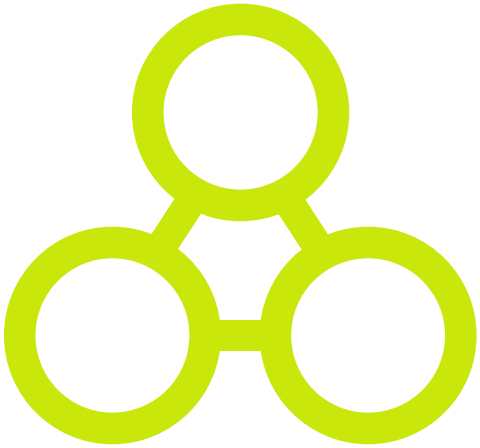


Introdução à Computação

Jordana Sarmenghi Salamon
jssalamon@inf.ufes.br
jordanasalamon@gmail.com
http://inf.ufes.br/~jssalamon

Departamento de Informática
Universidade Federal do Espírito Santo

Agenda

- Segurança
  - Riscos de Segurança em aplicações
  - Ataques contra servidores Web
  - OWASP
  - Boas práticas
- Criptografia
- Privacidade

Segurança

- Cenário atual de incidentes de segurança é reflexo direto de:
  - Aumento da complexidade dos sistemas
  - Softwares com muitas vulnerabilidades
    - Segurança não é parte dos requisitos
    - Falta capacitação/formação para desenvolver com requisitos de segurança
    - Pressão econômica para lançar, mesmo com problemas

Segurança

- Para administradores de sistemas, redes e profissionais web:
  - Segurança não é parte dos requisitos
  - Ferramentas de segurança não conseguem remediar os problemas
  - Ferramentas de ataque “estão a um clique de distância”
  - Descrédito: “Segurança, isso é paranoia. Não vai acontecer”

Riscos de Segurança em Aplicações

- Os atacantes podem potencialmente usar muitos caminhos diferentes através da sua aplicação para prejudicar uma organização.
- Cada um desses caminhos representa um risco que pode ou não ser sério o suficiente para justificar a atenção.
- Às vezes, esses caminhos são triviais para encontrar e explorar e às vezes são extremamente difíceis.

Riscos de Segurança em Aplicações

- Da mesma forma, o dano que é causado pode não ter nenhuma consequência, ou pode deixá-lo fora do negócio.

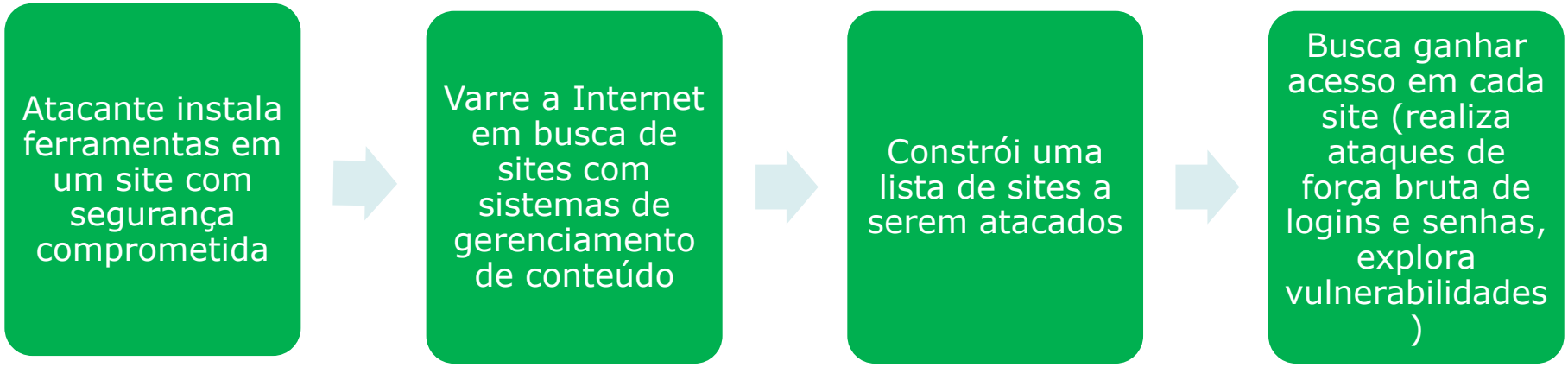
- Para determinar o risco para sua organização, você pode avaliar a probabilidade associada a cada agente que pode ser uma ameaça, a cada vetor de ataque e a cada fraqueza de segurança e combiná-la com uma estimativa do impacto técnico e comercial para sua organização. Juntos, esses fatores determinam seu risco geral.

Ataques contra servidores Web

- Porque atacar sites/aplicações?
  - Desejo de autopromoção
  - Motivação política / Ideológica
  - Motivação financeira
- Porque atacar servidores?
  - Hardware mais poderoso
  - Mais banda de Internet
  - Disponibilidade (non-stop)

Ataques contra servidores Web

Sistema de Gerenciamento de Conteúdo é um aplicativo usado para criar, editar, gerenciar e publicar conteúdo de forma consistentemente organizada permitindo que o mesmo seja modificado, removido e adicionado com facilidade.



Ataques contra servidores Web

- Ao conseguir acesso aos sites, pode-se:
  - alterar o seu conteúdo
  - desferir ataques contra outros sistemas ou redes (como DDoS, enviar spam, tentar invadir outros sistemas, etc)
  - levantar páginas de phishing para obtenção de dados pessoais
  - inserir scripts maliciosos, que exploram vulnerabilidades dos navegadores dos visitantes do site, com o objetivo de infectar os usuários (ataques de drive-by)
  - instalar suas ferramentas e iniciar a busca por outros sites com Sistemas de Gerenciamento de Conteúdo para reiniciar o ciclo do ataque

Ataques DDoS

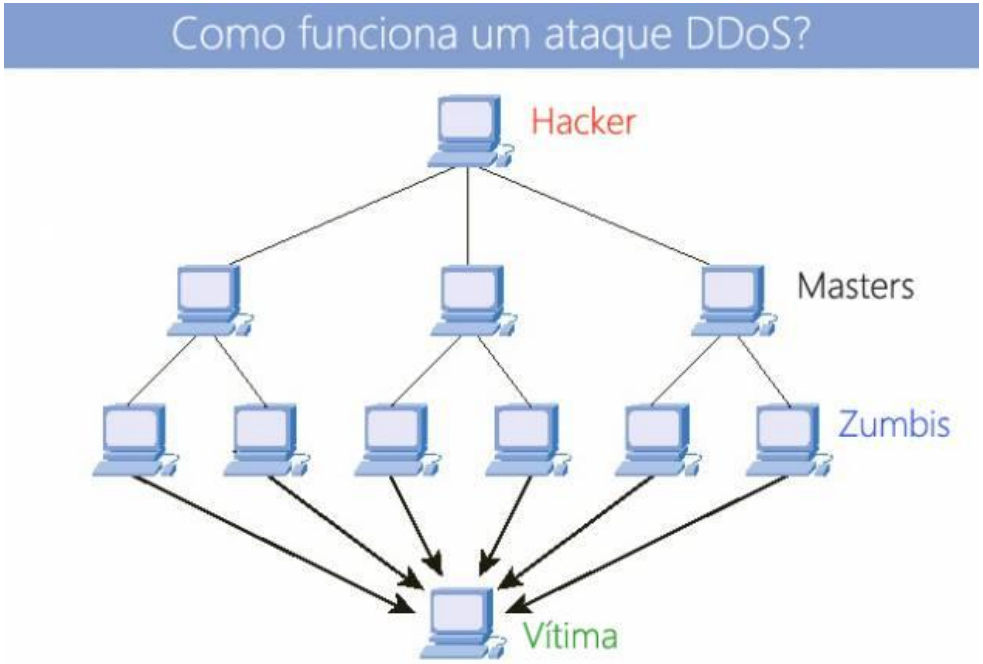
- Um ataque de negação de serviço (Denial of Service Attack), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis. **Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.**

Ataques DDoS

- Os ataques de negação de serviço são feitos geralmente de duas formas:
  - Forçar o sistema vítima a reinicializar ou consumir todos os recursos (como memória ou processamento por exemplo) de forma que ele não possa mais fornecer seu serviço.
  - Obstruir a mídia de comunicação entre os utilizadores e o sistema vítima de forma a não se comunicarem adequadamente.

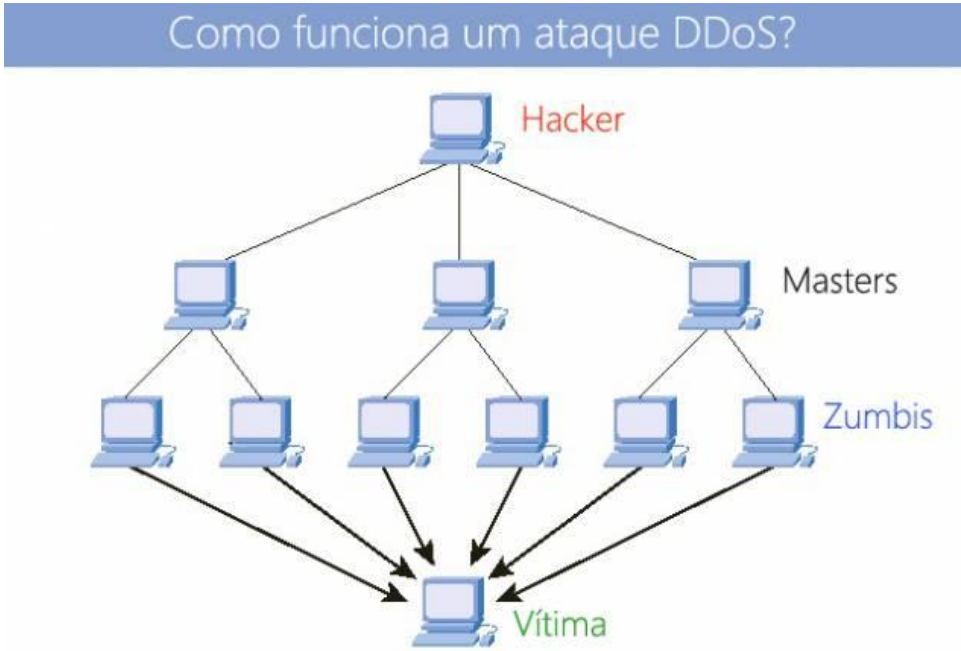
Ataques DDoS

- Num ataque distribuído de negação de serviço (também conhecido como DDoS, **Distributed Denial of Service**), um computador mestre denominado possui sob seu comando computadores Zombies, aos quais as tarefas de ataque são distribuídas.



Ataques DDoS

- O ataque consiste em fazer com que os Zombies (máquinas infectadas e sob comando do Mestre) se preparem para requisitar a um determinado recurso num determinado servidor numa mesma hora de uma mesma data.



Ataques DDoS

- Assim, na determinada hora, todos os zombies requisitam o mesmo recurso do mesmo servidor. Como servidores web possuem um número limitado de utilizadores que pode atender simultaneamente (slots), o grande e repentino número de requisições de acesso esgota esse número, fazendo com que o servidor não seja capaz de atender a mais nenhum pedido.

Ataques DDoS

- O principal objetivo de um ataque de negação de serviço é deixar um recurso computacional inacessível aos seus utilizadores legítimos. As duas classes principais de métodos de ataque são **diminuição de largura de banda** e **esgotamento de recursos**.

Ataques DDoS

- **Ataques por Inundação**
  - Ataques por inundação se caracterizam por enviarem um grande volume de tráfego ao sistema da vítima primária de modo a congestionar a sua banda. O impacto deste ataque pode variar entre deixar o sistema lento, derrubá-lo ou sobrecarregar a banda da rede da vítima.

Ataques DDoS

- **Ataques por Amplificação**
  - Ataques por amplificação se caracterizam por enviarem requisições forjadas para uma grande quantidade de computadores ou para um endereço IP de broadcast, que por sua vez responderão às requisições. Forjando o endereço IP de origem das requisições para o endereço IP da vítima primária fará com que todas as respostas sejam direcionadas para o alvo do ataque.

Ataques DDoS

- **Ataques por Amplificação**
  - Quando uma requisição possui um endereço IP de broadcast como endereço de destino, o roteador replica o pacote e o envia para todos os endereços IP dentro do intervalo de broadcast. Em ataques por amplificação, endereços de broadcast são usados para amplificar e refletir o tráfego de ataque, reduzindo então a banda da vítima primária.

Ataques DDoS

- **Ataques por Exploração de Protocolos**
  - Ataques por exploração de protocolos se caracterizam por consumir excessivamente os recursos da vítima primária explorando alguma característica específica ou falha de implementação de algum protocolo instalado no sistema da vítima.

OWASP

- The Open Web Application Security Project

- OWASP Top 10 –
- **A list of the 10 Most Critical Web Application Security Risks**

OWASP Top 10 – 2017 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities
A10 – Underprotected APIs (NEW)

OWASP Top 10 Application Security Risks

A1 - Injection

- As falhas de injeção, como a injeção SQL, OS, XXE e LDAP, ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados hostis do invasor podem enganar o interpretador para executar comandos não intencionais ou acessar dados sem a devida autorização.

A2 – Broken Authentication and Session Management

- As funções de aplicação relacionadas à autenticação e ao gerenciamento de sessão geralmente são implementadas incorretamente, permitindo que os invasores comprometam senhas, chaves ou tokens de sessão ou explorem outras falhas de implementação para assumir identidades de outros usuários (temporariamente ou permanentemente).

OWASP Top 10 Application Security Risks

A3 – Cross-Site Scripting (XSS)

- As falhas XSS ocorrem sempre que um aplicativo inclui dados não confiáveis em uma nova página da Web sem validação ou escape adequadamente, ou atualiza uma página da Web existente com dados fornecidos pelo usuário usando uma API do navegador que pode criar JavaScript. O XSS permite que os invasores executem scripts no navegador da vítima, que podem seqüestrar sessões de usuários, desfigurar sites da Web ou redirecionar o usuário para sites mal-intencionados.

A4 – Broken Acess Controll

- As restrições sobre o que os usuários autenticados podem fazer não são aplicadas corretamente. Os atacantes podem explorar essas falhas para acessar funcionalidades e / ou dados não autorizados, como acessar contas de outros usuários, visualizar arquivos sensíveis, modificar dados de outros usuários, alterar direitos de acesso, etc.

OWASP Top 10 Application Security Risks

A5 – Security Misconfiguration

- Uma boa segurança exige ter uma configuração segura definida e implantada para a aplicação, frameworks, servidor de aplicativos, servidor web, servidor de banco de dados, plataforma, etc. Configurações seguras devem ser definidas, implementadas e mantidas, pois os padrões geralmente são inseguros. Além disso, o software deve ser mantido atualizado.

A6 – Sensitive Data Exposure

- Muitas aplicações web e APIs não protegem de forma adequada os dados confidenciais, como financeiros, de saúde e informações de identificação pessoal. Os atacantes podem roubar ou modificar esses dados deficientemente protegidos para conduzir fraudes em cartões de crédito, roubo de identidade ou outros crimes. Os dados sensíveis merecem proteção extra, como criptografia quando em repouso no banco de dados ou em trânsito, bem como precauções especiais quando trocados com o navegador.

OWASP Top 10 Application Security Risks

A7 – Insufficient Attack Protection

- A maioria das aplicações e APIs não possui capacidade básica para detectar, prevenir e responder a ataques manuais e automáticos. A proteção a ataques vai muito além da validação de entrada básica e envolve, de forma automática, a detecção, registro, resposta e até bloqueio de tentativas de exploração. Os proprietários de aplicações também precisam ser capazes de implantar patches rapidamente para proteger contra ataques.

A8 – Cross-Site Request Forgery (CSRF)

- Um ataque CSRF força o navegador de uma vítima logada a enviar uma solicitação HTTP forjada, incluindo o cookie de sessão da vítima e qualquer outra informação de autenticação incluída automaticamente, para uma aplicação web vulnerável. Esse ataque permite que o atacante force o navegador de uma vítima a gerar solicitações que o aplicativo vulnerável pensa serem pedidos legítimos da vítima.

OWASP Top 10 Application Security Risks

A9 – Using Components with Known Vulnerabilites

- Componentes, como bibliotecas, frameworks e outros módulos de software, são executados com os mesmos privilégios que a aplicação. Se um componente vulnerável for explorado, esse ataque pode facilitar a perda séria de dados ou a aquisição do servidor pelo atacante. Aplicações e APIs que usam componentes com vulnerabilidades conhecidas podem prejudicar as defesas de aplicações e permitir vários ataques e impactos.

A10 – Underprotected APIs

- As aplicações modernas geralmente envolvem aplicativos e APIs rich client, como JavaScript no navegador e aplicativos móveis, que se conectam a uma API de algum tipo (SOAP / XML, REST / JSON, RPC, GWT, etc.). Essas APIs geralmente são desprotegidas e contêm várias vulnerabilidades.

Boas Práticas: Para desenvolvedores

- Pensar em Segurança desde os requisitos
- Requisitos de Confidencialidade, Integridade e Disponibilidade
- Cuidados na codificação:
  - Validar entrada de dados (não apenas no browser do usuário com JavaScript)
  - Cuidado com abuso da interface – dados controlados pelo usuário (comentários em blogs, campos de perfil)

Boas Práticas: Para desenvolvedores

- Tratamento de erros (fail safe)
- Autenticação e controle de sessão
- Garantir as duas pontas da conexão (evitar man-in-the-middle, redirect)
- Cuidado com exposição (transmissão e armazenamento) de IDs de usuário
- Criptografia
  - Não incluir senhas / chaves no código fonte

Boas Práticas: Para administradores

- Não instale/execute o software com usuário privilegiado (root / Administrator);
- Crie usuários distintos para diferentes softwares e funções
  - Web/app server, DB
  - Privilégios mínimos
- Utilize senhas fortes (proteja-se de força bruta)
  - Considerar two factor authentication

Boas Práticas: Para administradores

- Mantenha o servidor atualizado
  - Sistema Operacional, Software do web/app server e demais plugins
- Não utilize conta padrão de administração
- Restrinja acesso à interface de administração
- Seja criterioso nas permissões a arquivos e diretórios
- Siga os guias de segurança dos respectivos fornecedores
- Acompanhe logs para verificar tentativas de ataque
- Faça backup e teste a restauração

Criptografia

- **Criptografia** é o estudo dos princípios e técnicas pelas quais **a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário**, o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

Criptografia

- Uma informação não-cifrada que é enviada de uma pessoa para outra é chamada de "texto claro" (**plaintext**).
- **Cifragem** é o processo de conversão de um texto claro para um código cifrado e **decifragem** é o processo contrário, de recuperar o texto original a partir de um texto cifrado.

Criptografia

- Por meio do uso da criptografia você pode:
  - proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas;
  - criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;

Criptografia

- Por meio do uso da criptografia você pode:
  - proteger seus backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
  - proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

Criptografia

- **Cifra**
- **A cifra é um ou mais algoritmos que cifram e decifram um texto.**

  A operação do algoritmo costuma ter como parâmetro uma chave criptográfica. Tal parâmetro costuma ser secreto (conhecido somente pelos comunicantes). A cifra pode ser conhecida, mas não a chave; assim como se entende o mecanismo de uma fechadura comum, mas não se pode abrir a porta sem uma chave real.

Criptografia

- **Chave Criptográfica**
- **Uma chave criptográfica é um valor secreto que interage com o algoritmo de encriptação.** A fechadura da porta da frente da sua casa tem uma série de pinos. Cada um desses pinos possui múltiplas posições possíveis. Quando alguém põe a chave na fechadura, cada um dos pinos é movido para uma posição específica. Se as posições ditadas pela chave são as que a fechadura precisa para ser aberta, ela abre, caso contrário, não.

Criptografia

- A criptografia tem quatro objetivos principais:
  - **confidencialidade da mensagem**: só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada. Além disso, a obtenção de informação sobre o conteúdo da mensagem (como uma distribuição estatística de certos caracteres) não deve ser possível, uma vez que, se o for, torna mais fácil a análise criptográfica.

Criptografia

- **integridade da mensagem**: o destinatário deverá ser capaz de verificar se a mensagem foi alterada durante a transmissão.
- **autenticação do remetente**: o destinatário deverá ser capaz de verificar que se o remetente é realmente quem diz ser.
- **não-repúdio ou irretratabilidade do remetente**: não deverá ser possível ao remetente negar a autoria de sua mensagem.

Criptografia

- Normalmente, existem algoritmos específicos para cada uma destas funções. Mesmo em sistemas criptográficos bem concebidos, bem implementados e usados adequadamente, alguns dos objetivos acima não são práticos (ou mesmo desejáveis) em algumas circunstâncias. Por exemplo, o remetente de uma mensagem pode querer permanecer anônimo, ou o sistema pode destinar-se a um ambiente com recursos computacionais limitados.

Criptografia

- **Criptografia de chave simétrica e de chaves assimétricas**

- De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias: **criptografia de chave simétrica e criptografia de chaves assimétricas.**

Criptografia

- **Criptografia de chave simétrica**: também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados.

Criptografia

- Casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave).

Criptografia

- **Criptografia de chaves assimétricas**: também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono.

Criptografia

- Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um smartcard ou um token.

Criptografia

- **A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido.**

Criptografia

- Todavia, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável, em virtude da:
  - **necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes** (o que na Internet pode ser bastante complicado);

Criptografia

- **dificuldade de gerenciamento de grandes quantidades de chaves** (imagine quantas chaves secretas seriam necessárias para você se comunicar com todos os seus amigos).

Criptografia

- A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve estes problemas visto que facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves.

Criptografia

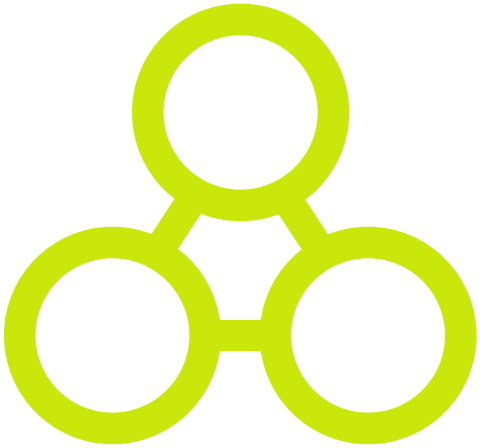
- Para aproveitar as vantagens de cada um destes métodos, o ideal é o **uso combinado de ambos**, onde a criptografia de chave simétrica é usada para a codificação da informação e a criptografia de chaves assimétricas é utilizada para o compartilhamento da chave secreta (neste caso, também chamada de chave de sessão). Este uso combinado é o que é utilizado pelos navegadores Web e programas leitores de e-mails.

Privacidade

- E agora, uns vídeos....

Referências

- https://www.cert.br/docs/palestras/certbr-webbr2014.pdf
- https://cartilha.cert.br/
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010%20-%202017%20RC1-English.pdf
- https://pt.wikipedia.org/wiki/Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o
- https://pt.wikipedia.org/wiki/Criptografia
- https://cartilha.cert.br/criptografia/
- https://www.ted.com/talks/gary_kovacs_tracking_the_trackers#t-373866
- https://www.ted.com/talks/andy_yen_think_your_email_s_private_think_again
- https://www.ted.com/talks/glenn_greenwald_why_privacy_matters



Introdução à Computação

Jordana Sarmenghi Salamon
jssalamon@inf.ufes.br
jordanasalamon@gmail.com
http://inf.ufes.br/~jssalamon

Departamento de Informática
Universidade Federal do Espírito Santo