。  
 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、商用暗号化システムで見られる多くの失敗は、これについていくつかの証拠を提供します。  
–ロジャー・ジョンストン18。  
 これまでに説明した例には、以下が含まれます。•銀行カードで使用されるEMVチップと携帯電話で認証に使用されるSIM;•交通チケットとして使用される非接触カードとサービス制御用のペイTVデコーダーで使用されるスマートカード;•アクセサリに使用されるチッププリンタートナーカートリッジとゲームコンソールアクセサリーの制御;•電話、ラップトップ、サーバーのTPMチップが信頼できるルートを提供し、安全な起動とハードディスクの暗号化をサポート;•銀行サーバーだけでなく銀行PINの暗号化に使用されるハードウェアセキュリティモジュール農場であるが、ATMといくつかのPOS端末である; 54718。  
 はじめに•Androidフォンで非接触型決済のクレデンシャルを保存するために使用されるNFCチップ、および指紋と暗号鍵を保存するiPhoneのエンクレーブチップ;•鉄道チケットから切手、アクティブ化する魔法の番号まですべてを販売する自動販売機に埋め込まれた暗号モジュールあなたの電気メーター;•低コストの海外メーカーの製品を手に入れたいが、「3番目のシフト」に同意せずに作られた追加の製品を見たくない企業が製造管理に使用するさまざまなチップ。  
 セクション4。  
1私は、車のリモートキー入力デバイスをリバースエンジニアリングして、クラスの休憩をもたらし、特に車の盗難を増加させた方法を説明しました。セクション13。  
5私は、Mifareカードのリバースエンジニアリングを行って、多くの建物の鍵や輸送チケットシステムを侵害した方法について説明しました。そしてセクション12。  
1。  
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、製品をロックしたい企業とそれらをロック解除したい企業との間の武装競争で磨かれました。  
 弁護士のための他のハッカー、特許侵害を証明するための製品のリバースエンジニアリング。  
 そして最後に、灰色の領域がたくさんあります。  
さまざまな製品と品質の大きな変化を考えると、セキュリティエンジニアは改ざん耐性とは何か、それができることとできないことを理解する必要があります。  
コンピュータが物理的な改ざんに抵抗できない場合、攻撃者はソフトウェアを簡単に変更できます。  
 また、ATMは基本的に金庫のPCで、紙幣ディスペンサーとアラームセンサーが付いています。壁や台座にボルトで固定されることがよくあります。  
 セクション15で説明した古い方式。  
 しかし、改ざん防止デバイスは、dataSecurity Engineering548Ross Anderson18に機密性を提供できます。  
 歴史、そしてSGXやTrustZonehold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見えなくなります。  
2歴史暗号における改ざん防止の使用は数世紀前にさかのぼります[1001]。  
 コードは水溶性インクで印刷されています。ロシアのワンタイムパッドは硝酸セルロースに印刷されていたので、火をつければ激怒します。そして、1台の米国の戦時中の暗号化マシンは、自己破壊テルミット料金で運びました。  
 一部の機械式暗号化マシンは、ケースを開くと主要な設定が消去されるように構築されており、初期の電子デバイスがそれに続きました。  
 目標は「キーマテリアルのストリート値をゼロにすること」でした。これは、キーを簡単に抽出できない改ざん防止デバイス、またはキーの抽出が明らかな明白なデバイスを改ざんすることによって達成できます。  
 電子キーの配布が行われたとき、典型的な解決策は「フィルガン」でした。これは、制御された方法で暗号キーを分配するポータブルデバイスです。  
 SIMカードと銀行カードは、最も目に見える例です。  
 ライブキーマテリアルは、システムが適切に認定された後にのみ提供されます。  
 ここで私たちの主題は、タムパーリングに対する物理的な防御です。  
3ハードウェアセキュリティモジュールIBM 4758（図18。  
2）は、2000年代初頭の主要な商用暗号プロセッサであり、4つの理由で重要です。  
 第二に、その歴史、ハードウェア、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、発見され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。  
3。  
1：– IBM 4758暗号化プロセッサ（Steve Weingartの好意による）バックストーリーは、1970年代に始まり、Mikhail Atallaが銀行PINを管理するためのブラックボックス暗号化モジュールを考案しました。  
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]。  
これは、独立した暗号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）の開発につながりました。  
最初は、これには、電源をいくつかのリッドスイッチを介してキーメモリに配線することが含まれていました。  
 終了すると、HSMカストディアンはキーマテリアルをリロードします。  
暗号プロセッサをハッキングする方法（1）明らかな攻撃は、単に鍵を盗むことです。  
 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。  
3。  
2：–部分的に開いた4758は、（左上から下に向かって）回路、アルミニウム電磁シールド、不正開封検知メッシュ、およびポッティング材料（フランクスタハノの厚意による）の紙の鍵をさらに簡単に表示しました。  
 PROM（またはペーパーキー）は、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、カストディアンにライブキーを消去するように指示し、エンジニアにデバイスを修正させてから、後でキーを再ロード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？ Somanagersは多くの場合、両方のキーをエンジニアに渡して手間を省きます。  
 私は、銀行窓口の通信ファイルに保管されている現金自動預け払い機のペーパーマスターキーのケースにも遭遇しました。  
 第2世代のデバイスでは、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、より良い製品により、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）がデバイスのコア（タンパーセンサー、暗号化プロセッサ、キーメモリ、アラーム回路など）から分離されました。  
 アイデアセキュリティエンジニアリング551ロスアンダーソン18。  
 ハードウェアセキュリティモジュールでは、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りました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。  
たとえば、ポッティングをナイフでこすり取り、プローブをロジックアナライザーからチップの1つにドロップします。  
 RSA、DES、AESなどの暗号アルゴリズムには、計算中に任意のビットプレーンを監視できる攻撃者がキーを回復できるという特性があります[860]。  
 1980年代中頃にIBMのµABYSSシステムに初期の試験例が登場しました。このシステムでは、デバイスがエポキシに埋め込まれているため、デバイスの周囲に緩く巻かれた40ゲージのニクロム線のループを使用し、センシング回路に接続していました[1998]。  
 しかし、ワイヤーインエポキシ技術は、サンドブラストを使用して侵食を遅らせることに対して脆弱である可能性があります。センシング線がポッティングの表面で見えるようになると、シャントをポッティングの周りに接続できます。  
IBMの次の主要製品である4753は、金属シールドと、導電性インクのパターンが印刷されたメンブレンを組み合わせ、類似の化学物質のより耐久性のある材料で囲んだものを使用していました。  
 4758の改ざん検知膜は改良されました。4つの重なり合ったジグザグの導電パターンがウレタンシートにドープされています。これは、化学的に類似した物質に埋め込まれているため、攻撃者がデバイスに侵入することで、導電経路を検出することさえ困難でした。それに接続しています。  
 設計については、[1795]で詳しく説明しています。  
 特定のセキュリティモジュールが数年間同じマスターキーを使用して実行されると、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。経験上、一部のエキゾチックな機器の専門家が一部のツールを使用して他のツールを使用せずに修理することを保証するために最低賃金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。  
3。  
 関連する工学と物理学の問題は[837]と[840]で議論されており、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データを抽出する方法を発見しました。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）コンピュータのメモリも低温によって凍結する可能性があります。  
 これは、液体窒素の温度では数分に及ぶ。  
2008年に、Alex Haldermanと同僚はこれをPCと電話の暗号化キーに対するコールドブート攻撃に発展させました[854]。  
 パワーダウン時にキーをゼロ化するメカニズムがない限り、ディスクの内容のソフトウェアによる暗号化は無効にできます。  
 暗号化チップが保証するものを本当に理解する必要があります。これについては、AdvancedCryptographic Engineeringの章で詳しく説明します。  
 しかし、最新のRAMチップは、さまざまなメモリの残留動作を示します。フィーチャーサイズが縮小するにつれて、残留磁気は長くなり、標準の製品ライン内でも予測できない方法で長くなったようです。  
これは、製造業者にとってこのプロパティが重要ではないコンポーネントのプロパティに依存することの危険性を示しています。  
 誤警報率と見逃された警報率の間、つまりセキュリティと堅牢性の間にはトレードオフがあります。  
 凍結すると自己破壊するデバイスは、通常の流通経路では信頼性の高い方法で送ることができません。これは、航空機のホールドが-40oCにもなるためです。  
）軍事機器メーカーには逆の問題があります：彼らのキットは-55oから+ 155o Cの定格でなければなりません。  
 耐タンパー性、耐温度性、耐放射線性、セキュリティエンジニアリング、553Ross Andersonの同時目標への適合18。  
 ハードウェアセキュリティモジュール出荷の安全性、重量、コストは重要なものです。  
 「Tempest」、「Power Analysis」、「Side-Channel Attacks」、または「Emission Security」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。  
 ハイエンドシステムで見られた攻撃には、物理​​的フローではなく論理的フローの悪用が含まれています。  
 ごく最近、2019年に、Gabriel CampanaとJean-BaptisteB´edruneは、ソフトウェア開発キットに付属のHSMエミュレータをファジングすることにより、Gemalto Safenet Protect ServerPSI-E2 / PSE2への大きなオーバーフロー攻撃を発見しました。実際のHSM、および任意のファームウェアをアップロードするコードを記述しました。これは永続的で、すべての秘密をダウンロードできます[203]。  
 しかし、ほとんどのユーザーは[915]で説明されているCCAと呼ばれる銀行暗号アプリケーションを実行していました。  
 影響は、ホストにアクセスできるプログラマーが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可能性があることでした。  
 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、これらがセキュリティモジュール全体に新しい体系的な脆弱性を導入するため、阻止するのが困難でした[22]。  
2つのAPI間のソフトウェアは信頼できる場合がありますが、外部APIが安全でない場合、信頼できるものにするのは難しい場合があります。  
 多くの銀行は、デバイスを攻撃から保護するために他のアクセス制御メカニズムに実際に依存しながら、正式なコンプライアンスのために使用する安全なHSMに最高額を支払います。  
 Security Engineering554Ross Anderson18でAPI攻撃について説明します。  
 高度な暗号工学の章の評価の詳細。  
4評価HSMの評価に関するいくつかのコメントは、安価なデバイスについて説明する前にまとめておきます。  
 クラス1の攻撃者–「巧妙な部外者」–は非常にインテリジェントであることが多いですが、システムに関する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、相当の専門技術教育と経験を持っています。  
 彼らはしばしば高度な分析のためのツールと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スペシャリストのチームを編成できます。  
 彼らは、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。  
 ちなみに、この分類は少し古くなっています。クラス1の攻撃者がクラス3の機器へのアクセスを貸していることがわかります。私たちの場合、私たちは数学、物理学、ソフトウェア、およびバンキングのバックグラウンドを持つ人々を抱えており、友好的なメーカーから、競合他社の製品のサンプルを提供してもらいました。  
 1994年の最初の標準であるFIPS 140-1では、4つのレベルの保護が設定されており、レベル4が最高でした。これは、2001年に導入された次のバージョンであるFIPS 140-2に残りました。  
 実際、IBMエンジニアによる評価に関する最初の論文は6つのレベル[2001]を提案しました。FIPS規格は、これらの最初の3つをレベル1〜3として採用し、提案されたレベル6をレベル4として採用しました（4758設計者Steve Weingartは、ストーリー[2000]）。  
5または3+は、1990年代から2019年まで、より優れた商用システムの多くが狙われていた場所です。  
ISO 19790を支持してFIPS140を放棄するかどうかについて約10年の協議がありました-ベンダー、特にそれらのセキュリティエンジニアリング555ロスアンダーソン18によってサポートされた動き。  
 スマートカードおよびその他のセキュリティチップ米国外。  
最終的に、米国商務省は、ISO規格19790：2012および24759：2017を単に参照し、いくつかの改良を指定した、更新されたバージョンであるFIPS 140-3を放棄して承認しました。  
18。  
 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。 Mifareカードと車のキーの破損の影響についてはすでに説明しました。  
 プリンタカートリッジのアクセサリコントロールチップも多くの「価値」を保護し、攻撃と防御の両方で真の革新を推進しています。  
18。  
1HistorySmartcardsは、70年代半ばから80年代半ばまで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。  
 それらは1994年にフランスと南アフリカで銀行カードとして使用され始め、続いて英国とノルウェーでの裁判が行われました。これにより、2003年からヨーロッパの他の地域で展開され、銀行と簿記に関する章で言及したEMV標準が生まれました。そして米国は2015年頃からです。  
 銀行で使用されるスマートカードは標準サイズの銀行カードを使用しますが、最新の携帯電話でははるかに小さいサイズが使用されます。  
 STU-IIIでは、米国政府でSecurity Engineering556Ross Anderson18が使用している安全な電話。  
 スマートカードとその他のセキュリティチップ1987–2009では、各ユーザーが「暗号化イグニッションキー」を持ち、物理的なキーのように見えて感じるようにパッケージ化されていました。一部の前払い電気メーターと有料テレビのセットトップボックスは、同じアプローチを使用していました。  
 非接触型スマートカードには、スマートカードチップとワイヤーループアンテナが含まれています。ほとんどの車のキーは、より広い範囲を提供するためにバッテリーを追加した、サミディアのやや複雑なバージョンです。  
銀行カードとは別に、最も普及しているアプリケーションは携帯電話SIMです。  
安価なカードを使用してより高価な電子機器をパーソナライズする戦略は、有料テレビのセットトップボックスからスマートメーターまで、他のアプリケーションに見られます。  
 攻撃が成功した場合、カードは比較的迅速かつ安価に交換できます。  
5。  
 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、公開鍵暗号化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、またはその両方（ハードウェア暗号化の方が簡単です）サイドチャネル攻撃から保護するため）。  
 シリアルI / Oとメモリの階層–プログラムと不変データを保持するROMまたはフラッシュ、ユーザーのアカウント番号、暗号鍵、PIN再試行カウンター、値カウンターなどの顧客データを保持するフラッシュまたはEEPROM。計算中に一時的なデータを保持するandRAM。  
 物理的、電気的、低レベルの論理接続は、ファイルシステムのようなアクセスプロトコルとともに、ISO 7816で規定されています。  
オーバーレイSIMを購入することもできます–コンタクトストップとボトムを備えた160ミクロン厚のスマートカード。これをJavaCardでプログラミングして、他のスマートカードでミドルパーソン攻撃を実行できます（ターゲットデバイスの上にオーバーレイを貼り付けます）。  
セキュリティエンジニアリング557ロスアンダーソン18。  
 スマートカードとその他のセキュリティチップ18。  
3セキュリティの進化スマートカードベンダーから初めて売り込みを聞いたとき-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る限り、やる気のある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いため、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いた「スタートレック」が1993年に突然暗号化されたことです。  
 これは多くの熱心なコンピュータ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。  
 クローン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3,000万ドルになったと報告されている[1330]。  
たとえば、一部の初期の有料テレビシステムでは、すべてのチャネルにアクセスできるカードを各顧客に提供し、導入期間後に顧客が購読していなかったチャネルをキャンセルするためのメッセージを無線で送信しました。  
 そのため、ベンダーがあなたのサービスをキャンセルできない場合でも、サブスクリプションをキャンセルできます。  
スマートカードをハッキングする方法（2）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EEP-Security Engineering558Ross Anderson18をフリーズさせる可能性があります。  
 プログラミング電圧VP Pを削除することによるスマートカードおよびその他のセキュリティチップROMの内容。  
 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の減少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、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。  
 大学時代に見つかった低コストのSEMは、数十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、強盗と同様に、誤報と見逃し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。  
 初期のスマートカードは、回路の微視的スケール、チップ表面の薄いガラスパッシベーション層、および通常はエポキシの一種であるポッティングを除いて、物理的な改ざんに対する保護がありませんでした。  
 ほとんどの場合、エポキシを溶解するのに十分な量の硝酸をオフミットする硝酸で十分です。  
 これらは、半導体業界で生産ラインのサンプルをテストするために使用されており、中古品を購入できます（図18を参照）。  
 チップのパッシベーション層に穴を開けるためのレーザーなどの特別なアクセサリーが付いている場合があります。  
 バストレースを記録できる場合は、プログラムの動作のトレースが得られます。  
）So3このような防御的なプログラミングは、コンピュータがトランジスタではなくバルブを使用し、数時間ごとに故障するために使用されていた初期のコンピューティングでは一般的でした。  
セキュリティエンジニアリング559ロスアンダーソン18。  
 スマートカードとその他のセキュリティチップ図18。  
5）。  
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、サービスの損失を被ります[2064]。  
 これを行う1つの方法は、制御ラインの接地されたマイクロプローブニードルを命令ラッチにドロップすることです。これにより、電源投入時にそこにある命令が繰り返し実行されます。  
 実際、かつてセキュリティエンジニアリング560ロスアンダーソン18。  
 スマートカードとその他のセキュリティチップ図18。  
 したがって、1つのプロービングニードルを使用して、カードに任意のコードを実行させ、理論的にはシリアルポートに秘密鍵の情報を出力させることができます。しかし、バスのメモリ内容を調べることは通常より便利です。  
 したがって、十分に理解されていなくても、試行錯誤によってメモリの線形化を実現できることがよくあります。  
 したがって、MSBバスラインをレーザーで撃つことにより、メモリを簡単に読み取ることができます[1781]。  
 最近のプロセッサには、メモリの線形化を妨げるトラップがあります。たとえば、数千の命令ごとにリセットされない限りカードをリセットするウォッチドッグタイマーなどです。  
 他にも多くの例があります。  
 一般的なターゲットの1つはテスト回路です。  
5。  
場合によっては、チップ内でヒューズが飛んで、攻撃者がファシリティを使用するのを止めます。  
 他の場合では、テストルーチンはパスワードで保護されています。パスワードは見つけることができます[1775]。  
7。  
 Adi Shamirは、CPUの乗算ユニットにエラーがある場合（単一の計算ab = cであっても、結果が常に1ビットで間違って返される場合）、RSA暗号文を復号化（またはRSA平文の署名）するように設計できることを指摘しました。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キングする方法（6）有料テレビカード業界が次に試みたのは、ハードウェア暗号化プロセッサを組み込むことで、攻撃者にソフトウェアのクローンを作成するだけでなく、ハードウェア回路を再構築させ、より高価なプロセッサを強制的に使用させることでした。彼らの海賊カード。  
 ハッカーはちょうど2つのチップ間のワイヤーをタップしました。  
 これが数千のゲートで構成されている場合、攻撃者は顕微鏡写真から手動で回路を追跡できます。  
 これで機器をレンタルでき、回路再構築ソフトウェアを購入できます。短いリソースは今やskillreverseエンジニアです。  
このようなラボは、チップメーカーの競合他社に代わって集積回路を分析し、特許侵害を探して、ビジネスの多くを獲得しています。  
 有料テレビカードのコピーが2002年まで犯罪にならなかったカナダにある多くの実験室（これらの実験室が有料テレビの運用者により訴えられた少なくとも2つの事件があったが）。  
スマートカードをハッキングする方法（7）1995年に、STMはチップ表面の保護シールドである新しい防御を開拓しました。  
5。  
 チップに電源が投入されるとすぐに、破損または短絡が検知され、チップがキーを上書きします。  
 1つのバイパスは、センサーラインを針でVDDに保持することですが、これは壊れやすい場合があります。他のベンダーは、実際の信号が送られる複数のセンサーラインを持っています。  
 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により、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、目的の信号を運ぶ金属ラインにメッシュを通して穴を開け、絶縁体でそれを埋め、絶縁体の中心を通して別の穴を開け、金属で埋め、そしてコンタクトを上部にめっきすることです。 X 'は数ミクロンの幅で、プローブステーションの針と接触します（図18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おり、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を損傷するのではなく、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）1998年に、Paul Kocherが微分電力分析（DPA）と呼ばれる新しい攻撃を発表したとき、スマートカード業界は揺さぶられました。  
 スマートカードメーカーは、1980年代以降、これが理論的に可能であることを知っており、いくつかの大まかな対策まで特許化していました。  
 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とらない場合、これはキーマテリアルをリークする可能性があります4。sideSecurity Engineering563Ross Anderson18の章を参照してください。  
 スマートカードとその他のセキュリティチップ図18。  
 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）フィーチャーのサイズが縮小するため、機械的なプロービング技術は着実に難しくなっています。  
 最初のレポートは、1995年にレーザーを使用して電圧を直接読み取る方法を説明したサンディア国立研究所からのものでした[32]。  
 2002年、セルゲイと私は、プロービングステーションの顕微鏡に取り付けられた写真用のフラッシュガンを使用して、ICの選択されたトランジスタに過渡故障を誘発することを報告しました[1782]。  
 フラッシュガンからレーザーにアップグレードすることにより、光伝導性を理解し、光を単一のトランジスターに集中することを学ぶと、多くの直接攻撃が可能になります。  
セキュリティエンジニアリング564ロスアンダーソン18。  
 スマートカードとその他のセキュリティチップマイクロコントローラーは、保護状態をラッチするフリップフロップを切り替えることで開くことができます。  
2002年の後半、セルゲイは同じ安価な顕微鏡に取り付けられたレーザーを使用して、マイクロコントローラーのメモリを直接読み取ることを報告しました。  
 デバイス全体でレーザーをスキャンすることにより、どのトランジスタがオンで、どのトランジスタがオンであるかをマッピングします。  
 侵襲性と非侵襲性の既存のカテゴリの間にあるため、攻撃を半侵襲的分析と名付けました。  
チップの前面からの光プローブは、約5年間最先端の技術でした。  
18と0。  
 チップの表面からの直接的な光プローブ攻撃は困難になりました。フィーチャサイズのせいではなく、金属層が邪魔になるためです。  
 グルーロジック（本質的にランダム化された配置配線）によって難易度が増加しました。  
 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。  
7はランダムなゲートの海のように見えます。  
 CPU、命令デコーダ、バスを見つけるには、いくらかの作業が必要です。  
」これらは、それ以来10年間、タンパーラボの主な研究目標を提供してきました。  
35µ。  
シリコンが透明な1µ。  
 物理的な制限の1つは、電荷キャリアの再結合に時間がかかるため、数MHzをはるかに超える帯域幅を取得できないことです。  
 シリコンの液浸レンズにより、レーザースポットサイズは約1ミクロンですが、OFI攻撃で28nmシリコンまでのシングルイベントアップセットを作成し続けることができます[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。  
5。  
7：–「グルーロジック」（Sergei Sko-robogatovの厚意による）を備えたSX28マイクロコントローラは、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]。  
チップメーカーは、別のVP Pプログラミング電圧でチップをターゲットとする攻撃が、レーザーを使用してチャージポンプを妨害することによって再発明されるのではないかと心配していました。  
 セルゲイの衝突攻撃は、第13章で説明されているロックへの衝突攻撃に触発されました。  
セキュリティエンジニアリング566ロスアンダーソン18。  
 スマートカードとその他のセキュリティチップしかし、おそらく最も重要な最近のブレークスルーは2016年で、フランククルボン、セルゲイスコロボガトフ、およびクリスウッズが最新世代の走査型電子顕微鏡を使用して、フラッシュとEEPROMの直接読み取りを自動化する方法を発見しました。  
 （私たちはこれをブローランプでパリンプセストを読むことと比較していました。  
 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その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ったことです。  
スマートカードのハッキング方法（12）中国のリバースエンジニアリングサービスでは、ゲートごとに30cが課金されるため、ブルートフォースアプローチは、チップ全体をリバースし、詳細に理解することなくシミュレータにドロップすることです。次に、あらゆる種類のオプションがあります。  
 シミュレーションを使用して、サイドチャネル攻撃を探したり、FIB編集を計画したり、デバイスをファジー化して他の脆弱性を探したりすることもできます。  
 1996年に早くも、英国のNatWestBankによる支払いトライアルで使用されていたMondexカードは、正式に検証されたオペレーティングシステムを誇っていました。  
 悪意のあるSMSは、国の攻撃者が標的のユーザーのSIMにマルウェアをダウンロードして、その場所を追跡できるようにするために使用されました[575]。  
5。  
ハードウェア乱数ジェネレーター（RNG）は、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。  
 弱いnonces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。  
 暗号化チップには、カウンター暗号化モードで使用される特別なキー生成キーがあった可能性があります。オペレーティングシステムはしばしば似たようなものを持っていました。  
5。  
 また、Windowsに組み込まれており、NSAトラップドアが含まれているように見えるNIST Dual-EC-DRBGについても触れました[1734]。 Ed Snowdenは後に、多くの技術系企業がライセンスしたツールでこの標準を使用するために、NSAがRSAに1,000万ドルを支払ったことを確認しました[1290]。  
 そのようなジェネレーターはテストするのが難しいことで有名です。障害は、温度、電源電圧、放射などの外部ノイズによって引き起こされる可能性があります。  
 多くの場合、暗号化製品は、環境と内部の両方の多くのソースからのランダム性を混ぜ合わせます[838]。これは、最高レベルの認証の要件です。  
 また、ハードウェアRNGは通常、独占的であいまいな設計であり、場合によっては単一のファブに固有であることにも注意する必要があります。そのため、微妙なバックドアが含まれていないことは言うまでもなく、設計が健全であることを確認することは困難です。  
暗号化チップの製造には通常、シリアル番号と暗号化キーがフラッシュまたはEEPROMにロードされるパーソナライズ段階が含まれます。  
 したがって、デバイスから出ることのない固有のキーを使用してチップを製造できるかどうかを尋ねる場合があります。  
 しかし、これには時間がかかり、チップ上のRNGも必要となるようです。  
 1980年代に、SandiaNational Laboratoriesは偽造できない紙幣の紙を作ることが可能かどうか米国連邦準備制度理事会に尋ねられ、彼らは光ファイバーをマッシュに切り刻むというアイデアを思いついたので、ユニークなスペックルパターン[1746]で各ノートを認識できました。 。  
 集積回路についても同様の工夫ができるでしょうか？ 2000年に、OliverとFritzK¨ommerlingは、金属繊維を搭載したローディングチップパッケージと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。  
 人々がデザインや他のパンフレットを提案するにつれて、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ますセキュリティエンジニアリング568ロスアンダーソン18。  
 スマートカードとその他のセキュリティチップは、エラー修正とともに、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マーケティングは、はるかに多くのことを主張することが多く、1つの主張（および研究目標）は、ハードウェアのチャレンジ/レスポンスメカニズムとして機能する「強力なPUF」です。  
 たとえば、パーソナライゼーション時にチップに1000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できます。  
2020年の最新技術は、マルチプレクサとそれに続くアービターのチェーンで構成されるXORアービターPUFです。  
 攻撃者が各回路パスの相対遅延を計算するのを困難にするために、多数のアービターの出力がXORされます。  
 同じ著者がHeikoLohrkeとChristian Boitと協力して、チップの発光によって導か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できるようになり、PUFのエントロピーが大幅に減少します[1859]。  
これらは、パーソナライゼーション、保証、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ていることが多いため、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はわかりません。最後に、PUFの強度は、fabが排除しようと最善を尽くすバリエーションに依存するため、シリコンプロセスの変更により、突然PUF設計が不安定になる可能性があります。  
5。  
 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。  
 ユーザーがクリッパーにプレーンテキストと暗号化用のキーを提供すると、チップは暗号文だけでなく、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提供のキーを含む法執行アクセスフィールド（LEAF）も返しました。  
5。  
よくあることですが、失敗したのは改ざん防止ではなく、プロトコルです。  
 ClipperはCapstoneチップに置き換えられ、暗号戦争は別の方法で続行され、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。  
高電圧プログラミングパルスは、2つの金属層間のポリシリコンを通る導電経路を溶かすために使用されます。  
 最近の変種はスポット破壊PUFで、トランジスタのバンクに約半分の電圧がゲート酸化膜の破壊に耐えるだけ長い間十分に高い電圧が印加され、ランダムな障害が発生して1と0として読み取られます[422]。  
 アンチヒューズデバイスをリバースエンジニアリングするには、基本的に3つの方法があります。  
 そのようなチップはすべて、プログラミング中にビットストリームを読み返して検証するために使用されるテスト回路を備えており、多くの場合、後で単一のヒューズを溶かすことによってこれを無効にしました。  
 次に、FIBを使用してそれを修復するか、2本のプローブ針でブリッジして、ビットストリームを読み取ります。  
•多くのヒューズを読み取る必要がある場合、AESキーの格納に使用される場合と同様に、ブルートフォースアプローチは、一度に1層ずつチップを剥ぎ取り、ヒューズを直接読み取ることです。それらは、適切な化学的染みの下で見えるようになります。  
•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。  
5。  
 キーを1ビットずつ読み取るために、いつでも光障害誘導を試すことができます。また、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するかもしれません。  
 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、ロールバックを許可すると、顧客は古いビットストリームを再生してアップグレードを回避できる可能性があります。  
 したがって、停止して、だれかが破損したアップグレードによって製品ベースを破壊しようとする可能性があるかどうかを考えてください。もしそうなら、あなたは安全なビットストリームローダーを検討するかもしれません。  
2番目のタイプのラージチップセキュリティ製品は、認証ロジックが組み込まれたシステムオンチップ（SoC）です。  
 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のプレミアム価格の請求が含まれており、販売者はコピーコントロールテクノロジーを使用して、コンソールのベンダー料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プロトコルは単純であり（プロトコル攻撃が見つからなかったため）、ランダム化されていました（攻撃者はトランザクションの繰り返しから何も学ぶことができませんでした）。  
 小さなチップの認証ロジックでは、トップメタルシールド、コピートラップ、レイアウトの難読化を行って非表示にする必要がありますが、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。  
 この慣行は、いくつかの興味深いエッジケースをもたらしました。  
セキュリティエンジニアリング571ロスアンダーソン18。  
 スマートカードとその他のセキュリティチップ今日、私たちがどこでも見つけている魔法のデバイスをどのようにハッキングすることができますか？メモリの読み出しは、最も信頼できる攻撃パスになり得ます。  
 プログラミング方法を知っている糖尿病患者は、自分のインスリンポンプを制御することを好みますが、ベンダーは市場管理と責任の両方の理由から、それらを停止しようとします。  
 分析は[1778]で説明されています。初期の例は、Markus KuhnがDS5002プロセッサで発明した暗号化命令検索攻撃です[1102]。  
 Markusは、プロセッサの命令の一部に目に見える外部効果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に対する積極的な攻撃を示しました。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によって提示されました。  
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、そのコンテンツは組み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）。  
 これで、半ダース以上の試行を行うことができます。  
 詳細は[1777]にあります。  
5。  
私が言及する3番目のタイプの攻撃は、厳密に言えばサイドチャネルですが、高度な暗号チップを攻撃する主要な方法の1つになりつつあるため、ここで紹介する発光分析です。  
 これは、高価な単一光子計数光電子増倍管を使用して古い0からAES鍵を読み取るJulie FerrignoとMartin Hlavacによって、2008年に最初に暗号実装を攻撃するために使用されました。  
12µ [681]。  
5Vから2Vにすると、光子出力が6倍になります。  
 次に、AESアルゴリズムのタイミングが確立されたら、ラウンドキーごとに1がかかることを知っていました。  
0の場合は5V。  
 2001年にアクテルの設計について相談したので、これはかなり恥ずかしいことでした。  
7メタルレイヤーとフラッシュメモリを備えた13µテクノロジー、および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が組み込まれています。侵略的にそれを読むのは退屈だったでしょう。  
 光学放射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したい場合は、暗号化と同じように放射を観察します。これにより、フォールトアタッカーの光学的に強化されたパワー分析を試すときにレーザーの狙いを定めることができます。 。  
18。  
6最先端の機能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？ 1990年代後半にすべてが壊れ、この本の2001年版では、次のように書いています。「熟練した攻撃者による侵入に対してスマートカードを耐性にすることができる、私が知っているテクノロジーまたはテクノロジーの組み合わせはありません。  
。  
 あなたは一年の遅れ、百万ドル以上の予算、そして成功の確実性を見ることはできません。  
 したがって、攻撃者は追いつき始めています。  
5。  
2007年には、少数のスマートカードOEM、少数のリバースラボ、および少数の関心のある研究者がいました。現在、多くのチップメーカーは顧客から改ざん防止を求められており、ルーターからRaspberry Piへの製品は、永続的なマルウェアに対抗するためのある種の安全なブート機能を獲得しています。  
 また、特に中国では、互換性を確保するためにデバイスをリバースする需要が高まっているため、商業用リバーシングラボの成長が促進されています。  
その結果、攻撃者はより多く、より効率的になっています。  
セキュリティ経済は依然として大きな弱点であり、セキュリティチップは多くの場合レモンの市場に出回っています。  
 購入の動機はコンプライアンスであり、実際のセキュリティが運用と衝突する場合、コンプライアンスを容易にするように設計されたより弱い標準を確認することは当然のことです。  
 ISO19790を支持するFIPSのほぼ棄権とCommon Criteriaで宣伝されているさまざまな保護プロファイルは、英国がCriteriaから離れるように、さらに混乱を招きます。  
 しかし、これは問題でしょうか？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オーダーのHSM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。  
 あなたは悪い端末がそれが見るすべてのEMVカードに対して生産力分析攻撃をすることができるようにしたくありません、しかしそれが起こったとしてもそれはmag-stripeカードがクローンされた方法であるのでそれは世界の終わりではありません、そしてダメージを制限する方法を知っています。  
 Butpay-TVは現在有線ブロードバンドに移行しており、より安全なチップが損失を削減する唯一の方法ではないことを企業は学びました。対策は効率的に連携します。  
5同僚のフランククルボン、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。  
6。  
ベンダーは、Certication要件を満たすために必要なだけの金額を費やしますが、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戦いの場であり続けると思います。  
 ただし、互いに認証する2つのデバイスのうち少なくとも1つが少なくとも時折オンラインになる場合、保護要件は衛星TVよりもはるかに厳しくありません。  
18。  
18。  
1信頼できるインターフェイスの問題上記のセクションで説明したデバイスには、本当に信頼できるユーザーインターフェイスはありません6。  
 しかし、2000ドルの4765または2ドルのスマートカードを使用してデジタル署名を行う場合でも、それらを駆動するPCは信頼できます。  
com $ 47。  
確かに、それはおそらくあなたの状況を悪化させます。  
 これの歴史と政治については、後でセクション26で説明します。  
2。  
 業界は数十の認定製品を正式に生産しています。  
 ですから、ロビイストは働いていて、今やあなたが税金を申告するためにロビイストを使うように要求する国もあります。  
セキュリティエンジニアリング575ロスアンダーソン18。  
 残存リスク相互作用;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ーを組み合わせました。  
 この場合、セキュアエレメントには、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がわかりませんでした。  
 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。  
6。  
 銀行では、カード発行者、端末の所有者、および顧客が異なります。クローンされたカード、偽の末端、ギャングランド商人、および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。  
18。  
3レモン市場、リスクダンピング、評価ゲームここで説明するHSMからFPGA、スマートカードに至るまでの各製品カテゴリには、保護の品質に幅広いばらつきがあるさまざまな製品があります。  
第1に、セキュリティエンジニアリングが576Ross Andersonであるかどうかに関係なく、高レベルの保証での提供は比較的少ない18。  
 RESIDUAL RISKFIPS-140レベル4または4を超えるCommon Criteriaレベル。  
 これはレモン市場につながります。そこでは、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製品を買いたがります。  
 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。  
 それは逆の場合にも起こりました。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おり、マイクロプローブに対する実際の防御策なしにチップ上で実行されました。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、リスクを最小限に抑えるのではなく、セキュリティで保護されたプロセッサを使用しています。  
 医療から防衛まで、購入者が実際の保護ではなく証明書のセキュリティを求めてい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。  
18。  
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。  
 CommonCriteria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。  
 覆い隠しはまた、輸出承認の一般的な要件であり、それが意図的な脆弱性をカバーしているという疑いにつながりました。  
 暗号化機能を組み込んだ多くの製品は、乱数ジェネレーターが十分にランダムではなかったために壊れており[775、576]、前述したように、NSAはNISTに弱い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。  
セキュリティエンジニアリング577ロスアンダーソン18。  
 では、1つの保護策を講じる必要がありますか？開発環境にエアギャップを設ける必要があるかどうかについては、2020年の1つの問題が解決しています。  
 これらの企業は現在、攻撃者が高度な永続的脅威を使用して会社のインフラストラクチャ全体を所有することになるリスクを強調するように評価者に要求しています。  
賢い評価者は、そのようなゲームマンシップに夢中にならないでしょう。  
 業界は初期に自社製品に対して敵対的な攻撃を行わなかったため、その製品は脆弱であり、最終的に他の製品によって破壊されました。  
 しかし、インセンティブはまだ間違っています。賢明なベンダーは、最も簡単な乗り物を提供する評価ラボに行きます。  
2。  
2。  
6。  
 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、他者が管理す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、「これは問題ですか？ 。  
。  
」当時、南アフリカで、SIMスワップ攻撃の1つの報告されたケースがありました。  
「そうです。 SIMスワップは現在米国で主流になっています。  
 ほとんどの国では、電話会社は顧客に対して顧客の認証に失敗したことに対して銀行が責任を負うことはありません。  
 しかし、SIMスワップの詐欺がほとんどないインドでは、規制当局は電話会社がSIMスワップ詐欺の責任を共有する必要があると判断し、SIMを販売する前に、電話会社は顧客の指紋を全国のAadharデータベースと照合する必要があります。  
7では、何を保護すればよいのでしょうか？このような複雑な世界で、改ざん防止チップが追加できる価値は何ですか？セキュリティエンジニアリング578ロスアンダーソン18。  
 では、何を保護する必要がありますか？まず、情報処理を単一の物理トークンに結び付けることができます。  
 これは、プリンターベンダーが安価な競合他社とだけでなく、任意の本物のインクカートリッジで製品を動作させることを望んでいるアクセサリーコントロールにも適用されます。  
 デバイスが盗まれたとしても、販売できるサービスの合計額は限られています。  
第三に、人間のオペレーターを信頼する必要性を減らすことができます。  
 安全な電話の暗号化イグニッションキーは、盗難者が正当な所有者になりすますことのみを許可し、実際のデバイスへのアクセス権があり、キーも電話も盗まれていない場合に限ります。  
第4に、セキュアブートを監視する物理的な信頼のルートを保護できるため、マルウェアの永続化が困難になります。  
 1つの質問は、自分のデバイスでLinuxの独自バージョンを実行したい活動家が実際にTPMを破らなければならないのか、それとも単に無視してマルウェアのリスクを自分で管理できるのかということです。  
 これには、リバースエンジニアリングが難しいFPGAにデザインの一部を埋め込むか、TPMを使用してデバイスがエコシステムで機能するために必要な資格情報を制御する必要があります。  
 工場が製品を出荷するときに、多くの資格情報をリリースするだけです。  
 これは、初期の製品障害の原因となる安価なノックオフから、国家の敵による高度なサプライチェーン攻撃まで、多くの罪をカバーしています。  
 この章で説明する手法は、多くのツールと同様に、偽造品との戦いにも使用できます。国家安全保障上の懸念の1つは、防衛システムが海外で製造されたチップにますます依存するようになるにつれて、ファブは後の攻撃を容易にするために追加の回路を導入する可能性があるということです。  
 これは2010年頃から重要な研究の対象となっており、プレシリコンとポストシリコンの両方でトロイの木馬を検出するメカニズムが開発されています。たとえば、「ゴールデン」リファレンスチップと評価のターゲットの差分サイドチャネル分析を行うことができます[1775]。  
8。  
 この分野の調査については、Xiao etal [2053]を参照してください。  
 ただし、これらのアプリケーションに共通しているのは、周囲の環境の信頼性とは無関係にセキュリティプロパティを提供できることです。  
 一般的なメカニズムは何度も失敗します。セキュリティは、システムに水をまき散らして、悪いことを起こさないようにする魔法のピクシーダストではありません。  
 注意しないと、アプリケーションのスマートカードや暗号化モジュールにお金がかからず、わずかしか追加されない場合があります。また、運が悪い場合は、業界が法的義務や業界標準を求めて、製品の使用を強制していることがわかります。  
8要約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。  
研究の問題改ざん防止プロセッサの設計には、基本的に2つの研究があります。  
 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？セルゲイスコロボガトフの2018年の第2回講演「ハードウェアセキュリティ：現在の課題と今後の方向性」[1780]の最良のガイド。  
 適度に保護されたチップを効果的に使用して、さまざまな種類の攻撃スケーリングを阻止するにはどうすればよいですか？セキュリティエンジニアリング580ロスアンダーソン18。  
 概要さらに読む私は、ハードウェア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（暗号用）、HOST（トロイの木馬とバックドア）、FDTC（フォールト攻撃）、Cardis（スマートカード）などの最新の論文がしばしば会議に登場します。  
初期の歴史–加重コードブックと水溶性インク– readDavid Kahnの本「The Code Breakers」[1001]。  
 言及されているIBM製品には、オンラインで豊富なドキュメント[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。  
リバースエンジニアリングでのFIBの使用方法に関するIO 2019 [1975]と、チップ防御テクノロジーの進化に関するChris Tarnovskyによる同じイベントでの講演[1862]。