OWASP – 2013

The Open Web Application Security Project

Exposição de Dados Sensíveis

Gabriel Faria

A6: Exposição de dados sensíveis

Muitas aplicações web não protegem devidamente os dados sensíveis, tais como cartões de crédito, credenciais de autenticação[...]

- Exemplo de dados considerados sensíveis:
  - Histórico médico;
  - Credenciais de acesso;
  - Dados pessoais – CPF, Identidade;
  - Cartão de crédito;

A6: Exposição de dados sensíveis

- Abrange a proteção de dados sensíveis...
  - No momento que o dado é inserido pelo usuário da aplicação;
  - No transporte desse dado até o servidor;
  - No armazenamento;
  - No retorno do dado até o usuário.

Casos famosos

- **PlayStation Networks**
- Um grupo de hackers invadiu a PlayStation Network e deixou o serviço fora do ar para 77 milhões de usuários.
- Além disso, houve também o roubo de dados de mais de 24 milhões de contas que continham senhas, dados de cartão de crédito e histórico de compras. A Sony teve prejuízo de US$ 24 bilhões.

Casos famosos

- **Sony Pictures**
- “Vazou tudo”
  - Filmes que seriam lançados ainda;
  - Planos de produções futuras;
  - E-mails que revelavam informações sigilosas;
    - Ex.: “Por que ainda damos dinheiro para o Adam Sandler fazer filme ruim?”;
- *“O ataque pode custar mais de US$ 100 milhões para a Sony”*

Valor dos dados - negócio

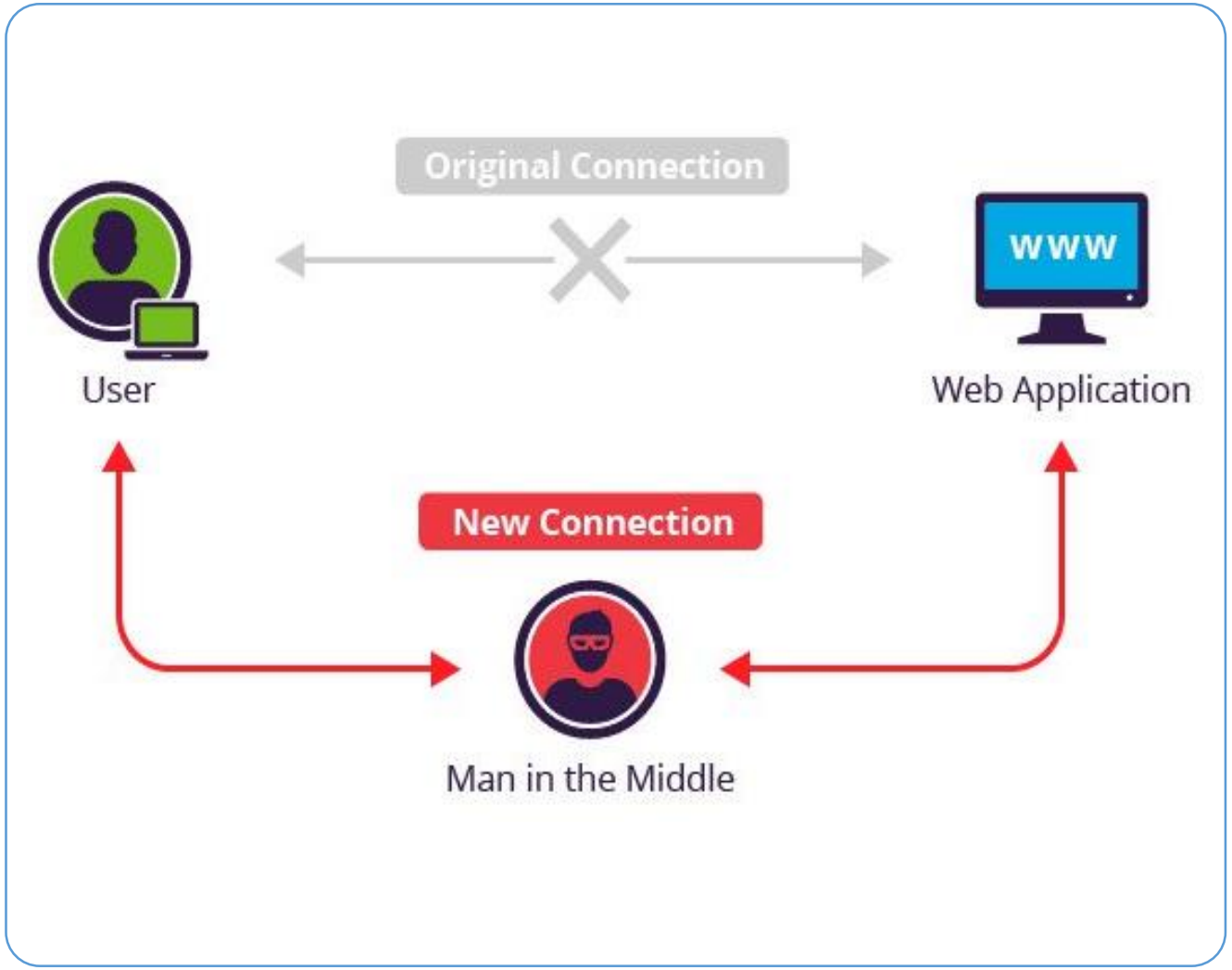
- Considere o valor de negócio dos dados para a aplicação.
  - Alguns dados podem ser mais valiosos em determinadas aplicações.
- Considere o impacto que os dados podem causar ao serem expostos.
  - Reputação da empresa;
  - Não cumprimento da responsabilidade legal da empresa com o sigilo dos dados;

Valor dos dados – impactos técnicos

- Considere as falhas de segurança possíveis - ataques;
- O que ocorreria com o sistema se ele sofresse com esses ataques?
- Quais dados elas podem comprometer – normalmente todos.

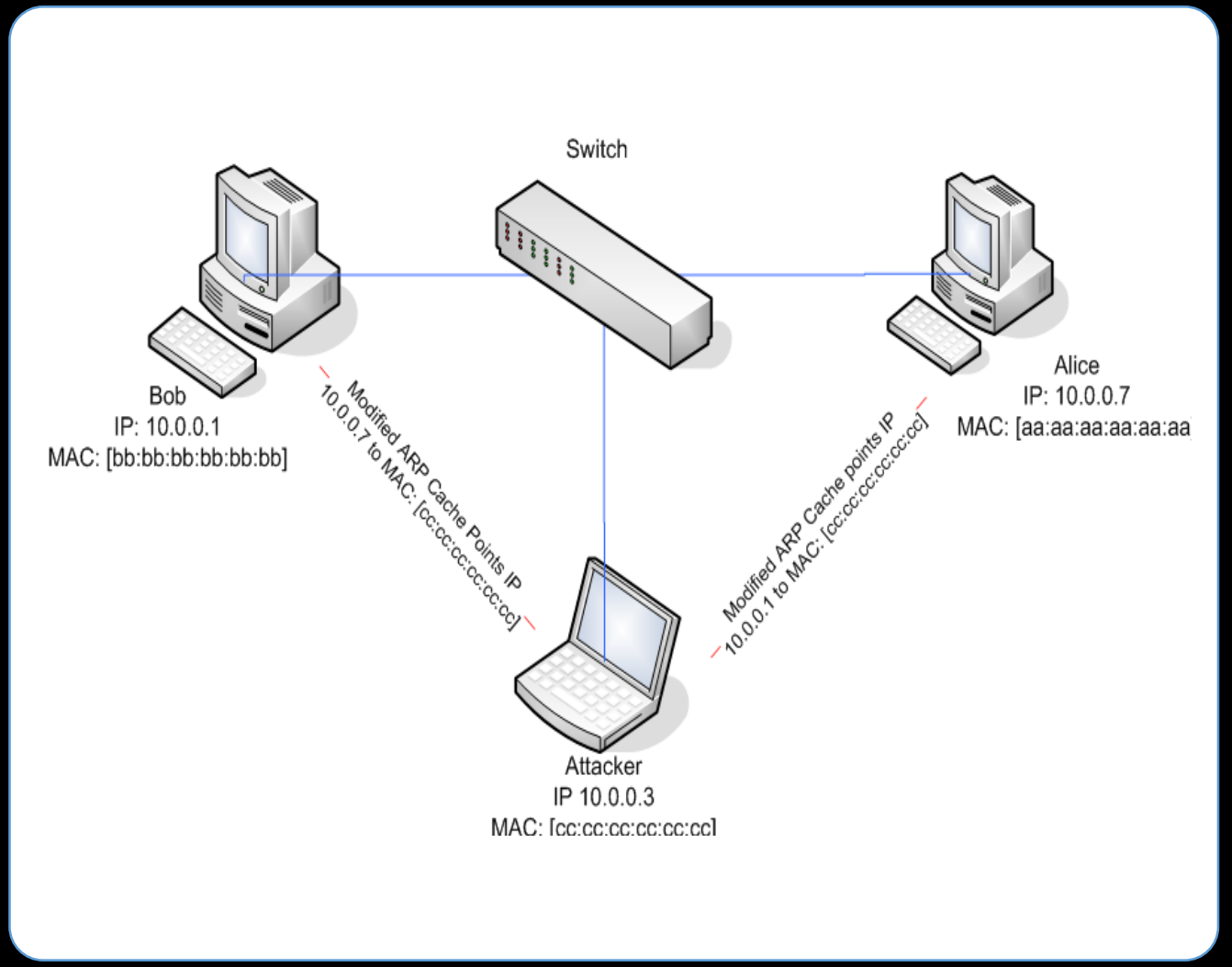
Ataque man-in-the-middle

É um ataque em que a comunicação entre dois hosts é interceptada por um terceiro, que faz a captura de pacotes “fingindo” ser outro endereço na rede.



MITM - Tabela ARP

- Todo dispositivo na rede possui uma tabela ARP que armazena qual é o IP que possui um determinado endereço MAC na rede;
- Para fazer isso, frequentemente as máquinas da rede enviam requisições para atualizar sua tabela;
- É possível configurar um endereço para enganar outras máquinas e forçarem a atualização da tabela para identificar o seu MAC como o IP de outra máquina



[Mais sobre MITM]

Criptografia

- Simétrica:
  - Utiliza chave privada (chave compartilhada);
  - Mensagem é encriptada e decriptada com a mesma chave.
- Assimétrica:
  - Uma chave encripta o arquivo e outra decripta;
  - Emissor utiliza uma chave pública do receptor para encriptar uma mensagem, e será decriptada com a chave privada do emissor.
  - Ex.: Servidores Git utilizam chaves públicas SSH para autenticar.

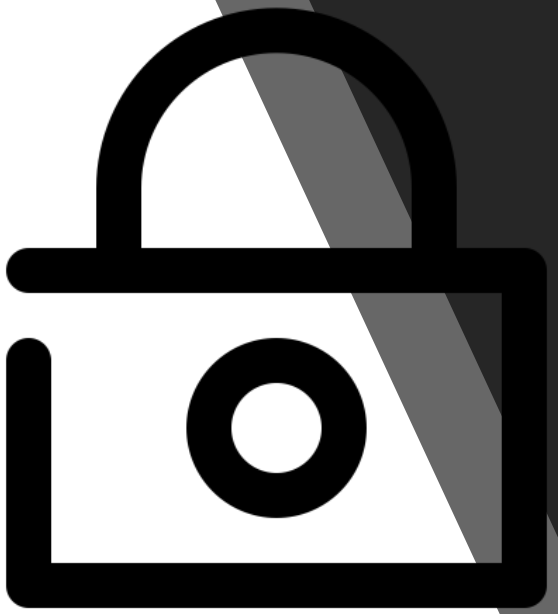
Exemplos de cenários de ataque

- Um site simplesmente não usa SSL. O atacante simplesmente intercepta os pacotes na rede e consegue entender facilmente o que está sendo trafegado.

- Utilização de uma ferramenta de sniffer para analisar o tráfego na rede e capturar pacotes: **Tcpdump** ou **Wireshark**;

- Ex.: http://aluno.wizard.com.br/index.php?option=com_user&view=login

Proteger o tráfego de dados



- Protocolo SSL - aumentar segurança em transmissão de dados;
- Páginas web com HTTPS;
- São altamente recomentados para transmitir dados sensíveis;
- Certificados de segurança – comprova que o site acessado é ele mesmo;
- Não permite que qualquer um acesse os dados trafegados entre o cliente e o servidor;

Função de hash

- Utiliza um valor de hash fixo, computado sobre um texto plano:
  - MD5: 5e11ea786b6e29df06f5a641663202ce
- Não pode retornar ao valor original;
- Verificar integridade de dados:
  - Torrent;
  - Git.
- Armazenamento de senhas
  - Comparação de hash no lugar de texto plano.

Rainbow Tables

- Uma “tabela” que contém n hashs pré-calculados e o texto plano que os originam;
- Utilizado para voltar hashs de senha em texto plano – apenas textos e não arquivos;

- Ex.: Hash MD5
- https://hashkiller.co.uk/md5-decrypter.aspx

Hash	Texto plano
e8d95a51f3af4a3b134bf6bb680a213a	senha
e10adc3949ba59abbe56e057f20f883e	123456
de1c5c17844ed62dc0a7df819101fca3	1234567891000
482c811da5d5b4bc6d497ffa98491e38	password123
3031d1e611bac44226c243b37267a64f	

Salt – Salgando senhas

- Salt é uma sequência adicionada na senha;
- Aumentará a complexidade;
  - Poderá tornar a senha mais simples gerada pelo usuário em uma senha extremamente complexa;
- Ex.: Salt: TheHobbitOrThereNBackAgain + senha

Estou vulnerável?

- Determinar quais dados devem receber proteção extra;
- Determinar como esses dados serão guardados em longo prazo (BD);
- Caso sejam trafegados em rede, os dados sensíveis **não** devem trafegar em texto claro, principalmente em tráfego de internet;
- Verificar se o algoritmo de hash realmente protege o dado caso ele seja capturado;
- Por quanto tempo precisa-se guardar determinados dados?
- Realmente é necessário guardar alguns dados?
  - Dados que você não possui não podem ser roubados.

Referências

- http://revistamonet.globo.com/Celebridades/noticia/2014/12/documentos-vazados-por-hackers-revelam-que-funcionarios-da-sony-nao-gostam-muito-de-adam-sandler.html
- https://tecnoblog.net/171371/sony-pictures-ataque-hacker-tudo-sobre/
- http://g1.globo.com/tecnologia/noticia/2011/04/vazamento-de-dados-da-psn-e-considerado-o-5-maior-da-historia.html
- http://www.100security.com.br/capturando-senhas-com-sslstrip-e-bloquear-o-ataque-com-arpon/
- http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html
- http://www.tecmundo.com.br/seguranca/1896-o-que-e-ssl-.htm
- https://git-scm.com/book/pt-br/v1/Git-no-Servidor-Gerando-Sua-Chave-P%C3%BAblica-SSH
- https://youtu.be/UJ6uSV1KREM
- https://youtu.be/G0aemrKG9PM
- https://cocatech.com.br/senhas-hash-e-salt