Tradução de um capítulo do livro, The Hardware Hacking Handbook Breaking Embedded Security with Hardware Attacks by Jasper van Woudenberg and Colin O'Flynn.

Tradução do Capítulo 3, C A S I N G T H E J O I N T: I D E N T I F Y I N G C O M P O N E N T S AND GATHERING INFORMATION

Frank Herbert escreveu em "Duna", "Um começo é um momento muito delicado." Como você provavelmente sabe, a maneira como você começa um projeto define o tom para o seu sucesso. Operar com suposições falsas ou ignorar uma pequena informação pode descarrilar um projeto e desperdiçar tempo precioso. Portanto, com qualquer projeto de engenharia reversa ou pesquisa (hardware não sendo diferente), reunir e revisar o máximo de informações possível nas fases iniciais da investigação de um sistema-alvo é crítico. A maioria dos projetos baseados em hardware começa com uma fase de curiosidade e coleta de informações, e este capítulo destina-se a ajudar nessa fase. Se você estiver realizando uma revisão do sistema-alvo sem arquivos de design, especificações ou uma lista de materiais (BOM), naturalmente começa abrindo o dispositivo e vendo o que há dentro. Essa é a parte divertida! Este capítulo descreve técnicas para identificar componentes ou interfaces interessantes e compartilha ideias para reunir informações e especificações para um dispositivo e seus componentes.

A fase de coleta de informações não é linear. Você encontrará uma variedade de peças de quebra-cabeça. Neste capítulo, mostramos maneiras de encontrar as peças, e cabe a você juntá-las, em qualquer ordem, para fazer a imagem suficientemente completa.

Coleta de Informações

A coleta de informações, doxing, reconhecimento, fazer o desenvolvedor Joe revelar segredos—como você expressar isso, essa é uma etapa importante que economiza tempo. Muitas informações estão disponíveis se você souber onde procurar. Começamos com o menor esforço, que é no teclado, e depois alcançaremos a chave de fenda e outras ferramentas. Antes de mergulhar nas profundezas da internet, você pode considerar simplesmente buscar o nome do produto junto com a palavra-chave "desmontagem". É comum haver desmontagens de produtos populares postadas em várias fontes; o site iFixit, por exemplo, tem muitas desmontagens populares, incluindo anotações detalhadas dos produtos. Para bens de consumo, fique atento a várias gerações dos produtos. O dispositivo de alarme de fumaça inteligente Nest Protect de segunda geração é muito diferente internamente do dispositivo de primeira geração, por exemplo. É comum que empresas não diferenciem realmente essas gerações, pois simplesmente param de vender dispositivos de geração mais antiga, então você pode precisar descobrir isso a partir dos números do modelo ou similar.

Arquivos da Comissão Federal de Comunicações (FCC)

A Comissão Federal de Comunicações (FCC) é uma agência governamental dos Estados Unidos responsável por tudo, desde impor multas por expor partes do corpo na TV até garantir que os dispositivos sem fio de alta velocidade mais recentes não interfiram entre si. Ela estabelece regulamentos que os fabricantes de qualquer dispositivo digital vendido nos EUA devem seguir. Esses regulamentos são projetados para garantir que um determinado dispositivo não gere quantidades excessivas de interferência (por exemplo, seu dispositivo super rápido causando queda na recepção da TV do seu vizinho) e continua a operar mesmo na presença de algum nível de interferência eletromagnética (EM).

Outros países têm agências e regras semelhantes. A FCC é interessante porque os EUA são um mercado tão grande, então a maioria dos produtos foi projetada e/ou testada para atender às regras da FCC, e a FCC torna o banco de dados de informações arquivadas publicamente disponível.

Sobre Arquivos da FCC

Qualquer dispositivo digital que emita ondas de rádio, conhecido como radiador intencional, exige testes. A FCC exige que os fabricantes testem cuidadosamente as emissões de seus dispositivos e forneçam documentação comprovando que os dispositivos atendem às regras da FCC. É um processo muito caro, e a FCC precisa garantir que seja fácil para o público verificar a conformidade. Este é o motivo pelo qual, por exemplo, o computador de tamanho flash drive de código aberto chamado USB armory Mk I é rotulado como uma plataforma de desenvolvimento que "pode causar interferência em dispositivos elétricos ou eletrônicos próximos". Provar que essa etiqueta pode ser injustificada é caro.

Para verificação de conformidade pelo público, um radiador intencional deve publicar algo conhecido como seu ID da FCC, que é impresso na etiqueta do dispositivo. Você pode pesquisar este ID no site da FCC e confirmar que o dispositivo realmente passou no teste de conformidade. Isso também significa que detectar etiquetas falsas da FCC é fácil porque qualquer pessoa pode verificar o status, não apenas agentes da FCC. O ID da FCC de um dispositivo pode estar dentro de uma tampa de bateria.

Se um dispositivo não for um radiador intencional, ainda deve ter o logotipo de conformidade da FCC, mas não terá um ID da FCC. Esses radiadores não intencionais têm requisitos de relatórios menos rigorosos, e a documentação de teste geralmente não está disponível.

Encontrando Arquivos da FCC

Como exemplo, a etiqueta do roteador sem fio na Figura 3-1 mostra que o ID da FCC é KA2IR818LA1, que você pode encontrar no site de Pesquisa de ID da FCC. A ferramenta

de pesquisa separa o ID em duas partes: o código do outorgante e o código do produto. A FCC atribui o código do outorgante, que é sempre o mesmo para uma determinada empresa. Esse código era anteriormente apenas os primeiros três caracteres do ID da FCC, mas a partir de 1º de maio de 2013, ele pode ser três ou cinco caracteres. A empresa atribui o código do produto, que pode ser qualquer coisa entre 1 e 14 caracteres.

Voltando ao roteador, o código do outorgante é KA2, e o código do produto é IR818LA1. Inserindo essas informações na caixa de pesquisa dá os resultados mostrados na Figura 3-2. Este dispositivo tem três arquivamentos, pois pode operar em várias bandas de frequência. O link "Detalhes" fornece relatórios e cartas, incluindo fotos externas e internas do produto—normalmente fotos das placas, bem como detalhes sobre os circuitos integrados.

Carregando as fotos internas com base no ID da FCC KA2IR818LA1, você deve ser capaz de identificar facilmente o processador principal como um RTL8881AB. Você também pode ver algum tipo de conector, que provavelmente é baseado em serial, pois tem cerca de quatro pinos e vários pontos de teste na placa de circuito impresso (PCI). Você encontrou todas essas informações sem mesmo tocar em uma chave de fenda.

NOTA Um site de terceiros interessante, https://FCCID.io/, também fornece arquivamentos da FCC, e tem uma função de pesquisa melhor e visualizador integrado.

Equivalentes da FCC

A campainha Nest na Figura 3-3 não mostra um ID da FCC. Por quê? Colin comprou este dispositivo, e ele está localizado no Canadá, então o dispositivo não requer um ID da FCC. Em vez disso, ele está marcado apenas com o código da Indústria do Canadá (IC), que permite pesquisar no banco de dados “Radio Equipment List (REL)” para um número de "certificação" correspondente.

Pesquisando no banco de dados IC REL por 9754A-NC51 fornece mais informações, mas não há fotos internas detalhadas disponíveis no site público. A parte do código do produto (NC51) é compartilhada entre o ID da FCC e o designador da IC, então uma maneira rápida de encontrar mais informações é fazer uma pesquisa parcial no site da FCCID.io por NC51. Encontramos que o ID da FCC é ZQANC51, o que nos permitiu encontrar as fotos internas.

Patentes

Patentes são efetivamente licenças dadas aos desenvolvedores de produtos para processar empresas que vendem um produto que copia a operação bem definida do produto original, em uma área geográfica específica, por um período de tempo

limitado. Patentes, em teoria, são emitidas apenas se essa operação bem definida for algo inovador. O objetivo é proteger invenções, e como este capítulo é sobre coleta de informações e não política, deixaremos por aqui.

A maioria das empresas gosta de patentes, pois podem usá-las para impedir que um concorrente lance um produto usando alguma nova tecnologia ou design. Mas há um porém: as patentes devem explicar como essa nova tecnologia funciona. A ideia é que, em troca de revelar detalhes preciosos sobre a nova tecnologia, o sistema legal pode impedir que qualquer outra pessoa use esses detalhes para competir com o inventor por aquele período de tempo limitado.

Encontrando Patentes

Ao pesquisar um dispositivo, você pode descobrir que as patentes fornecem informações úteis sobre como a segurança ou outros aspectos do design foram tratados. Por exemplo, ao pesquisar um disco rígido protegido por senha, encontramos uma patente que descreve um método de proteger discos rígidos embaralhando a tabela de partições.

Produtos ou manuais podem ser marcados com algum tipo de declaração como "Protegido pela Patente dos EUA 7.324.123." Você pode facilmente procurar este número de patente no site do Escritório de Patentes e Marcas Registradas dos Estados Unidos (USPTO) ou em um site de terceiros, como o Google Patents. Recomendamos o Google Patents, pois ele pesquisa em vários bancos de dados e também contém uma ferramenta de pesquisa facilmente navegável para uso geral.

Muitas vezes, os produtos são rotulados como "Patente Pendente", ou você pode encontrar apenas referências a patentes na literatura do produto. Isso normalmente significa que a empresa simplesmente solicitou uma patente; pode até não ser visualizável publicamente ainda. Nesse caso, a única maneira razoável de buscar essas patentes é pelo nome da empresa. Descubra a quem a patente é provavelmente atribuída; por exemplo, uma patente pode ser de propriedade do fabricante de um chip dentro do dispositivo e não do fabricante do próprio dispositivo. Frequentemente, você pode encontrar patentes relacionadas emitidas para a empresa e, em seguida, pesquisar pelo escritório de advocacia da empresa ou até mesmo por outras patentes relacionadas por inventores associados.

Se você encontrar uma patente (ou solicitação de patente), a solicitação publicada não é toda a informação que você pode usar. Um sistema chamado USPTO Public PAIR permite que você revise quase toda a correspondência entre o USPTO e o requerente da patente. Esses documentos não são indexados por mecanismos de busca, então você não os encontrará sem usar o sistema USPTO Public PAIR. Você pode ver, por exemplo, se o USPTO tem discutido contra um pedido em casos onde as patentes estão pendentes, ou encontrar documentação de suporte que os requerentes podem

ter carregado. Às vezes, você pode encontrar versões anteriores de uma patente ou os argumentos de um requerente, incluindo informações adicionais que você não encontrará no Google Patents.

Alguns exemplos de usos interessantes de patentes para engenharia reversa incluem o ataque Thangrycat pela Red Balloon Security, detalhado em uma apresentação no DEF CON intitulada "100 Seconds of Solitude: Defeating Cisco Trust Anchor with FPGA Bitstream Shenanigans." Nesse ataque, a Red Balloon Security derrotou a raiz de confiança da Cisco, que usava um componente eletrônico chamado campo reconfigurável (FPGA). Detalhes da arquitetura foram explicados útilmente na Patente dos EUA 9.830.456, que forneceu insights que, de outra forma, exigiriam esforço considerável para engenharia reversa.

Outro exemplo onde as patentes foram úteis para hackers de hardware é uma apresentação no Black Hat USA intitulada "GOD MODE UNLOCKED: Hardware Backdoors in x86 CPUs," por Christopher Domas. Aqui, a Patente dos EUA 8.296.528 explicou como um processador separado poderia ser conectado ao núcleo principal x86 e deu dicas de detalhes que resultaram em uma completa violação do mecanismo de segurança do núcleo.

As patentes podem até listar detalhes sobre dispositivos seguros. Por exemplo, um leitor de cartão de crédito da Square contém uma "malha" anti-manipulação integrada a uma cobertura plástica para a seção segura do microcontrolador. A Figura 3-4 mostra as quatro grandes almofadas quadradas (falaremos mais sobre características de PCBs mais tarde neste capítulo) com seções ovais que se conectarão à cobertura de malha anti-manipulação.

A Figura 3-5 mostra a parte inferior da cobertura de malha anti-manipulação que se acopla ao PCB mostrado na Figura 3-4.

Figura 3-4: O interior do leitor de cartão de crédito Square com quatro conectores de malha anti-manipulação perto de cada canto

Figura 3-5: A cobertura de malha do leitor da Square; as conexões expostas se conectarão ao PCB mostrado na Figura 3-4

Quando você remove a malha, o dispositivo para de funcionar, então a engenharia reversa do dispositivo rapidamente se torna cara. Se você pesquisar no Google Patents por US10251260B1, no entanto, você encontrará detalhes sobre como a malha funciona. Experimente isso agora e veja se você pode associar as fotos das Figuras 3-4 e 3-5 com as figuras da patente. Se você não trabalhou com PCBs antes, volte a essas figuras novamente depois de terminar este capítulo, pois explicaremos algumas das características da PCB que você pode ver aqui.

Folhetos Técnicos e Esquemas

Os fabricantes publicam folhetos técnicos (seja publicamente ou sob NDA) para que os designers possam aprender como usar seus componentes, mas geralmente não publicam esquemas completos. Em vez disso, você normalmente pode encontrar projetos lógicos compartilhados publicamente que mostram como os componentes estão interconectados. Por exemplo, um layout de PCB mostra o design físico—ou seja, onde todos os componentes estão colocados e como os fios estão roteados, mas geralmente não está publicamente disponível.

Tente encontrar um folheto técnico online para seu dispositivo ou placa de desenvolvimento favorita, como para um módulo de computador Raspberry Pi ou um processador Intel 8086, ou um folheto técnico aleatório para memória flash ou DRAM. Ou, se quiser ir para o analógico, encontre um folheto técnico de nivelamento. Normalmente, você só precisa fazer uma pesquisa na internet simples para códigos de produto ou outros identificadores, conforme mencionado anteriormente. Sites como findchips também são úteis para localizar produtos atuais.

Folhetos técnicos para um componente específico podem ser um pouco mais difíceis de encontrar. Para componentes, primeiro determine o número do componente (veja a seção “Identificando ICs na Placa”). O número do componente geralmente parece uma coleção aleatória de letras e números, mas eles codificam as várias configurações disponíveis de um componente. Por exemplo, o folheto técnico para o MT29F4G08AAAWP decompõe o número do componente da seguinte maneira:

• MT significa Micron Technology. • 29F é a família de produtos de memória flash NAND. • 4G indica uma capacidade de armazenamento de 4GB. • 08 indica um dispositivo de 8 bits. • O primeiro “A” significa um die, um pino de comando e um pino de status do dispositivo. • O segundo “A” indica uma tensão operacional de 3,3 V. • O terceiro “A” é um conjunto de recursos listados. • WP indica que o componente é um encapsulamento fino de 48 pinos (TSOP).

Ao pesquisar, basta digitar qualquer número do componente que você encontrar na die. Se você não conseguir encontrar o número exato, remova alguns dos caracteres finais e pesquise novamente ou permita que seu mecanismo de busca sugira alguns nomes quase correspondentes.

Frequentemente, você terá muitas correspondências, porque em peças muito pequenas, um número completo do componente não é impresso, mas apenas um código de marcação mais curto. Infelizmente, pesquisar o código de marcação retornará centenas de correspondências não relacionadas. Por exemplo, um componente específico na placa pode ser rotulado simplesmente como UP9, o que é quase impossível de pesquisar. Se você pesquisar o código de marcação juntamente com o tipo de encapsulamento, frequentemente obterá resultados mais úteis. Nesse exemplo, identificamos o encapsulamento como sendo do tipo SOT-353 (discutiremos

tipos de encapsulamentos posteriormente neste capítulo). Para códigos de marcação específicos, você pode encontrar bancos de dados de códigos de marcação SMD (dispositivo montado em superfície), como https://smd.yooneed.one/ e http://www.s-manuals.com/smd/, que, combinados com seu conhecimento do encapsulamento, podem levá-lo ao dispositivo (neste caso, um Diodes, Inc., 74LVC1G14SE).

Após olhar alguns folhetos técnicos, você descobrirá que eles têm algo em comum. Eles raramente contêm informações interessantes do ponto de vista da segurança. Estamos principalmente interessados em interagir com um dispositivo, o que significa descobrir como ele funciona e como se conectar a ele. A introdução geralmente conterá a funcionalidade: é um processador, uma memória flash ou o que for. Para se conectar a ele, procuramos pelo pinout e quaisquer parâmetros que descrevam os pinos, como funcionalidade, protocolo ou níveis de tensão. Você quase certamente encontrará algumas das interfaces discutidas no Capítulo 2.

Buscando Informação: O Dispositivo USB Armory

Vamos procurar informações sobre o dispositivo USB armory Mk I da Inverse Path (adquirido pela F-Secure) como exemplo. É um hardware de código aberto, então teremos acesso a muitos detalhes. Antes de ler todos os spoilers aqui, tente pesquisá-lo por conta própria. Veja se consegue encontrar o seguinte:

• O fabricante e número do componente do principal sistema em um chip (SoC), bem como o folheto técnico para ele. • Os GPIO e UART no PCB. • Quaisquer portas JTAG expostas na placa. • Os fios de alimentação e tensão no PCB. • Os fios do cristal de clock externo e frequência. • Onde a interface I2C do SoC principal se conecta a outro CI e qual é o protocolo. • Os pinos de configuração de inicialização no SoC, onde eles estão conectados no PCB e quais modos e configurações de inicialização isso seleciona.

Fabricante, Número do Componente e Folheto Técnico

A partir das páginas do GitHub e wiki do USB armory, podemos ver que o USB armory é baseado em um NXP i.MX53 ARM Cortex-A8. O folheto técnico é chamado IMX53IEC.pdf e está disponível em vários locais. Ao pesquisar por "vulnerabilidade imx53," encontramos uma vulnerabilidade conhecida de X.509 no blog da Quarkslab. Se você procurar mais, pode encontrar um aviso de segurança intitulado “Security Advisory: High Assurance Boot (HABv4) Bypass,” que observa que essas vulnerabilidades não estão presentes no Mk II.

Os GPIO e UART no PCB

Pesquisando por “USB armory GPIO,” chegamos ao wiki do GitHub (https://github.com/f-secure-foundry/usbarmory/wiki/GPIOs/), que fornece o detalhe dos GPIOs. No folheto técnico obtido anteriormente, podemos encontrar todos os

GPIOs, UARTs, I2C e SPI do i.MX53. Qualquer uma dessas portas de comunicação seria interessante para monitorar; eles certamente transportariam saída de console ou depuração.

Portas JTAG

O JTAG, se não estiver bloqueado, deve fornecer acesso de baixo nível ao chip através das instalações de depuração da ARM, então queremos informações sobre quaisquer portas JTAG expostas na placa. Explorando as páginas do GitHub um pouco mais, encontramos a página JTAG específica para o Mk I, que inclui uma foto do PCB.

Conectores dos pinos JTAG do USB armory

A Figura 3-6 mostra as conexões TCK, TMS, TDI, TDO, nTRST e GND (terra) padrão do JTAG. O pad 2v8 fornece uma fonte de 2,8 V, mas o que dizer do pad MOD? O folheto técnico não é muito claro sobre isso. O JTAG_MOD/sjc_MOD está na lista de pinos do i.MX53, mas não há explicação sobre seu significado. Um pouco de pesquisa para produtos relacionados leva a uma explicação no folheto técnico do módulo do computador i.MX6 (procure “IMX6DQ6SDLHDG.pdf”; o site original da NXP requer login, mas o PDF é espelhado em outros lugares). Este folheto técnico explica que baixo adiciona todas as portas de acesso de teste do sistema (TAPs) à cadeia, enquanto alto o torna compatível com IEEE1149.1 (útil apenas para escaneamento de fronteira, que discutiremos na seção “Using the JTAG Boundary Scan for Mapping”). Lendo o esquema na parte inferior da página JTAG Mk I, você é aconselhado a conectá-lo ao terra por meio de um resistor de pulldown; isso puxa para baixo para ativar TAPs do sistema. Como você pode ver, às vezes sintetizar diferentes fontes de informação completa a imagem.

Fonte de Alimentação e Tensão

Para os fios de alimentação e tensão no PCB, voltamos ao folheto técnico obtido anteriormente. Procure por “power,” “Vcc,” “Vdd,” “Vcore,” “Vfuse,” e “ground/Vss.” Você descobrirá que um SoC moderno inclui muitos casos repetidos desses termos, cada um representando um pino. Vários subsistemas nos planos de energia têm várias tensões de entrada, o que é uma das razões para essa abundância de pinos. Por exemplo, a memória flash pode ter uma tensão mais alta do que a tensão do núcleo. Você também pode encontrar múltiplas tensões de E/S que suportam uma variedade de padrões.

Uma segunda razão para os muitos pinos é que eles são frequentemente duplicados, às vezes várias vezes. Isso ajuda a manter os pinos de energia e terra fisicamente próximos uns dos outros, reduzindo a indutância para ajudar a fornecer transientes rápidos de energia para o chip.

O folheto técnico certamente inclui muitos pinos de energia, que neste chip são designados como VCC (tensão do núcleo periférico) e VDDGP (tensão do núcleo ARM), entre outros. Procuramos pinos de energia para encontrar maneiras de injetar falhas e realizar análises de energia, que são técnicas que você aprenderá nos próximos capítulos. Por exemplo, se você quiser ouvir criptografia no núcleo ARM, você tentaria sondar o VDDGP. Se você quiser injetar falhas no cache L1 (VDDAL1), controle de acesso JTAG (NVCC_JTAG), ou gravações de fusíveis (NVCC_FUSE), tentaria controlar aqueles.

Um esquema é realmente útil para aprender como esses pinos de energia estão conectados na placa de circuito. Encontramos um no repositório de hardware do GitHub como armory.pdf. A página 3 deste PDF lista as conexões de energia para o SoC. Se você seguir os rastros da PCI dessas conexões de energia, verá um monte de capacitores de desacoplamento (marcados como C48, C49, etc.), que são usados para remover ruído da fonte de energia. Você também notará que os nomes das conexões terminam em rótulos como PMIC_SW1_VDDGP e PMIC_SW2_VCC. PMIC significa IC de gerenciamento de energia—um chip dedicado a fornecer as tensões corretas. A página 2 do PDF mostra como a principal fonte de energia (USB_VBUS) alimenta o principal plano de energia (5V_MAIN) e entra no PMIC, que por sua vez fornece uma variedade de tensões reguladas ao SoC.

Isso nos diz logicamente como tudo está conectado, mas ainda não nos diz onde esses fios estão na PCB. Para isso, precisamos abrir os arquivos de layout do PCB, encontrados nos arquivos de design do KiCAD.

O KiCAD é um software de código aberto para projetar PCBs. Estamos usando apenas um por cento de sua funcionalidade aqui para verificar o layout do PCB. Abrimos o arquivo de design armory.kicad_pcb com o comando pcbnew do KiCAD. Uma PCB pode incluir várias camadas de trilhas/conexões, onde cada uma dessas camadas é mostrada no lado direito da janela do programa, com caixas de seleção para ativar e desativar elas. Primeiro desative todas para ver apenas os pads na PCI.

Você verá o "U2" (grade de matriz de bolas do SoC principal) no centro, o "U1"/PMIC à esquerda, e o "U4"/chip DRAM à direita.

O KiCAD tem uma ferramenta legal para destacar uma rede, apropriadamente chamada de highlight net, que permite clicar em qualquer lugar e seguir a conexão. Suponhamos que queremos brincar com a energia do JTAG. Dê zoom no SoC até você ver os nomes das bolas e encontre a bola NVCC_JTAG, que de acordo com o folheto técnico é G9. Você verá o que está mostrado na Figura 3-7.

Lembre-se dos pads JTAG? Parece que o NVCC_JTAG está conectado ao pad 2v8 usado para energia do JTAG. No entanto, próximo ao PMIC, você também verá alguns fios destacados. Eles fazem parte da mesma rede; apenas não conseguimos ver essa parte

porque desligamos todas as camadas. Clicando em todas as camadas ligadas e desligadas, encontramos uma camada que as conecta: GND_POWER_1 (veja a Figura 3-8). Os pontos brancos são vias, que são pequenos buracos revestidos que conectam uma trilha em uma camada a uma trilha em outra camada. Uma via está na conexão esquerda para o PMIC, e então um plano de energia conecta-se à via na direita, que conecta-se ao fio que vai para o NVCC_JTAG. Se quiséssemos controlar a energia no NVCC_JTAG para injeção de falhas ou análise de energia, poderíamos cortar fisicamente a trilha para o PMIC e fornecer nossa própria energia de 2,8 V soldando um fio ao pad 2v8.

Usando o KiCAD para destacar uma rede de interconexão

Destacando a camada GND_POWER_1

Relógio Cristal e Frequência

Para identificar os fios do cristal de clock externo e a frequência dos relógios, recorremos novamente ao folheto técnico obtido anteriormente. Procure por “clock/CLK/XTAL,” e você encontrará quatro pinos osciladores externos interessantes: XTAL e CKIL (e seus inputs complementares EXTAL e ECKIL), e dois inputs de propósito geral, CKIH1 e CKIH2. O manual de referência do i.MX53 (iMX53RM.pdf, que tem 5.100 páginas de conteúdo) indica que esses inputs, por sua vez, podem ser programados para fornecer um clock para vários periféricos, como a rede CAN e a porta SPDIF. Analisando os esquemas do board, descobrimos que (E)XTAL está conectado a um oscilador de 24 MHz, (E)CKIL está conectado a um oscilador de 32.768 Hz, e CKIH1 e CKIH2 estão conectados ao terra. Os esquemas do USB armory mostram que esses pinos estão conectados a dois conjuntos de pads, que correspondem a dois osciladores. Esses osciladores são os componentes bastante grandes