Padrões e protocolos seguros: o que devemos usar em nossas redes hoje e amanhã

17/07/2024

PROTOCOLOS SEGUROS

Robson Albuquerque – robson@redes.unb.br

1

Robson Albuquerque

- Mestre e Doutor em Engenharia Elétrica pela Universidade de Brasília (UnB)
- Mestre e Doutor em Sistemas informáticos pela Universidad Complutense de Madrid (UCM)
- Pós-Doutor pela UnB em Segurança Cibernética
- Pesquisador na UnB e na UCM
- Mais de 25 anos de experiência profissional em diversas áreas de atuação
- Inúmeras publicações técnicas e científicas

2

DISCLAIMER

- O conteúdo aqui apresentado representa minha visão sobre novas tecnologias, desafios e perspectivas para segurança da informação e cibernética. Não representa necessariamente a visão dos meus empregadores e nem da Universidade da qual sou pesquisador;
- Imagens utilizadas nesta apresentação são de propriedade e crédito dos respectivos criadores e fontes;

AGENDA

PROTOCOLOS E SUAS CARACTERÍSTICAS

SEGURANÇA CIBERNÉTICA OU SEGURANÇA DA INFORMAÇÃO?

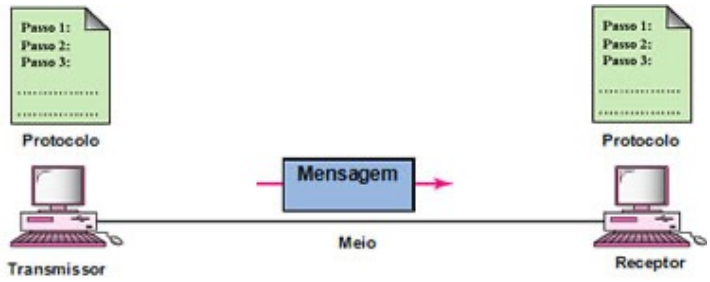
PROTOCOLOS SEGUROS

PROTOCOLOS E SUAS CARACTERÍSTICAS

COMUNICAR-SE É NATURAL PARA O SER HUMANO

NA INTERNET

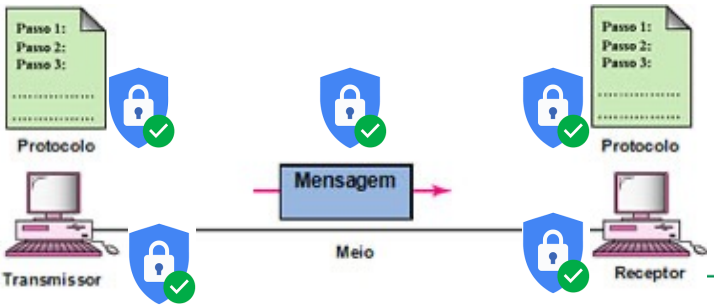
REGRAS DE COMUNICAÇÃO:



PROTOCOLOS E SUAS CARACTERÍSTICAS

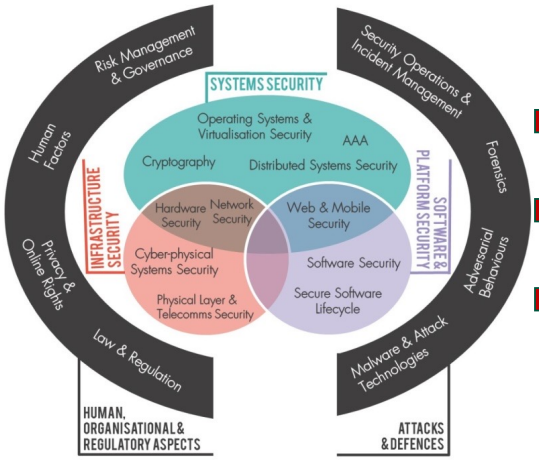
Pré-requitos básicos em qualquer processo de comunicação:

- **Devem permitir que a comunicação aconteça de maneira precisa;**
- **Devem ser seguras;**
- **Devem ser livres de erros;**



latitude
Laboratório de tecnologias da tomada de decisão

SEGURANÇA CIBERNÉTICA OU SEGURANÇA DA INFORMAÇÃO



Disponibilidade

Confidencialidade

Integridade

nic.br

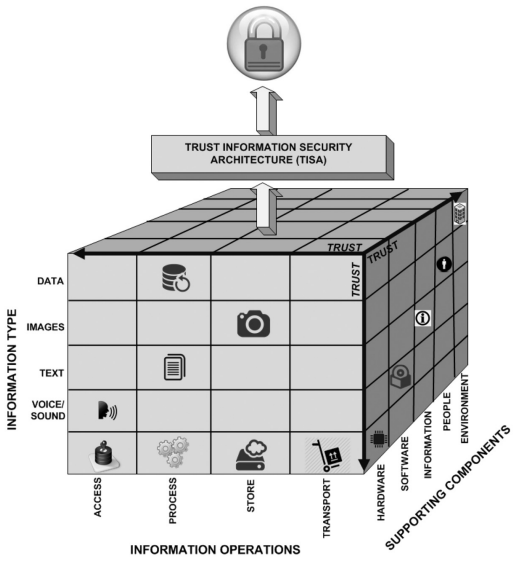
Cybok 1.1

faculdade de tecnologia UnB

7

latitude
Laboratório de tecnologias da tomada de decisão

SEGURANÇA CIBERNÉTICA OU SEGURANÇA DA INFORMAÇÃO



https://www.mdpi.com/1424-8220/14/12/22754

nic.br

faculdade de tecnologia UnB

8

PROTOCOLOS SEGUROS

NÓS SIMPLESMENTE “CONFIAMOS” NOS PROTOCOLOS…

A MAIORIA DOS USUÁRIOS NÃO CONSEGUE VERIFICAR POR SI PRÓPRIO QUESTÕES DE SEGURANÇA…

AS IMPLEMENTAÇÕES DOS PROTOCOLOS SÃO ABERTAS (OU DEVERIAM)…

VEJAMOS ALGUNS PONTOS DE REFLEXÃO…

PROTOCOLOS SEGUROS

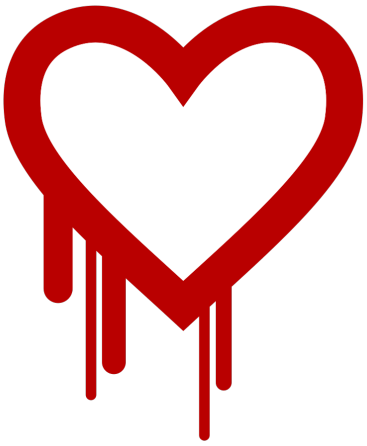
O QUE ACHA DESSE CÓDIGO?

```
unsigned char *buffer, *bp;
int r;
buffer = XXXXXXX_malloc(1 + 2 + payload + padding);
bp = buffer;
*bp++ = XXX1_HB_RESPONSE;
s2n(payload, bp);
memcpy(bp, pl, payload);
```

PROTOCOLOS SEGUROS

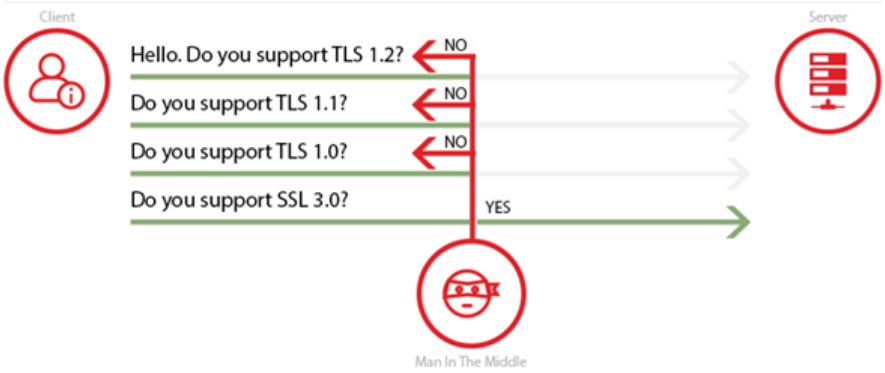
O CÓDIGO ANTERIOR FOI...

HEARTBLEED...



PROTOCOLOS SEGUROS

E esse handshake?



https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/

latitude
Laboratório de tecnologias da tomada de decisão

PROTOCOLOS SEGUROS

Padding Oracle On Downgraded Legacy Encryption

nic.br

faculdade de tecnologia UnB

latitude
Laboratório de tecnologias da tomada de decisão

PROTOCOLOS SEGUROS

O que acha disso? Confiaria nesse site?

 # TLS 1.1 (suites in server-preferred order)

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 4096 bits FS **WEAK**
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 4096 bits FS **WEAK**
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 4096 bits FS **WEAK**
- TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**
- TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**

Cipher Suites

 # TLS 1.2 (suites in server-preferred order)

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 4096 bits FS
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 4096 bits FS
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 4096 bits FS **WEAK**
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 4096 bits FS **WEAK**
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 4096 bits FS **WEAK**
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 4096 bits FS **WEAK**
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 4096 bits FS **WEAK**
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**
- TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**
- TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**

nic.br

faculdade de tecnologia UnB

PROTOCOLOS SEGUROS

SSL Report: enisa.eu

Assessed on: Tue, 25 Jun 2024 07:59:16 UTC | **HIDDEN** | Clear cache

Scan Another >>

	Server	Test time	Grade
1	2a02:5b40:4:224:0:0:0:d urlfw1.level27.eu Ready	Tue, 25 Jun 2024 07:54:22 UTC **Duration:** 146.778 sec	B
2	185.3.216.14 urlfw1.level27.eu Ready	Tue, 25 Jun 2024 07:56:49 UTC **Duration:** 147.183 sec	B

PROTOCOLOS SEGUROS

TEM VÁRIOS OUTROS EXEMPLOS POR AÍ…

LibSSH Authentication Bypass Vulnerability (CVE-2023-2283)

July 2, 2024 Advisory: regreSSHion RCE Vulnerability in OpenSSH Server [CVE-2024-6387]

No OPENSSL (https://www.openssl.org/news/vulnerabilities.html)

ENTÃO…. “O QUE DEVEMOS USAR EM NOSSAS REDES HOJE E AMANHÃ”

SE É PARA CONSIDERAR SEGURANÇA…É BASTANTE DIFÍCIL DIZER…

latitude
Laboratório de tecnologias da tomada de decisão

AGRADEÇO A OPORTUNIDADE

Prof. Robson de Oliveira Albuquerque, Dr
Laboratório LATITUDE
Departamento de Engenharia Elétrica – EnE
Faculdade de Tecnologia – FT
Universidade de Brasília – UnB
email: robson@redes.unb.br

nic.br

faculdade de tecnologia UnB