

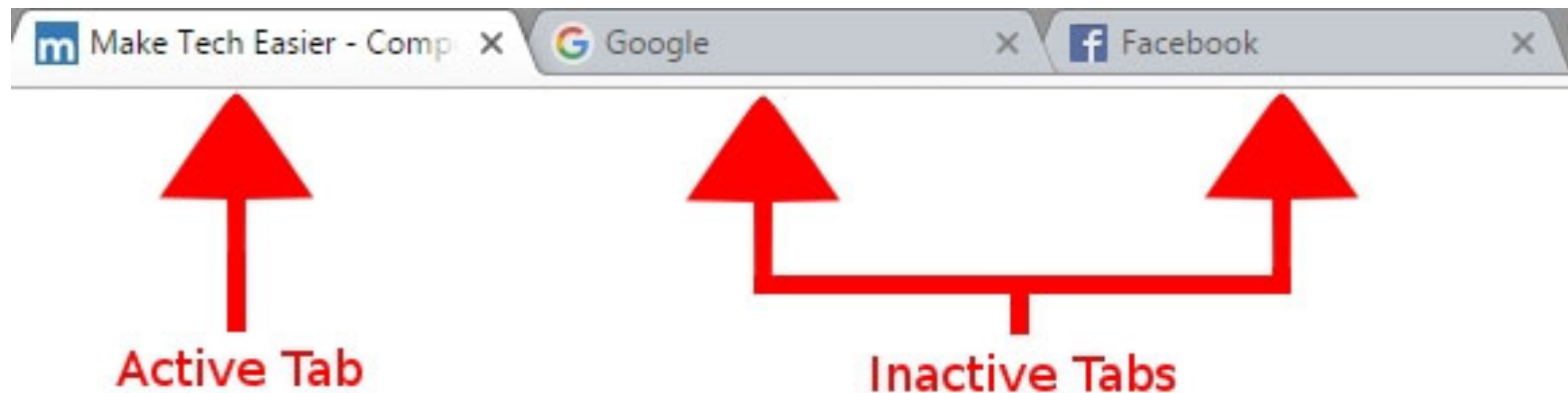
# Tabnapping

---

- ❑ Tabnapping/Tabnabbing/Tabnagging
- ❑ The word '*Tab Napping*' comes from the combination of 'tab' and 'kidnapping'.
- ❑ Most Internet users know to watch for the signs of a traditional phishing attack: An e-mail that asks you to click on a link and enter your e-mail or banking credentials at the resulting Web site. But a new phishing concept that exploits user inattention and trust in browser tabs is likely to fool even the most security-conscious Web surfers.

## Tabnapping cont...

- A user has multiple tabs open including gmail. Then the user surfs to gmail site and enter his credential and does some stuff then goes to another tab after he is done with his emails.
- Attacker sets up a website that looks completely normal like gmail. Within the websites code, they place a checker to see if the tab has become “inactive/dormant.” Inactive tabs are tabs that you’re not currently looking at.

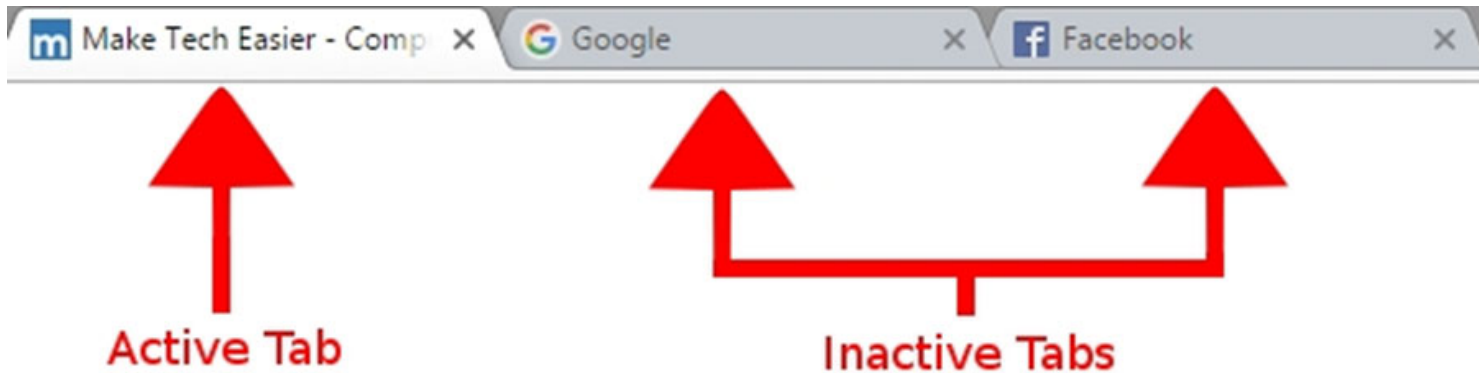


## Tabnapping cont...

---

- ❑ The fake page makes sure the **tab has been inactive for a sufficient amount of time**, to make sure you've forgotten about it. **Once the waiting time has expired**, it first **changes the website's content to a fake login page**, Gmail, for instance. It then changes the "favicon" of the site, which is the little picture icon you see on tabs.
- ❑ It uses **special JavaScript code** to **silently alter** the contents of a tabbed page along with the information displayed on the tab itself, so that when the user switches back to that tab it appears to be the login page for a site the user normally visits.
- ❑ Your original Gmail tab page URL will be replaced by fake page. **You will think your account is logged out automatically. You will again Login** your account and hacker will get your password you will be redirected to original facebook.com.

## Tabnapping cont...



Before:



After 5 Seconds:



## Tabnapping cont...

---

- Tips to protect you against tab napping
  - Make sure you **always check the URL** in the browser address page is correct before you enter any login details. A fake tabbed page will have a different URL to the website you think you're using.
  - Always check the URL has a secure **https://** address even if you don't have tabs open on the browser.
  - If the **URL looks suspicious** in any way, close the tab and reopen it by entering the correct URL again.
  - Avoid **leaving tabs open which require you to type in secure login** details. Don't open any tabs while doing online banking - open new windows instead.

# Whois

---

- Whois database includes the following information:
  - Names
  - Telephone numbers
  - Email addresses
  - Name (DNS) servers
- Once registrar is known, attacker can contact it.



# hsu.ac.ir

Updated 16 days ago

```
% This is the IRNIC Whois server v1.6.2.
% Available on web at http://whois.nic.ir/
% Find the terms and conditions of use on http://www.nic.ir/
%
% This server uses UTF-8 as the encoding for requests and responses.

% NOTE: This output has been filtered.

% Information related to 'hsu.ac.ir'
```

```
domain:          hsu.ac.ir
ascii:           hsu.ac.ir
remarks:         (Domain Holder) Hakim Sabzevari University
remarks:         (Domain Holder Address) Tohid shahr, pardis daneshgahe
holder-c:        ha1868-irnic
admin-c:         ha1868-irnic
tech-c:          ha1868-irnic
nserver:         ns1.hsu.ac.ir
nserver:         ns2.hsu.ac.ir
last-updated:    2017-05-03
expire-date:     2022-05-01
source:          IRNIC # Filtered

nic-hdl:         ha1868-irnic
org:             Hakim Sabzevari University
e-mail:          hosseini@sttu.ac.ir
address:         Tohid shahr, pardis daneshgahe hakim sabzevari, sabzeva
phone:           +98 51 44012636
fax-no:          +98 51 44012636
source:          IRNIC # Filtered
```



# Whois defense

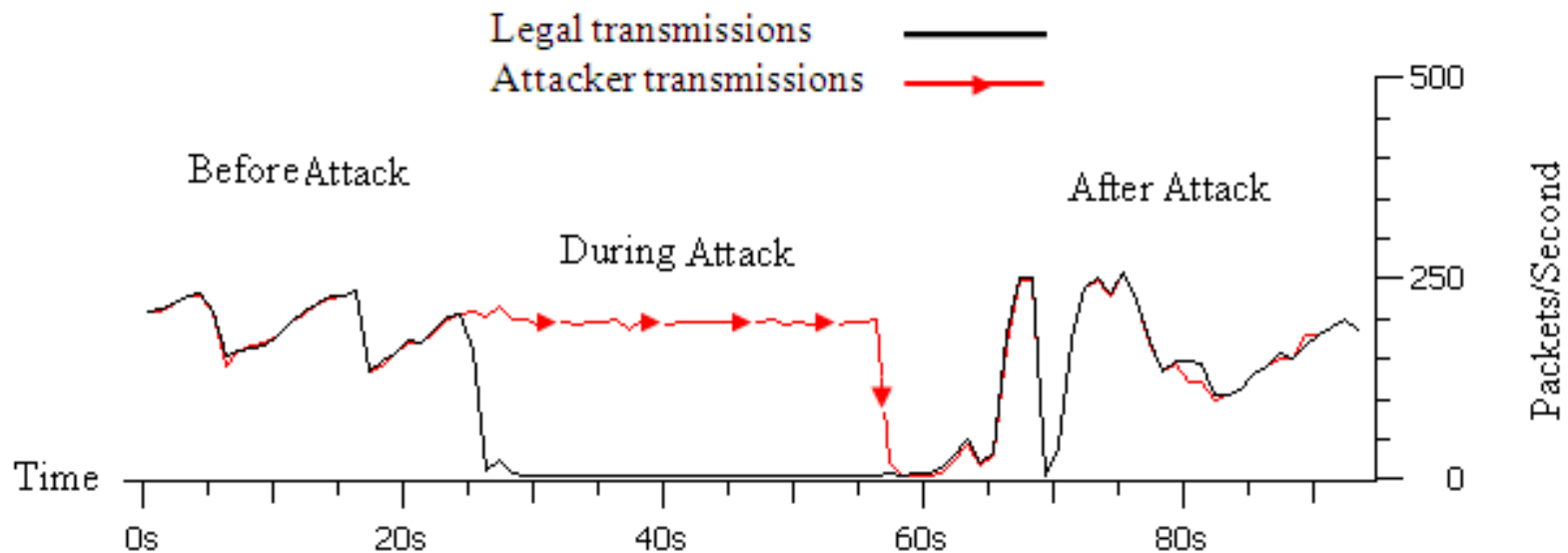
---

- ❑ To defense against whois this is **not a good idea to put false information into databases**. The reason is that **those information are important for people to contact you**. For example, **if your network is under attack**, it is possible to analyze source address of the packets. Then whois database is used **to obtain info about the domain from where the attack is coming**. In this case they can inform the administrators that their systems are source of an attack.
- ❑ In fact, there is **no real defense** against Whois so it is better to train against social engineering.

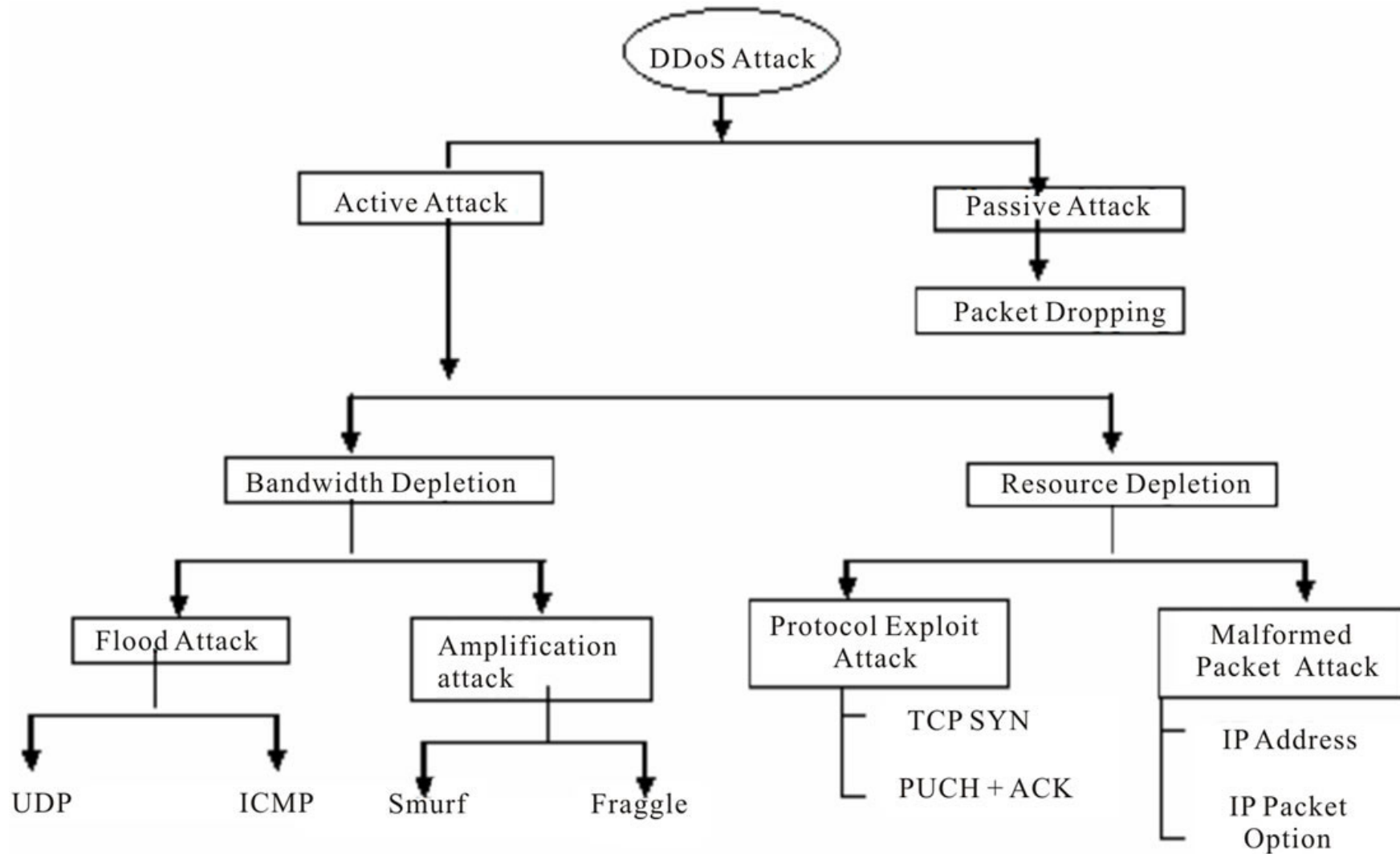


# DoS attacks

- Denial of service (DoS) attack attempts to **make a server or other network resources unavailable by flooding** it with fake requests. After a short time, the server **runs out of resources** and no longer function for its legal users.



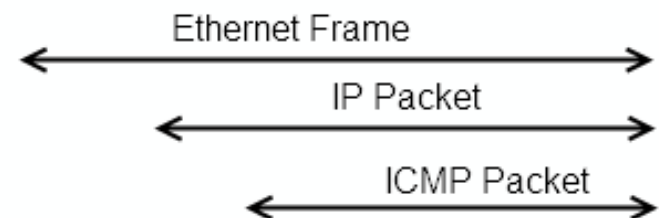
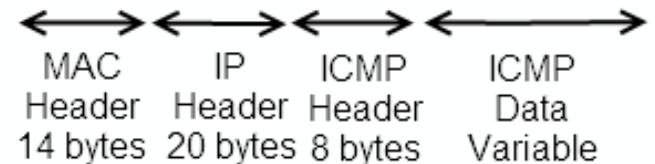
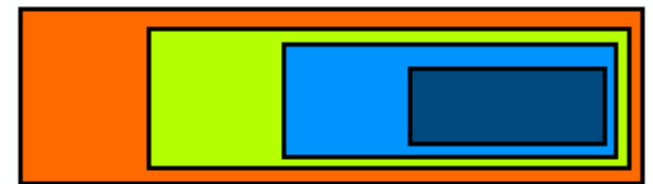
## DoS attacks cont...



# Ping of death

- The normal size of **ICMP payload is 32 bytes** which is shown in the following figure.
- To start a ping of death, the **attacker sends larger ICMP packets** (e.g. 1400 bytes). Since the received ICMP packet is larger than the normal IP packet size, it is fragmented. This causes more data to be stored results in buffer overflows or kernel dumps, so the network crashes.

ICMP Packet Overview



# Ping command

```
C:\>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] : [-k host-list]]
           [-w timeout] target_name

Options:
  -t           Ping the specified host until stopped.
               To see statistics and continue - type Control-Break;
               To stop - type Control-C.
  -a           Resolve addresses to hostnames.
  -n count     Number of echo requests to send.
  -l size      Send buffer size.
  -f           Set Don't Fragment flag in packet.
  -i TTL       Time To Live.
  -v TOS       Type Of Service.
  -r count     Record route for count hops.
  -s count     Timestamp for count hops.
  -j host-list Loose source route along host-list.
  -k host-list Strict source route along host-list.
  -w timeout   Timeout in milliseconds to wait for each reply.

C:\>ping www.google.com

Pinging www.l.google.com [173.194.67.106] with 32 bytes of data:
Reply from 173.194.67.106: bytes=32 time=2517ms TTL=39
Reply from 173.194.67.106: bytes=32 time=2133ms TTL=39
Reply from 173.194.67.106: bytes=32 time=2300ms TTL=39
Reply from 173.194.67.106: bytes=32 time=2037ms TTL=39

Ping statistics for 173.194.67.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2037ms, Maximum = 2517ms, Average = 2246ms

C:\>
```

# Ping command options

---

- ❑ **-t** = Using this option will ping the *target* until you force it to stop using Ctrl-C.
- ❑ **-n count** = This option sets the number of ICMP Echo Request messages to send. If you execute the ping command without this option, four requests will be sent.
- ❑ **-l size** = Use this option to set the size, in bytes, of the echo request packet from 32 to 65,527. The ping command will send a default size if you don't use the **-l** option.
- ❑ **-f** = Use this ping command option to prevent ICMP Echo Requests from being fragmented by routers between you and the *target*.
- ❑ **-i TTL** = This option sets the Time to Live (TTL) value, the maximum of which is 255.
- ❑ **ping -n 5 -l 1500 www.google.com**

# Before ping of death attack

No.	Time	Source	Destination	Protocol	Info
17	2.931514	192.168.1.102	255.255.255.255	UDP	Source port: 52330 Destination port: 52330
18	2.961717	192.168.1.102	255.255.255.255	UDP	Source port: 52330 Destination port: 52330
19	2.991689	192.168.1.102	255.255.255.255	UDP	Source port: 52330 Destination port: 52330
20	3.000663	fe80::49c5:fba4:36eff02::c		SSDP	M-SEARCH * HTTP/1.1
21	3.143563	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
22	3.336261	173.194.69.106	192.168.1.102	ICMP	Echo (ping) reply
23	3.882952	192.168.1.69	224.0.0.1	IGMP	V2 Membership Query, general
24	3.885710	192.168.1.69	224.0.0.1	IGMP	V2 Membership Query, general
25	3.885712	192.168.1.69	224.0.0.1	IGMP	V2 Membership Query, general
26	3.888143	192.168.1.69	224.0.0.1	IGMP	V2 Membership Query, general
27	4.145799	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
28	4.338659	173.194.69.106	192.168.1.102	ICMP	Echo (ping) reply
29	5.147787	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
30	5.340658	173.194.69.106	192.168.1.102	ICMP	Echo (ping) reply
31	5.459631	192.168.1.69	192.168.1.102	TCP	34511 > 80 [SYN] Seq=34480 win=20480 Len=0 MSS=1400
32	6.000692	fe80::49c5:fba4:36eff02::c		SSDP	M-SEARCH * HTTP/1.1

- ⊕ Frame 21: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- ⊕ Ethernet II, Src: b4:74:9f:71:8c:96 (b4:74:9f:71:8c:96), Dst: 90:e6:ba:bd:cf:82 (90:e6:ba:bd:cf:82)
- ⊕ Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 173.194.69.106 (173.194.69.106)
- ⊖ Internet Control Message Protocol
  - Type: 8 (Echo (ping) request)
  - Code: 0
  - Checksum: 0x4cc8 [correct]
  - Identifier: 0x0001
  - Sequence number: 147 (0x0093)
- ⊕ Data (32 bytes)

# Starting ping of death attack

```
C:\Windows\system32\cmd.exe - ping www.google.com -t -l 1400

C:\Users\mina>ping www.google.com -t -l 1400

Pinging www.google.com [173.194.69.106] with 1400 bytes of data:
Reply from 173.194.69.106: bytes=64 (sent 1400) time=237ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=222ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=221ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=220ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=218ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=218ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=218ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Request timed out.
Reply from 173.194.69.106: bytes=64 (sent 1400) time=220ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=222ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=229ms TTL=41
Request timed out.
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=218ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=232ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=220ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=218ms TTL=41
Request timed out.
Reply from 173.194.69.106: bytes=64 (sent 1400) time=229ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=220ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=218ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=223ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=220ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=221ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=218ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=220ms TTL=41
Request timed out.
Reply from 173.194.69.106: bytes=64 (sent 1400) time=220ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=220ms TTL=41
Reply from 173.194.69.106: bytes=64 (sent 1400) time=219ms TTL=41
```

# During ping of death attack

No.	Time	Source	Destination	Protocol	Info
32	11.365450	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
33	11.583391	173.194.69.106	192.168.1.102	ICMP	Echo (ping) reply
34	12.367166	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
35	12.585869	173.194.69.106	192.168.1.102	ICMP	Echo (ping) reply
36	13.369487	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
37	13.522465	fe80::49c5:fba4:36eff02::c		SSDP	M-SEARCH * HTTP/1.1
38	13.586961	173.194.69.106	192.168.1.102	ICMP	Echo (ping) reply
39	14.371568	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
40	14.589152	173.194.69.106	192.168.1.102	ICMP	Echo (ping) reply
41	15.374774	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
42	15.591858	173.194.69.106	192.168.1.102	ICMP	Echo (ping) reply
43	16.377577	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
44	16.595811	173.194.69.106	192.168.1.102	ICMP	Echo (ping) reply
45	16.739948	192.168.1.69	192.168.1.102	TCP	34503 > 80 [SYN] Seq=40619 win=20480 Len=0 MSS=1400
46	17.378605	192.168.1.102	173.194.69.106	ICMP	Echo (ping) request
47	17.523474	fe80::49c5:fba4:36eff02::c		SSDP	M-SEARCH * HTTP/1.1

- ⊕ Frame 32: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits)
- ⊕ Ethernet II, Src: b4:74:9f:71:8c:96 (b4:74:9f:71:8c:96), Dst: 90:e6:ba:bd:cf:82 (90:e6:ba:bd:cf:82)
- ⊕ Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 173.194.69.106 (173.194.69.106)
- ⊖ Internet Control Message Protocol
  - Type: 8 (Echo (ping) request)
  - Code: 0
  - Checksum: 0x9310 [correct]
  - Identifier: 0x0001
  - Sequence number: 128 (0x0080)
- ⊕ Data (1400 bytes)



# Defense against ping of death

---

- ❑ **Routers** should be configured to prevent creation/reception of ICMP packets of invalid size.
- ❑ **Update firewall-antivirus**

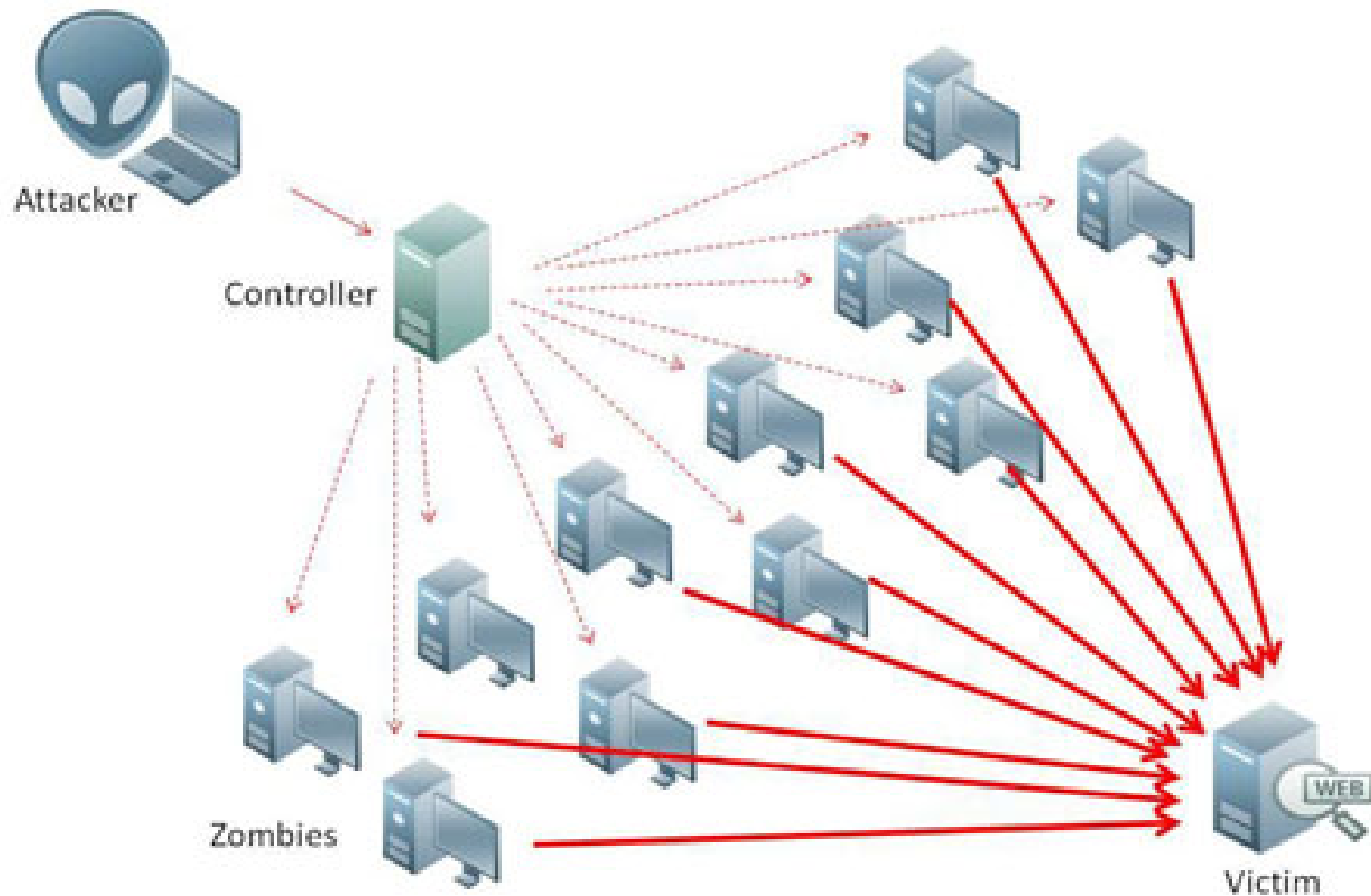
# Replay attacks

---

- ❑ The attacker monitors the network to obtain the desired packet to be retransmitted (replayed), either immediately or at later time. The aim is to cause unexpected results or to misuse the limited network resources.
- ❑ The attacker is also able to extend the replay attack into DoS attack by continuously retransmitting the captured packet to the network. Since the packet is valid, the receiver has to manage large stream of the replayed packets in a short time, which will degrade the network performance and the quality of the services.
- ❑ The important point about this attack is that, even if the network is protected by security algorithms, the network is still prone to the replay attack. Reason being, the attacker does not modify the packet, so the replayed packet is still a valid packet.

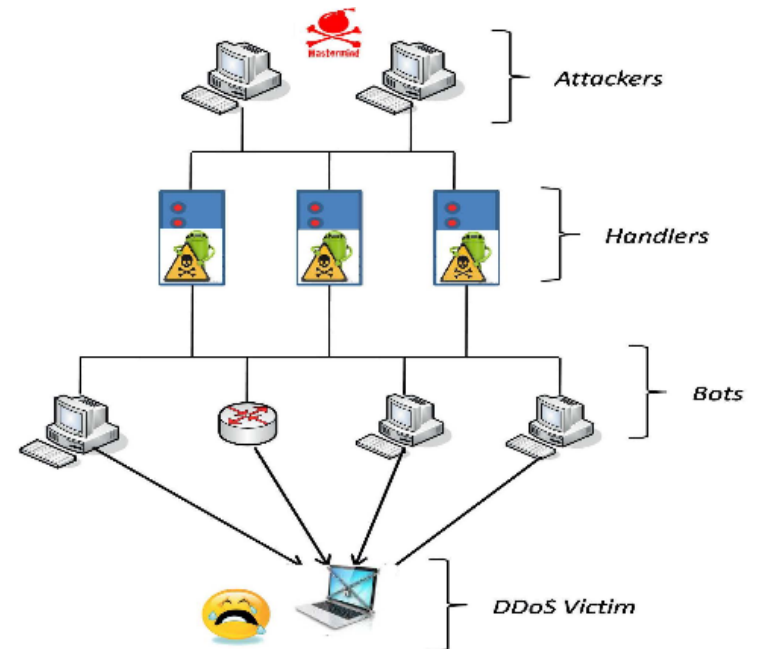
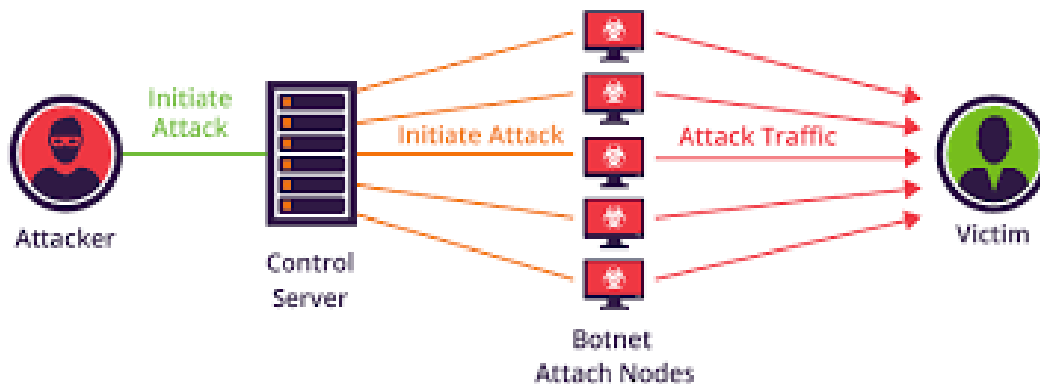
# DDoS

- A distributed DoS (DDoS) attack is a coordinated stream of requests is launched from many locations (zombies) simultaneously.

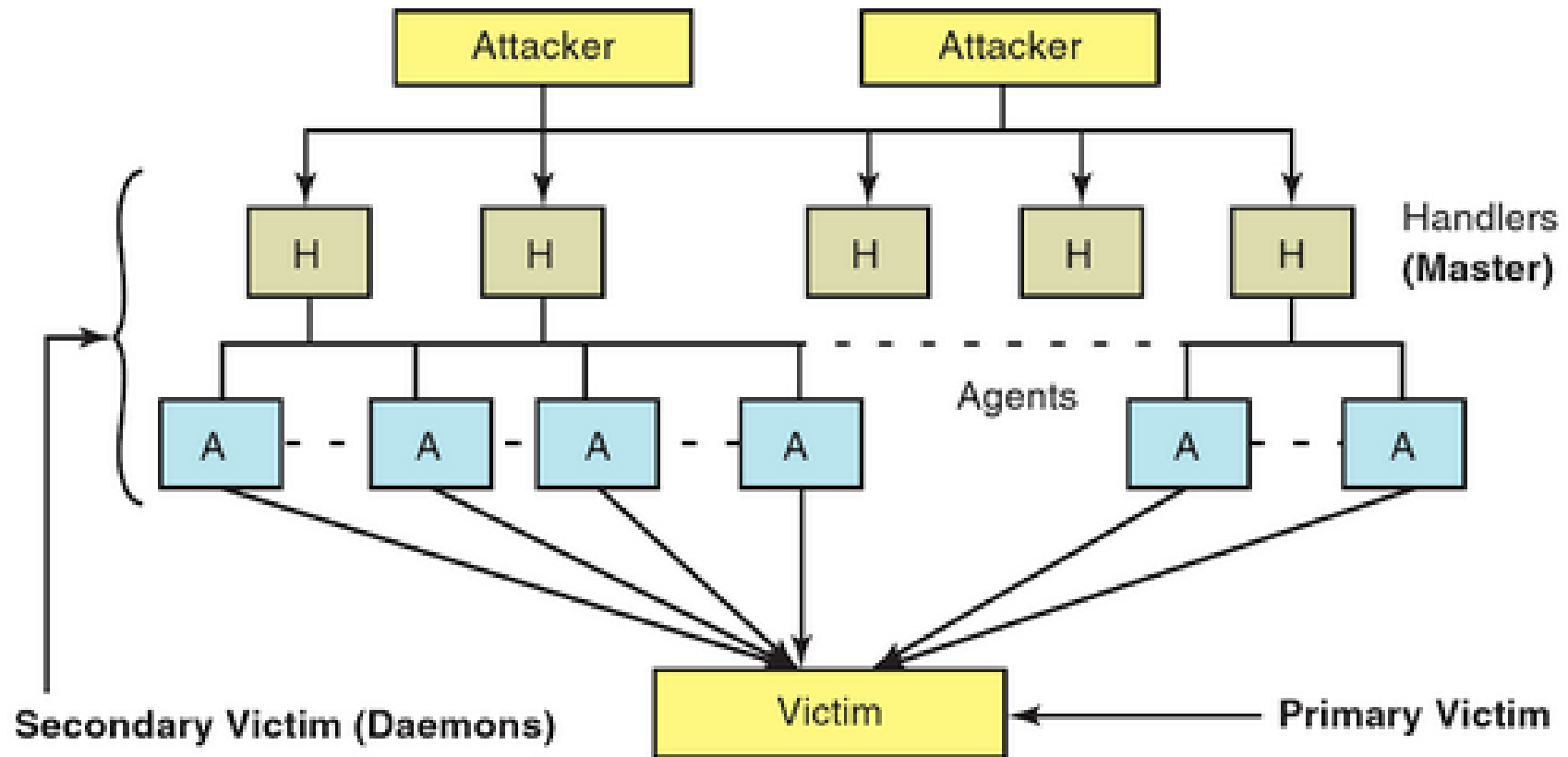


# DDoS cont...

- ❑ **attacker/botmaster/master command-and-control (C&C):** exploits a weakness in the system.
- ❑ **handlers/masters/command-and-control (C&C):** are **routers or servers** to which the attacker injects Malware.
- ❑ **agents/zombie/bot (robot):** since several **computers** are connected to each compromised handler, all these computers turn to compromised agents/zombie/bot.
- ❑ **Botnet (robot network)=**network of bots + master machine
- ❑ The attackers control the compromised handlers and agents to create the high traffic flow necessary to create a DDoS attack.



# Agent-Handler model of DDoS attack



**Figure 6-4** Many distributed denial-of service attacks use the agent/handler model.

# Bot

---

- Bot/Zombie is derived from the word robot and is an automated process that interacts with other network services.
- Bots can be used for either good or malicious intent:
  - A malicious bot is self-propagating malware/program on an infected machine that is activated to launch attacks on other machines
  - Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information, such as web crawlers, or interact automatically with Instant Messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites.

## Bot cont...

---

- ❑ In addition to the worm-like ability to self-propagate, bots can include the ability to **log keystrokes**, **gather passwords**, **capture and analyze packets**, gather financial information, launch **DDoS Attacks**, relay spam, and **open backdoors** on the infected host.
- ❑ Advanced botnets may take advantage of common **internet of things (IoT)** devices such as home electronics or appliances to increase automated attacks. Crypto mining is a common use of these bots for nefarious purposes.

# Googlebot

---

- ❑ Googlebot is Google's web crawling bot/spider.
- ❑ Crawling is the process by which Googlebot **discovers new and updated pages** to be added to the Google index.
- ❑ A huge set of computers are used to fetch (or "crawl") billions of pages on the web.
- ❑ Googlebot uses an algorithmic process: computer programs determine which sites to crawl, how often, and how many pages to fetch from each site.



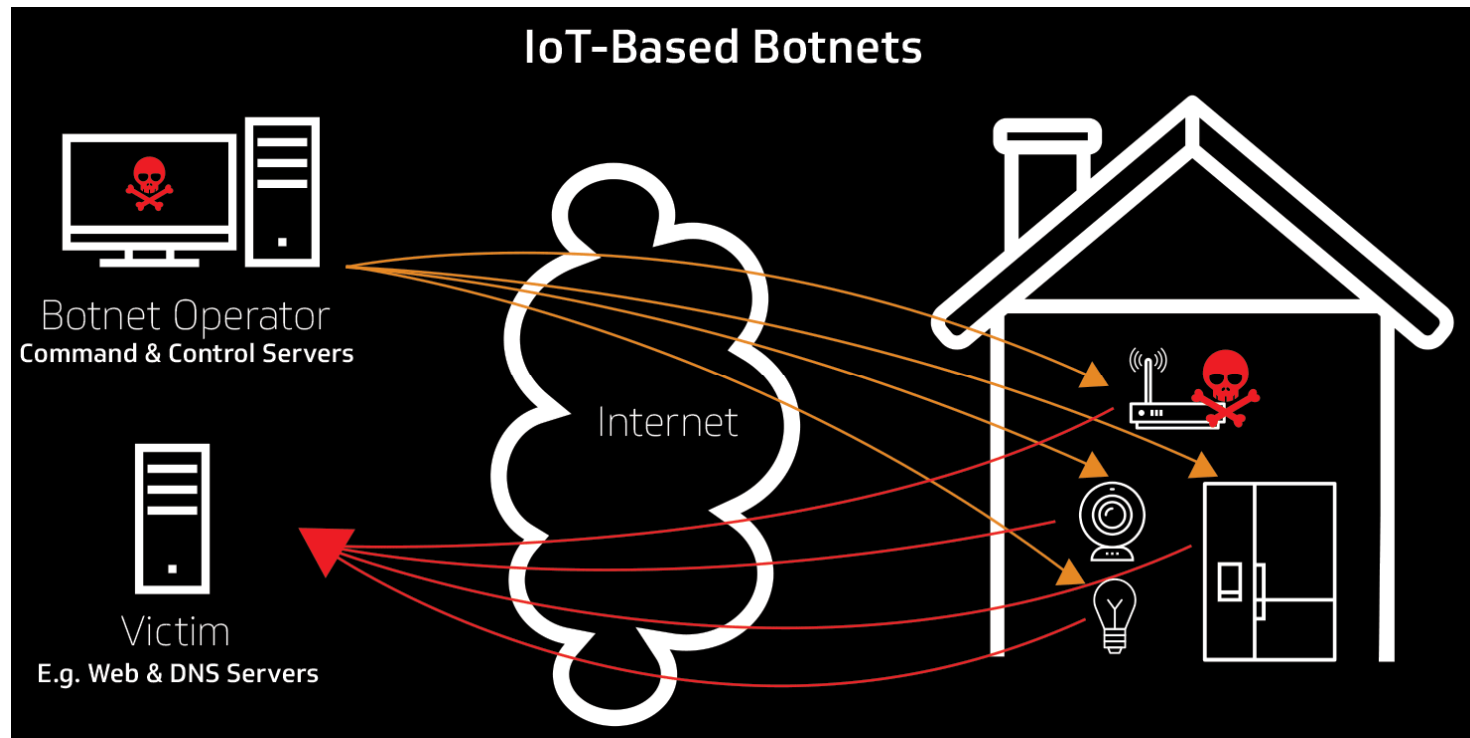
# Botnet

---

- Botnet is a group of internet-connected computers, which **communicate with each other** to complete some **repetitive tasks**.
- Normally, this term is used in negative meaning and it indicates a network of **computers which are infected** by malware and their computational resources are used by other illegal activities like
  - DDoS attacks
  - Spamming
  - Sniffing the network traffic
  - Keylogging
  - Spreading new malware within the same network
  - Data breach
  - ...

# IoT botnet

- An IoT botnet is a collection of **compromised IoT devices**, such as cameras, routers, DVRs, wearables and other embedded technologies, **infected with malware**.



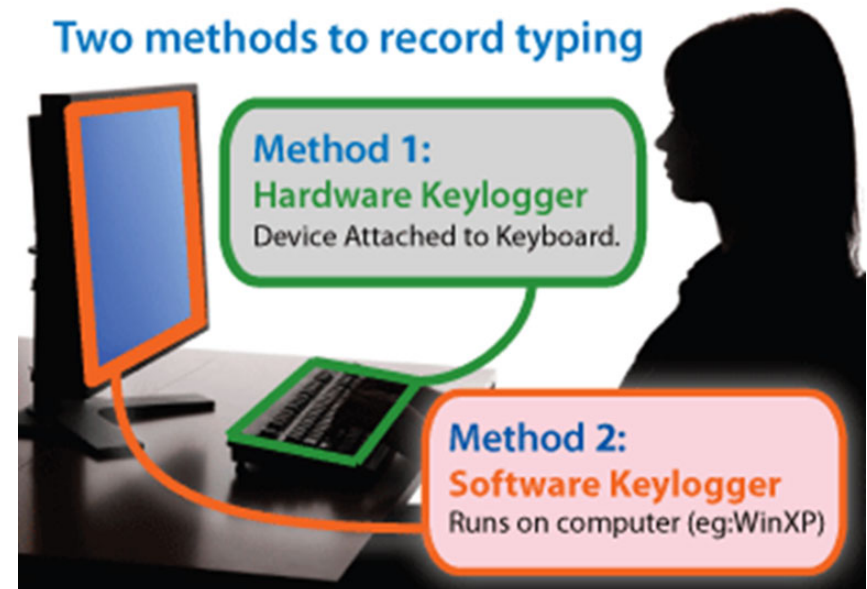
# Malware

---

- ❑ Malware stands for **Malicious Software**. It indicates any software which is used for **malicious purposes** like stealing private data, corrupting files, crashing hard disks, extorting money, etc.
- ❑ There are several types of malware:
  - Keylogger
  - Virus
  - Rootkit
  - Trojan
  - Worm

# Keylogger

- Keylogger **records every word typed by the victim from the keyboard**. The main purpose of keyloggers are for hacking online accounts because it records keyword, so it will also record password and username.
- There are two types of Keylogger:
  - Software keylogger
  - Hardware Keylogger/ keyGrabber



# Software Keylogger

---

- ❑ Software keylogger is software which records every keystroke. You can download free keylogger from the internet or make own if you can good knowledge of programming.
- ❑ Examples are:
  - Free Keylogger
  - REFOG Free Keylogger
  - DanuSoft Free Keylogger
  - Real Free Keylogger
  - Revealer Keylogger Free
  - Perfect Keylogger Lite
  - ...

# Hardware Keylogger

- Hardware Keylogger/ **keyGrabber** is hardware device which needs to connect to computer then it records our keystrokes. Nowadays Hardware keyloggers are attached to the keyboard for hacking credit cards etc.

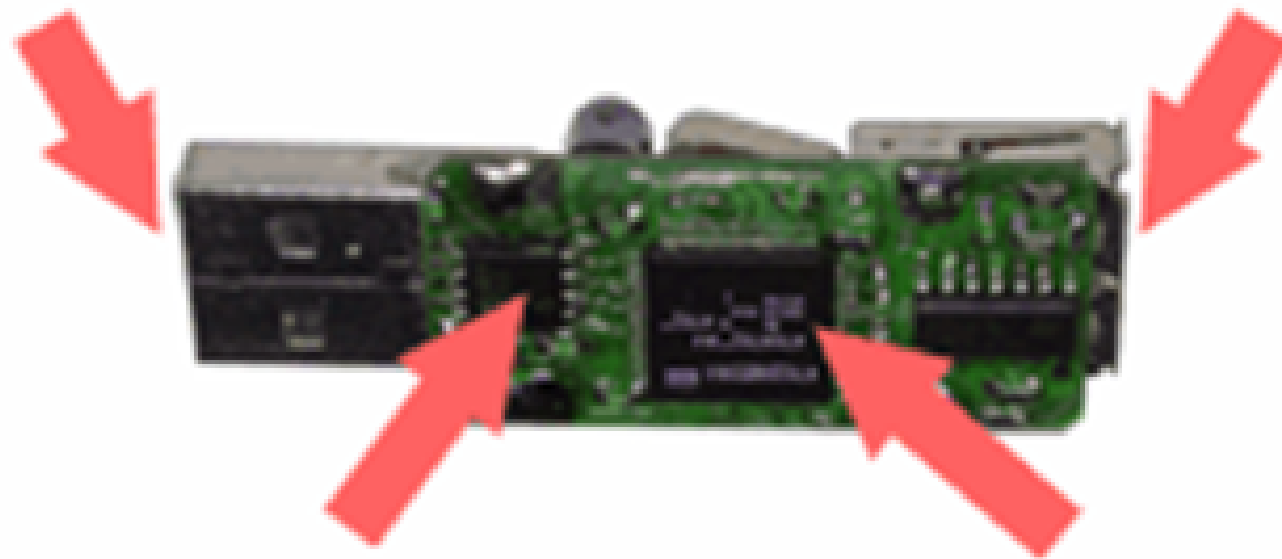


# Inside Keylogger

---

USB Connector (male)

USB Connector (female)



Memory Chip

Micro-Controller

# Keylogger defense

- ❑ Train users
- ❑ Implement effective Anti-Spyware, Anti-Virus
- ❑ Keep patches and versions current
- ❑ Firewall
- ❑ Virtual keyboards

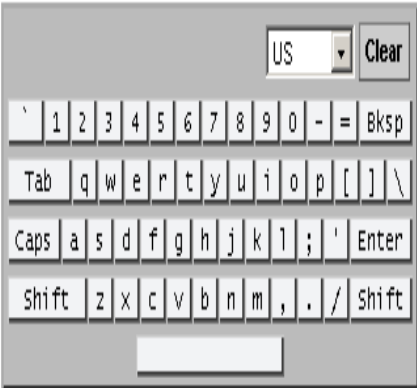


login to Application

login to Application

JserrID:

password:



The virtual keyboard can be used in conjunction with your keyboard. The value of the key will be entered by clicking on a key or when the cursor is over the key for 2 seconds.



جهت حصول امنیت بیشتر در وارد کردن رمز عبور می توانید از صفحه کلید مجازی استفاده نمایید

لطفا شناسه ورود و رمز عبور را وارد نمایید

شناسه ورود (کد ملی 10 رقم): \*

رمز عبور (PIN1): \*

تایید



## USB Rubber Ducky cont...



# Virus

- A computer virus is a computer program written by attacker which is **attached to another program or file** like a PDF, word document, exe file enabling it to **spread from one computer to another** and **infect them as it travels**.

