Resenha da Unidade 8 - Barramentos e interconexão.

Artigos de Referência para a resenha:

Gallo12, R., & Kawakami, H. (2011). SCuP-Secure Cryptographic Microprocessor. Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais.
Retrieved from http://www.ppgee.unb.br/sbseg2011/resources/downloads/sbseg/90828.pdf

SILVA, Yamar Aires da. Estudo e proposta de um novo documento de identificação eletrônica (e-ID) para o Brasil. 2007. xx, 147 f. Dissertação (Mestrado em Engenharia Elétrica)-Universidade de Brasília, Brasília, 2007.

Piccolo, Lara Schibelsky Godoy. Arquitetura do Set-top Box para TV Digital Interativa. Instituto de Computação – Unicamp, 2006. Disponível em http://www.ic.unicamp.br/~rodolfo/Cursos/mo401/2s2005/Trabalho/039632-settopbox.pdf

Elevando o nível de proteção...

A Arquitetura de Von Neumann, na qual os nossos dispositivos digitais dotados de processamento se baseiam, não seria tão eficiente nos dias de hoje sem o avanço dos barramentos. Ao pensarmos, em alto nível, em uma CPU executando instruções sobre dados, os quais foram obtidos, ambos, na memória principal, em um determinado instante e por um determinado motivo, pode nos influenciar a crermos que a velocidade da operação dependerá tão somente do clock da CPU, ou, ainda pior, do espaço de armazenamento da nossa memória principal. Mas, na realidade, o gargalo está em um nível mais baixo.

A Unidade de Controle (UC), naturalmente, precisa de um meio para “obter” dados da memória. Além disso, também é necessário um canal de sinalização, informando que o acesso será realizado. Não satisfeito, nosso inseparável amigo também requer outro meio para informar o endereço de memória que contém os dados/instruções necessários. Esses meios

são, respectivamente, o Barramento de Dados, Barramento de Controle e o Barramento de Endereço de Memória. Nos processadores Intel, o barramento de dados passou a ter 64bits a sua disposição, um pouco antes que o barramento de memória, que atualmente também conta com 64bits em praticamente todos os novos processadores x86. Mas, qual a relação desses barramentos com “proteção/segurança”?

O Barramento de Dados e o Barramento de Endereço de Memória são, ambos, um canal entre a Memória Principal(MP) e o Registradores de Dados de Memória(RDM) e Registrador de Endereço de Memória(REM). Assim, embora o Barramento de Memória seja unidirecional (apenas a UC aciona a MP, e não o contrário), não ocorre o mesmo com o Barramento de Dados, no qual tanto a UC quanto a MP podem “depositar” dados/instruções. Essa interconexão entre a MP e o Registrador de Dados (ou o Acumulador) é análoga
a
interconexão entre dois dispositivos em uma Rede de Computadores, na qual fica mais fácil vislumbrarmos a necessidade de um Firewall neste canal.

O firewall é o elemento responsável por analisar o conteúdo dos dados que trafegam em um canal, “fazendo a separação entre o joio e o trigo”. Dessa forma, no contexto dos Barramentos de Interconexão em Chips, os projetistas decidiram que, em certos tipos de chips, era necessário um tipo de firewall no hardware, a fim de evitar que instruções/dados maliciosas possam passar da MP para o RDM(ou outros registrados, a depender da arquitetura) e, com isso, serem executadas pelo processador.

Conforme pode ser visto nas referências desse texto, várias são as abordagens para se conseguir um efeito de Firewall na interconexão de chips. Em smartcards mais antigos, por exemplo, pode ser exigir que a aplicação realize um processo de autenticação antes de poder carregar instruções/dados na MP. Ou seja, o firewall não está, de fato, na interconexão(
barramento) entre a MP e o RDM, mas antes da MP. Essa abordagem, de fato, não é a mais segura, uma vez que uma aplicação
após
autenticada poderá depositar quaisquer tipos de instruções na MP(inclusive maliciosas), as quais, posteriormente, serão carregadas para os Registradores e executadas! Apesar de não ser ideal, é ainda melhor do que no caso de alguns Set-top Box para TVs digitais, que, embora tenham barramentos velozes, que interligam inclusive o controle remoto do usuário diretamente no barramento de dados da
CPU(
pelo menos é
o
que disseram o pessoal do artigo), não dispõem de um método para filtrar o conteúdo.

Por outro lado, smartcards mais elaborados, possuem um eficiente Firewall, que recebem o sugestivo nome de Firewall de Hardware (HWF). O HWF age controlando o acesso entre os mestres de barramento e os periféricos (repare que, neste caso, a proteção vai além de apenas a interconexão entre RDM e a MP). Dessa forma, pode-se evitar que qualquer periférico que tenha sido comprometido (como, por exemplo, o teclado de uma urna de votação eletrônica) possa ter acesso aos barramentos de conexão com dados em claro. Com uma aplicação corretamente escrita para essa arquitetura, o voto eletrônico é capturado e criptografado pelo processador. Caso a informação tente passar pelo barramento em claro (sem a criptografia), será impedida pelo HWF. Ao mesmo tempo em que, se um periférico tentar acessar o dado em claro, também poderá ser impedido. Propostas para Documentos de
Identificação Eletrônicas (e-ID)
seguem a mesma proposta,
implemetando
um HWF nos níveis mais baixos, a fim de evitar comprometimentos no chip.

Embora essa sofisticação seja incrivelmente funcional, não existem muitos relatos na literatura sobre incidentes de segurança causados pela falta de um HWF na interconexão do chip (pelo menos por enquanto). Ou, em outras palavras, em um nível tão baixo. Algo que as pesquisas não revelaram foi que, de fato, as maiores fraudes quase sempre ocorrem no Mais Alto Nível, l iteralmente
. E isso, infelizmente, está além de qualquer
chip(
eletrônico).
;)