どちらかの軍のスティリーのハムが聞こえます。固定された歩哨がほとんど受け取ることお互いの時計の秘密のささやき。火は火に対応し、その火炎を通して、各戦いは他のアンバーの顔を見ます。  
–ロジャーニーダム  
コンピュータや電話などの電子機器は、あらゆる方法で情報を漏洩します。  
サイドチャネル攻撃はいたるところにあり、そのうちの3〜4は数十億ドルの損失を引き起こしています。  
第1に、伝導または放射された電磁信号があり、ローカルで、場合によってはより長い距離で情報が侵害される可能性があります。  
冷戦の終結後、人々は通常誰も聞いていなかったことに気づき始めました。  
第2に、サイドチャネルは、単一のデバイス上のタスク間、または密接に結合されたデバイス間でデータをリークします。これらは、電力とタイミングの両方の情報を利用でき、共有システムリソースの競合も発生させます。  
3。  
これにより、2020〜5ですべてのスーパースカラーCPUが再設計される可能性があります。  
近くのキーボードで入力されたキーストローク、または実際に独自のタッチスクリーンのキーボードで電話が聞こえた場合など、共有されたローカルの物理リソースを悪用する攻撃があります。その検出は、マイク、加速度計、ジャイロ、さらにはカメラ。  
これまでのところ、電話や他のIoTデバイスに対するサイドチャネル攻撃は、大きな影響を与えるように拡大されていませんが、さらに多くのものが存在しています。  
最後に、共有されたソーシャルリソースを悪用する攻撃があります。  
これにより、多くの不十分なポリシー決定と、プライバシー法から逃れるために個人データを十分に匿名化できるかどうかについての多くの希望的な考えが生まれました。  
これに1ドルの価値を置くことは困難ですが、第11章で説明したように、医学研究などの分野では重要です。  
実際のスケーラブルな脅威を見落としたり、影を追いかけてお金を無駄にしたりせずにシステムを長期間保護したいセキュリティエンジニアは、基本を理解する必要があります。  
19.2エミッションセキュリティ  
テンペストを心配しているのは主に軍事組織です。コンピューターや他の電子機器から放出された漂遊RFが対戦相手によって拾われ、処理されているデータを再構築するために使用されます。  
。  
 および無線周波数干渉（RFI）  
 意図的にそれらを破壊する武器。  
 ますます多くの日常のデバイスがワイヤレスネットワークに接続され、デバイスがより多くのセンサーを取得するにつれて、これらすべての問題（RFI / EMC、サイドチャネル、電子戦の脅威）が悪化する可能性があります。  
19.2.1歴史  
彼らは、各回路をツイストペアにするために間隔をあけてワイヤーを交差させることを学びました。  
フランダースの泥沼に押し込められたユニットを接続するためにフィールド電話線が敷設され、数百ヤード離れた敵の塹壕と平行に数マイルも走ることがよくありました。  
地球の漏出が敵側からのメッセージを含むクロストークを引き起こすことがすぐに発見されました。  
1915年までに、バルブ増幅器は、漏電聴取範囲を電話用に100ヤード、モールス符号用に300ヤードに拡張しました。  
1916年までに、アースリターンサーキットは正面から3000ヤード以内で廃止されました[1380]。  
1950年代を通じて、米国と英国の両方が、独自の暗号化マシンからの電磁気的および音響的発散の抑制に苦労しました。 1957年から、テンペストの排出に対して「合理的に十分に保護された」マシン、KW-27がありました。  
1960年代までに、NATOはテンペスト基準に関する作業を開始しました。アメリカとイギリスは、ヨーロッパの同盟国に選択的で不完全な安全保障アドバイスを与えたので、彼らは彼らをスパイし続けることができました。  
アメリカ人とイギリス人がこれに気づいたとき、彼らはシークレットとそれ以上でのトラフィックの一時的なギャップとして手動のワンタイムパッドを使用し、脆弱な大使館のシールドされた部屋に暗号装置を置き始めました[600]。  
その後、排出量の安全保障は分類されたトピックになり、1980年までに設定された秘密のNATO規格は2000年に分類解除されただけでした。  
コンピュータデータも漏洩する可能性があるという事実は、オランダの研究者であるWim van Eckが改造されたテレビセットを使用してVDUで距離を置いて画像を再構成する方法を説明する記事を発表した1985年に注目されました[601]。排出量の安全保障と関連トピックに関する公開された研究は、後で説明するように、1990年代に始まりました。  
19.2.2技術監視と対策  
 ターゲットのデバイスがマルウェアに感染したとき。  
この段階で敵がそれを捕らえることができれば、その後の防御策はあまり役に立たないでしょう。  
これらのデバイスの主な制約は、バッテリーの寿命です。  
•次のステップでは、主電源、電話ケーブル、またはその他の外部電源から電力を引き出すデバイスがあり、無期限に使用できます。  
最近の同等品の中には、キーボードケーブルに接続されてコネクタのように見えるものがあります。電気アダプタのように見えますが、オーディオとビデオを所有者に送り返すものもあります。  
現在、ほとんどの携帯電話テクノロジーが使用されています。それらは、呼び出されたときに聞いて見るカスタムハンドセットとして見ることができます。  
それはアメリカ合衆国の大シールの木製のレプリカで、大使は彼の住居のオフィスの壁にそれを掛けました。  
冷戦の終わりまで、モスクワの大使館は定期的にマイクロ波を照射されていたので、技術の変種がおそらく使用され続けた。  
1984年、モスクワの米国大使館のIBM Selectricタイプライターで16個のバグが発見されました。それぞれが8つのキー操作を保存し、1回のバーストで送信しました。  
•レーザーマイクは、窓ガラスなど、対象の会話が行われている部屋の反射面または部分反射面にレーザービームを照射することで機能します。  
•しかし、現在、世界中の監視の大部分がクリープウェアによって行われている可能性があります。熟練した攻撃者によってリモートで、または強制的または操作的な家族によって、あるいは時には雇用条件として、ターゲットの電話にインストールされたソフトウェアによって。  
 そのような攻撃に対する保護を提供するためのツールの完全な袋を持っています。  
直接シーケンスのスペクトラム拡散は、そのパワースペクトルから見つけることができ、周波数ホッパーは通常、連続したスイープの異なる周波数で観測されます。  
しかし、監視受信機の有効性は、正当な携帯電話と同じ周波数とプロトコルを使用するバグによって制限されます。  
•非線形ジャンクション検出器は、至近距離にある隠れたデバイスを見つけることができます。  
ただし、バグが正当な機器内またはその近くに植え付けられている場合、非線形ジャンクション検出器はあまり役に立ちません。  
•実験室の周りに木を植えるなどして視線をそらすことは、レーザーマイクに対して効果的ですが、実際的でない場合があります。  
•一部の施設にはシールドルームがあり、バグが導入された場合でも、信号は外部に聞こえません[132]。  
 物理的なセキュリティと音響シールドの両方を備え、バグがないか定期的に掃除されます。脅威評価が有能なやる気のある対戦相手が十分に近づく可能性があることを示唆する場合、SCIFも電磁シールドを備えている可能性があります。  
音響および電磁シールドを備えたプレハブの部屋を販売するベンダーがあります。  
モスクワにある新しい米国大使館の建物は、構造内に多数のマイクが見つかったために放棄されなければなりませんでした。イギリスの対諜報機関のサービスは、新しい本社の建物の大部分を解体して再建することを決定しました。建設請負業者の1人の従業員が暫定IRAとの過去の関係を持っていることが判明した後、5000万ドル。  
技術の進歩により、バガーの生活は着実に楽になり、防御者の生活はますます困難になっています。  
ノートパソコン、タブレット、または携帯電話が、オーディオを録音して後でアップロードするクリープウェアを実行しているだけではありません。  
 物事はその存在下で言った。  
しかし、既存の電子機器を悪用する方法には、さらに多くの微妙な方法があります。  
19.3パッシブアタック  
ここでは光信号を除外し、後で音響攻撃と一緒に説明します。  
信号は、何らかの種類の回路（電力線や電話線など）を介して伝導できます。  
これらは軍によってそれぞれ「ハイジャック」と「テンペスト」と呼ばれています。  
たとえば、コンピュータから放射された無線信号は、主電源によって拾われ、近くの建物に伝導されます。19.3.1電源ケーブルと信号ケーブルを介した漏れ  
電源と信号ケーブルを適切にフィルター処理することで、注意深い設計により伝導情報の漏洩を抑制することができます。  
軍事用語では、赤い機器（機密データを保持）  
。  
しかし、コストはそれだけではありません。  
スタッフ全員がクリアランスを必要とするため、請負業者は高価です–排出ガス安全のためのNATO標準SDIP-20（以前のAMSG 720B）  
  
1972年にグラスゴー学校のコンピュータセンターでプログラミングを初めて学んだとき、1.5 MHzクロックのIBM 1401がありました。  
一部の人々はこれをデバッグ補助として使用しました。  
これがいたずらや楽しみのために使用できるとは思いもしませんでした。  
ビーム電流は、ドットレートの多くの高調波を含むビデオ信号で変調されます。その中には、金属コンポーネントと共振し、他のものよりもよく放射するものがあります。  
Wim van Eckがこれを発見し、1985年に公開しました[601]。機器の設計については彼の論文で説明されており、詳細は[1105]で説明されています。  
。  
ハンスゲオルクウルフは、8メートルの距離にある現金自動預け払い機からカードとPINデータを回復できるテンペスト攻撃を実証しました[1095]。  
軍の専門知識と装備は分類されたままであり、防衛界以外では利用できませんでした。  
これにより、オランダ政府は投票機器を「ゾーン1-12dB」のレベルでテンペストテストする必要があると定めました。  
ゾーン0として認定された機器は、1メートルの距離で悪用される可能性のある信号を放出してはなりません。対戦相手が隣の部屋にいても、壁は石膏ボードのように薄っぺらなものであっても、データを電子盗聴から保護する必要があります。  
 平均µV図19.1：–東芝のラップトップからのRF信号は、3つの石膏ボードの壁を通して数部屋離れた場所に再構築されました（Markus Kuhn [1104]の厚意による）  
-12dBの基準は、投票機が5メートル離れた盗聴者に投げられた投票に関するデータを漏らしてはならないことを意味します。  
ゾーニングの技術的な詳細は、[343]のように、2007年にドイツ人によって簡潔に公開されました。  
しかし、ゾーンリミットカーブを除くすべてがパブリックドメインにありました。ゾーンリミットカーブは、ニアフィールドドロップオフとファーフィールドドロップオフの違いを考慮に入れて、小さなダイポールアンテナまたはループアンテナからの20m、120m、1200mの距離間のワーストケースの相対減衰です。  
冷戦終結後、軍事予算が大幅に削減されて以来、ゾーンシステムは政府によって広く使用されるようになりました。  
スノーデン紙は、米国の主要なテンペストターゲットがニューヨークの国連外交使節であることを明らかにし、そこでさえ、そのような手法は、マルウェアを使用してコンピューターが危険にさらされなかったほんの一握りの国に対してのみ使用されました。  
 ほとんどすべての機器。  
どの機器が何を放射するかを知ることにより、施設の境界から最も離れた機器に関する最も機密性の高いデータを保持し、本当に必要な場合にのみ物をシールドすることができます。  
Markus Kuhnと私は、「Soft Tempest」と呼ばれる低コストの保護技術を開発しました。これは、しばらくの間、電子メール暗号化プログラムからオランダの投票機まで、一部の製品に導入されました[1105]。  
VDUからの情報を伴うRFエネルギーのほとんどがスペクトルの上部に集中していることを発見したので、適切なローパスフィルターで畳み込み、標準フォントのフーリエ変換の上位30％を削除しました（参照図19.3および19.4）  
図19.3 –通常のテキスト図19.4 –テキストのローパスフィルターこれは、ユーザーに表示される画面のコンテンツにほとんど気づかれない影響を及ぼします。  
図19.5 –画面、通常のテキスト図19.6 –画面、フィルタリングされたテキストただし、図19.7および19.8の写真に示すように、放出されるRFの違いは劇的です。  
ゾーンの違いに変換されたVDUでのソフトテンペストテクニックの使用[108]。  
図19.7 –通常のテキストのページ図19.8 –フィルタリングされたテキストのページただし、攻撃者はアクティブおよびパッシブの手法を使用できます。  
図19.9および19.10は、ビデオ信号が2 MHzのRFキャリアであり、300および1200 Hzの純粋なトーンで変調されている場合のPCの画面を示しています。  
そして、諜報機関はこれを知っていました。1995年のテレビのドキュメンタリーで、経済スパイでソフトウェアベースのRFを利用したCIAの報告がありました[1062]。電気通信および自動化された情報システム機器から。」マルウェアの可能性は、Tempestテストがテスト対象のデバイスを受動的に聞くだけでなく、対戦相手がデバイスを乗っ取るためにソフトウェアエクスプロイトを使用して最悪の場合の攻撃をシミュレートする信号を注入することを含む1つの理由です隠れチャネル[252]を設定します。  
機密データを処理する機器が携帯電話の近くで使用されている場合、電話のトランスミッタが機器に電流を誘導し、非線形ジャンクション効果によって機密データで変調されて再放射される可能性があります。  
ノンストップ攻撃は、船や航空機にとってEmsecの主要な懸念事項でもあります。ここでは、パッシブテンペスト攻撃を実行するのに十分近づくことができる攻撃者は、盗聴よりもはるかに深刻な害を及ぼす可能性がありますが、軍事船や航空機は非常に強力な無線機やレーダーを運ぶことが多いため、信号に注意する必要があります敵に役立つ何かで誤って調整されます。  
  
Ed Snowdenが確認したように、敵国の大使館に対するEmsecの脅威は現実のものです。  
 ソリューションの一部になります。  
防御面については、2007年4月に米国の沿岸警備隊の船舶に機器を設置するときにロッキードマーティンがテンペスト基準を無視していたことが判明したスキャンダルがありました。  
これらのドキュメントは、エミッションセキュリティの欠陥（ケーブルタイプの誤り、ケーブル分離ルールの違反、接地の誤り、フィルターの欠落、赤/黒の違反など）だけでなく、より一般的には失敗した仕事についても物語っています。  
これは議会の調査につながりました。  
最近の進展は、スマートフォンに対するテンペスト攻撃です。  
このような攻撃の主な問題は、通常、電話のクロック周波数がワークロードによって異なることです。この周波数をどうにかして固定できる場合（例：  
 その後、攻撃ははるかに簡単になります。実際、攻撃は、次に説明する種類の標準的なタイミング攻撃に減少します。  
19.4コンピュータ間およびコンピュータ内の攻撃  
簡単な例として、高度なプロセスは、時間tiで共有リソースをビジー状態に保ち、秘密鍵のi番目のビットが1であることを通知できます。  
。  
ノイズを導入することにより、隠れチャネル容量を制限することもできます。  
しかし、一部の隠れチャネル容量はほとんど常に[808]のままです。  
これは、多くのトップシークレットの衛星画像を漏らすことを難しくしますが、256ビットの暗号キーを漏らすことは当然です。  
また、ソフトウェアがネットワーク上の通信を開始できる分散システムでは、隠れチャネルを分析してブロックすることがさらに困難になります。  
そのようなチャネルは、暗号鍵を密輸するのに十分な帯域幅を簡単に持っています。  
  
1996年に、Paul Kocherは、RSAやDSAなどの公開鍵アルゴリズムの多くの実装が、かかった時間を通じて鍵情報を漏らしたことを示しました[1064]。  
Paulのアイデアは、指数を一度に1つずつ推測し、この推測の結果をタイミング測定に反映させ、分散が減少するかどうかを確認することでした。  
2003年までに、David BrumleyとDan BonehはOpenSSLを使用してApacheに対するタイミング攻撃を実装し、約100万回の復号化のタイミングでリモートサーバーから秘密鍵を抽出する方法を示しました[330]。  
。  
対称鍵ブロック暗号も脆弱です。  
攻撃者は、推測された値がS-boxルックアップでキャッシュミスを引き起こすかどうかを予測し、これを観察に対して検証することにより、暗号の最初のラウンドの出力についての推測を検証できます。  
多くの暗号ライブラリとツールキットは脆弱です。それらがアプリケーションの問題であるかどうか、そうである場合はどうするかを検討する必要があります。  
  
タイミング攻撃は遠くからでも機能しますが、ターゲットの機器に近づくことができれば、さらに多くのことができます。  
電力分析またはレールノイズ分析として知られていますが、これには、接地線に抵抗を挿入し、それを横切ってデジタルストレージスコープを接続して、デバイスの電流引き込みを観察するだけで済みます。  
これは、一度に1バイトずつ推測し、正しいバイトが推測されたときに別の電力トレースを探すことにより、マイクロコントローラーからパスワードを抽出する方法を示しています。0.9 −5  
。  
多くの状況での主なデータ依存の寄与は、非常に大きいバスドライバートランジスタによるものです（図18.7の上部を参照）。  
設計に応じて、電流は、状態が変化するバスの各ビットについて、数百ナノ秒の期間にわたって数百マイクロアンペア変化する可能性があります[1298]。  
 攻撃者に見えます。  
EEPROMの読み取りと書き込みは、さらに強力な信号を提供できます。  
。  
理解する（または推測する）攻撃者  
これは、1998年に、Paul Kocherによってタイミング攻撃のために開発された信号処理のアイデアを効率的な手法に適合させて、DESなどのブロック暗号で使用されるキービットを電力トレースのコレクションから抽出することで、業界の注目を集めました。カードソフトウェアの実装の詳細を知らずに[1065]。  
サブセットが関心のある情報と相関している場合、その差はゼロではないはずです[1067]。  
次に、暗号の内部状態の一部を推測します。  
したがって、攻撃者がアクセスできる暗号文である場合、攻撃者は最後のラウンドでSボックスへの6つの入力ビットを推測します。  
次に、平均トレースが計算され、比較されます。  
このプロセスは、ターゲットSボックスへの64個の可能な6ビット入力のそれぞれに対して繰り返されます。  
ただし、推測が間違っていると、トレースがランダムにソートされるため、差分トレースはランダムノイズのように見えます。  
DESの場合、これは56キービットのうち48を与えるので、残りは簡単に見つけることができます。  
これは非侵襲的な攻撃であるため、疑いを持たない顧客が携帯する銀行カードに対して改造された端末機器によって実行できます。  
ポールの発見は、人々が防御に取り組む間、銀行でのスマートカードの導入を2〜3年間遅らせました。  
一部はプロトコルレベルで機能します。たとえば、銀行カード委任のEMVプロトコル（バージョン4.1以降）  
このようにして、カードの外に見える2つの暗号文が同じ鍵を使用して生成されることはありません。  
このようにして、暗号の実装は、呼び出されるたびに変化します。  
より高価なカードには、モジュラー乗算とDES / AES専用の暗号化エンジンがあります。  
テーマには多くのバリエーションがあります。  
もう1つのバリエーションは、異なるセンサーを使用することです。DavidSamydeとJean-Jacques Quisquaterが作成した電磁分析では、デバイス全体の電流に単に依存するのではなく、チップの表面上で小さなピックアップコイルを動かしてローカル信号をピックアップします[1568 ]。  
Eyal Ronen、Colin Oˆa˘A´ZFlynn、Adi Shamir、Achi-Or Weingartenがフィリップスフエランプを乗っ取ることができるワームを実証したときに、電力分析攻撃の開発が進んだ後、2016年に電力分析の壮大なデモンストレーションが到着しました。これらのランプがファームウェアの更新を認証するために使用したAESキーを取得します[1614]。  
更新はZigBeeによって伝播する可能性があるため、マルウェアは1つのランプから次のランプへ連鎖的に拡散する可能性があります。著者らは、パリなどの都市では、核分裂のように連鎖反応が自立するのに十分なランプがあることを示しました。  
詳細については、たとえば、Marios ChoudaryおよびMarkus Kuhn [419]を参照してください。  
  
1996年、Markus Kuhnと私は、電源またはクロックラインに過渡電流またはグリッチを挿入すると、多くのスマートカードが壊れる可能性があると報告しました[106]。  
リセットを引き起こさずに、単一のクロックパルスを2つの幅の狭いパルスに置き換えることができますが、プロセッサに、実行するはずの命令ではなくNOPを実行させる必要があります。  
翌年、Dan Boneh、Richard DeMillo、Richard Liptonは、ランダムエラーが誘発されると、多くの公開鍵暗号アルゴリズムがひどく壊れることに気づきました[285]。  
d（mod pq）  
しかし、カードがpを法として正しいがqを法として正しくない欠陥のある署名Spを返す場合、p = gcd（pq、Se p ffi h（m）  
 これはシステムをすぐに壊します。  
、そしてメモリのどこにキーが保持されているかがわかっているので、暗号化を行い、先頭ビットをゼロ化し、別の暗号化を実行して結果が異なるかどうかを確認し、次のビットをゼロ化するなどして、キーを見つけることができます。 。レーザーによって引き起こされる不具合は、チップへの攻撃に限定されません。  
Kevin Fuらは、音声コマンドでレーザーポインターを変調することにより、数十メートル離れた場所からそのようなデバイスをアクティブにできることを発見しました。そのため、庭から窓を通してレーザーポインターを照らすことにより、Alexaに家の玄関のドアのロックを解除するように命令できました]。  
上記のセクション19.3では、光学的に強化された位置固定電力分析について説明しました。これは、電力分析中にレーザーを使用してターゲットトランジスタを部分的にイオン化します。  
  
非常に深刻なチップレベルのサイドチャネルは、DRAMメモリの内容が隣接する行にリークする可能性がある場合です。  
翌年、Mark SeabornとThomas Dullienは、アプリケーションコードがこのハードウェア障害を悪用してカーネル特権を獲得する方法を発見しました[1694]。  
脆弱なタイプのDRAMはまだ広く使用されており、攻撃は非常に多くの異なるソフトウェアメカニズムを対象としているため、しばらくの間存在する可能性があります。  
 ここで、DRAMチップコントローラは行を更新して、最も一般的なハンマリングパターンをブロックします。 Pietro Frigoらは、TRR防御を備えた42個のチップを分析するためのファザーを作成し、そのうち13個を攻撃する他のパターンを発見しました[725]。  
CPUは、周波数と電圧の動的スケーリングを使用して、ハードウェア障害挿入に対しても脆弱です。  
2017年、Adrian Tang、Simha Sethumadhavan、Sal StolfoがCLKscrew攻撃を発見しました。Nexus6のArmプロセッサーをオーバークロックして、TrustZoneを打ち破り、暗号キーを抽出して特権を昇格させました[1858]。  
ArmとIntelはCLKscrewとPlundervoltのマイクロコードパッチをリリースしましたが、同じジャンルの他のCPU攻撃を予想するかもしれません。  
長期的には、ハードウェアセキュリティにはより防御的な設計が必要になります。  
Rowhammerを発見した2人の科学者、Onur MutluとJeremie Kimは、メモリコントローラーが行を閉じると、チップの信頼性に合わせた確率で隣接する行を更新することを示唆しています[1369]。  
企業がデバイスを物理学によって設定された境界にますます近づけるにつれて、ますます多くのサイドチャネルが新しいチップテクノロジーに潜むことを考えると、半導体セキュリティにはより原理的なアプローチが必要です。  
一般的な半導体プロセス、または広く使用されているCPUのレベルで障害が発生した場合、修正には費用がかかります。  
19.4.5メルトダウン、スペクター、その他のエンクレーブサイドチャネル  
 CPUマイクロアーキテクチャに基づく攻撃のファミリーです。  
2年後、OnurAcıi¸cmez、¸CetinKayaKo¸c、Jean-Pierre Seifertは分岐予測分析（BPA）を発明しました  
最新の高性能CPUには、スーパスカラーアーキテクチャがあり、CPUは一度に1つの命令をフェッチして実行することはありませんが、パイプラインを備えており、パイプラインが12命令も先にフェッチされ、コードがどの分岐を取るかを予測しようとします。  
他の人は他のキャッシュの振る舞いを調査しました。 2015年、Fangfei Liu、Yuval Yarom、および同僚は、L3キャッシュがGPG秘密キーの復旧を可能にする実用的なプライムおよびプローブクロスコア攻撃を提供したことを示しました[1176]。  
最近のそのような攻撃は、Dayeol Leeと同僚によるMembuster攻撃で、OS特権を使用して、データをリークするキャッシュミスを誘発します[1134]。  
 これは、10年以上の作業で多くのアイデアが集まった分野でした。 CPUベンダーはもっと注意を払っていたはずです。  
どちらも、投機的なメモリ読み取りを活用し、素数およびプローブ、分岐予測、およびキャッシュサイドチャネルに関する以前の研究に基づいて構築されています。  
 一部のワークロードで15％のパフォーマンスヒットが発生し、場合によっては再起動することがあります。  
Meltdownは、メモリアクセスと特権チェックの間に競合状態を作成し、キャッシュサイドチャネルを介して禁止されたメモリを読み出します。  
チップメーカーは2017年のほとんどを密かにバグ修正に費やしました。  
実は（成長している）  
このロジックは、条件付きジャンプの後に実行されるコードパスを推測しようとします。不正なソフトウェアは、コードを誤って予測するようにトレーニングできます。  
それらが決して読み取られなくても、アクセス制御チェックは決して行われません。これにより、攻撃者が暗号鍵の素材を観察できる信頼できるタイミングサイドチャネルが提供されます[1069]。Meltdownはターゲットプロセスのデータを直接読み取りますが、Specterはターゲットプロセスをだまして、サイドチャネルを介してそのデータを公開します。  
2019年のセキュリティ会議は、微妙なマイクロアーキテクチャ機能を悪用する一連の他の攻撃をもたらしました：Zombieload、Fallout、Smotherspectre、およびRAMBleedは4つですが、2020年は、MeltdownとSpectre [339]、およびCrossTalkからのアイデアを組み合わせたLoad Value Injectionをもたらしました。これにより、CPUの1つのコアが別のコアを攻撃できるようになります[1570]。  
設計を検証するためにチップメーカーが開発したツールは、ロジックが正しい答えを与えるかどうかをチェックするだけで、所要時間ではないため、デザイン時にそれらを見つけることは簡単ではありません。  
彼らが見つけたすべてを修正するには何年もかかり、テクノロジーの性質を考えると、すべてが修正されることはないと思います。  
たとえば、CSDBがコードに現れた後、予測されたデータまたは状態を使用して、命令を投機的に実行することはできません[131]。  
これらすべてをシリコンに組み込むにはおそらく4年かかり、必要なサポートがソフトウェアツールチェーンに表示されるまでにはさらに数年かかります。プログラマがそれをすべて使用する方法を学ぶには、さらに長くかかります。  
そのため、2020年代に、信頼できないプロセスを実行するCPUで実行する暗号化は潜在的に危険にさらされます。  
（しかし、高度な暗号工学の章で説明するように、それによっていくつかの新しいワームの缶が開かれます。）  
19.5環境サイドチャネル  
このような攻撃は、音響、光学、デバイスの動き、および組み合わせも悪用します。攻撃者は、誰かが入力している音からテキストを回復する方法を見つけたら、同じ手法を、ネットワーク上やデバイスの動きの測定など、他の手段で観察されたキーストロークのタイミングに適用できます。  
19.5.1音響サイドチャネル  
機械を聞くことに関しては、最初のケースは1956年のスエズ危機の間であった可能性があり、イギリスが電話のバグを使用してエジプト大使館のHagelin暗号機の設定を見つけました。  
その後、KGBは1976年から1984年まで、モスクワの米国大使館にあるIBMタイプライターに実際にバグを挿入したことが判明しましたが、マイクではなく磁気バグを使用していました[790]。  
SSHがインタラクティブモードで使用されている場合、各キーストロークは個別のパケットで送信されるため、暗号化されたパケットタイミングは正確なキーストローク間タイミングを提供し、単純な隠れマルコフモデルでもコンテンツに関するキーストロークペアごとに約1ビットの情報を提供します。これにより、攻撃者が観察した暗号化された値のパスワードを推測する際に、約50倍の利点が得られる可能性があると述べた[1803]。  
彼らはニューラルネットワークをトレーニングして、ターゲットキーボードのキーを押すことによるクリックを認識し、数パーセントのエラー率で、誰かのタイプ入力を音響放射から拾うことができると結論付けました[136]。  
誰かが未知のキーボードで英語でテキストを約10分間入力したという記録を考えると、彼らは個々のキーを認識し、キー間時間と英語の既知の統計を使用して、どのキーがどれであるかを特定しました。  
他の研究者もすぐに参加しました。翌年までに、Yigael Berger、Avishai Wool、およびArie Yeredorは、改良された信号処理アルゴリズムを使用すると、音響再構成をはるかに効率的に行うことができることを示しました[228]。  
2012年に始まった深いニューラルネットワーク革命により、そのような信号からはるかに多くの情報を引き出すことが可能になりました。2016年までに、Alberto Compagno氏と同僚は、Skypeで誰かと話しているときにタイプすると、多くの情報を再構築できることを示しました[464]と再入力します。  
2017年までに、Ilia Shu-mailovは、携帯電話の1つのアプリが、デバイスの2つのマイクを使用して画面のタップを聞くことにより、別のアプリに入力されたパスワードとPINを回復する方法を考え出しました[1731]。  
 処理は、以前は洗練された電子戦キットの領域でした。ここにポケットに入れられたアプリケーションがあり、パスワード入力メカニズムがTrusted Execution Environmentに実装されている場合は保護を利用できるため、マルウェアがパスワードを直接タップすることはできませんが、不正なアプリがオンラインバンキングのパスワードを盗む可能性があります。19.5.2光サイドチャネル  
そして、誰もがポケットにカメラを持ち、書斎に3Dプリンターを持っているので、物理的なキーは簡単に複製することができます。  
夜、街を見て、オフィスで遅く働いている誰かが、コンピューターモニターからの拡散反射光によって顔とシャツが照らされているのを見たことがありますか。  
 2002年にMarkus Kuhnは、答えが「かなり上手い」ことを示しました。彼は高性能光電子増倍管をオシロスコープに接続し、一般的なVDU管で使用されている青と緑の蛍光体からの光が数マイクロ秒後に減衰することを発見しました。  
したがって、望遠鏡、光電子増倍管、および適切な画像処理ソフトウェアが与えられた場合、銀行員が顔またはシャツから散乱した光をデコードすることにより、銀行員が見ているコンピュータ画面を読み取ることが可能でした[1103]。  
 次の見出しはJoe LoughryとDavid Umphressによるもので、PC、モデム、ルーター、その他の通信機器のデータシリアルラインにあるLEDステータスインジケーターを調べました。  
設計者は、LEDが待機中の望遠鏡にデータを送信するのに十分な帯域幅を持っていることに気づくことを止めずに、シリアルデータラインから明快な明かりを灯していました[1189]。  
部屋でのスピーチや音楽は、ぶら下がっている電球に振動を引き起こし、望遠鏡と適切なフォトダイオードを使用して通りの向こう側から読み取ることができます[1387]。  
  
サーマルコバートチャネルは2006年に到着しました。スティーブンマードックは、リモートで測定できる一般的なコンピュータのクロックスキューが日変化を示し、これが周囲温度の関数であることを発見しました。  
経度はタイムゾーンに由来し、緯度は（よりゆっくりと）  
したがって、Torなどの匿名サービスの背後に隠れることは、見た目ほど簡単ではありません[1356、1358]。  
ただし、タッチスクリーンにも痕跡が残り、これらが電話で使用され始めた後、Adam Avivはスマッジ攻撃を文書化しました。これらの残留物は、Androidデバイスで一般的に使用されるパターンロックを解除する非常に効果的な方法です[145]。  
 Adamは、スマートフォンの加速度計をサイドチャネルとして使用することも開発しました。ユーザーが入力したときの電話の揺れの動きが重要な情報を明らかにすることを発見しました。  
加速度計はすでにPhilip Marquardtや他の人々によって、近くの従来のコンピューターのキーボードからの振動をデコードするために使用されていました[1229]。  
Laurent Simonと私は、PINをタップすると電話が傾くので、カメラを仮想ジャイロスコープに変えて遊んだ。カメラとマイクの組み合わせは、キーストローク推定のジャイロと同じくらい優れていることがわかりました[1756]。  
2015年にApple Watchが登場したことで、より多くの人々がスマートウォッチのサイドチャネルを研究するようになりました。今年の年末までに、Xiangyu Liuらは、スマートウォッチを使用すると、スマートフォンのPINエントリで加速度計の推論攻撃を実行できるだけでなく、通常のキーボードで入力したテキストを再構築できることを示しました。手首を使用すると、左側の文字[1177]でより正確になります。  
 答えは「まだ」ではないようです。  
ただし、セキュリティエンジニアは、豊富なセンサーセットを備えたスマートフォンなどのデバイスに移行すると、特定のアプリやコンテキストに情報を限定することがさらに困難になる、豊富なサイドチャネルセットを取得することを認識しておく必要があります。  
これはいつか私たちに厄介な驚きを与えると期待するかもしれません。  
19.6ソーシャルサイドチャネル  
典型的な例の1つは、今後の軍事作戦の事実を漏らしている国防総省へのピザ配達の増加です。  
あるケースでは、保険会社が彼女のGPが原因であると知っていた塗抹検査のために保険会社が彼女を思い出すことができなかったとき、女性のGUMクリニックへの訪問は漏れました[1310]。  
そのような問題については、推論制御の章ですでに詳しく説明しましたが、ここでその説明を繰り返すことは提案しません。  
政策立案者と技術産業はどちらも、医療記録などの機密データを匿名化すると機密性が低くなり、産業用原料として扱うのに適すると考える長年のふりをしてきました。社会的側面のチャネルも、技術政策論争の哲学的側面で役割を果たす。たとえば、Helen Nissenbaumは、プライバシーを「コンテキストの完全性」として定義するまでに至っています。  
 別のものに終わる（新聞など）  
複雑なサイドチャネルを持つユビキタスデバイスだけが問題ではありません。効果的なオプトアウトなしで広告に使用される大量のデータを収集すると、さらに多くの情報漏えいが発生します。  
’  
サイドチャネル攻撃には、意図しない無線周波数や伝導された電磁信号から、共有された計算状態を介した漏洩に至るまで、放射が危険にさらされることでシステムのセキュリティが破壊される可能性のある脅威の範囲全体が含まれます。現代の携帯電話やその他の消費者向けデバイス、そして社会的コンテキストを介した漏洩にも。  
もちろん、どのサイドチャネルが実際の脅威をもたらすかは、アプリケーションによって異なります。また、ほとんどの場合、それらのチャネルのほとんどが学術的に関心を持ち続けます。  
したがって、セキュリティエンジニアはリスクを認識する必要があります。  
2015年に重点が置かれたのは、電話、スマートウォッチ、その他の物理デバイスへのサイドチャネル攻撃でした。  
サイドチャネルの脆弱性は、システムが複雑になるにつれてユビキタスになってきています。  
テクニックが磨かれ、ソフトウェアが普及するにつれて、攻撃はより簡単になります。  
機械学習への関心の爆発は、テンペストから電力分析、ソーシャルチャネルの悪用に至るまで、あらゆる場所で攻撃を改善する効果があるにちがいありません。  
参考文献デビッドイースターによるテンペストの最近の歴史は、ロシア、アメリカ、イギリス、およびそれらのヨーロッパの同盟国の間の冷戦の闘争について語っています[600]。  
電力分析については、Paul Kocher [1065]およびThomas Messergues [1298]による論文を参照してください。  
Mark RandolphとWilliam Diehlによる2020年の調査は、より最近の研究[1576]をカバーしています。  
たとえば、2019年11月に、Daniel Moghimi、Berk Sunar、Thomas Eisenbarth、およびNadia Henningerは、Common Criteria EAL4 +に対して安全であることが認定されたSTMによって作成されたTPMおよびIntel CPUの仮想TPMに対するタイミング攻撃を発見し、ECDSAを抽出できるようにしましたキー;後者のケースは、VPN製品への実際の攻撃につながりました[1329]。  
主流のコンピューターハードウェアへの攻撃はまだ急速に進んでいます。  
投機的実行を悪用するCPUへの攻撃に関しては、メルトダウンおよびスペクター攻撃が非常に多くの注目を集め、マイクロアーキテクチャのセキュリティが一夜にして、逆流からこの分野で最もホットな研究領域の1つになりました。  
 ハードウェアが検証されている場合は、マニュアルに記載されていることを実行していると想定していたため、バグを探す意味がありませんでした。  
バグレポートは今後も続く予定であり、その間、CPUは非常に複雑になっているため、安定するまでに何年もかかる可能性があります。  
クラウディオらは、EchoLoad [381]と呼ばれる攻撃により、第1世代のメルトダウン緩和策を打ち破りました。