TECNOLOGIAS PARA PREVENÇÃO DE VULNERABILIDADE EM PROCESSADORES

OTTO, Mauricio Silveira[1]; SOARES, Rafael de Almeida[1];
POZZATTO, Maurício da Silva[1]; PEZZI, Daniel da Cunha[2]

Palavras-Chave: Processador. Segurança. Hardware. EVP.

1. Introdução

De acordo com o cenário atual, o mundo está a cada dia mais dependente dos computadores, seja para uso doméstico ou empresarial. No entanto, como descreve Niehues (2007), muitos sistemas são passíveis a falhas na segurança que podem ocasionar em muitos prejuízos a sociedade.

A segurança de sistemas é uma área informática que, segundo Soares (2000) e Da Silva (2004), envolve um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes integridade, disponibilidade, não repúdio, autenticidade e confidencialidade.

Diversas soluções de prevenção da vulnerabilidade de sistemas já foram desenvolvidas para aumentar os níveis de segurança, desde a reengenharia da análise dos quesitos de segurança até aplicações combinadas práticas por intermédio de *softwares* e *hardwares*.

Dessa forma, conforme Da Silva (2004), torna-se necessário dispor de estratégias a fim de compor uma arquitetura de segurança. Em muitos casos, aplica-se criptografia, incentivo a educação em questões de segurança, disponibilidade de tecnologia da informação com suporte a segurança, infraestrutura de gestão de segurança, disponibilidade de mecanismos de monitoramento de ataques, capacidade de alerta e ações coordenadas.

Com o objetivo de aumentar os níveis de segurança de sistemas, empresas fabricantes de processadores, como a Intel, AMD e VIA, desenvolveram recentemente tecnologias que visam proteger um computador de um erro irreversível.

Este artigo visa analisar as recentes tecnologias de prevenção de falhas baseadas em processadores, descrevendo suas características técnicas, peculiaridades e formas de atuação.

[1] Alunos do Curso de Ciência da Computação de UNICRUZ, mauriciootto@hotmail.com; rafaalmeidasoares@hotmail.com; mpozzatto@hotmail.com
[2] Professor orientador da pesquisa, danielpezzi@yahoo.com.br

2. O universo das falhas

Segundo Weber (1990), as falhas fazem parte do universo físico de um processador. Se um sistema não admitir, corrigir e alertar ao usuário sobre uma falha, ela pode se tornar um erro que faz parte do universo da informação e que pode conduzir a perda de dados.

Usuários avançados *crackers* se aproveitam dos erros e podem assumir controle sobre os comandos ou sobre os dados, implantando códigos maliciosos que podem executados em *modo kernel*, ou seja, na mesma prioridade do Sistema Operacional. Sendo assim, se tornam ameaças em potencial a segurança e a confiabilidade de um sistema.

Por outro lado, computadores de uso geral não podem admitir falhas nem erros, o que são quase inevitáveis. Por isso os sistemas devem estar preparados para tolerar estas falhas e tentar corrigi-las antes que ocorra o erro e posteriormente o defeito (WEBER, 1990).

3. Proteção por hardware em processadores

Os fabricantes de processadores, por sua vez, para evitar que falhas de segurança afetem a vida útil desses dispositivos, utilizam-se de tecnologias, em conjunto com o Sistema Operacional, de detecção e inibição de códigos maliciosos como um vírus ou cavalos de tróia.

3.1. *Enhanced Virus Protection* (EVP)

A fabricante de processadores AMD emprega o EVP, o qual atua em conjunto com certos sistemas operacionais (Windows Vista e XP SP2, Linux, Solaris, etc.), reduzindo significativamente os problemas com vírus, *worms*, cavalos de tróia e outras ameaças. Segundo AMD (2011), o EVP atua por meio de um mecanismo denominado *no execute* (NX), que rotula determinadas áreas da memória volátil como "*apenas dados*", ou seja, impede que sejam executadas operações maliciosas que possam corromper e manipular dados. Os processadores que utilizam esta tecnologia são: AMD Phenom X4 Quad-Core, AMD Athlon Dual-Core, AMD Athlon for Desktop, Mobile AMD Athlon, AMD Turion 64 X2 Dual-Core Mobile Technology e AMD Sempron.

3.2. *Execute Disable Bit* (XD)

Outro fabricante de processadores que investiu em segurança foi a Intel, que utiliza a tecnologia intitulada XD. De forma semelhante ao EVP, essa tecnologia classifica certas áreas da memória delimitando onde o código da aplicação pode e onde ele não pode ser executado. Quando algum vírus tenta inserir código malicioso, o processador desabilita sua execução, impedindo possíveis ações (INTEL, 2011).

3.3. *PadLock Security Engine*

A fabricante VIA Technologies também implementou uma tecnologia de segurança para processadores, chamada de *VIA PadLock Security Engine*, a qual tem implantado em todos os núcleos de seus processadores, visando combater principalmente as tentativas de roubos de informações.

Normalmente em processadores comuns, a criptografia é feita por meio de *software*, o que deixa os dados um tanto quanto vulneráveis a ataques. O *PadLock* implementa criptografia em *hardware*, ou seja, toda a manipulação de dados que os tornam ilegíveis aos usuários não-autorizados é feita por um circuito dentro do processador, sem necessidade de utilizar os recursos do sistema operacional, memória e *software*, fazendo com que sua utilização não tenha impacto sobre o desempenho do sistema (VIA 2011).

4. Estudo de caso

Com o intuito de avaliar a funcionalidade dos sistemas de proteção por processador foi estabelecido um estudo de caso. No experimento foram utilizadas duas ferramentas para identificação de *hardware*[3], o Sandra Lite 2011.SP4a (http://www.sisoftware.net/) e o SecurAble 1.0.2570.1 (http://www.grc.com/securable.htm). Ambas permitiram a identificação da existência de funções de segurança. Quanto ao *hardware*, testou-se três modelos de processadores utilizados nos laboratórios do Curso de Ciência da Computação da Unicruz: AMD Sempron 2.0 GHz, AMD Athlon Dual Core 2.2 GHz e INTEL Celeron 1.8 GHz.

Foram realizados testes para identificar o grau de segurança do sistema a partir da ativação dos recursos de prevenção. Para tanto, foi desativado o Antivírus Avast 6.0.1203 e aplicou-se uma bateria de testes. O primeiro teste envolveu o *EICAR - The AntiVirus Test File* (disponível em http://www.eicar.org/) – sistema que simula um vírus para testar a resistência do programa antivírus, como um falso-positivo. O EICAR não foi bloqueado por qualquer uma das técnicas de segurança por *hardware*, uma vez que não identificaram como algo prejudicial ao sistema. Além disso, foram programadas (em codificação C++) quatro ações com o propósito de travar o Sistema Operacional: a primeira sobrecarrega o Disco Rígido, a segunda sobrecarrega a memória principal, a terceira cria vários processos de si mesmo e a quarta faz muitos pedidos ao *host*. Como resultado, observou-se que todas foram bloqueadas pelo EVP e XD. Com o Antivírus Avast habilitado, a ação aconteceu do mesmo modo, sem a percepção do sistema antivírus.

Quanto a configuração, para habilitar a proteção por *hardware* nos processadores AMD bastou ativar a função de *Data Execution Prevention* (DEP) pelo Windows (suportada por Windows 2000, XP SP2, 2003, Vista e Seven e também algumas distribuições Linux, como a Red

[3] Software de diagnóstico de hardware (http://www.clubedohardware.com.br/pagina/download_hardware)

Hat Enterprise, Suse e Solaris). No Windows 7, localiza-se em Painel de Controle →Sistema e Segurança → Sistema → Configurações avançadas do sistema → Avançado → Desempenho → Configurações → Prevenção de execução de dados. Já no processador INTEL testado, é necessário ativar a função XD no *Setup* antes de habilitar o DEP via Sistema Operacional.

5. Considerações finais

Com o passar do tempo as tecnologias computacionais se aprimoram cada vez mais, e com isso aumentou também a necessidade de segurança e confiabilidade para seus usuários. O numero de empresas, instituições e grupos de trabalho que dependem da disponibilidade dos sistemas computacionais também aumentou, fazendo com que grandes empresas de *hardware* e de *software* aperfeiçoassem seus produtos, como AMD, Intel e VIA.

As tecnologias apresentadas neste artigo são fundamentais para a segurança dos sistemas, evitando invasões, roubos de informações e a indisponibilidade de sistemas. Dentre as soluções testadas, tanto o EVP quanto o XD foram eficazes na contenção de ações que poderiam causar problemas graves aos sistemas. Com isso, passaram a integrar o grupo de recursos de segurança dos laboratórios de informática do Curso de Ciência da Computação da Unicruz, que desde então utiliza EVP e XD, Deep Freeze[4] e Avast.

Por fim, é importante destacar que, para que se obtenha um nível de segurança adequada, é preciso atenção do usuário quanto a ativação do EVP, XD ou PadLock por meio do Sistema Operacional e/ou *Setup*. Além disso, o usuário deve ficar atento no momento de uma tentativa de execução de código malicioso, pois o Sistema Operacional, a partir do DEP, possibilita ao usuário autorizar ou não a continuidade de uma ação. Conclui-se então, que o uso dessas tecnologias de segurança por *hardware* são eficazes, contudo não dispensam outras medidas complementares, como antivírus, *firewall*, programas de recuperação e a adoção de práticas cuidadosas por parte dos usuários de computadores.

Referências

AMD. **AMD Technologies** <http://www.amd.com/>. Acesso em Junho de 2011.

DA SILVA, Antonio Mendes F. **Segurança da Informação: Sobre a Necessidade de Proteção de Sistemas de Informações**. Revista Espaço Acadêmico - nº 42, ISSN 1519.6186, nov. 2004.

INTEL. **Product Technologies** <http://www.intel.com/>. Acesso em junho de 2011.

MICROSOFT. **Data execution Prevention** <http://support.microsoft.com/kb/875351/pt-br>. Acesso em junho de 2011.

[4] Deep Freeze é um programa de recuperação de sistema que restaura as configurações originais do computador a cada reinicialização.

NIEHUES, Lucas Urgioni; CASAGRANDE, Rogério Antônio. **Ameaças Digitais: Um Estudo dos Riscos Envolvidos no uso da Internet, Seus Impactos e Formas de Proteção**. III Congresso Sul Catarinense de Computação: UNESC - Criciúma, 2007.

SOARES, L. F.; LEMOS, G.; COLCHER, S. **Redes de Computadores - das LANs, MANs e WANs ` as Redes ATM**. 2ª ed., Rio de Janeiro: Campus, 2000.

VIA. **VIA PadLock Security Initiative**. <http://www.via.com.tw/>. Acesso em junho de 2011.

WEBER, Raul Fernando. **Arquitetura de Computadores Pessoais**. Porto Alegre: Sagra Luzzatto, 2000.