FIDES: An Advanced Chip Multiprocessor Platform for Secure Next Generation Mobile Terminals

Inoue, H., Sakai, J., Torii, S., and Edahiro, M. 2008. FIDES: An advanced chip multiprocessor platform for secure next generation mobile terminals. *Trans. on Embedded Computing Sys.* 8, 1 (Dec. 2008), 1-16. DOI= http://doi.acm.org/10.1145/1457246.1457247

César Christian Castelo Fernández, RA: 089028

Este artigo apresenta uma nova tecnologia para o melhoramento da segurança nos terminais embutidos que tem S.O. Linux. Esta tecnologia, baseada na separação física dos domínios, é chamada de FIDES, e tem uma arquitetura multiprocessador com três domínios: Base Domain (funções básicas como Navegador de Internet, e-mail, etc), Trusted Domain (onde são executadas as aplicações validadas por algum provedor de telecomunicações) e Untrusted Domain (onde são executadas as aplicações não validadas). Estes domínios estão localizados em diferentes processadores físicamente. Além desta separação também é preciso ter uma lógica de separação ao nível do processador e ter componentes especiais do Sistema Operacional (SELinux, XIP e control para IDC).

Lógica de Separação ao nível do processador: Esta separação é feita no sistema de barramento usando uma matriz de acesso entre o barramento mestre e o barramento escravo. A sua função é decidir se um acesso de um barramento mestre a um barramento escravo pode ser feito. Esta matriz apenas pode ser definida pelo processador no domínio base.

Execution in Place (XIP): Quase sempre, os dados de leitura são gravados na ROM para precisar de menos RAM, e também, para reduzir o tempo de carregamento do sistema. Estes dados são executados na própria ROM, por isso são chamados de XIP. Atualmente a tecnologia XIP está implementada apenas para um processador. Os autores do artigo desenvolveram uma nova tecnologia XIP para arquiteturas multiprocessador.

Security-Enhanced Linux (SELinux): Nos sistemas embutidos sempre há políticas para controlar os direitos de acesso dos processos, as quais dizem as chamadas de sistema que o processo pode executar. O problema é que fazem com que o tempo de execução das chamadas seja maior; é por isso que o SELinux divide uma política em três, dependendo do domínio do processo: não estrita para o Domínio Base, com algumas restições para o Domínio Trusted, e com muitas restições para o Domínio Untrusted.

Dynamic Access Control for Inter-Domain Communication (IDC): Quando as aplicações têm comunicação entre domínios é preciso controlá-las para que não possam quebrar a segurança. Os autores desenvolveram um sistema dinâmico de controle de acesso, que pode mudar dinâmicamente os direitos de acesso dos processos quando são detectados ataques maliciosos dos processos ou acessos não permitidos na memoria. Os métodos usados para IDC são arquivos e sockets. A única desvantagem é que é muito dificil saber quando deve retornar ao direito de acesso original num processo.

Avaliação: É usado um processador MP211 com 3 processadores ARM, no qual, mostrou ter melhor desempenho e menor disipação de energía do que um processador único com maior velocidade. Foram feitas provas qualitativas com uma plataforma que apenas faz separação ao nivel de processos, e outra que também faz separação ao nivel de OS. O FIDES mostrou ter maior segurança para dispositivos móveis. Sobre a lógica de separação de barramentos, são precisos menos do que 20 K transistores; o barramento apenas precisa de uma área menor do que 0.026 mm^2; o consumo de energia não é problema. Enquanto aos kernels XIP, estes podem diminuir os requerimentos de memoria em um 182% em comparação com sistemas sem XIP. Enquanto que, a separação das políticas dos processos, por sua vez, deve ter um efeito positivo, isso se deve ao tempo de ligamento no sistema seja 2.1 vezes mais rápido; a relação entre o número de políticas e o tempo é linear. Para o controle dinâmico de acesso, na média há 100 chamadas de sistema. O excesso de processamento, quando foram mudados os direitos de acesso, foi de apenas 4%.

Concluções:
O FIDES oferece uma excelente plataforma para dispositivos móveis usando Linux.
A principal característica do FIDES é a sua grande segurança baseada na separação nos processos, no OS e no processador. As tecnologias usadas, SELinux, XIP e control no IDC não são dificeis de implemetar e tem bons resultados.
O FIDES é mais seguro do que outras plataformas com separação do software e hardware.
Trabalho futuro: segurança em sistemas multiprocessador simétricos, trabalhos com criptografia, integridade de sistemas de balanceamento de carga quando o número de aplicações simultâneas seja maior.