SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE II – IMPLEMENTAÇÃO DA SEGURANÇA NOS DADOS

PUC Minas
Virtual

2.2 – SERVIÇOS E TÉCNICAS DE AUTENTICAÇÃO

PUC Minas
Virtual

2.2.1 – INTRODUÇÃO À CRIPTOGRAFIA

SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

- Vamos iniciar nossa jornada em um assunto que é cheio de maravilhas e mistérios.
- É um caminho onde muitos ficaram para trás e tem muita coisa a ver **mágica**!
- Algoritmos criptográficos nos ajudam a **proteger nossos dados**, identificar nossos aliados e proteger nosso maior tesouro, desta era digital.
- Com o surgimento da internet e a **facilidade da transmissão** e **compartilhamento** dos dados de maneira precisa e extremamente **rápida**, a criptografia tornou-se uma ferramenta fundamental para permitir que apenas o **emissor** e o **receptor** tenham acesso **entendível** à informação trabalhada **.**

Um pouco de história

- A criptografia é uma técnica utilizada **há anos** que com o passar do tempo **evoluiu** a ponto de oferecer **soluções eficazes** no que diz respeito à **segurança da informação**.
- Pode parecer um assunto moderno pela evolução dos protocolos que necessitam exclusivamente da capacidade ofertada pela computação moderna, porém a criptografia é uma ciência tão antiga como a própria **"arte"** militar.
- A criptografia clássica começou a ser registrada em povos antigos, sendo muito utilizada na Idade Média e na segunda guerra. Os Hebreus faziam uso da técnica onde, na época a mais conhecida era a cifra de Cesar.

A CIFRA DE CÉSAR

FONTE: BATITUCCI, 2020.

- Aproximadamente em **50 a.C.** esta técnica foi observada, classificada como uma Cifra de Substituição, consistia em substituir cada letra da mensagem pela letra três posições depois dela.
- Como não entendiam os escritos nas transmissões das mensagens os interceptadores acreditavam que estas eram um idioma diferente do conhecido.

CRIPTOANÁLISE E AS GUERRAS

- A criptoanálise é uma das principais forças de uma nação em uma guerra e antigamente era feita por poucos engenheiros e matemáticos.
- A 1ª e a 2ª Guerras Mundiais foram marcadas por quebras sucessivas de códigos.
- Na 1ª guerra houve a quebra do código da Alemanha para o México e na 2ª a identificação da emboscada de Peral Harbour.
- **Além da máquina Enigma!**

FONTE: BATITUCCI, 2020.

FONTE: SILVA, 2020.

Qual o foco da utilização atual

- Para aplicações e ambientes cuja segurança das informações é algo relevante para o negócio, principalmente em sistemas que funcionam através da **internet**, onde o dado trafega em um **meio público** corre-se um risco maior de ele ser interceptado e fato este que pode gerar **prejuízos enormes para uma organização**.
- Com a mudança de paradigma para a utilização de serviços digitais para a maior parte da sociedade moderna, há uma forte dependência entre os sistemas de informação e as organizações.

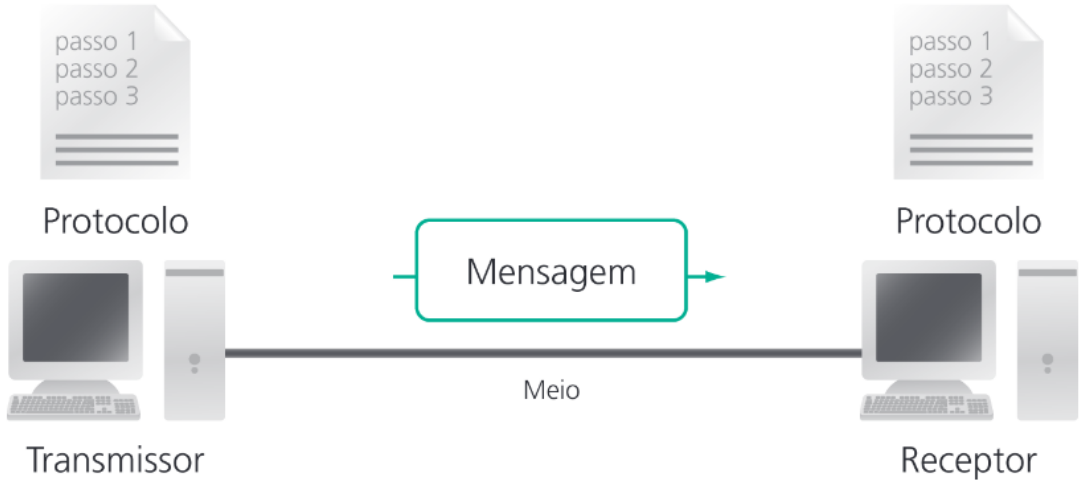
Qual o foco da utilização atual

- Os meios de proteção variam mas um deles é o uso da criptografia que não impede que determinada informação seja interceptada mas dificulta a compreensão do dado capturado.
- O termo criptografia surgiu da fusão das palavras gregas "*kryptós*" e "*gráphein*", que significam "oculto" e "escrever", respectivamente.
- Mediante vários conceitos podemos resumir que a **criptografia** é o estudo e práticas de **princípios e técnicas** para **comunicação segura** na **presença de terceiros.**

Qual o foco da utilização atual

- Uma outra abordagem que pode se feita sobre a criptografia porém de uma forma mais simplificada é que é uma ciência que visa defender protocolos contra sabotadores.
- Mas primeiro, o que é um **protocolo**?
    - **Simplificando, é uma lista de etapas que uma (ou mais pessoas) deve seguir para alcançar algo.**

COMO FUNCIONA UMA COMUNICAÇÃO ELETRÔNICA



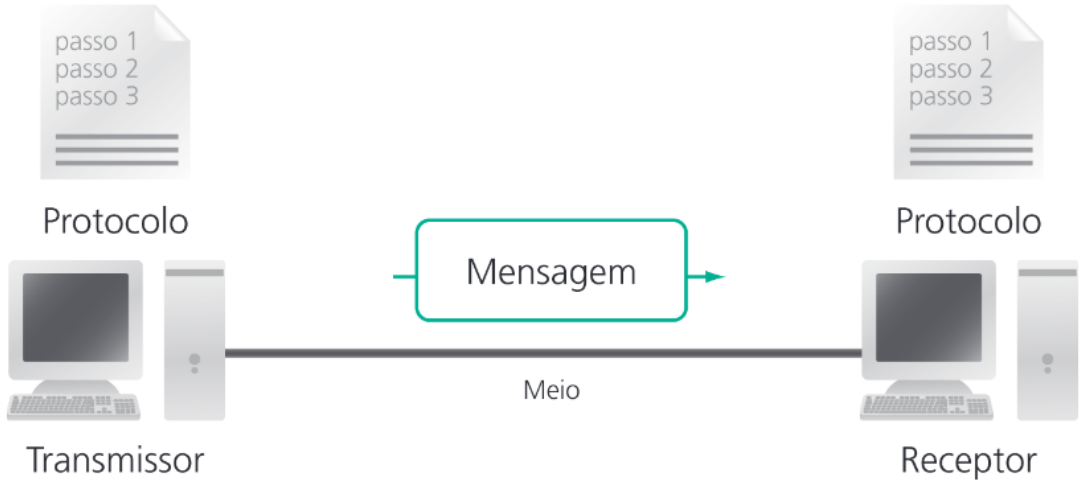
Fonte: ALENCAR, 2010.

- Um sistema básico de comunicação de dados é composto por cinco elementos:

1) Mensagem: é a informação a ser transmitida. Pode ser constituída de texto, números, figuras, áudio e vídeo – ou qualquer combinação desses elementos;

2) Transmissor: é o componente que envia a mensagem de dados. Pode ser um computador, uma estação de trabalho, um telefone, uma câmera de vídeo, entre;

COMO FUNCIONA UMA COMUNICAÇÃO ELETRÔNICA



Fonte: ALENCAR, 2010.

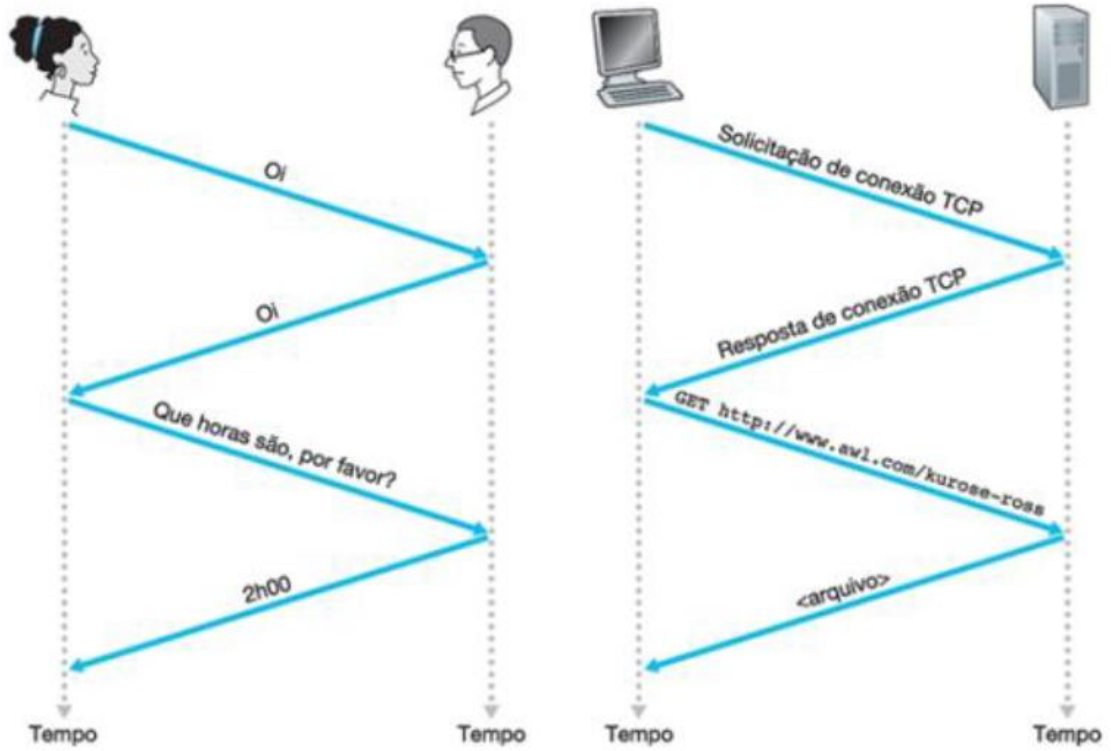
3) Receptor: é o componente que recebe a mensagem. Pode ser um computador, uma estação de trabalho, um telefone, uma câmera de vídeo, etc.;

4) Meio: é o caminho físico por onde viaja uma mensagem dirigida ao receptor e

5) Protocolo: é um conjunto de regras que governa a comunicação de dados. Ele representa um acordo entre os dispositivos que se comunicam e está diretamente relacionado à topologia lógica da rede.

COMO FUNCIONA UMA COMUNICAÇÃO ELETRÔNICA

- Um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações que podem ser realizadas na transmissão ou na recepção de uma mensagem ou outro evento.
- A importância dos protocolos se dá pela **organização das comunicações** que eles proporcionam, todos falando o mesmo idioma **(é como se fosse quase isto).**



Fonte: KUROSE (2010).

UM ADENDO IMPORTANTE

- O *Request for Comments* **(RFC)** é uma série de publicações que documenta padrões, serviços e protocolos oficiais da Internet que são mantidos pelo **IETF** (*Internet Engineering Task Force*): **grupo internacional aberto composto de técnicos, fabricantes, agências, fornecedores e pesquisadores que desenvolvem os padrões da Internet**.
- Alguns desses documentos existem com a única finalidade informativa e geralmente são identificados por números como **RFC 7231 ou RFC 2818** (Dê uma olhada nestas!).

Qual o foco da utilização atual

- É comum ouvirmos falar em dois tipos básicos de criptografia **em trânsito** e **em repouso**.
- Criptografar dados **em trânsito** tem como objetivo evitar decifração de transmissão de dados em tempo real, como escutas telefônicas.
- Criptografar dados **em repouso** quer dizer proteger dados armazenados em disco, seja em um banco de dados, em um sistema de arquivos ou em outro tipo de meio de armazenamento.

REFERENCIAS BIBLIOGRÁFICAS

BATITUCCI, Manuela **.** Criptografia: quando surgiu e onde é usada. 2020. Disponível em: <https://blog.mastermaq.com.br/como-surgiu-a-criptografia/>. Acesso em: 20 Set. 2022.

SILVA, Gabriel Leite Baptista da**.** Criptanálise. Disponível em: < https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/gabriel/hist.htm >. Acesso em 10 Set. 2022.

ALENCAR, Márcio Aurélio dos Santos. Fundamentos de redes de computadores / Márcio Aurélio dos Santos Alencar – Manaus : Universidade Federal do Amazonas, CETAM. 2010. Disponível em:<http://proedu.rnp.br/bitstream/handle/123456789/667/FundamentosRedesComputadores.pdf?sequence=2&isAllowed=y>.Acesso em: 27 Set. 2022.

REFERENCIAS BIBLIOGRÁFICAS

KUROSE, James F. e **ROSS,** Keith W. Redes de computadores e a Internet: uma abordagem top-down. 5. ed. São Paulo: Addison Wesley, 2011.

JAMHOUR, E. Qualidade de serviços em redes IP. Curitiba: Programa de Pós-Graduação em Informática, Pontifícia Universidade Católica do Paraná, 2009. Disponível em:<https://www.ppgia.pucpr.br/~jamhour/Pessoal/Mestrado/TARC/QoSIP.pdf>. Acesso em: 6 mar. 2021.

DINAMIZE, 2022. O que é RFC e para que serve?. Disponível em:<https://www.dinamize.com.br/blog/o-que-e-rfc/>. Acesso em: 27 Set. 2021.


PUC Minas
Virtual