
19.Cloud Abuse	1.Qualys. 2.White Hat Security	1. Windows/Linux/iOS 2. Windows/Linux/iOS	1. Open Source 2. Paid

Table 7 – The commercial tools for the various threats and OS under which it operates

DOI: 10.15680/IJIRCCE.2016. 0408127

V. CONCLUSION

The increasing uses of cyber services have become a major part of everyone’s life. But the prevaling threats make it difficult for users to enjoy these services properly. The main challenge is to develop new solutions to cope up with these threats so as to make these cyber platform more safe and secure for their users so they can enjoy these facilities better.

REFERENCES

1. Michael Fire, Member, IEEE, Roy Goldschmidt, and Yuval Elovici, Member, IEEE ,Online Social Networks: Threats and Solutions , IEEE communication surveys & tutorials, VOL. 16, NO. 4, fourth quarter 2014
2. M.A. Devmane, N.K. Rana , Privacy issues in online social networks.,International journal of computer applications. Vol 41,no. 13th,march 2012.
3. Houssam El Ismaili, HananeHoumani, HichamMadroumi , A Secure Electronic Transaction Payment Protocol Design and Implementation. Architecture of Systems Team - ENSEM, Hassan II University, 8118, Casablanca – Morocco (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 5, 2014.
4. NiranjanamurthyM , DR. DharmendraChahar , The study of E-Commerce Security Issues and solutions , ,International Journal of Advanced Research in Computer and Communication Engineering. Vol. 2, Issue 7, July 2013.
5. ZakariaKarim, Karim Mohammed Rezaul, AliarHossain , Towards Secure Information Systems in Online Banking , Applied Research Centre for Business and Information Technology (ARCBIT), Centre for Applied Internet Research (CAIR) ,2009
6. YulongZou, Senior Member, IEEE, Xianbin Wang, Senior Member, IEEE, and LajosHanzo, Fellow, IEEE , A Survey on Wireless Security: Technical ,Challenges, Recent Advances and Future Trends, 29th may ,2015
7. RadomirProdanovi and DejanSimi , A Survey of Wireless Security , Journal of Computing and Information Technology - CIT 15, 2007, 3, 237–255 , 2007
8. Lucas Jacob , Damien Hutchinson , Wi-Fi security: wireless with confidence , Deakin University , JemalAbawajyDeakin University 2011.
9. BartlomiejUscilowski , Mobile adware and malware analysis, Version 1.0, October 2013.
10. Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steven Hanna, and David Wagner , A Survey of Mobile Malware in the Wild , SPSM ’11 Proceedings of the 1st ACM workshop on Security and Privacy on smart phones and mobile devices , ACM , 2011
11. DeepikaDhiman , WLAN Security Issues and Solutions , IOSR Journal of Computer Engineering (IOSR-JCE) , Jan 2014
12. RadomirProdanoviand Dejan Simi , A Survey of Wireless Security , Journal of Computing and Information Technology - CIT 15, 2007, 3, 237–255 , 2007
13. WLAN Security Issues and Solutions , IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 16, Issue 1, Ver. IV, PP 67-75 , Jan. 2014
14. Security Threats and Solutions in Cloud Computing ,World Congress on Internet Security (WorldCIS-2013) , Hamm Eken ,Institute of Information,GaziUniversityAnkara, Turkey , 978-1-908320-22/3/$25.00 IEEE , 2013
15. A Survey on Security for Mobile Devices ,Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra ,
16. AbdullahiArabo and BernardiPranggono, Mobile Malware and Smart Device Security: Trends, Challenges and Solutions, 19th International Conference on Control Systems and Computer Science , 2013
17. Automotive Cyber security: An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles. IET-The Institution for Engineering and Technology