BLOCKBACKDOOR

SIMON M. MBURU

KABARAK UNIVERSITY

CS-M-0886-09-13

ALEX K. NYAMWANGE

KABARAK UNIVERSITY

CS-M-0684-05-13

4TH INTERNATIONAL RESEARCH CONFERENCE

TABLE OF CONTENTS

Abstract……1

Objectives of the paper……2

Types of backdoors in computer systems…….2

Types of backdoors in computer systems……3

Time bombs…….4

Cheat codes……..4

Cheat codes……..5

Single-shot cheat code…….5

Sequence cheat code……5

Dangers of having backdoors in systems……6

Dangers of having backdoors in systems……7

Kenya's history on information dissemination……8

Kenya's history on information dissemination……9

Evidence of espionage through backdoors……10

Backdoors network theory……..11

Backdoors network theory……..12

Solution to curbing hardware backdoors……...13

Solution to curbing hardware backdoors……...14

National Security Agency TAO……15

Conclusion……..16

References……17

BLOCK BACKDOOR

Abstract

A backdoor is an undocumented method of gaining access to a program or a computer by using another installed program that bypasses normal authentication. This paper deals specifically with hardware backdoors. These backdoors reside in the hardware components of a computer device and they are often very hard to detect using normal intrusion detection methods. Our research on the topic revealed that most hardware computer devices are either manufactured with backdoors within their circuits intentionally by the manufacturer or some vulnerability exists without the knowledge of the manufacturer. As hardware backdoors remain the most dangerous and undetected method used by information system intruders, it is as good as nothing if remote connections cannot be established to them. This paper will showcase how these backdoors work together on different devices in a

network system and the various methods that can be employment to curb the problem. This will ensure that whatever the number of backdoors residing in a device, they will be inaccessible to the intruder and remain harmless to the computer system or device. As Kenya anticipates digitalizing most of its systems for the realization of the Vision 2030, digital gadgets will be the order of the day and suppose they pose the risk of information security breach then a big problem lies ahead. The rapid embracement of digital devices, example vehicle speed governors, will most likely create an information security breach in communication systems since these devices could be potential targets.

OBJECTIVES OF THIS PAPER

1. To reveal types of backdoors in computer systems.
2. Dangers of having backdoors in various systems.
3. The history of information dissemination in Kenya and how it's being digitalized at a very rapid rate.
4. Provide real evidence of unauthorized surveillance through backdoors implanted into communication systems.
5. Show how a backdoor-network could exist on the various network appliances.
6. Suggest potential solutions to curbing hardware backdoors.
7. Reveal America's National Security Agency TAO program.

TYPES OF BACKDOORS IN COMPUTER SYSTEMS

Backdoors are categorized into two broad categories namely; software backdoors and hardware backdoors.

Software backdoors

As the name suggests, these backdoors are bugs that exist in computer programs and system software. The backdoor is generally written by the programmer who originally created the program and is often known to him. They can bypass security measures like firewalls, password protection, antivirus software and intrusion detection methods. The intruder sets up the backdoor -often known as a server- to listen on one of the 65535 ports computers have for internet communication. They then code a client program that communicates with the server program from a remote connection. Since the server is listening for any incoming connection on that port, the client will be able to connect to the server whenever it pleases and tell the machine that it's going to enter it therefore bypassing the computer's security mechanism. Software backdoors often come with open source software but fortunately they can be detected and be removed by using good antivirus software, maintaining updates to the entire system security mechanism and by taking extra caution when opening email attachments.

Hardware backdoors

Hardware backdoor is a malicious piece of code placed in hardware so that it cannot be removed and is very hard to detect. Even though hardware backdoors are rare and notoriously difficult to pull off, they are a cause of concern because the damage they would cause could be much greater than software-based threats. Regardless of any password or access control system used, hardware backdoors are very hard to detect and they typically have full access to the devices they run on. This means the non-volatile memory chips

like the BIOS on a PC or the firmware of a router or other network device could have such pieces of malicious code actively running. Some of the malicious codes require just a BIOS flash in order to implement them. This type of modification is the reason behind Microsoft's secure boot in Windows 8 to ensure the booting process in a PC is trusted from the firmware all the way to the OS. Although this move is brilliant it doesn't protect the user from other chips on the motherboard being modified. One of the most lethal hardware backdoors is known as the *Rakshasa.* To infect the hardware of a computer with Rakshasa, coreboot is used to flash the BIOS using SeaBIOS and iPXE bootkit. Since this bootkit is designed from open-source tools it is very hard for anti-malware software to tag it as malicious. The bootkit fetches malware over the web using untraceable wireless link during boot time if possible or HTTPS over the local network. The bootkit can be used to create fake passwords prompt for Bitlocker and Truecrypt potentially making full-disk encryption useless. This backdoor can be installed by anyone with physical access to the hardware –either at manufacturing time or using a USB flash drive.

Furthermore, hardware backdoors can be classified into two categories based on how they are triggered.

1. **Time bombs**- They mostly function as kill switches, whereby the programmer of the Hardware Design Language programs a time bomb backdoor that triggers itself after a certain amount of time has passed since the system startup. For instance a microcontroller can be programmed to fail after a specific number of clock cycles. Kill

switches can also be programmed to compromise the security of the system after the system has been used for a specific amount of time which could even be some days and so on. One aspect that makes ticking time bombs so dangerous is the fact that they don't need any external trigger methods and they can't be detected by any validation techniques.

2. **Cheat codes**- These backdoors are triggered by data values called cheat codes. Cheat codes are special input that play the role of turning on a backdoor. It can be simply thought as a secret way in which the attacker identifies himself to the hardware backdoor logic. This identification code must be unique to avoid being accidentally detected during validation tests. Unlike ticking time bombs, cheat codes require an additional attack vector: in addition to the malicious designer programming a backdoor into the HDL (Hardware Design Language) , there must be a user who can execute codes on the malicious hardware in order to provide the cheat code key. Two ways are used to communicate the cheat codes to the backdoor;

a. **Single-shot cheat code-** A single-shot cheat code usually arrives at an interface as a large piece of data such as an address example the address 0xdfgsfgsda could be a secret code that turns on a specific backdoor.

b. **Sequence cheat code-** Multiple pieces of data are communicated to the backdoor in pieces. The cheat code usually arrive in pieces over multiple cycles or multiple inputs and just like the single-shot cheat codes they are supplied through data or control interface. For instance,

if the secret trigger code is 0xdecafbad, and the malicious interface has a data interface big enough for a hex character, the attacker might pass the hex values 0xd, 0xe, 0xc, 0xf, 0xb, 0xa, 0xd over eight different cycles or data inputs. Single-shot cheat codes arrive in staggering fashion over long period of time depending on the preference of the attacker. As long as the timing and ordering of the code is defined by the attacker and recognized in the backdoor trigger logic, the individual bits that together comprise the sequence cheat code can come in almost any arrangement.

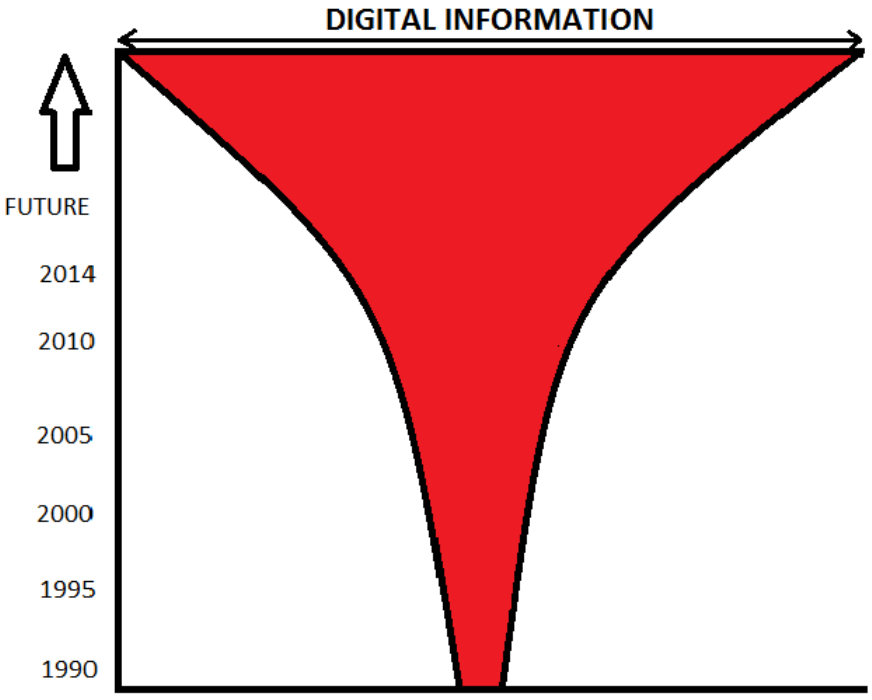
DANGERS OF HAVING BACKDOORS IN SYSTEMS

1. **Information and system sabotage**- The presence of backdoors in information systems or systems that disseminate crucial information could be sabotaged by an attacker and such information could be of very high value. Example if a bank's database containing records of people who have borrowed loans is sabotaged including all its backups, the bank could suffer huge loss because retrieving all the records might be impossible.
2. **Espionage**- Spying and obtaining crucial information that belongs to governments, corporations and other organizations could spark international cold wars. Nearly every country has very strict laws concerning espionage and the penalty for being caught is often severe, but how would you punish an attacker that you're not aware of? Backdoors could give attackers the chance to acquire important domestic secrets like military secrets, state secrets and so forth without

the knowledge of the victim since most backdoors especially hardware ones are often silent and very hard to detect. Industrial espionage has caused exposure of trade secrets between giant companies. Depending on the legal system, trade secrets are protected to prevent unfair competition but if the holder of the secrets is unaware of the leak, the offender could not be brought to book.

3. Hardware backdoors cannot be removed by conventional means example through using of anti-virus software or even by formatting the machine.
4. Hardware backdoors can circumvent other types of security, that is, passwords, firewalls encrypted file systems and so forth.
5. The most dreadful fact about backdoors is that they can and are mostly injected at manufacturing time by a potential attacker. Example if America wants to perform espionage on various African governments, they could intercept all the computer hardware devices being shipped to those countries and plant hardware backdoors (Edward Snowden, a former staff of National Security Agency revealed NSA's Tailored Access Operation move to plant every computer shipped out of America with hardware backdoors).

KENYA'S HISTORY ON INFORMATION DISSEMINATION AND ITS RAPID DIGITALIZATION



The above graph, called 'information mushroom' shows how digital information has been growing in Kenya since 1990 where the country had very little digital information because dissemination of information was mainly based on manual systems. Filing cabinets containing spring files and

other hardcopy recording methods were used to store and disseminate information in both private and government entities. Although computers came to Kenya in the late 80's, many organizations especially government ones were not able to embrace computerized methods of operations due to the fact that they were very expensive and little knowledge that was available about these gizmos. That trend continued up to the end of the 20th century when the country introduced mobile phone communication leading to the new trend of information digitalization. Five years into the 21st century most private organizations had already embraced computerized methods of operations because they were reliable and efficient compared to manual ones. Today, 2014, almost every organization in Kenya has its information being disseminated using digital devices like computers, laptops, ipads, digital personal assistants and many other digital gadgets. Storage of crucial government and organizational information now lies in large mainframe computers at data centers or in Server rooms at the business premises. Digital information is quite easy and very fast to manipulate since every operation performed on the data is computerized. As the graph depicts, digitalization of information is on an increasing rate and by Vision 2030 almost every government and private sector will have their operations digitalized. This trend sends cold shivers down the spine if we bear in mind that information insecurity is also on the rise especially when the NSA is planning to spy on every communication channel in the world. Top government secrets will be secrets no more, the whole country could enter into information colonization. The issue of terrorism in Kenya has seen the government investing in a 14.9 billion project for installing CCTV cameras and face-recognition systems in

all the major cities and towns. This move will increase the amount of digital information that the country poses and on the other hand it will also provide extra crucial information to the spies.

EVIDENCE OF UNAUTHORIZED SURVEILLANCE THROUGH BACKDOORS

On 27th May 2014, The Standard Newspaper published an article by the title "Kenya loses privacy war to snooping data spies." The article revealed how America's NSA programme had collected metadata on Kenya's cellular telephone network, quoting the article; "Last week reports leaked by National Security Agency whistleblower Edward Snowden revealed that Kenya is among five countries where the US intelligence agency has been intercepting, recording and archiving all phone calls for the last one year. The surveillance is said to be part of a top-secret NSA programme code-named Mystic –which has a backdoor to Kenya's cellular telephone network…" end of quote. Having a backdoor to an entire telephone network is possible only if almost every network appliance on the telephone network has a backdoor, which could be the subscribers' cell phones, server computers, routers and so forth. The question that is posed by security experts is, if Kenya's phone calls have been spied on for the last one year, what about the other top secret

information? Such revelation depicts how backdoors could ruin the reputation of a county.

A German magazine Der Spiegel published new allegations about US spying on Chancellor Angela Merkel. The magazine cited secret documents saying that her phone may have been bugged since 2002 and was still on NSA surveillance list weeks before President Obama visited Germany in June. The European Union leaders also voiced their concern about the scale of US surveillance which has gone to the extent of performing espionage on its allies.

On a separate report, Italy's L'Espresso reported that the UK and the US have been spying on Italian internet and phone traffic; these revelations were also sourced to NSA's whistleblower Edward Snowden.

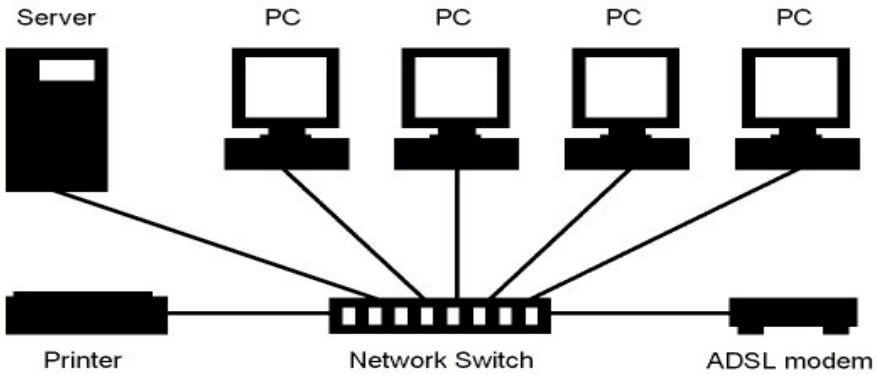
In May 2010, the TAO division reported its mission accomplished after a report classified as top secret said that it has successfully exploited a key mail server in the Mexican Presidential domain within the Mexican Presidential network to gain first-ever access to President Felipe Calderon's public email account. The mail domain was also used by cabinet members and contained diplomatic, economic and leadership communication which continue to provide insight into Mexico's system and internal stability.

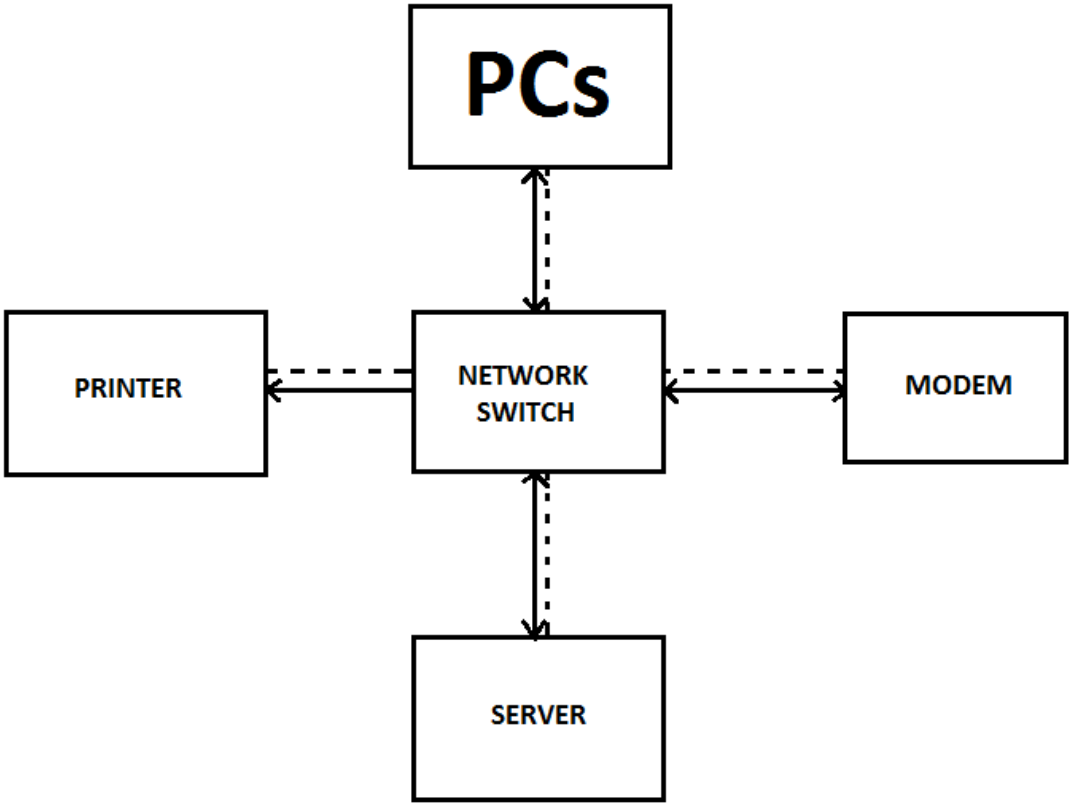
BACKDOOR NETWORKS THEORY

Backdoor networks are unknown but our research had led us to the conclusion that for an entire system to be attacked there must exist an entire network of backdoor vulnerabilities in the physical network itself. These vulnerabilities are caused by the various network appliances like the router,

switches, hubs, server computers, wireless devices and many others. If all these devices communicate to each other and they all have different backdoors that perform different tasks then a backdoor network will exist. Example if the backdoor of a router performs the task of redirecting packets and the wireless device backdoor performs the task of broadcasting those packets to another destination, and then we have a working network of backdoors. Kenya imports all of its computer devices either from Asia or America where allegations of placing hardware backdoors into devices has been roaming for some time. It is these very same devices that are used by the government and private sectors to create communication links that manipulate important top secret information. The entire network also intends to grow as the country embraces more digital platforms like the introduction of digital speed governors in public transport vehicles and so on.

Network diagram





The flowchart above depicts how the network appliances in the network diagram create an entire virtual network of backdoors. The dotted lines represent the backdoor network. In the diagram, we assume that each device including the PCs have hardware backdoors that enable the attacker to get access to the data being manipulated by the devices. Given that the devices are active and running, an attacker could use the backdoor in the modem to get access to all the other devices in the network which has backdoors that prompt this operation. Since the modem acts as a key point to enter the internet, all the other devices could be directed by the malicious code to feed it with their data. In this case the theory depicts that the backdoors are meant to create a virtual network that gives the user uninterrupted data access. This is just a small LAN network but the theory still applies to large communication networks like telephone networks.

SOLUTION TO CURBING HARDWARE BACKDOORS

Our research on hardware backdoors led us to two methods that can be used to silence them. Note that hardware backdoors cannot be permanently removed since they reside on the hardware BIOS or firmware. Trying to eliminate them permanently means reprogramming the entire hardware. During validation, the backdoors remain silent in order for the devices to be able to make it to the market. Once the devices reach their destination the backdoors have to be triggered for them to become active. If we could manage to prevent those triggers from turning the backdoors on, we can keep the backdoors dormant rendering them useless and harmless. The two methods that could be used to silence them are;

1. **Power resets-** This method prevents untrusted units from detecting how long they have been active thus preventing time based attacks. The technique is generally applicable to any digital hardware and is used to block time-bomb backdoors that are triggered automatically after a certain period of time has passed. Our key strategy is to make sure all the untrusted hardware components whether in core, memory system or off-chip remains in a state that they have been turned on recently. Power reset performs the act of frequently turning off and on each unit thus losing the data that is in local state such as in registers. For the microprocessor context, saving and restoring method will be used to ensure that the program in execution is not disrupted by the frequent power resets. The power reset technique is however not 100

percent effective since not all on-board memory in a computer system is volatile.

2. **Data obfuscation-** This technique applies to the type of backdoors that require data input for them to be triggered. These trigger codes are known as cheat codes as mentioned earlier. Data obfuscation simply performs the function of confusing and making it very difficult for the backdoor logic to recognize the trigger code (cheat code). The specific obfuscation method used depends on the hardware unit categorized as computational (units that perform operations on data values) and non-computational (units that don't perform any operations on data values but just to move them around). For non-computational units, a simple encryption scheme is used to obfuscate the data before it enters the unit. Obfuscation of computational units is complex and is beyond the scope of our level and this paper.

Another method that could be used to block backdoors is **sequence-breaking.** However, this method to our perspective is almost 100 percent ineffective since it requires an additional chip in the system that will perform the task of monitoring system performance. We opt to assume that the chip itself could have a backdoor plus in Kenya there is no place where we manufacture computer chips so the technique is not applicable.

NATIONAL SECURITY AGENCY TAILORED ACCESS OPERATIONS

The Tailored Access Operations known as TAO is a cyber-warfare intelligence-gathering unit of the National Security Agency NSA. A

document leaked by NSA's former contractor Edward Snowden revealed that the NSA has been intercepting computing devices on transit and bugging them before they are shipped to their clients. It's not clearly known whether the various computer companies in the US have partnership with the NSA to allow their devices to be bugged or it's just a sheepish move by the agency. Some of the documents leaked by Snowden revealed some shocking devices like the Portable Continuous Wave Generator. The PCWG is a remote device that works with tiny electronic implants to bounce invisible waves of energy off keyboards and monitors to see what is being typed. The shocking fact is that the device works even without internet connection and it doesn't have to be placed on the system motherboard.

TURMOIL surveillance system- This is a dragnet surveillance system used by NSA and it performs deep packet inspection. The system works closely with another system known as TURBINE that performs the task of deep packet injection. When both systems are combined they form what they call QFIRE which is then combined with additional infrastructure to be co-opted into routers and other network appliances.

CONCLUSION

In conclusion we urge computer and security experts to come together in order to free African countries from information insecurity by providing adequate solutions that will guarantee information privacy to our people. As Africa moves into the digital age proper data security measures should be given due consideration to rescue future generations. A long journey starts with a single step, thanks to Edward Snowden now we have a glimpse of an idea of the real situation.

REFERENCES

[1] Franklin Sunday,2014, 'Kenya loses privacy war to snooping data spies' ***The Standard Newspaper,*** 27th May, The Beat pullout page 4

[2] http://www.cs.columbia.edu/~simha/preprint_oakland11.pdf

[3] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.229.1557

[4] http://rt.com/usa/appelbaum-30c3-nsa-snowden-986

[5]https://www.ideals.illinois.edu/bitstream/handle/2142/35322/Edwards_Nathan.pdf

[6] http://people.umass.edu/gbecker/BeckerChes13.pdf

[7] http://www.infosecisland.com/blogview/15095-DHS-Imported-Devices-Infected-with-Malware.html