THE WAR AGAINST BEING AN INTERMEDIARY FOR ANOTHER ATTACK

Prepared By: Raghda Zahran , Msc. NYIT-Jordan campus.

Supervised By: Dr. Lo'ai Tawalbeh.

THE WAR AGAINST BEING AN INTERMEDIARY FOR ANOTHER ATTACK

Raghda Zahran , Msc. NYIT

ABSTRACT

Objective: To determine methods and measures needed to be taken to face the massive attack within networks
Design: Systematic review of cases, latest advances in the hacking field

Data sources: Important Security websites searched for published cases & measures taken.

Results: Compromising other systems and using them as a dummy tool to conduct an illegal act has given the distributed systems another meaning; the cruel intentions behind the act of taking over other computers within the same network or over the internet highlights the need to take all security measures that would stand out in such war.

Conclusion: There is a little evidence to date that could support LANs or WANs to stand out in the illegitimate control, but latest security measures should be implemented

Intrusion Tools

The range of tools, from the least intrusive to the most, are used to :

1. Scan
2. Spy
3. Insert data
4. Manipulate data
5. **Cause a computer to launch an attack on another computer.**

Intrusion techniques

Some techniques used to compromise other computers:

- Probing computers and systems by **'pinging'** or sending out messages that identify computers that are online, and then scanning these computers for open portals
- Infringing (**violating**)security by using **password** sniffer programs, password cracking programs, or keyboard logging programs to reveal passwords and other information;
- creating **backdoors** once an open portal is found and then using software to keep it open and to make it accessible to other computers over a network or the internet;
- Inserting code into computers such as **spyware** programs, which report activity on the target computer; malware is used to execute malicious code such as worms (self-replicating pieces of code that transmit themselves once released without requiring any further human intervention) or viruses (self-replicating pieces of code that are disguised as, or attached to,

another application and that become activated when a person tries to open what typically appears to be an email attachment);

- **Remotely controlling** other computers to affect internal data or operations: 'Trojan horses' are a form of code that once activated on a target computer, enable that computer to be commandeered to perform a pre-determined operation or to be actively controlled to perform operations in real time;
- **Remotely controlling** a computer to affect other computers, such as in a distributed denial of service DDOS attack where literally thousands of remotely controlled computers (bot armies) are made to bombard another computer or service causing it to be overloaded and degrade or fail.
- **Intercepting** wireless data transmissions.

What Is Hacking

All of the above is known as hacking:1

It is breaking into computer systems, frequently with intentions to alter or modify existing settings. Sometimes malicious in nature, these break-ins may cause damage or disruption to computer systems or networks. People with malevolent intent are often referred to as "crackers"--as in "cracking" into computers.

"Unauthorized access" entails approaching, trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and changing computer resources without consent. These laws relate to either or both, or any other actions that interfere with computers, systems, programs or networks.

Targets:

Hacking targets all sectors for different motives

- Profit
- Non-Profit

Interesting targets includes and not limited to:

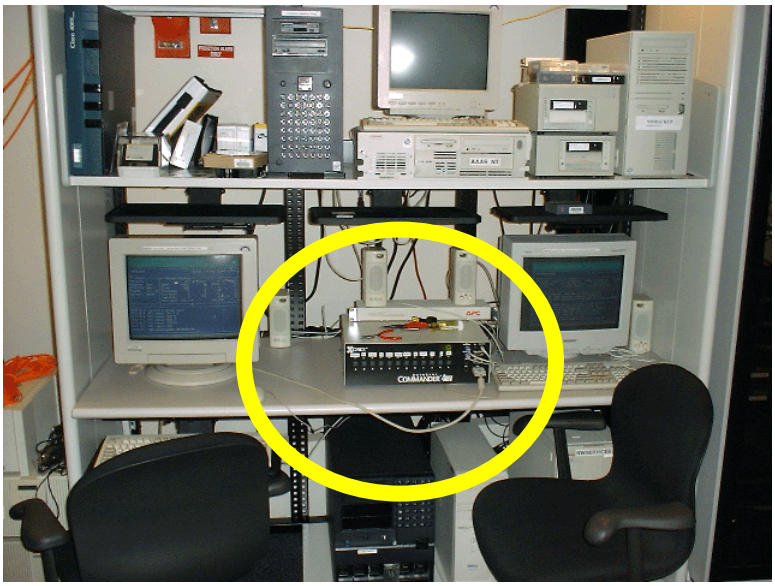
1. Electric companies & power grid
2. Commerce Department & E-Commerce websites
3. Online Brokerage Firms
4. Voice over IP (VOIP)
5. Home users for cash
6. National computers and information: Police , Social Security & Passports Dpts.
7. Military
8. Healthcare Sector
9. Financial services firms: Credit unions, banks, Insurance companies , Exchange firms etc.
10. Telecommunication
11. R&D labs
12. Domain Registers
13. Instant messengers
14. Web Advertisers
15. Certain Demographic Web Sites

Being an intermediary is almost like acting as a thin client [2]or dump terminal:
A thin client is a computer (client) in client-server architecture networks which depends on onother computer & without a hard disk drive, whereas a fat client includes a disk drive

HARDWARE CONTROL; KVM switch: Keyboard, Video, Mouse[3]

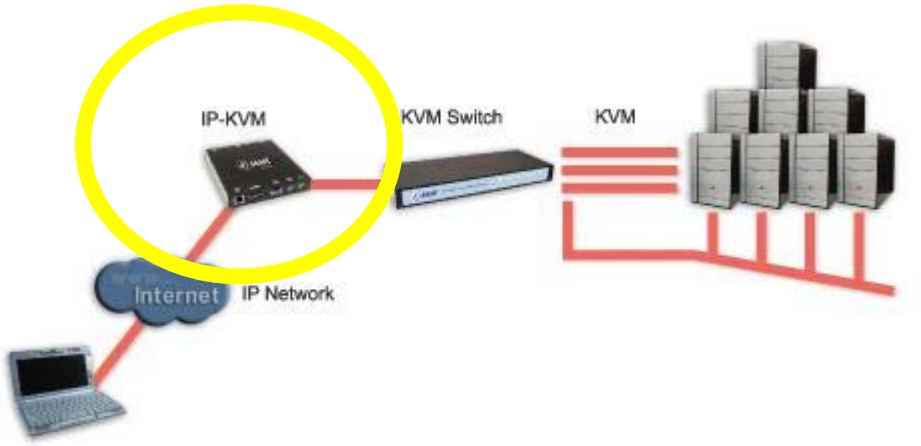
CONVENTIONAL KVM

By pressing buttons on the KVM witch, one can change control from one computer to the next.



IP - KVM

- The latest in kvm switch technology is the ability to control servers located in distant locations through use of the IP communication.
- With ip kvm you can control a server or computer from the other side of the world as if you were standing right in front of it!
- Utilizing the latest in technology your administrator can even configure CMOS and BIOS settings of a server in New York while sitting in a café in Paris!!
- The largest suppliers of KVM technology worldwide are Avocent, Black Box and Raritan[4]



Security Measures: Since the IP protocol is considered insecure, many kvm manufacturers have **added robust and feature rich security abilities to their products.**

KVM Alternatives; Remote control software is software used in remote administration to allow use of computers or other hardware at a separate location. A typical use is to control a server or desktop computer from another desktop computer. idea of *remote desktop software* is to enable you to operate your home computer as if you were seated in front of it, from a remote, internet-enabled computer.

The remote control software consists of two separate computer programs

- "host version" that is installed on the computer to be controlled
- "remote version" that is installed on the controlling computer

- The controlling computer displays a copy of the image received from the controlled computer's display screen. The copy is updated on a timed interval

Sample of Software used to remotely control other computers:

TRADE NAME	LAN	INTERNET	Platform
Anyplace Control™[5]	☑	☑	**Windows PC**
VNC (Virtual Network Computing)6[7]	☑	☑	**cross-platform**
GoToMyPC[8] 1-20 PCs.	☑	☑	**Windows PC**
Remote Desktop Control[9]	☑	☑	**Windows PC**
Symantec pcAnywhere[10]	☑	☑	**Linux® and Mac OS X**
Apple Remote Desktop[11]	☑	☑	**Macintosh computers**

Sample of trade software used for controlling other computers

Software has different attributes but all share two important senses for discussion:

- CONNECTIVITY: requires intranet connection for LAN control & internet Connection for control over the internet.
- MISUSE

Other attributes are:

1. Created for hacking purposes
2. Created for administrating and legal purposes but are exploited and used for cruel reasons
3. Published for free over the net
4. Require purchase
5. Requires installation / setup applications on both parties
6. Don't require installation / setup on both sides.
7. Requires a third party such as providing company's website (Web access) to administer the access and in this case sniffing is used
8. Control is solely conducted by the hacking side.

Preference measurements for the hacking side would be

1. Simplicity
2. High speed and performance.
3. Low network load, using an optimized data compression algorithms.
4. Strong security and high safety. Challenge-response authentication protocol and a RC4-like encryption algorithm make the program usage absolutely safe.
5. Multiple and simultaneous connections. With this feature, the network controller can efficiently control different remote PCs simultaneously. Moreover, two or more administrators can control one remote computer at the same time.
6. Spontaneous interface.
7. Ability to work on multiple platforms.

Security Measures:

- Using latest, most updated tool software that would detect any unusual event.
- Avoid opening any suspicious email
- PC Zone Alarm
- Review the event log
- If you feel that your computer is being hosted as a slave check for any suspicious services and immediately stop it
- Keep a continues physical backup and clear your machine from any crucial and valuable data.
- Force a confidential network check up procedure.
- Connect to only trusted secure sites
- Avoid downloading any software from the net directly

[1] http://www.ncsl.org/programs/lis/CIP/hacklaw.htm

[2] http://www.webopedia.com/TERM/t/thin_client.html

3 www.kvm-switch-review.com/

[4] http://en.wikipedia.org/wiki/KVM_switch

[5] http://www.anyplace-control.com/

[6] http://www.realvnc.com/

[7] http://www.wikihow.com/Control-Another-PC-Remotely

[8] https://www.gotomypc.com/en_US/entry.tmpl?_sid=149477441%3A1F8055980C3C791&Action=rgoto&_sf=2

[9] http://www.remote-desktop-control.com/

[10] http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=pf&pvid=pca12

[11] http://www.apple.com/remotedesktop/

Class Demo
Remote Anything
http://www.twd-industries.com