

LIKE



COMMENT

SHARE



SUBSCRIBE

Unit 5

UNIT V

CYBER CRIMES AND CYBER SECURITY

9

Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Keyloggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security



<https://www.scribd.com/document/661638611/WILEY-INDIA-Cyber-Security-Understanding-Cyber-Crimes-Computer-Forensics-and-Legal-Perspectives-Nina-Godbole-Sunit-Belapure-Kamlesh-Bajaj-2011>

Cyber Crime

Type of Cybercrime	Scenario	Outcome
Phishing	You receive a fake email from your bank	Attacker gains access to your login credentials
Ransomware	Downloading malicious software	Files encrypted, ransom demand for decryption key
Identity Theft	Hacker gains access to a database	Stolen personal information used for fraudulent activities
Online Scams	Fake online advertisement for a product	Payment made, but no receipt of promised goods or services
Cyberbullying	Harassment on social media or online platforms	Emotional distress, reputational harm, or real-world consequences

Key Points



- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.
- Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Classification of Cyber Crimes

1. Cybercrime against Individual

- a. Email Spoofing ✓
- b. Phishing ✓
- c. Spamming ✓
- d. Cyber Defamation ✓
- e. Cyberstalking and harassment ✓
- f. Computer Sabotage ✓
- g. Pornographic Offences ✓
- h. Password Sniffing ✓

2. Cybercrime against Property

- a. Credit card fraud ✓
- b. Intellectual Property Crime ✓
- c. Internet Time Theft ✓

3. Cybercrime against Organization

- a. Unauthorized Computer Access ✓
- b. Password Sniffing ✓
- c. Denial of Service attacks ✓
- d. Virus Attack ✓
- e. Email Bombing ✓
- f. Salami Attack ✓
- g. Logic Bomb ✓
- h. Trojan Horse ✓
- i. Data Diddling ✓
- j. Crimes from usenet group ✓
- k. Industrial Spying ✓
- l. Computer Network Intrusion ✓
- m. Software Piracy ✓

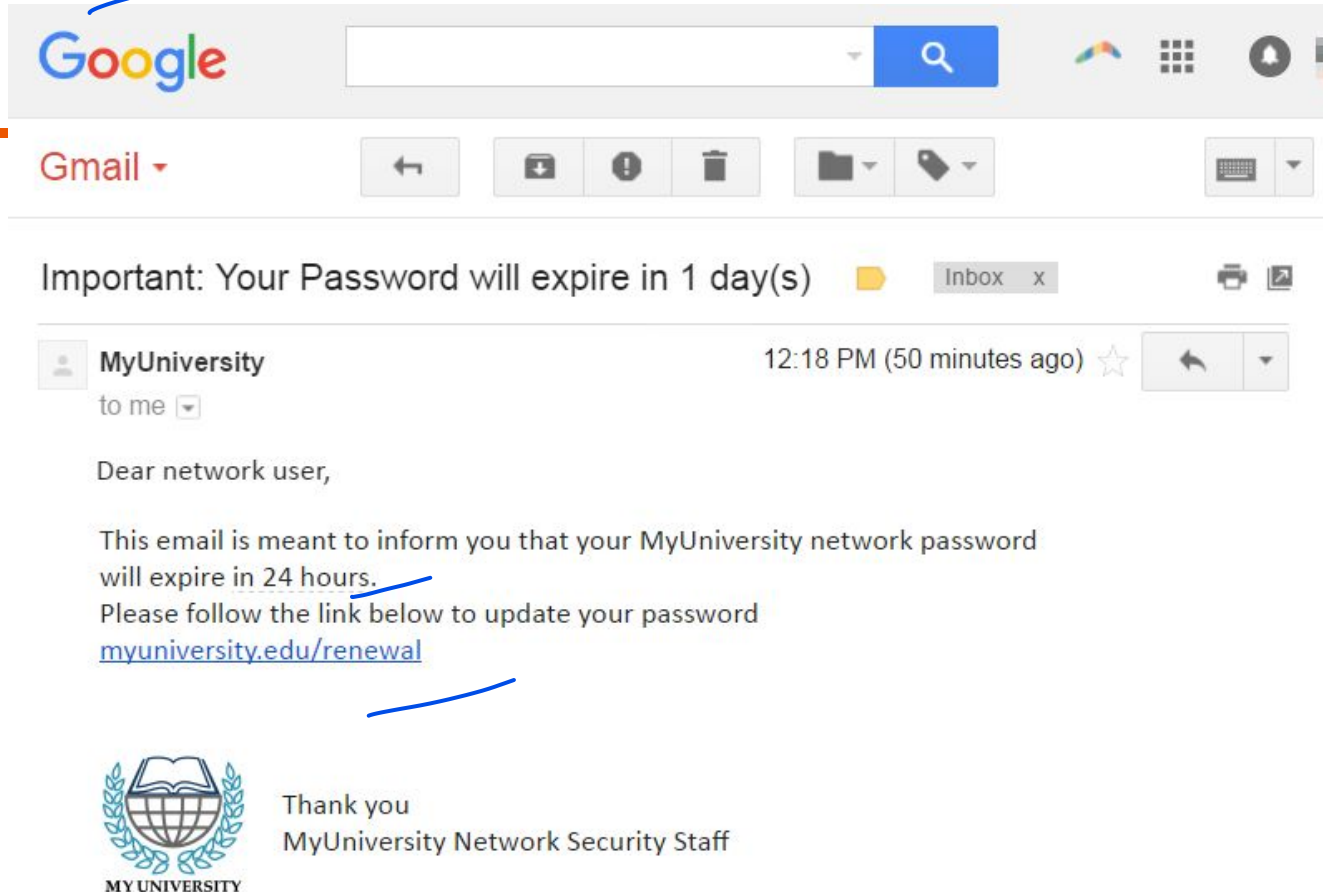
4. Cybercrime against society

- a. Forgery ✓
- b. Cyber Terrorism ✓
- c. Web Jacking ✓

1. Email Spoofing



2. Phishing



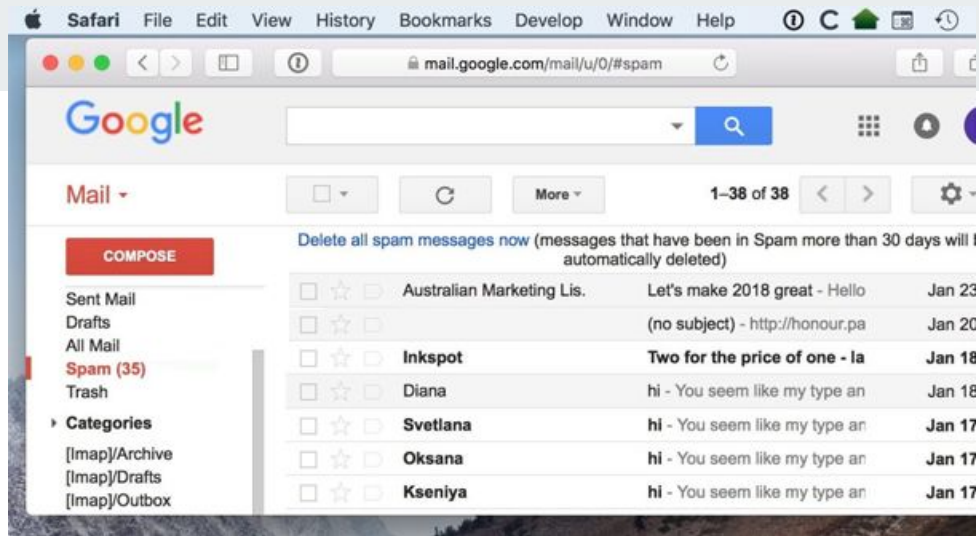
1. Email Spoofing:

- **Definition:** Email spoofing involves forging the sender's address to make the email appear as if it's from a trusted source.
- **Purpose:** Often used in phishing attacks to trick recipients into opening malicious attachments or clicking on fraudulent links.
- **Example:** A fake email appears to be from a reputable bank, prompting the recipient to provide sensitive information.

2. Phishing:

- **Definition:** Phishing is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity in an electronic communication.
- **Techniques:** Commonly involves fake emails, websites, or messages to trick individuals into revealing personal information, such as usernames and passwords.
- **Example:** An email claiming to be from a popular online service, asking the recipient to click on a link and log in.


3. Spamming



Spamming:

- **Definition:** Spamming refers to the mass distribution of unsolicited and irrelevant messages, often for advertising purposes.
- **Methods:** Utilizes email, instant messaging, or social media to reach a large audience.
- **Impact:** Can overload communication channels, waste resources, and sometimes deliver malicious content.

3. Spamming - Search Engine

- 
1. Repeating Keywords
 2. Use of non-related keywords
 3. REdirection
 4. Use of colored Text
 5. Hidden Links
 6. Duplication of pages with different URLs
 7. Use of different pages that direct to same URL



4. Cyber Defamation




4. Cyber Defamation:

- **Definition:** Cyber defamation involves making false statements about an individual or entity through online platforms.
- **Consequences:** Reputation damage, emotional distress, and potential legal action against the defamer.
- **Examples:** False accusations, spreading rumors, or posting damaging content online with the intent to harm someone's reputation.

5. Cyber Stalking and Harassment



5. Cyberstalking and Harassment:

- **Definition:** Involves persistent, unwanted online attention, contact, or harassment towards an individual. 
- **Methods:** Use of social media, emails, or other online platforms to intimidate or threaten the victim. 
- **Impact:** Emotional distress, fear, and potential escalation to real-world harm. 

6. Computer Sabotage:

- **Definition:** Deliberate actions to disrupt, damage, or destroy computer systems, networks, or data.
- **Motivations:** Varies from revenge to ideological reasons; can result in financial losses and operational disruptions.
- **Examples:** Spreading malware, conducting DoS attacks, or hacking critical infrastructure.

7. Pornographic Offences:

- **Definition:** Involves the distribution, creation, or possession of explicit and illegal sexual content, often involving minors.
- **Illegality:** Violates laws related to child pornography and can lead to severe legal consequences.

8. Password Sniffing:

- **Definition:** Password sniffing involves intercepting and capturing login credentials as they travel over a network.
- **Methods:** Typically associated with the use of specialized software or hardware to eavesdrop on network traffic.
- **Risk:** Allows attackers to gain unauthorized access to accounts and sensitive information.

Credit Card Fraud:

- **Definition:** Unauthorized use of credit card information for financial gain.
- **Methods:** Stolen card details used for online purchases or fraudulent transactions.
- **Consequences:** Financial losses for cardholders, potential damage to credit scores.
- **Prevention:** Regularly monitor credit card statements, use secure websites for transactions.

Intellectual Property Crime:

- **Definition:** Violations related to the unauthorized use or reproduction of intellectual property.
- **Examples:** Copyright infringement, patent violations, trademark counterfeiting.
- **Impact:** Financial losses for creators, damage to brand reputation, stifling innovation.
- **Enforcement:** Legal actions, copyright takedowns, intellectual property laws.

Internet Time Theft:

- **Definition:** Unauthorized use of internet or computer resources for personal purposes during work hours.
- **Methods:** Employees using company time and resources for non-work activities.
- **Consequences:** Decreased productivity, loss of work hours, potential disciplinary actions.
- **Prevention:** Implementation of internet usage policies, monitoring tools, and employee education.

1. Unauthorized Computer Access:

- **Definition:** Gaining access to a computer, network, or system without permission.
- **Methods:** Exploiting vulnerabilities, using stolen credentials, or bypassing security measures.
- **Consequences:** Unauthorized access to sensitive information, data breaches, and potential legal repercussions.

2. Password Sniffing:

- **Definition:** Intercepting and capturing login credentials as they travel over a network.
- **Methods:** Use of specialized software or hardware to eavesdrop on network traffic.
- **Risk:** Allows attackers to gain unauthorized access to accounts and sensitive information.

3. Denial of Service Attacks:

- **Definition:** Overloading a system, network, or website with traffic to make it unavailable.
- **Methods:** Flood of requests, exploitation of vulnerabilities, or resource exhaustion.
- **Impact:** Disruption of services, downtime, and potential financial losses.

4. Virus Attack:

- **Definition:** Malicious software that infects and spreads within computer systems.
- **Methods:** Infected files, email attachments, or compromised websites.
- **Consequences:** Data corruption, system instability, and potential theft of sensitive information.

5. Email Bombing:

- **Definition:** Sending a massive volume of emails to overwhelm an email account or server.
- **Methods:** Automated scripts or programs generating and sending numerous emails.
- **Impact:** Email account inaccessibility, disruption of communication.

6. Salami Attack:

- **Definition:** Small, unauthorized transactions that accumulate to a significant loss.
- **Methods:** Manipulating financial transactions to siphon small amounts without detection.
- **Consequences:** Financial losses that may go unnoticed until a significant sum is taken.

Logic Bomb:

- **Definition:** Malicious code or program triggered by a specific event or condition.
- **Methods:** Inserting code that activates under certain circumstances, causing harm.
- **Impact:** Data destruction, system disruption, or other malicious activities.

Trojan Horse:

- **Definition:** Malicious software disguised as legitimate software to deceive users.
- **Methods:** Typically spread through email attachments, downloads, or software bundling.
- **Consequences:** Unauthorized access, data theft, or additional malware installation.

Data Diddling:

- **Definition:** Unauthorized manipulation or alteration of data before or during entry.
- **Methods:** Changing data to benefit the perpetrator without detection.
- **Consequences:** Misleading information, financial fraud, or operational disruptions.

Crimes from Usenet Group:

Definition: Illegal activities conducted through Usenet discussion groups.

- **Examples:** Distribution of pirated software, hacking discussions, or trading stolen information.

Consequences: Legal repercussions, loss of privacy, and potential network security issues.

Industrial Spying:

- **Definition:** Gathering confidential business information from competitors or other entities.
- **Methods:** Espionage, hacking, or social engineering to gain access to sensitive data.
- **Consequences:** Economic losses, compromised trade secrets, and damaged business relationships.

Computer Network Intrusion:

- **Definition:** Unauthorized access or entry into a computer network.
- **Methods:** Exploiting vulnerabilities, using malware, or bypassing security measures.
- **Consequences:** Data breaches, compromised systems, and potential exposure of sensitive information.

Software Piracy:

- **Definition:** Unauthorized copying, distribution, or use of software without proper licensing.
- **Methods:** Illegally downloading, sharing, or selling software without the developer's permission.
- **Consequences:** Financial losses for software developers, legal actions, and potential security risks.

1. Forgery:

- **Definition:** The creation, alteration, or imitation of documents, signatures, or data with the intent to deceive.
- **Methods:** Digital forgery involves manipulating electronic documents, images, or data.
- **Consequences:** Misrepresentation, fraud, and potential financial or legal repercussions.

2. Cyber Terrorism:

- **Definition:** The use of technology and cyberspace to conduct terrorist activities, including attacks on critical infrastructure or the dissemination of terror-related information.
- **Methods:** Disrupting computer networks, conducting propaganda campaigns, or launching cyber attacks with political or ideological motives.
- **Consequences:** Serious disruption of essential services, economic damage, and potential loss of life.

3. Web Jacking:

- **Definition:** Unauthorized control or manipulation of a website's content, often for malicious purposes.
- **Methods:** Exploiting vulnerabilities in a website's security, gaining unauthorized access to the site's administration, or manipulating content through hacking techniques.
- **Consequences:** Defacement of websites, dissemination of false information, or use for criminal activities.

LIKE



COMMENT



SHARE



SUBSCRIBE



Password Cracking - to recover the password from data that has been stored or transmitted.

Why it is needed?

1. To recover forgotten password
2. To check for security of passwords at organization level.
- ③ To gain unauthorized access into someone's else account

How manual cracking is tried?

1. Choose a random account.
2. Create list of possible passwords
3. Try logging in with each passwords until the login is successful

Very easy guesses:

1. DOB
2. Place of birth
3. Mobile Number
4. Fathers name
5. Vehicle number
6. Simple words like password, open etc.



What are password cracking tools?

Password crackers can be used maliciously or legitimately to recover lost passwords. Among the password cracking tools available are the following three:

1. **Cain and Abel**. This password recovery software can recover passwords for Microsoft Windows user accounts and Microsoft Access passwords. Cain and Abel uses a graphical user interface, making it more user-friendly than comparable tools. The software uses dictionary lists and brute-force attack methods.
2. **Ophcrack**. This password cracker uses rainbow tables and brute-force attacks to crack passwords. It runs on Windows, macOS and Linux.
3. **John the Ripper**. This tool uses a dictionary list approach and is available primarily for macOS and Linux systems. The program has a command prompt to crack passwords, making it more difficult to use than software like Cain and Abel.

Online Password Cracking:

U_1
 $H_1 \rightarrow S_1$

1. Definition:

- **Online attacks** involve attempting to crack passwords while the target system is online and accessible.
- **Example:** Repeated login attempts on a web application or network service.

2. Methods:

- **Brute Force:** Repeatedly trying all possible combinations of passwords until the correct one is found.
- **Dictionary Attacks:** Using precompiled lists of commonly used passwords or words from dictionaries.

3. Characteristics:

- **Requires Connectivity:** The attacker needs to be connected to the target system or service.
- **Detection:** Online attacks are more likely to be detected by security systems that monitor login attempts and patterns.

Offline Password Cracking:

1. Definition:

- **Offline attacks** involve attempting to crack passwords without actively connecting to the target system or service.
- **Example:** Stealing password hashes from a compromised database and attempting to crack them locally.

2. Methods:

- **Rainbow Tables:** Precomputed tables of hash values for a large set of possible passwords.
- **Brute Force with Stolen Hashes:** Attempting to crack passwords using computational power without needing to connect to the actual system.

3. Characteristics:

- **No Active Connection:** The attacker doesn't need to be connected to the target system during the password cracking process.
- **Reduced Detection:** Because there's no continuous connection, offline attacks may be harder to detect compared to online attacks.

- **Short passwords:** A single word such as Igloo or Peanuts, as well as a numerical phrase like 12345.
- **Recognizable keystroke patterns:** Any pattern that you make on your keyboard like QWERTY or 1QAZ2WSX.
- **Personal information in passwords:** Including information such as date of birth, street name and first name. For example, a password of *John99* or *Maplewood099* for someone named John who was born in 1999 and lives on Maplewood Street.
- **Passwords varied with a single character:** Changing from lowercase to capital letters or adding a period or exclamation mark for “different” passwords across multiple accounts. For example, using the password Alice2004 on one account and using the password AlicE2004 on another account.
- **Common passwords:** Using common passwords like password, password123 and 123456.
- **Repeated letters or numbers:** Password combinations that are just repeated such as *55555* and *bbbb*.

Rules for a Strong Password

✓ Upper and Lowercase Letters

No Personal Data, Like Your Birthday

Bu0#L8/cij8X,#m>uzf

✓ At Least 12 Characters

Symbols

Varied, Non-Sequential Numbers

No Dictionary Words

Examples of Weak Passwords

B0u#L

Too Short


spidercat9

Contains Dictionary Words

xcf01234

Has Sequential Numbers

General Rules for Password Confidentiality

- 
1. Each user should have unique login credentials. ✓
 2. Password should be strong. Rules must be enforced by website to ensure strong passwords. ✓
 3. Passwords should not be shared with anyone. ✓
 4. Passwords should be changed regularly. ✓
 5. User accounts inactive for specific time frame should be suspended. ✓
 6. User accounts after specific session duration should ask for re-login. ✓
 7. Continuous wrong password tries should lock the account. ✓
 8. Passwords should not be shared with anyone. ✓
 9. For high risk system, any violation should be reported to concerned person. ✓

LIKE



COMMENT



SHARE



SUBSCRIBE



How Keystroke Logging Works

- Keystroke logging is an act of tracking and recording every keystroke entry made on a computer, often without the permission or knowledge of the user. A “keystroke” is just any interaction you make with a button on your keyboard.
- Keystrokes are how you “speak” to your computers. Each keystroke transmits a signal that tells your computer programs what you want them to do.
- These commands may include:
 - Length of the keypress
 - Time of keypress
 - Velocity of keypress
 - Name of the key used

Software Keylogger:

1. Definition:

- **Software keyloggers** are programs or scripts that are installed on a computer or device to monitor and record keystrokes.

2. Installation:

- **Remote Installation:** Some software keyloggers can be installed remotely by exploiting vulnerabilities or using social engineering techniques.
- **Local Installation:** Users may inadvertently install software keyloggers by downloading infected files or clicking on malicious links.

3. Functionality:

- **Keystroke Logging:** Records every keystroke made on the infected device.
- **Screen Capture:** Some advanced software keyloggers capture screenshots or record the screen activity.
- **Clipboard Logging:** Captures data copied to the clipboard.

4. Detection and Prevention:

- **Antivirus Software:** Regularly updated antivirus programs can detect and remove known software keyloggers.

Hardware Keylogger:

1. Definition:

- **Hardware keyloggers** are physical devices connected between the computer keyboard and the computer itself, intercepting and logging keystrokes.

2. Physical Connection:

- **Inline Devices:** Hardware keyloggers are often small and discreet, resembling connectors or adapters, and are connected between the keyboard and the computer.
- **Wireless Devices:** Some advanced hardware keyloggers use wireless technology to transmit captured data.

3. Functionality:

- **Undetectable by Software:** Since hardware keyloggers operate at the hardware level, they are often undetectable by antivirus or anti-malware software.
- **No Software Installation:** Does not rely on software to function, making it difficult to detect through traditional means.
- **Non-Volatile Memory:** Some devices have non-volatile memory to store logged data even when disconnected from the target device.



Anti Key Logger

- An anti-keylogger is a type of software or security tool designed to detect and prevent the activity of keyloggers on a computer or device.

- The primary purpose of anti-keyloggers is to protect sensitive information such as passwords, usernames, credit card numbers, and other confidential data from being captured and recorded by malicious keylogging software.

1. Detection of Keylogging Activity:

- Anti-keyloggers actively monitor system behavior to identify patterns associated with keylogging activities. They look for signs of suspicious behavior, such as capturing keystrokes, recording clipboard data, or taking screenshots.

2. Real-time Protection:

- Many anti-keyloggers provide real-time protection by actively scanning and analyzing the behavior of running processes and applications. They can identify and block keyloggers before they have a chance to capture sensitive information.

3. Signature-Based Detection:

- Some anti-keyloggers use signature-based detection methods to recognize known patterns or signatures associated with existing keyloggers. This approach relies on a database of known keyloggers that is regularly updated.

4. Behavioral Analysis:

- Anti-keyloggers may employ behavioral analysis techniques to identify suspicious activities based on the behavior of programs. This involves looking at how programs interact with the system and whether their actions resemble those of typical keyloggers. ✓

Spywares



- **Spyware** is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent. A commonly accepted spyware definition is a strand of malware designed to access and damage a device without the user's consent.
- Spyware collects personal and sensitive information that it sends to advertisers, data collection firms, or malicious actors for a profit. Attackers use it to track, steal, and sell user data, such as internet usage, credit card, and bank account details, or steal user credentials to spoof their identities.
- Spyware is one of the most commonly used cyberattack methods that can be difficult for users and businesses to identify and can do serious harm to networks. It also leaves businesses vulnerable to data breaches and data misuse, often affects device and network performance, and slows down user activity.

How spyware works?

1. **Install:** The spyware is secretly placed on a device through methods like downloading an app, visiting a harmful website, or opening a malicious file attachment.
2. **Observe and Collect:** Once in place, the spyware silently watches the user's online activities, recording data like usernames, passwords, and other sensitive information. It uses techniques like taking screenshots, logging keystrokes, and using tracking codes.
3. **Exploit or Sell:** The attacker then decides how to use the gathered data. They might exploit it by impersonating the user, launching cyber attacks, or use it for other malicious purposes. Alternatively, they may sell the stolen data to third parties for financial gain, including data organizations, other hackers, or on the dark web.

Types of Impact

1. Data Theft:

- **Description:** Spyware commonly leads to data theft, where personal information is taken without consent.
- **Impact:** Stolen data may be sold to third parties, hackers, or organizations for various purposes.

2. Identity Fraud:

- **Description:** Spyware, if it gathers enough data, can lead to identity fraud.
- **Impact:** Attackers can use stolen information, such as login credentials and browsing history, to impersonate the user online.

3. Device Damage:

- **Description:** Poorly designed spyware can harm the computer it infects.
- **Impact:** Drains system performance, consumes internet bandwidth, memory, and processing power. It can cause crashes, disable security software, and even lead to permanent damage to the computer.

LIKE



COMMENT



SHARE





SUBSCRIBE




SQL Injection Attack

- SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application.
- Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database.
- They can also use SQL Injection to add, modify, and delete records in the database.
- An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle etc



```
SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'
```

Because of the `OR 1=1` statement, the `WHERE` clause returns the first `id` from the `users` table no matter what the `username` and `password` are. The first user `id` in a database is very often the administrator. In this way, the attacker not only bypasses authentication but also gains administrator privileges. They can



Steps

1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc. The attacker also looks for the webpages that display the HTML commands such as POST or GET by checking the site's source code.
2. To check the source code of any website, right click on the webpage and click on "view source", source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for "FORM" tag in the HTML code. Everything between the <FORM> and </FORM> have potential parameters that might be useful to find the vulnerabilities.
3. The attacker inputs a single quote under the text box provided on the webpage to accept the username and password. This checks whether the user-input variable is sanitized or interpreted literally by the server. If the response is an error message such as use "a"="a" (or something similar) then the website is found to be susceptible to an SQL injection attack.
4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

1. Input validation

- Replace all single quotes (escape quotes) to two single quotes.
- Sanitize the input: User input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously. For example, character sequences such as ; , --, select, insert and xp_ can be used to perform an SQL injection attack.
- Numeric values should be checked while accepting a query string value. Function – IsNumeric() for Active Server Pages (ASP) should be used to check these **numeric values**.
- Keep all text boxes and form fields as short as possible to limit the length of user input.

2. **Modify error reports**: SQL errors should not be displayed to outside users and to avoid this, the developer should handle or configure the error reports very carefully. These errors some time display full query pointing to the syntax error involved and the attacker can use it for further attacks.

3. Other preventions

- The default system accounts for SQL server 2000 should never be used.
- Isolate database server and web server. Both should reside on different machines.
- Most often attackers may make use of several extended stored procedures such as xp_cmdshell and xp_grantlogin in SQL injection attacks. In case such extended stored procedures are not used or have unused triggers, stored procedures, user-defined functions, etc., then these should be moved to an isolated server.

LIKE



COMMENT



SHARE



SUBSCRIBE

