CENTRO UNIVERSITÁRIO HERMÍNIO OMETTO - FHO
Av. Maximiliano Baruto, 500 CEP 13607-339 Araras SP
Tel (19) 3543 -1439 Fax (19) 3543 -1440

Aluno: Alexandro Souza RA: 93871

Aluno: André Carneiro RA: 92854

Aluno: Elias A. da Silva RA: 92756

Aluno: Gabriel Resende RA: 94038

Aluno: Gabriel Seratti RA: 88156

Aluno: Jonas Sbarai RA: 93967

MB1 – Trabalho de Segurança em Hardware

ARARAS/SP

10/2020

CENTRO UNIVERSITÁRIO HERMÍNIO OMETTO - FHO
Av. Maximiliano Baruto, 500 CEP 13607-339 Araras SP
Tel (19) 3543 -1439 Fax (19) 3543 -1440

A – As possíveis ocorrências de violação à segurança em hardware

Para realizar um ataque violando a segurança do hardware destruindo o sistema, mesmo que tenha uma dificuldade maior na realização do mesmo, o impacto sempre será maior destruindo o sistema. Tendo em vista isso, podemos listar as seguintes ocorrências de violações:

Devemos lembrar que desde a criação da matéria prima, não podemos garantir que estamos seguros, os desenvolvedores do design podem modifica-lo sem que saibamos e com isso, não tem como descriptografar o que tem dentro do chip.

Problemas de segurança de hardware surgem de sua própria vulnerabilidade a ataques (por exemplo, ataques de canal lateral ou Trojan) em diferentes níveis (como chip ou PCB), bem como da falta de suporte robusto de hardware para software e segurança do sistema.

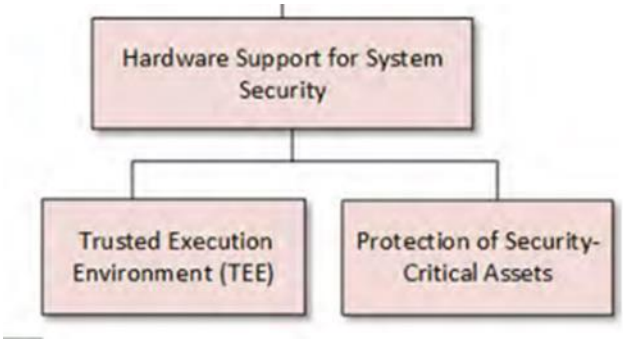
Por outro lado, os problemas de confiança de hardware surgem do envolvimento de entidades não confiáveis no ciclo de vida de um hardware, incluindo IP não confiável ou design auxiliado por computador (CAD) fornecedores de ferramentas e instalações de design, fabricação, teste ou distribuição não confiáveis. Eles são capazes de violar a confiabilidade de um sistema ou componente de hardware e podem causar desvios do comportamento funcional pretendido, desempenho ou confiabilidade.

Problemas de confiança geralmente levam à segurança preocupações, por exemplo, fornecedor de IP não confiável pode incluir implante malicioso em um design, o que pode levar a negação de serviço (DoS) ou ataques de vazamento de informações durante a operação de campo. **(1.4 livro)**

Além dessas ocorrências de violação de hardware, temos a análise de potência, que com um osciloscópio faz inúmeros cálculos, medindo energia ao longo do tempo, com a oscilação podemos detectar inúmeros ataques, senhas de criptografia, tudo. Podendo ter também uma brecha no sistema por uma injeção de falha física, com um laser isso é possível, do qual mudaria o número da memória pois mudou a instrução abrindo brecha no sistema.

Outro ponto que podemos destacar é a da violação de segurança num chip de acelerômetro que faz seus processo ficarem rápidos e como consequência é o aquecimento elevado mais que o normal, podemos atacar pelo input da configuração do FPGA alterando ou até apagando dados do chip programado, podemos usar também GPIO para tentar capturar informações de retorno para devolver com os parâmetros errados podendo levar a falhar ou até mesmo um erro fatal que faz com que o chip não tenha condições de operar.

B – Os blocos em que a execução confiável pode ser aplicada



Todos esses blocos buscam medidas para evitar ataques no hardware, realizando toda a segurança do sistema.

C – Quais as técnicas mais nocivas a este sistema?

Dado o SoC tendo uma fpga, podemos afirmar que a técnica mais nociva a ser exercida seria a do bitstream que configura o mesmo. Ou até mesmo fazendo uma engenharia reversa e poder ter controle sobre o hardware, tanto o hardware em relação a fpga, quanto a tecnologia do fpga em relação ao hardware. Sabendo qual é o hardware e obtendo o bitstream, conseguimos entender como foi programado.

CENTRO UNIVERSITÁRIO HERMÍNIO OMETTO - FHO
Av. Maximiliano Baruto, 500 CEP 13607-339 Araras SP
Tel (19) 3543 -1439 Fax (19) 3543 -1440

D – Quais os processos podem ser incorporados à montagem da placa para garantir uma melhor segurança? (Pense desde a compra de componentes, inclusive fabricação, até a montagem)

Primeiramente teríamos que ter uma relação de confiança em relação ao fornecedor do design, para que ele não tenha realizado nenhuma alteração para benefício próprio. Em relação ao pré-silical tudo deve ser confiscado devidamente, além da parte de segurança que deve ser confiscada e todos os componentes eletrônicos, corremos o risco de o dispositivo não rodar devidamente bem, com isso, o pré-silical é fundamental. Começando com a parte de validação de segurança, seria necessário fazer empiricamente e com uma maior destreza: a modelagem das ameaças, revisão de design(em possíveis causas de ataques), planos de testes de segurança e verificações da arquitetura.

Na segunda etapa, teria a revisão de código, revisão do RTL(simulação) e uma verificação formal RTL. E antes de fabricarmos para finalidade de testes, no pós-silical deverá ser realizado um pentest(inserindo falhas no hardware) e o próprio teste. Após isso, poderá ser produzido tendo com uma melhor segurança da placa.

E – Qual técnica você utilizaria para hackear a placa e qual informação você iria buscar?

Técnica do bitstream, tentaria obter o bitstream para conseguir entender como foi programado, podendo assim poder fazer a alteração que desejarmos.