Computer Secrecy and Obscuration: A Challenge

[1] Lilavati Samant, [2] Amrita Naik

[1, 2] Computer Engineering department, Don Bosco College of Engineering,
Goa University, Goa.

Abstract - Computer often perform life-critical tasks Security and Privacy of our data is very important and achieving the same is very critical task. We should be aware of types of threats and solutions to our computer and in turn Data.

***Keywords* - Computer Security, Privacy, Data.**

1. Introduction

Privacy is a limitation of others' access to an individual through information, attention, or physical proximity. Security must be mathematically rigorous and must capture all realistic attacks that a malicious participant may try to stage. Security Includes protection of information from theft or corruption, or the preservation of availability, as defined in the security policy.

Goals of Computer Security:

- Integrity:
  - Guarantee that the data is what we expect
- Confidentiality
  - The information must just be accessible to the authorized people
- Reliability
  - Computers should work without having unexpected problems
- Authentication
  - Guarantee that only authorized persons can access to the resources

Types of Security

- Network Security
- System and software security
- Physical Security

2. Types of Threats

a)System And Network Threats

- Worms – use spawn mechanism; standalone program
- Internet worm
  - Exploited UNIX networking features (remote access) and bugs in *finger* and *sendmail* programs.
  - Grappling hook program uploaded main worm program

- Port scanning
  - Automated attempt to connect to a range of ports on one or a range of IP addresses.
- Denial of Service
  - Overload the targeted computer preventing it from doing any useful work
  - Distributed denial-of-service (DDOS) come from multiple sites at once.

2.1 Security Attacks

Types of Attacks:

- Network Attacks
  - Packet sniffing, man-in-the-middle, DNS hacking
- Web attacks
  - Phishing, SQL Injection, Cross Site Scripting
- OS, applications and software attacks
  - Virus, Trojan, Worms, Rootkits, Buffer Overflow
- Social Engineering
  - (NOT social networking)
- Not all hackers are evil wrongdoers trying to steal your info
  - Ethical Hackers, Consultants, Penetration testers, Researchers
    Do hacking for a good purpose.

Network Attacks:

- Packet Sniffing
  - Internet traffic consists of data "packets", and these can be "sniffed"

  - Leads to other attacks such as password sniffing, cookie stealing session hijacking, information stealing
- Man in the Middle
  - Insert a router in the path between client and server, and change the packets as they pass through
- DNS hijacking
  - Insert malicious routes into DNS tables to send traffic for genuine sites to malicious sites

Web Attacks:

- Phishing
  - An evil website pretends to be a trusted website
- SQL Injection
  - SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- Cross Site Scripting
  - Writing a complex Javascript program that steals data left by other sites that you have visited in same browsing session

Social Engineering:

Manipulating a person or persons into divulging confidential information

  - Social Engineers are coming up with much better and much more elaborate schemes to attack users.
  - Even corporate executives can be tricked into revealing VERY secret info
  - To protect yourself NEVER give out your password to ANYBODY.
  - Any system administrator should have the ability to change your password without having to know an old password

Password Attacks:

Password Guessing

  - Ineffective except in targeted cases
- Dictionary Attacks
  - Password are stored in computers as hashes, and these hashes can sometimes get exposed
  - Check all known words with the stored hashes
- Rainbow Tables
  - Trade off storage and computation – uses a large number of pre-computed hashes without having a dictionary
  - Innovative algorithm that can find passwords fast!

2.2.1 Attack Methods

Worm:

- Definition
  - Piece of code that automatically reproduces itself over the network. It doesn’t need the user intervention to propagate (autonomous).
- Infection
  - Via buffer overflow, file sharing, configuration errors and other vulnerabilities.
- Target selection algorithm
  - Email addresses, DNS, IP, network neighborhood
- Payload
  - Malicious programsBackdoor, DDoS agent, etc

Viruses:

Fragment of code embedded in legitimate program. Mainly effects personal PC systems. These are often downloaded via emails or as active components in web pages.

Virus:

- Definition
  - Piece of code that automatically reproduces itself. It’s attached to other programs or files, but requires user intervention to propagate.
- Infection (targets/carriers)
  - Executable files
  - Boot sectors
  - Documents (macros), scripts (web pages), etc.
- Propagation is made by the user. The mechanisms are storage elements, mails, downloaded files or shared folders

Backdoor, trojan, rootkits :

- Goal
  - The goal of *backdoor*, *Trojan* and *rootkits* is to take possession of a machine subsequently through an infection made via a backdoor.

- Backdoor
  - A *backdoor* is a program placed by a black-hacker that allows him to access a

system. A *backdoor* have many functionalities such as keyboard-sniffer, display spying, etc.

- Trojan
  - A *Trojan* is software that seems useful or benign, but is actually hiding a malicious functionality.
- Rootkits (the ultimate virus)
  - *Rootkits* operate like *backdoor* and *Trojan*, but also modify existing programs in the operating system. That allows a black-hacker to control the system without being detected. A *rootkit* can be in user-mode or in kernel-mode.
- Trap Doors: Inserting a method of breaching security in a system
- Threat Monitoring: Look for unusual activity.
- Audit Log: Record time, user and type of access on all objects and trace problems back to the source.

Firewall: A mechanism that allows only certain traffic between trusted and entrusted systems.

2.2 Typical Security Attacks

Typical security attack can occur in following forms:

Modification: Changing a portion of the message.

Spurious messages: Introducing bogus messages with valid addresses and consistency criteria.
Site impersonation: Claiming to be some other logical node.

Replay of previous transmission: repeating previous valid messages. (ex: authorization of cash withdrawal.)

Vulnerabilities in Systems:

- There are vulnerabilities in most software systems.
  - Buffer Overflow is the most dangerous and common one

- Buffer Overflow:
  - All programs run from memory.
  - Some programs allow access to reserved memory locations when given incorrect input.
  - Hackers find out where to place incorrect input and take control.
  - Easy to abuse by hackers, allows a hacker complete access to all resources

3. Computer Security

Computer security involves protecting information, hardware and software from unauthorized use and damage and from sabotage and natural disasters.

3.1 Measures to Protect Computer Security

- Restricting access both to the hardware locations (physical access) and into the system itself (over the network) using firewalls
- Implementing a plan to prevent break-ins
- Changing passwords frequently
- Making backup copies
- Using anti-virus software
- Encrypting data to frustrate interception
- Anticipating disasters (disaster recovery plan)
- Hiring trustworthy employees.

3.1.1 External Protection of a System

Unauthorized access occurs when someone tries to access service, system, program using someone else's account or other inappropriate methods. Protection of passwords is difficult.

Issues include:

- It's very easy to guess passwords since people use simple and easily remembered words.
- Need exists to change passwords continually.
- Limiting number of tries before locking up.

To achieve security:

- Many techniques exist for ensuring computer and network security
  - Cryptography
  - Secure networks
  - Antivirus software
  - Firewalls
- In addition, users have to practice “safe computing”
- – Not downloading from unsafe websites
- – Not opening attachments
- – Not trusting what you see on websites
- – Avoiding Scams

4. Cyber Crime

The expression ‘Crime’ is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The “Offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force.Cyber Crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react.

Types of cyber-crime:

- Hacking
- Denial of service
- Credit card fraud
- Phishing
- Spoofing
- Cyber defacement
- Spamming
- Threatening

Hacking:is an illegal intrusion into a computer system without permission of the computer owner / user.

Types of Hacking:

1. Website Hacking
2. Network Hacking
3. Ethical Hacking
4. Email Hacking
5. Password Hacking
6. Online Banking Hacking
7. Computer Hacking

- Website Hacking
  - Hacking a website means taking control from the website owner to a person who hacks the website.
- Network Hacking
  - Network Hacking is generally means gathering information about domain by using tools like Telnet, Ns look UP, Ping, Tracert, Netstat, etc over the network.
- Ethical Hacking
  - Ethical hacking is where a person hacks to find weaknesses in a system and then usually patches them.
- E-mail Hacking
  - Email hacking is illicit access to an email account or email correspondence.
- Password Hacking
  - Password Hacking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- Online Banking Hacking
  - Unauthorized accessing bank accounts without knowing the password or without permission of account holder are known as Online banking hacking.
- Computer Hacking
  - Computer Hacking is when files on your computer are viewed, created, or edited without your authorization.

***Virus Dissemination**:*

Virusis malicious software that attaches itself to other software and causes break down of the operating system in extreme cases.

The kinds of viruses:

- ❖ Worms,
- ❖ Trojan Horse,
- ❖ Time Bomb Virus,
- ❖ Logic Bomb,
- ❖ True Love
- ❖ Spyware
- ❖ Malware
- ❖ Hoaxes

Software Piracy: Theft of software through illegal copying of original programs and distribution of the products intended to pass for the original.Retail revenue losses worldwide are ever increasing due to this crime.

This can be done in various ways

1. End user copying,
2. Hard disk loading,
3. Illegal downloads from the internet etc.

ATM/Credit Card Fraud:

- You simply have to type credit card number into www page of the vendor for online transaction.
- If electronic transactions are not secured, the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.
- Plastic money transaction use skimmer for swapping the card.
- Attacker use Skimmer having memory to store information in magnetic stripe of a credit, debit or ATM card during shopping.
- This information, copied onto another blank card's magnetic stripe, is then used by an

identity thief to make purchases or withdraw cash in the name of the actual account holder.

Net Extortion:

Copying the company's confidential data in order to extort huge amounts of money from the said company.

Phishing:
It is the technique of pulling out confidential information of the account holders from their banks /financial institutions by deceptive means.

Spoofing:
A technique used to gain unauthorized access to computers, whereby the intruder sends hoax messages to a computer with such an IP address which indicates that the message is coming from trusted host.

***Cyber Defamation*:**
Sending defamatory messages through e-mail to the victim or his relatives, friends, etc. or posting of the defamatory material on a website.

Cyber Security:
Involves protection of sensitive personal & business information through prevention, detection and response to different online attacks

Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks. Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.

Cyber Laws in India:

Under The Information Technology Act, 2000

- CHAPTER XI – OFFENCES – 66.
- Hacking with computer system.
  - Whoever with the Intent to cause or knowing that he is likely to cause Wrongful Loss or Damage to the public or any person destroys or Deletes or Alters any Information.
  - Residing in a Computer Resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
  - Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
  - Whoever without permission of the owner of the computer
  - – Secures Access;
  - – Downloads, Copies or extracts any data, computer database or any information;
  - – Introduce or causes to be introduce any Virus or Contaminant;
  - – Disrupts or causes disruption;
  - – Denies or causes denial of access to any person;
  - – Provides any assistance to any person to facilitate access
  - – Charges the services availed of by a person to the account of another person by Tampering with or Manipulating any Computer, Computer System, or Computer Network;

Shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Indian Crime Scene:

- The majority of cybercrimes are centered on forgery, fraud and Phishing,
- India is the third-most targeted country for Phishing attacks after the US and the UK,
- Social networks as well as ecommerce sites are major targets,
- 6.9 million bot-infected systems in 2010
- 14,348 website defacements in 2010
- 6,850 .in and 4,150 .com domains were defaced during 2011,
- 15,000 sites hacked in 2011
- India is the number 1 country in the world for generating spam.

Safety Tips for Cyber Crime:
- Use antivirus software's.
- Insert firewalls.
- Uninstall unnecessary software
- Maintain backup.
- Check security settings.
- Stay anonymous - choose a genderless screen name.
- Never give your full name or address to strangers.
- Learn more about Internet privacy.

5. Conclusion

The Computers are powerful, programmable machines whoever programs them controls them (and not you). Networks are ubiquitous. Carries can genuine as well as malicious traffic. End result: Complete computer security is unattainable once your system is connected to World

Wide Web. We can just take precautions and follows the rules to avoid the threats.

References

[1] Jerry Breecher, ppt titled "Operating System Security"

[2] Director Sir, Appu Kuttan, MIT Bhopal, Cyber Security ppt, TEQIP workshop,2015

[3] www.wikipedia.com

Author Profile:

Lilavati Samant , Mtech (CS&E),VTU Belgaum. Currently working as assistant professor, computer Engineering Department, Don Boasco College of Engineering, Fatorda, Goa.

Mrs Amrita Naik ,ME (IT),Goa University. Currently working as assistant professor, computer Engineering Department, Don Boasco College of Engineering, Fatorda, Goa.