意図したとおりに機能し、正しく使用されている場合は安全な暗号化システムを構築することは比較的簡単ですが、悪用されたり1つ以上の状況でセキュリティを損なわないシステムを構築することは依然として非常に困難です。そのサブコンポーネントの一部が失敗する（または誤動作することが「推奨される」）  
これは現在、クローズドワールドがオープンワールドよりもはるかに進んでいる唯一の領域であり、商用の暗号化システムで見られる多くの失敗は、これについての証拠を提供します。  
  
–ロジャー・ジョンストン  
  
改ざん防止装置は今や至る所にあります。  
市場に出ているデバイスの多くは安全ではありません。  
しかし、いくつかはかなり良いです。  
スマートカードの改ざん耐性は、加入者カードを複製する有料テレビの海賊と有料テレビ業界がそれらを阻止しようとする長い戦争の中で進化し、自社製品を封鎖したい企業と他の企業との武装競争で磨かれました。それらのロックを解除します。  
その他のハッカーは、弁護士、リバースエンジニアリング製品を利用して特許侵害を証明しています。  
そして最後に、灰色の領域がたくさんあります。  
 それはあなたがそれをどのように行うか、そしてあなたがどの国にいるかに依存します。  
この章では、過去30年間の攻撃と防御の進化について説明します。  
データセンターのコンピュータは、物理的なバリア、センサー、およびアラームによって保護されています。  
改ざん防止が完全性と可用性のためだけに必要な場合は、トランザクションを同時に実行して結果に投票するさまざまなサーバーでレプリケーションを使用して実装できる場合があります。これは現在、ブロックチェーンと他のコンセンサスプロトコルで再発明されています。  
しかし、改ざん防止デバイスはデータの機密性も提供することができ、SGXやTrustZoneなどのエンクレーブをサポートするCPUの登場により、クラウドサービスで暗​​号化されたデータを使用したコンピューティングの可能性が失われます。  
18.2歴史  
海軍のコードブックは重み付けされていたので、捕獲が差し迫っていれば船外に投げることができました。イギリスの政府大臣の補佐官が州の書類を運ぶために使用した発送箱は、確実に沈むように先頭が並んでいました  
しかし、主要な資料はしばしば奇襲攻撃で捕捉されたため、改ざん対応プロセスを自動化する試みが行われました。  
悪名高いウォーカー一家が20年以上にわたって米海軍の鍵素材をロシア人に販売した後[876]、エンジニアは輸送中の鍵をどのように保護するかという問題にもさらに注意を向けました。  
紙の鍵はかつて、改ざんの証拠を示すように設計された「おとぎ話のような容器」に入れて運ばれました。  
今日、暗号鍵の物質の物理的な輸送には通常、スマートカード、または鍵としてパッケージ化された同様のチップが含まれます。  
主要な資料の制御もより広い目的を獲得し、米国と英国の政府はそれを使用してネットワークを承認済みデバイスに制限しました。  
初期鍵がロードされると、認証プロトコルを使用して追加の鍵を配布できます。  
  
IBM 4758（図18.1および18.2）  
まず、耐タンパー性の最高レベル（FIPS 140-1レベル4）で評価された最初の商用製品でした。  
第二に、その歴史、ハードウェアおよびソフトウェアを含む、それに関する広範な文献があります[1795、1998、2001]。  
第4に、現在のIBMフラグシップ製品である4765は、見つかったいくつかのバグを修正することを除いて、大幅に変更されていません。  
 裏話は1970年代に始まり、ミハイルアタラは銀行のPINを管理するためのブラックボックス暗号モジュールのアイデアを持っていました。  
その後、ブロック暗号を使用して単一の銀行、さらには多くの銀行のネットワークでPINを管理する方法について、徹底的な調査が行われました[1301]。  
これにより、スタンドアロンの暗号化モジュールまたはハードウェアセキュリティモジュール（HSM）が開発されました  
これらは、暗号化ハードウェアと特別なキーメモリ、スタティックRAMを備えた堅牢な金属製のエンクロージャに格納されたマイクロコンピュータであり、スタティックRAMは、エンクロージャが開かれたときにゼロ化されます。  
そのため、保守員が電池を交換するときはいつでも、蓋を開けて鍵を破壊していました。  
このようにして、HSMの所有者は、そのキーが自身の信頼できるスタッフの独自の管理下にあることを期待できます。明らかな攻撃は、キーを盗むことです。  
PROMはポケットに入れて持ち帰り、読み取ることができます。  
 回路、アルミニウム電磁シールド、不正開封検知メッシュ、ポッティング材料（フランク・スタハノの厚意による）  
修正は共有制御でした。2つまたは3つのマスターキーコンポーネントを持ち、それらを組み合わせて実際のマスターキーを作成しました。  
 異なる部門の管理下にある異なる金庫に保管されます。  
マニュアルは、ライブキーを消去し、エンジニアにデバイスを修理させ、その後キーを再ロードするようにカストディアンに指示する場合があります。  
とにかく誰がマニュアルを読むのですか？  
あるケースでは、不正なエンジニアが、端末として機能するがロギングをオンにしたラップトップを使用してキーを入力させました[54]。  
暗号プロセッサをハックする方法（2）  
第2世代のデバイスは、フォトセルとチルトスイッチを追加することで、物理的な攻撃を困難にしました。  
約2000年までに、より良い製品がサービス可能なすべてのコンポーネント（バッテリーなど）を分離しました  
。  
物理的な攻撃には切削や穴あけが含まれ、エンジニアが銀行のコンピューター室に同行する警備員によって検出される可能性があるという考えでした1。  
これは、FIPS標準に基づく中レベルの評価に必要な保護レベルです。  
 ただし、有能な攻撃者が監視対象外のデバイスに短時間でもアクセスできる場合-そして現実的には、ガードが何が起こっているのかをガードが理解していないため、これはおそらくメンテナンスエンジニアが持っていることです-それからデバイスをポッティングするコアが不十分です。  
理論的には、粘着性のあるエポキシを削ると、内部のコンポーネントが損傷するはずです。実際には、それは忍耐の問題です。  
そのため、ハイエンド製品は改ざん検知バリアを獲得しました。  
理論は、ミリング、エッチング、レーザーアブレーションなどの技術がワイヤーを壊し、キーを消去するというものでした。  
2018年にSergei Skoroboga-tovは、酸エッチングとマスキングの組み合わせを使用して、Vasco Digipass 270でバッテリー駆動のチップを露出させることができました。適切なラボテクニックを使用すると、エポキシのワイヤーで保護されたライブ回路を実際に攻撃できることがわかりました。  
どんな攻撃でも高い確率で膜を壊すという考えでした。  
このポッティングは、暗号化コアを含む金属シールドを囲みます。  
暗号プロセッサをハックする方法（4）  
特定のセキュリティモジュールが同じマスターキーを使用して数年間実行されると、それらの値はデバイスのスタティックRAMに焼き付けられました。  
1それは少なくとも理論でした。経験によれば、いくつかのエキゾチックな機器の専門家がいくつかのツールを使用してそれを修復し、他のツールを使用しないようにするために最低賃金の警備員に依頼することは少し多くのことを示唆しています。  
関連する工学および物理学の問題は[837]および[840]で説明されており、セルゲイスコロボガトフは2005年に、マイクロコントローラーのフラッシュメモリから数回「消去」された後でも、データを抽出する方法を発見しました[1770]。好むと好まざるとにかかわらず、フラッシュチップのウェアレベリングプロセッサは、信頼できるコンピューティングベースの一部になります。  
暗号プロセッサをハッキングする方法（5）  
1980年代までに、-20°C未満では、電源を切った後、スタティックRAMの内容が数秒間持続する可能性があることがわかりました。  
そのため、攻撃者はデバイスを凍結し、電源を切り、改ざん検知バリアを突破し、キーを含むRAMチップを抽出して、テストリグで再度電源を投入する可能性があります。  
最新のDRAMは、電源を切った後も数秒間、さらに低温ではさらに長くメモリの内容を保持します。凍結スプレーでメモリを冷却し、軽量のオペレーティングシステムでデバイスを再起動すると、キーを読み取ることができます。  
TPMなどの特別なハードウェアにキーを保持しても、ハードディスクの暗号化パスワードを推測できる回数が制限されている場合は十分ではありませんが、正しいパスワードを取得したら、マスターキーをメインメモリにコピーして、 CPUは残りの作業を実行できます。  
とにかく、より優れた暗号化デバイスには、温度と放射線のアラームがあります。  
したがって、製品が特定のメーカーのSRAMチップを使用した残留テストに合格する場合でも、1年後に購入された同じメーカーのチップを使用した同じテストに合格しない場合があります[1768]。HSMアラームの主な制約は、より一般的なアラームと遭遇したものと同様です。  
振動、電力過渡、および電磁干渉が問題になる可能性がありますが、温度が最悪です。  
（私たちはeBayで暗号モジュールを購入し、到着時にそれらが死んでいるのを発見しました。）  
一部の軍事機器は保護用爆発を使用しています。メモリチップは、缶からガスを放出することなくチップを破壊するために正確に計算されたテルミット装填量でスチール缶に埋め込まれます。  
暗号プロセッサをハックする方法（6）  
「テンペスト」、「電力分析」、「サイドチャネル攻撃」、または「エミッションセキュリティ」としてさまざまに知られているこの手法は、次の章で取り上げるほど大きなテーマです。  
このシールドは改ざん検知膜の内側にあり、敵がアンテナとして機能する可能性のあるスロットを切断するのを防ぎます。  
 4758のハードウェアを攻撃する方法を考え出したことはありません。  
1つのハードウェアセキュリティモジュールであるChrysalis-ITS Luna CA3には、Mike Bond、Daniel Cvrˇcek、Steven Murdochによってリバースエンジニアリングされたキートークンのソフトウェアがあり、認証されていない「顧客検証キー」が導入され、輸出の認証に使用されるコードを見つけました。ライブキー[283]。  
これは、正式に検証されたオペレーティングシステムを備えたIBMの4758では発生しませんでした。  
Mike Bondと私は、アプリケーションプログラミングインターフェイス（API）が  
その結果、ホストへのアクセス権を持つプログラマーは、セキュリティモジュールに一連のコマンドを送信して、PINまたはキーを漏洩させることができました。  
そのような攻撃は、Visaが新しい支払いネットワーク機能をサポートするために新しい暗号化操作を義務付けることが時々あり、セキュリティモジュール全体に新しいシステムの脆弱性をもたらすため、阻止するのは困難でした[22]。  
 HSMがサポートするために使用されているあらゆる業界の標準を実装する外部の1つ。  
実際には、API攻撃を予測してブロックする必要があります。  
ソフトウェアベースの害からHSMを保護するためにファイアウォールを販売している専門企業さえあります。  
  
安価なデバイスについて説明する前に、HSMの評価に関するいくつかのコメントをまとめておきます。  
クラス1の攻撃者–「巧妙な部外者」–は非常に知的なことが多いですが、システムについての知識が不十分な場合があります。  
彼らはしばしばそれを作成しようとするのではなく、システムの既存の弱点を利用しようとします。  
クラス2の攻撃者（「知識のあるインサイダー」）は、専門的な技術教育と経験を十分に持っています。  
彼らはしばしば非常に洗練されたツールと分析のための機器を持っています。  
クラス3の攻撃者–「資金提供組織」–は、優れた資金リソースに支えられた関連スキルと補足スキルを持つ専門家チームを編成できます。  
攻撃チームの一部としてクラス2の敵を使用する可能性があります。  
 資金提供を受けた組織をブロックします。  
そして、今日のクラス3の攻撃者は、国立研究所だけでなく、あなたの商業的競争相手や大学のセキュリティチームですらあります。  
FIPS認定制度は、米国政府の認可を受けた研究所によって運営されています。  
レベル4とレベル3の間には大きなギャップがありました。そのレベルのデバイスは、多くの場合、専門家による攻撃が容易でした。  
。  
このような機器は、クラス1の攻撃コミュニティを排除しようとしますが、クラス2の生活を困難にし、クラス3の生活を高価にします。  
FIPSアプローチの批評家は、バッファフローやAPI攻撃などの非侵襲的セキュリティは対象外であると指摘しました。その役割の概念は、他のシステムコンポーネントではなく、企業の人間の役者に関連付けられていたこと。サイドチャネル分析のいくつかの方法をカバーできなかった;それは一般的に時代遅れの技術を目的としたものだった; FIPS規格には、NSAバックドアを含むことが知られている、二重楕円曲線決定論的ランダムビットジェネレーターが含まれています。また、NISTが標準を定期的に更新するのではなく、実装ガイドラインを発行することで頻繁に変更された[1410]。  
これは2019年9月に施行され、2021年にはFIPS 140-2に基づくテストが終了します。  
18.5スマートカードおよびその他のセキュリティチップ  
ほとんどはカードとしてパッケージ化されていますが、一部は物理的なキーのように見えます。多くの攻撃が開発されています。私たちはすでにMifareカードと車のキーの破れの影響について話しました。  
プリンタカートリッジのアクセサリ制御チップは、多くの「価値」も保護し、攻撃と防御の両方で真の革新を推進しています。  
  
スマートカードは、70年代半ばから80年代半ばにかけてフランスで開発されました。初期の歴史については、[832]を参照してください。  
 GSM携帯電話および衛星テレビ局の加入者カードとして。  
スマートカードは、マイクロプロセッサ、メモリ、シリアルインターフェイスがシングルチップに統合され、プラスチックカードにパッケージ化された、内蔵型のマイクロコントローラーです。  
スマートカードチップは、他の方法でもパッケージ化されています。  
トラステッドブートをサポートするためにコンピューターのマザーボードに組み込まれているTPMチップは、基本的にはパラレルポートが追加されたスマートカードチップであるため、TPMは、コンピューターの起動に適切なソフトウェアが使用されていることを確認できます。  
以下では、パッケージングフォームファクターをほとんど無視し、シングルチップ暗号化モジュールを「スマートカード」または「チップカード」と呼びます。  
携帯電話はSIMによってユーザーごとにパーソナライズされており、SIMにはネットワークに対して自分を認証するためのキーが含まれています。  
このデバイスは、グローバル市場向けに大量生産することができ、各加入者はサービスの支払いに使用するカードを取得します。  
  
典型的なスマートカードは、マイクロプロセッサーを含む最大25平方ミリメートルのシリコンの単一のダイで構成されています（カードがﬂ exeされていると、大きなダイは壊れる可能性が高くなります）。  
安価な製品には、8051や6805などの8ビットプロセッサがあり、より高価な製品には、公開鍵暗号を行うモジュラー乗算回路、またはArmなどの32ビットプロセッサ、あるいはその両方（ハードウェア暗号サイドチャネル攻撃から保護する方が簡単です）  
ハイエンドのものはまた、ハードウェア乱数発生器を持っている傾向があります。  
メモリは通常のコンピュータの標準によって制限されます。デバイスの外部では、電源、リセット、クロック、およびシリアルポートのみが接続されます。  
アプリケーションプログラミングデータユニット（APDU）の最下部を含む、いくつかの主要なソフトウェアアーキテクチャが提供されています。  
 を使用してカスタムapp2をコード化できます。  
。  
  
スマートカードベンダーからの売り込みを初めて聞いたとき-私が銀行員として働いていた1986年に-私は、デバイスが安全である理由を尋ねました。  
私はこれを信じていませんでしたが、申し立てが間違っていることを証明する時間や手段がありませんでした。  
いずれにせよ、SIMカードにのみ使用されている限り、意欲的な対戦相手は存在しませんでした。  
これを変えたのが衛星テレビだった。  
事業者は通常、1か2か国の映画の権利しか購入していなかったため、加入者カードを他の国で販売することはできませんでした。  
重要な要素は、ヨーロッパの人々が何年も英国の衛星放送から取り上げてきた「スタートレック」が1993年に突然暗号化されたことでした。  
これは多くの熱心な若いコンピューターサイエンスとエンジニアリングの学生に脆弱性を探す動機を与えました。  
そのため、ハッカーは自分の製品を公然と売ることができます。  
複製されたスマートカードが関与していると報告された最初の大規模な金融詐欺は、約1年後の1995年2月/ 3月でした。  
売り上げは約3,000万ドルと報告されています[1330]。  
 初期のハッキングは、カード自体ではなくプロトコルを標的にしていました。  
これにより、スマートカードとデコーダーの間にデバイスが挿入され、カード宛てのメッセージを傍受して破棄する攻撃が始まりました。  
同じ種類の攻撃がドイツのテレホンカードシステムで開始され、手作りのチップカードが売春宿や亡命希望者のためのホステルで販売されていました[1813、184]。  
 スマートカードは外部電源を使用し、暗号化キーやバリューカウンターなどのセキュリティ状態をEEPROMに保存するため、攻撃者はプログラミング電圧VP Pを取り除くことにより、EEPROMの内容を凍結する可能性があります。  
したがって、この接触を粘着テープで覆うことにより、カード所有者はバリューカウンターが減少するのを防ぐことができます。  
修正は、電圧乗算器を使用して供給電圧VCCから内部でVP Pを生成することでした。  
値制御をバイパスするだけでなく、PIN再試行カウンターをバイパスして、可能なすべてのPINを次々に試すこともできます。カウンターをデクリメントしてチェックし、PINを取得して確認し、それが正しい場合はカウンターを再度インクリメントします3。  
 別の初期の攻撃は、走査型電子顕微鏡（SEM）を使用してチップ表面の電圧を読み取ることでした  
当時大学にあった低コストのSEMは、数10キロヘルツを超える電圧コントラスト顕微鏡法を実行できなかったため、攻撃者はクロックを遅くしていました。  
最近のスマートカードプロセッサには、低クロック周波数を検出してカードをリセットするためのウォッチドッグタイマーまたはその他の回路が備わっているか、動的ロジックを使用しています。  
しかし、盗難警報と同様に、誤警報と見逃した警報の間にはトレードオフがあります。  
最終的に、カードは内部クロックを取得しました。  
 有料テレビ事業者が簡単な攻撃を阻止すると、海賊は物理的な調査に目を向けました。  
チップをデパッケージするための技法はよく知られており、[197]などの半導体テストに関する標準的な研究で詳細に説明されています。  
プローブステーションは、チップの表面に微細なプローブを着地させるためのマイクロマニピュレーターが取り付けられた顕微鏡で構成されています。  
。  
プロービング攻撃の通常のターゲットは、プロセッサのバスです。  
（かつては、カードがリセット直後にメモリのチェックサムを計算することを推奨されていた業界の慣例でした。すべてのコードとデータの完全なリストを提供します。）  
その当時、3ビットをマスクした場合、確認のために結果が7以下であることを確認しました。  
。  
有料テレビカード業界で最初に使用された防御策は、各カードに複数のキーまたはアルゴリズムを与え、現在使用中のものだけがプロセッサバスに表示されるように配置することでした。  
このようにして、海賊の顧客は、攻撃が繰り返され、新しい海賊カードまたはアップデートが配布されるまで、サービスを失うことになります[2064]。  
 この戦略は、アナリストがチップの命令デコーダーにダメージを与え、ジャンプや呼び出しなど、プログラムのアドレスをインクリメントする以外に変更する命令が壊れるというオリバー・クママーリングのメモリ線形化攻撃によって打ち負かされました[1078]。  
これで、メモリの内容をバスから読み取ることができます。  
 デバイスのROMとEEPROMの一部が理解されている場合、攻撃者は不要な命令をスキップして、デバイスに選択した命令のみを実行させることができます。  
これは、リターン指向のプログラミング攻撃の初期バージョンと考えることができます。  
命令デコーダには、接地された針がプログラムされた制御フローの変更を防ぐ場所がいくつかあります。  
特に脆弱なスマートカードファミリの1つは、Hitachi H8 / 300アーキテクチャでした。このアーキテクチャには、最上位ビットが1の場合、CPUは常にブランチなしでシングルサイクル命令を実行するという特性を持つ16ビットバスがありました。  
RISCコアをベースにした他のCPUもこれに悩まされる傾向があります。  
メモリの線形化は、障害誘導攻撃の例です。  
障害は、ハードウェアプローブから過渡電力やレーザー照明まで、さまざまな方法でプロセッサに注入できます。  
典型的なチップはROMにセルフテストルーチンがあり、工場で実行され、すべてのメモリの内容を読み取って検証することができます。  
しかし、攻撃者はこのメカニズムに障害を引き起こす可能性があります。フラッシュメモリのビットを反転するか[1776]、またはヒューズを見つけて2本のプロービングニードルでブリッジするか[302]のいずれかです。  
セクション5.7.1で、RSAアルゴリズムは障害が発生すると壊れやすいことに注意しました。 1回のレーザーショットで、シグネチャをpを法として正しく、qを法として間違ったものにするだけで、攻撃者はキーpqを因数分解できます。  
 そのため、計算はmod pは正しく行われるが、qは正しく行われないため、キーを因数分解できる[1705]。  
スマートカードをハックする方法（6）  
最初のそのような実装では、暗号化プロセッサはカードにパッケージ化された別個のチップであり、興味深いプロトコル障害がありました。現在のビデオストリームを復号化するために必要なキーを常に計算し、それをCPUに渡しますそれを外の世界に渡すかどうかを決定します。  
次のバージョンでは、CPU自体に暗号化ハードウェアが組み込まれていました。しかし、ゲート数が多く、サブミクロンのプロセスが深い場合、攻撃を成功させるには、深刻なツールが必要です。チップの層をエッチングまたは削り取り、電子顕微鏡写真を撮り、画像処理ソフトウェアを使用して回路を再構築する必要があります[269]。  
1990年代後半までに、一部の海賊は商用リバースエンジニアリングラボにチップを再構築させるようになり始めました。  
また、著作権侵害ではなく互換性のためにこれを行うことは合法であるため、アクセサリ制御に使用されるチップを反転します。  
。  
スマートカードをハッキングする方法（7）  
これは蛇行したセンサーラインで、上部の金属層にジグザグの丸いグランドラインがありました。  
センサーメッシュシールドは、攻撃のコストを押し上げる可能性があります。  
したがって、それらをカットした場合、それらを修復する必要があり、その作業のためのツールは集束イオンビームワークステーション（FIB）です。  
これは走査型電子顕微鏡に似た装置ですが、電子の代わりにイオンビームを使用します。  
イオンビームで分解されたガスを導入することで、導体または絶縁体を数十ナノメートルの精度で敷設できます。  
FIBは、半導体テストから冶金学および科学捜査、ナノテクノロジーに至るまで、あらゆる種類のアプリケーションで非常に有用であるため、物理学および材料科学の実験室で広く利用でき、1時間あたり約100ドルでレンタルできます。  
直接的なアプローチは、メッシュを通して目的の信号を運ぶ金属ラインに穴を開け、絶縁体で埋め、絶縁体の中心に別の穴を開け、金属で埋め、コンタクトを上部にめっきすることです–通常幅が数ミクロンのプラチナ「X」。これをプローブステーションの針と接触させます（図18.6を参照）  
電子顕微鏡の電圧コントラストモードと後方散乱モードを使用して正確にカットする場所を特定するなど、さらに多くのトリックがあるため、メッシュのセクション全体を無効にできます。  
一部のチップには、炭化ケイ素または窒化ホウ素の保護コーティングが施されています。これにより、FIBオペレーターは、電荷の蓄積によってチップに損傷を与えるのではなく、ゆっくりと進むことができます。  
スマートカードをハッキングする方法（8）  
。  
スマートカードメーカーは、これが理論的には可能であることを1980年代から知っており、いくつかの大まかな対策についても特許を取得しています。  
彼はタイミングに基づいてさらに簡単な攻撃を考え出しました。暗号化操作が同じ数のクロックサイクルを必要としない場合、これもキーマテリアルを漏洩する可能性があります4。  
側面図18.6の章を参照してください。–バスラインを下から見えるようにするためのFIBクロスを備えたST16スマートカードの保護メッシュ（写真提供：OliverK¨ommerling）  
1998年に市場に出回ったすべてのスマートカードはDPAに対して非常に脆弱であることが判明し、対策が開発されている間、これは業界の発展を2、3年間遅らせました。  
非侵襲的な攻撃は、電力分析の場合と同様に、対戦相手がデバイスにアクセスする必要があるローカル攻撃にさらに分類できます。タイミング攻撃など、どこにでもいる可能性のあるリモート攻撃。  
スマートカードをハッキングする方法（9）  
開発する次の攻撃技術は光プローブでした。  
2001年以来、主にケンブリッジの同僚であるセルゲイスコロボガトフによって、光学プローブが効果的で低コストの技術に発展してきました。  
光がシリコンを電離させ、トランジスタを導通させます。  
たとえば、チャネル。  
これにより、RSAなどの壊れやすい暗号システムのような一時的な障害攻撃だけでなく、空間と時間の両方で正確に指示および制御される障害を引き起こす新しい方法が提供されました。  
基本的な考え方は単純です。トランジスタにレーザーを当てると、光電流が誘導され、デバイスの消費電力が増加します（既に導通していない場合を除く）。  
これを、フリップフロップとRAMメモリを読み取るためのかなり信頼できる方法に開発しました[1648]。  
パッシベーションを壊さないため、侵襲的ではありません。エポキシは取り除きますので、非侵襲的とは見なされません。  
この本の第2版（2007年）までに  
チップの表面からの直接的な光プローブ攻撃は、フィーチャーサイズのためではなく、金属層が邪魔するために困難になりました。難易度はグルーロジック（基本的にランダム化された配置配線）によって増加しました。  
バス路線が選択され、攻撃の対象になる可能性があります。  
簡単に区別できる機能は、EEPROM（左上）だけです。  
。  
私は第2版で、「現在の2つの脆弱性のウィンドウはメモリと裏面です」と書いています。これらは、それ以来10年間、タンパーラボの主要な研究目標を提供してきました。  
 0.35µ未満になると、背面攻撃は実用的な半侵襲的なオプションになります。  
65nm未満のフィーチャーサイズの場合、機械的研磨と化学的エッチングの組み合わせを使用して、チップを2〜5µに薄肉化する必要があります。そして今、シリコン液浸レンズのような、解像度を改善する特別な方法があります。  
裏面攻撃は、直接観察によってROMコンテンツを抽出するために使用される場合がありますが、主な手法は、光学的障害誘導（OFI）です。  
シリコン液浸レンズにより、レーザースポットサイズは約1ミクロンですが、OFI攻撃により28 nmシリコンまでのシングルイベントアップセットが引き続き発生します[593]。  
3つの大手ベンダーはすべて40nm製品を発表しています。  
 しばらくの間実用的です。  
ここでの開始点の1つは、光学的に強化された位置固定パワー分析でした。  
これにより、より選択的な分析が可能になります[1771]。  
 2010年までに、ほとんどのセキュリティチップのロジックは、認識できる機能がほとんどないグルーロジックでしたが、フラッシュメモリには高電圧と大きなチャージポンプが必要なため、フラッシュアレイは大きく、簡単に識別できます。  
そのため、メモリが書き込まれたときにブロックごとの検証のみの操作でセキュアフラッシュを作成することにより、メモリの破損とメモリリードバックアクセスの悪用の両方を阻止しようとしました。  
ロックバンピングがシリンダーを望ましい状態に強制するのと同じように、フラッシュバンピングがバス検証をメモリ検証の結果を報告するときに強制的に望ましい状態にします[1774]。  
メモリセルはフローティングゲートに数百個の電子が存在するかしないかによってビットを保存するため、目的に合わせて設計された回路を使用せずにそれらを読み取るのは難しいです。チップの裏側。  
 それを機能させるには、非常に注意深いサンプル準備、パッシブ電圧コントラスト（PVC）をサポートするSEMが必要です  
このようなツールと手法を使用すると、通常のスマートカードまたは他のセキュリティチップから256KのフラッシュまたはEEPROMを読み取ることが可能になり、シングルビットエラーが6ダースに達する可能性があります。  
スマートカード業界への影響は、チップのメモリ全体を読み取ることができるようになることです。  
スマートカードをハックする方法（12）  
典型的なスマートカードには100,000のゲートがあることを考えると、これは$ 30,000のシミュレーターを入手できることを意味します。  
特定のタイプの1つのカードを十分に理解したら、カードごとのクローン作成コストは、メモリ抽出のコストになります。  
スマートカードはコンピューターであるため、送信するパラメーターの文字列が長すぎてスタックが上書きされるなど、通常のコンピューター攻撃に陥ることがあります。  
しかし、遅くとも2019年には、ソフトウェア攻撃は少なくとも1枚のSIMカードに対して機能しました。  
  
多くの暗号化チップは、乱数ジェネレーター、物理的にクローンできない関数、またはその両方を備えています。  
 プロトコルナンスとセッションキーを生成するために使用されます。  
貧弱なナンスはリプレイ攻撃につながりますが、弱いセッションキーはECDSAなどの暗号化アルゴリズムの長期署名キーを危険にさらす可能性があります。  
。  
ただし、カウンタがリセットされると、出力が繰り返されます。このテーマにはいくつかのバリエーションがあります。  
ハードウェア乱数ジェネレーターは、通常、ジッターを量子化するか、交差結合インバーターペアなどのメタスタビリティのソースを使用します。  
NIST SP800- A / B / Cなどの規格では、RNG出力をテスト回路で実行する必要があります。  
これらのソースを組み合わせる方法は、しばしば重要なことであり、賢すぎようとする設計には注意する必要があります[1033]。  
保守的な設計の例としては、ハードウェアRNGとそれに続くソフトウェアPRNGの両方を組み合わせた2012年以降のIntelチップで使用されているものがあります[856]。  
これは別の攻撃ポイントです。EdSnowdenは、GCHQがGemaltoがカードをパーソナライズするために使用したメカニズムをハッキングし、数百万のSIMでキーのコピーを入手したと報告しました。各チップは秘密鍵を作成し、公開鍵をエクスポートします。ベンダーはこれをパーソナライズ中に認証します。  
別の方法はありますか？  
 は、製造中に自然に発生する変動からデバイスを識別する手段です。  
このようなメカニズムはクローン不可能である必要があり、改ざんされた場合、その動作は検出可能に変化するはずです。  
 2000年、OliverとFritzK¨ommerlingは、チップパッケージに金属繊維を搭載し、その特性を測定して、チップの内容を暗号化するキーを生成することを提案しました。  
人々が設計を提案し、他の人がそれらを壊したので、攻撃と防御の通常の共進化が続きました。  
典型的な「弱いPUF」は、プロセスの変動性から電源投入時に一貫した乱数を生成します。 SRAM PUFは、一部のSRAMセルの初期状態を読み取り、エラー訂正とともに、安定したランダムIDとして、またはメモリを暗号化するため、またはPRNGを駆動するためのAESキーとして使用されます。  
PUFマーケティングでは、多くの場合、はるかに多くの主張があり、1つの主張（および研究目標）があります。  
入力が与えられると、各チップ（および各入力）に対して十分に異なる出力を返します  
たとえば、パーソナライゼーションでチップに千のチャレンジを送信し、後でキーを更新するために応答を保存する場合があります。  
2020年の最新技術は、マルチプレクサのチェーンとそれに続くアービターで構成されるXORアービターPUFのようです。  
攻撃者が各回路パスの相対遅延を計算するのを難しくするために、多数のアービターの出力がXORされます。  
同じ著者がHeiko LohrkeとChristian Boitと協力して、チップの発光によって誘導されるレーザー障害誘導攻撃を開発しました。これにより、一部のアービターが無効になり、他のアービターがより早く学習され、PUFのエントロピーが大幅に減少します[1859]。  
これらは多くの場合、パーソナライズ、保証、およびアップグレードの目的でサプライチェーンの一部に開放されたままなので、適切に機能するデバイスを発明できたとしても、そのようなデバイスがどのような追加の保護を提供するかを確認することは困難です。  
最後に、PUFの強さは、ファブが排除しようと最善を尽くす変動に依存するため、シリコンプロセスの変更により、PUF設計が突然不安定になる可能性があります。  
18.5.5より大きなチップ  
これらの製品の祖父は、クリントン政権がDESの代わりとして1993年に提案したClipperチップかもしれません。  
、これは、Skipjackブロック暗号と、FBIがそれを使用して暗号化されたトラフィックを復号化できるように設計されたプロトコルを含む改ざん防止チップです。  
 これには、デバイスに埋め込まれたFBIキーで暗号化されたユーザー指定のキーが含まれていました。  
よくあることですが、失敗したのは改ざん防止ではなく、プロトコルでした。  
ClipperはCapstoneチップに置き換えられ、暗号戦争は他の方法で続行され、Skipjackブロック暗号はパブリックドメインに配置されました[1400]。  
Clipperチップは分類されず、輸出可能であると主張されていましたが、何度も試してもサンプルを手に入れることはできませんでした。  
 チップ上のメタル1レイヤーとメタル2レイヤーの間にアンチヒューズを溶かしてビットを設定します。  
このテクノロジーはQuickLogic FPGAでも使用され、企業が独自のアルゴリズムを隠す方法として宣伝され、「リバースエンジニアリングは事実上不可能」であると主張しました。詳細と顕微鏡写真は、そのデータブック[801]に掲載されています。  
ヒュージブルリンクは他のデバイスでも使用されます。たとえば、最近のiPhoneでは、AESキーがシステムオンチップに焼き付けられています。  
•最初に注目するのはプログラミング回路です。  
サンプルデバイスとプログラマを入手できる場合は、差動光学プローブ[1772]を使用してこのヒューズを見つけることができます。  
この攻撃手法は、アンチヒューズFPGAだけでなく、フラッシュやEEPROMの種類でも機能します。  
この攻撃は破壊的であるため、通常、各デバイスで異なるキー（iPhoneやスポットブレークダウンPUFなど）に対する関心は限定的です。  
•デバイスが暗号化アルゴリズムを実装している場合、サイドチャネル攻撃が最も速い方法である可能性があります。いつでも光障害誘導を試して、一度に1ビットずつキーを読み取ることができます。2000年代後半から、後で説明するように、光放射を処理する方法も知っています。  
現在販売されているほとんどのFPGAは、アンチヒューズではなくコンベンショナルメモリを備えているため、再プログラム可能にすることができます。  
より高速なパワーアップのために、ビットストリーム全体をフラッシュに保存する不揮発性デバイスを選択できます。  
ただし、アップグレードメカニズムによるサービス拒否攻撃に注意してください。  
しかし、2回目に提供されたビットストリームが破損している場合、製品が死んでしまいますか？  
また、攻撃者が製品にランダムに暗号化されたビットストリームをロードさせると、短絡が発生し、部品が破壊される可能性があります。  
また、古いビットストリームと新しいビットストリームを同時にサポートするのに十分なオンチップメモリ​​を備えた、より高価なFPGAを検討することもできます。  
 認証ロジックが組み込まれています。  
ゲームコンソールメーカーのビジネスモデルには、ソフトウェアと追加のメモリカードにプレミアム価格を請求することが含まれ、その販売者はコピーコントロールテクノロジーを使用してコンソールベンダーにロイヤルティを支払う必要がありました。これは、コンソールの初期費用を補助するために使用されました。  
これはいくつかの興味深い保護トリックを使用しました。 MagicGateプロトコルは両方ともシンプルでした（そのため、プロトコル攻撃は見つかりませんでした）  
。  
小さなチップの認証ロジックには、上部の金属シールド、コピートラップ、レイアウトの難読化が必要な場合がありますが、大きなチップの同じロジックでは、何十億もの他のトランジスタの中に隠れてしまう可能性があります。  
この慣行により、いくつかの興味深いエッジケースが生じています。  
それで、今日私たちがどこでも見つけた魔法のデバイスをどのようにハッキングできますか？  
例として、Sergei Skorobogatovは、新しいPVC Flash / EEPROM読み出し技術を使用して、OmniPodインスリンポンプを反転させました。  
したがって、OmniPodのシステムオンチップは、デバイスの承認済みコントローラーを使用して認証プロトコルを実行し、糖尿病患者をサポートするNGOであるNightscout Foundationは、患者が治療を行うのではなく、自分の健康ニーズに合わせて制御を最適化できるようにキーを抽出することを望んでいましたOmnipodによって考案されたプロトコル。  
2番目の攻撃パスは、デバイスが暗号化されたデータを使用して計算するかどうかを確認することです。そうである場合は、プロトコルの障害またはサイドチャネルを探して、その方法を調べます。  
このデバイスは、データがロードおよび保存されるときにフライ上のメモリアドレスとコンテンツを暗号化するハードウェアを使用してバス暗号化を開拓したので、低コストの改ざん検知パッケージに同時に搭載できる少量のRAMに限定されませんでした（1995）  
Markusは、プロセッサの命令の一部に目に見える外的影響があることに気づきました。特に1つの命令により、メモリ内の次のバイトがデバイスのパラレルポートに出力されました。  
この手法を使用して数バイトの暗号化関数を表にした後、短いプログラムを暗号化して実行し、メモリ全体の内容をダンプできます。  
2017年、セルゲイスコロボガトフは自動車業界で使用されているシステムオンチップへの積極的な攻撃を実証しました。これはメモリの暗号化を使用してバスのプローブを困難にしました。  
より難しい問題がiPhoneから出されました。  
セルゲイは彼が間違っていることを証明するために着手し、8月までに実際の攻撃があった。  
AESは暗号解読に対して脆弱ではなく、暗号化は一度に1つのキャッシュラインで機能するように見えるため、暗号命令の検索は機能しません。  
スマートフォンの不揮発性メモリはNANDフラッシュチップであり、そのコンテンツは埋め込みデバイスキーによって1つのキャッシュラインで暗号化されているため、あるスマートフォンのチップを別のスマートフォンで読み取ることはできません。  
次に、半ダースのPIN推測を行うと、電話の速度が低下し始めます（10回後にロックされます）。  
次に、メモリチップを取り外し、元の内容を復元します。  
もう少し作業を進めると、チップのクローンを作成したり、回路基板を構築してそれをエミュレートしたりできるため、より速く推測できます。  
結局、FBIは法医学の会社であるCellebriteからのサービスを使用しましたが、それは後にiPhone ROM [793]のCheckm8バグを悪用していることが判明しました。  
半導体接合が切り替わると光子が放出され、光子放出顕微鏡法は確立された故障解析手法であり、シリコンは主にn-MOSトランジスタのドレイン領域近くの近赤外線で放出されます。翌年までに、Sergei Skorobogatov氏は、趣味の天文学者に販売された光電子増倍管が理想に近いことを発見し、電圧ブーストトリックを発見しました。  
次に、AESアルゴリズムのタイミングが確立され、各ラウンドキーに1.6µsがかかることを知った後、個々のバス書き込みの0.2µsに対して電圧をさらに2.5Vに増加させ、光子出力と時間の増加をさらに4倍にしました。これにより、バスからラウンドキーの各単語を明確に読み取ることができました。  
ProASIC3は、7つの金属層とフラッシュメモリを備えた0.13µテクノロジーで製造されており、当時知られている攻撃をブロックするためのあらゆる種類の対策を組み込んでいました。侵略的にそれを読むのは退屈だったでしょう。  
発光分析が組み合わせ攻撃で使用されるようになりました。リバースエンジニアリングを行うには大きすぎるチップを攻撃する場合は、暗号化と同様に発光を観察します。これにより、フォールト攻撃を試みたり光学的にレーザーを狙う場所がわかります。 -強化された電力分析。  
  
有能なやる気のある対戦相手からシングルチップ製品をどれだけうまく保護できますか？  
1年の遅れ、100万ドル以上の予算、そして成功の確実性は見られません。」さて、2019年、ムーアの法則は完全に機能しなくなりました。暗号化チップはほとんどが100 nmでスタックしていますが、半導体テスト機器業界は9 nm処理をサポートすることを目指しており、パッシブ電圧コントラスト顕微鏡法などの革新を実現しています。そして研究者達は彼らの製品を使用する革新的な方法を見つけています。  
業界の範囲も拡大しています。  
したがって、大学院生がハードウェアリバースエンジニアリングの技術と技術を学ぶのに適した中程度の製品がこれまで以上に存在します5。  
市場は現在、人々がレイアウト再構築ソフトウェアや光学故障誘導ワークステーションなどの生きている販売専門ツールを作るのに十分な大きさです。  
スマートカードのクローン作成のコストは着実に数万から数千、おそらくは数千に下がると思います。  
HSMを購入する銀行家は、FIPSレベル3とレベル4の大きな違いに気付かないでしょう。また、レベル3はスイスのアーミーナイフで打ち負かされる場合があることを理解しています。  
APIのセキュリティは非常に厳しく、HSMの内部APIと外部APIの違いにより、混乱しすぎています。  
混乱のマーケティングと負債のゲームは続く見込みです。  
 まず、HSMビジネスのほとんどはクラウドに移行しており、AzureとAWSはそれぞれ2,000のHSMのオーダーを持ち、Googleがキャッチアップを行っています。  
価格が下がると、HSMベンダーのエンジニアの専門知識が失われます。クラウドサービスプロバイダーがデータセンターを保護するため、HSMは暗号化チップに置き換えられる可能性があります。  
悪い端末が、それが見るすべてのEMVカードに対して実動電力分析攻撃を実行できるようにしたくないのですが、それが起こったとしても、それは磁気ストライプカードが複製された方法なので、それは世界の終わりではありません。被害を抑える方法を知っています。  
しかし、有料テレビは現在有線ブロードバンドに移行しており、企業は損失を削減する方法はより安全なチップだけではないことを学びました。より複雑なスマートカードが役割を果たしましたが、改善の多くは海賊に対する法的措置、および技術的および法的措置を効率的に連携させる。  
5私の同僚であるフランククルボン、マーカスクーン、セルゲイスコロボガトフは現在、大学院生向けのコースを運営しています。  
ベンダーは認定要件を満たすために必要なだけの金額を費やしますが、この要件は滑りやすく、ゲーム化されます。  
アクセサリコントロールはハードウェアの最も厳しい分野であり続けると思います。  
ただし、相互に認証する2つのデバイスのうち少なくとも1つが少なくとも時々オンラインになる場合、保護要件は衛星テレビよりもはるかに厳しくありません。  
  
したがって、セキュリティエンジニアは、デバイスの価格や技術的な改ざん耐性とはほぼ無関係な改ざん防止プロセッサを含むシステムの多くの障害モードに注意を払う必要があります。18.6.1信頼できるインターフェースの問題  
銀行のセキュリティモジュールの一部には物理的なロック（または2つ）があります  
 特権トランザクションを実行できます。  
「アンダーソンのセキュリティエンジニアリングのコピーにamazon.comに$ 47.99を支払ってください」というテキストが表示されているのに、署名のために実際に送信されるメッセージが「13アカシアアベニューにある私の家を返済し、収益をマフィアリアルエステートインクに支払ってください」である場合、その後、耐タンパー性はあなたをあまり買っていません。  
ニックボーム、イアンブラウン、ブライアングラッドマンは、適格な電子署名デバイスを使用すると、「私が現在提示しているキーによって検証されるすべての署名について、無条件で責任を負うことに同意し、引き受けます」と指摘しました。それに依存した結果として誰かが取るすべてのリスク '[277]。  
EU eIDAS規制では、すべてのEU政府が以前に紙にインクを必要としたトランザクションの適格な電子署名を受け入れること、および署名デバイスの技術的な認証の基準を設定することを要求しています。  
紙に書かれたインクの性質と比較して責任がシフトすることを考えると、賢明な人は、必要とされない限り、適格な電子署名デバイスを使用しません。  
これにより、ドイツの研究者たちは、署名、署名検証サービス、およびPDFファイルの方法を詳細に検討するようになりました。6iPhoneセキュアエンクレーブプロセッサ（SEP）  
相互作用する;ご想像のとおり、結果はやや衝撃的です。  
彼らは、PDF署名に対する3つの新しい攻撃を発見し、22人のビューアのうち21人で署名の検証を回避する方法を見つけ、8つのオンライン検証サービスのうち6つを騙しました[1326]。  
別の例は、一部の人々が暗号通貨を格納するために使用するハードウェアウォレットから来ています。  
後のものは、安全な要素として機能するスマートカードチップと、ディスプレイを駆動する安全性の低いマイクロコントローラを組み合わせたものです。  
この場合、セキュアエレメントは、メインプロセッサが侵害されたコードを実行しているかどうかを知りませんでした。  
第14章の前払い電気メーターの例を思い出してください。そこでは、改ざん防止プロセッサーがバリューカウンターを維持し、各オペレーターにクレジット制限を適用し、自動販売機の盗難時の損失を制限できます。  
プリンターのインクカートリッジからゲーム機、プリペイド電話カードまで、他のアプリケーションでは、ベンダーは主に使用制御に関心があります。  
18.6.2競合  
銀行では、カード発行者、端末の所有者、および顧客は異なります。クローンされたカード、偽の端末、ギャングランドの商人、浮気銀行のすべての相互作用を熟慮する必要があります。  
彼らの顧客は製品を所有しているかもしれませんが、できればそれを改ざんするインセンティブがあります。  
  
ゲームここで説明するHSMからFPGA、スマートカードまでの各製品カテゴリには、保護の品質にさまざまなバリエーションがあるさまざまな製品があります。  
第1に、FIPS-140レベル4または4を超えるCommon Criteriaレベルであるかどうかにかかわらず、高レベルの保証で提供されるサービスは比較的少ないです。  
これは、最も知識のあるバイヤーを除くすべての人が最も安いFIPSレベル3またはCC EAL4製品を購入するように誘惑されるレモン市場につながります。  
2001年に4758を購入した人は、レベル4の評価を、それが壊れないことを意味すると解釈した可能性があります。  
それは逆の方法でも起こりました。CommonCriteriaレベル6の評価を備えたスマートカードがありましたが、これはオペレーティングシステムのみを参照していました。これはチップ上で実行され、マイクロプローブに対する実際の防御はありませんでした。  
3番目に、HSMはFIPSで評価される傾向がありますが、スマートカードベンダーはCommon Criteriaを使用する傾向があります。  
最後に、多くの企業は、リスクを最小限にするのではなく、安全なプロセッサを使用してリスクをダンプしています。  
薬から防衛まで、購入者が実際の保護ではなくセキュリティの証明書を必要とする多くの環境があり、これは評価システムのフローとさまざまな方法で相互作用します。  
  
多くの設計者は、暗号プロセッサを秘密にしようと懸命に努力してきました。  
Common Criteriaの下で多くのスマートカードを評価するために依然として使用されている保護プロファイルは、設計のあいまいさを強調しています。  
あいまいさは輸出承認の一般的な要件でもあり、故意の脆弱性を隠蔽しているという疑いが生じました。暗号化機能を組み込んだ多くの製品は、乱数ジェネレータが十分にランダムではなかったために機能しなくなりました[775、576]。また、前述したように、NSAはNISTに脆弱なものを標準化させました。  
この開放性により、IBM製品へのAPI攻撃、およびIntelと最近のArmへのサイドチャネル攻撃とROP攻撃の発見が容易になりました。  
2020年の課題の1つは、開発環境にギャップを設ける必要があるかどうかです。  
 スタッフがフライトやホテルを予約できるようになりました。  
ツールチェーンを再構築してワークフローを変更しなければならないため、常にオンラインで業務を行っている企業にとっては、それは不便なことになります。  
内部情報で使用されるスマートカードへの実際の攻撃はほとんどありません。それらのほとんどは、小売店で購入したカードに対するプロービング攻撃またはサイドチャネル攻撃から始まりました。  
1990年代後半以降、VISAなどの一部の組織では、侵入テストを指定しています[1963]。  
評価の基礎となる経済学と政治については、セクション28.2.7.2で説明します。  
18.6.5変化する環境  
一般的な問題は「レバレッジ」です。企業は、適切な契約を交渉することなく、他者が維持しているインフラストラクチャを活用しようとします。  
この本の第2版では、「この問題はありますか？  
おそらくそうではないと思います。テキストメッセージを使用して銀行取引を確認することで、銀行と顧客の両方に限界費用をほぼゼロにして、価値のある2番目の認証チャネルを提供できます。」当時、南アフリカでSIMスワップ攻撃が報告されたケースが1件ありました。  
 iPhoneがAppleの望みどおりに飛び立ち、誰もが自分の電話としてだけでなくWebブラウザとしてもiPhoneを使用するようになったとしたらどうでしょうか。  
これは実際には現地の法律や規制と結びついています。  
結局のところ、電話会社は数分しか売っておらず、盗まれた分の限界費用はほぼゼロです。  
  
そのような複雑な世界で、改ざん防止チップがどんな価値を追加することができますか？  
有料テレビの加入者カードは、グレーマーケットで売買することができますが、コピーされない限り、ステーションオペレーターは大きな収入を失うことはありません。  
第2に、第13章で説明した郵便料金測定と同様に、値カウンターを維持できます。  
プリンターでは、インクカートリッジをプログラムして、あまり多くのインクだけをディスペンスしてから、インクの乾燥を宣言することができます。  
一部の政府システムにおける彼らの主な目的は、「主要な資料の価値をゼロにすること」でした。  
ATMネットワークに適用される同じ一般的な考慮事項は、職務分離ポリシーを実装するだけでなく、人々から多くの信頼を物事に移します。  
この独自の使命は、高度な物理的保護を必要としません。有能なやる気のあるソフトウェア攻撃者に対するセキュリティが鍵となります。  
第5に、信頼できないハードウェア請負業者による過剰生産のリスクを制御できます。「第3シフト」の問題と呼ばれることもあります。ここでは、雇う工場が2つのシフトを実行してデバイスを作り、3番目のシフトがグレーマーケット販売のためにさらにシフトします。  
物事がクラウドサービスとアプリを獲得するにつれて、企業は前者の戦略から後者に移行します。後者はハードウェアコストが低く、管理が容易です。  
第6に、そのような技術は、偽造電子部品からのより一般的なリスクのいくつかを制御することができます。  
調査については、Guin et al [833]を参照してください。  
サプライチェーン攻撃に関しては、最も危険なのはハードウェアのトロイの木馬かもしれません。  
たとえば、追加のロジックによって、64ビットの乗算と2つの特定の入力がキルスイッチとして機能する場合があります。  
もちろん、これは信頼できる工場でリファレンスチップを製造できることを前提としています。  
これは不完全なリストです。  
ただし、注意が必要です。実際に必要とされ、提供される保護特性は非常に微妙な場合があり、改ざん防止デバイスは、完全なソリューションよりも有用なコンポーネントであることがよくあります。  
あなたはあなたが止めたいどんな悪いことを理解する必要があります。  
  
改ざん防止装置とシステムには長い歴史があります。  
私は、一連の攻撃と防御のサイクルを通じてハードウェアの耐タンパー性がどのように発達したか、そしてアプリケーションの例を挙げて話をしました。  
 しかし、特にオンラインサービスが断続的である可能性のある環境では、処理を物理オブジェクトにリンクし、スケーラブルな脅威からセキュリティ状態を保護する必要があるアプリケーションに価値をもたらすことがよくあります。1つ目は、「より速く、より良く、より安く、より安全な」プロセッサを作ることです。ハイエンドデバイスが提供する保護を、1ドル未満のコストのチップにどのようにもたらすことができるでしょうか。  
最新のチップテストテクノロジーを使用して、「より速く、より良く、より安く、斬新な」攻撃を行うにはどうすればよいですか？  
より幅広い研究分野は、安全性の低いコンポーネントからより安全なシステムを構築する方法です。  
 参考資料ハードウェアの改ざん防止に関するナレッジペーパーの最新の体系化については知りません。  
Xboxのハッキングに関するBunnie Huangの本はまだ良い読み物です[930]。  
過去10年間の研究に関しては、CHES（crypt）などの会議で最新の最新の論文がよく発表されます。  
、FDTC（フォールト攻撃）  
。  
初期の歴史–加重コードブックと水溶性インク– David Kahnの本「The Code Breakers」[1001]を読んでください。  
言及されているIBM製品には、オンラインの広範なドキュメント[951]があり、US FIPSドキュメント[1397]を見つけることもできます。