THE DARK WEB

1) The Way Things Were - Not so long ago, before the World Wide Web came into prominence, to buy stuff we had no option but to either use cash, cheques, credit cards with signatures, you know? The type which used the mechanical swipe machine with a counterfoil. Then magnetic strips came along and more recently embedded security chips appeared where you had to enter your 4 digit Personal Identification Number or PIN code. However all that is now changing, and changing fast!

2) What's in your wallet? – Cash, credit and now debit cards form the main ecological mix within most people's wallets and purses, however a new beast is rearing its head, the contactless card.

3) Why Contactless Cards – there are a number of reasons why these cards a gaining popularity. Here are some given by the UK Card Association –
    a. There's no need to have the correct change
    b. There's no need to mess about entering your PIN in to the terminal every time.
    c. From time to time, you may have to enter your PIN in to the terminal, this is just a security check - to verify that you, the authorised cardholder, are still in possession of the card.
    d. There's no need to queue for so long; as contactless speeds up the time it takes to make a payment It reduces the need to find a cash machine or carry cash It's more convenient than other types of payment
    e. There's no need to carry an additional card - contactless functionality can be provided on a standard credit, debit, charge or pre-paid card

4) Is this Possible - Play video clip from NCIS, which shows how it may be possible for someone to remotely scan your card and then use it to make a clone.

5) What about this? – Play video clip which explains a bit about the way RFID works and how this facility can be abused.

6) It Gets Worse! – This video clip shows how even your smartphone may be used to allow thieves to hack into your contactless card over the Internet from anywhere in the world.

7) Are there any Safeguards – The industry have basically come up with two safeguards for stopping or least limiting fraudulent use of your contactless card –
    a. There is a £20 limit per transaction imposed when used
    b. After a maximum of 5 transactions you will have to enter a pin to continue using the card

8) What Happens Next? – If you are unlucky enough to have your card scanned then either the details can be used to clone your card or the information could be sold on the old fashioned black market or it can be sold online over sites on the Dark Web.

9) Some Internet Basics - Before the Dark Web existed there was the Internet. To understand how the Dark Web functions it may be worthwhile taking a quick look at some of the Nuts and Bolts of how the Internet works -

a. Why the Internet? – The Cold War, Russian A-Bomb 29th August, 1949; Sputnik 1 launched 4th October, 1957. Because of these factors the Advanced Research Projects Agency or ARPA was created by DoD in the USA in 1958, later to be renamed the Defence Advanced Research Projects Agency or DARPA. The need to facilitate research between DARPA facilities and universities was seen as essential to keeping the US safe from foreign threats, basically paranoia. One way to achieve this was to develop a resilient data communications infrastructure, even if part of it was taken out by an Atomic Bomb, communication between many government, DoD and other facilities would still be possible.

b. First steps – ARPANET – In 1963 J.C.R. Licklider convinced ARPA to fund research into creating a network infrastructure, based on his ideas, which would allow multiple distributed computers the ability to communicate and transfer data between themselves and in 1969 the first contract was given to BBN Technologies to develop such a network. The main component of which was the ***Interface Message Processor***, now known as a ***router***. Development on what's become to be known as TCP/IP, a critical communications protocol which underpins all network communication, began in January 1973.

c. The Concept – conceptually, the Internet is a ***packet-switched network*** in the form of a large interconnecting mesh, not a web, the nodes of which are comprised of routers. A router is a device that is able to receive, store and transmit data in the form of packets, following various rules using network or IP addresses over the network infrastructure from one computer to another.

d. What is TCP/IP – The TCP bit stands for Transmission Control Protocol, this ensures that data sent from one computer to another, amongst other things, arrives safely and in the right order while the IP or Internet Protocol part of this package provides the information necessary for delivering the encapsulated data to its destination address.

e. Why IP? – Every device on a network such as the Internet has an IP address. IPv4 most popular, now superseded by IPv6. IPv4 addresses use ***dotted decimal format*** to display their information, but to really understand what's going, on you need to read it in binary, however this is not necessary for this presentation.

   Let's take a look at a typical IP address – 192.168.0.1

   Although it is not obvious there are two parts to this address, in this particular class of address (see below) the first three columns represent the network address while the last column gives you the address for the device or host connected to the network. This is defined by a thing called the ***Sub-net Mask.*** You may have come across this while rummaging around in the Internet settings for your PC. As this is usually configured automatically you probably would have not seen any figures entered here and therefore wouldn't have been any the wiser as to its significance.

   There are 5 classes of network addresses -

   Class A – range from 1.x.x.x to 126.x.x.x and are mostly used by extremely large institutions i.e. governments, universities, multinational companies, ISPs etc. Here the first column is the network address and the next three columns gives the number of hosts, a maximum of 16,777,214 per network address. It is worth mentioning that there are only 126 of these large users in existence. Address 10.x.x.x can be used by an internal network and are ignored by a router.

   Class B – range from 128.x.x.x to 191.254.x.x and are also used by large companies and government bodies but can only support 65,534 hosts on a network and 16,384 networks in total.

   Class C – range from 192.0.1.x to 223.255.254.x and can only support 254 hosts per network but have somewhere over 2 million networks available.

Class D – range from 224.0.0.0 to 239.255.255.255 and support multicasts, messages sent to many hosts.

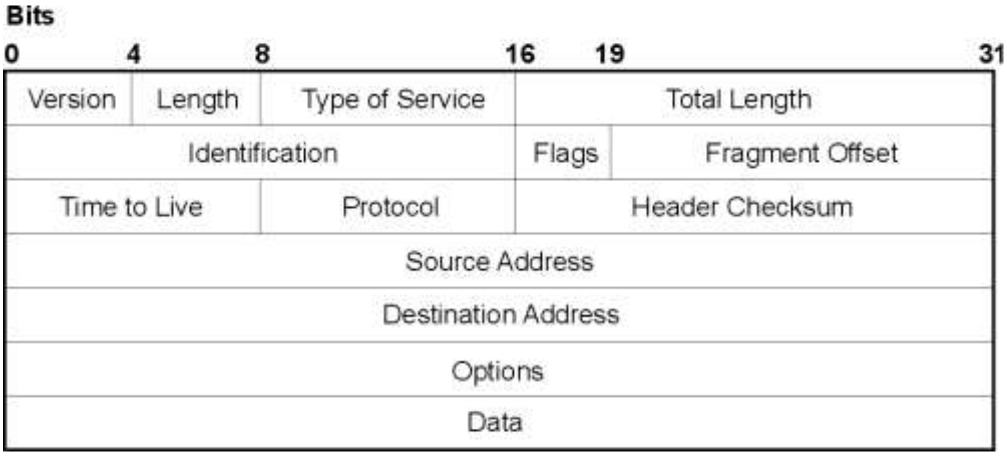
Class E – addresses are used for experimental purposes

There is one address missing from here and that is 127.x.x.x which is used for what is primarily used for loopback testing

Class C addresses are primarily used by you and me for our own internal home networks. The reason why the addresses used by a home router always starts with 192.168.___.___ is that they are configured to block these addresses from being passed through to the Internet, If this wasn't the case, someone who knew what your IP address was could easily gain access to your computer also we'd run out of IP addresses fast. Routers support a function called Network Address Translation or NAT which blocks all internal IP addresses in a home network from being passed to the Internet. They are effectively invisible from outside scrutiny.

Another useful function of modern day routers is the facility to automatically allocate IP addresses to devices connected to the home network. This is called Dynamic Host Control Protocol or DHCP. Once upon a time you would have had to manually configure your networked computers with static IP addresses along with the appropriate subnet mask to allow them to communicate over a home Local Area Network (LAN). However nowadays life is much easier, all that configuration is done automatically by using DHCP. However in certain instances especially if you are a hardened Gamer you may have to delve into things like IP addresses, sub-net mask and port addresses to allow you to play your multi-player "shoot-em-up" with your Internet buddies.

10) Packet up – Every packet that is transmitted over a packet-switching network such as the Internet, the largest such network in existence is constructed of two major pieces: the packet header and the data. Within the header are several distinct pieces of information about the packet itself. This information includes the version of the protocol being used (IPv4 or IPv6), the length of the packet, the number of packets used to send the total data in question, the source and destination addresses, a checksum (used in error correction calculations), and the Time To Live (TTL) data, which defines how many devices the packet may be transmitted along, or hops, before the message is allowed to time out. The data itself is divided into segments of length that can vary, generally in a range of 0 to 64 kB. Packets are transmitted over Ethernet networks, the most common physical type, within frames, or pre-set data blocks that have their own header and trailer information.



Bits

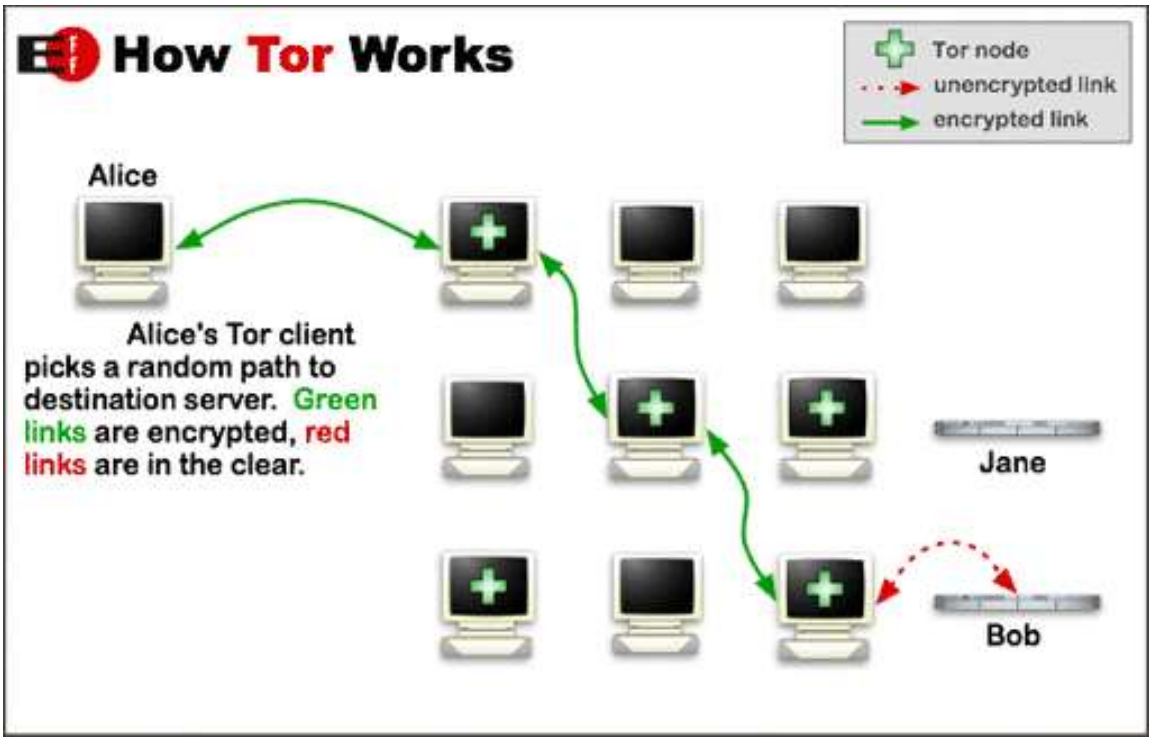
0	4	8	16	19 31
Version	Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				
Data				

wWw – The World Wide Web created in 1990 by Sir Tim Burners Lee is a service that works on top of the Internet and at its heart has two main concepts. The first is the Universal Resource Locater or URL which allows someone to access websites by typing a sites' name into a browser, such as Internet Explorer, rather than having to memorise an IP address. The second major capability of the WWW is the ability to link between one web page, document, web site and more, by using Hypertext Mark-up Language or HTML which utilises the Hypertext Transfer Protocol or HTTP over the Internet infrastructure. No longer did the information available to you have to conform to a linear format, by using Hypertext you could jump from one item to another just by clicking on a link. This became known as Surfing the Web, you sort of went with the flow.

The ability to use URLs and Hypertext relies on a large number of computer systems dotted around the world, called Name Servers which are part of the Domain Name System (DNS). These reside on the Internet and are run by some ISPs, large companies, universities and other large organisations including the London Internet Exchange, at Telehouse Docklands, which is a major hub for much Internet traffic in the UK. Their job is to convert your URL say www.google.co.uk to an IP address by means of a look up table. These tables are forever being updated and synchronised with other Name Servers on the Net.

11) Origins of the Dark Web – Back in the 80's the US Navy became aware that communication over ARPANET was not as secure as maybe it should be. Not only that the data was able to be traced from its originating source to its final destination. The source and destination IP addresses were open to inspection by anyone with the relevant ability and equipment. This could lead to breaches in national security. In the 90's development began on ways to secure such sensitive information and in 2002 the TOR (stands for The Onion Router) was launched. Later in 2006 the US Navy handed over development and maintenance to an external not-for-profit organisation.

TOR works by utilising over 5000 volunteer servers over the Internet. By using a specially designed web browser data is routed through these servers which add various levels of encryption to the data as it passes through them to its final destination where the encryption is finally removed. Because of this secure process the TOR network started to be used by drug dealers, money launderers and sellers and buyers of all sorts of illegal stuff, like credit and debit card information, hence the name the Dark Web.


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

Though the Dark Web has a bit of a reputation for these sorts of goings on, it is also used in many places especially the Middle East, China and other countries where there is a high level of scrutiny of dissidents and others who want to let the world know of atrocities and other activities being committed by their governments or other factions. The Dark Web has been instrumental in reporting the horrors which have befallen many in places such as Syria and Afghanistan.