Securing Android-Powered Mobile Devices Using SELinux

Inspiração: Shabtai et al, in Security & Privacy, IEEE

Claudio André

Redes Móveis

Idéia central

- Usar um OS de uso geral como Linux pode abrir brechas de segurança.
- Processos centrais rodam como root.
- Brechas nestes processos podem comprometer todo o sistema.
- Aplicabilidade do SELinux neste contexto.

Redes Móveis

SELinux - Security-Enhanced Linux

- Desenvolvido na NSA ("National Security Agency").
- Estabelecer uma política de segurança sobre os processos e objetos do sistema.
- Implementação MAC.

Redes Móveis

SELinux - Security-Enhanced Linux

- MAC ("Mandatory Access Control"). Obrigatório, requerido.
- DAC ("Discretionary Access Control") Discrição ou discernimento de alguém.

Redes Móveis

Características

- Controle sobre inicialização, herança e execução dos programas.
- Controle sobre arquivos, diretórios, descritores de arquivos.
- Controle sobre sockets, mensagens, interfaces de rede.

Redes Móveis

AppArmor - Application Armor (armadura)

- Era mantido pela Novell.
- 2 anos atrás Novell “ripped off the team”.
- Seus defensores alegam que é mais fácil e simples de utilizar.
- É independente do FS.

Redes Móveis

SELinux - Security-Enhanced Linux

- Usa LSM (Linux Security Modules).
- Integrado na árvore 2.6.
- Limita ou bloqueia o dano.
- Nada de instalar anti-isto ou anti-aquilo no telefone.

Redes Móveis

SELinux - Security-Enhanced Linux

- Outros trabalhos verificaram a viabilidade do uso em um dispositivo “mais pobre em recursos”.
- Resultado (melhorias) aplicado na árvore 2.6.

Redes Móveis

Cenários

- Proteger processos;
- Proteger arquivos;
- Proteger o sistema.

Redes Móveis

Desafios

- Kernel Android não suporta SELinux;
- Não há como carregar politicas;
- Emagrecer a politica padrão SELinux;
- Tratar atributos estendidos;
- Aplicar SELinux ao Dalvik.

Redes Móveis

Resultados

- Impacto IO - desprezível;
- Memória - desprezível;
- Tamanho da imagem 7%;
- Alguma perda onde algo acontece (abrir, fechar, ler, gravar);

Obrigado

Claudio André