DETECÇÃO E EXTRAÇÃO DE ASSINATURAS DE CONSUMO DE ENERGIA EM ARQUITETURAS CRIPTOGRÁFICAS COM PIPELINE DE EXECUÇÃO

PAULO HENRIQUE MARTINS; RAFAEL IANKOWSKI SOARES[2]

[1]*Universidade Federal de Pelotas 1 –phmartins@inf.ufpel.edu.br 1*
[2]*Universidade Federal de Pelotas – rafael.soares@inf.ufpel.edu.br*

1. INTRODUÇÃO

A criptografia foi desenvolvida para permitir que dois entes possam se comunicar de forma sigilosa em um meio não sigiloso, modificando a informação de tal forma que terceiros não possam compreender. Sistemas embarcados modernos utilizam algoritmos criptográficos para garantir esse sigilo. Teoricamente, esses sistemas são seguros, no entanto, é possível que informações sigilosas vazem a partir de sua implementação física por meio de Ataques a Canais Laterais (do inglês, Side Channel Attacks - SCA) propostos por Kocher (Kocher, 1996). Kocher provou ser possível obter essas informações relacionando o dado processado com grandezas físicas como o consumo de potência, radiação eletromagnética no momento em que o algoritmo esta em execução.

Na literatura existem diferentes estratégias de Ataques a Canais Laterais, entre eles destaca-se um poderoso método conhecido como Análise Diferencial de Potência (do inglês, Differential Power Analysis - DPA) que é um método estatístico para analisar correlações de dados com o consumo de potência. O método consiste em analisar somente a assinatura de consumo ou também denotado como ilha síncrona neste trabalho, resultante da execução do algoritmo, o restante do traço de consumo de potência é considerado ruído. A partir dos traços referentes a execução, subconjuntos de traços são criados para computar a diferença da média de todos esses subconjuntos. Um método bastante utilizado para identificar e extrair a assinatura do consumo de energia é um limiar fixo que permite diferenciar a assinatura do ruído presente nos traços adquiridos. Neste método, amplitudes maiores que o limiar são consideradas assinaturas alvo do ataque. Por outro lado, essa técnica não é eficiente, pois qualquer ruído que ultrapasse o limiar é considerado execução, tornando a tarefa de extrair assinaturas de potência complexa. Neste contexto, este trabalho visa propor um algoritmo para detecção e extração de assinaturas de consumo de potência em arquiteturas criptográficas com pipeline de execução onde os traços de consumo de potência correspondem a execuções paralelas dos estágios do pipeline o que aumentam a complexidade da etapa de extração das assinaturas alvo.

2. METODOLOGIA

Inicialmente será realizada uma revisão e análise profundada do funcionamento das arquiteturas GALS pipeline propostas por Soares et al. em (Soares et al. 2011). Para cada implementação das arquiteturas GALS pipeline, estão disponíveis 100.000 traços de consumo de energia. Cabe ressaltar que estes traços foram obtidos por Soares et al. em (Soares, 2011), e o processo de aquisição não faz parte do escopo deste trabalho.

Uma revisão sobre técnicas de processamento digital de sinais é realizada a fim de dominar métodos que sejam úteis no processamento e identificação das

assinaturas, como por exemplo o uso de filtros. A ferramenta utilizada para o desenvolvimento deste trabalho, principalmente para processamento dos traços, é o MATLAB que possui uma biblioteca rica de funções para processamento de sinais. Portanto, será realizada um intenso estudo da ferramenta, com a finalidade de obter seu domínio.

Uma revisão do Estado da Arte referente a técnicas de identificação de assinaturas de potência, visando encontrar a que mais se adequa ao tema proposto, buscando implementar ao menos uma dessas técnicas para que sirva de comparação a técnica proposta neste trabalho. Com base nesta revisão bibliográfica, propor uma técnica que permita identificar as assinaturas alvo de ataques no contexto do problema supracitado. Em seguida, verificar o desempenho das propostas levando em conta a eficácia na identificação das extrações de assinaturas nos traços de consumo de energia disponíveis para a sua validação.

Opcionalmente, após a aplicação dos algoritmos será feito uma avaliação dos mesmos no fluxo de execução de um ataque DPA, avaliando a taxa de sucesso dos ataques sobre tais conjuntos de traços. Eventualmente, poderão ser identificadas melhorias nos métodos já existentes, a fim de obtermos um método de detecção de assinaturas de consumo de energia mais eficiente para os ataques DPA. Para a realização de testes, o algoritmo foi executado em um conjunto de 100000 traços de consumo de energia diferentes.

3. RESULTADOS E DISCUSSÃO

O algoritmo proposto consiste em percorrer o traço todo identificando as assinaturas de consumo de energia provenientes da execução do algoritmo criptográfico que na sua arquitetura estão contidas as SBOXs onde a mensagem é cifrada junto com a chave, passando por oito rodadas de SBOXs antes de obter a mensagem cifrada. Para identificar uma assinatura, o algoritmo filtra o traço para diminuir a quantidade de ruído existente, em seguida um limiar é estabelecido para detectar o inicio de uma assinatura, onde o que estiver abaixo é desconsiderado. Após a aquisição do ponto inicial, é retirado um recorte partindo deste ponto até 5000 pontos à frente do ponto inicial com a finalidade de encontrar a frequência fundamental deste recorte por meio da Transformada Rápida de Fourier, sendo assim é possível identificar onde inicia e onde termina cada rodada, possibilitando a identificação bastante precisa do inicio e fim de uma assinatura de consumo de energia composta por oito rodadas. O principal objetivo deste trabalho é extrair essas assinaturas ainda que o sistema criptográfico esteja dotado de contramedidas GALS pipeline, onde uma assinatura pode estar sobreposta a outra com frequências diferentes. O algoritmo consegue identificar se uma assinatura esta sobreposta a outra verificando se o final encontrado nesta primeira etapa esta muito distante do real, sendo assim o mesmo processo realizado na primeira é etapa é realizado a partir do final para poder extrair a assinatura que esta sobreposta. O algoritmo repete esse processo para todas as seis assinaturas existentes no traço.

Para analisar os resultados do algoritmo proposto, foi efetuada a extração pelo algoritmo em um subconjunto de 30 traços de consumo de energia, em seguida foi verificado visualmente o ponto onde se inicia e termina uma rodada e os pontos iniciais e finais encontrados pelo algoritmo para calcular a diferença do real com o encontrado pelo algoritmo, e assim encontrar a média e o desvio padrão, que podem ser encontrados na Tabela 1. Porém, ainda existem ajustes a serem feitos, para diminuir o erro. Porém, o ataque em si, não foi realizado. Após

a etapa anterior esta prevista a aplicação do algoritmo em 100000 traços de consumo de energia para extrair as assinaturas de consumo necessário para o DPA.

4. CONCLUSÕES

Analisando os resultados obtidos é possível concluir que a identificação de assinaturas de consumo de energia em uma arquitetura com processamento paralelo tal como o pipeline é uma tarefa complexa, pois quando a sobreposição de assinaturas ocorre, a definição de um ponto inicial é apenas uma estimação. Entretanto, o algoritmo proposto cumpre com sua função de encontrar os pontos iniciais e finais de todas as ilhas síncronas presentes nos traços de consumo de energia, mesmo onde ocorre a sobreposição de traços de consumo. Apesar dos resultados mostrarem que a distância entre o ponto real e o calculado pelo algoritmo são significativas, a maioria dos pontos encontrados estão próximos o suficiente para viabilização um ataque DPA.

É importante também, salientar a contribuição do trabalho no que diz respeito a traços que estão dotados de GALS pipeline de 2 ilhas síncronas onde os traços podem estar sobrepostos, que por sua vez houve uma boa taxa de identificação de tais traços e de suas rodadas. Por outro lado, existem limitações no algoritmo, não só no que se diz respeito ao limiar estabelecido, mas sim em casos onde a assinatura de consumo é excessivamente anômala.

Com uma análise mais apurada do algoritmo e do problema para o qual foi proposto, certamente existam otimizações a serem feitas com a finalidade de reduzir o tempo de execução e reduzir o caso onde as assinaturas não são identificadas.

Tabela 1 –Média e desvio padrão da diferença dos pontos finais e iniciais computados pelo algoritmo com o ponto real.

Pontos Iniciais		Pontos Finais	
Média	Desvio Padrão	Média	Desvio Padrão
193,5722222	458,5669832	-14,84444444	623,183697

5. REFERÊNCIAS BIBLIOGRÁFICAS

KOCHER, P. C. **Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems**. In: Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '96), Springer-Verlag, 1996. p.104-113.

KOCHER, P.; JAFFE, J.; JUN, B. **Differential Power Analysis**. In: Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '99). Springer-Verlag, 1999. p.388-397.

LE, T.-H. et al. **How can Signal Processing Benefit Side Channel Attacks** In: SIGNAL PROCESSING APPLICATIONS FOR PUBLIC SECURITY AND FORENSICS, 2007. SAFE '07. **Anais. . .** [S.l.: s.n.], 2007. p.1-7.

LODER, L.; SOUZA, A.; FAY, M. and SOARES, R. **Towards a Framework to Perform DPA Attacks on GALS Pipeline Architectures**, In: *Symposium on Integrated Circuits and Systems Design (SBCCI)*, Aug - Sep, 2014, pp. 1-7.