ssl alternatives

SimpleSSH: A Basic Interoperability Profile for the SSH Protocol
https://www.cs.auckland.ac.nz/~pgut001/pubs/simplessh.txt

Convergence (SSL)
https://en.wikipedia.org/wiki/Convergence_(SSL)

Notaries
https://github.com/moxie0/Convergence/wiki/Notaries

Moxie Marlinspike
https://en.wikipedia.org/wiki/Moxie_Marlinspike

client certificates

Client Certificate Authentication with HAProxy
https://www.loadbalancer.org/blog/client-certificate-authentication-with-haproxy/

p11

OpenSC / libp11
https://github.com/OpenSC/libp11/blob/master/README.md

CHAPTER 5. CONFIGURING APPLICATIONS TO USE CRYPTOGRAPHIC HARDWARE THROUGH PKCS #11
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/configuring-applications-to-use-cryptographic-hardware-through-pkcs-11_security-hardening

p11-kit
https://github.com/p11-glue/p11-kit

p11-glue
https://p11-glue.github.io/p11-glue/

Project: p11-kit
https://p11-glue.github.io/p11-glue/p11-kit.html

pkcs11.conf — Configuration files for PKCS#11 modules
https://p11-glue.github.io/p11-glue/p11-kit/manual/pkcs11-conf.html

Example
https://p11-glue.github.io/p11-glue/p11-kit/manual/config-example.html

MilitaryCAC
https://militarycac.com/linux.htm

sniff & decrypt

Transport Layer Security (TLS)
https://wiki.wireshark.org/TLS

Why wireshark cannot display TLS/SSL
https://osqa-ask.wireshark.org/questions/34075/why-wireshark-cannot-display-tlsssl

TCP protocol instead of SSL/TLS in Wireshark
https://stackoverflow.com/questions/28789179/tcp-protocol-instead-of-ssl-tls-in-wireshark/49423430

ssl2

trust store tuning

CAcert
http://www.cacert.org/

Adding CACert root certificates to your Slackware
https://alien.slackbook.org/blog/adding-cacert-root-certificates-to-your-slackware/

ssl tuning - online checkers

https://www.ssllabs.com/ssltest/analyze.html

https://cryptcheck.fr

firefox: from green to gray

Improved Security and Privacy Indicators in Firefox 70
https://blog.mozilla.org/security/2019/10/15/improved-security-and-privacy-indicators-in-firefox-70/

ssl

books

Implementing SSL
https://commandlinefanatic.com/cgi-bin/showpage.cgi?page=implementingssl

ssl engines

https://www.wolfssl.com/

pkix

Public key infrastructure
https://en.wikipedia.org/wiki/Public_key_infrastructure

X.509
https://en.wikipedia.org/wiki/X.509

pkix - lencr

Standing on Our Own Two Feet [Updated]
https://letsencrypt.org/2020/11/06/own-two-feet.html

Extending Android Device Compatibility for Let's Encrypt Certificates
https://letsencrypt.org/2020/12/21/extending-android-compatibility.html

lab/ctf

Question: Can you break TLS? [200PTS]
https://github.com/zack-lau/WriteUps/blob/master/HITB-Facebook-CTF-2016/capture_Mexico-tls/README.md

no ssl required

Securing access to Wikimedia sites with HTTPS
https://diff.wikimedia.org/2015/06/12/securing-wikimedia-sites-with-https/

mitm-happy

HTTP Strict Transport Security
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

HTTP Strict Transport Security (HSTS) and NGINX
https://www.nginx.com/blog/http-strict-transport-security-hsts-and-nginx/

HSTS Preloading using Nginx, Letsencrypt and Capistrano.
https://dev.to/sonica/hsts-preloading-using-nginx-letsencrypt-and-capistrano-18l7

Setting up HSTS in nginx
https://scotthelme.co.uk/setting-up-hsts-in-nginx/

videos

ssl is dead

USENIX Enigma 2016 - PKI at Scale Using Short-lived Certificates
https://www.youtube.com/watch?v=7YPIsbz8Pig

USENIX Enigma 2016 - Several Horror Stories about the Encrypted Web
https://www.youtube.com/watch?v=bi3SA6jgIZ8

USENIX Enigma 2016 - Trust Beyond the First Hop–What Really Happens to Data Sent to HTTPS Websites
https://www.youtube.com/watch?v=Ef7W-SjueS4 ==> “warning fatigue”

industrialization

Yahoo SSL deployments
https://www.netmeister.org/blog/razors-edge/oreilly-security-2017-razors-edge.mp4