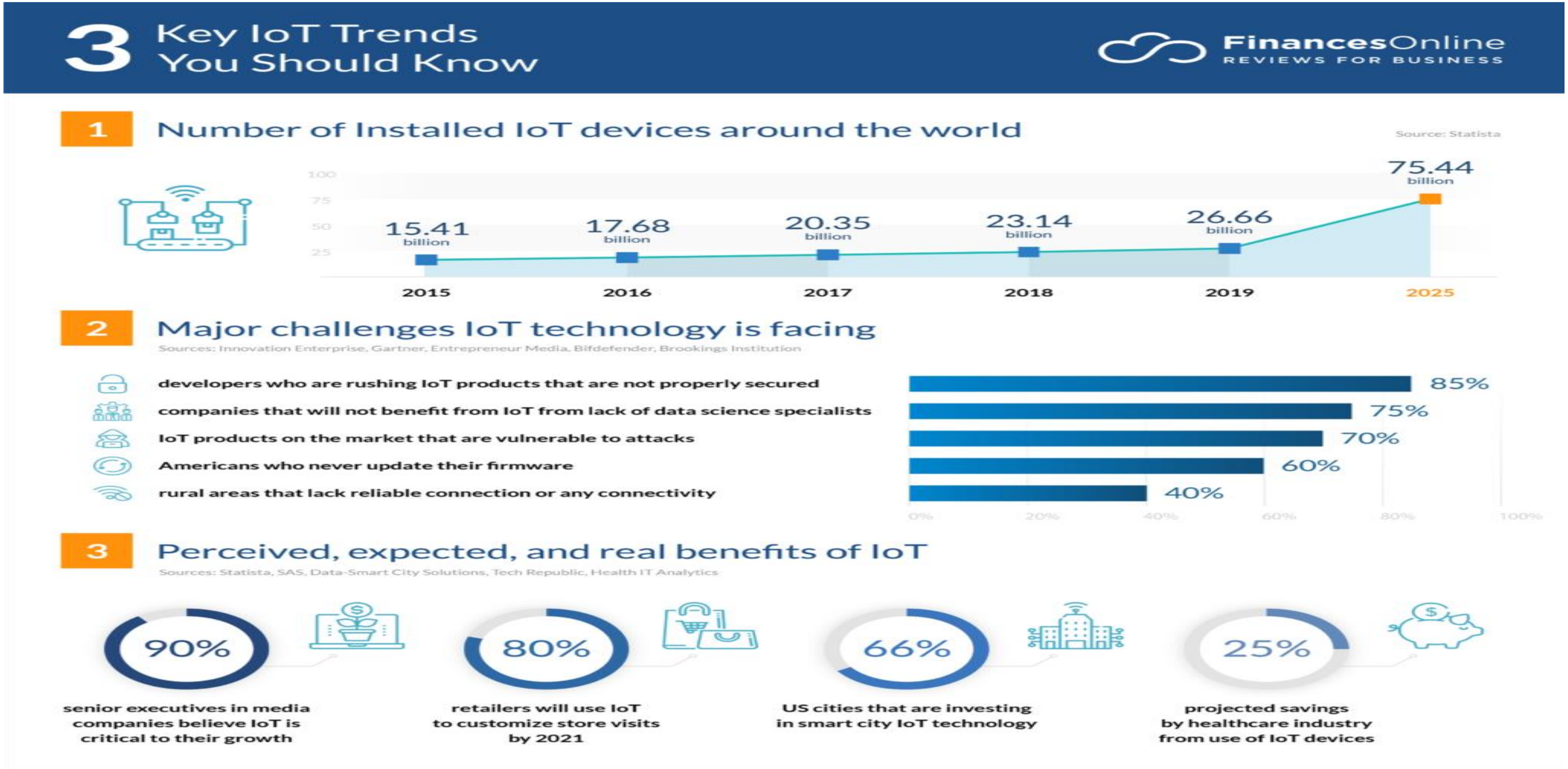
IoT Security

Agenda

- Introduction to Security in IoT Devices
- IoT Trends
- Security Goals
- Security Services
- Security Mechanisms
- IoT Vulnerabilities
- Types of Attacks in IoT environment
- IoT attack Detection Mechanisms

IoT Trends



3 Key IoT Trends You Should Know

FinancesOnline
REVIEWS FOR BUSINESS

1 Number of Installed IoT devices around the world

Source: Statista

2 Major challenges IoT technology is facing

Sources: Innovation Enterprise, Gartner, Entrepreneur Media, Bitdefender, Brookings Institution

developers who are rushing IoT products that are not properly secured	85%
companies that will not benefit from IoT from lack of data science specialists	75%
IoT products on the market that are vulnerable to attacks	70%
Americans who never update their firmware	60%
rural areas that lack reliable connection or any connectivity	40%

3 Perceived, expected, and real benefits of IoT

Sources: Statista, SAS, Data-Smart City Solutions, Tech Republic, Health IT Analytics

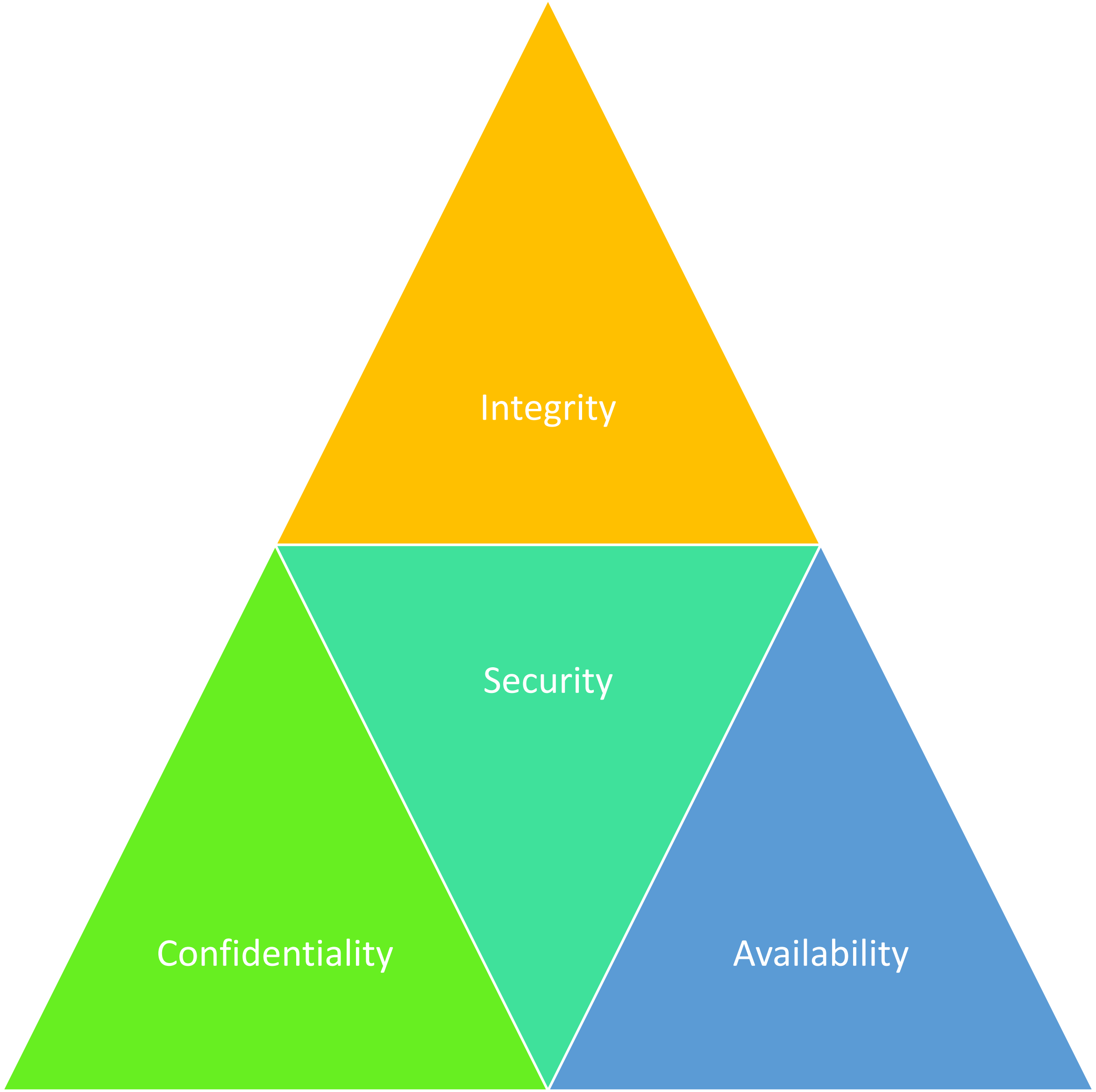
90% senior executives in media companies believe IoT is critical to their growth

80% retailers will use IoT to customize store visits by 2021

66% US cities that are investing in smart city IoT technology

25% projected savings by healthcare industry from use of IoT devices

Security Goals



Security Goals

Confidentiality: Confidentiality means protection of data or assets from the unauthorized access. It is applicable not only to the data stored in the system but also to the data in transmission .eg hiding sensitive information in military or in industry from competitors.

Integrity: Protection of data from modification of any kind like insertion, deletion and replaying by the attacker i.e only the authorized user can make changes to the data.

Availability: It means that the information should be available to the user as and when he needs it. Data is of no use if it is not available on time.

Accountability: user is taking responsibility for his or her actions or it is possible to trace the actions to the system or user so that the responsibility for those actions can be established.

Security Services

Data Confidentiality: It is designed to protect data from disclosure attack. Aim is to protect data from traffic analysis and snooping.

Data Integrity: It is designed to protect data from unauthorized modification.

Authentication: It helps in proving the authenticity of the user/party at the other end of the line. It can be done in two ways:-

- **Peer Entity Authentication:** It Proves the authenticity of the two parties during connection establishment in connection oriented communication
- **Data origin Authentication:** It Proves the authenticity of the source or origin of data in connectionless communication

Security Services

Non-repudiation: This service protects against the repudiation by either of the two parties involved in communication i.e sender and receiver. With the proof of origin, sender cannot deny sending and with the proof of delivery, receiver cannot deny the reception of data.

Access control: Here the word access can involve reading, writing, modifying and executing programs and so on and the term access control means protecting the data from unauthorised access.

Security Mechanisms

Security Mechanisms are used to provide security services. A security service may be provided by one or combination of more than one security mechanism. Various security mechanisms are:-

Encipherment: Encipherment means covering or hiding the data. It can be done using cryptography or steganography

Data Integrity: It means creating a short checkvalue from the given data using some specific process and appending that checkvalue to the message at the sender side. At the receiver side, receiver also calculates the checkvalue using received data and then compares it with the one received from the sender. If the two checkvalues are same then the data integrity is preserved.

Digital Signature: It is a means of verifying the data by the sender and receiver by signing it electronically

Security Mechanisms

Security Mechanisms are used to provide security services. A security service may be provided by one or combination of more than one security mechanism. Various security mechanisms are:-

Authentication Exchange: In authentication exchange, the sender and the receiver exchanges some messages among themselves to prove their identities to each other

Traffic Padding: It involves adding some bogus data to the original data traffic to prevent adversary from accomplishing his task of gaining unauthorised access using traffic analysis.

Routing Control: It means to select and to change continuously the routes available between the two parties to prevent eavesdropping on a specific route.

Notarization: It means appointing a third trusted party between the sender and the receiver to control the communication between them.

Access Control: It can use various methods to prove that the particular user has access to the particular data or resources. Some methods of proving access could be passwords or PINs.

How do you find
VULNERABILITIES?

Vulnerabilities

Vulnerability can be defined as the incompetency of the system which can be exploited by the attacker to attack the system security.

Common Vulnerabilities

- Deficient Physical Security
- Insufficient Energy Harvesting
- Inadequate Authentication
- Improper Encryption
- Unnecessary Open Ports
- Insufficient Access Control
- Improper Patch Management Capabilities

Deficient Physical Security

Since most of the IoT devices operate independently in an unattended environment, an adversary can very easily get physical access to the system and can take control over them.

What attacker can do after gaining physical access to the system ?

- Physical Damage to the device.
- Unveiling cryptographic scheme used
- Gain root passwords
- Modify boot parameters
- Firmware Replication using malicious node

Insufficient Energy Harvesting

As IoT devices are characterized to have low energy and also no mechanism to renew it on their own.

What an attacker can do?

Can drain the battery of the device and make it unavailable to users.

Inadequate Authentication

Due to the presence of constraints such as low computational power and limited energy, IoT devices cannot implement complex authentication mechanism because of which it is quite easy for an attacker to attack such devices.

What an attacker can do?

can append any spoofed malicious node.

Authentication keys exchanged may be corrupted.

Improper Encryption

More complex the encryption algorithm, stronger will be the cryptosystem, but the fact that IoT systems have limited resources make the encryption algorithms less effective, less efficient and less robust. .

What an attacker can do?

can easily break the cryptosystem and can gain access to the sensitive data.

Unnecessary Open Ports

Many IoT devices while running vulnerable services may have unnecessary open ports

What an attacker can do?

an attacker can connect through open ports and exploit lots of vulnerabilities.

Insufficient Access Control

A strong credential management system is required to protect data from unauthorised access. Most of the IoT devices in conjunction with their cloud management solutions do not use sufficiently complex passwords. Rather, most of the devices do not ask user to change the default user credentials after installation.

What an attacker can do?

an attacker can easily access the device

Weak Programming Practices

To minimize the attack vectors and to increase the functional capabilities of IoT devices, their operating system and the embedded firmware should be patched properly. But unfortunately most of the manufacturers do not recurrently maintain security patches.

What an attacker can do?

Can easily modify firmware

Improper Patch Management Capabilities

It has been reported by many researchers that various firmware are released with some vulnerabilities such as root users as main access point, backdoors and lack of secure socket layer usage.

What an attacker can do?

Can easily modify firmware

Can inject false data

Insufficient Audit Mechanisms

Since most of the IoT devices do not have thorough logging procedures, making it possible to hide IoT generated malicious activities.

What an attacker can do?

Various malicious activities of attacker may go un-noticed

Attacks in IoT

Types of Attacks Based on Security Goals

Any activity that threaten any security goal or that compromise the IoT device can be termed as an attack to IoT system. Attacks can be classified broadly on the basis of the security goal that they threaten:

- **Attack against confidentiality:** These types of attacks are mainly done to get unauthorized access to the data or any resource to perform further malicious actions.
- **Attack against integrity:** Attacker can make unauthorized modifications to the data
- **Attack against Availability:** attacker makes the system unavailable to the legitimate users.

Another Way of Categorising Attacks

Active Attacks

- may change the data or harm the system.
- threaten the integrity and availability
- are normally easier to detect than to prevent, because an attacker can launch them in a variety of ways.
- Cannot be prevented by using encipherment
- Eg. Firmware modification, False data injection

Passive Attacks

- The attacker’s goal is just to obtain information.
- does not modify data or harm the system.
- threaten confidentiality
- Difficult to detect
- can be prevented by encipherment of the data.
- eg. snooping and traffic analysis are passive attacks.

Attack Against Confidentiality

Various attacks that threaten the confidentiality are:

- Snooping/Eavesdropping:
- Traffic Analysis
- Dictionary Attack
- Side Channel Attack
- Sybil Attack

Snooping/Eavesdropping

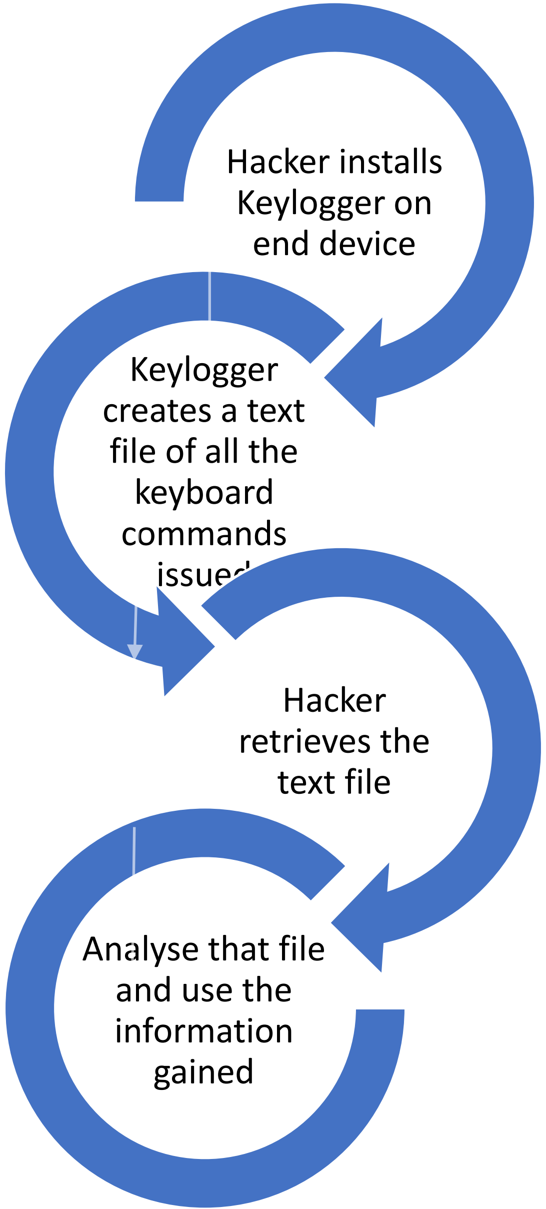
Snooping or Eavesdropping means unauthorized access to or inception of data.

It may include activities from just watching the emails that appear on victim’s computer screen, to examining his keystrokes.

More sophisticated snooping attack may include use of software tools for examining the user’s activities remotely or examining the data when the data is in motion.

An example of such tool is ***Keylogger,*** which is a software used to observe keystrokes including sensitive information such as login credentials and password of the victim.

Snooping/Eavesdropping



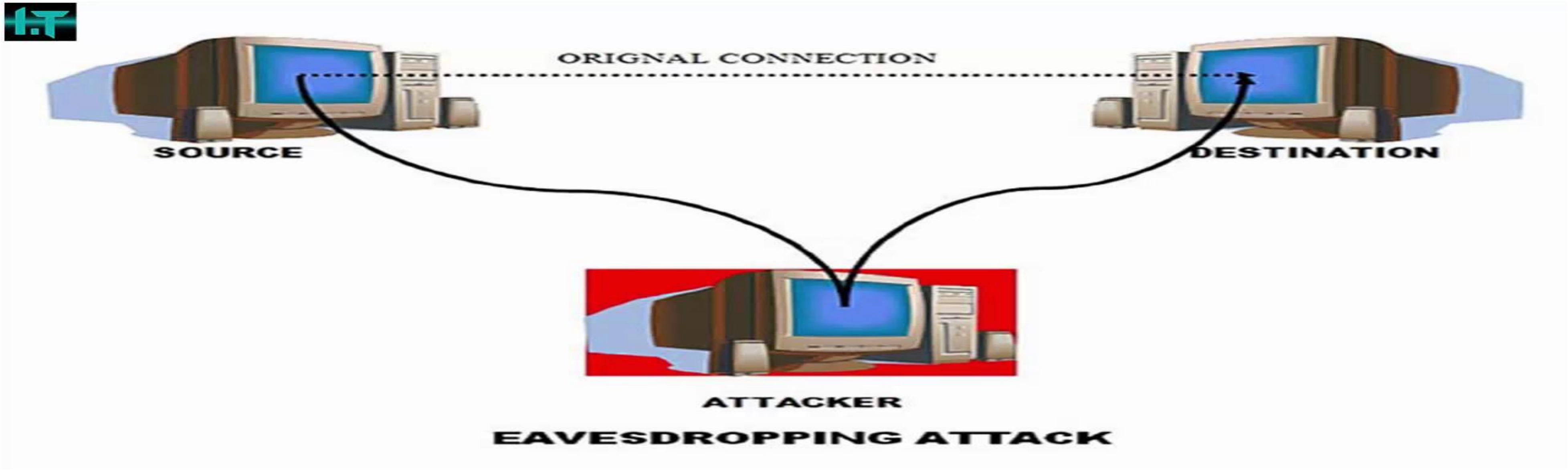
Hacker installs Keylogger on end device

Keylogger creates a text file of all the keyboard commands issued

Hacker retrieves the text file

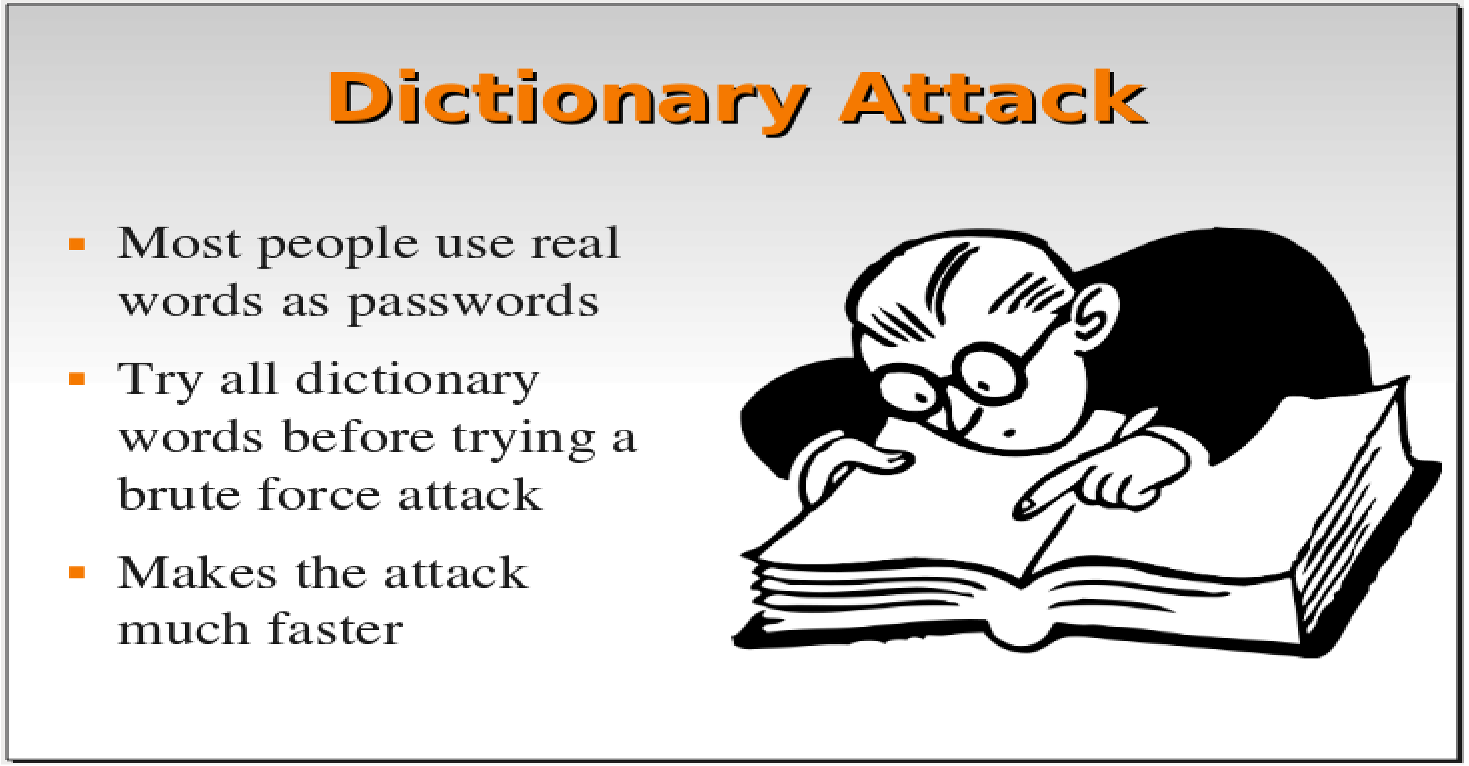
Analyse that file and use the information gained

Snooping/Eavesdropping



Dictionary Attack

- Dictionary Attack aims to gain illicit access IoT devices by using restricted subset of keyspace.
- It may involve trying millions of possibilities which may be obtained from past security breaches.

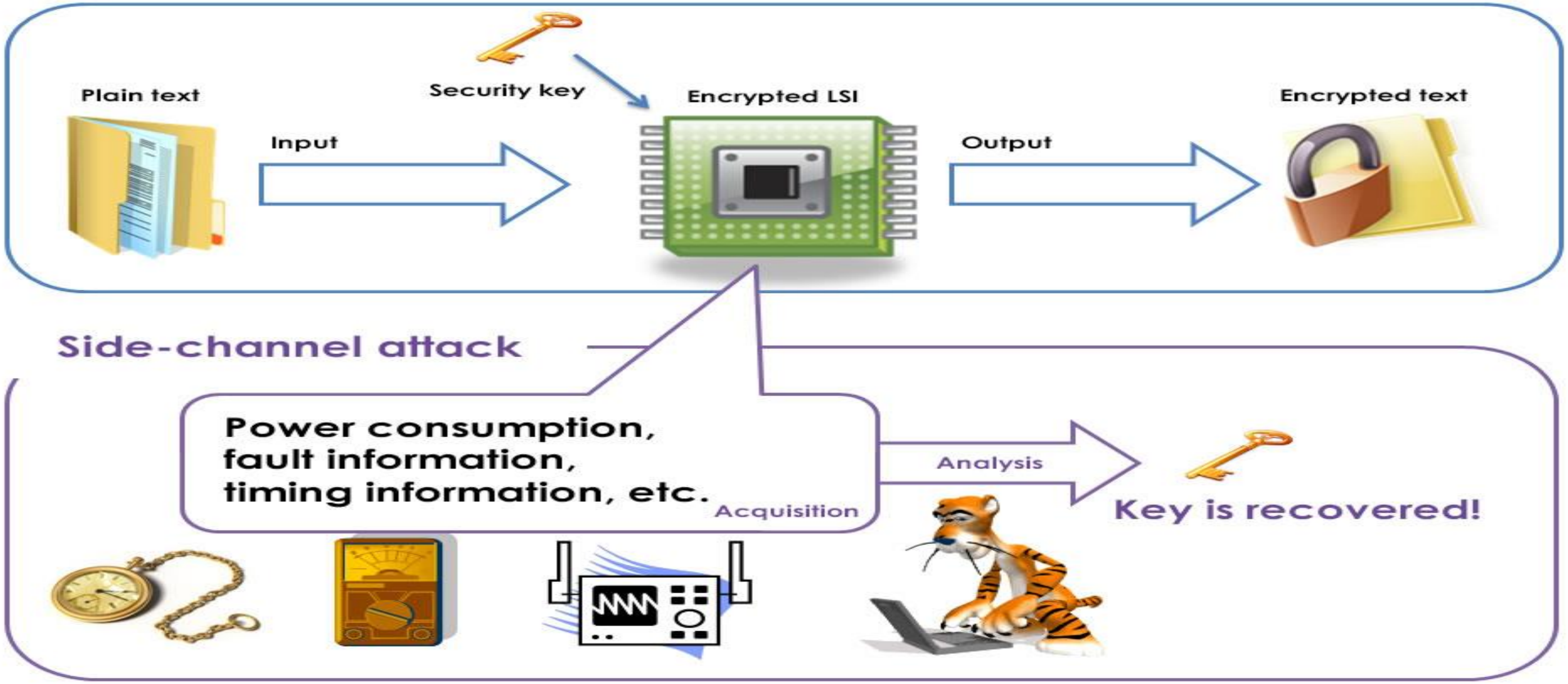


Dictionary Attack

- Most people use real words as passwords
- Try all dictionary words before trying a brute force attack
- Makes the attack much faster

Side Channel Attack

- Side channel attack refers to attack strategy where the attacker exploits the extra information related to the way a particular protocol or algorithm is implemented.
- This extra information could be power consumption, timing information, sound, electromagnetic leaks etc.



Side Channel Attack

Timing Attack: In timing attack, an adversary tries to attack the cryptosystem by analysing on how much time does an algorithm take to execute. Each logical operation in computer takes some time to execute which can differ depending on the input provided. By measuring the time accurately for each operation, attacker can use backward approach to determine the input.

Cache Attack: Here, attacker can monitor the cache accesses done by the victim in a shared physical system such as virtualized environment or a type of cloud service.

Power monitoring attack: This attack can be performed by analysing the power consumption by the hardware during computation.

Electromagnetic attack: These attacks are based on leaked electromagnetic radiation, that can directly give plaintext or other information.

Sybil Attack

In sybil attack a single entity (or device) can create or operate as multiple identities (accounts based on IP addresses, user accounts)in peer to peer network.

To the rest of the world, these different fake identities appears to be genuine identities.

Attacks Against Data Integrity

- False Data Injection Attack
- Firmware Modification Attack
- Cross Channel Scripting Attack

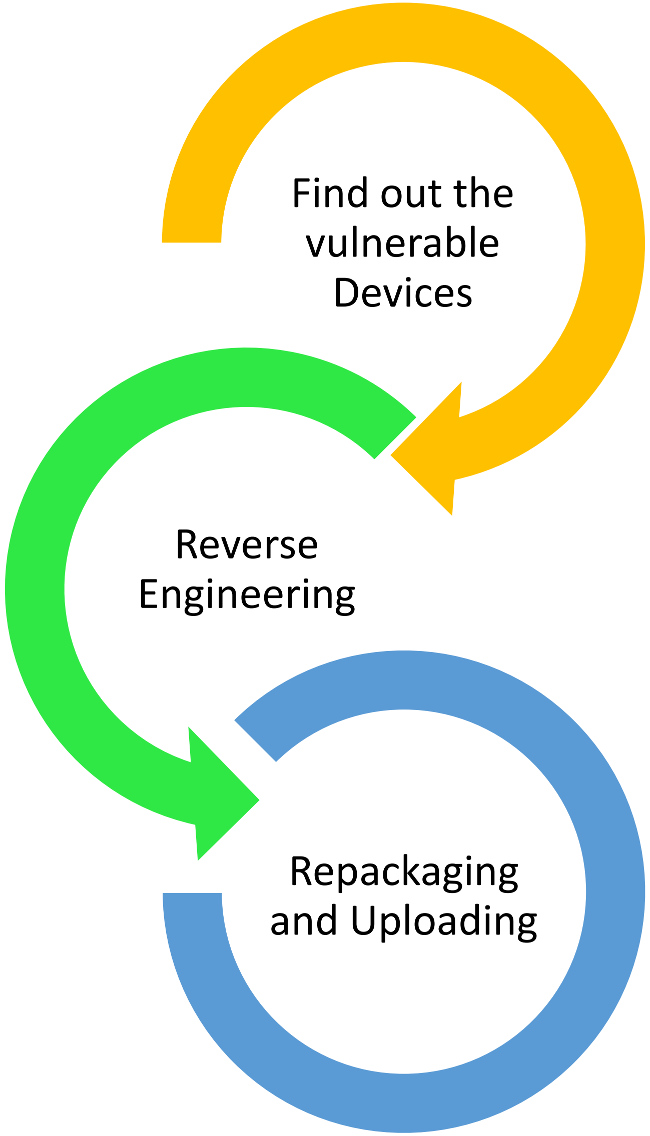
False Data Injection Attack

In FDI , an attacker injects some malicious data to the IoT sensor due to which various integrity violations may occur.

For example, injecting false data may lead to incorrect estimation of the state of the device employed in some critical environment.

Firmware Modification Attack

As the name suggests, firmware modification means maliciously changing the firmware of the system to change the functionality of the system.



Cross Channel Scripting (CCS Attack)

is a Java Script code injection attack that permits an attacker to execute injected JavaScript in victim's web browser in order to gain access to the sensitive resources like cookies, password, credit card numbers etc.

is an attack on the client-side web browser, but its capabilities are exploited on the web server side.

This script is injected in such a way that it seems to be benign component of the website and finally this script is executed within the domain of the trust of the website.

This is possible only if the web application accepts an input from the user-side into its web pages because an attacker can inject a malicious JavaScript string that will be reflected as a code on the browser of victim

Attack Against Data Integrity

Various attacks possible against data integrity are:-

1. **Modification:** The attacker after gaining access to the data can modify it for his own benefits. Eg. an attacker can intercept the transaction request from user to the bank and then modify that request for his benefit
2. **Masquerading/spoofing:** an attacker impersonates as somebody else. Eg. an attacker somehow manages to get the bank card and PIN and then he pretends that he is that customer in front of the bank.
3. **Replaying:** an attacker gets a copy of the message and then he replays the same message later on. Eg. Bob requests his bank to transfer some money from his account to Eve's account, Eve intercepts that message and then tries to replay it again in the future.

Attack Against Data Integrity

Various attacks possible against data integrity are:-

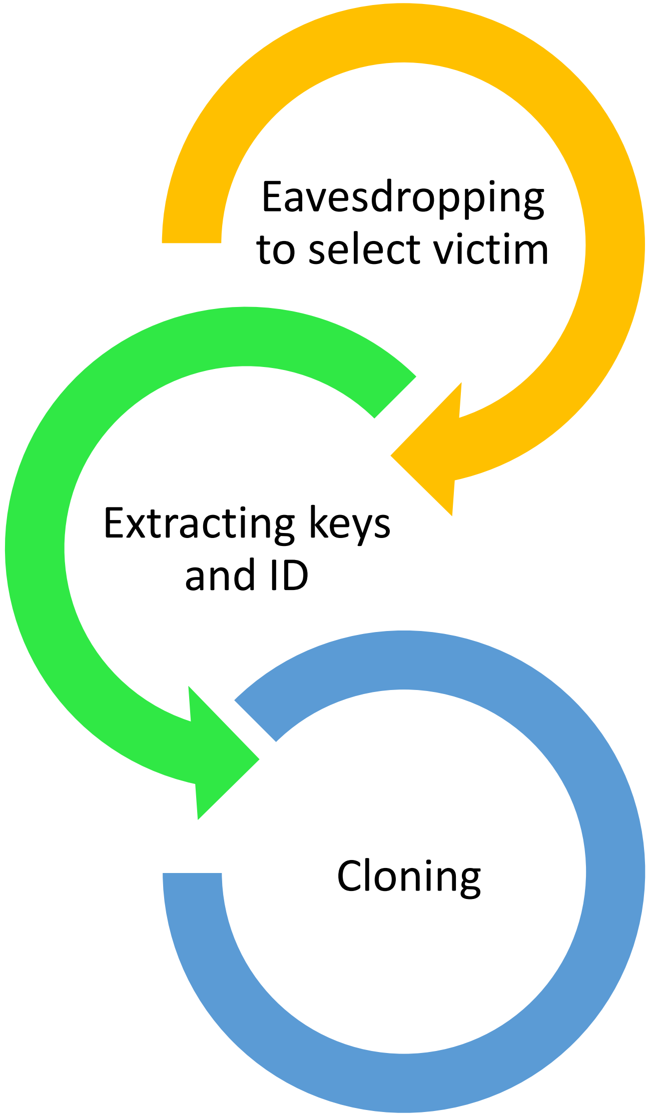
4. **Repudiation:** Repudiation means either the sender is denying the fact that he has sent the message or the receiver is denying the fact that he has received the message.
5. **False Data Injection (FDI):** In FDI data integrity can be violated by fusing some legal or corrupted data to the IoT sensor. For example if FDI leads to incorrect estimation of the state of the IoT device it can cause very damaging effects and in extreme case it can even cost human life.
6. **Firmware Modification Attack:** Such types of attacks makes malicious changes to the firmware of the device leading to the functional disruption of the victim device

Attack Against Availability

- Device/node Capture
- Routing Attack
- Denial of Service(DoS)
- Distributed Denial of Service(DDoS)
- Battery Draining Attack

Node/Device Capture

In node capture attack, an adversary can gain physical access to the device which are usually placed in a hostile environment



Routing Attack

An adversary degrades the performance of the network by modifying the network topology. Malicious node is given the power to advertise an artificial routing path containing large number of nodes in order to compel them to send packets through such fake paths. Various kinds of Routing attacks are:

- Sinkhole Attack
- Blackhole Attack
- Wormhole Attack
- Rank Attack
- Sybil or clone ID
- HELLO flooding Attack

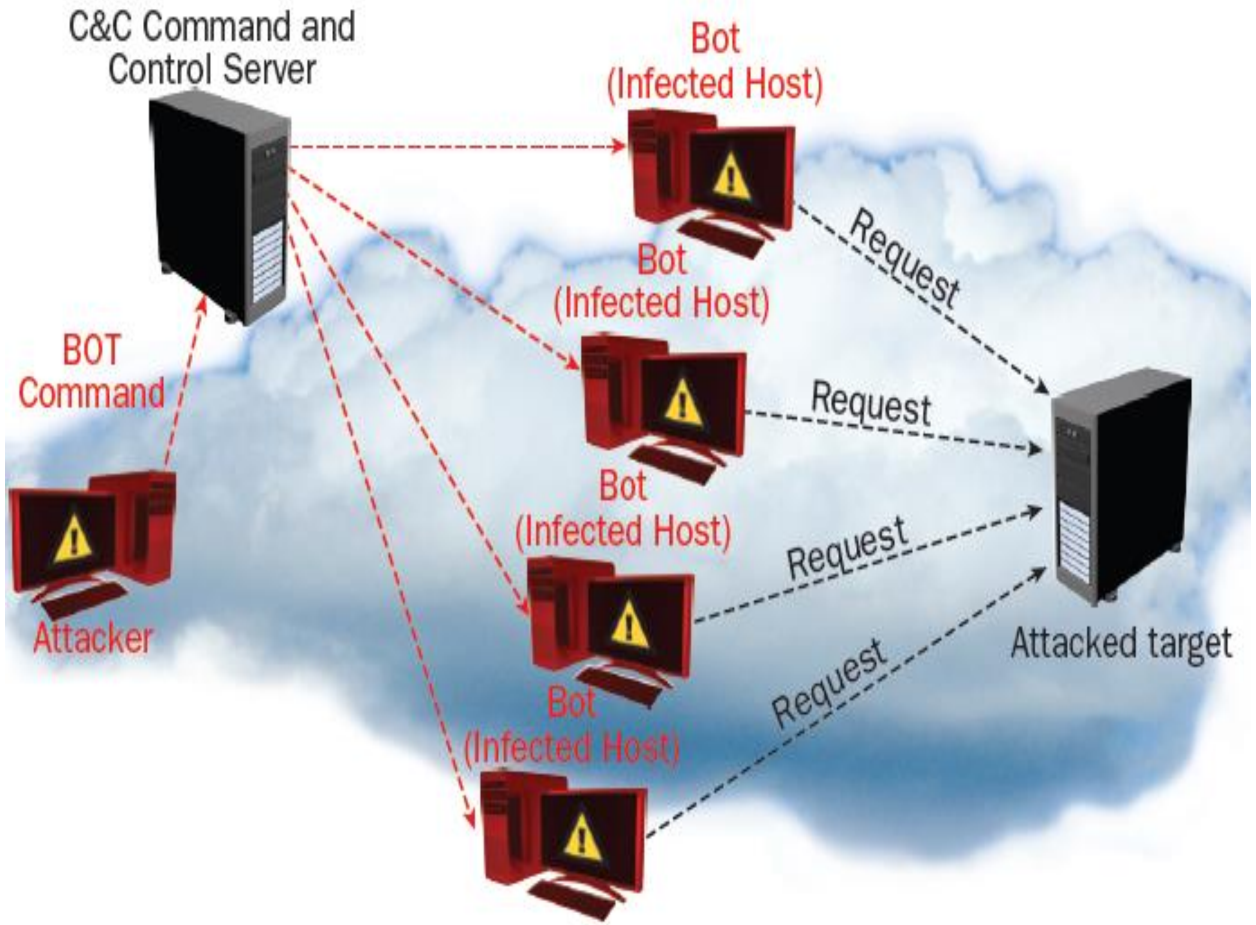
Denial Of Service Attack

DoS attack is an attack strategy in which an attacker overwhelms the resources of the victim's system to such an extent that the attacked system is not able to provide any service or resources to the legitimate users.

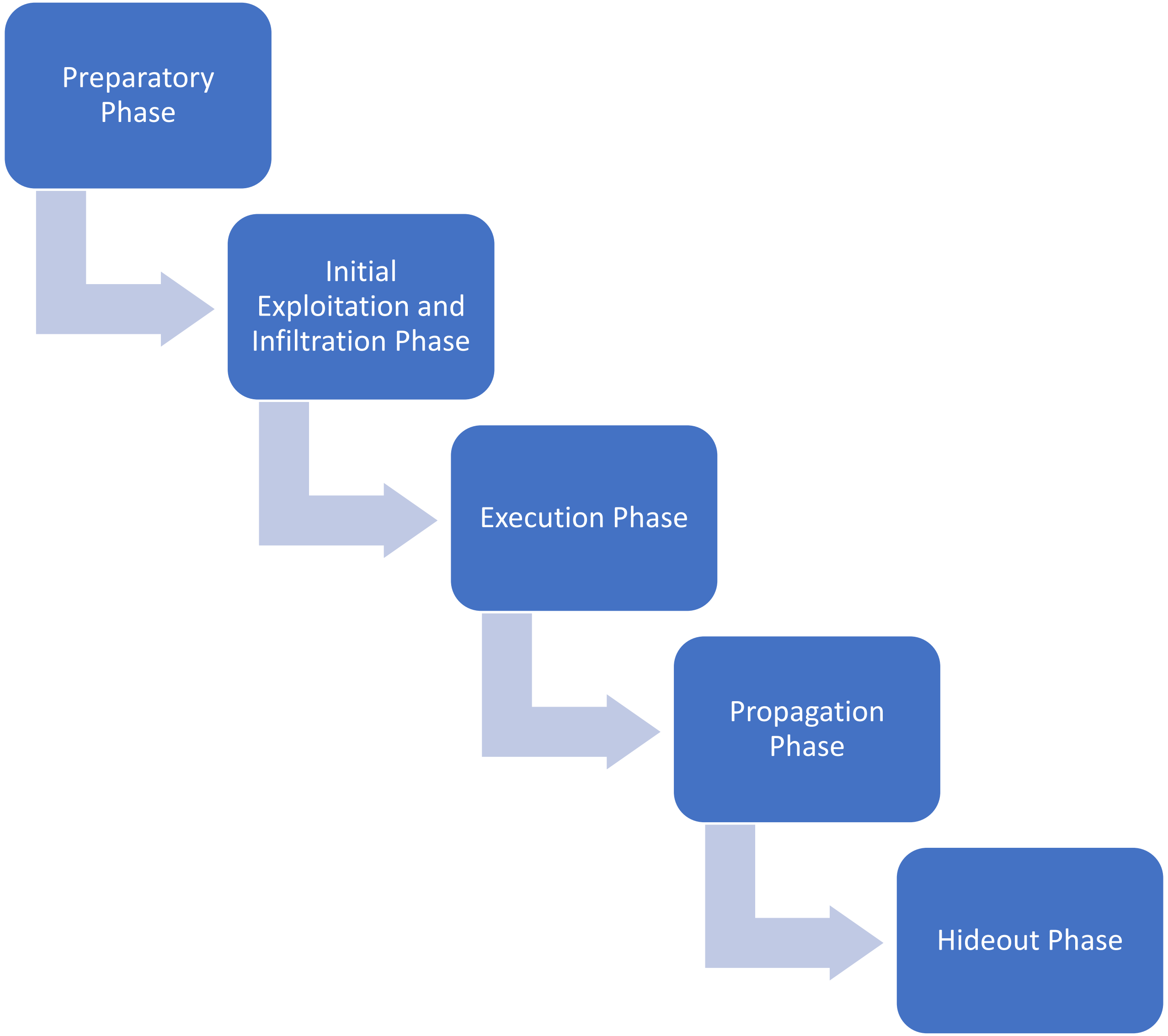
It affects the availability of the system.

DDoS Attack

In Distributed Denial of Service(DDoS) attack, resources of the victim system are flooded with the multiple requests from the large number of malware infected bots, so that the victim becomes unavailable to the legitimate users.



DDoS Attack Methodology



Preparatory Phase

Initial Exploitation and Infiltration Phase

Execution Phase

Propagation Phase

Hideout Phase

DDoS Attack Methodology

1. **Preparatory Phase:** Attacker examines the target system and check for the devices with vulnerabilities, these vulnerabilities could be use of default credentials, unnecessary open ports, device hardware or software weaknesses etc.
2. **Initial Exploitation and Infiltration Phase:** Malware enters the vulnerable device and then tries to login using Brute force technique
3. **Execution Phase:** Steps taken by malware in execution phase

- Download the additional payload from the server and delete any other malware present in the system.
- reconfigure the device to make it a part of Botnet,
- execute the downloaded malware binary and
- finally perform the particular malicious task.

Bot communicates with the controller regularly.

Types of DDoS Attack

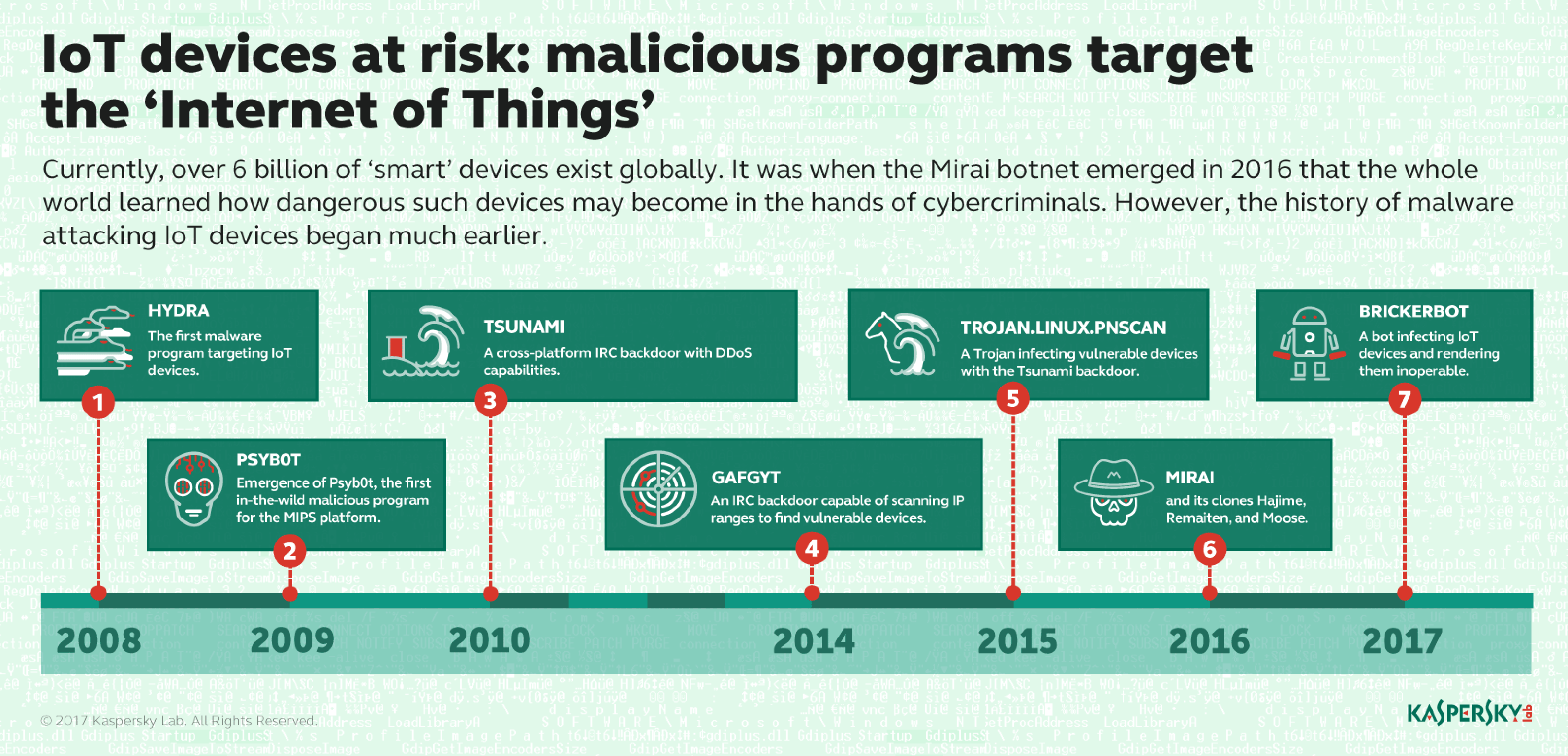
Volumetric/Flooding Attack

Amplification Attack

Protocol Exploit

Logical/Software Attack

Malware Attack



IoT devices at risk: malicious programs target the ‘Internet of Things’

Currently, over 6 billion of ‘smart’ devices exist globally. It was when the Mirai botnet emerged in 2016 that the whole world learned how dangerous such devices may become in the hands of cybercriminals. However, the history of malware attacking IoT devices began much earlier.

1 2008 — **HYDRA**: The first malware program targeting IoT devices.

2 2009 — **PSYB0T**: Emergence of Psyb0t, the first in-the-wild malicious program for the MIPS platform.

3 2010 — **TSUNAMI**: A cross-platform IRC backdoor with DDoS capabilities.

4 2014 — **GAFGYT**: An IRC backdoor capable of scanning IP ranges to find vulnerable devices.

5 2015 — **TROJAN.LINUX.PNSCAN**: A Trojan infecting vulnerable devices with the Tsunami backdoor.

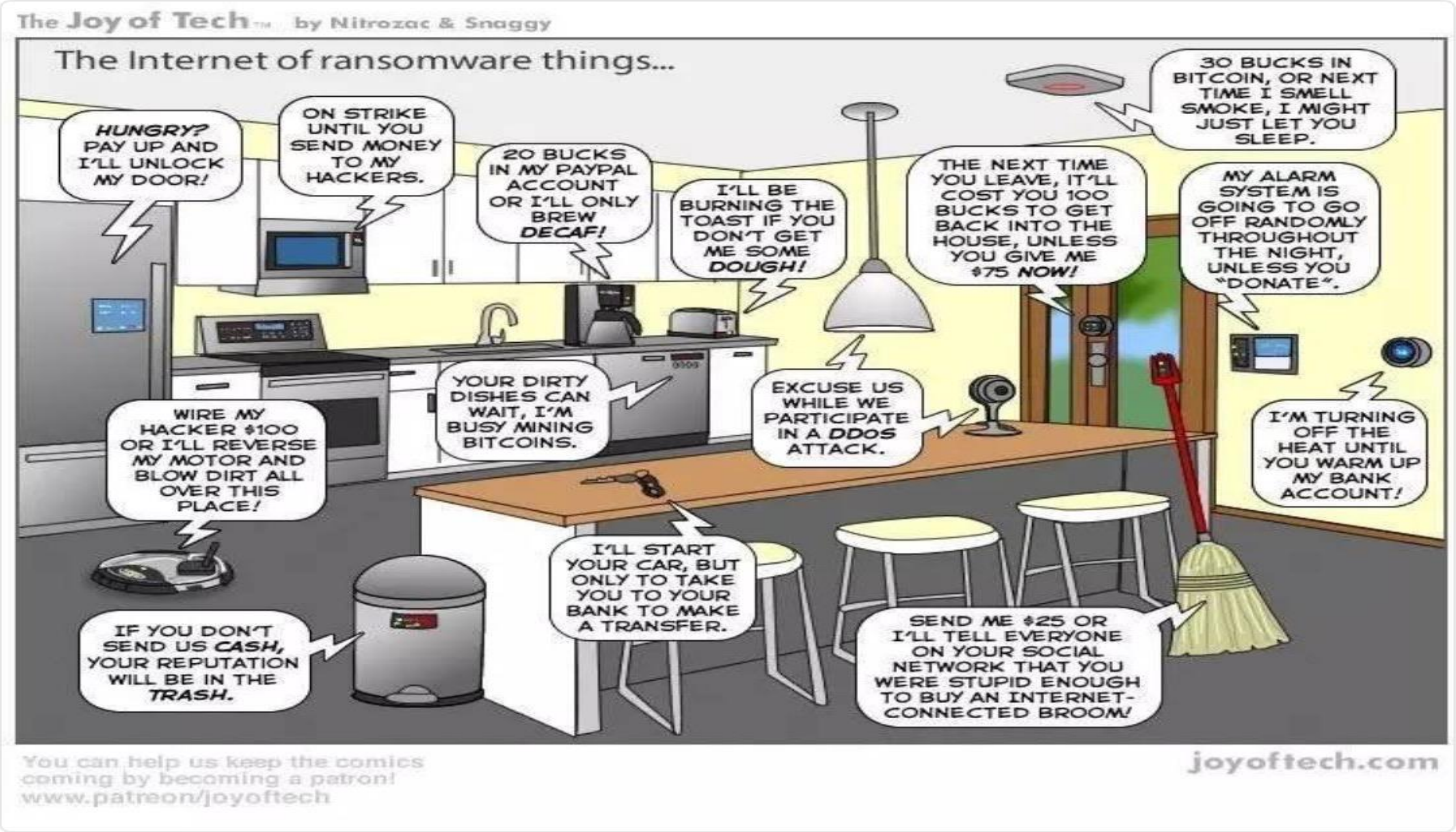
6 2016 — **MIRAI**: and its clones Hajime, Remaiten, and Moose.

7 2017 — **BRICKERBOT**: A bot infecting IoT devices and rendering them inoperable.

Ransomware Attack

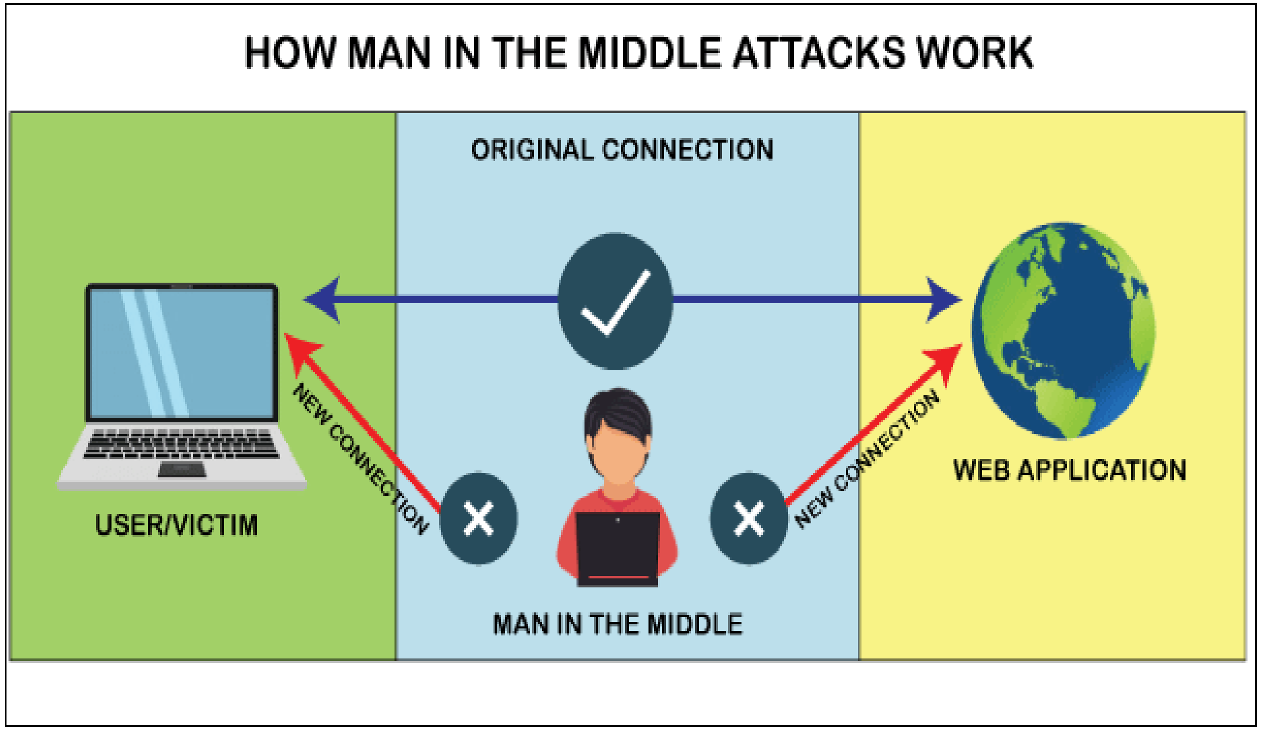
It is a kind of malware attack, where the attacker takes hold of some file, folder or an entire device forcibly and does not release it until the ransom amount is paid.

It is one of the most common cyberattacks.


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

Man In The Middle (MITM) Attack

MITM occurs when a threat actor inserts himself between two parties, often a user and an application, to intercept their communications and data transfers and utilize them for nefarious ends such as making unauthorized purchases or hacking.



Traditional Defence Mechanisms

Filter Packets

Adopt Encryption

Employ Robust password Authentication Scheme

Audit and log Activities

Use Intrusion Detection System

Prevent Intrusion Using Intrusion prevention System

Thank you