Redes de confiança no InteGrade

José de Ribamar Braga Pinheiro Junior
IME/USP

Roteiro

- Segurança de Grades Computacionais
- Abordagens
- Requisitos para o Integrade
- SDSI/SPKI
- Vantagens e desvantagens
- Conclusões

Segurança de Grades

- Aspectos envolvidos:
  - Autenticação
  - Controle de Acesso
  - Integridade
  - Confidencialidade
  - Não repúdio

Segurança em Grades

- Considerações importantes:
  - Ambiente dinâmico e heterogênio
  - Usuários
    - Autenticação única
  - Aplicações
    - Não sabem onde vão executar
  - Recursos
    - Não sabem quais aplicações vão executar
  - Políticas de segurança Local

Segurança em Grades

- Considerações importantes:
  - Serviços de segurança devem focar as relações entre:
    - usuário e recurso
    - processo e recurso
    - processo e processo

Segurança em Grades - Abordagem

- Abordagem centralizada
  - facilidade na administração do sistema
  - perda desempenho
  - ponto único de vulnerabilidade e falha
- Abordagem distribuída
  - autenticação e autorização são realizadas por cada máquina
  - escalabilidade
  - dificuldade de manter coerência das políticas de autorização

Segurança em Grades - mecanismos

Mecanismo	Espaço de nomes	Autenticação	Autorização	Escalável	Interoperável	Tolerante a faltas
Kerberos	local	centralizada	descentralizada	sim	sim	—-
X.509	global	centralizada	descentralizada	sim	sim	—
SPKI/SDSI	local	descentralizada	descentralizada	sim	sim	sim
SESAME	global	centralizada	descentralizada	sim	sim	—

Segurança no InteGrade

- Requisitos considerados
  - Ausência de autoridade central
  - Proteção dos dados na maquina provedora de recursos
  - Impedir que um cedente forneça resultados falsos de computação
  - Assinatura digital das aplicações

Segurança no InteGrade

- Recursos a serem protegidos
  - Rede
  - Processador
  - Memória
  - Disco

Redes de confiança

- SPKI/SDSI
  - Implementação de um sistema de autenticação/autorização descentralizado
  - SPKI
    - Criado por Carl Elison e outros
    - um modelo de autorização simples
  - SDSI
    - Projetado no MIT por Ronald Rivest e buttler Lampson
    - infra-estrutura de chaves publicas com espaço de nome local

SPKI

- Utiliza criptossistemas de chaves públicas
- O sujeito é representado por uma chave pública e não pelo nome
- Liberdade para gerar certificados e delegar acessos
- Direitos podem ser transmitidos
- Autorizações podem ser livrevemente definidas e distribuídas
- Datas de validade são escritas nos certificados
- São representadas em *s-expression* (como em LISP)

Chaves Públicas

- Constituída por um par de chave uma pública e outra privada
- exemplo:

```
(public key
   (rsa pkcs1 md5 (e #010001#)
            (n |
ANeWQ0+7nhwMzuahgLPPMbOi6jUP0RPgZTzpLAhJ6qm/1DT1LVRYF
78izo5zJqtTCB/yYoSExEEM2e8Anx7trz+wK6U4HdBcEwexjkXXo3BM9
D433bpVm8iM61y8FMaYH743gvectGZ3BBBGNzH6KHAERXjW0te2y9
UpT1GzWart|)
   )      )
```

Nomes SDSI

- Cria uma referência amigável para as chaves públicas
- exemplo:
  - Jose possuidor da chave (K_{JOSE}) obteve de alguma forma a chave do namorado de Maria ($K_{NAMORADO}$).
  - Nome completo: K_{JOSE}'s MARIA's NAMORADO (referência para a chave pública do namorado de maria dentro do espaço de nomes de jose)

Nomes SDSI

- exemplo
  - *S-expression*:
    (name (public key (rsa pkcs1 md5 (e #010001#) (n |
    AMhMF5tkowUb4S8+RwNKuiX+vtoCeW1aGLohzRDPFZUx4SAJ3UjRs0H
    aK4cgph8F+UBcYP70en1qKDRh+55I/mQNQIH5oBah/aa4UTQze6N7eG1d
    djFfznF NWdeteIybyeggjkmVkRetzRI9xlW8v/Jwwl64lSrs5s9a4QYCoUZv|)))
    Maria Namorado))

Certificados SPKI/SDSI

- Certificado de definição de nomes
  - liga um nome local ao sujeito que se deseja identificar
- Certificado de autorização
  - define permissões que um sujeito (o emissor do certificado) delega para um outro sujeito (o sujeito do certificado).

Certificados SPKI/SDSI

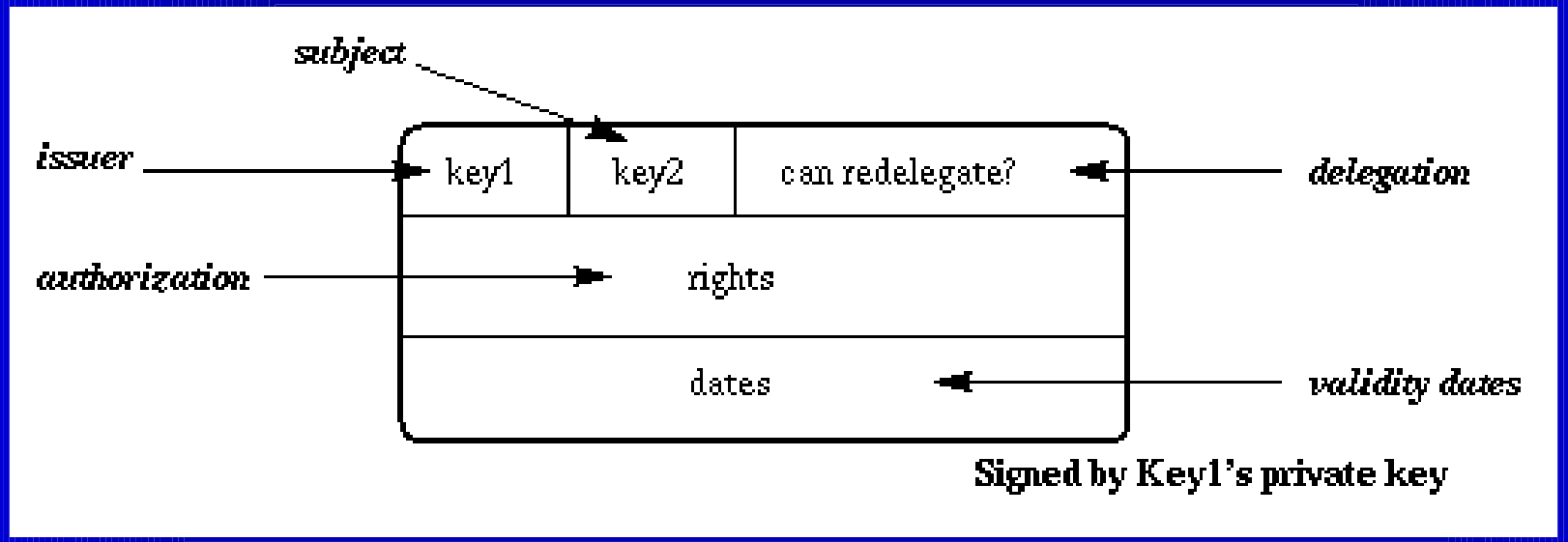
- Certificado de definição de nomes
  - são utilizados para publicar nomes locais a fim de que outros principais possam chegar à chave pública de um nome definido localmente.
  - consiste em quatro campos: (K, N, P, VS)
    - K a chave do emissor (issuer)
    - N um identificador (identifier) – Nome local que irá identificar o certificado
    - P o sujeito do certificado (subject)
    - VS uma especificação de validade (valid specification)

Certificados SPKI/SDSI

- Certificado de definição de nomes
  - *s-expression*: (cert (issuer (name K N)) (subject P) <valid>)
  - exemplos:
    - K_{JOSE} irmão ---> K_{LEO}
      - (cert (issuer (name K_{JOSE} irmã o)) (subject K_{LEO}) <valid>),
      - JOSÉ detentor da chave K_{JOSE} emitiu um certificado para seu irmão Leo detentor da chave K_{LEO}
    - K_{JOSE} sobrinhos ---> K_{LORENA}
    - K_{JOSE} sobrinhos---> K_{LEO} filhos

Certificados SPKI/SDSI

- Certificado de autorização



Cetificado SPKI

- Significado da 5-tupla
  - Issuer – Chave pública que assina o certificado
  - Subject – Sujeito que recebe o certificado
  - Delegation – Indica se é dado o direito de redelegar o certificado para outro
  - Authorization – Define os direitos de acesso definido para este certificado
  - Validaty dates – período de validade do certificado

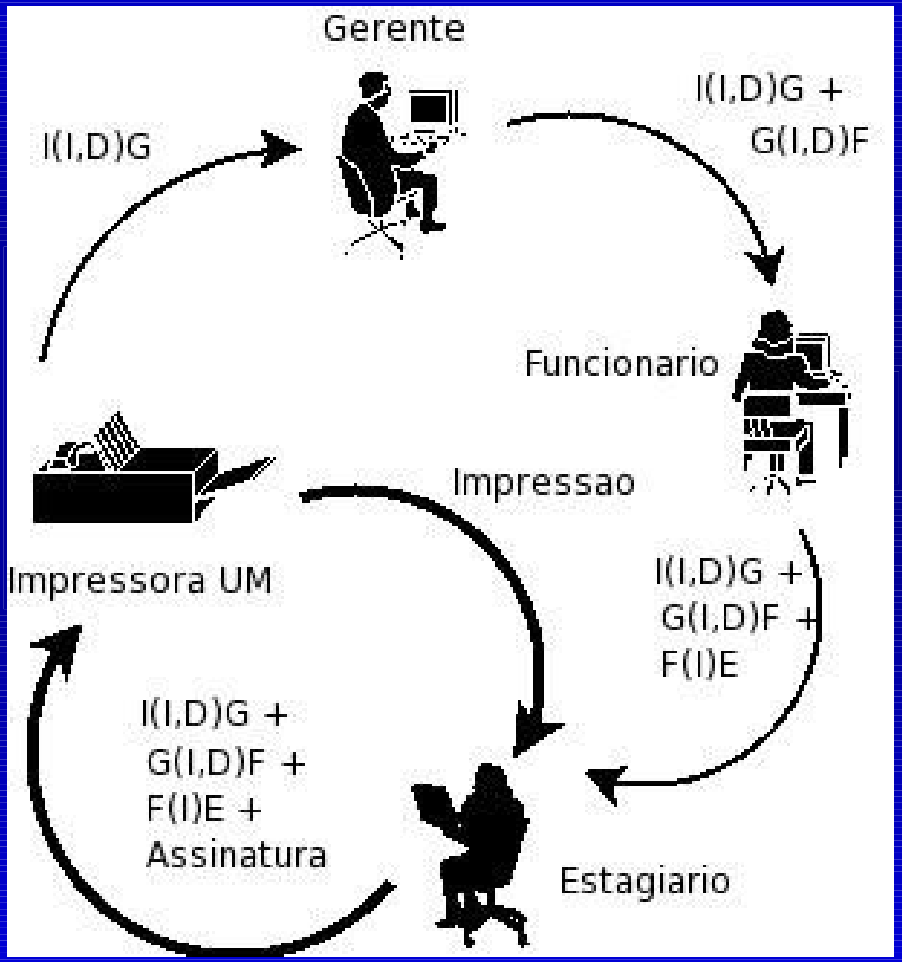
Cetificados SPKI

- Exemplo:

(cert
(issuer (public key (rsa pkcs1 md5 (e #010001#) (n |
AMhMF5tkowUb4S8+RwNKuiX+vtoCeW1aGLohzRDPFZUx4SAJ3UjRs0HaK4cg
ph8F+UBcYP70en1qKDRh+55l/mQNQIH5oBah/aa4UTQze6N7eG1ddjFfznFNWd
etelyby eggjkmVkRetzRl9xlW8v/Jwwl64lSrs5s9a4QYCoUZv|)))))
(subject (name (public key (rsa pkcs1 md5 (e #010001#) (n |
AmhMF5tkowUb4S8+RwNKuiX+vtoCeW1aGLohzRDPFZUx4SAJ3UjRs0HaK4cg
ph8F+UBcYP70en1qKDRh+55l/mQNQIH5oBah/aa4UTQze6N7eG1ddjFfznFNWd
ete lybyeggjkmVkRetzRl9xlW8v/Jwwl64lSrs5s9a4QYCoUZv|))) Doutorandos))
(propagate)
(tag rw dir /home/pub))

Cetificados SPKI

- exemplo:



Redução de Certificados

- Exemplo:
  - Cert1 e Cert2, compostos pelas quintuplas (E1,S1,A1,D1,V1) e (E2,S2,A2,D2,V2), respectivamente, formam uma cadeia de autorização se as seguintes condições forem verdadeiras:
    - S1 = E2 e D1 = true, ou seja, o sujeito do certificado Cert1 dever ser o emissor do certificado Cert2
    - O campo de delegaçãoao D1 dever estar ativo, permitindo assim a sua delegação

Redução de Certificados

- Exemplo:
  - O emissor E1, depois de garantir a autoridade da cadeia que lhe fora dada, emite um novo certificado de autorização diretamente para o sujeito S2.
  - O campo de autorização deste novo certificado ser formado através da interseção, string a string, dos campos de autorização A1 e A2.
  - Da mesma forma, o campo de validade ser formado através da intersecção dos campos de validade V1 e V2.
  - Resultando assim no certificado Cert3, composto pela quintupla (E1,S3,(A1 \ A2),D3,(V 1 \ V 2)).

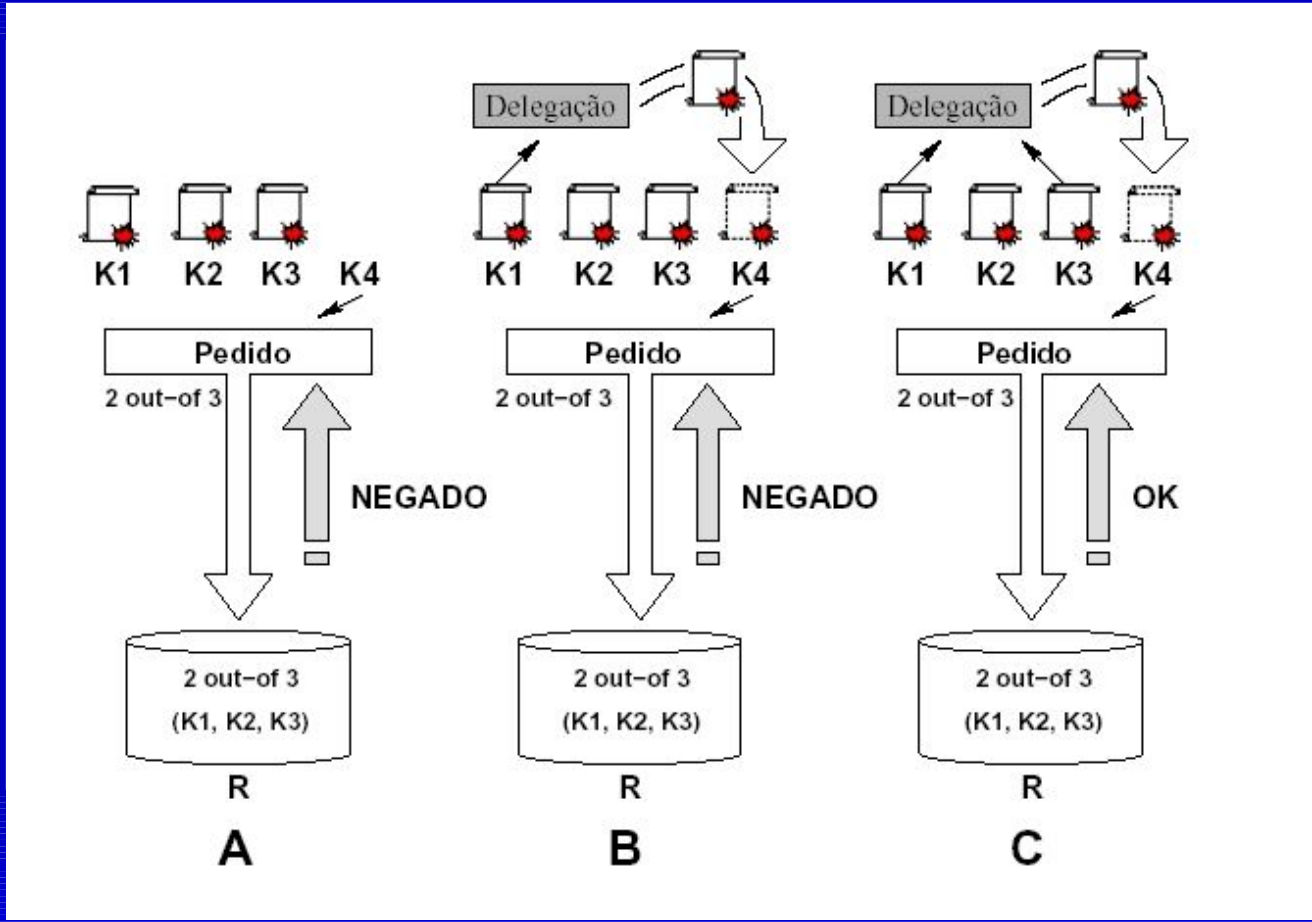
Tolerância a falhas

- Threshold Subjects
- K dentre N sujeitos devem assinar um pedido ou uma delegação, para que o mesmo seja válido.
- Os sujeitos podem ser uma chave pública, um nome ou ainda um grupo.

Tolerância a falhas

- (k of n "2" "3"
  (public key (rsa pkcs1 md5 (e #010001#)
  (n |ANd+qGqLehQ35rlRlJlJ2I0rLLb/xY6TOgfYO7zGAubbK8Cp81y/k4i5N8QNEHJM7+q/OpkfYQdKSx/gHXNsIcbaamBzkJb7Pl2DWo+Ld8ekc7AZgHqs0Riyn6KPY6Ljp1lfPaWUehXxZ27rE/zhHXcj4P6D3FdjO/eEUy7IEDz|)))
  (public key (rsa pkcs1 md5 (e #010001#)
  (n |AmhMF5tkowUb4S8+RwNKuiX+vtoCeW1aGLohzRDPFZUx4SAJ3UjRs0HaK4cgph8F+UBcYP70en1qKDRh+55I/mQNQIH5oBah/aa4UTQze6N7eG1ddjFfznFNWdeteIybyeggjkmVkRetzRl9xlW8v/Jwwl64lSrs5s9a4QYCoUZv|)))
  (public key (rsa pkcs1 md5 (e #010001#) (n |AKhVyMWvoCZdaXJm/1wbnaC6SYH4G2B11Qmae0OGeVBtqV2/1MXohcd205Xc4Y89IKeJmZbFMQ+df+riwwRaMacO4zWbsNfYxK+hjxI8QBz5qgm5RJ1prV9o23z2pCqfcucSIxLUjzYn8vgxrjHTfoRCxDxOYKYMNcpWz81KT2dp|)))))

Tolerância a falhas



Vantagens e Desvantagens

- Vantagens
  - Certificados podem ser publicados e são de fácil manutenção
  - O uso de certificados economizam espaço em disco e de processamento distribuindo as tarefas para os usuários
  - Os certificados podem ser usados para subsitituir a autenticação tradicional
  - Se o certificado expira ou é revogado o resto continuará valendo

Vantagens e Desvantagens

- Desvantagens
  - Cadeias de certificados podem ser longas demais dificultando seu gerenciamento
  - Não é possível controlar a redelegação de um certificado

Revisando os Requisitos considerados

- Ausência de autoridade central
- Proteção dos dados na maquina provedora de recursos
- Impedir que um cedente forneça resultados falsos de computação
- Assinatura digital das aplicações

Conclusões

- O uso de redes de confiança permite a descentralização da segurança
- Ele permite resolver a maioria dos Requisitos do InteGrade
- O problema de busca para gerenciamento de chaves deve ser resolvido pelo próprio InteGrade.

Perguntas

?