

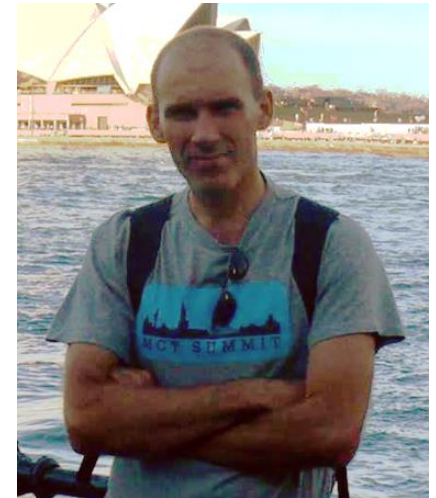
https / SSL / TLS - niby bezpieczne, ale czy na pewno nikt nas nie podsłuchuje, a może nawet zmienia informacje?

Mariusz Ferdyn

Materiały: <http://www.subscribepage.com/mf>

In the IT world for over 20 years

- 1992 - associate with Bajtek / Commodore & Amiga magazine
- 1995 - hardware selling
- 2000 - work for corporations, banks, IT companies ...
- 2007 - Microsoft certified Trainer
- 2016 - MVP



<https://www.facebook.com/mariusz.ferdyn>

<https://mva.microsoft.com/search/SearchResults.aspx?q=mariusz%20ferdyn>

http://virtualstudy.pro/en/publikacje?filter_search=Ferdyn%20Mariusz

<https://channel9.msdn.com/Series/Nowosci-z-konferencji-Microsoft-Ignite-2016-Kontenery-Device-Guard-Shielded-VMs-Nested-Virtualizatio>

Czego nie

POODLE

Aktualizacje

Wyłączanie

 IIS Crypto

 IIS Crypto 2.0

 Schannel

 Cipher Suites

 Templates

 Site Scanner

 About

Cipher Suites

Enable, disable or reorder various cipher suites that are negotiated for the TLS handshake. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used.

☒	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	
☒	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	
☒	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	
☒	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	
☒	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	
☒	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	
☒	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	
☒	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	
☒	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	
☒	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	
☒	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	
☒	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	
☒	TLS_RSA_WITH_AES_256_GCM_SHA384	
☒	TLS_RSA_WITH_AES_128_GCM_SHA256	
☒	TLS_RSA_WITH_AES_256_CBC_SHA256	
☒	TLS_RSA_WITH_AES_128_CBC_SHA256	
☒	TLS_RSA_WITH_AES_256_CBC_SHA	
☒	TLS_RSA_WITH_AES_128_CBC_SHA	
☒	TLS_RSA_WITH_3DES_EDE_CBC_SHA	
☐	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	
☐	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	
☐	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	
☐	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	
☐	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	
☐	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	

Best Practices

Apply



Podśluchiwanie ruchu (na czystym systemie)
xperf, logman

Fiddler – a co to takiego

Zły administrator i to domeny AD

Zabezpieczamy się

Podsluchiwanie ruchu - xperf, logman - Fiddler

DEMO

ITechDays

Zły administrator i to domeny AD

DEMO

ITechDays

- Antywirus / Internet Security
- EMET
- https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning

Zabezpieczamy się

DEMO

ITechDays

Dziękuję za uwagę

<https://www.facebook.com/mariusz.ferdyn>

Materiały: <http://www.subscribepage.com/mf>