ClubHACK Mag

1st Indian "HACKING" Magazine

Issue 28 | May 2012
www.clubhack.com

Look both side before crossing one way track

TechGyan Steganography Over Covert Channels | Mom's Guide HTTPS |

ToolGyan Kautilya | LegalGyan SECTION 66C - Puishment For Identity Theft |

Hello friends!!

Sagar Nangare

We are now in mid of 2012. As predicted by many techno geeks, this year is phenomenal for IT related technologies including security, networking and web technologies. In April cloud war is started between two big rivals Microsoft & Google. Both making sure that its going to be secure and useful for smart phone users as well. With introduction of new such technologies we must ensure security over the web. Here HTTPS comes into picture and we brought this topic in CHMag's Mom'sguide. Along with it topics like Steganography, a new toolkit - Kautilya, preventing SQL injections are covered.

If you have good write up and topic that you think people should know about it then please share with CHMag. Also if you have suggestions, feedback & articles, send it on info@chmag.in.
Keep reading!!

Issue 28, May2012.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Pankit Thakkar
pankit@chmag.in

K.V.Prashant
good.best.guy@gmail.com

Sagar Nangare
sagar@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

Steganography Over Covert Channels

Steganography and Cryptography

Security and privacy have been a concern for people for centuries. Whether it is private citizens, governments, military, or business, it seems everyone has information that needs to be kept private and out of the hands of unintended third parties. Information wants to be free but it is necessary to keep information private. That need has come about because governments have sensitive information, corporations send confidential financial records, and individuals send personal information to others and conduct financial transactions online. Information can be hidden so it cannot be seen. The information can also be made undecipherable. This is accomplished using steganography and cryptography. These two processes are closely related. While cryptography is about protecting the content of a message, steganography is about concealing the very existence of the message itself. They can be combined together to provide double protection. Notwithstanding, both steganography and cryptography can stand on their own independent of the other. Cryptography encodes a message in plain sight that cannot be read with normal efforts. Steganography hides the information so outsiders are not aware of its presence. It travels under the nose of the common man.

Definition of Steganography

Steganography is a method of hiding a message. Steganography comes from the Greek words (στεγανο-ς, γραφ-ειν) or steganos and graphein which means "covered writing". (SINGH 5) When using steganography, the goal is not necessarily to make a message unreadable, but to hide the fact that a message even exists. The hidden message is placed within the data boundaries of a digital file such as an email, mp3 music file, mp4 movie file, spreadsheet, MS Word document, text file, pdf file, et. al. Any third party could look at or listen to the digital file that the message is hiding in and not be aware that the hidden message is present. When the digital file reaches the intended party, the recipient should have the knowledge necessary to extract the hidden message from the digital file.

Steganography simply works this way:

1. Start with a secret message using a previously agreed upon algorithm insert the secret message into a cover object creating the stego object.
2. Then the stego object is sent to the to the receiver.
3. The receiver accepts the stego object.
4. The receiver extracts the hidden message using the agreed upon algorithm.

Present Day Steganography

Steganography preceded cryptography. Before mankind was able to encode messages with cryptography, messages would be hidden with steganographic means. It would be hidden in wax tables, under soldier's hair, or with invisible ink. Today, hiding of data with steganography can be performed within the static medium of the new digital technologies: pictures, video and audio files, Word documents, Powerpoint documents, Excel spreadsheets, movie files, et. al. Almost any digital file on a hard drive can have information embedded into it without any apparent presence. This is static steganography and it occurs on the bit/byte level. Taking this a further step and one not apparent to the layman, data can also be hidden in the medium of the Internet, the layer that the data flows over, in the packets that travel from computer to computer, over twisted pair, Ethernet and optical connections, through firewalls and routers, from network to network, untouched by the fingers of any telegrapher or data technician, in the electrical current that flows over the power transmission lines. This is dynamic steganography. This is the covert channel of the Internet.

Steganography can be covertly implemented further in the timing channels of information varied by the fourth dimension of time, or the side channels, such as the power bursts that our appliances and televisions subsists upon or the concurrent magnetic waves that emanate from various household and commercial devices. These are some of the covert channels of physical hardware.

Steganography and the Internet

Dynamic steganography can accomplished over the Internet using the medium referred to as the covert channels. Network steganography is a method of hiding data in normal data transmissions on the modern network of the Internet. These methods of hiding can be used for good or nefarious purposes, legal or illegal activities, unapproved or sanctioned processes. Any interception by a rival of the owner of this hidden data, also known as stego-data, could compromise the sending entity, cause a loss of information and resources and lead to its downfall. There must be a good reason to go to such trouble and effort to hide data using these surreptitious techniques. Today, sending messages electronically is a common mode of conveyance. Email, web documents, video, audio, file-transfer protocol, attachments such as legal documents are all used over the Internet to exchange information. With increasingly fast processors, intercepting, detecting and deciphering messages has become easier, which means more secure means of hiding information is necessary to overcome any detection. There are many unique and creative methods of securing communications with steganography and its close relative: cryptography.

Covert Channels

In these modern and technologically sophisticated times, using covert channels has become a means of transmitting information securely. How widespread its use is not known. A covert channel is a communication channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy. (BERG) For instance, Internet appliances such as two routers could use these covert channels to pass information between themselves. This information could be instructions to the other appliance to use an alternate path, redo the last transaction, or increase the speed of transmission. There are many methods available to enhance and guide the ongoing and orderly operational exchange of packets.

Lampson introduced the concept of covert channels in 1973. (LAMPSON 613) It is a means of communication that is not part of the original design of the system. (LLAMAS) It could even be said that a covert channel is a security flaw. It is a part of a program or system that can cause the system to violate its security requirements. It can be an electronic means of sending and hiding messages. (OWENS) Covert channels can be a means of taking any normal electronic communications and adding some secret element that does not cause noticeable interference to the original item such as a picture, sound file or other digital communication medium. (WAYNER 152)

Covert channels occur in two states: static or dynamic. There is the static hiding of data in electronic files sitting on a hard drive. When hiding data in a timing channel, the difference is that the data is dynamic, moving and always changing its location on the network. It's here, now it's there. If small amounts of insignificant bits or bytes are replaced, the effect on the moving vessel file should be fairly unnoticeable to the casual viewer or listener. (WAYNER 155) If the byte count of the file changes, detection can be less difficult to attain. Performing a checksum on the file will raise a flag and possible give up the embedding. The ability to detect the hidden data is next to impossible as the data streams over the wires in the midst of the billions of bits that now pass. All Internet traffic would have to be monitored for hidden data, perhaps an insurmountable task.

The World Wide network of the Internet is the perfect medium for steganography to occur. Data can be hidden in web pages and the embedded images that pass over the Internet, a relatively easy task to perform and perhaps just as easy to examine. An even more surreptitious and unique way to hide messages would be in the unused fields of the TCP/IP packet headers. The operation of the Internet runs on the Transmission Control Protocol and Internet Protocol (TCP/IP). The fields in the TCP/IP packet header help guide the movement as they hop across the Internet and coordinate the reassembly of these packets when they reach their destination. These packets hold all the overt data that travels over the Internet: web pages, ftp data, video and audio, email, images and pictures. These Internet packets are directed to their destination by the information contained in the fields of the header at the beginning of each packet. Because packets are so small, only 1024 bytes, it takes many, many separate packets to convey all the information in a webpage or in any digital file. Unless specifically monitored with specific software or hardware, most users

are not aware of the packets nor do they ever see them. Inside the packet are data frames where slices of the data reside. These data slices make up over 80 per cent of each TCP/IP packet. Until they reach their destination, the packets are incomplete and fragmented. Sometimes packets get lost and must be retransmitted. A handshake and acknowledgement initiates a session, then a sending and receiving of packets occurs like a dance, each participant performing their next step. When they reach their ultimate destination, the packets are finally reordered and reassembled. The sheer volume of the Internet and the great number of the simple network packets guarantees that covert messages can be hidden in the unused header fields of the packets containing all transmitted information. It's not as granular as a molecular layer. Ross Anderson said: "For covertness reasons, you'd probably want to hide your traffic in traffic that's very common." (MCCULLAGH) Nothing is more common than the ubiquitous Internet TCP/IP packet.

Uses of Steganography

Steganography, in the form of media watermarking and fingerprinting, has been found to be useful for legitimate commercial applications. Applications of steganography include not only covert communications, but it can enable the tracing of the original source of pirated, stolen and illegal copies of protected books, audio or video files. Watermarking provides the ability to identify these copied files.

In a typical application of image watermarking, some message is encoded imperceptibly embedded into the host file like a copyright notice identifying the intellectual property owner or rightful user. (COLLBERG) One example of utilizing watermarking is to embed a digital signature in a printed document for verifying authenticity. This signature is made up of information such as the serial number, the model and manufacturer of the printer used, date of document printing, and author of the document. This information is inserted into the initial characters of each page of a document. This steganographic function, unknown to many, is a common feature of many printers used today on a daily basis. (MIKKILINENI) Music files sold over iTunes are also encoded with watermarks that identify the purchaser and host computer where the audio files were purchased. This allows them to be used by the rightful purchaser while preventing the illegal transfer of these files to others. Apple's iTunes software examines the sound files on iPods and uses the hidden authorization codes to authenticate and allow legitimate use of purchased music files. Similarly, DVDs issued to members of the Academy of Motion Picture Arts and Sciences are tracked with watermarks to combat piracy through media source identification.

It has also been suggested that sending information requested by users in mobile banking system can be made more safe and secure through the practice of steganography. The indirect sending of information increases the security for users in mobile-banking system. (SHIRALI-SHAHREZA)

The uses and methods to hide data are many and will continue to grow and expand. The imagination of men and the many technical methods and rules of science will only put limits on how data will be dealt with while traveling under our noses. The need to hide that data will be always present

as the exploits and attacks increase to uncover and decipher information that does or does not belong to the hacker.

This is not to say that steganography cannot be used for good. The user of any tool, a corporation or terrorist, will determine whether the steganographic purpose is good or evil. Enslaved peoples can also use these tools to get their story out to the free world. Using cryptography and steganography, people who have freedom of information and speech are now able to receive the stories and tales of others who do not, those who should be able to enjoy the inalienable rights that belong to all humans. The recent Arab spring in Algeria, Tunisia, and Egypt has been attributed to use of the Internet to overcome corrupt political regimes and silence political dictators and despots. Steganography can keep people free.

Terrorism on the Internet

It is an invisible arms race. (GOTH) There are often reports in the news of use of the Internet by terrorist groups operating within the U.S. Many of these encrypted digital messages might be passed by way of covert channels, embedded within other innocent-looking files or in the covert channels that hide next to the overt pathway of the Internet. (MANEY) A covert channel is typically used when the participants know that they are being monitored in the usual mainstream and mundane communications channels of snail mail, financial records, telephone calls and even electronic mail. The huge bandwidth of the world's largest network of the Internet offers an alternate medium of covert channels from snail and email, and messaging for transport of hidden data.

The process of using the Internet for terrorist activities has been in the news more and more as Homeland Security "cries wolf" louder and louder. Steganographic and encryption software is so powerful that it's usage and export is regulated by law. It's usage can allow criminals, malcontents, and terrorists in addition to lawful actors to operate and communicate through public channels practically unfettered. Such software and encryption algorithms are categorized as weapons and cannot be exported outside the nation's borders. There are many free and Open Source software packages available to anyone who wishes to hide data. Recent terrorist activity has been tentatively linked to the likely occurrence of steganography and is seen by the usual governmental agencies as a likely method of sending covert information. (KELLEY) With the wide use and abundance of the many powerful and free Open Source steganographic and cryptographic tools on the Internet, law enforcement authorities should and do have serious concerns about detection of questionable material and information through web page source files, images, audio, and video and other medium. No doubt there is more effective in-house software developed by corporations and governmental agencies to accomplish undetectable steganography.

Steganalysis and Detection

Steganalysis is described as the process of detection and identification of hidden stego-data. There are many issues to be considered when studying steganographic systems. While steganography deals with the various techniques used for hiding information, the goal of steganalysis is to detect and/or estimate the presence of any potentially hidden information. This has to be done with little or no knowledge about the unknown steganographic algorithm

used to hide the message in the original cover-object, if it does exist.

One way to track Internet steganography would be to develop Internet appliances that have the capability to detect embedded documents in cover data in the data packet field and anomalies in any other packet header field. Packet analysis is also performed using packet sniffers programs, such as tcpdump, OmniPeek, and Wireshark. They capture raw network data over the wire. (SANDERS)

Specialized hardware devices are, in fact available, but are not openly marketed to the general public and only available to approved users such as law enforcement and Homeland security agencies. These devices go beyond the capability and functionality of normal routers, firewalls and intrusion detection systems. These appliances are only available to law enforcement agencies and operate under the radar. These are called wardens and add to the cybersecurity defenses already available.

There are three types of wardens:

1. A passive warden can only spy on the channel but cannot alter any messages;
2. An active warden is able to slightly modify the messages, but without altering the semantic context;
3. A malicious warden may alter the messages without impunity. (CRAVERS)

CALEA

In October 1994, Congress took action to protect public safety and ensure national security by enacting the Communications Assistance for Law Enforcement Act of 1994 or CALEA. The objective of the implementation of CALEA was to assure law enforcement's ability to conduct lawfully authorized electronic surveillance while preserving public safety and the public's right to privacy. Technology can provide the necessary tools that law enforcement agencies must have to detect questionable activities. Such agencies such are the FBI, the NSA and the CIA must be able to detect questionable activities by both domestic and international malcontents. There do not exist rooms where real individuals listen to calls manually as there were during the early years of wiretapping telephone calls for J. Edgar Hoover. There does exist certain specialized computers in server rooms that do the automated interception, monitoring, and collection of data. There is occasional eavesdropping and wiretapping of lawful citizens, participants in the political process, and others who may be in violation of the serious legal guidelines society refers to a laws. The mandate of the Federal law of Homeland Security and specific court orders authorizes wiretapping of phone calls or monitoring of Internet traffic. Such activities require and authorize specialized equipment be placed on the main network pipeline of broadband Internet access providers (ISPs) and voice over Internet protocol (VOIP) providers to do that legal privacy override of examining electronic transmissions of all types. Internet service providers and telecommunications carriers must assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization.

Hiding Data in the Unused Header Fields of the TCP/IP Packets

One possible steganographic method is to use the network and transport layers of the TCP/IP protocol suite. These layers are normally unavailable to not only the common Internet user but also the average system or network administrator. One approach, for data hiding is to utilize the unused fields in TCP/IP packet header to transmit a stego-message. Accomplishment of this method would require specialized modification of certain Internet appliances, such as routers, filters, and firewalls within the existing network hardware and infrastructure. The treatment of these fields by Cisco and Nortel routers is unknown. There are no guarantees that this data would remain unaltered through its path from its initial transmission to its receipt at its intended destination. This would have to be affirmed and tested for maintenance of the data in its unaltered and undisturbed state as it moves over any network. Protocols and operational safeguards would have to be established to guarantee the availability of data hiding at the TCP/IP protocol suite. (AHSAN) Someone thought this capability was useful because they patented the process (U.S. Patent Office, Patent No: US007415018B2 Aug `9.2008). The process of steganography over TCP/IP is patentable under current patent law guidelines. Useful or not, this capability can be dangerous in the wrong hands.

One example of hiding data in a covert channel uses software for crafting stegenographic data to be placed in certain unused header fields of the Internet transport data packet. This software uses fields such as the Initial Sequence Number (ISN) or other appropriate field in the packet header. The new ISNs will carry the secret message, which could be, for example, a password sniffed by malicious software running on a compromised machine.

A covert channel can be very hard to detect. That's the idea. The packets used for carrying the message can appear innocuous and beyond suspicion. The idea of a covert channel seems very simple and unique, but it must be carefully implemented so as to not disturb normal user operations. Just as covert channels can be implemented using superior computing power so can detection be implemented to intercept and prevent such surreptitious activity. Stealth technology is one of the methods used by attackers to hide their malicious actions after a successful break-in. Taking surreptitious control of a computer or system, installation of backdoors, planting of a rootkit, alteration of the system's operating system is an example of using chained exploits that work together. (WHITAKER) Rootkits can modify the operating system to insert a kernel module that can perform further exploits such as steganography or a coordinated denial-of service attack (DDOS). (TROST) There are different approaches to detection and can be supported using Open Source software on the receiving server. (RUTKOWSKA) This involves detecting this kind of activity while continuing to identify and develop new offensive techniques to combat the new steganographic technique.

Comprehensive National Cybersecurity Initiative

Further government action has been mandated recently. In May 2009, President Obama accepted the recommendations of the Cyberspace Policy Review. The Comprehensive National Cyber security

Initiative (CNCI), launched by President George W. Bush in detailed those recommendations. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cyber security strategy. These CNCI initiatives will play a key role in supporting the achievement of many of the key recommendations of President Obama's Cyberspace Policy Review. The CNCI initiatives are designed to help secure the United States in cyberspace.

The existing EINSTEIN 2 capability enables analysis of network flow information to identify potential malicious activity while conducting automatic full packet inspection of traffic entering or exiting U.S. Government networks for malicious activity using signature-based intrusion detection (IDS) technology. A planned EINSTEIN 3 initiative will expand these capabilities to foster safety and security on the wires, heading off any covert activities that may intrude on the nation's communication channels. The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cyber security analysis, situational awareness and security response. (NAKASHIMA) The government created the Internet as part of a DARPA project over forty years ago. Its usage was expanded for commercial use and to include the general public in the 90s. The appropriate agencies need to guarantee a mature Internet with the ability to deter and turn away any malicious attacks, exploits, or intrusions. EINSTEIN 3 is part of this effort.

Network appliances and steganalysis detection

Network appliances such as routers and firewalls play a large role in handling and parsing network traffic. Directing data between portions of a network is the primary purpose of a router. Therefore, the security of routers and their configuration settings is vital to network operation. In addition to directing and forwarding packets, a router may be responsible for filtering traffic, allowing some data packets to pass and rejecting mal-formed or suspect packets. This filtering function is a very important responsibility for routers; it allows them to protect computers and other network components from illegitimate or hostile traffic.

Intelligent Support Systems for Lawful Interception, Criminal Investigation, and Intelligence Gathering (ISS), holds wiretapping conferences and seminars for the law enforcement community, military, governmental agencies and homeland security agencies. One featured company, Packet Forensics, was marketing Internet spying boxes to the feds at a recent ISS conference. (SINGL) The web site of Packet Forensics lists the products available from the company, though some pages are restricted to authorized law enforcement and intelligence organizations only. These protected pages must describe defense and intelligence applications and hardware platforms too sensitive to release details to the public. Generally, these Internet appliances automate the processes that allow observation and collection of data on Internet traffic and/or phone calls when given the legal authority by either court order or mandate provided by legal statute to do so. They can forward captured packets for storage and further analysis later by a system designed for extreme DPI. These Internet appliances perform lawful interception, investigative analysis and intelligence gathering, stealthily, while protecting the privacy rights and civil

liberties of the law-abiding users of the Internet. (SINGL) These appliances can handle a large number of surveillance requests while heading off any and all possible terrorist exploits before they occur. These appliances can record and collect the evidence needed to convict the guilty. These devices perform deep packet inspection, searching for thousands of different strings deep inside each packet. These products are highly recommended to officials so digital communication traffic can be scanned and examined. SSL encryption is built into web browser software and protects our web traffic. Such traffic cannot normally be decrypted and read by any packet-sniffing tool. SSL encryption is designed to protect users data from regular eavesdropping. Such SSL encryption is not safe from the products of Packet Forensics and other powerful tools. They most likely will be able to overcome and decrypt most SSL algorithms. These devices provide for regulatory compliance such as required by CALEA, and comply with lawful intercept requirements and meet the essential needs of law enforcement. Such devices can be part of a packet processing and network compliance platform. These particular appliances can be linked together in closed networks called darknets to collect and share real-time network intelligence. Packet Forensics products are subject to the export control laws administered by the United and may not be exported outside the US without prior Federal government approval. Two of the products available for viewing on the web site of Packet Forensics (www.packetforensics.com) are LI-5B and PF.LI-2 (next picture).

Packet Forensics LI-5B

Packet Forensics LI-2

Deep Packet Inspection

Of billions of messages that roam the Internet, there must exist some messages that are malicious, containing worms or viruses, malware or spyware, which organized criminals, and terrorists utilize to commit cybercrimes. Here, deep packet inspection (DPI) comes to the rescue, since it allows monitoring and filtering of packets wherever they happen to pass. DPI can also meet other objectives in security, and legal compliance. This technology enables instant, ubiquitous monitoring of everything that travels the Internet.

DPI is the next surveillance application that enters society unnoticed and available for use by authorities to combat crime, even before it happens. Security and traffic cameras, miniature cameras, directional microphones, automated face and number-plate recognition, data mining, and profiling add to all the technologies used by Big Brother to watch over its citizenry. Ours is a database society with a great increase of data generation, processing, and storage

needs. DPI captures data for later examination and diverts it for messaging and analysis. This capability adds to the tools in the government surveillance toolkit uses as a beneficial observer.

Once broadband providers and other companies embrace DPI, they can monitor and select passing traffic much more sophisticatedly than by merely scanning header information. This capacity can prove of great benefit to law enforcement agencies and intelligence services, using its existing investigation powers to enlist the assistance of broadband providers. Particularly relevant is that DPI allows for real-time monitoring, and hence facilitates a preventative approach as opposed to the retroactive approach that law enforcement traditionally used.

DPI adds to the trend that broader groups of unsuspected citizens are under surveillance: rather than investigating relatively few individuals on the basis of reasonable indications that they have committed a crime, more people, including groups, are nowadays being watched for slight indications of being involved in potential crimes. This is profiling of the masses. The movie Minority Report illustrated the use of data to predict the likelihood of a crime occurring in the near future to justify the pre-emptive arrest of un-guilty parties. The explosion of data generation, inspection, and storage enable the government to collect and use significantly more data about citizens. This increase is not only quantitative but also qualitative.

More checks and balances are required to safeguard citizen rights and privacy. The increased government powers needs to be balanced by additional checks and safeguards. Citizens must know which data are being collected and processed and why. This does not mean that the government can have a phishing trip and examine all traffic. Only specific individuals or corporations can their traffic examined. The courts have deemed profiling illegal on numerous times. Independent authorities should regularly review and check whether the government uses its powers correctly and legitimately.

Data protection is a key element. The legal framework for data protection has become outdated. The assumption of preventing data processing as much as possible is no longer valid in the current networked database society. Large-scale data collection and correlation is inevitable nowadays, and the emergence of DPI serves to emphasis this. Instead of focusing data protection on prevention in the data collection stage, it should rather be focused on better utilization of the data. Data protection is valuable not so much to enhance privacy, but to ensure transparency of government and non-discrimination.

While data protection can serve to regulate the use of data, it remains to be discussed whether DPI should be allowed for government use in the first place. Here, other elements of privacy come to the fore: protection of the home, family relations, and personal communications. These elements are likely to be infringed by DPI. Since privacy is a core, though not specifically stated, constitutional value to safeguard citizens' liberty and autonomy in a democratic constitutional state, DPI should be critically assessed. The common man is king of his castle and its borders should not be violated. DPI could be accepted as a necessary addition to the investigative tools used by law enforcement already if used properly. The power of DPI

to run roughshod over the rights of the suspected requires a fundamental rethinking of what legal protection is afforded here. Society needs substantial new checks and balances to counter-balance the increase in government power over its citizens. (JAAP-KOOPS)

The company Phorm uses DPI to peek into the web surfing habits of end users in order to serve targeted advertising. (PHORM) It is suspected that the National Security Agency has inserted sophisticated DPI equipment into the network backbone of the Internet so that it can sweep up huge volumes of domestic emails and Internet searches. While privacy activists and computer geeks are up in arms, the vast majority of Internet users either don't seem to care or don't fully understand what is happening.

Without encryption, e-commerce wouldn't be possible. The cryptographic technology of SSL is built into every web browser. The security of Amazon, EBay, PayPal, and every online bank depends upon the consumer to being able to make purchases and conduct transactions over the Internet confidently and securely.

Most web surfers do not realize how much of their information flows nakedly over the network, nor how easy it is for others to snoop on their web surfing. The predecessor of the Internet, the Arpanet was once a happy safe place, in the 60s and 70s, when the first packets were sent between government contractors and research institutions. Those early hundreds of participants knew each other well and trusted each other. It is no longer the case. It is the wild west, unbridled and without a sheriff to keep us safe. There are evil forces out there, be they hackers, spies, under-age script kiddies, or unscrupulous broadband providers. The good guys must deploy cryptographic technologies to protect the general public. But DPI can also be perceived as a bad thing and a possible threat to the privacy of individuals. It is clear that DPI is potentially dangerous tool. (WILSON) The solution to the problem of Internet privacy is not just legislation making snooping illegal, but the industry-wide adoption of cryptography by default. Nothing will protect our privacy or security from deep packet inspection than encryption. (SOGHOIAN)

Broadband providers increasingly use deep packet inspection technologies (DPI) that examine consumers' online activities and communications in order to tailor advertisements to their unique tastes. Users of Google's free Gmail email service find that the advertisements in the right side reflect to contents of their email. Friends find the same is true with Facebook. It's no wonder that privacy concerns remain despite the assurances that this data is not collected and sold. Nothing prevents providers from simply altering their policies. DPI operates invisibly. Broadband providers can collect our online communications and sell them and their contents, including medical data and private correspondence, to employers, insurance companies, credit bureaus, and landlords. They could become powerful data brokers of our online communications.

Another concern is the government's ability to subpoena the digital surveillance of a person's online life from broadband providers. Consumers deserve to be heard before the disclosure of such information to the governmental agencies or commercial entities. The courts have held that DPI can violate individual's important property or

liberty interests. It's a taking of privacy, as if their house was being searched. Consumers may choose to curtail their online communications rather than give up their personal data. This would chill the development of our ideas and free speech.

Broadband providers hide notice of their deep packet inspection practices in the densely worded legalese of the privacy policy boilerplate. If some providers switch to an opt-in approach or reject DPI entirely, consumers still cannot totally control the use of DPI technologies by those with whom they communicate. Governments should ban the use of DPI for commercial benefit and create a "Do Not Track" list to protect consumers. Broadband providers should be required to disclose their data collection practices. DPI can be used for constructive purposes such as to combat spam, without compromising consumer rights and privacy. (CITRON)

Data is always in one of two states: at rest or in motion. Data is at rest on a hard drive of a single computer. Data is safe when the host computer and its network connections are secure from intruders. Data can be secured further by encrypting it. Data that is in motion is traveling over a network. This traveling data makes many hops and travels through numerous subnets, network appliances, routers and IDS in its passage. This gives numerous instances of interception or capture of the TCP/IP packets at possible weak security points. The process of packet capture is turning data in motion into data at rest by grabbing data that is moving across a network link and storing it for parsing and examination. It can be compared to the use of cameras by toll roads to verify the vehicle is assigned to the transponder in that car by capturing the license plate as the vehicle passes through the toll booth. There is software, legitimate, and illegal, Open Source, shareware and freeware, and for free and for sale, available for the performance of packet capture. Such freeware or shareware such Open Source software includes Wireshark (ethereal), Metasploit or Nmap.

Packet Crafting

Packet crafting describes the art of creating and generating packets that can contain stego-data. Packet crafting can be done using the same software used for both legitimate purposes and the illegal and unauthorized reasons. Network administrators create and use such software tools to test network devices such as routers, firewalls, intrusion detection devices and to audit network protocols and correct weak implementations of network configurations. Thus one must create packets and insert and alter data in specific fields. The packets must be sent onto the network at one location. Then the packets must be intercepted and decoded and the content must be analyzed and interpreted. Whether or not these packets were rejected or allowed to flow through a network is noted. Vulnerabilities to exploits must be found and eliminated to protect data and information residing on servers and personal computers.

Conclusion

There exists a hidden level of communications where data can be sent and received under the noses of the common man. These covert channels exists unknown to the layman and can be used to protect electronic communications. This Internet exploit exists to be used for good or bad. Until this channel is blocked it will exist to

be used by anyone willing to utilize this capability.

Bibliography

Ahsan, Kamran. Covert Channel Analysis and Data Hiding in TCP/IP . MS thesis. University of Toronto, 2002. 15 Mar. 2009 http://gray-world.net/papers/ahsan02.pdf .
Wesley Professional, 2005.

Berg, S. Glossary of Computer Security Terms. USA, National Computer Security Center, 1998.

Citron, Danielle Keats; "The Privacy Implications of Deep Packet Inspection"; http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/ .

Collberg, C. S., Thomborson, C., and Townsend, G. M. 2007. Dynamic graph-based software fingerprinting. ACM Trans. Program. Lang. Syst. 29, 6 (Oct. 2007), 35. DOI= http://doi.acm.org/10.1145/1286821.1286826 .

Craver, J. S., "On Public-Key Steganography in the Presence of an Active Warden," Proc. 2nd Int'l. Wksp. Information Hiding, Apr. 1998, pp. 355–68 .

Goth, G. "Steganalysis Gets past the Hype." IEEE Distributed Systems Online 6.4 (2005): 2. Web.

Jaap-Koops, Bert; "Deep Packet Inspection and the Transparency of Citizens"; http://dpi.priv.gc.ca/index.php/essays/deep-packet-inspection-and-the-transparency-of-citizens .

Kelley, Jack. Militants wire Web with links to jihad. USA TODAY. www.usatoday.com/news/world/2002/07/10/web-terror-cover.htm .

Lampson, Butler W. "A Note on the Confinement Problem"; Xerox Palo Alto Research Center . http://dl.acm.org/citation.cfm?coll=GUIDE&dl=GUIDE&id=362389 .

Llamas, D, et. al. An Evaluation Framework for the Analysis of Covert Channels in the TCP/IP protocol suite. University of St. Andrews,Scotland, UK.

Maney, Kevin. Bin Laden's Messages Could Be Hiding In Plain Sight. USA Today December 19, 2001. http://www.usatoday.com/life/cyber/ccarch/2001/12/19/maney.htm .

McCullagh, Declan, "Secret Messages Come in .Wavs." Wired.com. Wired News, 20 Feb. 2001. Web. 11 Feb. 2012. <http://www.wired.com/print/politics/law/news/2001/02/41861>.

Mikkilineni, Aravind K.; Chiang, Pei-Ju; Chiu, George T.-C.; Allebach, Jan P.; Delp, Edward J.; "Data Hiding Capacity and Embedding Techniques for Printed Text Documents".

Nakashima, Ellen; "White House declassifies outline of cybersecurity program"; Washington Post; March 3, 2010.

Owens, Mark. A Discussion of Covert Channels and Steganography. InfoSec Reading Room. SANS Institute. 19 Mar. 2002. http://www.sans.org/reading_room/whitepapers/covert/a_discussion_of_covert_channels_and_steganography_678 .

"The Phorm Files - The Register." The Phorm Files - The Register. The Register, 29 Feb. 2008. Web. 05 Mar. 2012. <http://www.theregister.co.uk/2008/02/29/phorm_roundup/> .

Rutkowska , Joanna. "The Implementation of Passive Covert Channels in the Linux Kernel"; invisiblethings.org .

Sanders, Chris. Practical Packet Analysis: Using Wireshark to Solve Real-world Network

Problems. San Francisco: No Starch, 2008. Print.

Shirali-Shahreza, Mohammad. "Improving Mobile Banking Security Using Steganography." International Conference on Information Technology (ITNG'07). (23007): Print.

Singel, Ryan; "Law Enforcement Appliance Subverts SSL"; http://www.wired.com/threatlevel/2010/03/packet-forensics ; March 24, 2010 .

Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 1999.

Soghoian, Christopher; "Deep Packet Inspection – Bring It On"; http://dpi.priv.gc.ca/index.php/essays/deep-packet-inspection-%E2%80%93-bring-it-on/ .

Trost, Ryan. Practical Intrusion Analysis: Prevention and Detection for the Twenty-first Century. Upper Saddle River, NJ: Addison-Wesley, 2010. Print.

Wayner, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking. 2nd edition. Burlington, MA: Morgan Kaufmann, 2008. Print

Whitaker, Andrew, Keatron Evans, and Jack B. Voth. Chained Exploits: Advanced Hacking Attacks from Start to Finish. Upper Saddle River, NJ: Addison-Wesley, 2009. Print.

Wilson, Carol. "DPI: The Good, the Bad, the Stuff No One Talks about." Penton Media, Inc., 2008. Web. 2011. <http://www.connectedplanetonline.com/iptv/0718_dpi>.

Hal Wigoda
hal.wigoda@gmail.com

Hal Wigoda is an IT professional of over 40 years of experience. Hal currently specializes in Security of Open Systems and Mobile Devices.

phd Positive Hack Days 2012

real security | 0-day vulnerabilities | the best hackers | live hacking | CTF

International forum on information security practices

30 31 MAY / 2012

MOSCOW / RUSSIA

organized by

POSITIVE TECHNOLOGIES

In the program

learn all the latest - six streams of the conference, workshops, training and a hands-on lab keynoted **by Bruce Schneier**

check your level - international competitions **Capture The Flag and HackQuest**

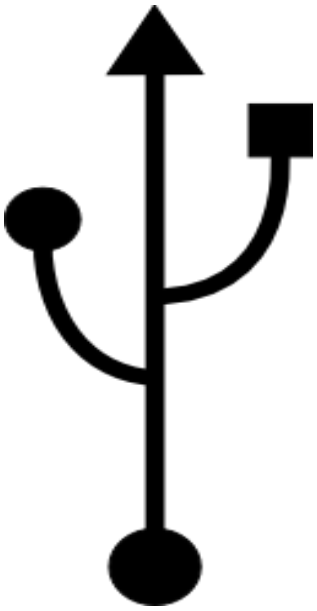
show the world what you can do - Contest and challenges

crack your phone or laptop and get $ - **Hack2own**

How to get to PHDays

- participate in a hackquest from anywhere in the world
- organize and watch the online broadcast from anywhere in the world

WWW.PHDAYS.COM
TWITTER @PHDAYS
PHD@PHDAYS.COM



Kautilya

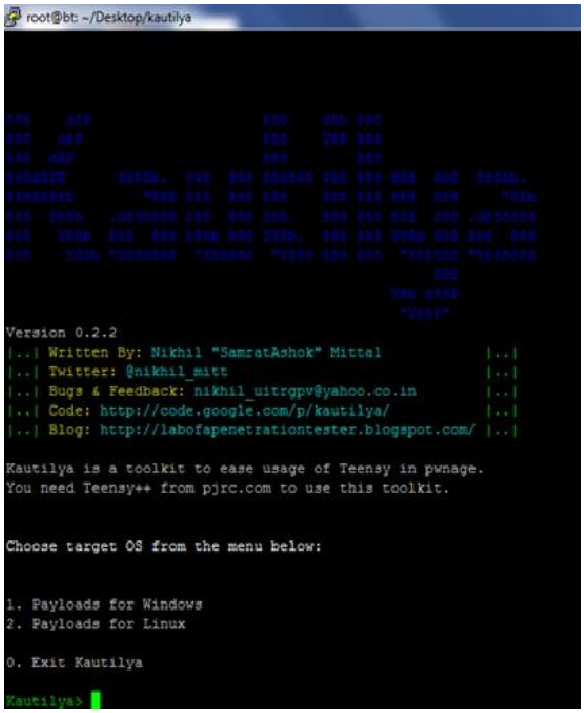
Introduction

One liner about Kautilya - Kautilya is a toolkit which makes it easy to use USB Human Interface Device (like Teensy++), in breaking into a system. Now let's understand what does that mean.

First let's understand Teensy++ (I will use Teensy for Teensy++ from now on). It is a USB HID which could be used as a programmable keyboard, mouse, joystick and serial monitor. What could go wrong? Imagine a programmable keyboard, which when connected to a system types out commands pre-programmed in it. It types faster than you and makes no mistakes. It can type commands and scripts and could use an operating system against itself, that too in few seconds. If you can program the device properly keeping in mind most of the possibilities and quirks it could be a really nice pwnage device.

During a penetration test, you generally do not have enough time to learn how to program a device. Although, programming Teensy is really easy (that is why I am able to do it ;)), it would be wonderful if someone program a tool which gives a ready to use payload for Teensy. This is exactly what Kautilya is designed for. You just need to select a few options and a sketch is generated which could be then compiled and uploaded to the device. Kautilya is written in Ruby and is named after Chanakya.

As of this writing it contains twenty payloads for Windows 7 and three for Linux (tested on Ubuntu 11).



Screenshot 1: Kautilya version 0.2.2

Using Kautilya in a Pen test

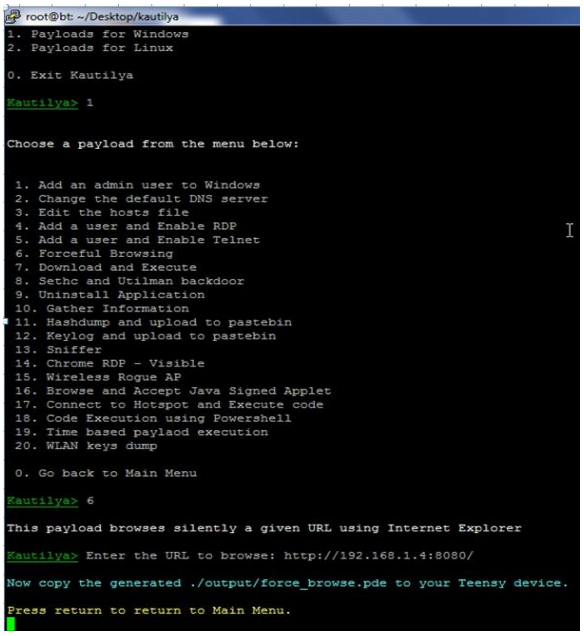
Here is the step by step process (assuming you have a Teensy with you):

1) Download Kautilya
2) Select your payload, select options and an output payload will be generated.
3) Compile and upload this payload to Teensy using Arduino + Teensyduino. (A step by step guide on installation and configuration of Arduino could be found on my blog)
4) Connect the device to victim, either directly if you have physical access or by using Social Engineering.
5) Enjoy the pwnage :)

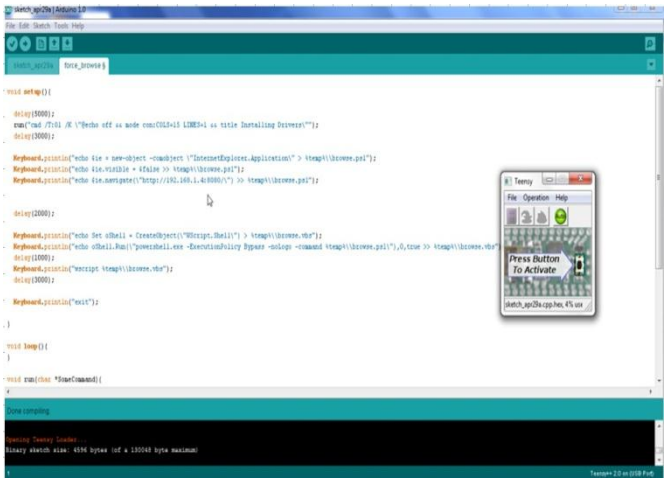
Let's have a look at some of the payloads which could be helpful in a Pen Test.

Force Browse

This payload opens up a hidden instance of Internet Explorer and browses to the user provided URL. An ideal use case could be hosting an exploit of msf or a hook of BeEF on the given URL. The payload is able to execute on a normal user privilege and is very silent.



Screenshot 2: Generating a payload using Kautilya

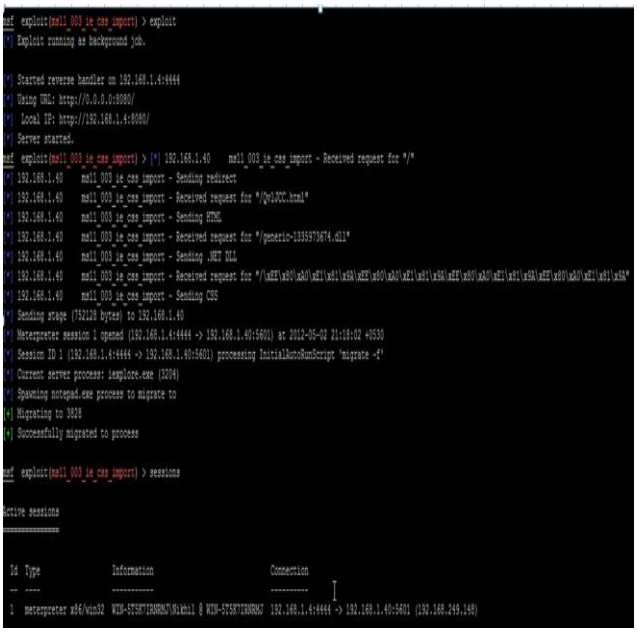


Screenshot 3: Compile and load the payload to Teensy

Assuming you are able to connect the device by some means to the victim. Below is what a victim will see on his desktop. Note the small command window which writes dark blue on black background.

Screenshot 4: Victim desktop

After a few seconds if you look at your msfconsole.



Screenshot 5: A meterpreter session

Connect to a hotspot and executed code

This payload connects to a hotspot controlled by you (assuming you are the attacker), downloads a meterpreter exe in text format, converts it back to executable and executes it. The testing of this payload was done using a HTC Android phone and kWS web server on the phone. You need to manually convert the executable to text format using a powershell script exetotext.ps1 in the extras directory of Kautilya. This script exetotext.ps1 is based on a blog by Matt at his blog exploit Monday.

Screenshot 6: Using the "connect to hotspot and execute code" payload

This payload is ideal for a scenario when there is a restricted or no internet connection on the victim and you are reasonably near to the victim. A drawback of this payload is the victim will get disconnected from other existing WiFi networks. The output of this payload will be same as above under default behavior. You can easily modify this payload as per the needs and it could be used for much more.

Is this a real threat?

This is a question I am asked many times during my talks about Kautilya, is this a real threat? Yes. If you are doing pen testing even for few months, you will feel a need of something which could be used without actually exploiting something. You would love using the features and built in tools to pwn a system as this raises less or no flags. How to use this in a pen test is up to your wisdom, use it actively by connecting ii to an unattended system during internal pen tests or hide the device inside mouse or pen drive etc for Social Engineering attacks.

Conclusion

As long as those defending the systems and those breaking the systems do not realize the risk pwning a system using HID will be very easy. I have never seen any environment where HIDs are blocked during large number of Penetration Tests which I have carried out for clients of my firm PricewaterhouseCoopers. No countermeasure or antivirus flags it as a threat. Some company marketed that they can do it, but it turned out to be false . USB HID threats are here to stay.

Nikhil Mittal

nikhil_uitrgpv@yahoo.co.in

Nikhil Mittal is a hacker, info sec researcher and enthusiast. His area of interest includes penetration testing, attack research, defence strategies and post exploitation research.

He specializes in assessing security risks at secure environments which require novel attack vectors and "out of the box" approach. He has worked extensively on using HID in Penetration Tests and powershell for post exploitation. He is creator of Kautilya, a toolkit which makes it easy to use Teensy in penetration tests. He has spoken/trained at Clubhack'10, Hackfest'11, Clubhack'11, Black Hat Abu Dhabi'11, Troopers'12, PHDays'12 Shakacon'12, GrrCon'12 and Black Hat Europe'12.

HTTPS (Hyper Text Transfer Protocol Secure)

Introduction

Hypertext Transfer Protocol (HTTP) is a protocol where communication happens in clear text. To ensure authenticity, confidentiality and integrity of messages Netscape designed HTTPS protocol. Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol (HTTP) with the SSL (Secure socket layer)/TLS (Transport layer security) protocol. It provides encrypted communication and secure identification of a network web server.

HTTPS encrypts and decrypts the page requests and page information between the client browser and the web server using a secure Socket Layer (SSL). HTTPS by default uses port 443 as opposed to the standard HTTP port of 80. URL's beginning with HTTPS indicate that the connection between client and browser is encrypted using SSL.

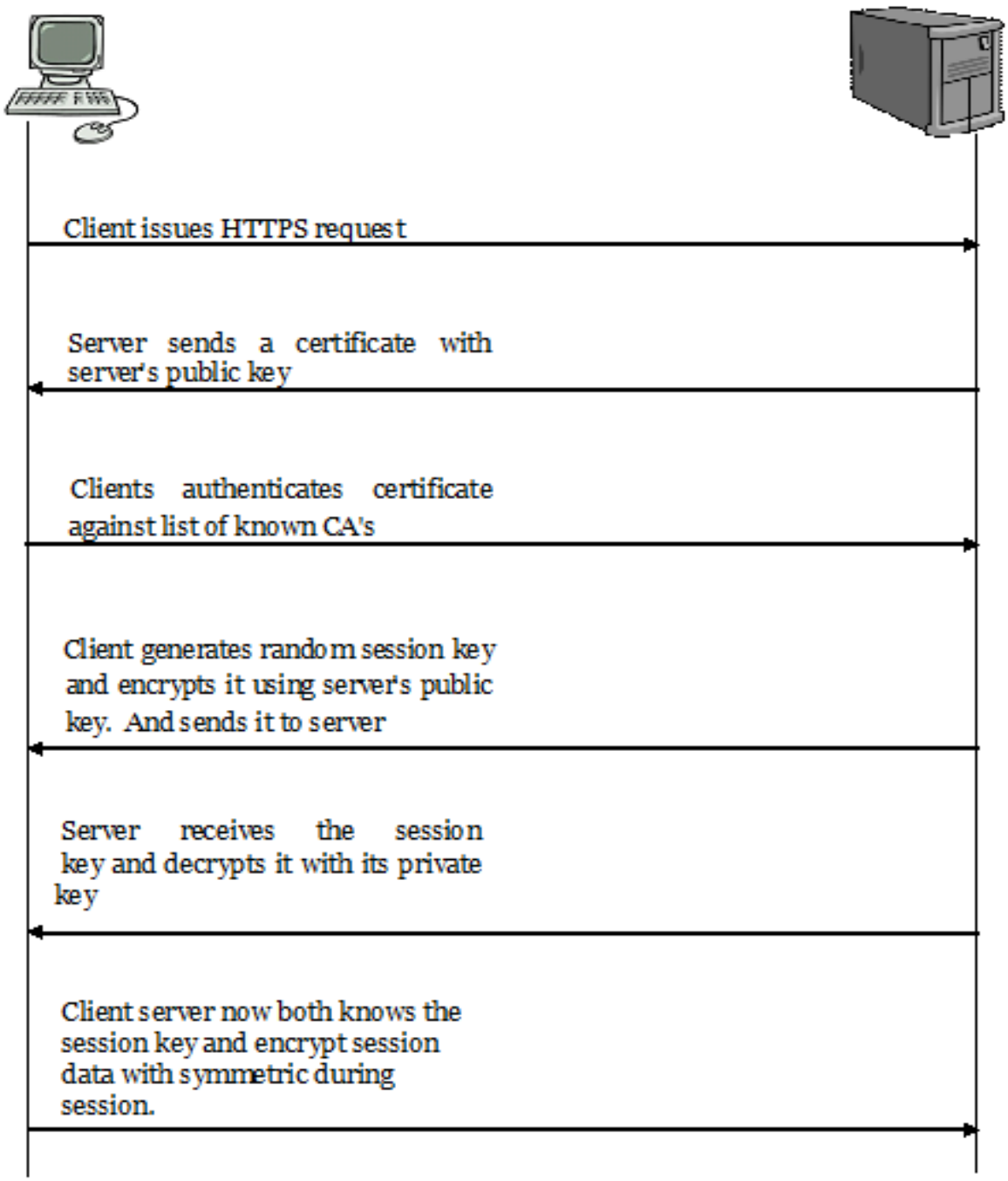
SSL works at the transport layer of Transmission Control Protocol/Internet Protocol (TCP/IP), which makes the protocol independent of the application layer protocol functioning on top of it. SSL is an open standard protocol and is supported by a range of both servers and clients.

SSL works in three phases:

- **Authentication** - Authentication checks the server who they claim they are.
- **Encryption** - Encryption with the key exchange creates a secure tunnel and doesn't allow unauthorized person to make sense of data.
- **Integrity** - Checks that any unauthorized system cannot modify the encrypted data.

SSL handshake uses asymmetric and symmetric encryption. Asymmetric encryption is used to share the session keys and symmetric key algorithm is used for data encryption

Asymmetric encryption has a lot of overhead so not feasible to use for entire session.



Client first requests a HTTPS session to server, then server sends back Certificate which has its public key embedded in it. Only server has access to this private key no one else.

Now client authenticates certificate against list of known root CAs (If a CA is unknown/self-signed, then browser gives user an option to accept certificate at user's risk). Client will then create a session key which only he knows and will encrypt it with the public key received from the server and then it will send across the internet to the server. Server will decrypt that session key with its private key. Now server and client both know the session key.

Once the SSL handshake is completed and session key is exchanged with the asymmetric encryption. Now the rest of the session is encrypted with the symmetric session key.

We use symmetric encryption because its quicker and uses less resources. Symmetric encryption is used to encrypt the session data.

Rohit Parab.
rohit.parab9@gmail.com

He is the Bachelor of Computer Science. He is Freelancer Software Developer and Independent Security Researcher (Mumbai Area).

SECTION 66C - PUNISHMENT FOR IDENTITY THEFT

Introduction

The term identity theft was coined in 1964. However, it is not literally possible to steal an identity so the term is usually interpreted with identity fraud or impersonation.

Identity Theft is a form of stealing someone's identity by pretending to be someone else typically in order to access resources or obtain credit and other benefits in that person's name.

SOME OF THE INCIDENTS

- The CEO of an identity theft protection company, Lifelock, Todd Davis's social security number was exposed by Matt Lauer on NBC's Today Show. Davis' identity was used to obtain a $500 cash advance loan.
- Li Ming, a graduate student at West Chester University of Pennsylvania faked his own death, complete with a forged obituary in his local paper. Nine months later, Li attempted to obtain a new driver's license with the intention of applying for new credit cards eventually.

PUNISHMENT FOR IDENTITY THEFT

Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be

punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

Comments

This section applies to cases where someone who dishonestly or fraudulently does the following –

- makes use of electronic signature of any other person, or
- makes use of password of any other person, or
- makes use of any other unique identification feature of any other person.

Illustration

Vivek and Rajan were business partners. Few months back they had a fight over some issues and then parted their ways. Vivek opened a new firm which into the same line of business as of Rajan. In next few months Vivek took over most of the Rajan's clients.

Disgruntled by this, Rajan decided to take revenge. Rajan managed a fake ID proof and addresses proof in the name of Vivek and applied for a digital signature certificate. He then digitally signed documents and emails to enter into electronic contract on Vivek's name and solicited his clients by presuming to be Vivek.

Rajan can be held liable under this section.

Acts covered	(1) dishonestly /fraudulently using someone's electronic signature/password or any other unique identification feature (2) dishonestly retaining stolen computer resource or communication device
Investigation authorities	Police officer not below the rank of Inspector Controller of Certifying Authorities or a person authorised by him
Relevant courts	Judicial Magistrate First Class ➔Court of Session
Cognizable/Bailable	Yes/Yes

Sagar Rahurkar

mailto:contact@sagarrahurkar.com

Sagar Rahurkar is a Law graduate, a Certified Fraud Examiner (CFE) and a certified Digital Evidence Analyst. He specializes in Cyber Laws, Fraud examination, and Intellectual Property Law related issues. He has conducted exclusive training programs for law enforcement agencies like Police, Income Tax.

Don't Get Injected – Fix Your Code

When I began doing security review for web applications, one common issue that I encountered was 'SQL Injection'. Developers used to pose several questions at me saying that their software is secure as they had followed several measures to mitigate this insidious issue.

The main mitigation adopted was to use Stored Procedures or input validation. While this does reduce certain type of Injections, It doesn't prevent all. In this article, I will explain what SQL Injection is and what one can do to prevent it.

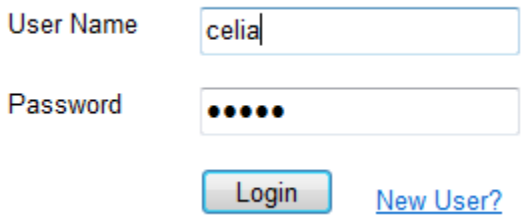
SQL Injection:

SQL Injection attacks occur in all database driven web applications. There is a risk in every web application that accepts an end user's input and uses it to send database queries to an underlying database. A hacker can manipulate the user input and send malicious queries to the database. The impact could range from stealing user's information, taking control of the server to complete wipe out of the database.

So, the onus is on the developer to ensure that the application's integrity and reliability is preserved.

SQL Injection: An Example

Consider the below login page which accepts a username and password and lets the user log in.

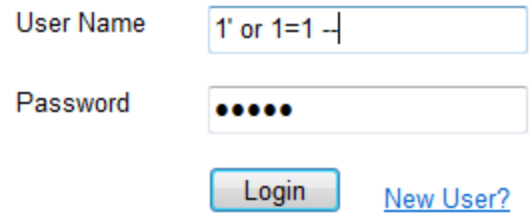


Let's assume that the below query is executed when one tries to log on to the database.

In this case, the query would look like:-

SELECT * FROM USERS WHERE USERNAME='celia' AND PASSWORD ='password';

While a naïve user would only provide the correct password and proceed to access the business functionality of the application, a hacker wouldn't. Now, consider the same form but with input shown as below.



This is how the query will take shape now.

SELECT * FROM USERS WHERE USERNAME='1' or 1=1--' AND PASSWORD ='password'

As you would see, this will let the user login even when he doesn't know the username and password. This is a very simple case of SQL Injection.

Mitigation:

The steps suggested here are absolutely needed if you want to mitigate SQL Injection. They are not just recommendation.

- Always validate your input for the right size, format, type and range.
- Use SQL parameterized Queries
- Use Stored Procedures
- Give the least minimum privilege to the database user account that is executing the queries.

Input Validation:

It is very important for your application that it should know what input to expect, what data type it can contain, the format of its input and the minimum and maximum lengths. Though it is bit difficult/time consuming to implement these validations for all input fields, it is a fool proof approach if you want your application to be reliable for a long time.

SQL Parameterized Queries:

Never use string concatenation to build your queries dynamically. Always use place holders or parameterized statements to build your queries. An example is given below.

```
String query = "SELECT * FROM USERS WHERE username=? And password=? ";
PreparedStatement prepStmt = con.prepareStatement(query);
prepStmt.setString(1, username);
prepStmt.setString(2, password);
ResultSet rs = prepStmt.executeQuery();
```

An argument when passed through the above statement, will be automatically escaped by the JDBC driver.

Stored Procedures:

Stored procedures by themselves do not help in mitigating SQL Injection. By using a stored procedure, type checking is automatically available for the parameters. Hence, when one uses this method in combinating with parameterized statements, one can minimize SQL injection to a great level. Consider the same SQL written as a procedure call.

```
CallableStatement stmt = conn.prepareCall("{call SELECT_USER (?,?)}");
stmt.setString(1, username);
stmt.setString(2, password);
stmt.execute();
```

The procedure that executes in the back end might look similar to below.

```
create or replace procedure
SELECT_USER( user IN varchar2,
pass IN varchar2, userid OUT
NUMBER,tablename IN varchar2) IS
BEGIN
SELECT USERID from users where
username =user and
password=pass;
Commit;
END;
```

One point to note here is to not use exec @sql or dynamic sql inside a stored procedure. If one does that, the advantage of using stored procedure is reduced and SQL Injection will be possible. Check out the below vulnerable code. This code does make the use of Stored Procedures but uses dynamic SQL. This code is still vulnerable to SQL Injection.

create or replace procedure SELECT_USER(user IN varchar2, pass IN varchar2, userid OUT NUMBER,tablename IN varchar2) IS

```
BEGIN
@query= ' SELECT * FROM USERS
WHERE ' ||
      'username = '''|| user ||
      'AND password = ''' ||
password || '''';
Exec @query;
Commit;
END;
```

Likewise, Stored Procedures should be used in conjunction with input validation. Just because type checking is done, it doesn't mean that one can get away without validating their user input.

Minimum Privilege:

Last but not the least, always ensure that the database user executing the queries has only SELECT or the minimum required privilege to use the application. This will prevent the database getting corrupted or wiped out should an attack occur.

So, Start following these simple requirements in your applications and you can be sure that you wouldn't have a security consultant coming to you and asking you to fix your code.

Celia

Celia has been with Infosys for the past 5 years and has been associated with Internet Application Security since August 2010. Her expertise includes Product Development, Secure Code Development, Penetration Testing and Secure Code Analysis. She is a Certified Ethical Hacker and is currently engaged in application security consulting.

ClubHACK

Look both side before crossing one way track

Photography: Madhav Goel

https://www.facebook.com/madhavgoyalphotography

Concept & Design: pankit@chmag.in

Issue 28 | May 2012

www.clubhack.com