CLEANING A HTTPS FEED

REPORT ON THE FILTERING OF THE HYPERTEXT TRANSFER PROTOCOL OVER TRANSPORT LAYER SECURITY OR SECURE SOCKET LAYER CONNECTIONS

AUTHOR: Benjamin D. McGinnes

DATE: 20/1/2010

CONTENTS

SUMMARY

The Australian Federal Government has proposed the introduction of a filtering policy of content available to Australians via the global Internet. Though initially promoted as a way of protecting children and adolescents against illegal and undefined "inappropriate" material, the policy includes a mandatory level of filtering which would be applied to all Internet users within Australia, regardless of age.

The proposed filtering system of the Australian Communications and Media Authority (ACMA) described in the *Closed Environment Testing of ISP-Level Internet Content Filtering* report includes the analysis and filtering of data transmitted via the Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol over Transport Layer Security (TLS) or Secure Socket Layer (SSL), which are both referred to as HTTPS, or collectively as HTTP/S.

Filtering data transmitted via HTTPS means that data, which is intended to be passed securely between a client and server, would be deliberately compromised by the Internet filtering technologies mandated under the new policy. The result being that all data transmitted via HTTPS would be compromised. This data would include, but may not be limited to, personal authentication information (e.g. usernames and passwords for any website), credit card details, online banking information, personal medical information (e.g. through health insurance websites), proprietary commercial data, online shopping orders and more.

All methods of HTTPS filtering would result in data, which is intended to be securely transmitted, being susceptible to theft or misuse by either Internet Service Provider (ISP) employees, public servants or both, depending on how the HTTPS filtering method is deployed and maintained.

INTRODUCTION

The purpose of this paper is to demonstrate that the application of the Clean Feed Internet filtering policy to HTTPS Internet traffic will have undesirable consequences. This comes in two main parts:

1. The technical aspects of implementing the filtering of HTTPS transactions. Specifically this details the ways in which HTTPS traffic is, or may be, analysed and filtered and what type of data may then be available to any unintended party.
2. The economic implications of the policy on Australian businesses and Australian electronic commerce.

This paper does not cover, though may touch on part of:

1. Details of methods of circumventing the filtering.
2. Details of potential conflicts of the policy with existing Australian State or Federal legislation.
3. Details of potential conflicts of the policy with existing international treaties to which Australia is a signatory state.

Since the majority of this report was written, the Minister for Broadband, Communications and the Digital Economy has released Enex TestLab's *Internet Service Provider (ISP) Filtering 'Live' Pilot Report*.[1] The pilot program tested blocking a list of Uniform Resource Locators (URLs) from a number of blacklists, including the ACMA blacklist. It also tested filtering of additional content which is, or may be, Refused Classification in Australia.

The report stated that testing was performed on web content, but did not specify whether that content was restricted to that transmitted via an ordinary HTTP connection or whether it also included content transmitted via HTTPS. The methods of filtering used in the pilot program, including Deep Packet Inspection (DPI), are incapable of determining the full URL of a HTTPS connection without cracking the encryption used. The pass-by[2] and pass-through[3] methods used by the filtering solutions tested are only able to determine the hostname and IP address of a connection. Although the filtering methods tested in the pilot are incapable of filtering HTTPS and other encrypted content, there is no guarantee that the filtering regime will not be expanded to include it in the future using different technology.

Should blocking specific HTTPS URLs or dynamic filtering of content transmitted via HTTPS be required, then one of the methods of circumventing or cracking the encryption will be required. This is also the case for encrypted data transmitted via other protocols, including email, instant messaging and VPNs.

[1] http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot, Enex TestLab for the Department of Broadband, Communication and the Digital Economy (DBCDE), 2009.

[2] *Internet Service Provider (ISP) Filtering 'Live' Pilot Report*, pp. 8-9, Enex TestLab, 2009.

[3] *Internet Service Provider (ISP) Filtering 'Live' Pilot Report*, p. 9, Enex TestLab, 2009.

At this stage there is no indication as to whether the mandatory implementation of this policy, which affects all Australians regardless of age, will be applied only via a blacklist or whether it will also include filtering. Nor is there any indication as to whether the mandatory implementation may be expanded from blocking to filtering.

TECHNICAL IMPLEMENTATION

The Clean Feed Internet filtering proposal of ACMA, under the guidance of Senator Stephen Conroy, includes in its list of features the filtering of online content transmitted by both HTTP and HTTPS, along with blocking or filtering of content transmitted via other protocols.[4]

The format for content in each of these protocols is essentially the same, with one key difference: HTTP traffic is transmitted openly, while HTTPS traffic is transmitted across an encrypted connection between the user or client and server.

Filtering HTTP traffic is essentially simply a matter of intercepting packets of HTTP data transmitted back and forth between client and server hosts and examining the content of those packets for content which matches a set of rules specified by the filtering product's configuration.

As with HTTP, HTTPS runs on a default port, port 443, making it easy to identify most traffic transmitted in that manner by scanning for traffic connecting to servers via port 443. Just as it is possible to run a web server on an alternate port, it is possible to operate a secure web server on an alternate port. Filtering HTTP or HTTPS traffic on alternate ports requires the packets of Internet data be examined to determine whether they contain HTTP or HTTPS instructions to connect to servers operating on alternate ports, rather than merely scanning all traffic connecting to servers on the two default ports (i.e. 80 and 443). In the case of HTTPS this would be the handshake steps to establish the secure connection, as the HTTP GET and POST requests are only transmitted within an encrypted transmission.[5] A filtering system utilising a method of examining the content of all traffic on non-standard ports would incur increased processing loads on both the systems performing the filtering and network routing.

Filtering HTTPS traffic is theoretically similar to filtering HTTP traffic, but requires an additional step to circumvent the encryption used to establish the Transport Layer Security (TLS) or Secure Socket Layer (SSL) connection between the client and server. There are three ways to achieve this:

1. Place a HTTPS proxy server between the client and server hosts which masquerades as the intended server to the client and then connects to the correct server after filtering the content.
2. Obtain the keys used by the client and server to encrypt and decrypt the data transmitted across the SSL or TLS connection.
3. Crack the encryption method or algorithm used to encrypt the data.

HTTPS Proxy Server Filter

A HTTPS Proxy server would be the easiest of the three options to implement. Its configuration and essential behaviour would be similar to that of a regular HTTP proxy server.

[4] *Closed Environment Testing of ISP-Level Internet Content Filtering*, pp. 44-46, ACMA, 2008.

[5] *HTTP Over TLS*, http://tools.ietf.org/html/rfc2818#section-2.1, Internet Engineering Task Force, 2000.

With a normal HTTP proxy server a client connects to the proxy server instead of directly to the destination server and passes all its requests for content to the proxy server. The proxy server then connects to the external Internet servers to obtain the requested data and return it to the client. The proxy server may also serve this data from its cache if it is available.

Data sent and received by by a HTTP proxy server is transmitted in clear text, making it easily scanned by filtering software according to the filtering policies specified in its configuration.

When a client connects to a secure server via HTTPS the client receives confirmation of that secure connection upon acceptance of a digital certificate, such as an SSL certificate or TLS certificate. The certificate contains information identifying the server, the organisation which owns it and the site it is attached to, along with certain cryptographic identifying information which can be used to verify it is genuine (e.g. the certificate key's digital fingerprint).

When a client connects to a secure server via a HTTPS proxy server the client establishes a secure connection only to that proxy server. The configuration of the HTTPS proxy server then determines whether the transmission continues to its destination according to the filtering policies it is configured with. That configuration may be to establish a new secure connection from the HTTPS proxy to the destination server, to establish an insecure HTTP connection or to terminate the transaction. The client host will be unable to verify the details of that connection.

The HTTPS proxy server would provide the client host with a certificate of its own, not the certificate of the destination host. If it simply served the client with the destination's certificate an error would be generated indicating that the HTTPS proxy server's identifying information (e.g. hostname, IP address, etc.) did not match the destination which owned the certificate. The HTTPS proxy server can only serve its own certificate.

If the client or a user knows the details of the destination's certificate they could confirm whether or not they have a secure connection to the intended host server or another server. Even if the HTTPS proxy server attempted to conceal this by matching details of the destination server's certificate (e.g. organisation name, signing authority name, date of expiration, etc.), the client could still verify the details using the cryptographic fingerprint if the destination server's certificate details are known.

Regardless of whether the client recognises the connection is running through a proxy or not, the content of any such transaction is now wholly open to the HTTPS proxy server. This proxy server can then be configured to scan for any type of data intended to be transmitted securely. This data may include the type intended to be banned by the ACMA, illegal or “inappropriate” material, but it could include any other data type the proxy server's administrator decides to scan for. An unscrupulous administrator could, for example, configure the HTTPS proxy filter to follow the government set guidelines and also send him or her a copy of any credit card or banking information transmitted through the server.

Without any transparency of the HTTPS proxy server's configuration, which would be at the discretion of the individual ISP maintaining it, there would be know way of knowing precisely what is being done with any of the data which passes through it. For this reason the HTTPS proxy method of filtering is more accurately described as a Man-in-the-Middle attack.

TLS/SSL Key Escrow

The second filtering method requires the filtering server have access to the cryptographic key of any secure website intended for use by Internet users in Australia. This would allow users to connect directly to their intended destination server, but still enable the filtering required by the Clean Feed policy to occur. Holding TLS or SSL keys by a third party in this manner is referred to as a key escrow system.

When a TLS or SSL session is established between a client and server the client generates a session ID which is sent to the server and encrypted with the server's public key. The server responds with it's own part of the session and the pair share a secret master key for that encrypted session and only for that session.

A filtering system utilising key escrow would only have the secret key of the server that corresponds with the public key provided to clients with the SSL or TLS certificate. It would then need to monitor the start of the transaction to obtain the session master key created during the SSL or TLS handshake process in order to monitor the remainder of the encrypted session.

A key escrow system would enable the government to block all HTTPS connections, except those secure sites willing to provide their TLS or SSL key to an escrow repository linked to the filtering system. This would only allow the passage of encrypted data which could be decrypted in order to be filtered according to whichever filtering policy had been selected. As with a HTTPS proxy server, there would be no transparency regarding which filters were actually being applied.

While it does not, unlike the HTTPS proxy, attempt to masquerade as the destination intended to be reached by a user, it does enable the filtering system to analyse all data transmitted. This system depends on the willingness of individual secure sites to provide their private encryption keys to a third party, or to more than one.

TLS/SSL Cryptographic Cracking

Cracking the encrypted connection between a client and server is the most unlikely method of filtering HTTPS transactions. Primarily because the computing resources required are significantly beyond the scope of most organisations, as such it would essentially be the province of military or national security organisations, such as Australia's Defence Signals Directorate (DSD), the United States' National Security Agency (NSA) or the United Kingdom's Government Communications Headquarters (GCHQ).

There are essentially two methods of cracking encryption: by leveraging a flaw in the mathematical algorithm used to encrypt the data and by a brute force attack.

The advantage of identifying and utilising a flaw in an encryption algorithm is that, once it is done, all data encrypted using that algorithm can be decrypted. The main disadvantage is that if such a flaw exists then it is only a matter of time before other parties discover the flaw and publicise it. When these flaws are made public, security systems move away from using the flawed algorithms to algorithms which either lack such flaws or have not yet been found to contain such flaws.

The alternative method of cracking the encryption is a brute force attack against either: the cipher used to encrypt the data; or the password, code or pass phrase used to unlock the data.

The sole advantage of this method is that success is difficult to determine by another party, such as the transmitter of the encrypted data. The main disadvantage is the time and resources required to perform a brute force attack against a cipher or encrypted data.

Current estimates of brute force attack requirements[6] indicate that the time required to perform a complete attack against current commercial 128-bit encryption, even under the best theoretical conditions, would take billions of years. Add to that the work to improve this security, such as that outlined by the NSA,[7] means that most data would be re-encrypted using improved newer standards before a prior standard could be effectively broken by a brute force attack.[8]

To incorporate the filtering of HTTPS data in a real time Internet censorship system would require as little load on system and network resources as possible as the filtering would need to be applied to any HTTPS connection established by any Internet host, client or server, within Australia at any time. For this reason the HTTPS proxy method of filtering is the easiest to implement because it does not require the cooperation of any website, either within Australia or overseas, for copies of encryption keys, nor does it require large computing resources to crack SSL or TLS encryption.

The use of a HTTPS proxy between a user and the server they intended to connect to would be simple to identify by the difference in the digital certificate served to the user by the proxy when compared with the details of the certificate of the intended destination server. The only circumstance under which the identification of the HTTPS proxy's presence would be viewed as a negative is if the filtering system is intended to be undetected by Australian Internet users.

If the intention is to filter HTTPS data without Australian users being aware that the filtering is occurring at the time, then the method of filtering will need to utilise either a key escrow system or cracking of the encryption.

The key escrow system will work, but depends entirely on the willingness of every secure website which an Australian Internet user wishes to connect to sharing its secret key or keys with the escrow system or face being arbitrarily blocked by the Internet filtering system. Even with the cooperation of the owners of every secure website, which would be unlikely as it would be dictated by the security policies of the website owners and many of those being outside of Australia, a key escrow system would require a considerable administrative effort to maintain. As most website certificates are updated every one or two years the escrow system would need to be updated at the same time as every single website's certificate is updated.

[6] Brute force attack, http://en.wikipedia.org/wiki/Brute_force_attack, Wikipedia, 2008

[7] *NSA Suite B Cryptography*, http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml, United States of America National Security Agency, 2009

[8] Note that many sites are now using a 256-bit AES cipher instead of older 128-bit ciphers (most often the 128-bit RC4 cipher).

Given the administrative complexities and costs of maintaining an effective key escrow system and given the high likelihood that many sites, especially those outside of Australia's jurisdiction, would have security policies which prevent sharing the secret key of a secure website with a third party of any type, it is unlikely that a key escrow system will be able to be effectively deployed. If it were deployed under those circumstances then Australian Internet users would effectively be limited to the relatively small number of sites willing to share their secret keys with the Australian Communications and Media Authority. While every other site which does not share its keys, for any reason, would be arbitrarily blocked.

Should the Internet filtering system require Australian Internet users being unaware of the filtering taking place, as with a HTTPS proxy, and the HTTPS key escrow system being effectively infeasible, then the only remaining course of action would be to attempt to crack the encryption used by the SSL or TLS connections. While it is theoretically possible to do this, the resources required for cracking even a single SSL or TLS stream are considerable. The methods of cracking the encryption would depend on the algorithms used (e.g. RC4, Triple DES, AES) and the computing resources required would depend on the size of the key (e.g. 128-bit, 192-bit, 256-bit).[9] As a consequence it is extremely improbable, if not impossible, for an attack on these ciphers to succeed in real time.

Since TLS has been designed to prevent an undetected attack, or decryption by a third party, and since the purpose of an Internet filter is to interfere with a transmission which contravenes the censorship policy it is less likely that the Clean Feed system will require an undetected method of filtering HTTPS. This coupled with the difficulties associated with the TLS/SSL key escrow and encryption cracking methods means that the HTTPS proxy method is the one which is most likely to be deployed.

[9] Other bit sizes are also chosen, depending on the policies of the site. For example the Commonwealth Bank of Australia's current (2009) NetBank key is a 168-bit Triple DES cipher, while the WikiLeaks website's current key is a significantly stronger 256-bit AES cipher.

ECONOMIC IMPACT

In the 2007-08 fiscal year Australian businesses received approximately $81 billion income from Internet receipts;[10] nearly one and a half times the amount of 2005-06 fiscal year, at $56.7 billion, which was more than double the amount of the 2002-03 fiscal year, at $24.3 billion.[11] This is a growth rate of approximately $24 billion every two to three years.

Most, though not all, of that turnover is sourced from electronic commerce; such as credit card transactions via online shopping sites or through transfers of funds from online banking. Mandatory filtering of all HTTPS traffic would, as described in the previous section, render these avenues of commerce insecure.

While it would be possible, even likely, for the ACMA to establish whitelists of e-commerce sites known to not contain data which would be illegal, such as the Internet banking sites of Australian banks, this still leaves thousands of online shops and merchant gateways which would not be added to such a whitelist.

At this stage no such whitelist has been announced, nor have any procedures for an exemption of secure e-commerce sites to be added to such a whitelist. It is equally likely that the administrative procedures required to maintain such a whitelist would incur additional, and currently unnecessary, costs on the owner of any secure website who wishes to have traffic between their site and Internet users in Australia remain unfiltered.

For Australian businesses this may become a requirement of operating an electronic commerce point of sale or service; just part of the cost of doing business. For international sites it may be easier and cheaper to simply prevent electronic commerce transactions originating from Australian Internet hosts; by blocking all Australian IP addresses to their merchant gateway systems, for example.

The inverse is also a significant factor: international Internet users will be unlikely to utilise electronic commerce sites hosted in Australia when they realise that their commercial transactions will become subject to the mandatory filtering of HTTPS traffic. Secure certificate authorities, such as Verisign or Thawte, may require sites be hosted where they will not be automatically filtered. This would have the flow-on effect of existing Australian e-commerce sites moving offshore in order to meet the requirements of obtaining SSL or TLS certificate policies. Certificate authorities not enforcing such a measure, or providing an alternative type of certificate for Australian servers to differentiate them, could see their primary certificate products undermined in reputation and value.

[10] Internet income ($b), http://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/BF7CE3F9E4EE448CCA25761700190B66?opendocument, ABS, 2009

[11] Internet income ($b), http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8129.0Main+Features12005-06?OpenDocument, ABS, 2007

Australian Internet and Hosting Service Providers

The cost to ISPs and Hosting Service Providers (HSPs) in Australia comes from two main sources: the costs associated with implementing and maintaining the required filtering and the additional costs of maintaining e-commerce sites.

The first of these is the cost of adding the computing, networking and human resources necessary to implement the mandatory filter to all traffic passing across their network. These costs will only affect ISPs or HSPs, which are also ISPs.

The second category of costs are those that comprise the costs of hosting an electronic commerce site. These include additional costs to e-commerce website administration and the flow on effects from site operators seeking to avoid those additional costs.

- For e-commerce site operators the additional cost of obtaining a whitelist exemption, if such a possibility becomes available through the ACMA, would almost certainly require an ACMA authorised review each time new content is added to the site or risk removal from the whitelist. Should TLS or SSL certificate authorities modify their products to differentiate an Australian not-quite-so-secure and filtered site from an ordinary secure site, then the cost of that change will be passed on to the segment of the market that uses it: Australian website operators.

- For the lower end of the e-commerce market, the new costs could be the difference between making or breaking their businesses. It would be both easier and cheaper to move their sites offshore, to one of the many website hosting services in the United States or to a local company which simply resells hosting services based outside of Australia, the latter option would provide GST inclusive billing. Though the lowest end of the e-commerce market already tends to use website hosting through resellers of foreign hosting providers, either locally or internationally, there is still a segment of the small to midrange market which remains in Australia; this will likely shift more to foreign hosting services.

Businesses which currently maintain their own systems collocated at data centres may decide to switch to one or more international locations, a task made easier by advancements in virtualisation which can cut costs further.

This in turn will result in a significant effect on those hosting providers which operate their own data centres in Australia. Though it is difficult to determine the percentage of currently locally hosted content which will move offshore, it may be enough to reduce the amount of colocation space required by Australian business and therefore the number of hosting and colocation providers operating in Australia.

HSPs which rely solely upon providing website hosting and colocation facilities run the risk of either going out of business or being acquired by other, larger corporations. While a diminished pool of HSPs and data centres operating in Australia will reduce choice for businesses seeking a local data solution and possibly raise the cost to those businesses seeking or requiring a local solution.

CONCLUSIONS

Regardless of the method or methods used to scan and filter traffic transmitted across ostensibly secure protocols, such as TLS or SSL, the effect of doing so will undermine the value presently inherent in utilising those protocols.

An entrenched regime by the Australian Government, either in conjunction with the Australian Internet industry or standing alone, to scan traffic primarily used to secure authentication and commercial information will result in the ostracism of any host known to be susceptible to such scanning. Users of Australian hosts visiting international commercial sites will, in time, find their ability to utilise those sites blocked by the sites themselves, as part of a policy to maintain consistently secure connections for their business transactions. Operators of Australian hosts providing commercial services or services requiring authentication will experience a reduction over time of traffic from international sources.

Australian online providers of goods and services will experience a significant and increasing reduction in revenue from Internet sources, both within Australia and without. While Australian online consumers will gradually find themselves frozen out of foreign e-commerce sites. The eventual result being that the only Australian e-commerce will be between Australian providers and Australian consumers. Which will be limited to only those who are willing to risk the possibility that the transactions may be intercepted by another party and those who are ignorant of that possibility.

Those consumers who do choose to take that risk knowingly will almost certainly only utilise methods of payment which will mitigate their risk, such as the charge back option available with credit cards. While others will turn to methods of circumventing the filtering scheme in order to protect their financial data and security.

Australia's online commercial activity will not be completely destroyed by this situation; people are now too used to the convenience of paying bills online or doing their shopping online to completely abandon it. It will, however, be significantly atrophied.

It is difficult to determine the degree to which Australia's online commerce will be reduced or the rate at which that reduction will occur. All that can be guaranteed is that, without an exemption to filtering for all financial transactions or an effective method of circumventing that filtering, there will be a reduction in the financial transactions.

The inevitable result of the shrinking of Australia's online commercial activity will be reduced profits for Australian businesses and losses of Australian jobs.

GLOSSARY

ABS: the Australian Bureau of Statistics

ACMA: the Australian Communications and Media Authority

AES: Advanced Encryption Standard

Blacklist: A list of sites or content which is banned or blocked.

Blocking: Arbitrary prevention of access to content transmitted over a specified protocol.

Client: A host on a network which connects to a server in order to transmit data to it and receive data from it. The client usually initiates such transactions.

Cryptography: The study and practice of concealing information with cyphers in order to transmit it to specified recipients.

Decryption: The process of deciphering encrypted information following transmission.

DES: Data Encryption Standard

DPI: Deep Packet Inspection

DSD: the Defence Signals Directorate

Encryption: The process of concealing information in order to transmit that information securely to intended recipients.

Filtering: Analysis of content to determine which is acceptable or not acceptable according to specified rules of the filter.

Fingerprint: A unique hexadecimal value generated via cryptographic techniques to verify or authenticate a cryptographic certificate or key.

GCHQ: the United Kingdom's Government Communications Headquarters

HSP: Hosting Service Provider

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol over a secure protocol (e.g. TLS or SSL)

HTTP/S: combined acronym for HTTP and HTTPS

IP: Internet Protocol

ISP: Internet Service Provider

Key escrow: A system of holding encryption keys in order to decrypt encrypted data independently of the original sender and recipient.

MitM: Man-in-the-Middle attack

NSA: the United States of America's National Security Agency

Phishing: A form of online fraud in which one site masquerades as another in order to illegally obtain data, usually financial data such as Internet banking logins.

Server: A host on a network which provides content over one or more protocols (e.g. HTTP or HTTPS).

SSL: Secure Socket Layer; the predecessor to TLS

TCP: Transmission Control Protocol

TLS: Transport Layer Security

URL: Uniform Resource Locator

Whitelist: A list of sites or content which is exempt from blocking or filtering.

BIBLIOGRAPHY

Fact Sheets and Online Resources

Australian Communications and Media Authority (2009), *Regulating online content*.
http://www.acma.gov.au/WEB/STANDARD/pc=INT_IND_CONTENT_ABOUT

Defence Signals Directorate (2009), *Australian Government Information Security Manual*.
http://www.dsd.gov.au/library/infosec/ism.html
http://www.dsd.gov.au/_lib/pdf_doc/ism/ISM_Sep09_rev1.pdf

Department of Broadband, Communications and the Digital Economy (2009), *Cyber-safety Plan*.
http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan

Department of Broadband, Communications and the Digital Economy (2009), *Internet Service Provider (ISP) filtering*.
http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering

Department of Broadband, Communications and the Digital Economy (2008), *Internet Service Provider Content Filtering Pilot Technical Testing Framework*.
http://www.dbcde.gov.au/__data/assets/pdf_file/0006/89160/technical-testing-framework.pdf

Department of Broadband, Communications and the Digital Economy (2009), *Internet Service Provider (ISP) Filtering 'Live' Pilot*.
http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot

Internet Engineering Task Force (2000), *Upgrading to TLS within HTTP/1.1*.
http://www.ietf.org/rfc/rfc2817.txt
http://tools.ietf.org/html/rfc2817

Internet Engineering Task Force (2000), *HTTP over TLS*.
http://www.ietf.org/rfc/rfc2818.txt
http://tools.ietf.org/html/rfc2818

Internet Engineering Task Force (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*
http://www.ietf.org/rfc/rfc5246.txt
http://tools.ietf.org/html/rfc5246

National Security Agency (2008), *Fact Sheet NSA Suite B Cryptography*.
http://www.nsa.gov/ia/industry/crypto_suite_b.cfm
http://www.cas.mcmaster.ca/~soltys/math5440-w08/NSA_Suite_B.pdf

National Security Agency (2009), *NSA Suite B Cryptography*.
http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

Schneier, Bruce (1998), *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*.
http://www.schneier.com/paper-key-escrow.html

Sun Microsystems (1998), *Introduction to SSL*.
http://docs.sun.com/source/816-6156-10/contents.htm

Wikipedia (2009), *Censorship in Australia.*
http://en.wikipedia.org/wiki/Censorship_in_Australia

Wikipedia (2009), *Internet censorship in Australia.*
http://en.wikipedia.org/wiki/Internet_censorship_in_Australia

Wikipedia (2009), *Cryptography Portal*.
http://en.wikipedia.org/wiki/Portal:Cryptography

Wikipedia (2009), *Brute force attack*.
http://en.wikipedia.org/wiki/Brute_force_attack

Wikipedia (2009), *Transport Layer Security*
http://en.wikipedia.org/wiki/Transport_Layer_Security

Wikipedia (2009), *Deep packet inspection*
http://en.wikipedia.org/wiki/Deep_packet_inspection

WikiLeaks
https://secure.wikileaks.org/wiki/Wikileaks
http://www.wikileaks.org/

Reports

ABS (2007), *8129.0 - Business Use of Information Technology, 2005-06*. http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8129.0Main+Features12005-06?OpenDocument

ABS (2009), *8129.0 - Business Use of Information Technology, 2007-08*. http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8129.0Main+Features12007-08?OpenDocument

ACMA (2008), *Closed Environment Testing of ISP-Level Internet Content Filtering*. Report to the Minister for Broadband, Communications and the Digital Economy, June 2008. http://www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf

DBCDE (2009), *Mandatory Internet Service Provider (ISP) Filtering: Measures to Increase Accountability and Transparency for Refused Classification Material – consultation paper*. Consultation paper to the Minister for Broadband, Communications and the Digital Economy, December 2009. http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/refused_classification_content_list_review

Enex TestLab (2009), *Internet Service Provider (ISP) Filtering 'Live' Pilot Report*. Report to the Minister for Broadband, Communications and the Digital Economy, December 2009. http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot

Electronic Frontiers Australia (2008), *Labor's Mandatory ISP Internet Blocking Plan*. http://www.efa.org.au/censorship/mandatory-isp-blocking/

Legislation and Treaties

The Australia New Zealand Closer Economic Agreement (ANZCERTA), 1983.
http://www.dfat.gov.au/geo/new_zealand/anz_cer/anzcerta1.pdf

Australia-United States Free Trade Agreement (AUSFTA), 2005.
http://www.dfat.gov.au/trade/negotiations/us_fta/final-text/index.html

The Australian Constitution
http://www.aph.gov.au/SEnate/general/constitution/index.htm

Classification (Publications, Films and Computer Games) Act 1995.
http://www.austlii.edu.au/au/legis/cth/consol_act/cfacga1995489

Guidelines for the Classification of Films and Computer Games, 2005.
http://www.comlaw.gov.au/comlaw%5Cmanagement.nsf/lookupindexpagesbyid/IP200508205?OpenDocument

The National Classification Code, May 2005.
http://www.comlaw.gov.au/comlaw%5Cmanagement.nsf/lookupindexpagesbyid/IP200508203?OpenDocument

Singapore-Australia Free Trade Agreement (SAFTA), 2003.
http://www.dfat.gov.au/trade/negotiations/safta/index.html

Thailand-Australia Free Trade Agreement (TAFTA), 2005.
http://www.dfat.gov.au/trade/negotiations/aust-thai/index.html

News

ABC News, *iiNet pulls out of Govt 'censorship' trials*
http://www.abc.net.au/news/stories/2009/03/23/2524090.htm

AVN, '*It's a Sad Day in Australia': Government Approves ISP Filters*
http://business.avn.com/articles/36990.html

Crikey, *ACMA's blacklist just got read all over*
http://www.crikey.com.au/2009/03/20/acmas-blacklist-just-got-read-all-over/

Crikey, *Yet another ACMA internet blacklist springs a leak*
http://www.crikey.com.au/2009/03/23/yet-another-acma-internet-blacklist-springs-a-leak/

Crikey, *Conroy's continued lies and gaffes*
http://www.crikey.com.au/2009/04/02/conroy%e2%80%99s-continued-lies-and-gaffes/

Crikey, *Internet filtering: speed won't be the issue*
http://www.crikey.com.au/2009/07/27/internet-filtering-speed-won%e2%80%99t-be-the-issue/

Crikey, *Labor Senator Kate Lundy speaks out against mandatory internet censorship*
http://www.crikey.com.au/2010/01/13/labor-senator-kate-lundy-speaks-out-against-mandatory-internet-censorship/

The Age, *Net Censorship Move A Smokescreen: Expert*
http://www.theage.com.au/technology/technology-news/net-censorship-move-a-smokescreen-expert-20091216-kw7d.html

Online Commentary and Discussion

Goh, David, *#nocleanfeed - a bit of a technical description of the problem*
http://thorfinn.dreamwidth.org/50042.html

Lundy, Kate, *My thoughts on the Filter*
http://www.katelundy.com.au/2009/12/17/my-thoughts-on-the-filter/

Lundy, Kate, *Further thoughts on the Filter*
http://www.katelundy.com.au/2009/12/21/further-thoughts-on-the-filter/

McGinnes, Benjamin D., *Clean Feed, part 3*
http://hasimir.livejournal.com/258199.html

McGinnes, Benjamin D., *Clean Feed, part 8*
http://hasimir.livejournal.com/296077.html

McGinnes, Benjamin D., *Clean Feed, part 9*
http://hasimir.livejournal.com/296225.html

Newton, Mark, *Filter advocates need to check their facts*
http://www.abc.net.au/news/stories/2008/11/10/2414895.htm

Q&A, *Adventures in Democracy*
http://www.abc.net.au/tv/qanda/txt/s2521164.htm

Spoonman, Triple M radio, *Internet Censorship*
http://austereo.castmetrix.net/podcast/378302368699163267/1/SpoonmanInternetcensorship.mp3