Segurança Informática e nas Organizações

Resumos
2016/2017

João Alegria | 68661

Capítulo 6

Protocolos de Identificação

A autenticação de entidades consiste na obtenção de um comprovativo de que elas possuem um atributo que afirmam possuir, ou que é suposto que possuam.
A autenticação de entidades envolve um processo de prova, na qual o autenticador obtém uma prova fidedigna de que a entidade autenticada, ou autenticado, possui o atributo que afirma possuir.
Um protocolo de autenticação é um conjunto de mensagens trocadas entre vários interlocutores e que tem por objetivo realizar a autenticação de um ou mais deles perante um ou mais dos demais.

Caracterização dos protocolos de autenticação

- ***Elementos de prova***

São usados três tipos de paradigmas em termos de elementos de prova:

- *O que sabe*: Uma entidade prova a sua autenticidade mostrando que conhece uma determinada informação secreta, denominada genericamente por senha. Se a senha for conhecida pelos intervenientes diretos no processo de autenticação, pode provar que o interlocutor é quem afirma ser.
- *O que possui*: Neste paradigma uma entidade prova a sua autenticidade mostrando que possui um determinado dispositivo de segurança ou que é o dono legítimo desse dispositivo de segurança.
- *O que se é*: Neste paradigma é apresentado alguma característica que permite diferenciar das demais. Normalmente este paradigma aplica-se a humanos e a característica diferenciadora é obtida através da biometria.

Quando se usam estes três paradigmas combinados diz-se que a sua autenticação é multimétodo.

Autenticação

- ***Objetivos***
  - Autenticar entidades interatuantes
    - pessoas, serviços, servidores, máquinas, redes, etc
  - Permitir aplicação de políticas e mecanismos de autorização
    - autorização -> autenticação
  - Apoiar outras ações no âmbito de segurança
    - distribuição de chaves para comunicação segura

- ***Requisitos***

Confiança	**Secretismo**	**Robustez**
Nível de confiança	Não divulgação de credenciais usadas pelas entidades legítimas	- Impedir ataques às trocas de dados do protocolo - Impedir cenários de DoS interativos - Impedir ataques desligados com dicionários
Simplicidade	**Lidar com vulnerabilidades vindas de pessoas**	
Deverá ser tão simples quanto possível para evitar que os utentes escolham simplificações perigosas	Têm uma tendência natural para facilitar ou para tomarem iniciativas perigosas	

• *Entidades e modelos de implantação*

Entidades	Modelos de Implantação

Pessoa
Máquinas
Redes
Serviços / Servidores
	- Ao longo do tempo
	  - quando a interação se inicia
	  - continuamente ao longo da interação
	- Direcional
	  - unidirecional
	  - bidirecional

Protocolos de Autenticação: Aproximações Elementares

• ***Aproximação Direta***

Apresentar credencias e esperar pelo veredicto

• ***Aproximação com Desafio-Resposta***

É lançado um desafio, o utilizador responde e é calculado e fornecido uma resposta com base no desafio e nas credenciais. Espera-se pelo veredicto.

Autenticação de pessoas

- Aproximação <u>Direta com senha memorizada</u>

Funcionamento	A senha é confrontada com um valor guardado para a pessoa que está a ser autenticada, dada a sua entidade reclamada (*username*) Valor pessoal guardado
Vantagens	Simplicidade
Problemas	Utilização de senhas fracas/inseguras (permite ataques por dicionário) Transmissão de senhas em claro em canais de comunicação inseguros (escutas podem revelar senhas)

- Aproximação <u>Direta com biometria</u>

A autenticação biométrica baseia-se na avaliação de características físicas dos autenticadores para aferir a sua autenticidade face a uma identidade reclamada. Essas características podem ser diversas, e tanto fisiológicas e estáticas (dimensões e distancias faciais) como comportamentos e dinâmicas (ritmo de escrita num teclado).

Funcionamento	- Uma pessoa autentica-se com as medidas do seu corpo (impressão digital, íris, geometria da face, timbre) - Estas medidas são comparadas com um registo pessoal e similar - através de uma referência biométrica
Vantagens	- As pessoas não necessitam de memorizar nada - As pessoas não necessitam de escolher senhas - As credenciais não podem ser transferidas entre pessoas
Problemas	- A biometria ainda está incipiente (inicio) - As pessoas não podem mudar as credenciais caso sejam roubadas - Pode criar riscos para as pessoas (remoção de partes do corpo para personificar a vítima) - Pode revelar informação pessoal sensível (doenças) - Não é uma solução interessante e segura para autenticações remotas - Não é um método de autenticação ideal quando se tem muitos clientes

- Aproximação <u>Direta com senhas descartáveis</u>

A autenticação com senhas descartáveis é um tipo de autenticação com apresentação direta de credenciais onde as mesmas nunca se repetem, só são usadas uma vez. Este tipo de autenticação é interessante quando se pretende evitar riscos que o mesmo apresenta quando as credenciais podem ser capturadas por terceiros e reutilizadas novamente.
Exemplos: RSA SecurID, matriz com códigos bancários

Descrição	- Senhas *one-time-password*, só se podem utilizar uma vez - É uma solução interessante para criar sessões remotas sobre comunicação não seguras - Pode envolver a troca de um desafio para indicar a senha descartável a ser usada
Vantagens	- Podem ser escutadas (isso não adianta a quem o fizer para personificar o dono da senha)
Problemas	- Não evita todos os problemas decorrentes da captura de senhas trocadas entre eles - Tipicamente não permite autenticação mútua - As entidades precisam de saber que senhas devem usar em diferentes ocasiões. Implica uma forma de sincronização. - As pessoas podem precisar de recursos extras para manter ou gerir senhas descartáveis.

<u>RSA SecurID</u>

O RSA SecurID é um sistema de autenticação com senhas descartáveis que usa chaves secretas, partilhadas entre autenticador e autenticado. O autenticado guarda a chave num equipamento próprio, que a usa para produzir senhas descartáveis num ritmo fixo.

- Equipamento de autenticação pessoal
- Geram um número único a uma taxa fixa (normalmente de um em um minuto, associado a uma pessoa)
- Não realiza autenticação mútua
- Autenticação com senhas únicas
  - uma pessoa gera um OTP combinando o seu userID com o número apresentado no equipamento
  - um RSA ACE Server faz o mesmo, dado o userID e verifica a igualdade
  - robusto contra ataques de dicionários - pois as chaves não são escolhidas

- Aproximação <u>Desafio-Resposta</u>

Funcionamento	- O autenticador fornece um desafio - A entidade a ser autenticada transforma o desafio usando as suas credenciais de autenticação - O resultado é enviado para o autenticador - O autenticador verifica o resultado, produzindo um resultado semelhante e verifica a igualdade
Vantagens	- As credenciais de autenticação não são expostas
Problemas	- Ataques com dicionários autónomos usando pares desafio-resposta.

- Aproximação Desafio-Resposta com Smartcards

Credenciais de Autenticação	- Smartcard - A chave privada nele guardada e o pin de acesso à chave privada
O autenticador sabe	- A chave pública correspondente
Protocolo	- O autenticador gera um desafio aleatório - O dono do smartcard cifra o desafio com a sua chave privada - O autenticador decifra o resultado com a chave pública, se o resultado for igual ao desafio, a autenticação teve sucesso.

- Aproximação Desafio-Resposta com Senha Memorizada

Credenciais de Autenticação	- Senha selecionada pelo utente
O autenticador sabe	- Uma transformação da senha
Protocolo	- O autenticador gera um desafio aleatório - O utente calcula uma transformação do desafio e da senha resposta = síntese (desafio, senha) - O autenticador faz o mesmo ou o inverso, se os resultados forem iguais, a autenticação teve sucesso

Caso de Estudo: S/Key

- Credenciais de autenticação: senha
- O autenticador sabe:
  - A última chave única (OTP)
  - O índice da última OTP usada
  - Uma semente (ou raíz) de todas as
- Preparação do autenticador:
  - O autenticador define uma semente aleatória
  - A pessoa gera a OTP inicial
  - O autenticador guarda a semente, o *n(o índice)* e OTP*n* como elementos de validação da autenticidade.
- Não pode ser adaptado para usar pares de chaves assimétricos com credências
- A sua principal vulnerabilidade está no facto de não facultar autenticação mútua, uma vez que o autenticador não consegue ser autenticado. Assim, um utente pode ser iludido e iniciar processos de autenticação com autenticadores falsos, facultando-lhes senhas descartáveis que poderão usar para personificar a vítima.

Caso de Estudo: PAP, CHAP e MS-CHAP

- Protocolos usados com PPP (Point-to-Point Protocol)
  - Autenticação unidirecional: Apenas o cliente se autentica, o autenticador não se autentica
- PAP (PPP Authentication Protocol)
  - Apresentação simples de um par UID/Senha
  - Transmissão (insegura) da senha em claro
- CHAP (Challenge - response Authentication Protocol) - Protocolo Desafio-Resposta
  - O autenticador pode requerer a autenticação em qualquer instante
  - versão 2: autenticação bidirecional (autenticação mútua)
- MS-CHAP (Microsoft CHAP)
  - Autenticação mútua
  - As senhas podem ser alteradas

- Aproximação Desafio-Resposta com chave partilhada

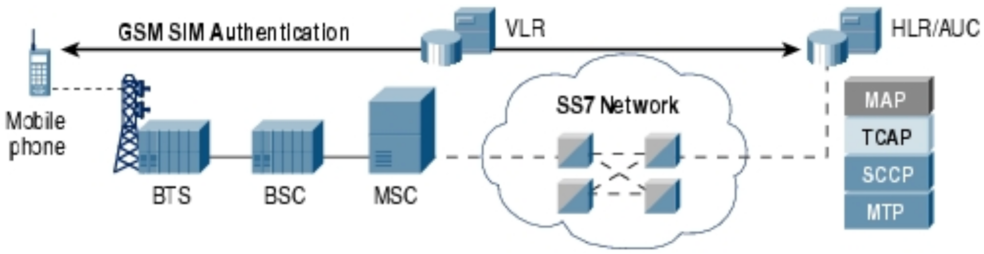
Uma solução para problemas com ataques consiste na substituição de uma senha memorizável por uma chave secreta, guardada de uma qualquer forma mas não memorizada. O facto de não ter de ser memorizável tem como vantagem o facto de não precisar de ser escolhida pelos utentes, podendo ser gerada aleatoriamente.
Assim, usa uma chave assimétrica criptográfica partilhada em vez de uma senha o que torna mais robusto contra ataques de dicionário e requer um dispositivo para guardar a chave.

- Não implica que os autenticadores protejam as credenciais de autenticação dos seus clientes.

Caso de Estudo: GSM

Nas redes "celulares" GSM, cada cliente, designado por um subscritor, possui um smartcard com um módulo SIM (Subscriber Identification Module). Um módulo SIM é uma componente da arquitetura de autenticação do GSM que é responsável pelo armazenamento, proteção e exploração de uma chave secreta de autenticação do subscritor titular. Na prática os módulos SIM são concretizados por smartcards de reduzida dimensão que são colocados no interior dos telefones.
O processo de autenticação consiste num protocolo desafio-resposta com chave secreta partilhada.

- É imune a ataques com dicionário



Autenticação de máquinas

A autenticação de máquinas pode ser efetuada por nome ou endereço ou com chaves criptográficas.
Por nome ou endereço: nome DNS, endereço IP, endereço MAC, entre outros.
É extremamente fraco pois não existe prova criptográfica.
Com chaves criptográficas: as chaves secretas são partilhadas com interlocutores usuais. Pares de chaves assimétricas por máquina, onde chaves públicas são pré-partilhadas com interlocutores e chaves públicas certificadas por terceiros.

Autenticação de Serviços / Servidores

A autenticação da máquina hospedeira diz que: todos os serviços co-localizados são automaticamente e indiretamente autenticados. Existem credenciais próprias do serviço.
A autenticação é feita por chaves secretas partilhadas com clientes quando evolvem a autenticação dos clientes com as mesmas e com pares de chaves assimétricas por máquina/serviço, certificadas por terceiros ou não.

Caso de Estudo: SSL / TLS
- Protocolo de comunicação segura sobre TCP/IP
- Mecanismos de Segurança
  - Confidencialidade e integridade da comunicação
  - Autenticação de interlocutores
- Serve para garantir a negociação de uma chave de sessão entre os interlocutores
- Permite opcionalmente autenticar o cliente
- A autenticação do cliente implica uma autenticação mútua, mas o inverso não
- Permite que o servidor use chaves públicas não certificadas
- O cliente pode escolher livremente quais credenciais que usa na autenticação

Caso de Estudo: SSH
O SSH permite duas formas de autenticar os clientes: usando senhas partilhadas e usando pares de chaves assimétricas.
A primeira consiste numa exploração direta de métodos de autenticação nativos do sistema operativo do autenticador, baseados em processos elementares de apresentação direta da senha pelo cliente. No caso SSH, esta apresentação da senha não tem riscos de segurança porque a senha circula entre cliente e servidor dentro do canal de comunicação seguro e criado previamente pelo SSH.
A segunda, usando o par de chaves assimétricas para autenticar o cliente, o mesmo apenas precisa, no máximo, de saber uma senha: a que protege a sua chave privada. Se essa senha for comprometida é apenas necessário troca-la num único local: no sistema onde a chave privada está guardada. A aplicação cliente SSH, onde quer que seja usada por esse cliente, terá de ser configurada para usar a sua chave privada a partir do local onde a mesma está guardada.
Estes pares de chaves assimétricos podem ser gerados por aplicações próprias apenas para serem usados pelo SSH, mas é igualmente possível usar outros pares de chaves assimétricas geradas para outros fins.
A aplicação cliente baseada e adaptada para trabalhar com smartcards através da interface PKCS#11 do Cartão de Cidadão na qual se indicam quais as credenciais a usar para autenticação do utente (nomeadamente, um cartão com o rótulo "*CARTAO DE CIDADAO*" e umas credenciais assimétricas, cujo certificado de chave pública possui o rótulo "*CITIZEN AUTHENTICATION CERTIFICATE*").

- É vulnerável a ataques de interposição (*man in the middle*)
- Permite que os utentes se autentiquem de forma flexível
- Protege a autenticação dos clientes realizando-a no âmbito de uma comunicação segura
- Pode criar problemas de decisão aos clientes quando se mudam as credenciais dos servidores

- Gere consolas seguras sobre TCP/IP
- Inicialmente concebido para substituir o telnet
- Atualmente usada para outras aplicações: criação de túneis seguros e FTP
- Mecanismos de segurança
  - Confidencialidade e integridade da comunicação: Distribuição de chaves
  - Autenticação de interlocutores
    - Servidores / Máquinas
  - Arquitetura SOHO