TLS INTERCEPTION CONSIDERED HARMFUL

ABOUT ME

Hanno Böck, https://hboeck.de/

Freelance journalist (often Golem.de)
Fuzzing free software (Core Infrastructure Initiative)

TLS VULNERABILITIES

BEAST, CRIME, Lucky13, FREAK, SKIP, POODLE, Heartbleed, Logjam, MACE, ...

BEAST

Exploits known issue in CBC mode of TLS 1.0 / SSL 3.0.
Fix: Use TLS 1.1/1.2.
Workaround: 1/n-1 record splitting.

CRIME

Compression leaks information about encrypted data.
Solution: Disable compression.

LUCKY THIRTEEN

TLS does MAC-then-Pad-then-Encrypt.
Timing sidechannel: separating MAC errors from padding errors.
Workaround: Timing safe implementation (difficult).
Solution: TLS 1.2 with Authenticated Encryption (only AES-GCM).

POODLE

SSLv3 allows arbitrary content in padding.
Solution for SSLv3: Don't use it.
Solution for TLS: Check padding (must be zeros).

FORWARD SECRECY

Create a temporary key for each connection.
Protects from later key leakage.
Hardly any reason not to use FS.

LESSONS LEARNED

Security bugs in the protocol.
Only TLS 1.2 using AES-GCM with Forward Secrecy considered safe.
TLS 1.0 with mitigations required for legacy support, complicated.

CERTIFICATE AUTHORITIES

Hundreds of CAs and sub-CAs.
Each can issue certs for all domains.
System is only as secure as the worst CA.

CERTIFICATE AUTHORITIES

Misissuance of certificate happens often: Comodo, Türktrust, CNNIC, IndiaCCA, Diginotar, ANSSI, ...

SOLUTIONS

Many proposals (Sovereign keys, TACK, Convergence, DANE, ...).
Most of them never got deployed widely.

HTTP PUBLIC KEY PINNING (HPKP)

First widely deployed mitigation for CA failures (Chrome and Firefox).
Browsers also contain list of pre-pinned hosts.

CERTIFICATE TRANSPARENCY

Public log of all certificates.
Promising, but only partly deployed yet.
Chrome has preliminary support.

CONCLUSION

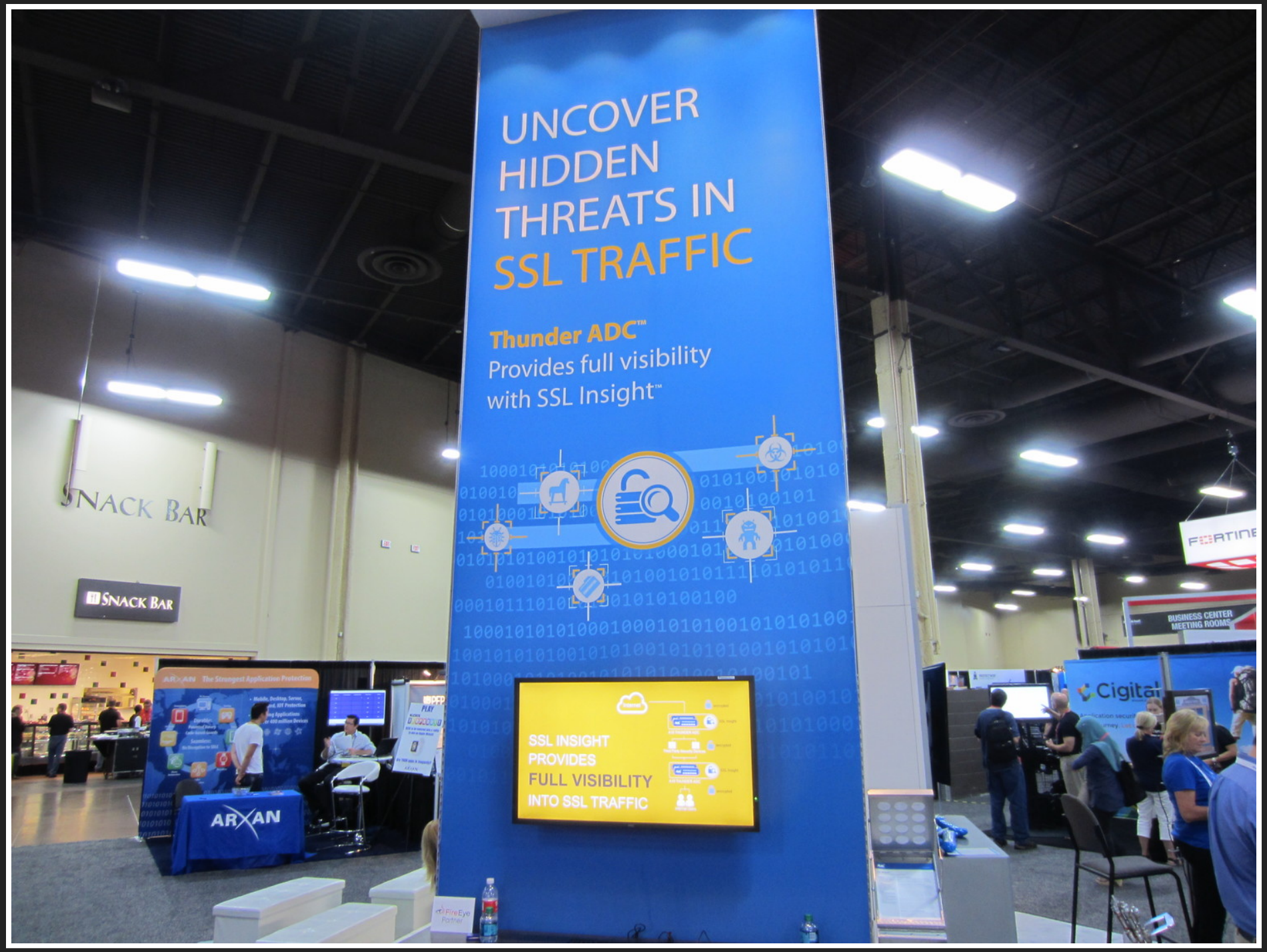
Mitigations for Certificate Authority problems are finally coming.
Proper certificate verification requires knowledge about current developments.

HTTPS USE IS GROWING

... and that's a good thing.
Certificates no longer expensive (StartSSL, Wosign, Let's encrypt).
HTTPS guarantees secrecy and integrity (often forgotten).


BLUE COAT
SSL/TLS TRAFFIC IS PERVASIVE & INTRODUCES RISK
SSL Encrypted Traffic in Enterprises
20% YoY Growth Rate
Target cyber breach hits 40 million payment cards at holiday peak
Ex-Sony Chief Amy Pascal Acknowledges She Was Fired
Sony Hack: 'Critical' Systems Won't Be Back Until February
25% - 35% of Enterprise Traffic is SSL/TLS encrypted …and growing*
Advanced Persistent Threats (APTs) increasingly use SSL as a transport
Breaches occur more frequently – damaging corporate reputation and integrity
Data Privacy concerns impede deployment
*Sources: NSS Labs, Gartner
BLUE COAT


INSPECT AND PROTECT
SSL
EVERY
WHERE
Raytheon
websense
ENTER A NEW ERA OF CYBER
intel Security
Bit9
ARM YOUR
EnCASE ENDPOINT SECURITY
EnCase
DELL
ENDPOINT SECURITY
RSA
600
ibOSS
CYBERSECURITY
f5


UNCOVER HIDDEN THREATS IN SSL TRAFFIC
Thunder ADC™
Provides full visibility with SSL Insight™
SSL INSIGHT PROVIDES FULL VISIBILITY INTO SSL TRAFFIC
SNACK BAR
SNACK BAR
ARXAN
Cigital
BUSINESS CENTER MEETING ROOMS

WEB TRAFFIC INTERCEPTION

Products want to manipulate web traffic. "Enterprise" security products, Antiviruses, Parental control, Adblockers, Ad injection, ...

HTTPS MAN-IN-THE-MIDDLE PROXIES

HTTPS guarantees secrecy and integrity(!).
"Solution": Let's install a certificate in the user's browser and do a Man-in-the-Middle-attack.

SUPERFISH

Analyzes images on webpages and provides matching ads.
Preinstalled on many Lenovo Laptops.

SHARED CERTIFICATE

All installations of Superfish used the same root certificate.
Problem: Private key can be extracted.


Komodia


Superfish™
Search Visually
TM


STAFFCOP


Ad-Aware
Web Companion


Qustodio


EASY-HIDE-IP.com


Kurupira
FOLLOW THE FOOTSTEPS OF THIS TRIBE

KOMODIA SAN BUG

Komodia products had another bug with Subject Alternative Name.
Allows generic TLS interception for all products using Komodia.

LAVASOFT / AD-ADWARE

"Lavasoft’s most recent release of Ad-Aware Web Companion (released on February 18th 2015) does not include this capability, but we are not yet able to confirm with certainty that the compromised component of the Komodia SSL Digestor has been removed." (Lavasoft Facebook page)

LAVASOFT / AD-ADWARE

Or in other words: We have a severe security vulnerability and we're not really sure if we fixed it.

PRIVDOG

Privdog is a startup founded by Melih Abdulhayoğlu (CEO of Comodo).
It replaces "dangerous" ads with its own ads.

NO VERIFICATION OF CERTIFICATES

Privdog does not use a shared cert (we'll get back to that later).
But it did not verify certificates at all.
By the way: It also sent home all URLs visited in clear text.

ANTIVIRUS APPLICATIONS INTERCEPTING TLS

Analysis of Avira, Kaspersky, ESET.
None as bad as Superfish/Privdog, but all of them lowered TLS security in one way or another.

KASPERSKY / FREAK

FREAK vulnerability: OpenSSL bug allowed downgrade to export ciphers with 512 bit.
Shortly after FREAK Kaspersky user warned about it in support forum.
1.5 months later it was still not fixed.

BREAKING HPKP

Shouldn't Key Pinning prevent TLS interception from happening?
Browsers compromised: Didn't want to break all TLS interception products.
Manually installed certs override key pinning.
No TLS interception software I tested checked key pinning header.

RESPONSIBILITY SHIFT

If products intercept TLS they are responsible for certificate validation and TLS implementation quality.
Are they qualified?

ADGUARD

Regenerates cert, but always with same key.
Chooses one out of 10 keys depending on CPU.

NETFILTER SDK

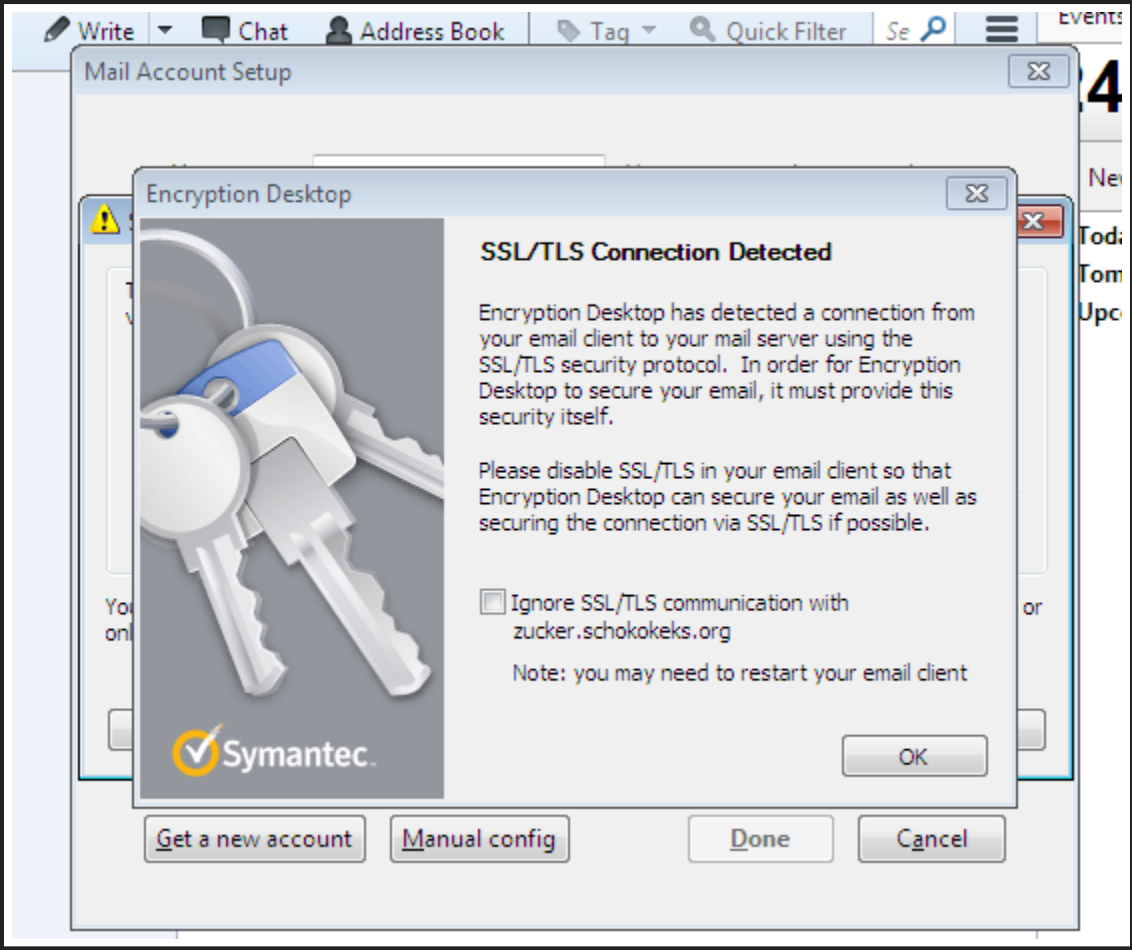
Adguard relied on Netfilter SDK (file ProtocolFilters.dll).
Shared key can be trivially extracted.

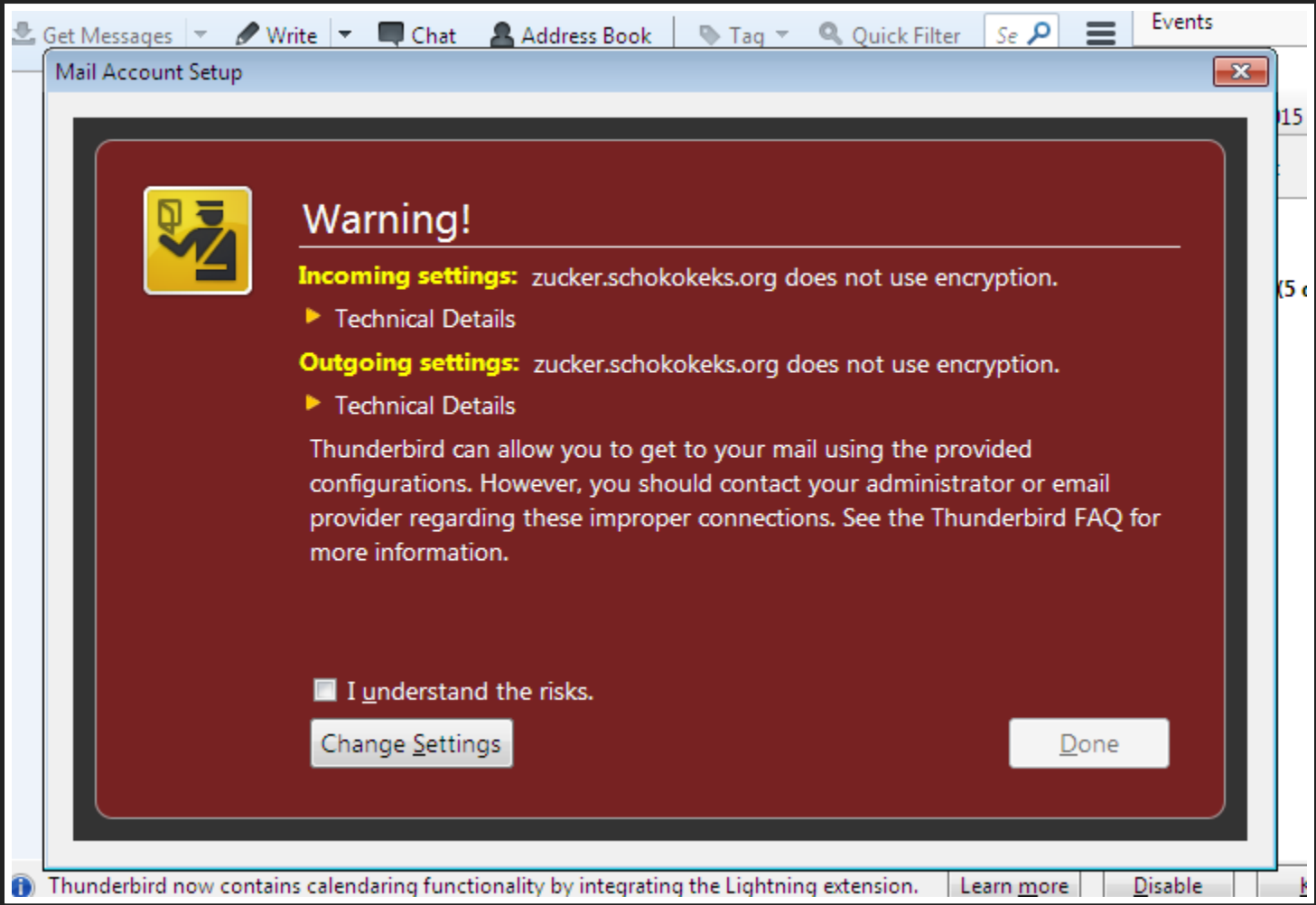
MEET PRIVDOG AGAIN

PrivDog also uses shared key.
It was completely broken in two different ways.

PROTOCOLFILTERS.DLL

Coupoon, CashReminder, SavingsDownloader, Scorpion Saver, SavingsbullFilter, BRApp, NCupons, Nurjax, Couponarific, delshark, rrsavings, triosir, screentk, ...


Write
Chat
Address Book
Tag
Quick Filter
Mail Account Setup
Encryption Desktop
SSL/TLS Connection Detected
Encryption Desktop has detected a connection from your email client to your mail server using the SSL/TLS security protocol. In order for Encryption Desktop to secure your email, it must provide this security itself.
Please disable SSL/TLS in your email client so that Encryption Desktop can secure your email as well as securing the connection via SSL/TLS if possible.
Ignore SSL/TLS communication with zucker.schokokeks.org
Note: you may need to restart your email client
OK
Symantec.
Get a new account
Manual config
Done
Cancel


Get Messages
Write
Chat
Address Book
Tag
Quick Filter
Events
Mail Account Setup
Warning!
Incoming settings: zucker.schokokeks.org does not use encryption.
Technical Details
Outgoing settings: zucker.schokokeks.org does not use encryption.
Technical Details
Thunderbird can allow you to get to your mail using the provided configurations. However, you should contact your administrator or email provider regarding these improper connections. See the Thunderbird FAQ for more information.
I understand the risks.
Change Settings
Done
Thunderbird now contains calendaring functionality by integrating the Lightning extension.
Learn more
Disable

SYMANTEC DESKTOP EMAIL ENCRYPTION

The software formerly known as PGP.
Only does TLS 1.0 without Forward Secrecy.

ENTERPRISE APPLIANCES

Open question: How bad are they?
Contact me if you have access.

"ENTERPRISE" TLS

F5 "we don't accept handshakes between 256 and 512 bytes" bug
POODLE TLS (F5, A10, Cisco, Check Point, Juniper, IBM)
MACE: Missing MAC and Finished message check (Cisco, Fortinet, F5, Juniper)

ALTERNATIVES

For many of the products that use TLS interception the question is whether they should exist at all.
If you want to modify traffic with user's consent do it after the encryption (e. g. browser extension).

TAKEAWAYS

"Potentially unwanted applications" are a severe securiy threat.
It should be considered malpractice.

TAKEAWAYS

TLS interception is dangerous.
Nobody gets it right.
Even security products fail.
Don't mess with our TLS connections.

https://github.com/hannob/superfishy
Questions? Discussion?