Segurança

Um dos fatores primordiais de qualquer sistema distribuído sempre foi segurança dos dados; é necessária uma atenção especial com a segurança dos dispositivos, pois há muitos pontos (maquinas e softwares) sendo usados para um mesmo sistema e, neste caso, todos devem estar seguros.

09 – Segurança

De nada adianta ter um firewall bloqueando o acesso ao servidor de web, enquanto o servidor de banco de dados está desprotegido, permitindo acesso aos dados do sistema; muito menos o contrario: se preocupar apenas com a segurança do servidor de banco de dados, e deixar aberto os acessos ao servidor web ou outros pontos do sistema.

09 – Segurança

Quando falamos em segurança dos sistemas distribuídos, além de cuidar da segurança dos dados, também devemos planejar a como este sistema deve escalar, para que ele atenda a demanda gerada pelos seus usuários; uma falha de segurança pode permitir ataques de diversas formas, incluindo acesso aos dados, invasões, sobrecarga ou DOS (deny of service).

09 – Segurança

Existem 4 tipos de ameaças de segurança que devem ser consideradas:

- Intercepção;
- Interrupção;
- Modificação;
- Fabricação.

09 – Segurança

Intercepção: é quando alguém, que não faz parte do sistema, ou seja, alguém não autorizado, ganha acesso a um serviço ou dados de um sistema; como exemplo disto temos quando um diretório de alguém é invadido e seus dados são copiados, um outro exemplo é o ataque Homem no Meio (Men In the Middle), que acontece quando a comunicação entre duas partes do sistema é interceptada por uma terceira parte, que poderá ler e usar os dados desta comunicação.

09 – Segurança

Interrupção: acontece quando um serviço, ou dados, ficam indisponíveis, inutilizáveis, ou são destruídos; como exemplo temos o DDOS, ataque de negação de serviço, de maneira que eles não podem mais ser acessados. Neste tipo de ataque, o atacante executa muitas chamadas a algum serviço especifico até que ele fique indisponível.

09 – Segurança

Modificação: acontece quando uma alteração de dados, ou do sistema, não autorizada, fazendo com que o comportamento deste sistema seja alterado e eles não consigam mais realizar as operações para as quais foram designados. Como exemplo de modificações temos o ataque onde alguém intercepta a comunicação entre dois pontos e altera as mensagens que são enviadas entre eles; outro caso de modificação é quando o sistema é alterado, de maneira a logar, secretamente os passos realizados pelos seus usuários.

09 – Segurança

Fabricação: uma informação ou trecho de código “mal intencionado” é adicionado ao sistema; por exemplo, quando um usuário consegue adicionar uma entrada na tabela de senhas, permitindo o acesso futuro; também pode ser possível entrar em um sistema, ao repetir uma mensagem previamente enviada, como o reenvio de uma mensagem de login com o usuário e a senha.

09 – Segurança

Simplesmente dizer que um sistema deverá se proteger contra todos os tipos de ataques não é a melhor forma de se construir um sistema seguro visto que novos ataques surgem a cada dia; o primeiro passo para se construir um sistema seguro é descrever quais são os requisitos de segurança da aplicação, ou qual será a sua politica de segurança; este conjunto de definições irá descrever quais ações cada entidade do sistema pode realizar e quais ações serão proibidas;

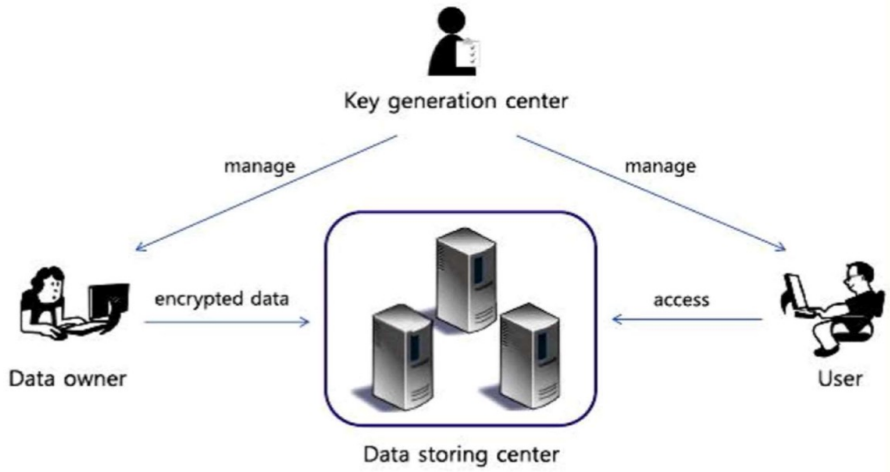
09 – Segurança

Uma vez definidas, as políticas de segurança de um sistema, pode-se concentrar nos mecanismos de segurança que o mesmo utilizará; os mais importantes são:

- Criptografia;
- Autenticação;
- Autorização;
- Auditoria.

09 – Segurança

Criptografia, ou a ***encriptação dos dados***, é essencial para a segurança de um sistema, já que ela transforma os dados em algo ilegível para quem não possui a chave de segurança responsável por descriptografar aqueles dados.



09 – Segurança

Com a ***Autenticação*** é possível verificar a identidade do usuário, servidor, host ou qualquer entidade do sistema; tipicamente a autenticação é realizada através de uma senha, mas existem varias outras maneiras de se realizar uma autenticação, como os tokens bancários, muito comuns hoje em dia.

09 – Segurança

Depois que um cliente está autenticado, ainda assim é preciso verificar se aquele usuário possui ***Autorização*** para realizar aquela operação no sistema. Podemos exemplificar isto em qualquer sistema, por exemplo, um usuário nunca poderá alterar a senha de outro usuário, ou então consultar dados pessoais de outro usuário, como e-mail, endereço, etc. A não ser sob uma autorização expressa do usuário, o qual os dados serão exibidos.

09 – Segurança

Não menos importantes são as ferramentas de ***Auditoria***, as quais permitem ao administrador do sistema verificar quais operações cada usuário realizou no sistema. Com isso é possível detectar invasões depois de elas terem ocorrido. Um dos papeis de bom hacker é nunca deixar rastros em um sistema acessado e isto só pode ser feito se ele conseguir apagar os logs deste sistema. Uma das formas de evitar isto é habilitar o log de acesso em um sistema, mas neste caso, o lugar onde este log será escrito e as permissões de acesso a este log, assim como os seus backups, são fatores primordiais para uma analise de uma invasão ao sistema.

09 – Segurança

Considerações de Design

Um sistema distribuído precisa ser implementado de maneira a permitir que um grande numero de políticas de segurança sejam implementadas e para fazer isso existem algumas considerações de Design a serem feitas.

09 – Segurança

Controle do Foco

Quando estamos desenvolvendo um sistema distribuído, podemos ter três diferentes maneiras de se resolver a segurança deste sistema. A primeira delas é focar nos dados que estão associados à aplicação, o que significa que deveremos focar em manter a integridade dos dados, em todos os serviços que irão alterar os dados daquele aplicativo. Este tipo de segurança poderá ser implementado na base de dados do aplicativo, já que varias constraints e chaves podem ser implementadas (nos bancos SQL) de forma a garantir a integridade dos dados.

09 – Segurança

Controle do Foco

Garantir a integridade dos dados é assegurar que quando um usuário for apagado, por exemplo, os dados relacionados a ele também serão apagados. Não pode haver um endereço gravado na tabela de endereços, de um usuário que já foi removido do sistema. As chaves estrangeiras em um sistema de banco de dados SQL fazem isto, mas se você estiver usando outro tipo de sistema de armazenamento de dados, você deverá tomar cuidados extras.

09 – Segurança

Controle do Foco

Outra forma de se resolver a segurança é especificar exatamente quais operações poderão ser realizadas, e por quem, os dados poderão ser acessados. Aqui deveremos especificar quem pode acessar quais dados, e com isso esta implementação estará focada em mecanismos de controle de acesso. Em um webservice, podemos especificar quais usuários, ou grupos de usuários, poderão acessar cada serviço.

09 – Segurança

Controle do Foco

Uma terceira forma de se pensar a segurança de um sistema é focar nos usuários que devem ter acesso aos serviços do aplicativo, não se importando com quais serviços eles podem acessar. Por exemplo, o banco de dados de uma escola alguns dados só podem ser acessados pelos gerentes. Em algumas escolas, o sistema guarda a diferença entre as notas lançadas , nas alterações de nota realizadas no sistema. Relatórios são desenvolvidos para listar as alterações de notas cujos valores diferem muito, com isso os administradores das escolas podem intimar o professor a esclarecer o que aconteceu para a nota do aluno mudar tanto.

09 – Segurança

Controle do Foco

Neste tipo de controle é focado na definição de papéis dos usuários no sistema, por exemplo os alunos não terão acesso a estes relatórios de alteração de nota, neste caso existem três papéis, o do professor, o do aluno e o do gerente. Como parte do desenvolvimento de um sistema seguro, é necessário levantar quais serão os papéis dos usuários do sistema e definir quais dados cada papel poderá acessar ou não.

09 – Segurança

Camadas dos mecanismos de segurança

Uma consideração importantíssima a se tomar é onde cada camada de segurança deve ser implementado. Por exemplo, as redes de computador são organizadas em camadas, lembre-se das 7 camadas do protocolo OSI.

Geralmente os mecanismos de segurança de um sistema distribuído são colocados na camada de middleware. Uma das ferramentas muito utilizadas na segurança da comunicação entre as maquinas de um sistema é o SSL (Secure Socket Layer), que é utilizado para enviar e receber mensagens seguras via conexões TCP. O SSL permite que duas maquinas criem um canal de comunicação segura.

09 – Segurança

Camadas dos mecanismos de segurança

O sistema de segurança que é instalado em uma camada de middleware só poderá ser confiável, se o serviço no qual ele se basear for confiável. Por exemplo, se um sistema de RPC for implementado com o uso do SSL, este sistema só será confiável, se o SSL utilizado em sua implementação, for confiável.

09 – Segurança

Distribuição dos mecanismos de segurança

A parte da segurança relativa a dependência dos serviços criou um termo chamado Base de Computadores Confiáveis (TCB Trusted Computer Base); uma TCB é um conjunto de mecanismos de segurança que são necessários para assegurar uma politica de segurança, e por isso ele deve ser confiável. Se o sistema distribuído foi construído sob o middleware de um sistema distribuído, a sua segurança poderá depender da segurança do sistema operacional utilizado.

09 – Segurança

Distribuição dos mecanismos de segurança

Em um servidor de arquivos, este serviço dependerá da segurança do seu sistema operacional local, não só para assegurar que nenhum processo, fora os do servidor, acessem os arquivos daquele sistema, como também dos vários dispositivos de segurança que evitam que o sistema inteiro seja derrubado.

Em um sistema distribuído de middleware também deverá confiar nas politicas de segurança do sistema operacional no qual ele é executado, pois se esta confiabilidade não existir parte destas politicas deverão ser implementadas pelo sistema distribuído.

09 – Segurança

Distribuição dos mecanismos de segurança

Uma solução de design para isto é separar os serviços de segurança dos outros serviços em instancias diferentes, fazendo com que os serviços seguros fiquem isolados do resto do sistema, o que torna a administração das regras de Firewall mais fácil e efetiva, já que as maquinas a serem protegidas serão reduzidas.

09 – Segurança

Criptografia

A criptografia é fundamental para a segurança de qualquer sistema, inclusive dos sistemas distribuídos, e todas aquelas técnicas de criptografia e hash são muito importantes.

Criptografia de uma mensagem é quando alteramos a mensagem através de um algoritmo afim de que somente quem tenha a chave de descriptografia consiga ler aquela mensagem.

09 – Segurança

Criptografia

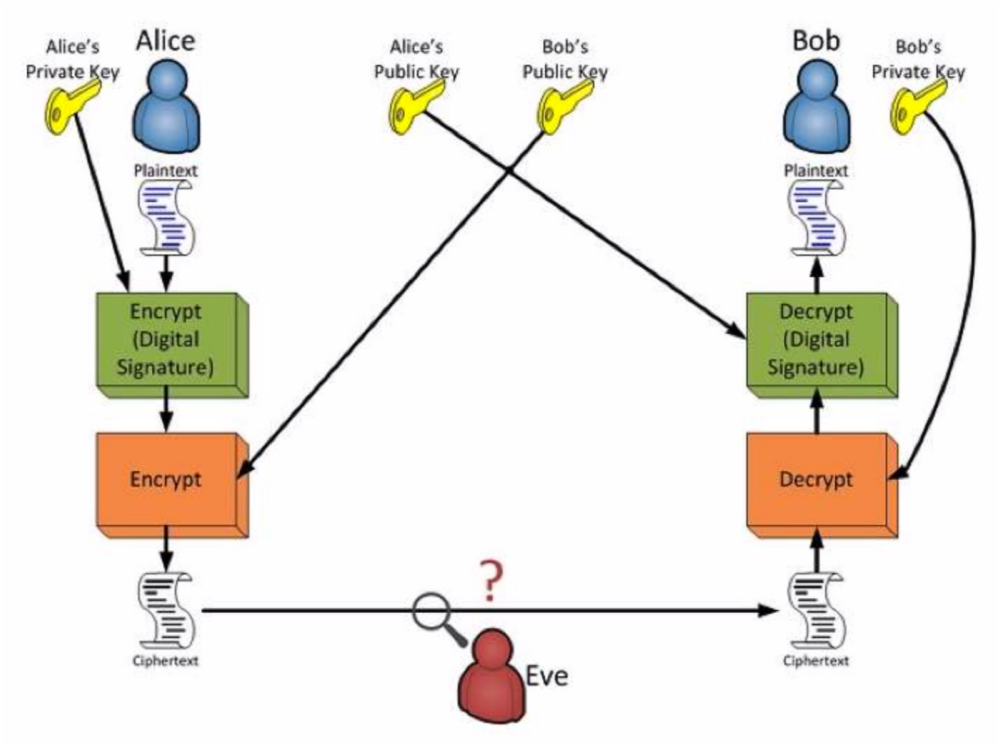
Funções de hás são utilizadas para esconder uma informação, como as senhas, e somente se você souber a chave, e a informação, é que será possível dizer se ela está correta ou não; as senhas “hasheadas” não podem ser recuperadas, quando um usuário digita a senha, com a chave é possível “hashear” a senha digitada e comparar com a armazenada, se elas forem iguais o usuário tem seu acesso liberado; desconfie de qualquer sistema que reenvie a sua senha por e-mail, quando você a esqueceu, isto geralmente significa que ela é armazenada em modo texto sem qualquer segurança.

09 – Segurança

A criptografia pode ser dividida em dois modos, o modo de chave única, onde a mesma chave é utilizada para criptografar e descriptografar a mensagem, E o modo de chave publica, privada, onde quem criptografa as mensagens possui uma chave e quem descriptografa deve possuir outra chave ; ao gerar a chave privada, uma chave publica também deve ser gerada, esta chave será distribuída para todos os clientes que desejam enviar mensagens aquele servidor; toda mensagem será criptografada utilizando a chave publica, mas para descriptografar esta mensagem, só será possível com a utilização da chave privada; dentre as varias técnicas de criptografia utilizadas, destacam-se o AES256 e de hash o SHA256.

09 – Segurança

Criptografia



09 – Segurança

Canais Seguros de comunicação

Como sabemos, qualquer sistema distribuído deve possuir uma rede de comunicação para trocar mensagem entre os seus dispositivos; um servidor, de um sistema distribuído, também pode ser um cliente de um outro servidor do mesmo sistema; na verdade cada serviço, com o seu cliente, irá atuar como um sistema de cliente/servidor, dentro do sistema distribuído, por isso estes sistemas são classificados como vários sistemas cliente/servidor.

09 – Segurança

Canais Seguros de comunicação

Para que a comunicação entre estes componentes do sistema seja segura, devemos estabelecer um meio seguro de comunicação entre eles, o que é feito através dos canais seguros de comunicação. Estes canais são abertos entre duas maquinas e através da autenticação e da criptografia, são garantidas a segurança na troca de mensagens.

09 – Segurança

Canais Seguros de comunicação

Uma outra requisição desta troca de mensagens é garantir que elas não serão alteradas no meio do caminho, e isto é garantido através da assinatura destas mensagens, por uma chave publica fornecida pelo recebedor, com isso garante-se que a mensagem foi enviada por aquele cliente.

09 – Segurança

Controle de Acesso

Depois de o cliente estabelecer uma conexão com o servidor, tem-se que verificar se o método, arquivo ou o serviço que ele está acessando pode ser acessado por aquele cliente.

Uma maneira muito utilizada nas implementações de controle de acesso é a criação de grupos, e aos grupos são dadas as autorizações de acesso aos métodos. Cada usuário pode ter um ou mais grupos, e quando ele acessa o sistema, o método verifica quais grupos ele faz parte, se algum deles tiver permissão de acesso aquele método, o usuário será liberado.

09 – Segurança

Controle de Acesso

Lembre-se que para implementar uma camada de verificação de acesso, esta verificação sempre, deverá ocorrer antes do método ser chamado. Em alguns casos isso é implementado através de metadados, em outros existe um método que sempre é chamado no inicio do método que está sendo acessado.

09 – Segurança

OAUTH

Com a evolução da internet e a criação de métodos e serviços que são acessados pela internet criou-se a necessidade de padronizar o acesso aos serviços. Com isso foi criado o OAUTH que é um protocolo aberto que permite uma padronização para uma autorização segura simples para métodos web, desktop e celulares.

09 – Segurança

OAUTH

Existem duas versões do OAUTH, sendo que na primeira cuidava da padronização da comunicação entre o usuário e um serviço, e a segunda versão permite também que o usuário dê acesso aos seus dados a outra aplicação, o que pode ser exemplificado pelos logins que utilizam senha de outros serviços. Você pode logar em um site, usando o usuário e a senha de outro serviço.

09 – Segurança

OAUTH