Padrões e Protocolos Seguros (*Live* nic.br)

TLS

Prof. André Grégio

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

Introdução ao TLS

O que é TLS?

- TLS (*Transport Layer Security*) é um **protocolo de segurança** que proporciona **privacidade** e **integridade** de dados na comunicação em rede!

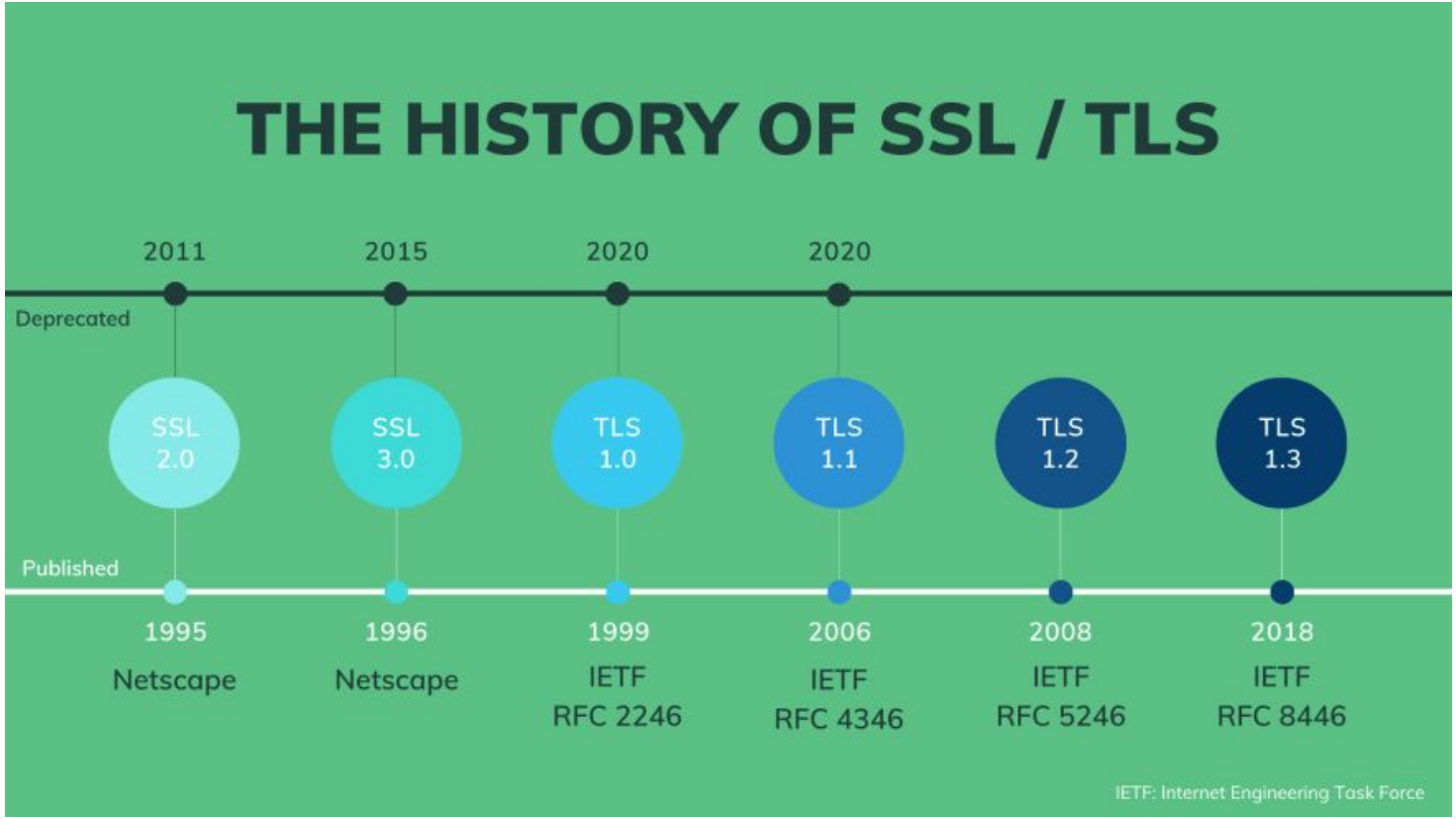
Introdução ao TLS

O que é TLS?

- TLS (*Transport Layer Security*) é um **protocolo de segurança** que proporciona **privacidade** e **integridade** de dados na comunicação em rede!
- Sucedeu o SSL (*Secure Sockets Layer*), protocolo criptográfico cujas versões 2.0 e 3.0 vieram à público:
  - Embora o SSL esteja **obsoleto**, alguns *sites Web* ainda o utilizam

(

SSL e TLS: Queda e Ascensão



Fonte: https://dev.to/techschoolguru/a-complete-overview-of-ssl-tls-and-its-cryptographic-system-36pd

Evolução do TLS

- TLS 1.0: Lançado em 1999, baseado no SSL 3.0.
- TLS 1.1: Introduzido em 2006, melhorias de segurança (ex., proteção contra ataques de CBC).
- TLS 1.2: Lançado em 2008, segurança aprimorada, algoritmos de criptografia mais fortes (mais POPULAR).
- TLS 1.3: Lançado em 2018, maior eficiência e segurança (mais RECENTE), remoção de cifras consideradas fracas.

Fonte: https://sslinsights.com/tls-1-2-vs-tls-1-3/

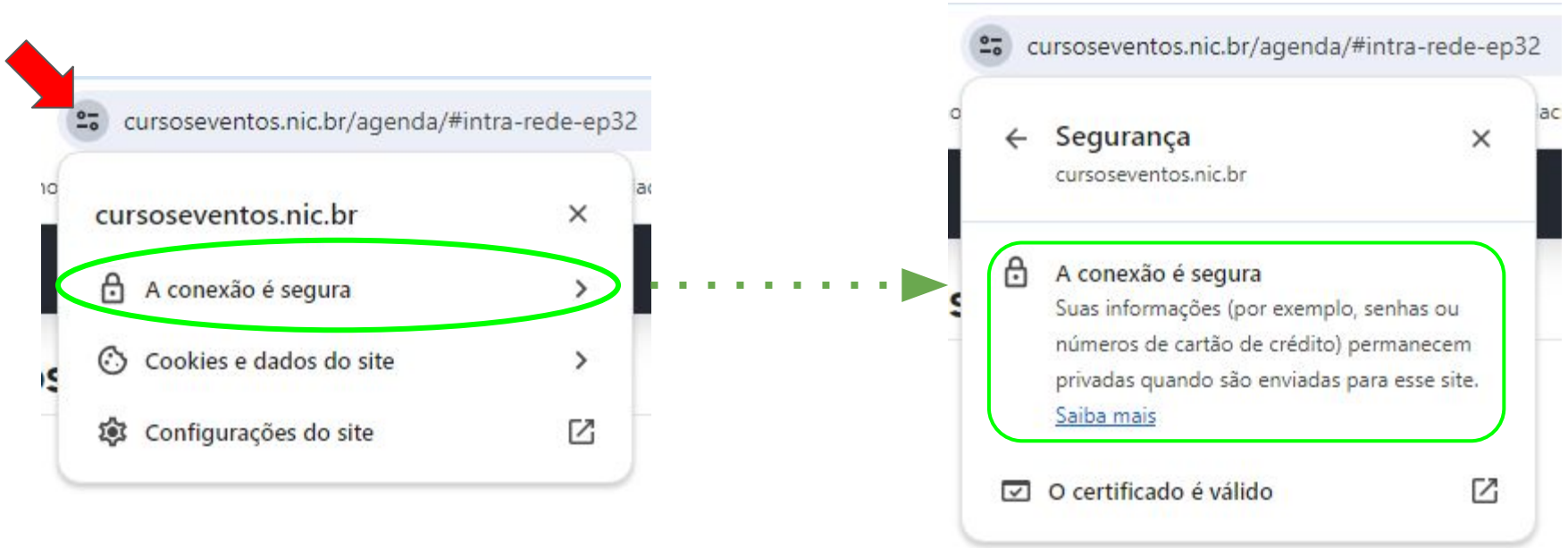
)

Introdução ao TLS

O que é TLS?

- TLS (*Transport Layer Security*) é um **protocolo de segurança** que proporciona **privacidade** e **integridade** de dados na comunicação em rede!
- Sucedeu o SSL (*Secure Sockets Layer*), protocolo criptográfico cujas versões 2.0 e 3.0 vieram à público:
  - Embora o SSL esteja obsoleto, alguns *sites Web* ainda o utilizam
- TLS é uma evolução do SSL e é o **“cadeadinho”** dos *sites* na Internet…

TLS, o cadeado das comunicações na Internet

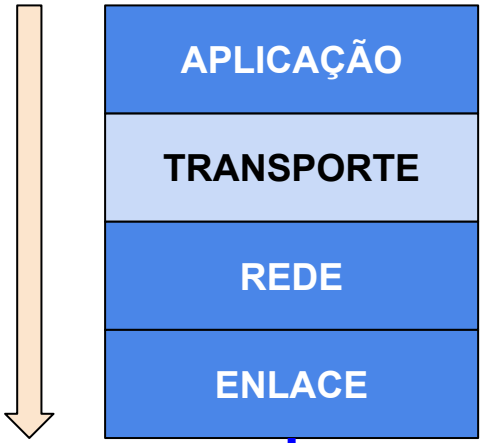


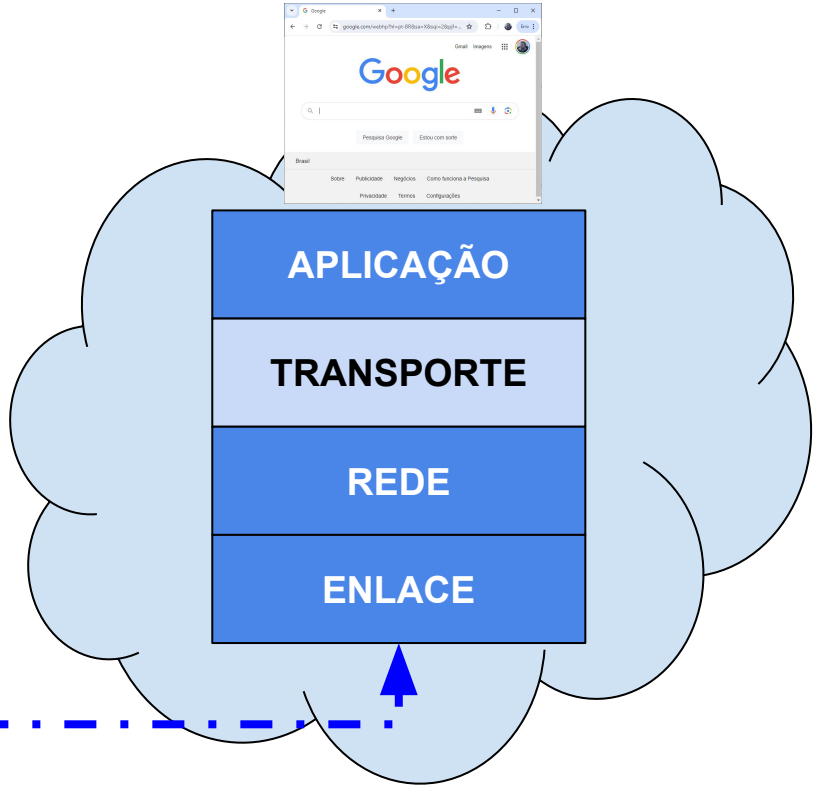
Por que o TLS é importante?

- Protege dados contra interceptação e manipulação
  - Preserva **confidencialidade** e **integridade** **(e disponibilidade…)**

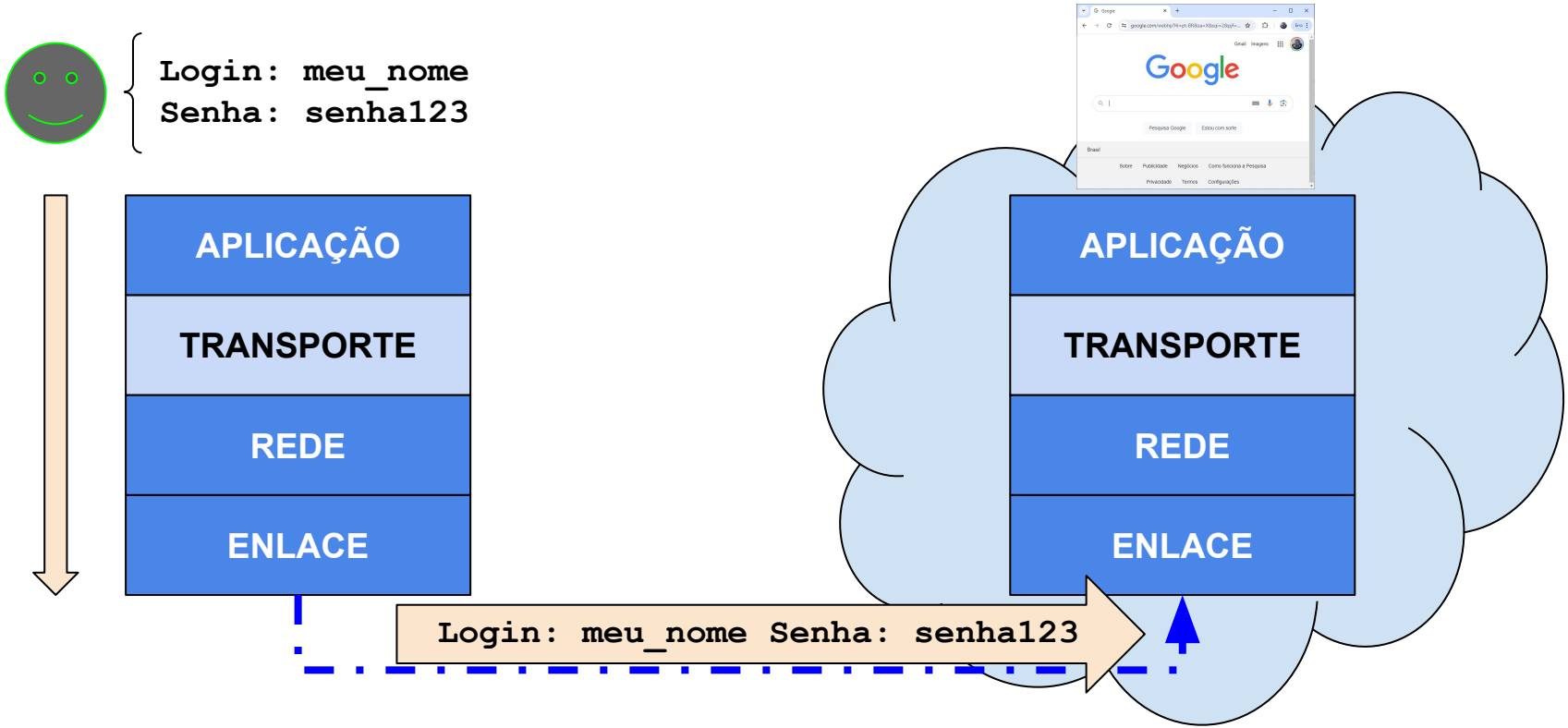
Sem TLS

```
Login: meu_nome
Senha: senha123
```

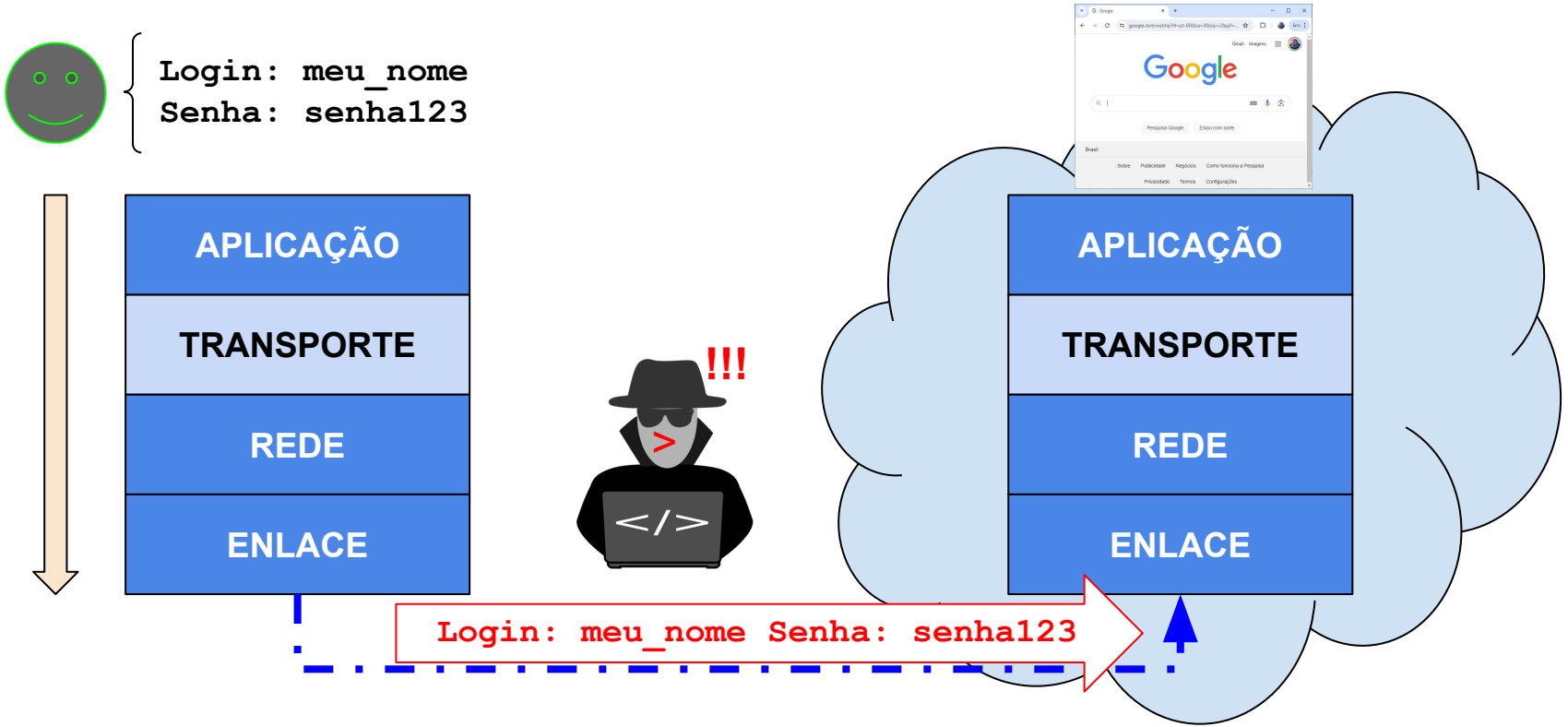




Sem TLS


Login: meu_nome
Senha: senha123
APLICAÇÃO
TRANSPORTE
REDE
ENLACE
Google
APLICAÇÃO
TRANSPORTE
REDE
ENLACE
Login: meu_nome Senha: senha123

Sem TLS

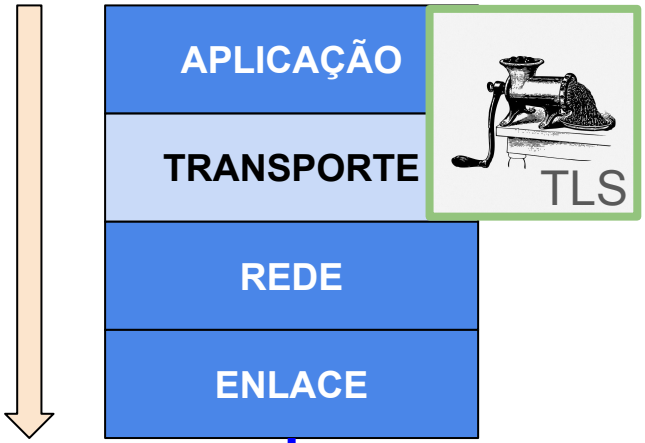

Login: meu_nome
Senha: senha123
APLICAÇÃO
TRANSPORTE
REDE
ENLACE
!!!
Google
APLICAÇÃO
TRANSPORTE
REDE
ENLACE
Login: meu_nome Senha: senha123

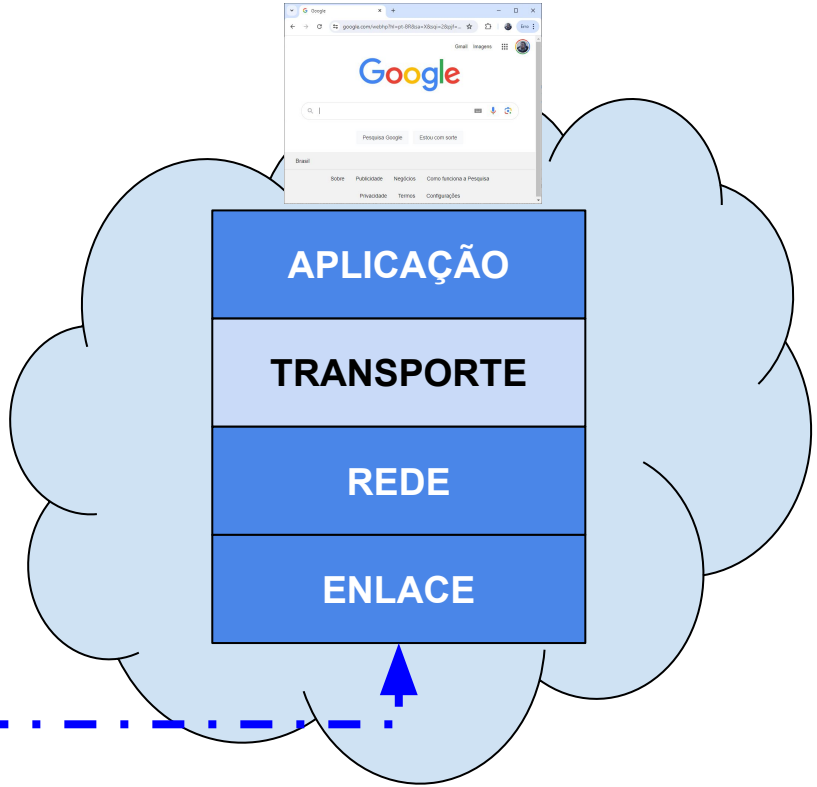
Por que o TLS é importante?

- Protege dados contra interceptação e manipulação
  - Preserva **confidencialidade** e **integridade** **(e disponibilidade…)**
- Garante que a comunicação seja **privada**
  - Preserva a **confidencialidade** via criptografia dos dados em tráfego

Com TLS

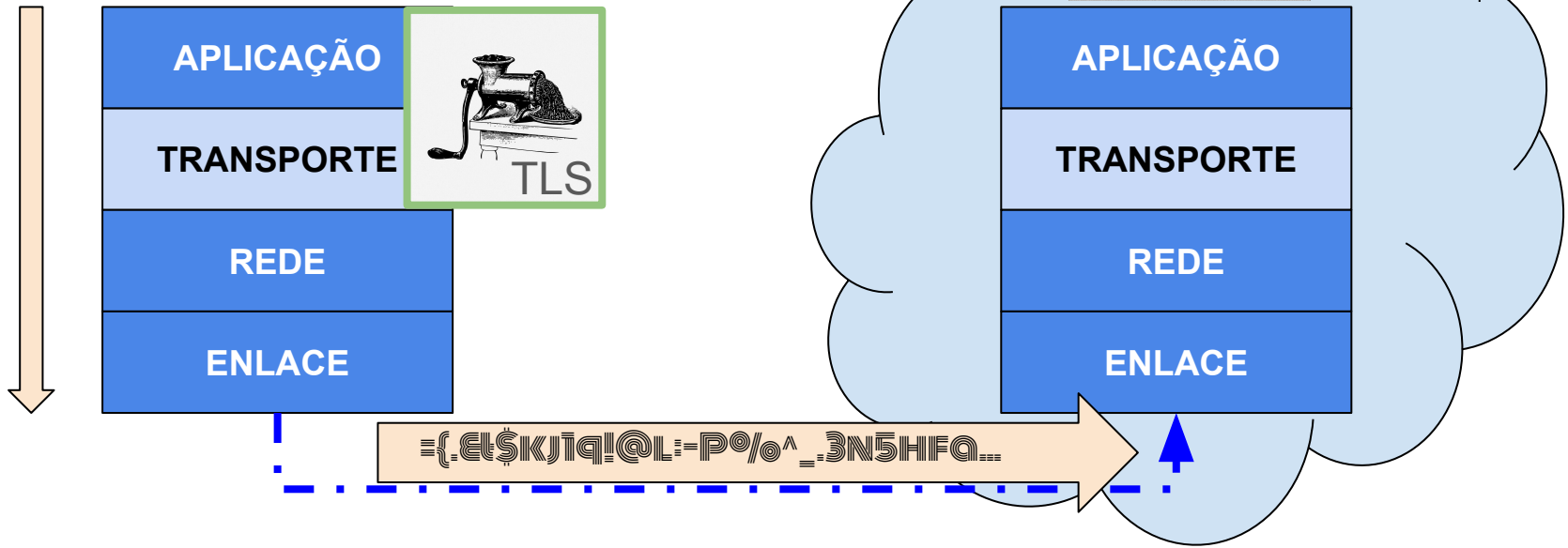
```
Login: meu_nome
Senha: senha123
```



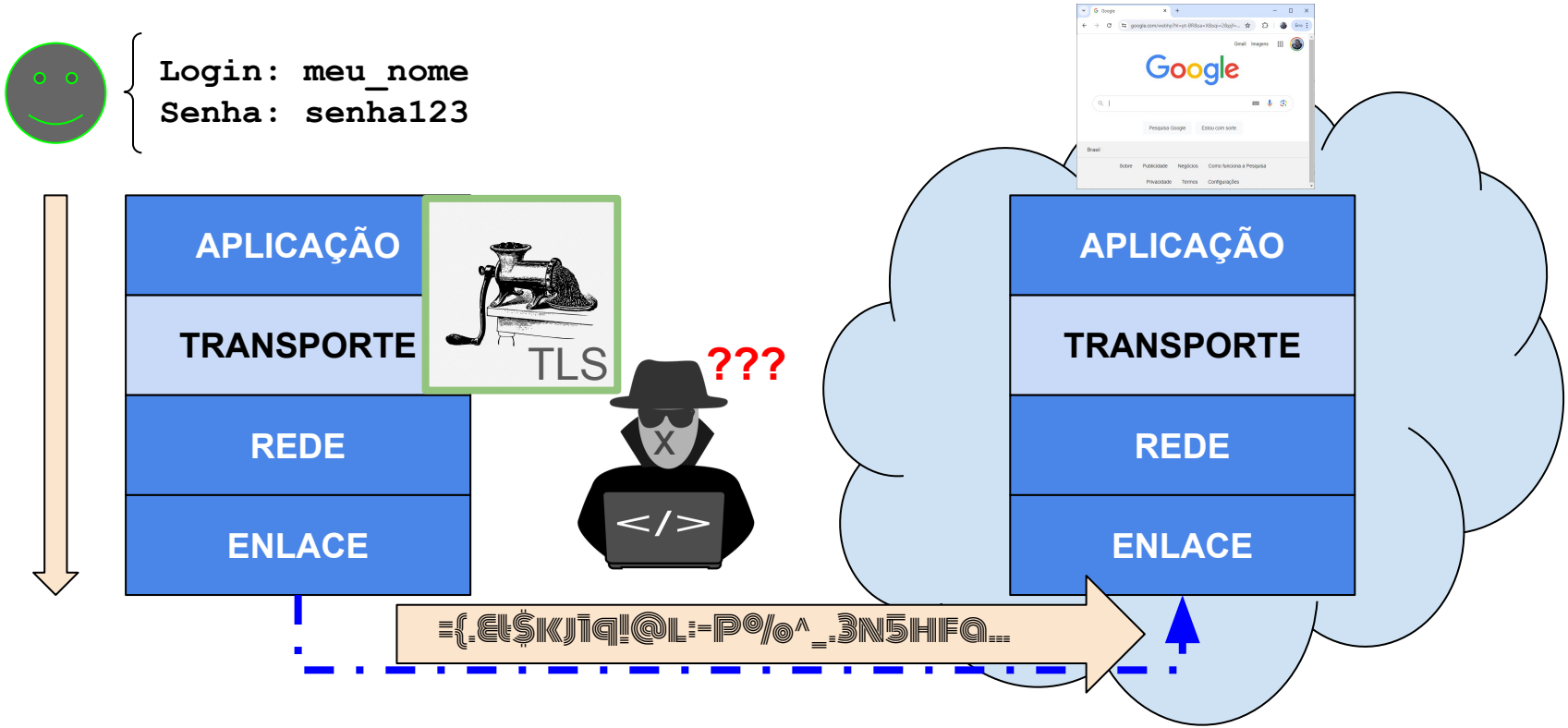


Com TLS

```
Login: meu_nome
Senha: senha123
```



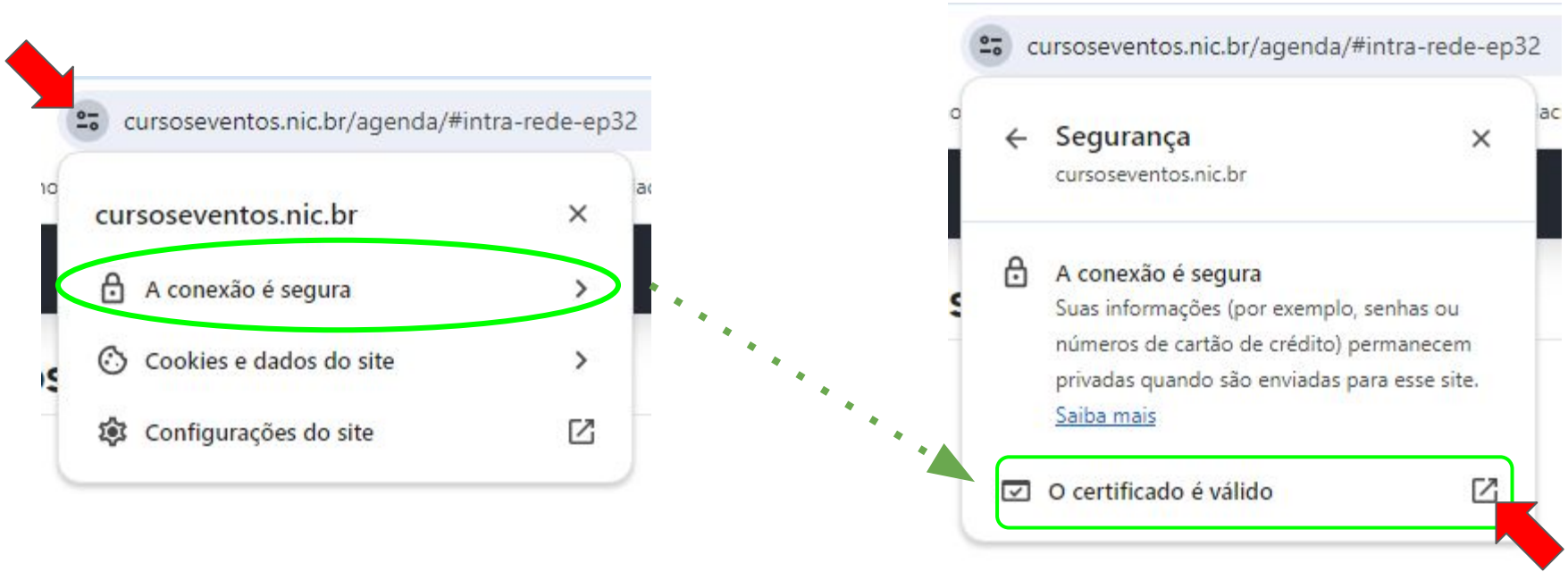
Com TLS


Login: meu_nome
Senha: senha123
APLICAÇÃO
TRANSPORTE
REDE
ENLACE
TLS
???
Google
APLICAÇÃO
TRANSPORTE
REDE
ENLACE

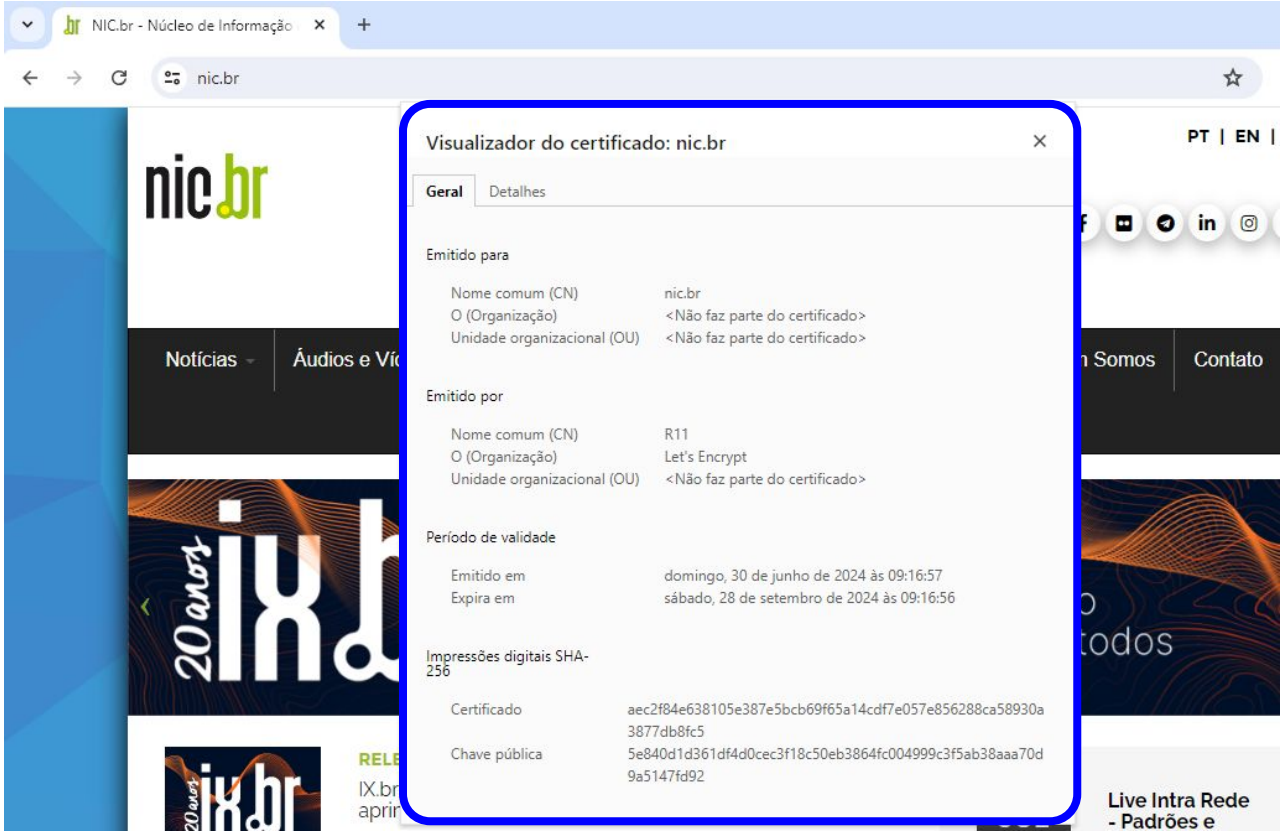
Por que o TLS é importante?

- Protege dados contra interceptação e manipulação
  - Preserva **confidencialidade** e **integridade (e disponibilidade...)**
- Garante que a comunicação seja **privada**
  - Preserva a **confidencialidade** via criptografia dos dados em tráfego
- Pode verificar a identidade das partes envolvidas
  - Efetua a **autenticação** do domínio visitado

Verificação de identidade com TLS



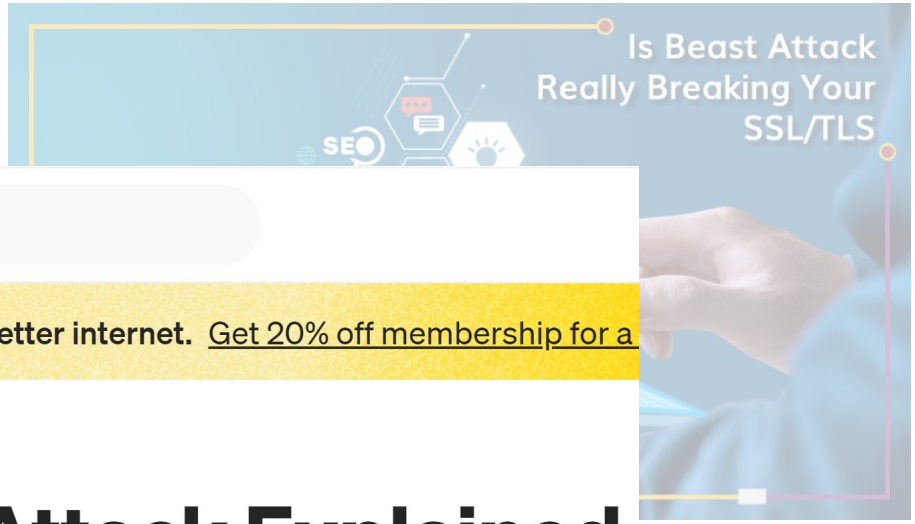
Verificação de identidade com TLS



TLS protege, mas também pode ser atacado…

https://www.briskinfosec.com/blogs/blogsdetail/Is-Beast-Attack-Really-Breaking-Your-SSL-TLS

TLS protege, mas também pode ser atacado…



Medium

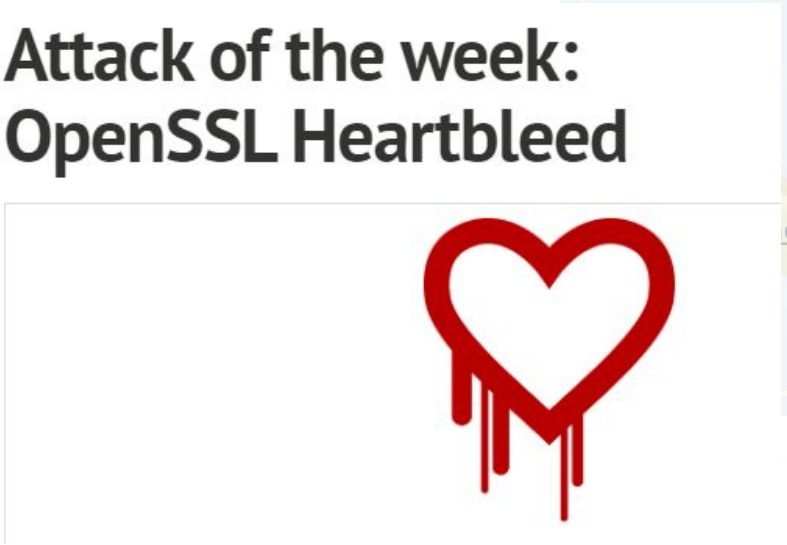
Search

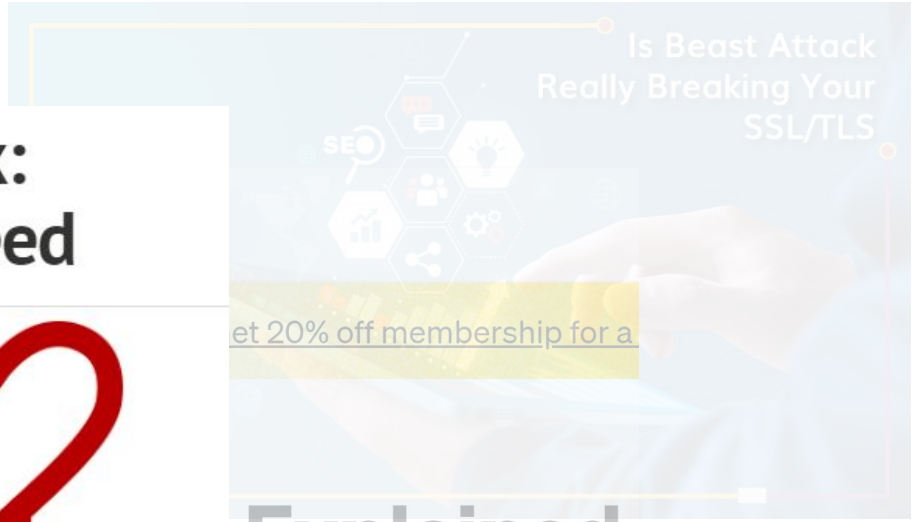
Be part of a better internet. Get 20% off membership for a

POODLE Attack Explained

https://medium.com/@c0D3M/poodle-attack-explained-ed6a1cd0667d

TLS protege, mas também pode ser atacado…





https://blog.cryptographyengineering.com/2014/04/08/attack-of-the-week-openssl-heartbleed/

TLS protege “democraticamente”

- *Malware* (**vírus de computador**) também utiliza TLS para esconder comunicação.
- Difícil detectar de tráfego malicioso criptografado.

https://www.socinvestigation.com/threat-intelligence-dridex-malware-latest-iocs-2/

https://www.kaspersky.com.br/resource-center/threats/trickbot

Ameaça cibernética ativa - Emotet e Trickbot

Emotet e Trickbot são dois malwares comumente envolvidos em atividades maliciosas na internet. Essas ameaças têm sido utilizadas conjuntamente e representam preocupação para organizações em todo o mundo.

Publicado em 05/12/2023 11h47 | Atualizado em 05/12/2023 15h28

Compartilhe:

https://www.gov.br/ctir/pt-br/assuntos/noticias/2023/ameaca-cibernetica-ativa-emotet-e-trickbot

Enfim…

- TLS é essencial para a segurança da Internet como a conhecemos…
  - Navegação segura na Web (HTTPS);
  - E-mail seguro;
  - Transferência de arquivos;
  - Aplicativos de mensagem e voz.
- Importante estar ciente dos usos maliciosos do TLS (conscientização é tudo!)
- Proteção envolve:
  - Utilização das versões mais recentes do TLS.
  - Instalação de certificados digitais de confiança.
  - Monitoração e atualização contínuas para prevenir ataques.

Obrigado!

contato

gregio@inf.ufpr.br

visite: **secret.inf.ufpr.br**