(Resumo) i-NVMM: A Secure Non-Volatile Main Memory System with Incremental Encryption

Siddhartha Chhabra and Yan Solihin. 2011. i-NVMM: a secure non-volatile main memory system with incremental encryption. In Proceedings of the 38th annual international symposium on Computer architecture (ISCA '11). ACM, New York, NY, USA, 177-188.
(artigo original)
Murilo Adriano Vasconcelos RA: 134072 (resumo)

***Resumo*—Esse artigo se trata de um modelo para a criptografia de dados contidos em memória principal não-volátil (em inglês - *non-volatile main memory system* ou *NVMM*) por motivos de segurança. Isso porquê NVMMs sofrem de uma vulnerabilidade de segurança onde a informação contida nelas não é perdida quando o sistema é desligado, tornando possível um acesso físico ao sistema com objetivo de extrair informações sensíveis da memória. Para isso os autores introduzem uma técnica de criptografia incremental chamada i-NVMM, onde a maior parte da memória fica criptografada e apenas uma pequena fatia da memória permanece não-criptografada conforme uma predição realizada se o dado será utilizado ou não pelo processador. Quando o sistema é desligado, somente a parte não-criptografada precisa ser criptografada.**

I. Motivação

A motivação na criptografia incremental é a observação de que o **conjunto de trabalho** de uma aplicação (páginas de memória que uma aplicação está usando ativamente) é muito menor que o **conjunto residente** (todas as páginas de memória pertencentes à aplicação). Identificando o conjunto de trabalho de uma aplicação e criptografando o restante do conjunto residente, o método i-NVMM mantém a maioria da memória principal criptografada sem penalizar muito a aplicação, implicando assim em um pequeno tempo de espera após o desligamento do sistema para a conclusão da criptografia dos dados.

II. Métodos

O i-NVMM insere um preditor para detectar páginas "inertes". Essa predição é realizada varrendo as páginas da memória principal periodicamente para identificar as páginas que não foram usadas há algum tempo. Quando essas páginas são identificadas, elas são criptografadas em um motor de criptografia localizado no módulo de memória. Esse processo de criptografia é realizado por completo pelo módulo de memória para que o processo não seja dependente do conjuntos de instruções de um processador (ISA), uma vez que as NVMM devem ser compatíveis com uma ampla variedade de plataformas.

Como o i-NVMM identifica as páginas inertes e as critografa previamente sem esperar que o sistema seja desligado, a janela de vulnerabilidade, que é o período em que os ataques podem acontecer com o sistema desligado, é diminuída significativamente.

Para que o processo de criptografia incremental não onere muito o tempo de processamento, é necessário que a predição seja razoável, pois no caso de *misprediction*, uma página que está criptografada terá que ser descriptografada antes de ser usada pelo processador novamente. Outra ponto é que idealmente, uma grande parte da memória deve estar criptografada (alta cobertura) para que a janela de vulnerabilidade seja pequena. Assim os autores encontram experimentalmente um intervalo de varredura por página de inertes de 5 bilhões de ciclos e um limiar de inércia de 1 bilhão de ciclos (isso é, se uma página não foi acessada nos últimos 1B ciclos, ela é considerada inerte).

III. Arquitetura

Para fazer a predição de páginas inertes, o i-NVMM mantém o *status* de cada página da memória. Por razões de desempenho, os autores escolheram o tamanho de página de 4KB. O *status* de cada página é armazenado em um componente chamado *Page Status Table* - PST que é composto pelos seguintes campos:

- **EncStatus**: 1-bit que diz se a página está criptografada ou não;
- **LastAcc**: o tempo do último acesso à página;
- **NumAcc**: o número de vezes em que a página foi acessada;
- **NextPage**: a próxima página que foi acessada após essa, e
- **Pending**: 1-bit que diz se a página está pendente para criptografia/descriptografia.

O campo *LastAcc* é utilizado para checar se a página deve ser marcada como inerte ou não. Já o campo *NumAcc* é utilizado para checar se uma página criptografada deve ser mandada para uma fila de descripografia (*misprediction*).

IV. Conclusão e Resultados

O artigo apresentou um modelo de criptografia incremental para memórias principais não-voláteis. Pelos experimentos apresentados (ver artigo completo), esse modelo se não mostrou oneroso quanto ao tempo de acesso à memória. O processo de criptografia é auto-contido no módulo de memória, ou seja, não depende de ISA específico. Na média, cerca de 78% da memória permanece criptografada, o que resulta em um processo de criptografia após o desligamento do sistema de 5 segundos, o que é plausível uma vez que se assemelha ao tempo de retenção das DRAMs atuais. Finalmente, segundo os experimentos realizados pelos autores, o i-NVMM adiciona uma média de apenas 3.7% no tempo total de execução e usa em média 5.1% mais energia e tem um impacto insignificante na escrita.