Securing Personal Computing Devices from State-Sponsored Monitoring

Fitsum Assalif

Fall 2014

Lewis University

Final v 1.0

Contents

1. Introduction 5
2. Exposed State-Sponsored Spying Malware 8
Common features across the attack types 8
Trusted Layer 9
Untrusted Layer 9
FinFisher 11
Remote Control System (RCS) 12
QUANTUMINSERT 13
3. Proposed Solution Areas 15
4. Computing Device (Hardware and Operating System) Security 17
Endpoint Protection System 19
BIOS Security 19
Physical Security 20
Full Disk Encryption 20
Operating System Hardening 21
Software updating /patching system 21
Location Security 23
5. Securing Data Transmitted and Stored on Internet 25
Local network security 25
Web Browsing Security 28
Email Security 31
Instant Messaging and VOIP Security 34
File Storage and Backup Security 37
6. User's Habits 38
7. Conclusions 40
8. References 41

Table of Figures

Figure 1. Strategic deployment of Fin Fly ISP [10] 11

Figure 2. Tactical Deployment of Fin Fly ISP [10] 12

Figure 3. All-in-one RCS architecture: logical layout [9] 13

Figure 4. Schematic of NSA's QUANTUMINSERT system [7] 14

Figure 5. Kali Linux software updater window 23

Figure 6. Open WiFI warning message on Windows 7 OS 27

Figure 7. Using VPN over public Wi-Fi 28

Figure 8. Bing search performed without HTTPS Everywhere plugin on Chrome 29

Figure 9. Bing search performed without using HTTPS Everywhere plugin in Chrome 30

Figure 10. DuckDuckGo secure and anonymous search engine 31

Figure 11. Encrypted email garbled text 33

Figure 12. Jitsi before establishing securing 35

Figure 13. Jitsi after establishing a secure communication 36

Figure 14. Chat history after using Jitsi for Google talk 36

Figure 15. Bugmenot.com providing shared accounts 39

Abstract

Due to the recent growth in state-sponsored remote spying and monitoring systems report, citizens need a guide to help them better secure their computing devices. These spying initiatives show a similarity in that they are well designed, are scalable and highly integrated with Internet service provider networks. In this paper sample state-sponsored malwares have been studied and possible solutions are presented. The solutions are guidelines or checklists a user can reference when acquiring and using a computing device to minimize the chance of infection by these highly sophisticated attack types. The guide has three technical solution recommendation parts with the final part being the users' habits. Despite how strong the technical solutions are, the final and critical layer is the human being using the device. Users should develop a habit of protecting their computing device physically and technically as well as protecting themselves from social engineering and making mistakes that can leak identity, credentials or sensitive information.

1. Introduction

State-sponsored spying on a country's own citizens has become a common concern of citizens and Internet freedom fighters. Even if this phenomena and privacy concerns seem recent, the roots go back to Dec 15, 1791. [1]The Fourth Amendment was released on that year for the purpose of protecting citizens from unreasonable search unless there is a probable cause and valid warranty. This amendment and its interpretations have been evolving with time due to the forms of information communication and storage technology advancement.

The advancement of technology has taken information storage from a paper in users' homes to online storage hosted by third parties and some government offices. Electronic communication technology which started with visual telegraph has also advanced to text, audio, and later to the current systems which allows us to integrate text, audio & video over internet in real time. [2] This progress has been very beneficial to the world. But, it has also brought the concern on privacy because the communication can be wiretapped, sniffed or manipulated on the wire while in transit.

Nowadays anyone's phone calls, text messages, emails, Instant Messages and any other online communications including voice and video can be intercepted by any third eye that has access of the communication channel. Accessing this information has become possible even without the user's consent depending on the skill, resource and access of the third party doing it. These entities could be malicious hackers, employers trying to protect Intellectual property, or governments. The scope of this work focuses on government or state-sponsored interception.

There have been reports on state sponsored interception of communication without user's consent in named countries under many studies and reports. [3] [4] [5] Despite which country is

doing it, these attacks use a common set of possible technologies to intercept and collected user's data. These methods fall into the following major categories:

- Installing backdoor or Trojan on targeted users [3]
- Intercepting data on the air or wire [6]
- Combining the above two methods to facilitate tracing targets, deliver backdoor and monitor centrally [7].

User's computing devices, which are responsible for sending and receiving information as well as storing it, are usually the final target of these attacks for many reasons. These devices provide the best point of access to view and collect data while a user is viewing it without worrying about the security measures taken to protect it on transmission. Accessing the computing device also gives a more permanent nature because the user could change location, network or application in use easily.

These software attacks use very advanced malwares to perform the attack and remote spying. The Information Security industry uses many terms to describe unwanted malicious software like the ones used by governments or individual hackers. The term malware is a broad category that also includes virus, spyware, adware, and worm. State sponsored malwares, like Magic Lantern, which is used by the FBI, however, fall into a group of malicious software called rootkits. Rootkits are different from the other malware groups on three main characteristics. Rootkits do not self-propagate, their main intention is not to generate revenue from advertisements like botnets, and they do not send large amount of traffic like Trojans. [8]

These being the basic features, any of the malware features can be fused with rootkit features to avoid detection and forensics. One good example is armoring as well as use of signed

certificates to avoid easy detection. For this paper the terms state-sponsored malware, stealth malware, spyware or rootkits are used to refer any kind of malicious software that are used by governments to spy targeted citizens. [9]

In this paper attack types will be discussed first followed by sample state-sponsored malware observed in the wild. The next three sections will discuss the solution areas classified as hardware and operating system, data transmitted and stored online and user habits. These chapters will discuss the weakness, vulnerabilities and possible implementation mistakes, and finally provide the best possible protections against these attacks.

2. Exposed State-Sponsored Spying Malware

There have been a series of state-sponsored monitoring and attack attempts through time. Due to the nature of the attacks and lack of interest in the commercial companies, documentation and research has mainly come out from non-profit, journalism and activist organizations like Citizenlab.

FinFisher, Remote Control System (RCS) and QUANTUMINSERT are from the widely discussed and recent state-sponsored malware. The architecture and features of this malware are discussed in this chapter. The observed common features followed by individual features will provide understanding of how these systems work as well as prepare citizens on how to protect themselves against the existing and future similar initiatives.

Common features across the attack types

Government could achieve delivery of malware to the targeted party in many ways. There is a similarity on the attack types used by disclosed architectures from commercial spywares of FinFisher, Gamma International, and Hacking Team. They demonstrate a well-designed attack and monitoring system, which is more advanced and can be done by an entity which is multi-staffed and well-organized. According to disclosed documents about Fin Fly ISP, QUANTUMINSERT and Hacking Team's spyware, there is a similarity in architecture. A broad summarized view of the architecture can be put as follows mashing all the three architectures: [9] [7] The summarized architecture can be broken down in two major sections: untrusted and trusted layers.

Trusted Layer

Trusted layers is the layer where the state sponsored system backend components are placed and operated. This is where all the servers processing the controlling and data processing are placed. It is considered trusted layer because the components in this layer do not have to be exposed directly to the targeted user or internet. Their communication with the compromised devices are considered anonymized or secure enough to avoid leading any interested party to this infrastructure. It is located within the premises of the state agency performing the action. These are the subcomponents which could be placed in the trusted layer:

- Master Server: The main server that controls status of other components and central database. This layer is where configurations to network devices, databases and consoles are done. It can be compared to primary domain controller server in functionality.
- Collectors and/or Network controllers: Collect data and communication from untrusted layer devices like network injectors, and infected devices. These are the data gateways which collect, normalize and filter any relevant data for use.
- Control Stations/Consoles: where analysts or administrators sit and perform the monitoring and installation of the malware. These are more like operators using the software to perform the actions. Technicians sitting at the consoles do not have to know how the backend is configured or works. They are simple users of a ready to use infrastructure following instructions.

Untrusted Layer

The untrusted layer is the layer on which the systems used have to interface with internet, compromised devices or third party servers. The components or devices on this layer can either be placed in ISP, hotels, coffee shops or anywhere network injection is planned. A good example

of this layer is the network injector used by FinFisher manufacturers, which can be placed in hotels and coffee shops to sniff as well as redirect users. This is useful when doing targeted and strategic attack for temporary actions or while following target at possible locations. The other good example is the proxy server which fetches contents from legitimate third party website, does on the fly injection and serves it to the compromised machine.

- Anonymizing servers: In some of the malwares anonymizing technology has been used to hide the agency behind these activities. This is observed on the Hacking Teams RCS spyware. [9]The anonymizing servers route the injection and collection of data not to be traced to the trusted layer. As the name indicates, this layer's purpose is to hide the information of the party performing the action.
- Network Injectors: Network injectors are used to deliver the malware once target identification is performed. These devices perform redirection, man in the middle attack or impersonation to deliver the malware.
- ISP module: This module s observed on Finfly ISP. [7] This module is used to help locate or identify the target by pulling account information as well as other characters so that network traffic can be detected easily.The Finfly ISP module profiles a user by collecting all available information from the ISP database to help identify and locate a user. It gets name, address, IP address, email address and all available data. These data are then used to accurately identify the targeted user before malware is delivered.

The three malware and their architectures are discussed below supported with screenshots of their disclosed architectures for further clarification.

FinFisher

The following picture shows one of the deployment modes of FinFisher. The FinFly ISP RADIUS Probe interfaces with the ISP database to collect user data. FinFly ISP is able to patch files that are downloaded by the target on-the-fly or send fake software updates for popular software. A strategic solution would be a permanent ISP/countrywide installation of FinFly ISP to select targets and deploy payloads from the remote headquarters without the need to be on location.

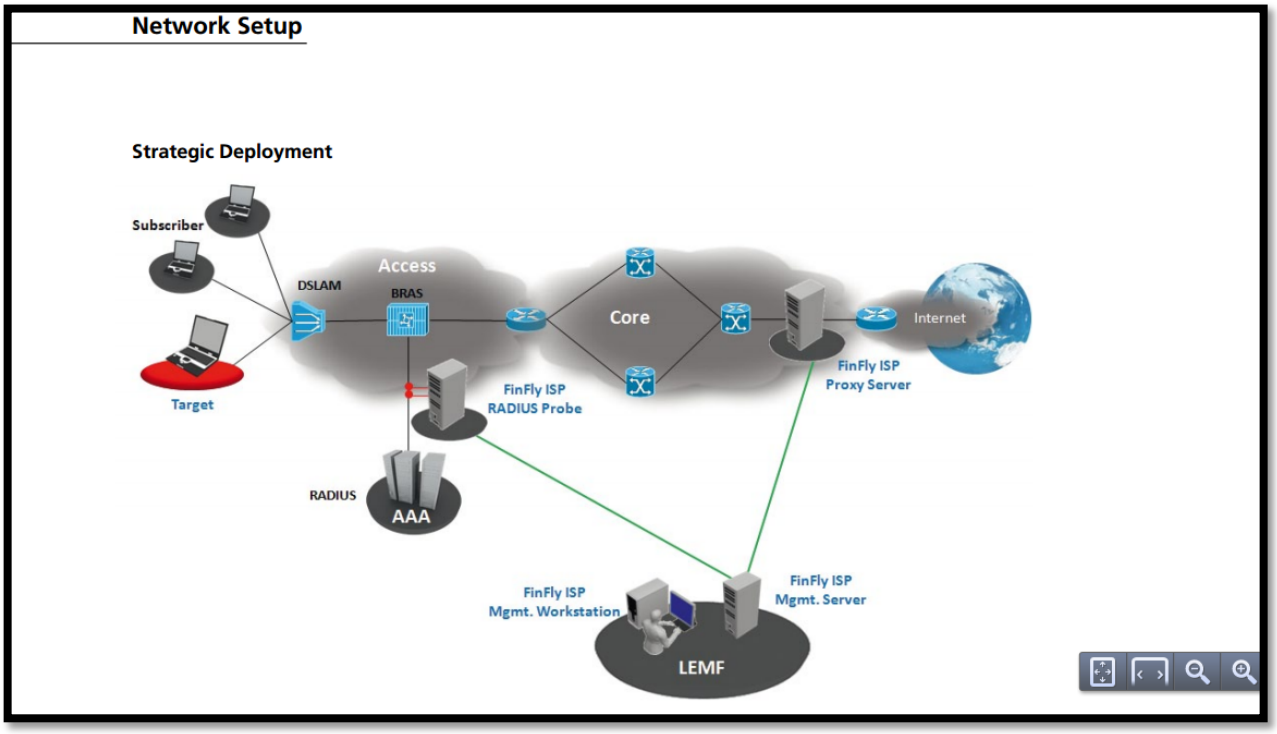

Figure 1. Strategic deployment of Fin Fly ISP [10]

The second option of deployment for FinFisher is the tactical option. A tactical solution is mobile and the hardware is dedicated to the deployment tasks inside the access network close to the targets' access points. It can be deployed on a short-term basis to meet tactical

requirements focused on a specific target or a small number of targets in an area. A good example for the use of the tactical option is a conference or convention locations.

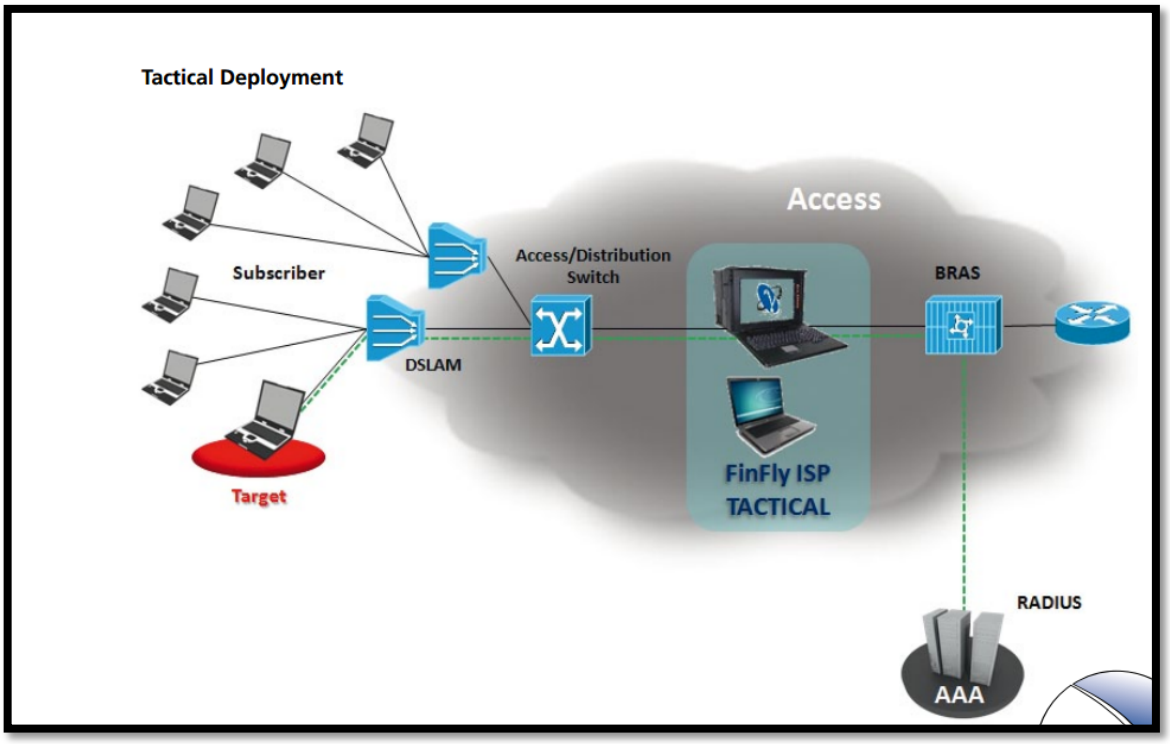

Figure 2. Tactical Deployment of Fin Fly ISP [10]

Remote Control System (RCS)

The following picture shows the All-in-One deployment option for RCS. The picture shows the logical architecture. This software has the anonymizing components which makes it a little different from the above two deployment options demonstrated by FinFisher. Once injection is done, collecting data can be done through the anonymizers. The published architecture also does not clearly show how the software interacts with an ISP.

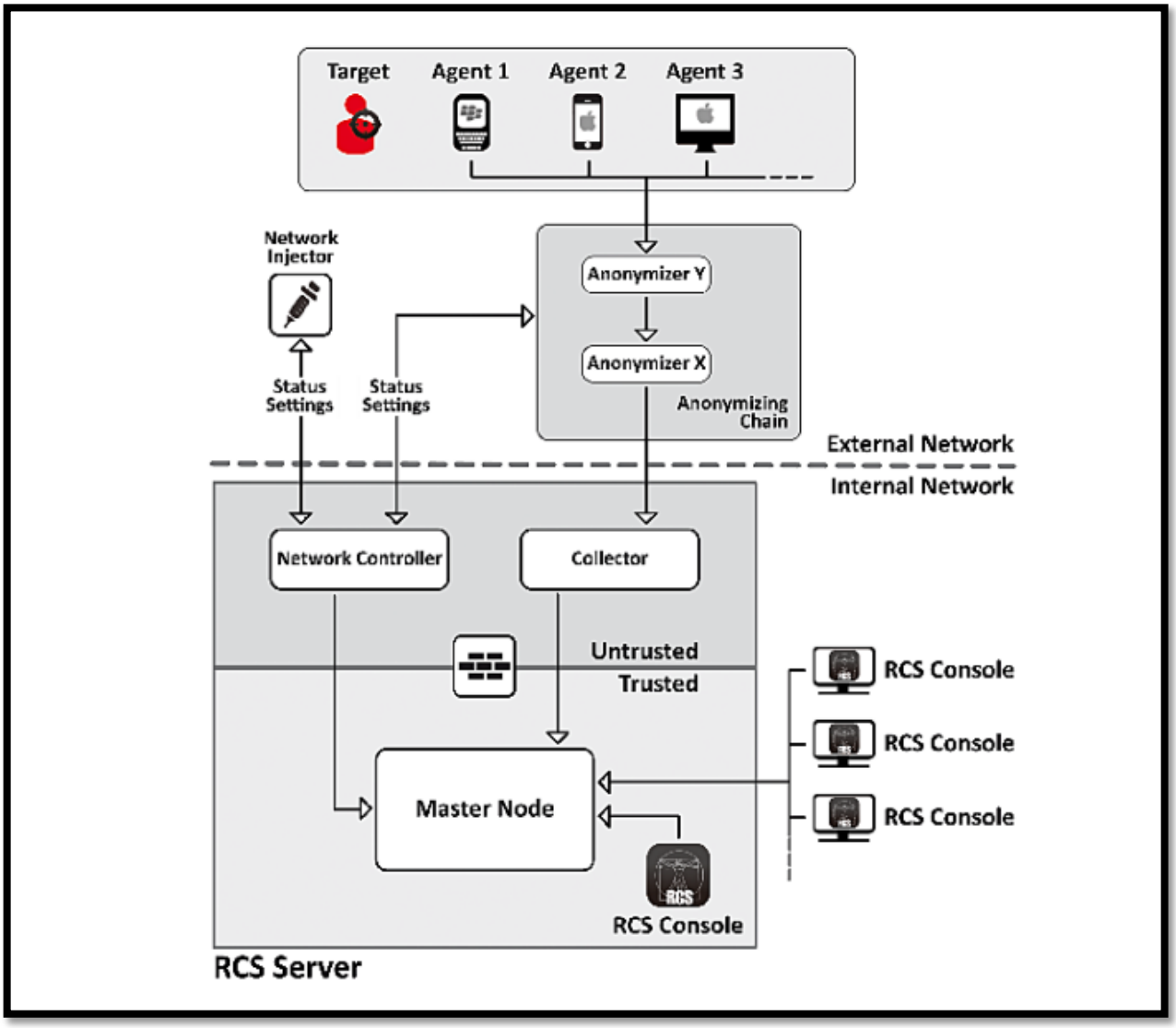

Figure 3. All-in-one RCS architecture: logical layout [9]

QUANTUMINSERT

The picture below shows QUANTUMINSERT, spying platform used by NSA. As shown on the picture, once a victim passes a wiretap QUANTUMINSERT simply packet injects a 302 redirect to a FOXACID server. Then the victim's browser starts talking to the FOXACID server, which quickly takes over the victim's computer.

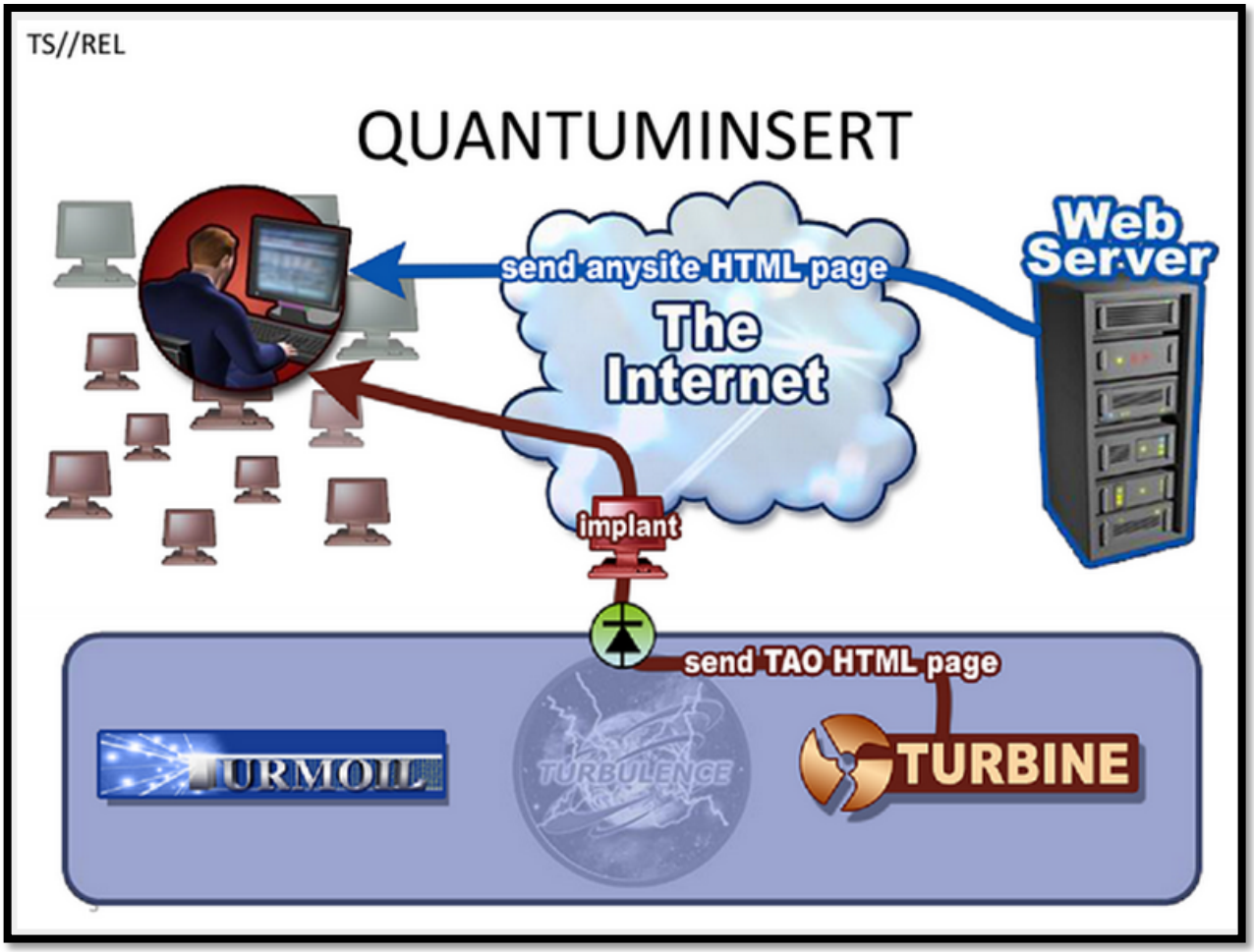

Figure 4. Schematic of NSA's QUANTUMINSERT system [7]

3. Proposed Solution Areas

This research will cover possible solutions and precautions to secure user's computing machines from these kinds of attacks. The approach used divides the solutions in the following sub sections:

1. Computing device (Hardware and Operating System) security
2. Securing data transmitted and stored on Internet
3. User's habits

The first two layers are technical approaches on selecting hardware and applications to secure environment and data. These solutions will make installing backdoors and intercepting user's traffic on the fly as difficult as possible according to the current technology. The third layer is the most important layer because giving a computer or phone with the most secure operating system to the least aware user is as dangerous as no security measures in place.

This work will research on solutions which could fill the gap in the current existing solutions which are failing to protect against from the latest attacks [7]: antivirus only approach, using HTTPS for login pages only, and browser's certificate management. Solutions which are not common in user domains, protection against backdoors, selected targeting attacks [5], and mobile operating systems are also component of the solution.

These solution areas and their subcomponents can be summarized in the following table. Fulfilling these minimum protection layer requirements will decrease the chance of being infected with state-sponsored attacks easily.

1	Computing device (Hardware and Operating System) Security	• Endpoint protection System • BIOS Security • Physical Security • Full Disk Encryption • Operating System hardening • Software updating /patching system (Operating System plus third party) • Location Security
2	Securing data transmitted and stored on Internet	• Local network security • Web Security • Email Security • Instant Messaging and VOIP Security • File Storage and Backup Security
3	User's habits.	This section talks about acceptable user habits about using the implemented features as well as online and offline digital security best practices.

Table 1. Proposed solution sections and sub-sections

These three components and their sub sections will be discussed in the following chapters.

4. Computing Device (Hardware and Operating System) Security

Computing hardware considered for this work are desktops, laptops and tablets. smartphones, even if very similar to computing devices, will be discussed separately because of the usage differences. Computing devices have hardware and software part. State sponsored malwares are targeting the software part as well as hardware, even getting down to the semiconductor level, in some cases. [11] A report released on September 2007 by Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics shows a concern for foreign involvement on manufacturing semiconductor and microchip devices. According to the report, these components can be tampered with to give access to other governments. This indicates the same concept can be applied by one's government to its own citizens. [12]The same report also mentions how Trusted Platform Module is unique to each device, which indicates that it can be used to identify each device. Tampered component which can give a chance to identify, track or access these devices will put the citizen at full risk of exposure. Embedded hardware based backdoor on end user computing devices has not been used for remotely spying users.

The most common standards used like NIST recommend the following core components for basic security [13]:

- Anti-Virus: detects malware by signature and known characteristics by vendor
- Anti-Spyware: detects spyware like remote tools and key logging
- Intrusion Prevention System: monitors and alerts about active intrusion or attack attempts, applications trying to make connection to external servers over unusual ports and protocols

- Firewall: handles network segregation, port and IP range blocking, sometimes application whitelisting
- Tuning Application Settings.

While this approach is the basic, it can also mislead users into false sense of protection. Anti-Virus and Anti-Spyware systems try to detect malice by signatures for a very long time. Although there are some vendors that use heuristics and threat intelligence databases that help to detect previously unknown malware, they are also moving away to the term Endpoint Protection System. The main difference mentioned by experts between Endpoint Protection System over Anti-Virus typically includes:

- Malware removal based on existing signature files and heuristic algorithms
- Built-in antispyware protection
- Ingress/Egress firewall
- IPS/IDS sensors and warning systems
- Application control and user management
- Data input/output control, including portable devices [14]

These features come as default inbuilt features and as a single software bundle. The above model listed all of them as independent applications, which gives the user the option to either install them or not. Users can also assume they are protected by using one or two or three of the applications. The integrated, endpoint protection system option enables or guides users towards using all the features at least with their default settings.

Endpoint Protection System

For the purpose of this work, the term 'Endpoint Protection System' will be used to refer a malware protection system that works in real time as well as when required to scan on demand. For better protection of the current state sponsored malwares, endpoint protection systems with at least the following components should be used: Malware protection based on existing signature and heuristic algorithms, Anti-Spyware protection, application white listing, Intrusion Prevention System and basic firewall. The Endpoint Protection System approach will help users implement all minimum requirement features instead of dwelling to an anti-virus only approach.

BIOS Security

BIOS is the piece of software responsible for performing Power on Self Tests on computing device hardware, finds and loads operating systems. [15]It is the first set of code or software loaded when the device is powered on. A research paper released by The MITRE Corporation has indicated that BIOS can be attacked by malicious users, with physical access of the hardware, so that it can be modified to load additional or malicious codes of software. BIOS is executed before Operating System starts. This makes it possible to achieve bypassing most of the security protection mechanisms applied at OS level. Despite how important BIOS is, there are only limited options of protecting your BIOS from being reset or modified. The first and most convenient protection mechanism is setting BIOS password of the computing device. This will enable any attempts to change a user BIOS difficult. The second and equally important component of protection is Physical Security. This is because BIOS passwords can be reset with variety of hardware manipulations; from unplugging jumpers to plugging in specific devices and cards at boot time. A good example is some Toshiba devices can reset BIOS password upon a special loopback device connection during boot. [15]

Physical Security, OS hardening and full disk encryption will be the focus of the next component of this work as they are crucial components of protecting the computing device from state sponsored as well as other malicious initiatives. These components will enable infecting a device or stealing stored data as difficult as possible in cases where the device falls in the wrong hands. That is also the layer where sharing location exposing information on social networking or location-based applications should come into consideration. A citizen, activist or journalist who has a reason to believe he is targeted by government should also be careful about his physical security.

Physical Security

A research done by Ponemon Institute in 2010 indicated that 86,445 laptops are stolen in 12-month period in United States. [16] Even if this research data is for corporate laptops, it is also an indication of the level of computing devices theft or loss. Since it is customary to protect and watch over personal belongings, physical security is not new concept as the online or data security. Computing devices should stay with the owner at all times, or should be locked to tables or reliable structures when placed in office or home. This decreases the chance of the device being stolen easily.

Full Disk Encryption

In cases of possibilities a computing device is lost or stolen, it is recommended to prepare the device so that the data to be inaccessible by unintended users. This can be achieved by implementing full disk encryption on endpoint devices. Full disk encryption encrypts the entire disk including swap, hibernation and system files. [17]Full disk encryption only protects the device when it is not powered on and logged in. This technology should be supported by user's habits on locking and powering down on long breaks. Otherwise data is readable by anyone who

can login to the machine by password guessing, brute force attempts or any authentication bypassing hacking techniques.

Operating System Hardening

Once hardware is selected, BIOS is secured, as well as Full disk encryption is implemented the next layer is the Operating System. Users should decide between selections of operating system Operating system provides a lot of features out of the box, but that does not mean it is safe to use. Out of the box operating systems need to be checked and modified accordingly to minimize exposing the computing device for attack. The common measures to be taken after booting up a fresh operating system is

- Create a user (with no Administrator privileges) account for everyday use
- Set password for the built-in administrator account
- Disable guest and other accounts if available
- Uninstall unwanted applications and any additional third party software
- Disable any service not needed at the moment. Good examples are file and printer sharing and Bluetooth
- Disable any automatic network connection configurations. E.g. disable automatic joining of open Wi-Fi
- Enable automatic update

Software updating /patching system

Once operating system and all required third party application are installed on a device, automatic updating should be configured. The OS and the applications may not always come from the same vendor which makes it a challenge to achieve a unified updating/patching

strategy. A good example is Windows automatic update, which only updates applications and OS components from Microsoft. All other critical run time and plugin application to our browsers, browsers, email clients, drivers need are left out on some OS. Thus, depending on the OS the user uses, it is good to select and use updating/patching systems which support all application on the computer.

Some Linux operating systems have a unified repository that checks and updates all applications, OS and drivers on a computer in unified matter. All it takes is one command or application interface to check, approve and install updates. The screenshot below is taken from Kali Linux distribution automatic update program. The application listed on it are not only the applications provided from the Kali Linux distributor company. One good example on the picture is Google Talk Plugin, which is a Google software being updated by the Operating System unified updater. The updater checked and presented the update for approval even if it is blocked by the automated update process.

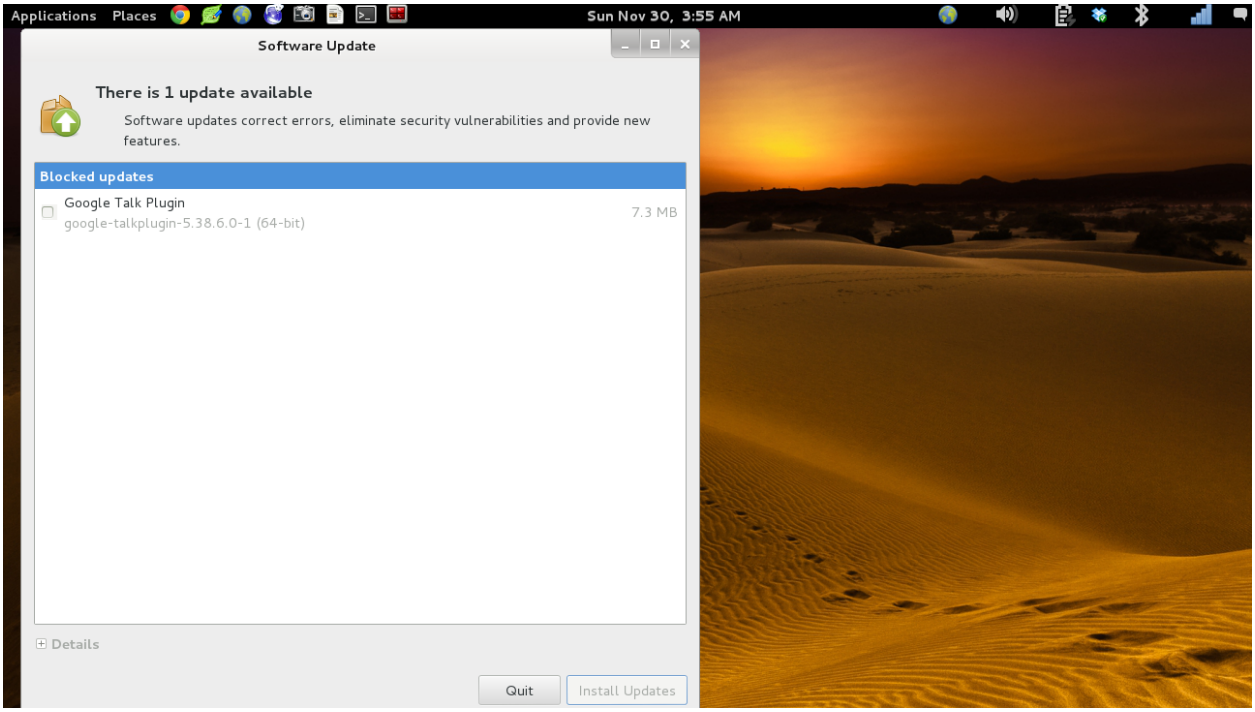

Figure 5. Kali Linux software updater window

Location Security

Online services like search engines, maps and social networks use user's location to provide better services. Even though this devices access user's location based on user's consent, it is highly likely to overlook the details in user agreement or the applications access of this data when running in background. Having location history available on online services makes targeted users vulnerable because the data can be used to track them in real time or guess where they would go to shop, eat, or watch a movie to mention a few examples.

Many precautions can be taken to prevent leaking of location information unintentionally. Always verify factory configurations during new hardware procurement. Verify where there are default anti-theft and similar systems which are enabled when the hardware is on sale. Use services or hardware which have implemented proper Location Privacy Pre-serving Mechanisms (LPPM). [18] This mechanism gets location for the application or device the user is using while

giving out minimum information to the network service provider by using well known location system security protocols. When unavoidable, use location services from untraceable devices like public kiosks or libraries which allow anonymous access.

Do not allow background service location access. Set services to use location service while in use or by approval prompt each time. If an application is logging or reporting location history in the background, the data could be accessible from the server side, which exposes the user. Turning on and using the location services when needed only gives awareness to the user that there is a possibility this location information can always be found. The user then can take additional measures as changing looks, or changing location as soon as possible.

Location information can also be found from any item with RFID (Radio Frequency Identification) tag. RFID tags have been used in items as simple as Lipsticks to passports. A good example is Saudi government's notifications system which was established in 2010 that allows male guardians of a family to get notifications when their wife, underage children or foreign workers passport is scanned. [19]Any shopping item with RFID tags also can be scanned to reveal buyer's identity if the seller has stored that information.

Once the acceptable security measures are taken at the first layer according to the paper, Computing Device (Hardware and Operating System), the computing device is ready to for use. The steps taken are to secure the hardware and bare operating system. These devices are then used to access many online and offline applications and services to fulfill user's computing requirements. Therefore, these devices will be exposed to third party software, peripheral devices, and the Internet.

5. Securing Data Transmitted and Stored on Internet

This part of the solutions has to do with being online and using services which will interact with server which is sitting somewhere else on internet. Even if being offline is one of the highest methods of security, it is very difficult to live without taking advantage of what the internet has to offer. A user will check for news, search for the closest grocery store, order some items online, and get driving directions to a meeting in downtown and hundreds of other similar scenarios. The sub sections below suggest solutions to provide the most reasonable level of security for users who are going to use online services.

Once the recommended steps to harden the security of a computing device are taken, the device is ready to be used to access offline and online services. Accessing online services an Internet connection which is comprised of Physical connection (wired or wireless) and a working network configuration (IP Address, default gateway, DNS server). This internet connection is routed by an Internet Service Provider (ISP) to the destination server. This communication channel can be logically divided into the following sub-layers for better understanding of security: Local network: home, office or school network where the computing device is connected, ISP network and destination service provider network. A user can only see and apply protection measures for local network .ISP and destination networks are managed by the owners and are not visible from outside.

Local network security

Internet connection can be shared among users of the same subscription at home, school, a coffee shop, hotel or office on location networks. In these scenarios, the connection can be shared over wireless or wired network. Local networks providers can read transiting network traffic and/or impersonate a server or client on the communication. This allows the network admin or operator

to intercept and capture traffic generated by a user on the same network. This also enables changing traffic accessed or files downloaded on the fly.

Putting this into consideration when using any network helps on selecting the right protection measures before coming online. From security perspective we can classify the networks in two broad categories, untrusted and trusted networks.

Untrusted networks are networks provided by coffee shops, libraries or restaurants. These networks do not guarantee users' security because they are provided. Open wireless network and network running on hub are weak by nature because they allow network users to snoop with each other easily. The protection from these kinds of networks is not to use them or use additional layer of security

The first and best option is to avoid using networks which do not have the minimum required level of security. On wireless networks avoid using open wireless or any network which is not using at least WPA2 wireless key. Operating systems provided warnings are symbols which indicate the wireless network is unprotected. Figure 6 below shows a warning message presented when connecting to open wireless network from Windows 7 OS.

Figure 6. Open WiFI warning message on Windows 7 OS

The wired network type to avoid like open wireless network is network running on hubs. Even if hub is a very old technology, it might be still in use for legitimate or malicious purposes in some places. Hubs broadcast every nodes information to the rest of the nodes on the same hub, which will enable attacker to listen and sniff other nodes network traffic

When the time comes that a user has to use unsecured networks, the second option is to use a VPN connection to user's home or a service provider to access internet through a secure gateway. If a user had to use an unsecured network, VPN can be used to encrypt and direct all traffic through the VPN exit. This VPN exist can be a configured router or firewall at user's home, or a paid service on internet. Figure 7 below demonstrates how VPN can be used over a

public Wi-Fi network. The blue line shows an encrypted tunnel between the user's computing device and the VPN exit. The internet traffic from the user travels over to the VPN exit and then leaves from the VPN exit to the destination server as shown on the brown line. The brown line shows the traffic path without VPN over public Wi-Fi.

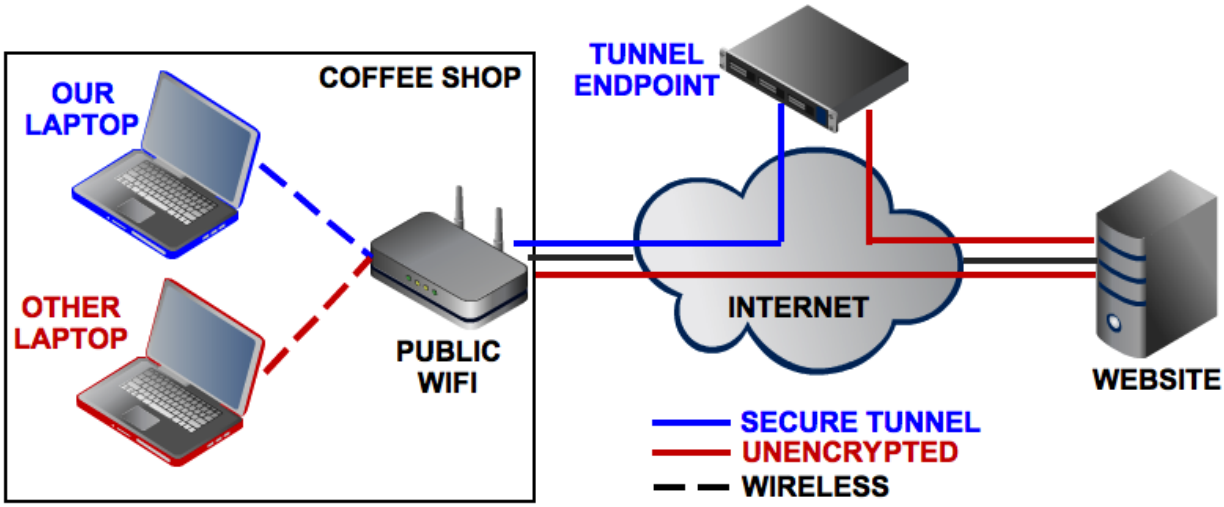

Figure 7. Using VPN over public Wi-Fi

The above two measures help a user secure themselves against untrusted networks. Once a user is on a network that is considered trusted like a properly configured home or corporate network, there are still additional measures to be taken for safe online communication

Web Browsing Security

Websites can be accessed using either HTTP or HTTPS. HTTP does not provide encryption between the server and computing device. It is highly recommended to request and use the HTTPS version of services available online. This can be automated by browser configurations or additional extensions to it. There is a widely used good example for this from Electronic Frontier Foundation. This browser extension called HTTPS Everywhere switches the connection request to HTTPS mode whenever available. Figure 8 and 9 below show one

example of using HTTPS enforcing plugins. A search for the text “test search” is performed on Bing search engine without using the plugin. The search by default used HTTP and the result is returned. This traffic can be clearly read by anyone who can sniff this traffic. After the plugin is activated on the browser, the same search is performed and the search is carried on HTTPS. This traffic, even if sniffed, is encrypted.

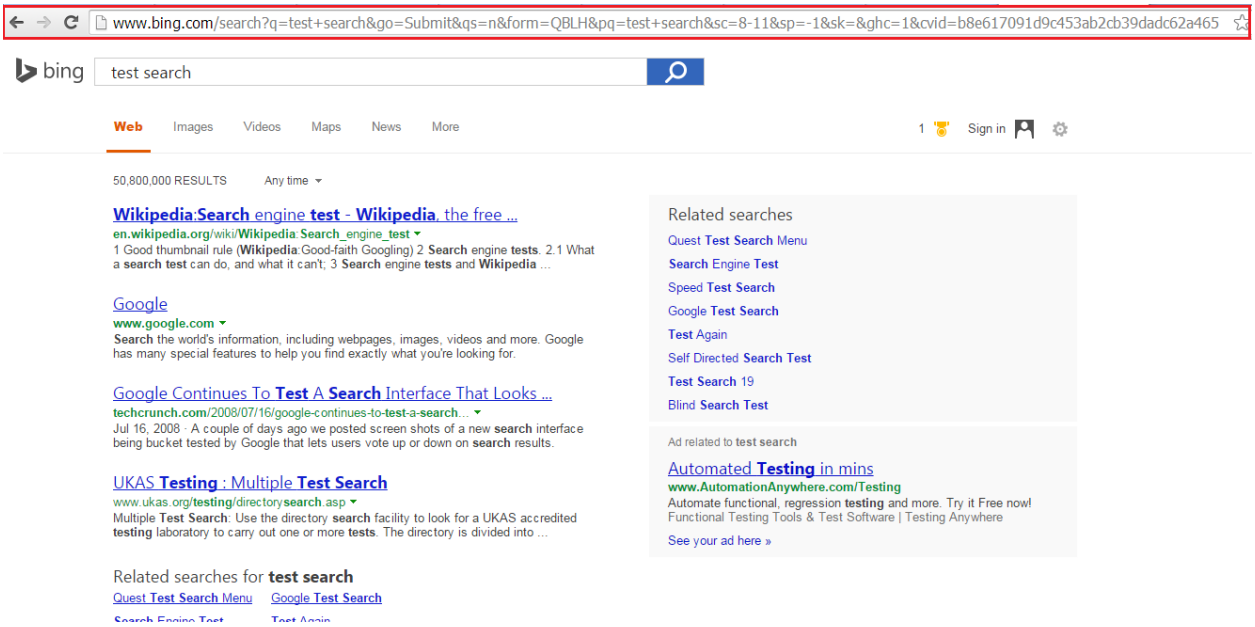

Figure 8. Bing search performed without HTTPS Everywhere plugin on Chrome

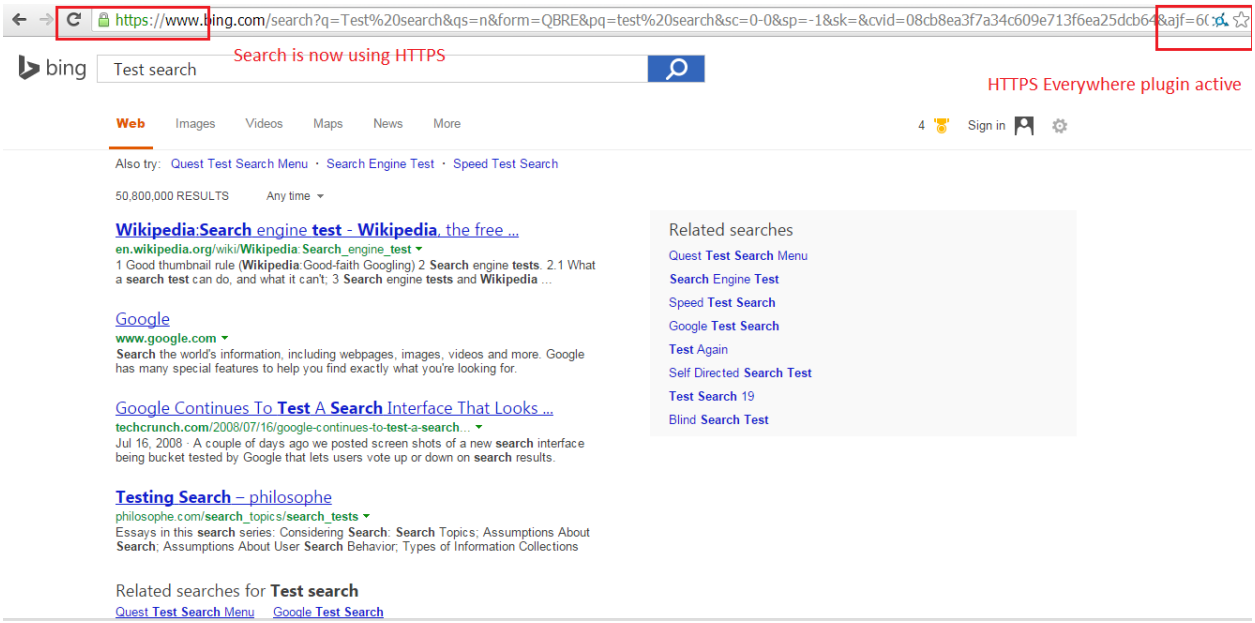

Figure 9. Bing search performed without using HTTPS Everywhere plugin in Chrome

The second most important consideration when using online services is that even if the communication with the services is secured, the service could also implement a tracking and identifying mechanism using cookies, HTTP referrers or user agents. The best solution for tracking is knowing the service. This can be achieved by reading privacy policies of a website. Search engines can be good examples for this. For example, Google search engine saves search history, and also uses HTTP referrer, which gives information about the users when search result is clicked. In this scenario the best alternative way to avoid being tracked is using search engines which do not track users and anonymize search data. DuckDuckGo.com is a good search engine known for its secure and anonymous search services.

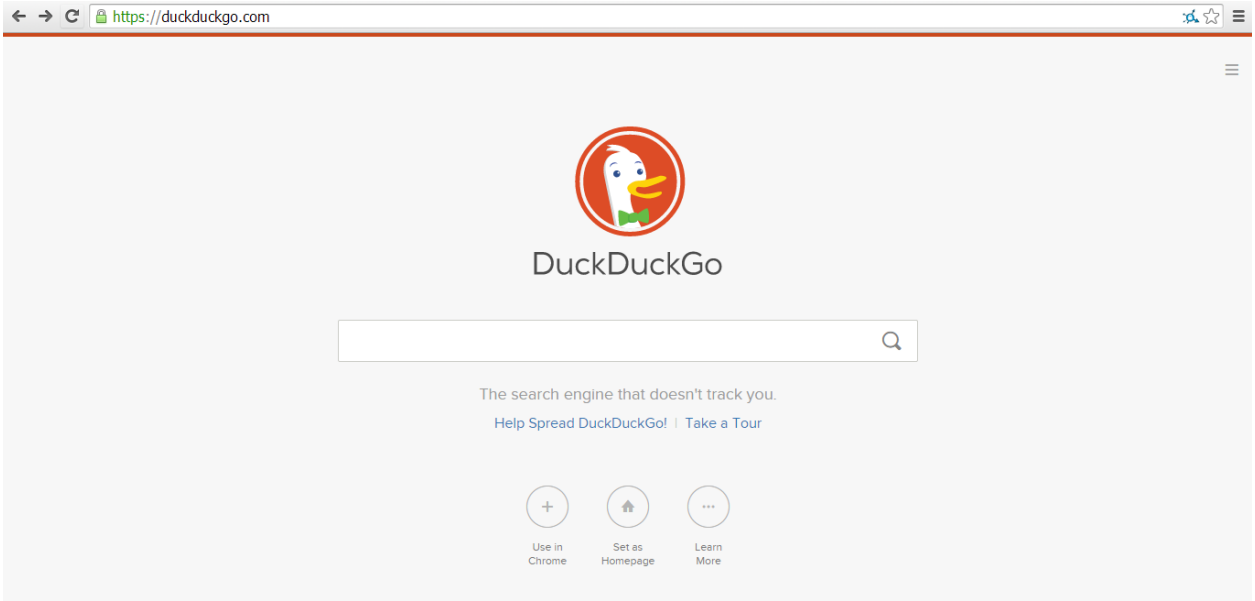

Figure 10. DuckDuckGo secure and anonymous search engine

Web browsing security depends highly on the user's ability to identify each service's privacy policy combining with tools like the ones mentioned above. The following bullet points provide summary of tips to use when browsing online services

- Avoid websites which use tracking e.g. Google Search engine
- Disallow third party cookies
- Turn off Referers
- Always use HTTPS

Email Security

Email accounts are secured by the user's password when they are not being accessed. But when a user is sending an email over wire, depending on what kind of application and communication protocol is used, they can be read by sniffing them over the wire. Phil Zimmerman, the creator of PGP, offers a different view:

> It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having a secret romance. Or you may be communicating with a political dissident in a repressive country. Whatever it is, you don't want your private electronic mail (email) or confidential documents read by anyone else. There's nothing wrong with asserting your privacy. Privacy is as apple-pie as the Constitution. [20]

Since email communication can be seen in clear text at several points when it traverses the internet and the servers we are using, it is recommended to use encryption to hide its content. This ensures that the contents of the email are only readable by the sender and receiver. A good example of this solution is open source PGP implementation, GnuGPG (http://www.openpgp.org/). Using encryption will show the email contents as garbled text messages. Picture 11, below displays how an encrypted email looks like before it is decrypted by the intended receiver who has the private key. This text, even if intercepted and viewed by any malicious user cannot will not reveal the human readable content.

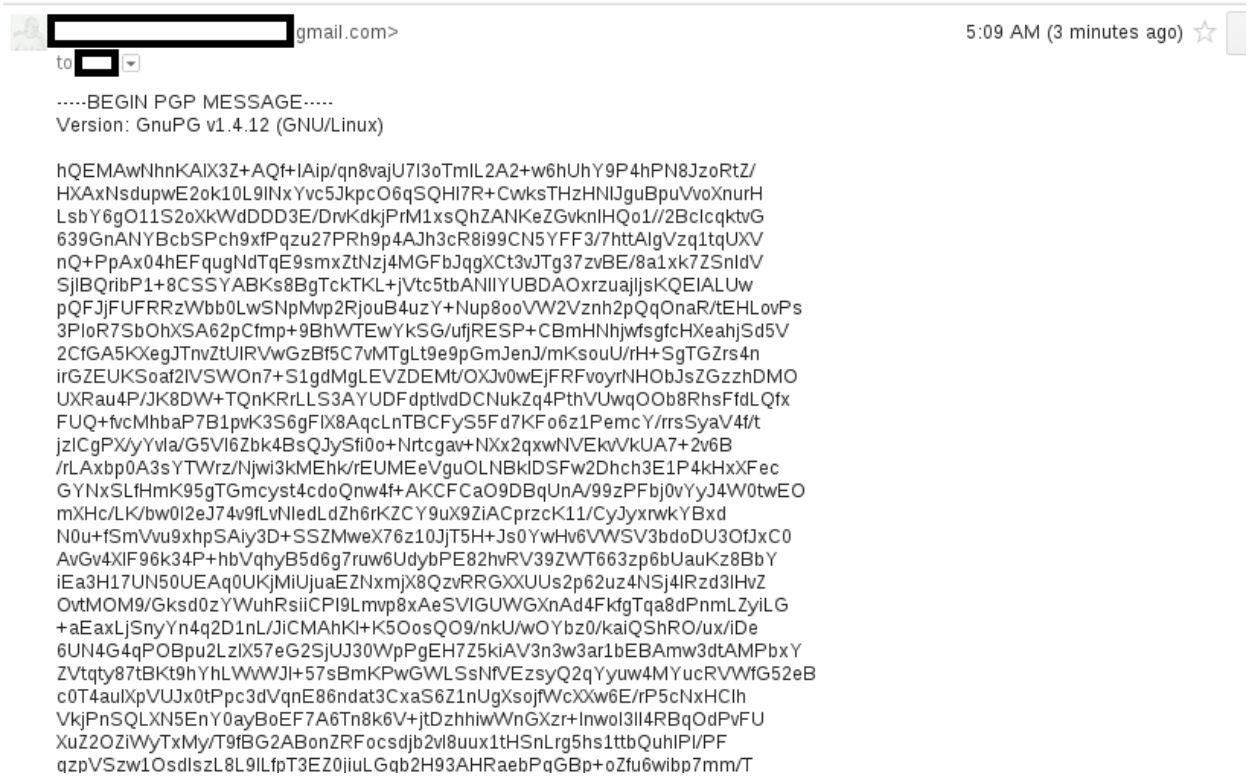

Figure 11. Encrypted email garbled text

These solutions use an asynchronous encryption system, which works by generating a private and public key pair for each user. The public key is distributed or posted on key server so that anyone trying to contact that person can have access to it. Then a message can be encrypted by the pubic of the receiver. That message can only be decrypted by the private key pair of the receiver.

Email encryption can be achieved by using desktop applications or starting from recently also by using browser extent ions. The encrypted email is secured as long as the sender and receiver keep their private keys as secured as possible. The encrypted message is decrypted by anyone who has access to the sender's or receiver's private keys.

Instant Messaging and VOIP Security

In addition to reading texts, watching videos or sending and receiving emails computing devices can be used for instant messaging communications which also include voice and video communication. The common instant messaging applications like Google talk, Yahoo messenger, and Viber do not encrypt the message on the wire. Instant messaging service s and applications should be chosen wisely before starting to use them. The second alternative solution could also be using Instant Messaging applications which can provide end-to-end encryption between the participants. There have been tools created for this in the past. These tools can be used with one of the compatible IM applications to provide

- End-to-End encryption with a temporary encryption key that will serve for the current conversation
- Deniability: The message authentication provides a feature where the two parties can authenticate with each other while in the conversation, but anyone can forge a message to look like from any of them after the conversation. This makes sure there is no digital signature traceable back to the user. [21]

One good example of this technology is Off-the-Record (OTR) Messaging. OTR provides the above features and can be used with a list of open source IM applications like Pidgin or Jitsi. [21]

Figure 12 is a screenshot taken by a one user using Jitsi while the other user using Google talk. When both sides are not using Jitsi, the communication cannot be secured. This conversation can be read on the wire as well as it is saved in plain text in chat history. When both users use Jitsi, the chat communication is encrypted as shows under Figure 13. The chat history

is also saved as encrypted (Figure 14) which enabled security during communication as well as storage.

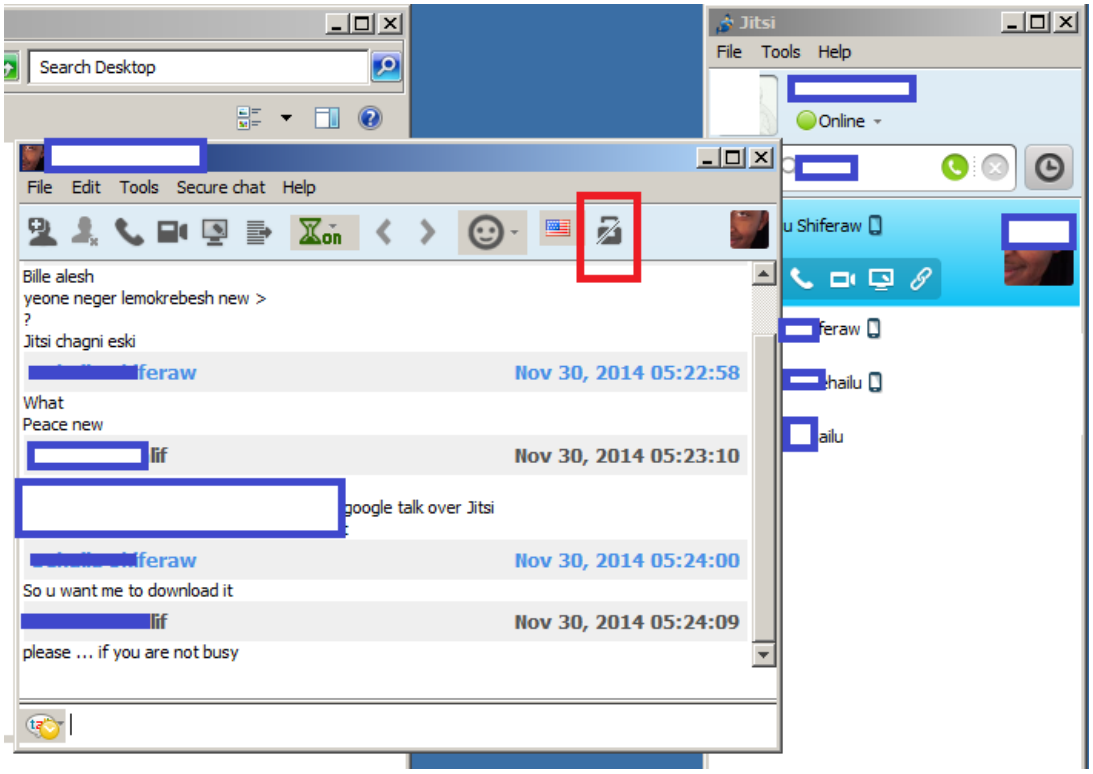

Figure 12. Jitsi before establishing securing

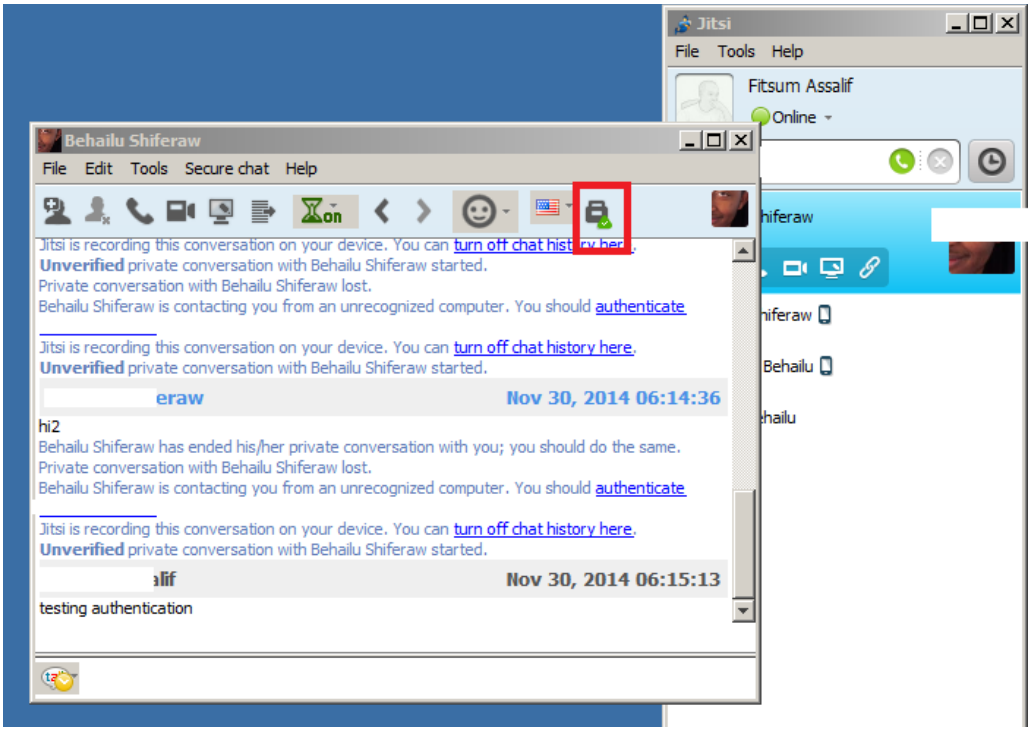

Figure 13. Jitsi after establishing a secure communication

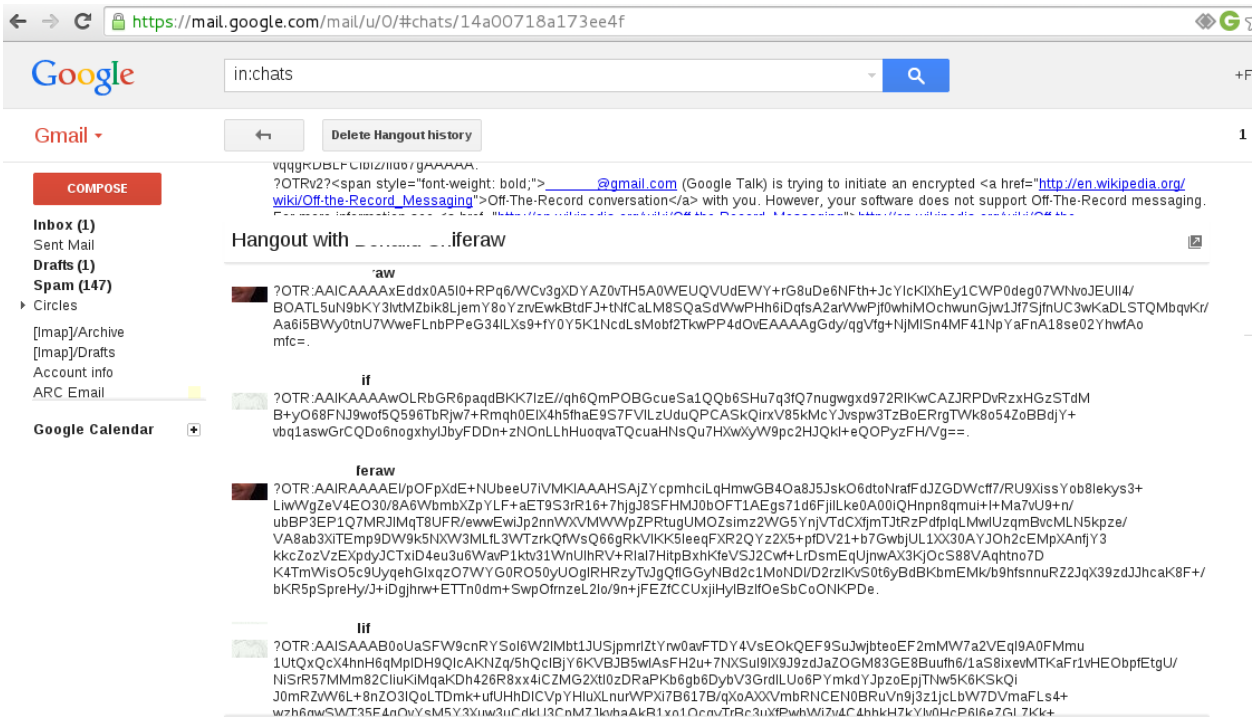

Figure 14. Chat history after using Jitsi for Google talk

File Storage and Backup Security

After the introduction of the cloud, there have been many services provided for file storage and/or backup services online. Some of the commonly used services are Dropbox, Google Drive, Box and SpiderOak. As any other web application, the basic security requirements apply to these file storage services. These requirements are whether the authentication and data transmission is secured, whether the service provider's end user agreement is in line with what we are looking for and finally will the data be handled properly so that it does not be accessed by third party without the user's knowledge or approval.

After taking all these measures it is possible the file will be passed to law enforcement or be accessed by sophisticated mechanisms without user's interest. This factor introduces the need to make sure data is unreadable even if it is finally accessed by government or any other third party. There are a couple of measures to be applied to reach to reasonable protection level.

The first and most common answer to all these security questions comes back to encryption. Users can encrypt data before being uploaded to these third party online file storages. This makes sure the user is the only one which can decrypt the data after being accessed from the site.

The second solution is studying in detail what kind file storage we are using. Per the service offering and descriptions of, SpiderOak can be considered a good example of service provider which provides data storage without actual data knowledge. The company calls this technology ZeroKnowldge [22].

6. User's Habits

Even if all the technological layers of protection are applied on a computing device, the user is the most critical and final component of security. User should take into consideration while all these effort has been applied to protect the machine, the user should be in line not to break those security measures. It is very easy to make a mistake when in hurry or stranded somewhere in an airport, or similar situations because humans tend to forget. There are no step-by-step procedures like a computer software for human behavior. But the main considerations are always to know the service user is using, read privacy notes, follow security and technology news, and maintain the running system. Here are summary of bullet points that are more like reminders of properly applying the technology solutions suggested in the sections above:

- Physically secure your device all the time:
    - Lock device physically to desk or keep it with you all the time
    - When travelling keep computing device in backpack or hand held back with you
    - Keep computing device out of clear sign like car seats, lock it in trunk
- Lock the screen when walking away from device for short time
- Sign out of all accounts and power off device when not using for long hours like more than two to three hours
- Don't login with personal accounts into public shared computers if it is really necessary to use them. Use anonymously or use services like bugmenot.com which provides shared

account to be used on many services without disclosing identity.

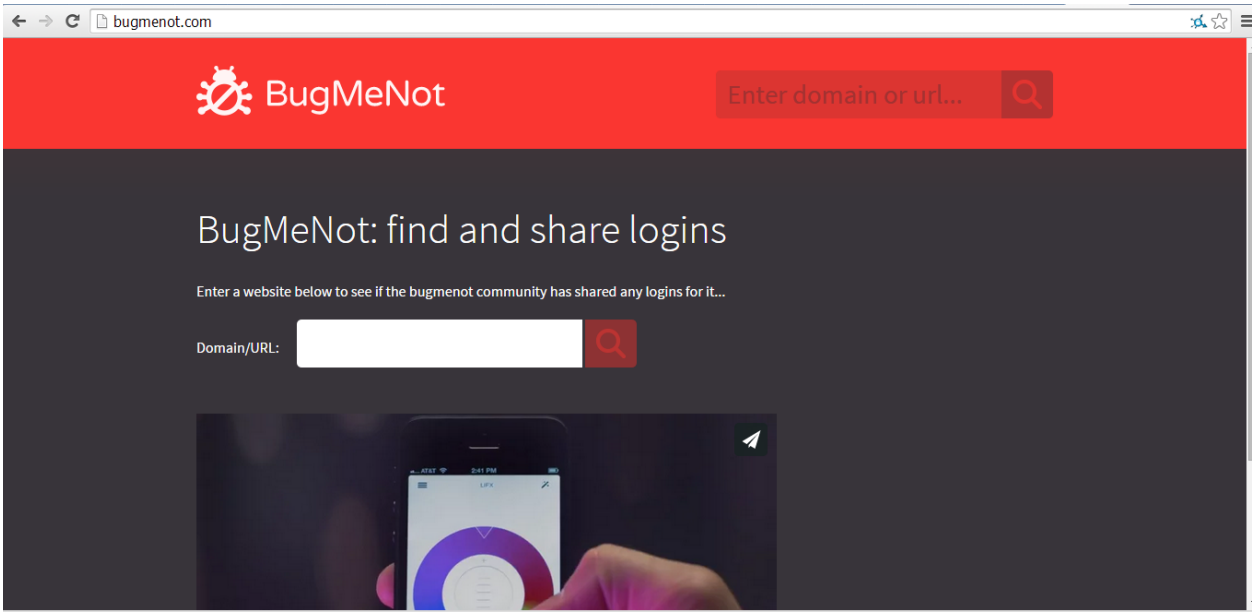

Figure 15. Bugmenot.com providing shared accounts

- Beware of social engineering, always authenticate properly incoming calls and messages regardless of the urgency or how true they look.
- Create awareness to the people you communicate with, live with and share secure connections like home networks with

And last but not least don't give reason for your government to put you on targeted list !

7. Conclusions

Sate sponsored attacks and monitoring to computing devices are growing in each country and they are not going anywhere in near future. These monitoring initiatives are done for many reasons. Some countries do it to control their own citizens while some other countries claim they use it to secure their own citizens against foreign and terrorist spying and attacks.

The main problem with these monitoring activities is citizens not knowing how the data will be handled, used or destroyed. These initiatives are secret due to the nature of the operation and use. Once a user is being monitored and data is collected, there is no control of where that data will end, who will use it and when it will be destroyed. For this reasons, it is recommended to implement a reasonable of protection from these activities.

There is no single key solution to avoid being tracked or attacked by state agencies. Citizens' get their identification systems, services as well as protection from their own government. A good example is social security number, which is the basic item a citizen needs to get any public, financial or public services in United Sates example. This makes it impossible to achieve complete security against government monitoring activities.

Citizens can apply possible security solutions not to leak unwanted information and protect themselves from state sponsored monitoring programs. The technical solutions suggested in the previous chapters guide citizens to a safe use of Internet and their own computing device. They, however, could not be the ultimate guide to hide from one's own government and stay in the shadows for long time.

8. References

[1] Sep 2014. [Online]. Available: https://www.eff.org/nsa-spying/timeline.

[2] Sep 2014. [Online]. Available: http://timerime.com/en/timeline/728928/Electronic+Communication/.

[3] M. Marquis-Boire, B. Marczak, C. Guarnieri and J. Scott-Railton, "FOR THEIR EYES ONLY: The Commercialization of Digital Spying," Toronto, 2013.

[4] D. Storm, Sep 2014. [Online]. Available: http://www.computerworld.com/article/2600348/mobile-security/are-your-calls-being-intercepted-17-fake-cell-towers-discovered-in-one-month.html.

[5] S. Le Blond, A. Uritesc, C. Gilbert, Z. L. Chua, P. Saxena and E. Kirda, "A Look at Targeted Attacks Through the Lense of an NGO".

[6] D. Storm, September 2014. [Online]. Available: http://www.computerworld.com/article/2600348/mobile-security/are-your-calls-being-intercepted-17-fake-cell-towers-discovered-in-one-month.html.

[7] M. Marquis-Boire, "Schrodinger's Cat Video and the Death of Clear-Text," Toronto, 2014.

[8] B. Blunden, The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, 2nd Edition ed., T. Anderson, Ed., Burlington, MA: Jones & Bartlett Learning, 2013.

[9] C. CURRIER and M. MARQUIS-BOIRE, October 2014. [Online]. Available: https://s3.amazonaws.com/s3.documentcloud.org/documents/1348002/rcs-9-technician-final.pdf.

[10] www.finfisher.com, *Remote Monitoring & Deployment Solutions: FINFLY ISP,* 2014.

[11] P. a. R. W. P. James Jay Carafano, "Combating Enemies Online: State-Sponsored and Terrorist use of the Internet," 2008.

[12] "Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software," Washington DC, 2007.

[13] K. K. J. N. Peter Mell, "Guide to Malware Incident Prevention and Handling," 2005.

[14] M. Kassner, Oct 2014. [Online]. Available: http://www.techrepublic.com/blog/it-

security/endpoint-security-what-makes-it-different-from-antivirus-solutions/.

[15] R. Allgeuer, “Why Bother about BIOS Security ?,” 2001.

[16] Ponemon Institute, “The Billion Dollar Lost Laptop Problem,” 2010.

[17] Symantec, “How Whole Disk Encryption Works,” 2014.

[18] G. T. C. T. J.-P. H. J.-Y. L. B. Reza Shokri†, “Protecting Location Privacy: Optimal Strategy against Localization Attacks,” K.U.Leuven, Leuven-Heverlee, Belgium, Cardiff, UK, 2012.

[19] H. Boghosian, Spying on Democracy: Government Surveillance, Corporate Power and Public Resistance, San Francisco: City Lights Books, 2013.

[20] P. Zimmermann, November 2014. [Online]. Available: https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

[21] I. G. a. t. O. D. Team, November 2014. [Online]. Available: https://otr.cypherpunks.ca/.

[22] SpiderOak, November 2014. [Online]. Available: https://spideroak.com/zero-knowledge/.

[23] J. B. X. K. S. C. Corey Kallenberg, *Defeating Signed BIOS Enforcement,* 2014.