Protecting Internet Traffic: Security Challenges and Solutions

Mohammed Aledhari, Western Michigan University, Sukanya Mandal, Nagender Aneja, Universiti Brunei Darussalam, Mikael Dautrey, Rajesh Nighot, Independent Consultant, Prasad Mantri, Jared Bielby, Independant Consultant

May 2017

Disclaimer

This document represents the considered judgement and personal views of the participating individuals listed on the following page with expertise in the subject field. It shall not be considered the official position of IEEE or any of its committees, and shall not be relied upon as a formal position of IEEE. It is produced by the IEEE Internet Initiative to enhance knowledge and promote discussion of the issues addressed.

Authors and Editors

Authors

- Mohammed Aledhari, Western Michigan University
- Sukanya Mandal
- Nagender Aneja, Universiti Brunei Darussalam
- Mikael Dautrey
- Rajesh Nighot, Independent Consultant
- Prasad Mantri
- Jared Bielby, Independant Consultant

Editors

- Sherrill Fink, Independant Technical Writer
- Nagender Aneja, Universiti Brunei Darussalam
- Mohammed Aledhari, Western Michigan University
- Jared Bielby, Independant Consultant
- Ali Kashif Bashir, Editor-in-Chief, IEEE Internet Policy Newsletter

Table of Contents

Executive Summary

The purpose of the following white paper is to present a set of well- investigated internet traffic security guidelines and best practices which others can use as a basis for future standards, certifications, laws, policies and/or product ratings. While most, if not all of the following guidelines apply to all internet-connected devices, the presented guidelines focus on internet traffic security best practices for wired or wireless networks. They detail security mechanisms necessary for consideration at the manufacturing design phase rather than after deployment of devices to internet service providers and end users. The paper leads with the assertion that a thorough study on protecting internet traffic does not yet exist, and proposes, based on our findings, that existing technology is not yet sufficient to meet the goal of protecting internet traffic. The best practices presented are centered around countering and preventing malicious activity. By setting up a secure network with industry standard security protocols, the risk and potential legal liabilities associated with an unsecured network can be proactively addressed.

Introduction

The purpose of the following white paper is to present a set of well- investigated internet traffic security guidelines and best practices which others can use as a basis for future standards, certifications, laws, policies and/or product ratings. While most, if not all of the following guidelines apply to all internet-connected devices, the presented guidelines focus on internet traffic security best practices for wired or wireless networks. They detail security mechanisms necessary for consideration at the manufacturing design phase rather than after deployment of devices to internet service providers and end users. The paper leads with the assertion that a thorough study on protecting internet traffic does not yet exist, and proposes, based on our findings, that existing technology is not yet sufficient to meet the goal of protecting internet traffic. The best practices presented are centered around countering and preventing malicious activity. By setting up a secure network with industry standard security protocols, the risk and potential legal liabilities associated with an unsecured network can be proactively addressed.

The paper is the result of a year-long research project by the IEEE Technology Policy Community working group for Protecting Internet Traffic. The Protecting Internet Traffic working group, an informal gathering of scholars, engineers and others within and outside IEEE membership, was formed in 2015 to provide a platform for follow-up discussions and activities coming out of the IEEE Internet Initiative events for Experts in Technology and Policy (ETAP).

Several localized ETAP events took place in 2015 and 2016 in various regions around the world, including Israel, China, India and the United States. These events brought together technologists, policy-makers and others with an interest and expertise in technology policy. Of the many internet technology policy concerns discussed during these events, the topic of protecting internet traffic was deemed a critical issue. As a result, several individuals decided to form a working group on protecting internet traffic, and to write a technical paper that provides foundational knowledge of the salient issues to an educated lay audience, including lawmakers, corporate and governmental policy makers, manufacturers, engineers and end users.

The group proposed a working hypothesis as a basis of its research project. They posited the following:

- While the Internet is an open and transparent network that carries unicast, multicast, or broadcast messages from a source station to one or more destination stations,
- The various nodes between the two stations are not known by the two stations; there may be as many nodes as required to connect the two stations and the path between the two stations may vary.
- While the stations are responsible for the transport layer (checking that each packet it sends to the other station is received, and so on), and where two stations may reside on a private network that control / protect the stations.
- When stations first connect, the two stations may or may not trust each other.
- It is posited here that the nodes involved in the connection and transport of packets are neither reliable nor trustworthy – some nodes may be attackers.

- However, some specific nodes and some specificity policies in the network may protect the network infrastructure against malicious stations. These include congestion control and many others. The more specific policy has higher priority. e.g. policy applied for a particular user has higher priority than a policy applied for all users.

Confidentiality, Integrity, and Availability (CIA)

Any classic definition of Internet security encompasses Confidentiality, Integrity, and Availability (CIA) [1]. On the Internet, Transport Layer Security (TLS) [2] / Secure Sockets Layer (SSL) [3] addresses Confidentiality and Integrity. TLS/SSL may have flaws, mainly in the randomness of key generation and the negotiation of security parameters between the two stations. But TLS/SSL is still one of the most proven security mechanisms on the Internet. Availability is providing access to the information by authorized users. The design principle of the Internet as a whole is expressed by the characteristics of Connectionless, Dynamic Routing, and Best Effort.

These mechanisms were implemented to deal with the failure of nodes. They are not appropriate when trying to drop the traffic of thousands of malicious stations. More generally, the design of the Internet is based on the assumption of cooperative nodes. In the present Internet, nodes do not operate in a trusted environment. Some major gaps have been treated, such as unsecured domain name system (DNS) with DNS secure (DNSSEC). But there are still major problems such as border gateway protocol (BGP) hijacking. Consequently, availability is still a challenge in today's Internet.

The classic definition of security is a prerequisite to define Internet traffic protection, but it is not sufficient. Technically, protection is more than one-to- one connection security. Studies demonstrate that meta-information about traffic leaks information on traffic header as well as on protocols used and related activities. Such meta-information is revealed by analyzing traffic patterns such as packet size, bandwidth consumption, and packet rate. As such, an attacker may decipher identities of the parties involved in any given connection by analyzing traffic pattern entering and exiting, even on an encrypted network such as Tor.

Protecting Traffic Comprises Managing Anonymity and Trust

Internet users need more than CIA. In an open network, managing anonymity and trust is critical. Moreover, as Internet transactions are asymmetrical, a user may require anonymity on his side and trust on the identity of the other station. Two tools try to answer these needs; Tor [4] and public key infrastructure (PKI) [5]. Tor network manages anonymity at a global scale. Tor is rather efficient but is not integrated in the Internet technology stack. PKIs manage trust. But there are barriers to their use.

Namely, if an organization needs a certificate that is recognized by browsers, they have to pay for it. For many reasons (price, complexity, etc.), many organizations use unregistered certificates for various services. As a result, users are accustomed to validating self-signed certificates. And as long as users validate self-signed certificates, we have only a pretense of actual trust. This can affect a large number of users if a node in the chain is compromised by an attacker.

Protecting Traffic Comprises Protecting the Network

As stated above, protecting traffic requires CIA in terms of both the network and its traffic transactions from potentially malicious interactions with other traffic, and includes routing, congestion, anti-distributed denial of service (DDOS) management [6], and mitigating the "Man in The Middle" attacks [7]. Understanding the risks entailed, it becomes critical to ask a.) How a network node can trust a station or another node it does not know, and b.) How a station can trust a network node it does not know.

Protecting a Station Inside a Private Network: The Security Versus Privacy Dilemma

Organizations that manage stations face the dilemma of encryption by default to protect traffic and decryption at the edge to block malicious traffic and sometimes control people inside the organization. SSL gateways are deployed to answer this need. They are resource-intensive, and they break the encryption layer between the stations.

Protecting Internet of Things (IoT)

The IoT [8] is rapidly expanding from light bulbs to industrial equipment. However, the Internet is an unreliable place for stations managed by people. It can be questioned whether it is even possible to keep automated stations safe on the Internet as it is.

Protecting Internet Traffic: Concerns

Many initiatives try to define new architectures to sort out the various weaknesses of the Internet, some examples being Recursive Networking Architecture, Named Data Networking and Software defined networking. The Protecting Internet Traffic working group has identified four major challenges and technical options for addressing these weaknesses:

1. *Writing a Formal definition of Protecting Internet Traffic:* We think it should be possible to write a formal definition of protecting Internet traffic, building on the formalism of modern cryptography.
2. *Designing a general solution to the problem of trust between stations and nodes, and between nodes:* We expect that new trust models such as block chain could be an effective part of the solution.
3. *Supervising traffic while preserving anonymity:* We expect that homomorphic cryptography technologies may help in this field.
4. *Managing congestion, malicious traffic and numerous rare traffic patterns:* We may expect that embedding Artificial Intelligence (AI) in routers may help deal with these needs.

Protecting Internet Traffic: Towards A Solution

Protecting internet traffic is essential for protecting personal and business information. High-profile attacks allow hackers to steal credit and debit card information, damaging reputations and causing financial havoc for victims. Business data is also at risk. Alone, computers are powerful tools. The Internet, however, provides even more potential for both power and misuse. For businesses and government entities, the Internet provides a means of allowing customers to handle accounts without having to come to a physical location or communicate via phone. However, when Internet-accessible information is not secured, the consequences can be disastrous. Databases often store social security numbers and credit card information, which can be used to rob victims and steal identities. We define an unsecured network as a network that does not require any credentials to use a gateway to the Internet. Using an unsecure network can result in numerous unwanted consequences including password and internet traffic capture, the compromise of company data, the theft of client/customer personal information, and legal repercussions for negligence.

Communication via an unprotected network enables a malicious savvy user to access and disturb user and/or organization systems. Once unauthorized individuals enter a network, they can capture email correspondences and website traffic logs. This means that they can gather client information, website traffic information (such as where and how users connect), and user personal information. Thus, communicating through an unsecured network becomes dangerous, potentially costing both the organization and customers.

Once unauthorized people have tapped into the network, it is very easy for them to start collecting data, such as client profiles and customer personal information, and even damage the organization's computers. As more organizations move to cloud-based operations, Internet security becomes even more important. The cloud paradigms require that information be made available over the Internet; personal documents are stored on remote servers. Top-notch security is essential for preventing this information from being stolen. Businesses, in particular, are at greater risk; stolen internal documents can cause a tremendous amount of harm. Internet traffic must be secured physically and non-physically.

Internet Traffic Perimeter Protection

Physical Access

The physical security of the network is a very important factor to prevent unauthorized access. Insiders pose risk accidently or intentionally. An operator may load flash drive and introduce a virus unknowingly or disgruntled employees may unplug cables or tamper with cables. Securing all wiring closets and buildings of the network infrastructure components can reduce significant risks and threats by banning unauthorized users and hackers having physical access.

Ensuring Device Security

Many Internet-connected appliances, such as cameras, televisions sets, and kitchen appliances are already enabled to spy on people in their own homes.

Such devices accumulate a lot of personal data that gets accessed by other devices or is held in databases by organizations. Five main factors of smart device development can help manufacturers ensure security:

1. Secure booting
2. Access control
3. Device authentication
4. Firewall and intrusion prevention system (IPS)
5. Updates and patches

Beyond that, however, Internet traffic security measures must be addressed throughout the entire lifecycle of all network equipment, from the initial design, the operational environment, the disposal and the recycling. The networking equipment can contain sensitive information as how to access the system or server and this information may be exploited by competitors or agents looking to harm the user. While manufacturers are responsible for implementing security-by-design, organizations and end users should also review security aspects of the equipment or device that they are going to deploy.

Network Segmentations

Dividing the network(s) into small networks using virtual local area network (VLAN) [9] is another factor to secure the network physically. For example, separating the network based on traffic (public access, voice over Internet Protocol (IP) [10], streaming, storage area network (SAN) [11], de-militarized zone (DMZ)) [12] or user (worker, administration, visitor) types.

Virtual Private Network (VPN)

A VPN [13] gives a user a simple, controllable and secure way of connecting to Internet. A VPN creates a secure, encrypted connection just like a tunnel between the user and the network server. The VPN service providers market has doubled over the last 3 years. The VPN market size was 45 billion U.S dollars in 2014 and is expected to reach 70 billion U.S dollars by 2017 [14]. VPN services are now widely used for protecting internet traffic by number of users including corporates across the world.

In a VPN, all network traffic is passed through a protected VPN tunnel, and outsiders are unable to track a user continuously. In this way, both the data and privacy are protected while being connected to the Internet. Encryption through VPN is not foolproof, however, it is still the most efficient method of keeping the identities of users unknown to hackers or malicious software. A highly skilled hacker can always breach security through internet connections; however, a VPN can protect against mass data collection and casual access to personal data for commercial benefit or targeted attack. A VPN is very useful for users connecting on shared Wi-Fi or public internet networks, because it can hide the IP address of user devices thereby preventing continuous tracking of said devices. A VPN can also be used for protecting internet traffic of mobile phones by assisting in protecting against theft. In general, a VPN is very effective at encrypting all internet traffic and can ensure that all data is kept hidden. A VPN can be employed by private and Government organizations as Remote access VPN, Intranet VPN, Extranet VPN, or WAN replacement.

A VPN can be classified as follows:

1. Firewall-based VPN
2. Hardware-based VPN
3. Software-based VPN
4. SSL or TLS protocol based VPN

A number of known performance problems with VPN services exist though users and organizations still choose to use them. For example, VPNs are known to slow down Internet connection. The internet traffic goes through a number of steps before the user device can be connected to the outside world, and therefore, Internet speed is likely to be sluggish. VPNs have improved greatly over the last three years and now provide high performance, making VPNs more comparable in speed than they used to be.

Many VPN service providers collect individual data. Therefore, both privacy and transparency policies should be reviewed prior to installing the VPN service. If the VPN user authentication is not strong, then unauthorized access to the network cannot be ruled out. As such, stronger user authentication is necessary for VPN users. The user devices can be infected with malicious software or malware. If this happens, when those devices connect to a VPN, the user authentication or password can be leaked to the attacker. The malware can also spread across to other network devices.

Interoperability over a VPN is often a problem, since compliant software from different vendors may not be able to work together and exchange or interpret information.

The Firewall

A firewall [15] is a hardware or software system that prevents unauthorized access to or from a network. It can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All data entering or leaving the Intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria. Generally, firewalls are configured to protect against unauthenticated interactive logins from the outside world. This helps prevent hackers from logging onto machines on one's network. More sophisticated firewalls block traffic from the outside to the inside but permit users on the inside to communicate a little more freely with the outside.

Firewalls are essential since they provide a single block point where security and auditing can be imposed. Firewalls provide an important logging and auditing function. Often, they provide summaries to the administrator about what type/volume of traffic has been processed through it. There are at least five basic firewall types:

1. Packet-filtering firewalls [16] operate at the router and compare each packet received to a set of established criteria (such as allowed IP addresses, packet type, port number, etc.) before being either dropped or forwarded.
2. Circuit-level gateways [17] monitor the transmission control protocol (TCP) [18] handshaking going on between the local and remote hosts to determine whether the session being initiated is legitimate and whether the remote system is considered "trusted." They do not inspect the packets themselves, however.
3. Stateful inspection firewalls [19], on the other hand, not only examine each packet but also keep track of whether or not that packet is part of an established TCP session. This feature offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.
4. Application-level gateways (proxies) [20] combine some of the attributes of packet-filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service for which they are intended (as specified by the destination port), but also by certain other characteristics such as hypertext transfer protocol (HTTP) [21] request string. While application-level gateways provide considerable data security, they can dramatically impact network performance.
5. Multilayer inspection firewalls [22] combine packet filtering with circuit monitoring, while still enabling direct connections between the local and remote hosts, which are transparent to the network. They accomplish this by relying on algorithms to recognize which service is being requested, rather than by simply providing a proxy for each protected service. Multilayer firewalls work by retaining the status (state) assigned to a packet by each firewall component through which it passes on the way up the protocol stack. This gives the user maximum control over which packets are allowed to reach their final destination but again affects network performance, although generally not so dramatically as proxies do.

ENSURING APPLICATION SECURITY

Application security [23] is considered the traditional element of internet traffic security, because most security breaches started out at the application layer. The goals of application security are to protect the following:

1. Confidentiality of data within the application.
2. Availability of the application.
3. Integrity of data within the application.

Beyond these three technical goals, protecting user's privacy has become paramount. As applications are more and more distributed, multi-tenants, privacy is a stronger objective than confidentiality. First, it supposes that there may be many containers inside an application, each container negotiating access to other containers data. Second, privacy has more to do with information than with data. Various Internet users side-channel fingerprinting methods demonstrate that information leaks more easily than data, even in a protected environment. Hacking has developed from a pastime with bragging rights to a serious, high-money business with innocent users as the victims. Governments all over the world have enacted regulations regarding the security of personal information (PI), with significant civil and criminal penalties to back up the regulations. No software provider can afford to ignore the importance of privacy. Data confidentiality is protected when the data cannot be read during transit or the data cannot be stolen while at rest. But privacy is more than confidentiality and is still a challenge, to specify and to implement.

AUTHENTICATION

Authentication and encryption mechanisms on the wired side of the network are often ignored because they are expensive and complex. Deploying 802.1X authentication [24] would not encrypt the Ethernet traffic, but also, they would not allow unauthorized users to access any network until they have provided login credentials. Also, 802.1X for authentication can be used on the wireless side as well, to implement enterprise-level Wi-Fi Protected Access 2 (WPA2) [25] security with advanced encryption standard (AES) encryption, which has many benefits over using the personal-level pre- shared key (PSK) of WPA2.

Another great benefit of 802.1X authentication is the ability to dynamically assign users to VLANs. Authentication is an absolutely essential element of a typical security model. Authentication is defined as the process of confirming the identification of a user (or in some cases, a machine) that is trying to log on or access resources. A number of different authentication mechanisms exist, but all serve this same purpose. Another element of the security plan is authorization. While authentication verifies the user's identity, authorization verifies that the user in question has the correct permissions and rights to access the requested resource. The two work together. Authentication occurs first, then authorization.

There are several physical means by which one can provide one's authentication credentials to the system. The most common—but not the most secure—is password authentication. Today's competitive business environment demands options that offer more protection when network resources include highly sensitive data. Smart cards, one time password, and biometric authentication types provide this extra protection.

Digital certificates [26] are also used for authentication and securing of communications, especially on unsecured networks (for example, the Internet). Certificates associate a public key to a user or other entity (a computer or service) that has the corresponding private key. Certificates are issued by certification authorities (CAs), which are trusted entities that

"vouch for" the identity of the user or computer. The CA digitally signs the certificates it issues, using its private key. The certificates are only valid for a specified time period; when a certificate expires, a new one must be issued. The issuing authority can also revoke certificates. Certificate services are part of a network's Public Key Infrastructure (PKI). Standards [27] for the most commonly used certificates are based on X.509 specifications.

ENCRYPTION

Encryption [28] is a mechanism for changing readable text, called plaintext, into an unreadable format, called ciphertext. Encryption mechanisms not only protect the confidentiality of data but also ensure that data have not been altered during transit and verifying the identity of the sender.

Encryption can be used for both wired and wireless networks. Encryption can be applied to two levels of the traffic lifecycle, which are application (most common) and protocol levels. Also, many encryption algorithms and techniques can be used to encrypt the traffic. Encryption techniques include symmetric, and asymmetric mechanisms. Hashing is a by-product of encryption, to guarantee messages integrity.

Symmetric Cryptography encryption [32] uses a secret key, called the shared secret, to scramble the data into unintelligible gibberish. The sender and receiver need to use the same key for encryption and decryption operations.

Asymmetric cryptography [33] uses encryption that splits the key into two smaller keys. One of the keys is public to be used for encryption operation and the other one is private to be used for decryption operation.

Encryption Algorithms

Today, strength of encryption is usually measured by key size. No matter how strong the algorithm, the encrypted data can be subject to brute force attacks in which all possible combinations of keys are tried. Eventually the encryption can be cracked. For most modern ciphers with decent key lengths, the time to crack them with brute force them is measured in millennia. However, an undisclosed flaw in an algorithm or an advance in computer technology or mathematical methods could sharply decrease these times. Generally, the thinking is that the key length should be suitable for keeping the data secure for a reasonable amount of time. If the item is very topical, such as battlefield communications or daily stock information, then a cipher that protects it for a matter of weeks or months is just fine. However, something like your credit card number or national security secrets need to be kept secure for a longer period, effectively forever. So, using weaker encryption algorithms or shorter key lengths for some things is okay, as long as the information usefulness to an outsider expires in a short amount of time. Some of encryption algorithms are listed below:

Data Encryption Standard (DES)

DES [34] is the original standard that the U.S. government began promoting for both government and business use. Originally thought to be practically unbreakable in the 1970s, the increase in power and decrease in cost of computing has made its 56-bit key functionally obsolete for highly sensitive information. However, it is still used in many commercial products and is considered acceptable for lower security applications. It is also used in products that have slower processors, such as smart cards and appliance devices that can't process a larger key size.

Triple DES

Triple DES [35], or 3DES as it is sometimes written, is the newer, improved version of DES, and its name implies what it does. It runs DES three times on the data in three phases: encrypt, decrypt, and then encrypt again. While it doesn't give a threefold increase in the strength of the cipher (because the first encryption key is used twice to encrypt the data and then a second key is used to encrypt the results of that process), it still gives an effective key length of 168 bits, which is plenty strong for almost all uses. Symmetric keys negotiation is often protected by Diffie-Hellman (DH).

Advanced Encryption Standard (AES)

When the U.S. government realized that DES would eventually reach the end of its useful life, it began a search for a replacement. The National Institute of Standards and Technology (NIST), a government standards body, announced an open competition for a new algorithm that would become the new government standard called AES [36]. There were many competitors including RC6 [37], Blowfish [38] by renowned cryptographer Bruce Schneier, and other worthy algorithms. They settled on AES, which is based on an algorithm called Rijndael, designed by two Belgian cryptographers.

This is significant because they used an open competition to decide on the standard. Also, selecting an algorithm by two non-American developers with no significant commercial interests helped to legitimize this selection worldwide. AES is rapidly becoming the new standard for encryption. It offers up to a 256-bit cipher key, which is more than enough power for the foreseeable future. Typically, AES is implemented in either 128- or 192-bit mode for performance considerations.

Blowfish

Blowfish [38] is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually. Blowfish is known for both its tremendous speed and overall effectiveness as many claims that it has never been defeated. Meanwhile, vendors have taken full advantage of its free availability in the public domain. Blowfish can be found in software categories ranging from e- commerce platforms for securing payments to password management tools, where it used to protect passwords. It is definitely one of the more flexible encryption methods available.

Twofish

Computer security expert Bruce Schneier is the mastermind behind Blowfish and its successor Twofish [39]. Keys used in this algorithm may be up to 256 bits in length, and as a symmetric technique, only one key is needed.

Twofish is regarded as one of the fastest of its kind and is ideal for use in both hardware and software environments. Like Blowfish, Twofish is freely available to anyone who wants to use it. As a result, you will find it bundled in encryption programs such as PhotoEncrypt [40], GPG [41], and the popular open source software TrueCrypt [42].

Rivest, Shamir, and Adelman (RSA)

RSA [43] is a public-key encryption algorithm and the standard for authenticating stations over the Internet (IPSEC/IKE, SSL authentication). It also happens to be one of the methods used in PGP and GPG programs [41]. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. It consists of the public key, which is used to encrypt the message, and a private key to decrypt it. RSA is mostly used in hybrid encryption schemes to exchange symmetric key or digital signature. In most web applications, file is encrypted with a symmetric key and the symmetric key is encrypted with RSA. In case of digital signature, the private key is used for encryption so that receiving party is sure that file has not been altered.

RC4, RC5, and RC6

RC_ is an encryption algorithm developed by Ronald Rivest [44], one of the developers of RSA, the first commercial application of public key cryptography. Improvements have been made over time to make it stronger and fix minor issues. The current version, RC6, allows up to a 2,040-bit key size and variable block size up to 128 bits.

The Future of Encryption

Cyber-attacks are constantly evolving, so security specialists must stay busy in the lab concocting new schemes to keep them at bay. Expert observers are hopeful that a new method called Honey Encryption [45] will deter hackers by serving up fake data for every incorrect guess of the key code.

This unique approach not only slows attackers down, but potentially buries the correct key in a haystack of false hopes. In addition, there are emerging methods like quantum key distribution [46], which shares keys embedded in photons over fiber optic, that might have viability now and many years into the future as well.

Encryption Applications

Hashes

Hashes [29] are a special use of one-way functions to provide authentication and verification using encryption. A hash function takes a file and puts it through a function so that it produces a much smaller file of a set size. By hashing a file, you produce a unique fingerprint of it. This gives you a way to make sure that the file has not been altered in any way. By hashing a suspect file and comparing the hash to the known good hash, you can tell if any changes have been made. It is unlikely that a file with a different structure would produce an identical hash. Even changing one character changes the hash significantly. The chances of two different files producing the same hash are infinitesimal.

Hashes are often provided on downloaded versions of software to make sure you are getting the real thing. This is important, especially with open source software, where it may have been passed around quite a bit or downloaded from another site. The official Web site will usually post the correct hash of the latest version. If the two do not match, then clearly some changes have been made, possibly without the permission or knowledge of the software developers. The most popular hashing algorithm is called MD5. Some common hashing algorithms are Message Digest 5 (MD5) [30] and Secure Hashing Algorithm (SHA) [31].

Digital Certificates

Digital certificates [26] are the "signature" of the Internet commerce world. These use a combination of encryption types to provide authentication. They prove that who you are connecting to is really who they say they are. In other words, a certificate is a "certification" of where the information is coming from. A certificate contains the public key of the organization encrypted with either its private key or the private key of a signing authority. Using a signing or certificate authority is considered the more secure method of the two. If you can decrypt the certificate with the public key, then you can reasonably assume the Web site belongs to that organization.

Certificates are usually tied to a particular domain. They can be issued by a central entity, called a Certificate Authority (CA), or created and signed locally as described above. There are several of these organizations, the biggest of which is VeriSign [47], the company that also runs the domain names system. They have sanctioned many other companies to offer certificates under their authority. Getting a certificate from VeriSign or one of the companies it authorizes is like having someone vouch for you. Generally, they will not issue you a certificate until they verify the information you are putting in the certificate, either by phone or via some kind of paper documentation, such as a corporate charter. Once they "certify" you, they will take this information, including the URLs you are going to use the certificate for, and digitally "sign" it by encrypting it with their private key.

Then a Web server or other programs can use this certificate. When outside users receive some data, such as a Web page from the server, and it has a certificate attached, they can use public key cryptography to decrypt the certificate and verify your identity. Certificates are used most often at e- commerce Web sites, but they can also be used for any form of communications. Secure shell (SSH) [48] and Nessus [49] both can use certificates for authentication. VPNs also can use certificates for authentication instead of passwords.

Pretty Good Privacy (PGP)

PGP was created by Phil Zimmerman in 1991 to provide easily accessible and usable encryption technology. There are both open-source and commercial implementations of PGP, some of them specifically adapted to niche applications like email encryption.

Encryption Protocols

IPsec

The IP protocol as originally designed was resilient, not secure. IP version 4 (IPv4), which is what most of the world uses for IP communications, does not provide any kind of authentication or confidentiality. Packet payloads are sent in the clear, and packet headers can easily be modified since they are not verified at the destination. The IP Protocol was designed to not include security so that the system is easy for developer. However, many Internet attacks rely on this basic insecurity in the Internet infrastructure. A new IP standard, called IPv6, was developed to provide authentication and confidentiality via encryption. It also expanded the IP address space by using a 128-bit address rather than the 32-bit currently used, and improved on several of other things as well. Fully implementing the IPv6 standard would require wide-scale hardware upgrades, so IPv6 deployment has been slow.

However, an implementation of security for IP, called IPsec [51], was developed that would not require major changes in the addressing scheme. Hardware vendors have jumped on this, and IPsec has gradually become a de facto standard for creating Internet VPNs. IPsec is not a specific encryption algorithm, but rather a framework for encrypting and verifying packets within the IP protocol. IPsec can use different algorithms and can be implemented in whole or just partially. A combination of public key and private key cryptography is used to encrypt the packet contents, and hashes add authentication as well. This function is called Authentication Header (AH). With AH, a hash is made of the IP header and passed along. When the packet arrives at the destination, a new hash is made of each header. If it does not compare to the one sent, then the header has been altered somehow in transit. This provides a high level of assurance that the packet came from where it says it does. You may choose to do encryption of the packet payload but not do AH, as this can slow down the throughput. AH can also get delayed or stalled in some environments with network address translation (NAT) or firewalls. There are also different two operation modes IPsec can be run in tunnel mode or transport mode. In tunnel mode, the entire packet—header and all—is encapsulated and encrypted, placed in another packet, and forwarded to a central VPN processor. The endpoints decrypt the packets and then forward them to the correct IP. A benefit of this method is that outsiders cannot even tell what the final destination is for the encrypted packet. Another advantage is that the VPN can be controlled and administered from a few central points. The downside is that this requires dedicated hardware at both ends to do the tunneling. In transport mode, only the packet payloads are encrypted; the headers are sent intact. This makes deployment a little easier and requires less infrastructure. You can still use AH when using transport mode and verify the source address of the packets.

Point-to-Point Tunneling Protocol (PPTP)

PPTP [52] is a standard that was developed by Microsoft, 3Com, and other large companies to provide encryption. Microsoft has added it to Windows 98 and later releases. This made it seem a likely candidate to be the major standard for widespread encryption technology. However, some major flaws were discovered in PPTP, which limited its acceptance. When Microsoft bundled IPsec with Windows 2000, it seemed a tacit admission that IPsec had won as the new encryption standard. However, PPTP is still a useful and inexpensive protocol for setting up VPNs between older Windows PCs.

Layer Two Tunneling Protocol (L2TP)

L2TP [53] is another industry-developed protocol, endorsed by Microsoft and Cisco. Although used frequently in hardware-based encryption devices, its use in software is relatively limited.

Secure Socket Layer (SSL)

The SSL [3] protocol was designed specifically for use on the Web, although it can be used for almost any type of TCP communications. Netscape originally developed it for their browser to help stimulate e-commerce. SSL provides data encryption, authentication on both ends, and message integrity using certificates. Most of the time, SSL is used when connecting to a Web server to ensure the information sent is being protected along the way. Most people do not even realize that SSL is running in the background. Usually it only authenticates one end, the server side, since most end users don't have certificates.

Encryption of Networks

Encryption of wired networks

Wired encryption is not commonly used, other than in highly classified facilities like military or defense contractors, because it is expensive to implement. However, internet protocol security (IPSec) protocol is commonly used to secure wired networks.

Encryption of wireless networks

The three main encryption methods of wireless include: hashing, symmetric cryptography or shared secret encryption, and asymmetric cryptography or public key encryption (PKE). Cryptography is defined as "the science and study of secret writing," that converts data into unreadable formats for unauthorized users.

End User Education and Employee Training

While the above study outlines effective procedures and best practices for protecting Internet traffic, no technology no matter how secure can prove efficient without also including an active role of the End-user. The End-user must be educated and held accountable to their knowledge and participation in effective Internet security. At the end of the day, education is not a minor security issue and cannot be replaced by adding more technology and security engineering. Most network attacks happen due to a lack of security awareness by both organization employees and end users. Without the participation of the end users, the technology alone cannot accomplish its intended task ultimately due to the control users have over their devices.

Thus, the four fundamental countermeasures for defending information and data are technology, operations and awareness, training, and education. The failure of any one of these measures can result in a total failure of securing an organization's valuable assets and end user data. An effective synthesis of all the above factors are part of digital literacy or digital skills that all End- users need be aware of.

When educating end users and employees, it is vital to explain the common risks and weaknesses of networks and how to prevent internet attacks. The most common attacks target open TCP/user datagram protocol (UDP) [54] ports, open serial ports, open password prompts, various places to inject code – web servers, unencrypted traffic and so forth, and radio communications. However, training End-users and employees about security best practices must include physical, technical and operational (or Procedural) factors. In the search for and implementation of high-end technology solutions, there is a tendency to neglect, overlock or simply not even recognize the common-sense or traditional factors at paly in effective security best practices which form the foundation of the security necessary to ensure the protection of Internet Traffic. It is to everyone's detriment if these factors are not viewed as Internet security protocols. Internet Security begins with physical security and then build on physical security with technical security.

Examples of physical security best practices include the effective training and use of guards, mantraps (access control vestibule), common locks, biometric devices, hard tokens, ID badges, sufficient building lighting, effective fencing, and location. Only with a basis of physical factors to buttress security can technical security best practices be implemented. Examples of technical security best practices include training in the use of Firewalls, the use Proxy Servers, the use of secure applications that utilize secure communication path such as SSL, WPA2 protocols, and knowledge and education on the value of disabling applications that are not required. Again, neglecting the assumed or established foundation of digital skills and digital literacy is detrimental. As such, the continued placement of priorities on common sense strategies is the beginning of best practices. Common sense strategies include, for instance, not replying to emails from suspicious sources, not opening suspicious or unsolicited links, and maintaining security and privacy of passwords (don't share passwords with others). Examples of operational security best practices include an overarching security policy, acceptable use policies, security awareness training policy, clean desk policy, mobile device policy, a business continuity plan, disaster recovery policies, and incident response procedures. It is only through the combination of sound technology, end-user education and effective and accountable policy that protecting Internet traffic can become an efficient reality.

Conclusion and Future Directions

Understanding the intricacies of protecting internet traffic is critical to the future of internet infrastructure and use, especially in terms of imminent IoT applications. From manufacturer accountability to end-user education, protecting internet traffic falls to all involved in the proliferation and use of internet technologies.

Internet traffic can be secured using hardware and software tools and algorithms. Encryption and authentication are at the core of internet traffic protection. People who are part of the system need to be educated about their roles in securing internet traffic. The challenge is to be able to effectively apply this knowledge to current and future applications of internet technologies. The goal of the working group on Protecting Internet Traffic was to present an informed overview of internet traffic security guidelines and best practices for use as a foundation to further research for future standards in technology and policy. Its purpose was to posit guidelines that detail security mechanisms necessary in the manufacturing of internet technologies. As IoT and other internet applications become further entrenched in day to day security transactions, trustworthy standards need to guide the process of protecting internet traffic. While a thorough study on protecting internet traffic does not yet exist, we hope that the above posited guidelines might serve as a starting point to bolstering existing technology to sufficiently meet the goal of protecting internet traffic. By setting up a secure network with industry standard security protocols, the risk and potential legal liabilities associated with an unsecured network can be proactively addressed, ensuring a safe and secure internet that can be enjoyed by all.

References

[1] Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. Communications of the ACM, 43(7), 125-128.

[2] Dierks, Tim. "The transport layer security (TLS) protocol version 1.2." (2008).

[3] Freier, A., Karlton, P., & Kocher, P. (2011). The secure sockets layer (SSL) protocol version 3.0.

[4] Bauer, K. S., Sherr, M., & Grunwald, D. (2011, August). ExperimenTor: A Testbed for Safe and Realistic Tor Experimentation. In CSET.

[5] Nash, A., Duane, W., & Joseph, C. (2001). PKI: Implementing and Managing E-security. McGraw-Hill, Inc.

[6] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

[7] Desmedt, Y. (2011). Man-in-the-middle attack. In Encyclopedia of Cryptography and Security (pp. 759-759). Springer US.

[8] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[9] Chan, K. K., Hartmann, P. W., Lamons, S. P., Lyons, T. G., & Milonas, A. C. (1989). U.S. Patent No. 4,823,338. Washington, DC: U.S. Patent and Trademark Office.

[10] Postel, J. (1981). Internet protocol.

[11] Padovano, M. (2003). U.S. Patent No. 6,606,690. Washington, DC: U.S. Patent and Trademark Office.

[12] Dawkins, J., & Hale, J. (2004, April). A systematic approach to multi- stage network attack analysis. In Information Assurance Workshop, 2004. Proceedings. Second IEEE International (pp. 48-56). IEEE.

[13] Seid, Howard A., and Albert Lespagnol. "Virtual private network." U.S. Patent No. 5,768,271. 16 Jun. 1998.

[14] Size of the virtual private network (VPN) market worldwide in 2014 and 2019 (in billion U.S. dollars) https://www.statista.com/statistics/542817/worldwide-virtual-private- network-market/

[15] Coley, Christopher D., and Ralph E. Wesinger Jr. "Firewall system for protecting network elements connected to a public network." U.S. Patent No. 5,826,014. 20 Oct. 1998.

[16] Coss, Michael John, David L. Majette, and Ronald L. Sharp. "Methods and apparatus for a computer network firewall with stateful packet filtering." U.S. Patent No. 6,141,749. 31 Oct. 2000.

[17] Bellovin, Steven M., and William R. Cheswick. "Network firewalls." IEEE communications magazine 32.9 (1994): 50-57.

[18] Postel, Jon. "Transmission control protocol." (1981).

[19] Roeckl, Chris, and Corporate Marketing Director. "Stateful inspection firewalls." Juniper Networks White Paper (2004).

[20] Luotonen, Ari. Web proxy servers. Prentice-Hall, Inc., 1998.

[21] Fielding, Roy, et al. Hypertext transfer protocol--HTTP/1.1. No. RFC 2616. 1999.

[22] Swander, Brian D., Gurdeep Singh Pall, and Nagampalli SS Narasimha Rao. "Multi-layer based method for implementing network firewalls." U.S. Patent No. 7,260,840. 21 Aug. 2007.

[23] Meier, J. D., et al. "Improving web application security: threats and countermeasures." Microsoft Corporation 3 (2003).

[24] Aboba, Bernard. "IEEE 802.1 X pre-authentication." Presentation to 802 (2002).

[25] Alliance, Wi-Fi. "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks." White paper, University of Cape Town (2003): 492-495.

[26] Brands, Stefan A. Rethinking public key infrastructures and digital certificates: building in privacy. Mit Press, 2000.

[27] Housley, Russell, et al. Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. No. RFC 3280. 2002.

[28] Needham, Roger M., and Michael D. Schroeder. "Using encryption for authentication in large networks of computers." Communications of the ACM 21.12 (1978): 993-999.

[29] Krawczyk, Hugo, Ran Canetti, and Mihir Bellare. "HMAC: Keyed-hashing for message authentication." (1997).

[30] Rivest, Ronald. "The MD5 message-digest algorithm." (1992).

[31] Eastlake 3rd, D., and Paul Jones. US secure hash algorithm 1 (SHA1). No. RFC 3174. 2001.

[32] Goldschlag, David, Michael Reed, and Paul Syverson. "Onion routing." Communications of the ACM 42.2 (1999): 39-41.

[33] Ganesan, Ravi. "Yaksha, an improved system and method for securing communications using split private key asymmetric cryptography." U.S. Patent No. 5,535,276. 9 Jul. 1996.

[34] EOZ, PC. "Data Encryption Standard." Computers and Security 7.5 (1998).

[35] Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications 67.19 (2013).

[36] Daemen, Joan, and Vincent Rijmen. The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[37] Rivest, Ronald L., Matthew JB Robshaw, and Yiqun Lisa Yin. "RC6 as the AES." AES Candidate Conference. 2000.

[38] Schneier, Bruce. "The Blowfish encryption algorithm." Dr Dobb's Journal-Software Tools for the Professional Programmer 19.4 (1994): 38-43.

[39] Schneier, Bruce, et al. "Twofish: A 128-bit block cipher." NIST AES Proposal 15 (1998).

[40] Verma, Amit, Simarpreet Kaur, and Bharti Chhabra. "Improvement in the Performance and Security of Advanced Encryption Standard Using AES Algorithm and Comparison with Blowfish." (2016).

[41] Lucas, Michael. PGP & GPG: Email for the practical paranoid. No Starch Press, 2006.

[42] Team, TrueCrypt. "TrueCrypt-Free open-source disk encryption software for Windows Vista/XP, Mac OS X, and Linux, Sept 2012." URL http://www. truecrypt. org/.[accessed 18 Sept-2012].

[43] Blakley, G. R., and I. Borosh. "Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages." Computers & Mathematics with Applications 5.3 (1979): 169-178.

[44] Baldwin, Robert, and Ronald Rivest. The rc5, rc5-cbc, rc5-cbc-pad, and rc5-cts algorithms. No. RFC 2040. 1996.

[45] Juels, Ari, and Thomas Ristenpart. "Honey encryption: Encryption beyond the brute-force barrier." IEEE Security & Privacy 12.4 (2014): 59-62.

[46] Ouellette, Jennifer. "Quantum key distribution." Industrial Physicist 10.6 (2004): 22-25.

[47] Infrastructure, Public-Key. "The VeriSign Difference, Feb. 3, 2001, Copyright 1999, VeriSign." 1-21.

[48] Ylonen, Tatu, and Chris Lonvick. "The secure shell (SSH) protocol architecture." (2006).

[49] Beale, Jay, et al. Nessus network auditing. Syngress Publishing, 2004.

[50] Zimmermann, Philip R. The official PGP user's guide. MIT press, 1995.

[51] Arkko, Jari, Vijay Devarapalli, and Francis Dupont. "Using IPsec to protect mobile IPv6 signaling between mobile nodes and home agents." (2004).

[52] Hamzeh, Kory, et al. Point-to-point tunneling protocol (PPTP). No. RFC 2637. 1999.

[53] Zorn, Glen, et al. "Layer Two Tunneling Protocol" L2TP"." (1999).

[54] Postel, Jon. User datagram protocol. No. RFC 768. 1980.

Appendices: List Of Common Internet Traffic Security Issues and Solution Recommendations

Malware

Malware, short for malicious software, is any program or file that is harmful for any computer. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions, and monitoring users' computer activity without their permission. Different types of malware have unique traits and differing capabilities. The most common types of malware are:

- **Spyware:** Spyware is a technology that acts as a spy and gathers information about an individual or an organization without his or her knowledge. This kind of program is secretly installed in one's computer, passing on information to interested advertisers or other parties. A spyware program can enter one's computer either during the installing of a new program or as a software virus.
- **Virus:** A virus is a program that replicates itself when one program is copied from one place to another. A virus can be transmitted as an attachment to an email or within a file.
- **Worm:** A worm is malware that replicates on its own without any host program. A worm is a self-replicating virus that grows in number and consumes system space, causing the system to slow down or stop other tasks.
- **Trojan Horse:** A Trojan Horse appears to be harmless upon installation, but in turn, gains access to a computer and do its own form of damage, like crashing a computer system.

Other types of malware exist that are programmed for specific purposes:

Ransomware: Ransomware is used for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment in exchange for the decryption key. Ransomware spreads through email attachments, infected programs, and compromised websites.

Rootkit: A rootkit is used to gain administrator level access to any computer system. Once access is gained, cybercriminals can exploit any data at will.

Backdoor Virus/Remote Access Trojan: A backdoor virus or remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. The malicious program is downloaded invisibly via an email attachment or game and secretly creates a backdoor (a means of access to a computer program that bypasses security mechanisms) into an infected system that allows threat actors remote access it without alerting the user or the system's security programs.

According to a report of Symantec's Global Intelligence Network (GIN), the email malware rate increased in November 2016, jumping from one in 158 emails in October to one in 85 emails while in December it decreased slightly. Email malware rates also increased across industries, as well as organization sizes, during November 2016. Although these attacks make computer systems vulnerable to data exploitation, there are certain measures which users can implement to avoid these kinds of attacks, including the following:

1. **Antivirus:** Deploy signature based antivirus programs on computer system, scanning the system every time it connects to a new network connection and scheduling daily scans for the whole computer system.
2. **Firewall:** Use a software-based application firewall that prevents incoming and outgoing malicious network traffic, thus enhancing security.
3. **Patch Updates:** Patch operating system vulnerabilities whenever any updates from the manufacturer becomes available.
4. **Restrict Privileges:** Restrict administrative privileges for operating system and applications to prevent unknown user from using infected drives or installing malware breeding softwares or opening infected emails.
5. **Education:** Educate oneself by undergoing security awareness training to learn about information security glitches and realize one's responsibility towards security as an individual.
6. **Website and Plugin Check:** Avoid visiting sites that may harbor malware, such as peer-to-peer file sharing sites, and do not download browser plugins that are on red alert. Read the reviews about plugins before downloading any.
7. **Update Oneself:** Keep oneself updated about latest security threats or cyber-attacks by reading security reports or news.

Spam

Spam consists of unwanted emails from unknown sources or strange emails from known sources. These are typically sent to large numbers of users for advertising, phishing, spreading malware etc. According to a report by

Symantec's Global Intelligence Network, the global spam rate declined slightly in December, to 54.2 percent, down 0.1 percentage points from November when it was the highest (last year). Organizations with 1001-1500 employees had the highest spam rate in December '16. Even though spam attacks are concern, taking the right precaution can help sway these attacks. Below, are some suggested precautionary measures.

Attachments and Hyperlinks: Never open email attachments and hyperlinks from unknown sources or unexpected attachments from known sources (a source is easily forged). These kinds of emails appear to be legitimate, but actually they are phishing frauds looking for sensitive information.

Pop-up Window: Be careful of pop-up windows which just appears out of nothing or sometimes may be when you just click on links. These pop-ups are dangerous and are looking for the right opportunity to steal information. Be careful to enter any sensitive/personal information in such windows.

Antivirus and Firewalls: Keep the latest definition of antiviruses and firewalls, so that recent threat types could be mitigated.

User Education: Keep yourself updated about the latest trends in spam attacks (when and how) and take precautionary measures accordingly.

Filters: Use browser filters to block malicious looking websites which might be another phishing link looking for the next opportunity to steal data.

Authentication: Utilize strong passwords--alphanumeric characters, capital letters, and changing passwords at regular intervals. This measure will help maintain proper authorization, authentication and identity management of users logging into the system. Thus, preventing threats from unauthorized users accessing sensitive information on the web.

Web-based Attacks

The web is a means of accessing information over the internet, which is actually an information sharing model built on top of the internet. These attacks target websites, web browsers, browser plugins and/or other web services. These attacks focus on web applications and targets layer 7 of the OSI model, which is the application layer.

The most common forms of web attacks are the following:

- **Spoofing:** Spoofing is when attackers communicate to the user from an unknown source by disguising the communication to appear to be from a source familiar to the user. This is done to gain access to someone else’s information and/or steal it, or to sabotage the normal operations of a website.
- **Information Leakage:** Information leakage is one of the costliest threat to an organization or nation. Leakage of information could change business deals or market value, or it may lead to loss of trust from customers.
- **Repudiation:** This attack happens when user’s actions are not logged properly, thus allowing malicious manipulation of system’s data or forgery of information. This attack can be used to change the authoring information of actions executed by a malicious user to log wrong data to log files. Its usage can be extended to general data manipulation in the name of others, in a similar manner as spoofing mail messages. If this attack takes place, the data stored on log files can be considered invalid or misleading.

With millions of things getting connected to the web day by day, it is evermore a lucrative repository for prying eyes to steal from. Web based application attacks can be taken care of by implementation of certain best practices:

Development Methodology: Practice secure software development methodologies to prevent buggy developments and enhance security.

Application Whitelist: Download applications based on the user rating and developer rating. Download applications which are from trusted developers.

Application Updates: Patch updates of every application as soon as they become available to keep up to date with the latest definitions.

Authentication: Use authentication methods such as basic/digest authentication, form-based authentication, integrated (SSO) authentication to authenticate an application before using it.

Authorization: Verify applications and authorization privileges before allowing an application to access sensitive information.

AAA: Enable authentication, authorization and accounting (AAA), a framework for intelligently controlling access to web applications, enforcing policies, auditing usage, and providing the information necessary to bill for services.

Configure and Monitor: Configure user applications. Prevent usage of applications from untrusted source. Also, undergo scheduled monitoring of applications to make sure everything is in proper order.

Denial of Service and Distributed Denial of Service Attacks

DoS or DDoS is a kind of security attack where an attacker decides to prevent legitimate users from accessing targeted computer systems, devices, or other network resources. These attacks make a resource (site, application, user systems, or servers) unavailable for the purpose for which they were designed. Some guidelines are provided by United States Computer Emergency Readiness Team (US-CERT) for determining a DoS attack is underway:

- Degradation in network performance, especially when attempting to open files stored on the network or accessing websites
- Inability to reach a particular website
- Difficulty in accessing any website
- A higher than usual volume of spam email

The motive behind these attacks are mainly for financial profit. DDoS specific attacks are attacks in which a multiple number of compromised systems attacks a single target, hence causing denial of service for users of the targeted system. The flooding of incoming messages to the target system essentially forces the system to shut down, thereby denying service to legitimate users. A computer under the control of an attacker is known as **zombie** or a **bot**. A group of co-opted computers is known as a **botnet** or zombie army. According to the DDoS intelligence report from Kaspersky Labs for Q3, 2016, some statistics regarding DDoS attacks include the following:

- Resources in 67 countries (vs. 70 in Q2) were targeted by DDoS attacks in Q3 2016.
- 62.6% of targeted resources were located in China.
- China, the US and South Korea remained leaders in terms of both the number of DDoS attacks and number of targets. For the first time both rankings included Italy.
- The longest DDoS attack in Q3 2016 lasted for 184 hours (or 7.6 days) – significantly shorter than the previous quarter’s maximum (291 hours or 12.1 days).
- A popular Chinese search engine was subjected to the largest number of attacks (19) over the reporting period.
- SYN DDoS, TCP DDoS and HTTP DDoS remain the most common DDoS attack scenarios. The proportion of attacks using the SYN DDoS method continued to grow, increasing by 5 p.p., while the shares of TCP DDoS and HTTP DDoS continued to decline.

- In Q3 2016, the percentage of attacks launched from Linux botnets continued to increase and reached 78.9% of all detected attacks.

Certain best practices could be adopted to survive a DoS attack:

Prepare: In case of a DoS attack (this is mainly at ISP and organization level), start well by preparing an incident response (an organized approach to addressing and managing the aftermath of a security breach or attack) plan well in advance of any attack.

Act: Contact your ISP, when you suspect a DoS attack. The ISP can help mitigate the attack by rerouting or throttling (the deliberate regulation of the data transfer rate in a communications system) malicious traffic and using load balancers (dividing the amount of work that a computer has to do between two or more computers so that more work gets done in the same amount of time and, in general, all users get served faster) to reduce the effect of the attack.

IDS: Use intrusion detection systems (a device or software application that alerts an administrator of a security breach, policy violation or other compromise that may adversely affect the administrator's information technology network), intrusion prevention systems (a preemptive approach to network security used to identify potential threats and respond to them swiftly), and firewalls that could help detect DoS attacks. (This is mainly at the ISP and organization level.)

Anti-DoS: Use a cloud based anti-DoS service.

Social Media

Most Social Media attacks mainly involve social engineering as a means to exploit individuals. These attacks involve using social skills to trick people and break normal security procedures. Appeal to vanity, appeal to authority and appeal to greed are the most commonly used techniques for social engineering. Also, people’s willingness to be extremely helpful can be another means.

Some very popular types of social engineering attacks are:

- **Phishing** - Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often appearing to be from a trusted source. These kinds of message are often meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.
- **Spear phishing** - Spear phishing is like phishing, but intended for a specific individual or organization.
- **Pretexting** - This is a kind of attack is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data to confirm the identity of the recipient.
- **Scareware** - This attack involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.

- **Baiting** - Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive, in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer to check it, unintentionally installing the malware.
- **Manual Sharing** - This attack relies on victims to actually do the work of sharing the scam by presenting them with intriguing videos, fake offers, or messages that they share with their friends.
- **Fake Offering** – This scam invites social network users to join a fake event or group with incentives, such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.
- **Likejacking** – Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.
- **Fake Apps** – Users are invited to subscribe to an application that appears to be integrated for use with a social network but is not as described, and it may be used to steal credentials or harvest other personal data.
- **Fake Plugin** – Users are invited to install a plugin to view a video, but the plugin is malicious and may spread by re-posting the fake video message to a victim's profile page without permission.

Statistical representation from Symantec shows that the phishing rate decreased in December, down to one in 3,357 emails with the highest being in October 2016. At one in 3,575 emails, businesses with 1-250 employees had the highest phishing rate on December 2016. Rapid growth and easy access of social media has formed path for social engineering attacks, waiting to collect information with the help of social engineering skills. Some best practices could be adopted to avoid these attacks -

1. **Filter Contents:** Filter email content, allowing only emails from known sources or which seem legitimate. Also, filter web content of incoming and outgoing traffic. Use only those web pages that appear legitimate and come from trusted sources.
2. **TLS Encryption:** Enable TLS encryption between servers to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.
3. **Observe:** Do not randomly "follow" people. First, check the contents they are posting (spam or legitimate), then decide whether to proceed. Social engineering can be avoided. Also, do not go by the number of followers, or outlook. See, listen, analyze, and then decide whether to proceed.
4. **Verified Badge:** While using social media, it is a good practice to go by the verified badge rather than just following any random post from unknown sources - this would help users avoid spams or phishing attacks.
5. **Education and Alertness:** Keep yourself updated with the latest facts in social engineering and be alert while revealing personal information through social media.

Mobile Devices Attacks

Mobile device attacks are also on the rise. Attackers are targeting popular applications and games and producing their fake replica on the play store itself. Cybercriminals are also using Trojan Ransomware in the Google Play store in

the disguise of an application. According to a report by securitymagazine.com, the following mobile attacks are on the rise:

1. **Android GMBot:** This spyware remotely controls infected devices to trick victims into providing their bank credentials.
2. **AceDeceiver iOS Malware:** This malware is designed to steal a person's Apple ID.
3. **SideStepper iOS "Vulnerability":** This technique was discovered to intercept and manipulate traffic between an MDM server and a managed device.
4. **High-severity OpenSSL Issues:** These vulnerabilities can potentially impact large numbers of applications and services, which could ultimately jeopardize enterprise data-in-motion.
5. **Marcher Android Malware:** This malware has evolved to mimic bank web pages that trick users into entering their login information through e- commerce web sites.

Increasing utilization of smartphones as well as the growth of connected things has made mobile devices prone to numerous vulnerabilities. These, could swayed with the help of some best practices.

1. **Update Applications:** Check mobile device applications regularly. Keep those that you use regularly, updated.
2. **Scan:** Install an antivirus software in your mobile device and perform schedule scans.
3. **Permissions:** Keep your mobile settings up to date. Disable auto update of applications and applications downloaded from unknown sources. Also, review application permissions on a regular basis.
4. **Check:** Keep an eye on suspicious links. If any link appears to be different, do not open it.
5. Verify: Download applications from trustworthy sources only. Check ratings and reviews of applications before downloading any. Also, check the applications marked as trusted or top developers by particular play stores.
6. **Review:** Mobile security policies must be regularly checked to ensure that the devices are up to date.