Opendium

HTTPS Interception

What is it, why is it important and how does it work?

What is it?

HTTPS interception encompasses several mechanisms that online safety systems or web filters use to examine encrypted internet communications. The terms "SSL interception" and "TLS interception" are sometimes also used interchangably.

Why is it important?

Safeguarding students is incredibly important for schools. Online safety systems such as web filters are a key part of any safeguarding strategy. These systems block inappropriate material, record an audit trail and report on any concerning behaviour.

To do this, they have to monitor the internet connection. Historically, most communications have been unencrypted and the system can just look at the communications as they pass by.

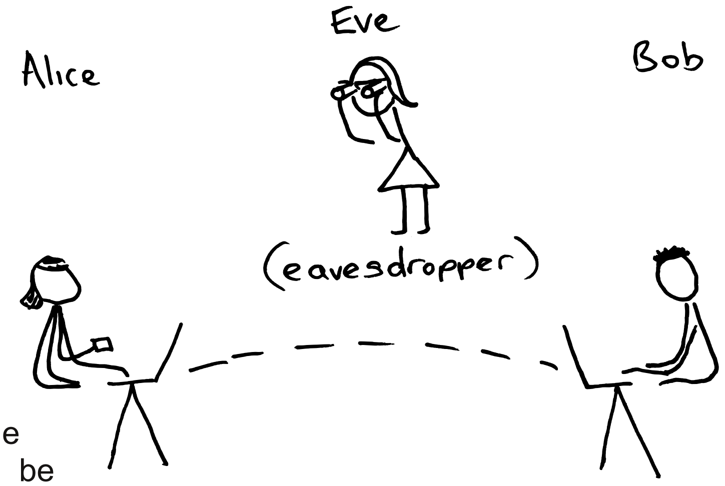
Encryption has always been used for financial transactions, such as online banking, shopping, etc. However, over the past few years many other web sites and apps have been gradually moving towards encryption. More recently, it was revealed that intelligence agencies have been engaging in mass surveillance operations and this has further encouraged the use of encryption.

Whilst encryption adds an important layer of security, it is at odds with some of the schools' safeguarding responsibilities. Filters can no longer passively watch communications and schools must find a balance between privacy and safety.

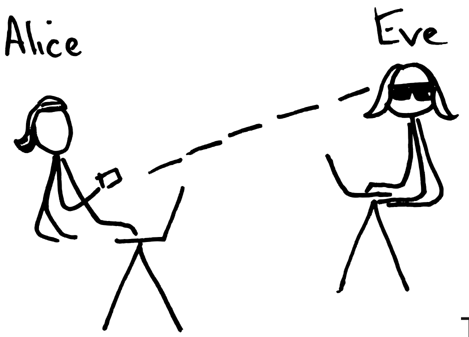
How does it work?

The "secure web" or HTTPS uses a technology known as Transport Layer Security (TLS) or Secure Sockets Layer (SSL). Its job is to keep communications secure.

TLS encrypts the communications between the two ends of the connection. Someone who is watching the internet connection can't snoop on the encrypted communications. For example:

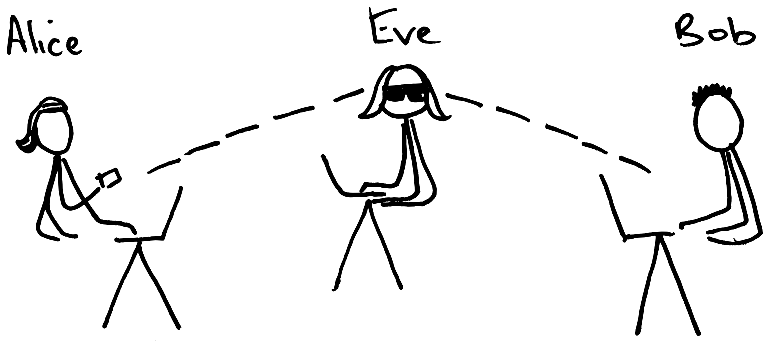


Alice is buying something from Bob's website by sending her credit card number. She wants to make sure that the only person who can see the credit card number is Bob. Alice makes an encrypted connection to Bob's website and sends her credit card number through that connection. The credit card number will be encrypted, sent across the internet and decrypted again at the other end. It doesn't matter if an eavesdropper overhears the communication because they won't be able to decrypt it and get the credit card number.

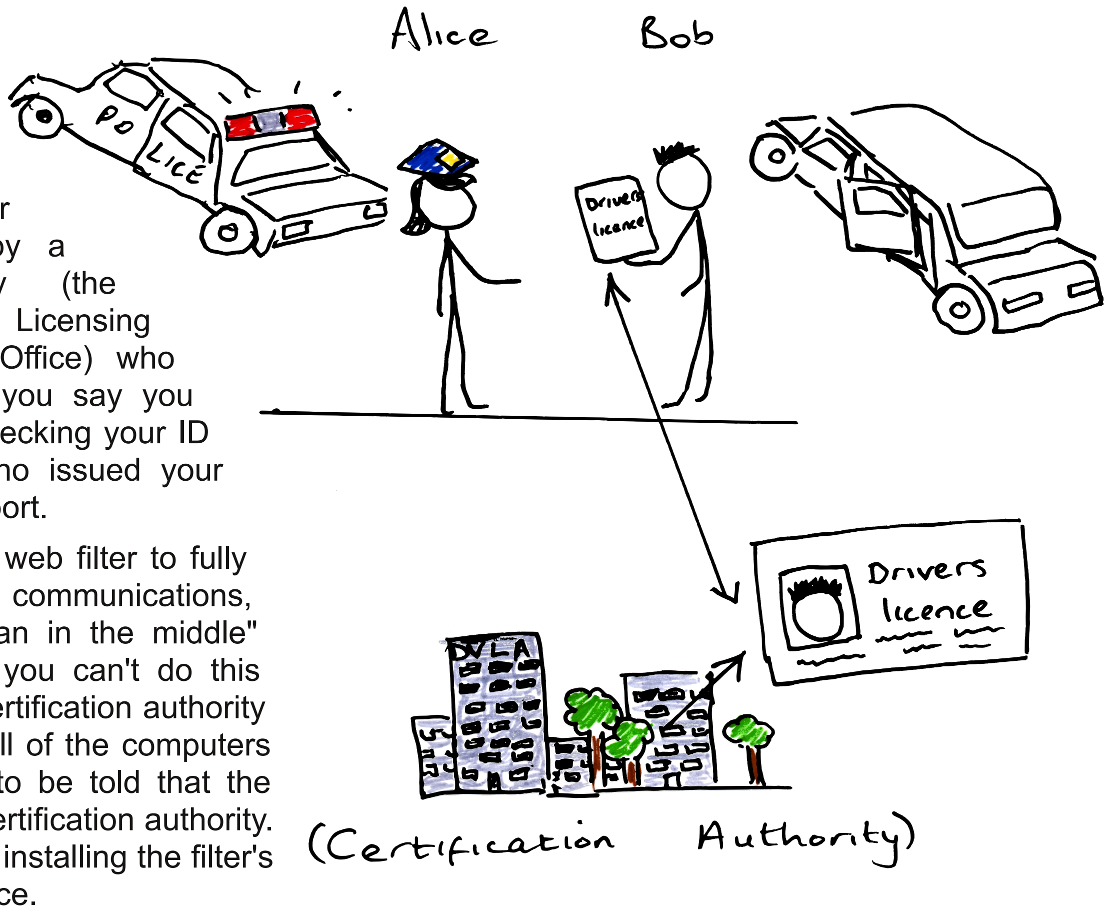


Of course, Alice needs to be completely sure that her encrypted connection is to Bob's website rather than to someone else. If she doesn't know who she connected to, the eavesdropper could pretend to be Bob's website.

By pretending to be Bob's website, the eavesdropper can receive and decrypt Alice's credit card number, and then encrypt it again and send it onto Bob whilst pretending to be Alice. No one would know that the eavesdropper has seen Alice's credit card number. This is known as a "man in the middle" attack[1].

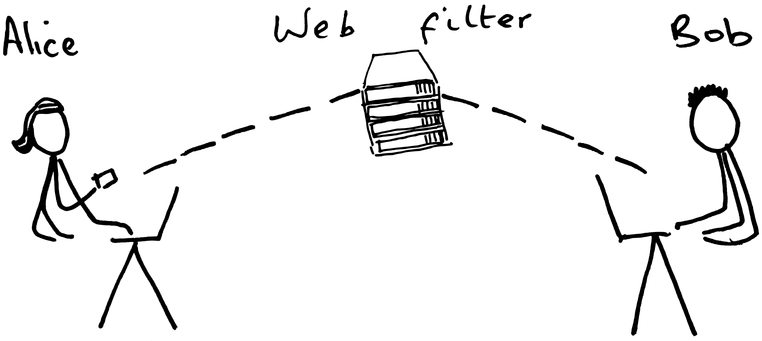


TLS avoids this problem by asking a third party to certify that Bob is who he says he is. When Alice connects to Bob's website, the website sends a certificate to identify itself. The certificate is signed by a certification authority who has checked that Bob is who he says he is. Computers come with a list of trusted certification authorities, so Alice can just check the certificate against that list. The certificate cannot be forged by anyone other than a trusted certification authority so Alice knows that she really has connected to Bob's website.



You can think of this like using your driving licence or passport to prove your identity. The driving licence or passport is issued by a certification authority (the Driver and Vehicle Licensing Agency or Passport Office) who checks you are who you say you are; and the person checking your ID trusts the authority who issued your driving licence or passport.

In order for a school's web filter to fully examine the encrypted communications, it must become a "man in the middle" eavesdropper. Since you can't do this without the help of a certification authority who everyone trusts, all of the computers on the network need to be told that the web filter is a trusted certification authority. This is usually done by installing the filter's certificate on each device.



When Alice connects to Bob's website, she will be presented with a certificate that is signed by the web filter rather than Bob's certificate. As her computer has been told that the filter is trustworthy, this will be accepted. In our Iceni online safety systems, this is referred to as "active HTTPS interception".

Some web filters are also able to filter and audit in a reduced capacity without fully decrypting the communications. A limited amount of information, such as the website's domain name, can be extracted without being a "man in the middle", and this can often be used for rudimentary filtering and auditing. Since no certificate needs to be installed on devices in this mode, this can be useful for guest devices, etc. Our Iceni systems call this "passive HTTPS inspection".

To intercept or not?

We firmly believe that it is no longer possible to effectively safeguard school age students without HTTPS interception and inspection. We also advocate providing some level of filtering even for trustworthy members of staff to protect against accidents. Some schools may decide that the reduced capabilities of passive HTTPS inspection are appropriate for staff whilst protecting their privacy. If devices belonging to visitors are to receive any filtering or logging, passive HTTPS inspection is often the only option, as installing certificates onto guest devices is not usually feasible.

The filtering technology employed by the different online safety products also needs to be considered when deciding what level of HTTPS interception should be employed. Almost all filtering systems utilise a database of known web addresses. Although passive inspection only allows websites to be filtered based on domain name, rather than the full web address, this is still fairly effective. Products such as Lightspeed Systems' Web Filter rely almost entirely on this type of filtering. However, this method can only control access to web sites that are already in the filter's database. Some other software such as our Iceni Web Filter, and Smoothwall's Web Filter, can improve their accuracy by also analysing the content of all websites as they are accessed. This latter type of system therefore benefits much more from active HTTPS interception.

Whichever filtering system you use, choosing not to use active interception will severely restrict its auditing and reporting capabilities. Reports such as suspicious web searches require information that can only be collected through active interception.

Compatibility

Some poorly written software does not consult the list of trusted certification authorities and therefore rejects the intercepted certificate. In order to allow such software to work, active interception must be disabled and filters will usually let you selectively disable HTTPS interception for specific websites.

The method used to retaining compatibility with such software varies between the various filtering products which are on the market. Our Iceni systems have a built in list of websites for which interception should be disabled to work around these compatibility problems, and you can add additional sites if necessary.

Privacy

Schools must find a balance between privacy and safety. Most filters will let you selectively disable HTTPS interception for some websites. Since practically every filtering system will collect some data about your users' browsing habits, your acceptable use policy (AUP) should already mention that you may monitor communications. If you are employing HTTPS interception, your AUP should reflect this too.

Permission should be sought from the user prior to installing the web filter's certificate onto personal devices.

Security

If the web filter is intercepting and decrypting HTTPS communications, its security must be considered. Logging data about banking transactions should probably be avoided, and our systems default to excluding banking sites from interception. Even with this safeguard, there is the potential for the filter's capabilities to be abused to capture or modify encrypted communications.

In February last year, laptop manufacturer Lenovo were found to be shipping computers pre-installed with software called Superfish VisualDiscovery[2]. Superfish intercepted HTTPS connections and injected adverts into them. More recently, it has been discovered that Dell may have been doing something similar. These cases are cause for serious security concerns. Anyone with access to the private certification authority key can forge certificates and therefore intercept secure communications. The private key was installed on all of the computers and they all used the same key, leading to the key being obtainable by anyone. This is not a concern for reputable web filters, as the private key is usually only installed on the web filter server itself and should be unique to the school.

References

1. https://en.wikipedia.org/wiki/Man-in-the-middle_attack

2. https://www.us-cert.gov/ncas/alerts/TA15-051A

Opendium is the only British supplier of online safety systems designed exclusively for schools. Established in 2005, we supply independent and state schools across the UK. Our world class web filtering technology with real-time content analysis allow schools to accurately filter and audit their internet connections. The extensive reporting capabilities identify any concerning behaviour and empower staff to address this directly with the individuals involved, or feed back into the school's eSafety curriculum as a whole.

For further information, or to book a demo, visit **opendium.com/demo** or follow us on Twitter at **twitter.com/opendium** for product updates and videos.

sales@opendium.com
www.opendium.com
(01792) 824568

Opendium Limited
Company No. 5465437

support@opendium.com
www.opendium.com
(01792) 825748