Projeto UE2020

Em atendimento ao chamado da Audiência pública da UE2020 Nº 1/2019 Processo Nº 2019.00.000006505-5, gostaríamos de apresentar duas contribuições/sugestões para a especificação.

Camada de resina

Na questão de segurança física, no item 59 do documento Anexo IV – Especificações Técnicas – Segurança, entendemos que o objetivo principal da utilização de epóxi ou resinas para a segurança física da eletrônica do perímetro criptográfico é impedir que ele seja acessado acesso, fornecendo opacidade e aumentando a probabilidade de quebra do dispositivo quando ocorrem ataques agressivos, como perfuração, fresamento, moagem, fusão ou dissolução. A espessura da resina é irrelevante como um parâmetro de projeto de segurança. O importante é sua a dureza, opacidade, adesão, o preenchimento adequado dos componentes e a temperatura de serviço (transição vítrea). O teste de dureza do módulo em diversas temperaturas é o método de teste crítico padrão do setor para avaliação desta qualidade e ferramentas pontiagudas não devem ser capazes de penetrar na região limite de segurança. Devido à alta expansão térmica das resinas e a confiabilidade dos processos de aplicação fina e de alta velocidade de componentes eletrônicos sobre as placas, esses sistemas se beneficiam mais dos métodos de encapsulamento de resina fina (<1 mm), e não dos métodos de envasamento espesso. Para essas considerações práticas de implementação e segurança, recomendamos remover qualquer requisito de espessura e substituir por metodologias de teste padrão do setor para módulos criptográficos, como aqueles usados pela orientação do FIPS140-2 citada abaixo (em tradução livre):

> *Guia de Implementação do FIPS PUB 140-2 e do Programa de Validação do Módulo Criptográfico do Instituto Nacional de Padrões e Tecnologia (NIST)*
>
> *AS.05.28: (Microplaqueta Única - Níveis 3 e 4) O módulo criptográfico deve ser coberto com um revestimento opaco inviolável duro (por exemplo, um epóxi opaco duro cobrindo a passivação).*
>
> *TE05.28.02: O testador deve verificar se o revestimento não pode ser facilmente penetrado na profundidade do circuito subjacente, e se ele deixa evidência de violação. A inspeção deve verificar se o revestimento cobre completamente o módulo, é visivelmente opaco e impede a observação direta, sondagem ou manipulação.*
>
> *AS.05.39: (Multiple-Chip Embedded - Níveis 3 e 4) a forma de realização de múltiplos chips do circuito dentro do módulo criptográfico deve ser coberta com um revestimento duro ou material de encapsulamento (por exemplo, um material epóxi rígido) que seja opaco dentro do espectro visível.*
>
> *TE05.39.06: (Opção 1 - Utilizar um material opaco duro) O testador deve verificar por inspeção e da documentação do fornecedor que o módulo é coberto com um material opaco duro. A documentação deve especificar o material que é usado. O testador deve verificar que não pode ser facilmente penetrado na profundidade do circuito subjacente. O testador deve verificar se o material cobre completamente o módulo e é visivelmente opaco dentro do espectro visível.*

AS.05.52: (Multiple-Chip Standalone - Níveis 3 e 4) A forma de realização múltipla do circuito dentro do módulo criptográfico deve ser coberta com um material de revestimento rígido (por exemplo, um material epóxi rígido) que seja opaco dentro do espectro visível .

TE05.52.02: (Opção 1 - coberto com um material de revestimento duro e opaco) Encapsulado dentro de um material de revestimento duro e opaco. O testador deve verificar, a partir da documentação do fornecedor e por inspeção, se o acesso interno é possível, que o circuito dentro do módulo é coberto com um material de revestimento opaco duro. A documentação deve especificar qual material de encapsulamento é usado e suas características de dureza.

Assim, no item 59 do documento referenciado acima sugerimos a seguinte alteração:

"59. Os perímetros criptográficos das urnas eletrônicas, cujos TRNGs não estiverem embarcados em um circuito integrado, devem estar protegidos por resina, com uma das seguintes características:

59.1. Opção A:

a) espessura mínima de 5 mm;

b) grau mínimo de dureza de 80 SHORE-D, que dificulte e evidencie tentativas de violação dos dispositivos;

59.2. Opção B:

a) espessura mínima de 1 mm;

b) grau mínimo de dureza de 85 SHORE-D ou mais, que dificulte e evidencie tentativas de violação dos dispositivos;

A opção B apresentada aqui acrescenta duas vantagens ao projeto: primeiro, com grau de dureza de 85 Shore -D o material torna praticamente impossível uma violação ao circuito que não acabe por danificar algum componente da placa, inviabilizando desta forma ataques deste tipo. Segundo, ao se adotar um material mais duro e resistente a diferentes tipos de ataques, não se necessita adicionar uma camada larga de proteção, simplificando o processo de fabricação e diminuindo os custos.

Proteção de chaves em caso de violação

Considerando que, de acordo com o documento Anexo IV – Especificações Técnicas – Segurança, o módulo do leitor biométrico é um considerado um módulo de segurança e deve, como tal, atender as especificações deste tipo de módulo.

Reagir a ataques, como implementado em situações similares aplicadas em periféricos de terminais bancários, significa tomar ações como destruir as chaves criptográficas quando qualquer evento de invasão é detectado, mesmo quando o ataque é realizado com o equipamento totalmente desligado.

Não encontramos em nenhum ponto do documento Anexo IV – Especificações Técnicas – Segurança menção a proteção das chaves do dispositivo Biométrico em caso de ataques quando este esta desligado, embora alguns itens deste documento (itens 59.5, 60 e 61) sugerem que o sistema deve ter meios de se proteger deste tipo de ataque de intrusão e apagar suas chaves de segurança.

A forma como este tipo de proteção é implementado em leitores biométricos em uso no mercado financeiro é através da adição de uma pequena bateria embutida dentro do perímetro criptográfico, cuja a única função é manter os sensores de intrusão ativos, que ativarão a destruição (zeroization) de todos os dados de segurança do equipamento, em especial chaves criptográficas.

Assim, sugerimos o seguinte texto próximo aos itens 60:

“60.1 O MSLB deverá ser resistente à abertura e intrusão (em implementação similar ao padrão FIPS140-2, nível 3) e ser lacrado com mecanismo interno de autodestruição em caso de violação (Tamper Proof), para proteger as chaves criptográficas armazenadas e proteger a placa de circuito responsável pela captura e manipulação do Template de injeções ou intervenções externas.

60.2 O MSLB deverá possuir bateria interna, para preservação da chave criptográfica, com tempo de vida útil estimado em 10 anos sem alimentação de energia.”