–ウィリアムシェイクスピア、キングヘンリーV、ACT IV最適化は、機能するものを取り、ほとんど機能するがより安価なものに置き換えることで構成されます。  
1はじめに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らします。  
 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もたらしています。  
 第一に、伝導されたまたは放射された電磁信号があり、それにより、情報がローカルで、場合によってはより長い範囲で侵害される可能性があります。  
 冷戦の終結後、人々は誰も聴いていない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、および共有システムリソースの競合を悪用する可能性があります。  
58219。  
 排出セキュリティ3。  
 これにより、2020–5を超えるすべてのスーパースカラーCPUが強制的に設計されます。  
 近くのキーボードで入力されたキーストローク、または実際にそのタッチスクリーン上のキーボードを聞いたときなど、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。その感知がマイク、加速度計とジャイロ、またはカメラで行われるかどうかは関係ありません。  
 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ほど拡大していませんが、それ以上に増えています。  
 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、プライバシー法を回避す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、お金を追いかける影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。  
2エミッションセキュリティエミッションセキュリティ、またはEmsecは、伝導または放射された電磁信号などの侵害を使用した攻撃を防止することです。  
 これは投票機にとっても問題になりました。オランダのグループが投票機で投票者が選択した当事者を遠くから確認できることを発見した後、自動預け払い機での攻撃も実証されました（これらは実際にはスケールしていません）。  
 （これらについては、電子戦に関する章で詳しく説明します。  
セキュリティエンジニアリング583ロスアンダーソン19。  
 排出セキュリティ19。  
1歴史電話線間のクロストークは、19世紀のテレフォニーのパイオニアにはよく知られており、その2線式回路は、支柱上のクロスツリーの段に積み重ねられていました。  
 クロストークは、1884年から85年に最初に軍隊の注目を集め、最初に知られている戦闘の悪用は1914年でした。  
 初期のWWIphone回路は、ケーブルの重量とかさを半分にするためにアースリターンを使用した単芯絶縁ケーブルでした。  
 リスニングポストが迅速に確立され、ツイストペアケーブルの使用を含む保護対策が導入されました。  
 無人の土地に放棄された電信線のもつれがこのような優れた通信チャネルを提供し、非常に多くのトラフィックを漏らし、それを取り除くことは命が費やされた仕事になることを人々は発見しました。  
インテリジェンスコミュニティは、ベルが米国政府にミキサーを販売してテレグラフトラフィックにワンタイムテープを追加し、プレーンテキストが暗号文に漏れていることを発見したとき、第二次世界大戦前後の暗号機器へのサイドチャネル攻撃を発見しました。  
 1960年、英国首相が欧州経済共同体への参加に関する交渉中にフランス大使館の監視を命じた後、彼の安全保障局の科学者は、大使館からの暗号化されたトラフィックがかすかな平文信号を運んでいることに気づき、それを回復するための機器を構築しました。  
 一方、ロシア人は、偽の放射を悪用し、それらのすべてを盗聴することに真剣な熟練を発達させました。  
 1967年と1970年のウィリスウェアのランドコーポレーションのレポート[1985、1986]で、コンピュータデータが漏洩する可能性についての公的な言及がありました。  
一方、家庭用テレビセットの局部発振器信号から漏れる漂遊RFは、英国の「TV検出器」の方向探知機器の対象となり、TVの所有者は公共放送サービスをサポートするために年間ライセンス料を支払う必要があります。漏洩したフランスの暗号マシンの話は、1987年にセキュリティサービスの内部告発者Peter Wrightによって漏洩しました[2047]。  
2。  
19。  
2テクニカルサーベイランスと対策テンペスト攻撃の詳細に入る前に、電磁スペクトルを使用する最も単純で最も広範囲に及ぶ攻撃は、無害な機器の意図しないRFエミッションを悪用している攻撃ではなく、攻撃者がリスニングデバイスを導入していること、または（最近）ターゲットのデバイスがマルウェアに感染した場合。  
 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。  
 バッテリー寿命は、これらのデバイスの主な制約です。  
•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、そのため永続的に使用できます。  
 最近の同等品の中には、キーボードケーブルにクリップしてコネクタのように見えるものがあります。他の人は電気アダプター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します。  
 ほとんどは携帯電話技術を使用しています。これらは、呼び出されたときに聞いて見るカスタムのハンドセットと見なすことができます。  
 それはアメリカ合衆国の大シールの木製のレプリカであり、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ため、この手法の変種がおそらく使用され続けたと思われます。  
 1984年、モスクワの米国大使館にあるIBM Selectricタイプライターで16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、それらを1つのバーストで送信しました。  
セキュリティエンジニアリング585ロスアンダーソン19。  
 放射のセキュリティ•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。ターゲットの電話にインストールされているソフトウェアによって、熟練した攻撃者によってリモートで行われるか、強制的または操作的な家族のメンバーによって行われることもあれば、雇用条件として行われることもあります。  
•優れた監視レシーバーは、数十秒ごとに無線スペクトルを約10KHzから3 GHzまで掃引し、放送、警察、航空管制などとして説明できない信号を探します。  
 バースト送信の方が優れています。  
 多くの組織が携帯電話の使用を禁止しようとしましたが、ほとんどはあきらめました。王立海軍でさえ、最終的には、船員が彼らのトマニーが去ったときに船内に携帯電話を保持することを許可する必要がありました。  
 弱い無線信号をブロードキャストし、機器内のトランジスタ、ダイオード、その他の非線形接合が信号を整流するときに生成される奇数の高調波をリッスンします。  
 まったく再放射しないように設計された高価なバグもあります。  
•通常の建物のWi-Fiを使用する非表示のワイヤレスカメラをトラフィックパターンで検出することが可能であり、研究者はこの目的のためにアプリを開発しました[415]。  
 NATO諸国では、Top Secretmaterialは、物理的なセキュリティと音響シールドの両方を備えた安全なコンパートメント化された情報施設（SCIF）に保管され、バグがないか定期的に清掃されます。脅威評価が有能なやる気のある対戦相手が十分に接近する可能性があることを示唆している場合、SCIFは電磁シールドも持っ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。  
 新しい米国大使館セキュリティエンジニアリング586ロスアンダーソン19。  
 パッシブ攻撃モスクワの建物は、多数のマイクロフォンが構造内で発見された後、放棄されなければなりませんでした。イギリスの対諜報部隊は、約5,000万ドルの費用で、新しい本社ビル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人の従業員は、暫定IRAと過去の関係があったことが判明しました。  
技術開発により、盗賊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。  
 ラップトップ、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。ケイラのしゃべる人形はドイツでは禁止されていました。見知らぬ人がそれを使って子供を遠くから聞いて話しかけることができるからです。  
19。  
 ここでは、光信号は除外し、後で音響攻撃と一緒に説明します。  
 信号は、ある種の回路（電力線や電話線など）を介して伝導することも、無線周波数エネルギーとして放射することもできます。  
これらは相互に排他的ではありません。多くの場合、RF脅威には伝導コンポーネントがあります。  
19。  
1電源ケーブルと信号ケーブルを介した漏洩すべてのハードウェアエンジニアは、高周波信号がいたるところに漏洩することを知っており、問題を引き起こすそれらを阻止するために努力する必要があります。  
 ただし、民間機器は、ラジオやテレビに干渉しないように十分にシールドする必要があります。悪用可能な情報漏えいを防止することは、はるかに困難な作業です。  
3。  
 暗号化マシンなど、赤と黒の両方の接続を備えた機器は正しく機能させるのが難しく、シールドされた機器は政府市場向けに作られた少量でしか入手できない傾向があります。  
 空軍基地の作戦室には、何百ものケーブルが通っています。それらすべてをフィルタリングし、赤と黒の分離を維持するために厳密な構成管理を課すと、何百万ものコストがかかる可能性があります。  
19。  
2RF信号による漏洩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、IBM 1401に1が付いていました。  
 機械室でこの周波数に調整されたラジオは、処理されるデータに応じて変化する大きな笛を発します。  
 学校の同僚にはもっと良いアイデアがありました。彼は異なる長さの一連のサブルーチンを書いたので、それらを順番に呼び出すことで、コンピューターは曲を再生できました。  
現在、より近代的な機器に移行し、2000年代初頭までモニターとして使用されていたVDUは、TV信号（現在表示されている画像で変調されたVHFまたはUHF無線信号）を自然に放射します。  
 ブロードバンドレシーバーがあれば、これらのエミッションを取得してビデオとして再構成できます。  
 一般的な信念に反して、より近代的なフラットディスプレイも一般的にスヌーピングが簡単です。典型的なラップトップには、システムユニットからディスプレイへのヒンジを通るシリアルラインがあり、これがビデオ信号を伝送します（図19。  
他の研究者は、ファックス機からシールドされたRS-232ケーブルを介してイーサネットに至るすべてのものをスヌーピングする実験を始めました[534、1796]。  
 シールドや妨害電波などの対策は適切に行うのが困難で費用がかかるため、ほとんどのビジネスセクターは問題を無視しました[143]。  
最後に、2006年10月に、電子投票機に反対するオランダのグループは、オランダの選挙投票用紙の90％を収集するために使用されたマシンが数十メートルの距離から盗聴される可能性があることを実証しました[785]。  
ゾーンシステムは次のように動作します。  
 ゾーン1の機器は20メートルの距離で敵から安全でなければならないため、オランダの「ゾーン1セキュリティエンジニアリング588ロスアンダーソン19。  
 パッシブアタック350 MHz、50 MHz BW、12フレーム（160 ms）平均化μV10121416182022図19。  
-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いて、そのすべてはすでにパブリックドメインにありました。これは、ニアフィールドとファーフィールドドロップの違いを考慮して、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を危険にさらすことができなかった少数の国に対してのみ使用されました。  
 COTS機器は、テスト時にゾーン2になる傾向があり、ゾーン3には特にノイズの多いキットが含まれます。  
 ゾーニングは排出ガス安全のコストを大幅に削減しました。  
3。  
 ソフトウェア技術を使用して、コンピューターシステムからの情報を含む電磁放射をフィルタリングまたはマスクします。3と19。  
図19。  
4 –テキストローパスフィルター済みこれは、ユーザーから見て、画面のコンテンツにほとんど気づかれない影響を与えます。  
5と19。  
3と19。  
図19。  
6 –画面、フィルター処理されたテキストただし、図19の写真に示すように、放出されるRFの違いは劇的です。  
8。  
アゾンの相違に変換されたVDUでのソフトテンペストテクニックの使用[108]。  
図19。  
8 –フィルターされたテキストのページただし、攻撃者はアクティブテクニックだけでなくパッシブテクニックも使用できます。  
 図19。  
図10は、ビデオ信号が300 MHzと1200 Hzのピュアトーンで変調された2 MHzのRFキャリアである場合のPCの画面の様子を示しています。  
3。  
9 – 300 Hz AM信号図19。  
 そして情報コミュニティ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[1062]で、経済スパイのソフトウェアベースのRFエクスプロイトを使用するCIAの報告がありました。  
e。  
」マルウェアの可能性は、テンペストテストがテスト中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のエクスプロイトを使用してセットアップしようとする最悪の場合の攻撃をシミュレートするinit信号を注入する理由の1つです隠れチャネル[252]。  
 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行う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搭載していることが多いため、信号が届かないように注意する必要があります敵に役立つ何かを誤って変調した。  
19。  
3何が問題になっているのか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。  
 それだけではありません。クリーニングの場所はムハバラットが負担するため、設備のセキュリティエンジニアリング591ロスアンダーソン19を緩めるのに役立ちます。  
 部屋のバグでバッテリーを交換するのと同じように、コンピュータ間およびコンピュータ内での攻撃  
 文書は、沿岸警備隊のディープウォータープロジェクトのWebサイトに残され、活動家のWebサイトである暗号解読に結ばれました。  
 これらの文書は、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）だけではなく、より一般的には失敗した仕事についての物語です。  
 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。この周波数が何らかの形で固定できる場合（e。  
 マルウェアによって）その後、攻撃ははるかに簡単になります。実際、攻撃は、これから説明する種類の標準的なタイミング攻撃に減少します。  
4コンピュータ間およびコンピュータ内の攻撃マルチレベルのセキュリティに関する章で、1973年にバトラーランプソンが指摘した隠れチャネルは、高レベルのプロセスが低レベルから低レベルに信号を送ることを許可する可能性があると述べた[1125]。  
 マシンが高低で共有され、リソースが固定スライスに割り当てられていない場合、高プロセスはディスクドライブをいっぱいにするか、多くのCPUサイクルを使用して信号を送ることができます（前者のケースをストレージチャネルと呼び、後者のタイミングチャネルですが、実際にはそれらは互いに変換されることがよくあります）。  
 ノイズを導入することで、隠れチャネルの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、もちろん、256ビットの暗号キーを漏らすことは簡単です。  
 また、ソフトウェアがネットワーク上で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およびブロックすることがさらに困難です。  
そのようなチャネルは簡単にセキュリティエンジニアリング592ロスアンダーソン19を持っています。  
 コンピュータ間およびコンピュータ内の攻撃暗号鍵を密輸するのに十分な帯域幅  
19。  
1タイミング分析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、それらの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]。  
 実際、SSL / TLSには一連のタイミング攻撃がありました。このプロトコルは1990年代後半に安全であることが証明されましたが、その実装以降、主にサイドチャネルを使用して、約1回の攻撃が発生しています。  
 John Kelsey、Bruce Schneier、David Wagner、Chris Hallは、1998年に、後にAESとなったアルゴリズムであるRijndaelが、キャッシュミスに基づくタイミング攻撃に対して脆弱であることを指摘しました[1034]。  
 それ以来、多くの研究者がこの攻撃を着実に改善しており、AEScanの素朴な実装は、数百の暗号化を観察することによって破られました[1489、232、1483]。  
 リークするのはアルゴリズムだけではありません。プロトコルと実装機能（パディングやエラー処理などのリークシークレットも）。  
4。  
 スマートカードメーカーは、1980年代から電力線や特許取得済みのさまざまな防御策を通じて情報が漏洩する可能性があることを認識していました。 1990年代初頭までに、ペイTVハッカーや一部の政府機関には、カードに描かれた電流を測定するだけで情報を収集できることが知られていました。  
 このような電力トレースの例を図19に示します。  
 これは、一度に1バイトずつ推測し、正しいバイトがSecurity Engineering593Ross Anderson19であるときに異なる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。  
 コンピュータ間およびコンピュータ内での攻撃と推測されます。  
10。  
30。  
50。  
70。  
91−5051015µsmA誤った入力正しい入力差図19。  
さまざまな命令にはまったく異なる電力プロファイルがあり、ご覧のとおり、消費電力も処理されるデータによって異なります。  
7）。  
したがって、攻撃者は、各データバイトとバス上の前のバイトとの差のハミング重み（遷移カウント）を確認できます。  
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。  
この漏洩の影響は、パスワードの抽出に限定されません。  
 これは、Paul Kocherによって1998年に業界の注目を集めました。PaulKocherは、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用し、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しました。カードソフトウェアの実装の詳細を知る[1065]。  
4。  
 サブセットが目的の情報と相関している場合、差異はゼロ以外である必要があります[1067]。  
次に、暗号の内部状態の一部を推測します。  
 したがって、攻撃者がアクセスする暗号文である場合、最後のラウンドでS-box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、targetS-box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、微分トレースはランダムな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持っている銀行カードに対して改造された端末機器を使って実行できます。  
Paul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、銀行カード用のEMVプロトコル（バージョン4.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。  
4。  
 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引き込みだけに頼るのではなく、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] 。EyalRonen、Colin Oˆa˘A´ZFlynn、Adi Shamir、およびAchi-Or Weingartenが、フィリップスフエの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更新の認証に使用したAESキー[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ったことを示した。  
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。  
19。  
3グリッチと差動障害の分析1996年に、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破損す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、本来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、ランダムな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]。  
 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を返す場合は、Security Engineering596Ross Anderson19になります。  
 コンピューター間およびコンピューター内の攻撃p = gcd（pq、Sep�h（m））これは、システムを一度に破壊します。  
 光プロービングはこのためのツールであることがわかり[1648]、レーザーを使用してキービットを一度に1にゼロに設定することは、現在では通常のリバースエンジニアリング手法になっています。  
 電話や、Google HomeやAmazon Alexaなどの音声制御デジタルアシスタントで使用されているように、MEMSマイクでレーザーを発射すると、クリック音が記録されることがわかります。  
現在、多くの現実世界の攻撃では、アクティブメソッドとパッシブメソッドの組み合わせが使用されています。  
上記の3では、光学的に強化された位置固定パワー分析について説明しました。これは、パワー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。  
5。  
19。  
4Rowhammer、CLKscrew、PlundervoltOneの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漏洩する場合です。  
 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することができるため、しばらくの間存在する可能性があります。  
 そして2020年に、Andrew Kwongandの同僚は、このメカニズムが読み取りと書き込みに使用できることを発見しました; Security Engineering597Ross Anderson19。  
 コンピュータ間およびコンピュータ内の攻撃攻撃者は、Rowhammerによって誘発されたビットチップと隣接する行のビットの間の依存関係を悪用して、それらのビットを推測できます。さらに、ECCメモリが各ビットチップを検出して修正した場合でも機能します[1114]。  
 電力を節約するために、最近の多くのCPUは負荷に応じて周波数を変更し、電圧を適切にスケーリングしています。  
 2019年に、キットマードックと同僚はPlundervoltを発見しました：ここでは、IntelCoreプロセッサーの文書化されていない電圧スケーリングインターフェイスを悪用して、フォールトを誘発する低電圧と、RSAおよびAESキーをフォールト分析を使用して抽出できるようにするAES-NI操作を引き起こしています。 SGX exclaves [1366]から任意のメモリの内容をリークするポインタ演算。  
 Rowhammer / RAMBleed攻撃は依然として問題です。  
 これは簡単なことではありません。DRAMのリフレッシュレートを上げるだけで、デバイスの電力消費が増えます。  
 これにより、システムレベルの複雑さが増す可能性があります。  
 チップベンダーは、後でパッチを当てるだけでなく、設計時に優れたセキュリティエンジニアを巻き込む必要があるという難しい方法を学んでいます。  
19。  
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チップメーカー（および実際に情報セキュリティの世界全体）を襲う最新の津波は、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。BPAは、CPUの分岐予測状態を監視することにより、スパイスレッドが並列暗号化スレッドから秘密鍵を抽出できるようにしました。予測の誤りにより、その時点で20サイクルのペナルティが課された。最良の状況では、RSA秘密鍵は単一の署名の観察から抽出できます[13]。  
4。  
2017年までに、Cachezoom攻撃により、攻撃者はSGXエンクレーブからキーを抽出できるようになりました[1328]。  
 （インテルの対応は、そのような攻撃が範囲外であることを宣言するだけでした。  
最も影響力のある攻撃は、2018年の初めに公開されたMeltdownとSpectreでした。  
 彼らは非常に深刻なので、IntelとArmの両方がCPUを再設計してブロックすることを発表しました。しかし、それには数年かかります。その間、ソフトウェアの緩和策（利用可能な場合）によっては、一部のワークロードや場合によっては再起動によって15％のパフォーマンスヒットが発生する可能性があります。  
Meltdownは、メモリアクセスと特権チェックの間の競合状態を作成し、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年の大半を密かにバグ修正に費やしました。  
 これは実際には、投機的実行の特殊なケースである分岐予測ロジックを悪用する（成長する）脆弱性のファミリーです。  
 次に、CPUは実行されない命令をフェッチし、これらの一部が禁止された操作（ユーザープログラムが保護されたカーネルメモリを読み取るときなど）を実行する場合、保護されたページがキャッシュからフェッチされます。  
 要するに、CPUの実行が正式に正しい場合でも、あらゆる種類の低レベルの最適化により、タイミングが秘密データに依存する可能性があり、一連のSpectreバリアント全体がこれを悪用するようになりました。  
スペクターの攻撃ファミリーは成長を続けています。 Spectreが発表されて間もなく、研究者はForeshadowと呼ばれる亜種を発見しました。これは、SGXやシステム管理モードなど、Specterが提供していないIntelプロセッサの機能の多くをクラックするものです。  
 PrettywellすべてのCPUが分岐予測を使用するようになりました-非常に小さなものを除いて-サイドチャネルがたくさんあるために複雑になりました。  
 理由セキュリティエンジニアリング599ロスアンダーソン19。  
 環境サイドチャネル今や発見されているのは、以前は眠っていたマイクロアーチ構造の隠しチャンネルの背水が、セキュリティ研究で突然最も話題になったことであり、何百人もの優秀な研究生が突然一生懸命に見ているようです。  
 たとえば、Armは新しいバリア命令CSDB、SSBB、およびPSSBBを導入しました。  
 v8からの新しいデータフィールドCVS2もあります。  
 これをすべてシリコンに組み込むには、おそらく4年かかります。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。さらに、プログラマがすべてを使用できるようになるまでには、さらに時間がかかります。  
したがって、2020年代に、信頼できないプロセスも実行する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。  
5環境サイドチャネル過去20年間、人間の行動とデバイスの環境を悪用する多数のサイドチャネル攻撃が発生しています。  
19。  
1音響サイドチャネル音響セキュリティは、セクション19で述べたように、機密性の高い会話で人やデバイスが海に落ちるのを防ぐという点で長い歴史があります。  
2。  
 後に、当局が古いIBMSelectricタイプライターでタイプした音を録音するだけでその内容を伝えることができ、ドットマトリックスプリンターで生成されたノイズからデータを回復できるという「民間の噂」がありました[323]。  
2001年、Dawn Song、David Wagner、Xuqing Tianは、キーストロークのタイミングには、SSHで暗号化されたトラフィックを観察するだけで相手が多くの情報を回復するのに十分な情報が含まれていることを示しました。  
5。  
2004年に、Dmitri AsonovとRakesh Agrawalは、コンピュータキーボードの異なるキーソンが十分に異なるサウンドを生成することを示しました。  
 2005年、Li Zhuang、Feng Zhou、およびDoug Tygarはこれらのスレッドを組み合わせて、さらに強力な攻撃を生み出しました。  
 したがって、彼らはアクセスしたことのないキーボードの記録からテキストをデコードすることができました[2072]。  
他の人は音響分析をはるかに低いレベルに下げました：Eran Tromerand Adi Shamirは、キーがPCからの音響放射を介して漏洩することを示しました。マザーボード上のコンデンサーによって主に10KHz以上の周波数で生成されました[1908]。また2016年に、MengyuanLiらは、スマートフォンで入力すると、指の動きがRF信号に干渉し、チャネル状態情報を変調するのに十分なwifiでマルチパスの動作を変更することを示しました。これにより、不正なWi-Fiホットスポットがキーストローク情報を推測できるようになります[1162]。  
 このような到着時差異（TDOA）処理は、以前は高度な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 ExecutionEnvironmentに実装されていればマルウェアが直接タップすることができないため、利用可能な保護にもかかわらず、不正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。  
5。  
 そして、誰もがポケットにカメラを持ち、書斎にa3-d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、街を見渡して、誰かが遅く働いているのを見たことがありますかセキュリティエンジニアリング601ロス・アンダーソン19。  
 環境サイドチャネル彼らのオフィスでは、彼らの顔とシャツは、彼らのコンピュータモニターからの反射を反映した乱用によって照らされましたか？グローから情報が回復するかどうか疑問に思ったことはありませんか？ 2002年、Markus Kuhnは答えが「かなりすべて」であったことを示しました。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、銀行員が彼の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、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たJoe LoughryとDavid Umphressによるものです。  
 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付かずに、シリアルデータラインの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ます。これは、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]。  
19。  
3その他のサイドチャネル熱的隠れチャネルは2006年に到着しました。スティーブンマードックが、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内変動を示し、これが周囲温度の関数であることを発見したときです。  
 経度はタイムゾーンから、緯度は（ゆっくりと）季節から取得されます。  
バイオメトリクスの章で説明するように、油性の指紋の残留物が指紋認証スキャナーを危険にさらす可能性があることは以前から知られていました。  
（汚点は、あらゆる種類のタッチスクリーンデバイスで使用されているPINを推測するのにも役立ちます。テスラも同様です。  
 制御されていない設定でも、ユーザーが歩いている間、彼のモデルは5Security Engineering602Ross Anderson19内でPINの20％とロック解除パターンの40％を分類できました。  
 ソーシャルサイドチャネルが試行されます[146]。  
 次に、Liang CaiとHao Chenは、accelerom-eterとジャイロの両方を使用して研究し、後者がより効果的であることを発見し、4桁のPINを偶然よりも約80倍よく推測できるようにしました[365]。  
 ジェスチャー入力もリークします。 1つのアプリに入力されたテキストは他のユーザーが読むことができますが、これは共有割り込み状態[1759]を利用する技術的なサイドチャネルです。  
これらのサイドチャネルは重要ですか？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、豊富なセンサーの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絞り込むことがさらに困難になる、豊富なサイドチャネルの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。  
6ソーシャルサイドチャネル多くのサイドチャネルはアプリケーション層で発生し、見過ごされがちです。  
 より微妙な例としては、英国では泌尿生殖器科の診療所への訪問から得られた個人の健康情報が、患者の同意がない限りGPと共有できないことが挙げられます。保険会社は、塗抹検査が診療所によってすでに行われていることを知っていて、2度支払いをしたくありませんでした。  
 これは、インパクトの強いサイドチャネルファミリーでもあることに注意してください。  
 次のスキャンダルが次々と持ち帰り、とりわけEUの一般データ保護規則を導いているように、これは明らかにそうではありません。  
7。  
 実際に害を及ぼすほとんどのプライバシーの失敗は、1つのコンテキスト（診療所など）からの情報が別のコンテキスト（新聞など）で終わることに起因します。  
これについては、後で「監視またはプライバシー」19の章で説明します。  
サイドチャネルリーケージは大きなトピックであり、ソフトウェアとセンサーをほぼすべてに取り込んでいるため、さらに複雑になります。  
 しかし、時々、彼らは噛みます。  
研究の問題2019年の上位のセキュリティ会議での研究論文の多くは、サイドチャネル、特にアクセス制御とエンクレーブを弱体化させるプロセッサへのサイドチャネル攻撃、およびTPMまたは支払いカードを無効にすることができるセキュリティチップへのサイドチャネル攻撃です。  
ソーシャルサイドチャネルは引き続き関心があり、プライバシーに関する研究を推進しています。  
 サプライチェーンが複雑になるほどバグ修正は難しくなり、パフォーマンス、パフォーマンス、または現金の面でコストがかかりすぎるため、脆弱性は修正されない場合があります。  
これは、古典的なテンペスト攻撃にも当てはまります。ソフトウェア無線（中間周波数ステージで信号をデジタル化し、その後のすべての処理をソフトウェアで行う無線）は、高価な軍事的好奇心ではなくなり[1117]、セルラー無線基地局に広く普及しています。 、GPSレシーバー、IoTデバイス、さらには愛好家の寝室まで。  
 どのサイドチャネルが別の10億ドル規模の問題になるまでスケールアップするかを予測することは困難ですが、一部のチャネルがそうなることは間違いありません。  
7。  
 classicvan Eckの記事[601]はまだ一読の価値があり、Soft Tempest、Teapotandに関するトピックに関する私たちの作業は[1105]にあります。  
 タイミングとパワー分析については、Paul Kocherと彼の同僚によるオリジナルの論文が古典的な参考文献です[1064、1065]。ステファンマンガード、エリザベスオズワルド、トーマスポップのすべての主要な側面を網羅した教科書があります[1214]。また、ポールコッチャーの2011年の調査報告書「微分力分析の概要」では、攻撃と防御の両方の詳細なエンジニアリングについて説明しています[1067]。  
セキュリティチップに対するタイミング攻撃とパワー攻撃の進歩に追いつくには、攻撃手法が常に向上するため、現在の研究文献に従う必要があります。  
 タイミング攻撃が発生してから20年以上経った今でも、認定製品や有名ブランドのいずれにも耐えることはできません。  
 メモリへの攻撃については、Onur Mutluand Jeremie KimによるRowhammerに関する2019年の調査報告[1369]を参照してください。  
 何年もの間、CPU設計者（およびほぼ全員）は、ハードウェアが検証されていれば、マニュアルに記載されていることを実行していたため、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きますが、CPUはその間に非常に複雑になっており、安定するまでに何年もかかる可能性があります。  
 Claudioandの同僚はまた、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破りました。