ICP - Infra-estrutura de Chave Pública

Prof. Michael Anthony Stanton

UFF

michael@ic.uff.br

Componentes da ICG

- Certificados X.509, perfis, PKCS
- CAs e CRLs, RAs, ARLs
- políticas e práticas
- modelos de confiança
- produtos viáveis que geram, invalidam, gerenciam, e armazenam chaves e certs

Por quê a ICG é Importante

- É hora de pôr pessoas e máquinas na rede de maneira segura
- Primeira vez que existe uma ferramenta de segurança/autenticação escalável
- Complexidade causada pelo mundo real: mobilidade, formalizácão de confiança, infra-estructur inadequada, etc.

Desenvolvimento geral

- Empresas utilizam instalações internas, “hard-coded”
- Governo Federal (EUA) desenvolve instalação externa, de uso e interoperabilidade limitados
- Outros governos desenvolvem serviços nationais centralizados

Ensino Superior e Pesquisa (ES&P)

- Algumas universidades implantaram infra-estrutura limitada para aplicações específicas, geralmente via WWW - MIT,Stanford
- Uso de “junk certs” em alguns casos
- Projeto piloto de bibliotecas (DLF) - UCOP, Columbia
- CREN instalou uma CA de mais alto nível
- Educause está trabalhando em políticas

ES&P e ICG

- estruturas gerenciais frouxamente acopladas
- pessoas geralmente pertencem a várias comunidades de interesse
- ainda não tem muito apela para o mercado comercial

Por quê ES&P é importante?

- ES&P um campo de provas escalável, e um precursor do mercado
- Base de usuários educados
- Missão de pesquisa implica em lidar com tópicos avançados
- Fácil avaliar impacto social
- Nesta área, nossas características de múltiplos papéis presage the future

Usos Funcionais de Certificados

- Ficha para accesso (p.ex. Bibliotecas)
- Autenticação de sessão (tempo real)
- Autorização (nativa, ou portador de atributos)
- Criptografia de correio ou arquivos (S/MIME)
- Integridade e confidencialidade de sessão (p.ex. SSL, TLS, IPSEC)
- Objetos assinados digitalmente

Requisitos de suporte técnico - 1

- Arquivamento
- “Escrow” (depósito seguro)
- CRL
- Renovação automática de cert
- Mobilidade
- Funcionamento interativo ou não

Requisitos de suporte técnico - 2

- Não repudiação
- NTP
- Diretórios
- Identificadores
- Carga de processamento

Uma matriz em desenvolvimento

- Linhas são usos funcionais
- Colunas são requisitos técnicos
- Entradas representam como o uso desejado requer componentes específicos da infra-estrutura
- Aspectos importantes de entradas incluem
  - o que precisa fazer fazer direito
  - como pode ser feito de modo errado
  - necessidade de interoperar

Três Contextos Críticos

- Se funciona para o usuário final
- Se funciona para o empreendimento
- Se funciona para a comunidade de interesse

X.509 e PKCS

- X.509 define certificados, modelos de confiança, e usos
- PKCS define detalhes críticos da implementação - p.ex. escolha específica de algoritmo criptográfico, formatos de chave para transportabilidade, etc.
- PKCS é orientado a RSA; patentes já caducaram

Camadas de isolamento

- Para separar programadores de aplicação do tumulto na camada de segurança
- Permite que provedores de serviço mudem as implementações do serviço
- Implementadas como APIs e bibliotecas associadas
- GSSAPI, GAAAPI, MS CryptoAPI (versão 2), Novell NICI, Java

Questões Abertas em ICP de ES&P - I

- perfis - gabaritos de certificados comuns para usos acadêmicos padrão
- políticas - enunciando eligibilidades, papeis e responsibilidades
- práticas - convenções específicas de operação padronizadas
- modelos de confiança - hierarquia, ponte, malha; dentro e fora do campus

Questões Abertas em ICP de ES&P - II

- redução de riscos - minimizar conseqüências
- CRLs - onde guardar, freqüência de divulgação
- produtos viáveis - custo, flexível, mobilidade, integração com bases embutidas, alternativas de domínio público/fonte aberto
- oportunidades para pesquisa - apls que usam políticas