エンジニアリング立たせるべき岩を与えてください、そして私は世界を動かします。  
20.1はじめに  
そのようなデザインは、3つのかなり異なる背景から来ています。  
2つ目は、第12章で説明したバンキングの世界です。スマートカードは認証トークンとして使用され、HSMはPINとキーを保護するために使用されます。  
これらすべてのケースで、実際の生活は私たちが予想したよりもやや乱雑であることがわかりました。  
しかし、エンジニアリングは、攻撃対象を減らすことや、フォールトツリー分析を単純化することだけではありません。  
この章では、暗号工学の6つの例について説明します。フルディスク暗号化、シグナルプロトコル、Tor、ハードウェアセキュリティモジュール、エンクレーブ、ブロックチェーンです。  
HSMを除くすべてがサイバー犯罪者によって使用されています。  
マシンの使用中にハードディスク上のデータを暗号化することにより、泥棒がデータではなくハードウェアのみを盗むことができるようになります。  
これはおそらく次のレベルの複雑さであり、機器の侵害に直面した場合に人々がソーシャルネットワークをできるだけ安全に管理できるようにすることです。  
Torは、あなたのトラフィックを監視している誰かにあなたが話している人やあなたが訪問しているWebサイトを知らせたくない場合に、匿名性を提供することでこれを次のレベルに引き上げます。  
しかし、その上で実行される暗号化アプリは、アプリケーションプログラミングインターフェイスへの攻撃の影響を受ける可能性があり、支払いアプリケーションと深く絡み合っているため、修正が非常に困難です。  
彼らは支払いアプリケーションでHSMを置き換え始めており、Signalでのプライベート連絡先の発見もサポートしています。  
たとえば、SGXチップからマスターシークレットキーを抽出できる場合、エコシステム全体を破壊できます。  
これは、2009年以来、相互に信頼できない当事者の協力から暗号化メカニズムを使用して出現する共有元帳に基づいてデジタル通貨を作成するプロジェクトです。  
しかし、暗号化と経済的インセンティブの組み合わせのおかげで、信頼できるコンピュータがどういうわけか出現し、攻撃に成功する可能性のある莫大な金額にもかかわらず、歩き続けています。  
いくつかの印象的な事実が現れます。  
  
フルディスク暗号化（FDE）の背後にある考え方  
ディスクに書き込まれるときにデータを暗号化し、再度読み取られるときに復号化を行います。  
そのため、医師がノートパソコンを電車の中に置き忘れても、ハードウェアだけが失われます。医療記録はそうではありません。  
ヨーロッパでは、プライバシー規制当局は一般に、FDEが搭載されたマシンの損失を、データを収集したり、データ主体の義務的な通知を必要とするほど深刻ではないと考えています。  
 他の人と一緒にクリックするだけです（Mac）  
ただし、表面の少し傷はありますが、品質には大きなばらつきがあります。  
最初の認証ステップを実行するプラットフォームが必要なので、エンジニアリングは簡単ではありません。  
最初の認証は他の点で注意が必要です。  
ハードウェアTPMチップはパスワードの推測を制限する可能性があり、2007年からこれはBitlockerを搭載したWindowsで利用可能になりました。  
サードパーティ製品はいくつかの追加機能を提供し始めました。たとえば、TrueCryptは、ユーザーが正しいパスワードを知らない限りディスクボリュームの存在自体が非表示のままになるステガノグラフィックファイルシステムを提供しました[114] 1。  
ただし、適切な統合にはかなりの数のプラットフォームが含まれるため、ほとんどの人は現在、電話またはラップトップのベンダーが提供するFDE機能を使用しています。  
MicrosoftのBitLockerやAppleのFileVaultなどのオファリングは、AESサポートを備えたCPUで実行した場合、数パーセントのオーバーヘッドしかありません。  
2008年に、プリンストンのAlex Haldermanと同僚は、コールドブート攻撃を思いつきました。これは、市場に出回っている主要なFDE製品を打ち負かし、まだ多くのマシンに問題を引き起こしている可能性があります[854]。  
2015年、私たちはほとんどのAndroidが安全でないことを発見しました。工場出荷時のリセット機能はほとんどのOEMによってひどく設計されていたため、FDEキーを含む認証情報を中古デバイスから復元できました[1757]。  
販売が終了するとパッチが適用されます。  
そして、付随的な被害があります。  
そして最後に、乱用可能性を考慮する必要があり、そのうち少なくとも2つの重要な種類があります。  
（もう1つのコンポーネントは暗号通貨です。これについては、この章の後半で説明します。）、たとえ発見者がパスワードを見たか、簡単に推測できる場合でも。  
  
スマートフォンが世界中に広がるにつれ、人々はSMSからWhatsApp、Telegram、Signalなどのメッセージングアプリに切り替えました。安価で柔軟性が高く、家族や友人のグループを作成できるようになりました。  
以前はPGPなどのプログラムを使用して電子メールを暗号化することが可能でしたが、かなり面倒でした（セクション3.2.1で説明）。  
新しいプラットフォームの登場により、メッセージの暗号化がユニバーサルになり、アプリのデフォルトとして出荷されるようになりました。スノーデンの開示は、公衆の需要をかき立てるのに役立ちました。  
メッセージングのエンドツーエンド暗号化の標準を設定し、そのメカニズムはWhatsAppを含む競合製品で採用されています。  
そのため、スマートフォンのキーマテリアルは、多くの場合、危険にさらされており、アプリに単一の長期間有効な秘密キーを用意するだけでは不十分です。  
これらは、妥協後のセキュリティとして正式に認定されました[451]。  
 アリス、ボブ、サーバー間のキーを設定するプロトコル。秘密鍵が確立されると、メッセージ鍵を導出するラチェットプロトコル。アドレス帳で他の人のシグナルキーを見つけるメカニズム。  
したがって、X3DHプロトコル[1227]では、各ユーザーUがIDキーIKUとプレキーSKUを、前者を使用して検証できる後者の署名とともにサーバーに公開します。  
アリスがボブにメッセージを送信する場合は、サーバーからボブのキーIKBとSKBをフェッチし、一時的なDiffie-HellmanキーEKAを生成して、実現可能なすべての方法でそれらをボブのキーと結合します：DH（IKA、SPKB）  
、およびDH（EKA、SPKB）  
これらは一緒にハッシュされ、新しいキーKABを提供します。  
オプションで、ボブは、アリスがEKAと組み合わせてミックスにハッシュする一時キーを1回だけアップロードできます。  
その目的は、いずれかの電話が侵害された場合にセキュリティを回復することです。  
 または、格納された秘密鍵を更新する一方向ハッシュ関数、およびDiffie-Hellman鍵交換。  
各メッセージは新しいDiffie Hellman鍵部分を伝達します。これは関連するチェーンの鍵と結合され、共有秘密鍵はKDFを介して渡されます。  
目標は、対戦相手がそれらの間のトラフィックにアクセスするために、アリスの電話またはボブのどちらかを絶えず侵害する必要があることです。  
チャーリーがサーバーを引き継ぎ、ボブの代わりに自分のIKをアリスに送信できる場合、すべての賭けはオフです。  
AppleのiMessageなどのシステムは、単一のIDキーKIを相手に送信するだけでなく、デバイスキーのキーリング全体（MacBook、iPhone、その他のAppleデバイスごとに1つ）を送信します。  
これにより、米国、英国、およびその他の国で政策の乱れが生じました。その問題については、セクション26.2.8で説明します。  
Signalはオープンソースになることでこれを未然に防ごうとします。  
オプションは、ボブの銀行口座からお金を盗もうとした場合とほとんど同じです。  
個人がマウントする最も簡単な攻撃は、おそらくセクション12.7.4で説明したSIMスワッピングです。  
国家は、高度なハッキングツールを備えており、SS7にアクセスできます。FSBが脅威モデルに含まれている場合は、番号がわからない電話を使用することをお勧めします。セクション2.2.1.10で説明したように、彼らが知っている電話はあなたのものであり、そうでなければ彼らはトレースを相関させるかもしれません。  
。  
違法なポリシーを新聞に漏らすことを考えている上級公務員で、あなたがその話を知っている10人のうちの1人なら、Signalを使用したことがあるのはあなただけかもしれません。  
 テーマ別収集のターゲットの長いリストにある場合は、連絡先のパターンを体系的に記録することから地方警察をブロックすることができます。ここで、Signalは確かに役立ちます。  
電子メール暗号化プログラムPGPなど、一般の人々がエンドツーエンドの暗号化を使用できるようにする以前の試みは、鍵の管理があまりにも面倒だったため、専門家のニッチの外ではそれほど魅力的ではありませんでした。  
ただし、サービス会社にアドレス帳のコピーを提供することはすでにプライバシー侵害です。また、ソーシャルグラフ、プロファイル名、場所、グループメンバーシップ、誰が誰にメッセージを送っているのかを平文で記録しておくと、調査員はすべてを入手できます。これは召喚状によって。Signalはプライベートコンタクトディスカバリを実装しました。これについては、後で使用するメカニズムであるSGXについて説明するセクション20.6で説明します。  
 システムの重要ではあるがあまり目立たない部分はメッセージサーバーです。  
 Signalはグループメンバーシップの記録を保持していますが、匿名のグループメッセージングの提案がありました。これにより、キーが変更されたときに配信されなかったメッセージを処理する方法についての議論があり、WhatsApp実装は、失敗したものよりも配信を優先することを批判されました。  
繰り返しますが、テクノロジーができることはそれだけです。グループの1人のメンバーが不誠実である場合、彼らは他の人を裏切ることができます。  
2016年の選挙後のアメリカと2020年の欧州委員会（ヨーロッパの公務員）での使用は大幅に増加しました。  
2020年7月に混乱があり、Signalの更新によりユーザーがPINを選択するように強制され、各ユーザーの連絡先データはエンクレーブで暗号化されているため、ユーザーが新しい電話を取得した場合に回復できるようになりました。電話番号を共有する以外の方法でSignalの連絡先を作成することもできます。  
人々は、仮名を使って何百万ものユーザーを人質にでき、安全な通信アプリに頼る知恵に疑問を抱き始めました。その裏付けの一部は政府から、そして一部は億万長者からのものでした3。  
 信号はトラフィックの記録を保持しないと主張しているが、NSAからのFISAの令状がそうすることを彼らに強制し、それについて嘘をついた場合はどうなりますか？  
  
オニオンルーター（Tor）  
それは1998年に米海軍研究所で始まり、メッセージはタマネギの層のように入れ子になっているため、オニオンルーティングと呼ばれていました[1590]。  
アイデアはルーティングをアイデンティティから分離することです。アリスをイブにリンクしたい人は、ボブ、キャロル、デイブを破壊するか、ボブとデビッドのシステムの内外のトラフィックを監視する必要があります。  
これは、暗号化されたメッセージを受け入れ、暗号化を取り除いてから、内部で検出したアドレスにメッセージを再送信します。  
まず、複数のミックスが必要です。対戦相手は、オペレーターを強制するか、単にトラフィックの内外を相互に関連付けることにより、単一の組み合わせを危険にさらす可能性があります。  
第三に、最も難しいのは規模の拡大です。  
海軍は2003年にTorを世界に開放しました。  
現在、Tor Projectによって維持されています。これは、デフォルトのTorクライアントとなっているTorブラウザを維持する米国の非営利団体です。  
同様の機能は、Braveなどの他のブラウザにも組み込まれています。  
Tor対応ブラウザをオンにすると、3つのTorリレーを見つけて回路を開き、それを介して外部に接続します。  
Facebookに接続してアメリカやヨーロッパの新聞を読むことができるように、イランやパキスタンなどの国で検閲を打破するために使用されます。  
また、麻薬やマルウェアを購入できる地下の闇市場への接続にも使用できます。  
児童の性的虐待のWebサイトを訪問するために使用できます。  
主要な脆弱性は初日から知られており、Tor自体が出現する6年前に、オニオンルーティングを世界に紹介した1998年の論文に記載されていました[1590]。  
まず、イブのウェブサイトが暗号化を使用していない場合、または出口ノードが中間者攻撃を実行できるような方法で使用している場合、悪意のある出口ノードはトラフィックを監視できます。  
これには、イラン、インド、日本、ロシアからのミッションを含む大使館が使用する多数のウェブメールアカウントのログオンとパスワードが含まれていました4。  
2番目の問題は、ユーザーを追跡するためにWebページが使用する多くのトリックです。  
しかし、多くのアプリケーションは、ユーザーに自分自身を明示的に識別させたり、気づかずに情報を漏らしたりします。  
 といくつかの特別な興味のある検索（あなたの趣味を明らかにする）  
第3に、Torなどの低レイテンシで高帯域幅のシステムは、トラフィック分析に本質的にさらされています[1363]。  
実際には、これは見た目よりも難しい5。  
5インテリジェンスコミュニティはTorに賛辞を送りました。TCHがリークしたGCHQスライドデッキは、トラフィック確認攻撃から保護しません。対戦相手は、入口と出口の両方のリレーを制御し、トラフィックのタイミング、ボリューム、または他の特性を関連付けて、特定の回路。これを行っていただけで、ボランティアがシステムにリレーして、プロトコルヘッダーをいじくり回して簡単にしました[561]。  
第4に、Torは約6,000のリレーのプールを介して接続するため、ファイアウォールは単にIPアドレスをブロックできます。  
このようなブロックを回避するために、ボランティアはTorブリッジ（Torエントリノードをパブリックディレクトリにリストされていない）を利用可能にします。  
中国は国のファイアウォールを迂回する人々が代わりにVPNを使用することを好むようです。これらはよりスケーラブルであるだけでなく、危機のときに完全にシャットダウンするのが簡単です（2020コロナウイルスの発生の初期段階など）。  
法執行機関は、Torタマネギサービス（Torネットワーク経由でのみ利用できるWebサイト）を見つけて閉鎖する機会を何度か持っています。通常のURLではなく、基本的に暗号化キーである「.onion」アドレスを持っています。  
。  
それらの多くは、後で説明する暗号通貨を使用しており、さまざまな方法で追跡することもできます。  
また、技術的な障害がない場合でも、匿名性は本質的に困難です。実際のトランザクション（そして実際、実際のWebトラフィック）  
FDEの場合と同様に、Torはコンプライアンスとの大きな絡み合いを持ち、さまざまな主体が監視を回避し、善悪を問わず法律を回避するのに役立ちます。  
それは間違いなくパフォーマンスのペナルティを課します–ウェブサイトはロードするのに数百ミリ秒ではなく1秒かかることがあります。  
匿名性システムには、適切なソフトウェアだけでなく、慎重な運用セキュリティも必要です。  
Torは、2002年に始まったボランティアプロジェクトを正式化するために2006年に設立された米国の非営利団体であるTorプロジェクトによって維持されています。  
人権に動機付けられた人々の国際社会であり続けています。  
大規模なセキュリティにはインフラストラクチャが必要です。これを主にボランティアの努力で提供するには、契約だけでなく、さまざまな利害関係者のアジェンダ間を変換し、価値について交渉できるリーダーが必要です。  
20.5 HSM  
HSMは、多くのWebサイトのSSL / TLSキーを保護するためにも使用されます。重要なライブキーを開発者のラップトップに置いたり、メモリダンプを通じてクラウドプロバイダーが簡単に抽出したりしたくない場合。  
改ざん防止の章では、HSMを改ざん防止するために使用されるメカニズムについて説明しました。  
また、HSMなどの信頼性の高いコンポーネントと信頼性の低いコンポーネントの間で計算を分割するときに、攻撃者がその分割を利用できないようにする必要もあります。  
これを体系的に分析するにはどうすればよいですか？  
1988年に、LongleyとRigbyは、セキュリティモジュールベンダーのEracom [1184]の仕事をしている間にキータイプを分離することの重要性を認識しました。  
しかし、2000年にMike Bond、Jolyon Clulow、そして私がHSM APIが非常に複雑になり、何百もの異なるトランザクションが数十の支払いプロトコルバリアントをサポートするための暗号操作の複雑な組み合わせを伴う非常に複雑になったことを観察し、そこにあるかどうかについて体系的に考え始めた2000それを壊す一連のHSMトランザクションかもしれません[71]。  
’マニュアルをじっと見つめた後、この種の脆弱性を数多く発見し始めました。  
20.5.1 xor-to-null-key攻撃  
HSMには、改ざん対応メモリに保持される多数のマスターキーが含まれています。  
ATMやその他の端末の鍵を、それらの管理に使用されるデータベースで管理すると便利です。現在、多くのHSMはAzureおよびAmazonクラウドに配置されており、複数のテナントにサービスを提供しています。  
たとえば、セキュリティモジュールのPCI標準では、PIN派生キー（セクション12.4.1で説明されているアカウント番号からPINを取得するために使用されるマスターキー）は、マスターDESの特定のペアの下に暗号化されて格納されます。キーをエクスポートできない作業キーとしてマークします。  
したがって、HSMには、キーコンポーネントを生成して、接続されたセキュリティプリンターで印刷するトランザクションがあります。  
2つのコンポーネントを組み合わせてターミナルマスターキーを生成する別のトランザクションがありました。2つの暗号化キーが与えられると、それらを復号化し、排他的またはまとめて、結果を返します–エクスポート不可としてマークするような方法で暗号化作業キー。エクスポート不可能な作業キーを他のキーで暗号化するトランザクションがさらにあったため、あなたは家に帰って無事でした。  
これで、PIN派生キーを復号化し、任意の顧客アカウントのPINを計算できます。  
上記の攻撃は何年もの間発見されていませんでした。  
実際、HSMは、ATMネットワーキングが1980年代に導入され、銀行が異機種ネットワークを相互に通信させるために、より多くの機能を要求したため、以前のより単純な設計から単純に進化しました。  
HSMにアカウント番号を提供し、それをMACキーであるように見せかけ、PIN検証キーで暗号化することができます。これにより、顧客のPINも直接提供されます。  
 当初、誰もがそうでした–現代のAPIは複雑すぎて、バグをカジュアルな検査で明らかにすることはできません。  
最新のHSMには強力なタイピングがあり、キーについて正式に推論することが容易になります。  
20.5.2下位互換性と時間を使用した攻撃  
当時のトップターゲットは、IBM製品の4758 [951]でした。  
後方互換性を悪用する攻撃に対して脆弱であることが判明しました[279]。  
この優れたアイデアは下位互換性をもたらしました。左のキーを右のキーと同じに設定すると、暗号化はシングルDESに戻ります。  
シングルDES鍵の「左半分」と別のDES鍵の「右半分」を取り、それらを1つのトリプルDES鍵にまとめ、これを使用して他の鍵をエクスポートできます。  
今はそれほど難しくはありませんが、2002年にはまだかなりの作業でした。  
その世代のHSMには、キーの「チェック値」がありました。ゼロの文字列を暗号化することによって計算された、各キーの一方向ハッシュです。  
（たとえば）の表を事前計算します  
HSMに目的のタイプのキーを生成させ、すでにテーブルにあるハッシュが表示されるまでハッシュを出力します。  
下位互換性と時間メモリのトレードオフ攻撃は、PCI PIN管理アプリではなく、HSMプラットフォーム自体に対するAPI攻撃の例です。  
20.5.3差分プロトコル攻撃  
ただし、数百のベンダーと数千の銀行を持つ分散システムのアーキテクチャを変更するのは難しいため、レガシーのキー管理とPIN管理のメカニズムはアプリレイヤーで存続します。  
HSM APIに対する次の攻撃の波は、2003年にJolyon Clulowによって開始されました。アプリケーションロジックをアクティブに操作して情報を漏らします。  
Clulowの最初の攻撃は、エラーメッセージを悪用しました[449]。  
このような攻撃を阻止するために、VisaはPINを暗号化する前にアカウント番号と排他ORするオプションのPINブロックフォーマットを導入しました。  
したがって、さまざまな間違ったアカウント番号を使用して数十のトランザクションをHSMに送信することで、PIN6を計算できます。  
これは、銀行がVISAやマスターカードなどのスイッチに送信するPINとPANの一方向暗号化であり、PIN変換に関するHSMの独自のPCIルールのときにスイッチにスタンドインPIN検証を実行させたい場合に使用します[977]。  
その後、Mike BondとPiotr Zielinskiがさらに攻撃を分類しました。  
 第12章の図12.3に示すように、PINを生成します。  
最初の4つは10進数に変換されますが、ほとんどの銀行は10を法とする16進数を使用してこれを行いますが、すべての銀行がそうするわけではありません。  
これは大きな間違いでした。  
 次に、HSMは暗号化された形式ではありますが、「0000」のPINを返します。  
暗号化された結果が変更された場合、DES出力の最初の4桁が0であったことがわかります。  
同じプロトコルを繰り返し実行したもののわずかに変更された実行を比較する攻撃を差分プロトコル分析と呼びます。  
銀行をクラウドに移動し、AmazonまたはAzure7で管理されているHSMを共有する場合は、さらに問題が発生する可能性があります。  
この非常に単純なケースでさえ、PIN生成のIBMメソッドを放棄しなければならないほど困難であるか、少なくともそのパラメーターを非常に厳しく絞り込んで、そもそもそれらを微調整できないようにする必要があるかもしれません。  
突然攻撃が発生するまで、より多くの顧客のニーズに対応するために、それらはますます複雑になっています。  
20.5.4 EMV攻撃  
ただし、セキュリティ研究者とHSMベンダーがバグを見つけて修正したように、銀行業界は新しいバグを義務付けました。目標は、銀行が発行したEMVカードを注文して、次回にオンライントランザクションを実行するときに、キーなどのパラメーターを変更できるようにすることでした。  
7あるベンダーは、テーブルには少なくとも8つの異なる値が必要であり、4回を超えて発生する値はないことを定めています。  
テキストメッセージの後に、銀行のスマートカードと共有するためのタイプのキーが続きます。  
攻撃は、ターゲットキーの1バイトだけが暗号化ブロックの境界を越えるようにメッセージの長さを選択することです。  
  
2019年の最新のHSMブレークは、公開キー暗号化のPKCS＃11標準をサポートするアプリケーションが認証機関で使用され、 TLSアクセラレータ。  
 彼らは、デバイスのエミュレーターを含むHSMのソフトウェア開発キットを入手し、いくつかの脆弱性が見つかるまでファジングしました。  
これは、不注意なソフトウェアエンジニアリングによって高度な暗号が致命的に損なわれた多くの例の1つにすぎません。  
20.5.6 HSMリスクの管理  
セキュリティエンジニアリングではよくあることですが、根本的な原因は特技です。  
銀行は依然としてPCI規則に準拠するためにHSMを使用する必要がありますが、銀行の暗号鍵は改ざん対応エンクロージャーだけでは保護されません。  
しかし、あらゆる規模の銀行のほとんどには、ソフトウェアのセキュリティとパッチのライフサイクルを理解している人がいますが、HSMに関する真剣な専門知識はあまりありません。  
クラウドHSMの管理はまだ進行中の作業であり、Microsoft Cloud Key Vaultなどの製品では、HSMと同様の機能を提供するエンクレーブの間でキーを前後に移動できます。  
実際、マイクロソフト製品のセールスポイントの1つは、「ハードウェアセキュリティモジュールに関する社内知識の必要性をなくす」[1309]です。  
  
エンクレーブは、完全に信頼していない人が操作するマシンで安全に計算を実行できるプラットフォームを提供することを目的としているという点で、HSMに似ています。  
 干渉しにくくするためにコードを難読化しました8。その後、2000年代初頭の「信頼されたコンピューティング」イニシアチブが続きました。  
 チップ。  
TrustZoneは通常、システムオンチップ（SoC）に実装されます。  
主なアプリケーションは携帯電話であり、ベンダーはユーザーが（規制上の理由により）ユーザーの改ざんからベースバンドを保護するメカニズムを求めていました。  
。  
TrustZoneなどのエンクレーブメカニズムを使用して、セクション12.7.4で説明した種類の攻撃に対して電話バンキングシステムを強化できますか？  
2015年まではクローズドシステムであり、OEMの署名がある場合にのみTrustZoneでコードを実行できました。  
さらに、コードは製品が使用するSoCによって異なります。  
また、ベンダーがクローズドプラットフォームについて行うセキュリティの主張を評価することも困難です。  
2015年に、IntelはSGXを発売しました。そのアクセス制御については、セクション6.3.1で説明しました。  
AWS、Azure、Googleなどのサービスでシステムを実行する方が安くなります。仮想化によりリソースを効率的に共有できるため、データセンターやシステム管理者などのコストを数千の顧客に分散させることができます。  
ハイパーバイザーソフトウェアの技術的な悪用などにより、機密データがクラウドサービスの他のテナントに漏洩しないようにするにはどうすればよいですか？  
また、令状を使用してデータにアクセスすることで、国家が国家に対してどのような保護を行っていますか。つまり、ハイパーバイザーの合法的な悪用です。  
これらの懸念があるため、SGXのセキュリティ境界はチップ自体の境界です。  
CPUのハードウェアは、機密性と完全性の両方を保護します。  
鍵となる暗号化メカニズムはソフトウェアの証明であり、これにより、CPUは、信頼できるハードウェア上で変更を加えることなく、実行しているソフトウェアの所有者を証明できます。  
エンクレーブの初期化、アドレス変換、ページの削除、例外処理などの詳細は非常に複雑です。説明と分析については、Victor CostanおよびSrini Devadas [479]を参照してください。  
特にMeltdownとSpectreがセクション19.4.5で説明したサイドチャネル攻撃の一時的な実行ファミリーを導入して以来、複数のサイドチャネル攻撃もあります。ここでの私の懸念は、エンクレーブをサポートするために使用される暗号と、その上で実行されているソフトウェアを証明すること、および他の暗号またはアプリケーションの暗号サポートのプラットフォームとしての適合性です。  
各チップにはヒューズがあり、ファブにはシールの秘密とプロビジョニングの秘密が書き込まれます。前者はIntelには知られていませんが、後者は知られています。  
 これにより、電源サイクル全体でキーマテリアルが確実に生成されます。  
これらのキーを使用すると、CPUはIntelに対してその真正性を証明し、Intelの拡張プライバシーID（EPID）のメンバー秘密キーである証明キーを提供できます。  
これらの操作は特権起動エンクレーブ（LE）で行われます  
もともとすべてのSGXコードはIntelによる署名が必要でしたが、最近のバージョンではサードパーティによる署名が許可されています。  
。  
1つの問題は、1つのチップのMDKが（どのCPUでもどこでも）妥協すると、同じグループ内のすべてのCPUの認証セキュリティが壊れることです。  
Intelも同じように脆弱です。MDKの明確な価値を考えると、SGXの保護メカニズムの外にSGXエンクレーブを作成できます。  
すべての証明はIntelによって不透明に行われ、ユーザーは結果を単に信頼する必要があるため、これらのグループがどれほど大きいかはわかりません。  
10SGXはキャッシュタイミング攻撃を防御しないため、エンクレーブコードを作成する場合、データ依存型ジャンプを使用できません。  
現在、実際の作業を行っているSGXシステムがいくつかあります。  
その開発者は、Signalブログ[1226]で、ソースコードの開発の難しさについての広範なディスカッションを公開しました。  
どのようにして洞察を持たずに大きなソーシャルグラフを作成できますか？  
ただし、これをSGXエンクレーブのメモリ制限（128Mb）内で行うと  
メモリアクセスパターンを介した情報漏えいを防ぐには、さらに多くのことを行う必要があります。そのようなパターンを介してブランチが観察される可能性があるため、コードの重要なセクションにブランチを含めないでください。  
SGXも低速です。メモリ暗号化自体はオーバーヘッドをほとんど追加しませんが、コンテキスト切り替えはキラーです。  
SGXアプリのもう1つの例は、MicrosoftのCloud Key Vaultです。これにより、Azureテナントは、コードとは別に、キー、パスワード、トークンなどのシークレットを保存できます[1309]。  
要するに、良いSGXコードを書くのは難しいです。  
賢い人なら、信頼できるマルウェアを書くことができます。  
そして、あなたがインテルを完全に信頼しているとしても。 NSAがFISAの令状を使用して、インテルにデバッグモードのエンクレーブを証明するように強制しないと信じている場合でも、 MDKの妥協やサイドチャネルの悪用について心配していなくても、HSMと同様に、アプリレイヤーが公開されるリスクがあります。  
Intel（およびArm）  
インテルは暗号化開発者を管理エンジン（ME）に向けている  
マシンの盗難が報告された場合、キーを消去してCPUをブリックすることができます。  
これは、Javaの信頼された実行環境を備えた別のエンクレーブをサポートします。この環境では、開発者は暗号化を実行できます。たとえば、決済端末では、MEからPINパッドまでのハードウェア信頼パスを設計できます[1698]。  
MEにも一連の脆弱性とエクスプロイトがありました。  
  
暗号の使用と制限に関する前のセクション、暗号を使用して匿名性をサポートする方法、および暗号アプリがスタックのさまざまなレベルのフローにどのように影響するかについて、暗号通貨とスマートコントラクトについて説明します。  
多くの人にとって、「クリプト」という言葉は暗号ではなくビットコインを指すようになりました。  
この匿名のデジタルキャッシュのシステムは、最初はサイファーパンクメーリングリストの愛好家や活動家の間で流通しましたが、2年以内に口コミで広まりました。  
買い手と売り手はTorタマネギサービスで会い、ビットコインを使用して商品やサービスの代金を支払うことができました。  
シルクロードは急速に規制薬の通信販売の市場となり、2013年10月にFBIがウルブリヒトを逮捕する前に、10億ドルを超える取引が通過しました[421]。  
シルクロードが取引されている間、価格は約1ドルから100ドル以上に上昇し、価格の上昇は投資家を魅了しました11。  
2017年までに、バブルが発生しました。ビットコインの価格は、1,000ドルを突破し、2017年12月のピークがほぼ20,000ドルに急上昇しました。ブースターは、人間や銀行が邪魔することなく、マシンが互いにスマートコントラクトをネゴシエートできるため、暗号通貨がイノベーションと自動化の新しい波を可能にするだろうと主張しました。  
、熱狂のピークは過ぎましたが、暗号通貨は投資家にとって新しい資産クラスになり、金融規制当局や法執行機関に複数の問題を提起しています。  
ソフトウェアを作成する人々以外に信頼できる当事者はおらず、参加者の推定IDはありません。  
セクション7.3.1。  
。  
1。  
2。  
3。  
 以前のトランザクションから、それを1つ以上のアドレスに転送します。  
4。  
他のユーザーは、リクエストされたトランザクションのセットを自由に選択し、それらが有効であることを確認し、それらをブロックチェーンの新しいブロックにマイニングできます。  
トランザクションの各ブロックは、ブロックの内容のSHA256ハッシュとランダムなソルトによってマイナーによって認証されます。  
このようなハッシュは作業の証拠を構成し、それらを見つけることはランダムなプロセスであるため、どの鉱山労働者が次の鉱山を見つけるかを予測することは困難です。  
パズルの難易度は自動的に調整されるため、約10分ごとに新しいブロックが採掘されます。  
鉱山労働者は、自分が採掘したブロックごとにブロック報酬を受け取ります。これを書いている時点では、これは12.5ビットコイン、つまり$ 100,00012を超えています。  
鉱山労働者は、各取引の入力が出力を超える金額である取引手数料も受け取ります。  
8。  
結果として、約6のブロックがさらに採掘されるまで、トランザクションは最終的なものとは見なされません。クラシックビットコインの場合は約1時間です。  
122020年の初めに、kWhあたり5cの電力を購入できる鉱山労働者は、機器のコストを無視すると、市場で取得するコインの約半分に相当するビットコインを採掘することが期待できます。  
したがって、鉱山掘削装置​​に投資する人々は、ビットコインの価格が上昇し、規制当局が需要を抑制するのに効果的ではないことを賭けています。  
競合が解決されない場合は、フォークが発生する可能性があります。システムは2つの互換性のない後続を生成します。  
しかし、一部のフォークは慎重に行われ、その起業家に加えて数千のビットコインクローンが開始されました。そのほとんどは詐欺でした。  
トランザクションには、支払いをプログラム可能にするスクリプトを含めることもできます。  
最初の2つは、プリンストンコンピュータサイエンティストのグループによる技術解説です。2015年に、ジョーボンノー、アンドリューミラー、ジェレミークラーク、アービンドナラヤナン、ジョシュアクロール、エドフェルテンによる18ページの知識体系化論文[293]は、308歳です。 Arvind Narayanan、Joe Bonneau、Ed Felten、Andrew Miller、Steven Goldfeder [1383]による2016年の本があります。  
執筆時点では、これらは古くなっているので、以下では、それ以降の開発に集中します。  
暗号通貨で何がうまくいかないのかを理解するには、暗号数学だけでなく、もっと多くのことを検討する必要があります。  
  
当初、すべてのビットコインユーザーは仲間でした。完全なクライアントソフトウェアはビットコインをマイニングし、マイニングしたコインを使うことができます。  
1つ以上のUTXOのロックを解除する秘密鍵を知ってビットコインを所有しているため、アカウントに固有の概念はありません。  
。  
ユーザーが選択したパスフレーズから秘密鍵を生成する、いわゆる「脳財布」は、ブロックチェーンに表示されている公開鍵を徹底的に検索する攻撃者によって破られました。推測可能なパスワードを持つ脳財布は、通常24時間以内に空にされました[1947]。  
真面目なオペレーターは、本質的に小さなHSMであり、オフラインで保管できるハードウェアウォレット（いわゆるコールドウォレット）を使用します。  
それでも、数百万ドル相当のビットコインを所有していることで知られている人々が自宅で武装強盗に押収され、強制的に譲渡されることは知られています。  
2013年までに、エクスチェンジまたは他のオンラインサービスプロバイダーがすべてを代行するホスト型ウォレットの登場を目にしました。  
しかし、以下で説明するように、ホストされたウォレットは、他の広範囲にわたる詐欺や悪用を引き起こしています。  
20.7.2鉱夫  
マイニングリグはFPGAを使用して登場し、その後ASICを使用して登場したため、汎用マシン上のソフトウェアよりも数年以内に引き継がれました。2019年の暗号通貨採掘の総エネルギー消費量は約75TWhで、CO2排出量は3,500万トンを超えました。これは、ニュージーランドの二酸化炭素排出量に匹敵します。  
鉱山労働者は、自分たちの収入を平均化する少数の鉱山プールに組織化しました。  
容量はレンタル可能で、いわゆる51％攻撃で暗号通貨を攻撃するために使用されることがあります。  
初期の頃、人々はそのような攻撃は即座に通貨の信頼性にとって致命的であると考えていましたが、現実はより複雑であることが判明しました。  
しかし、その市場価値には大きな影響はありませんでした。  
2020年8月にさらに2回の攻撃があり、そのうちの1つは$ 192,000を費やして$ 5.6mを盗むために必要なハッシュパワーを購入しました[1519]。  
  
ビットコインのスクリプト言語はシンプルですが、後の暗号通貨システムであるイーサリアムにはチューリング完全なVMがあり、そのバイトコードは通常Solidityと呼ばれる言語からコンパイルされています。  
バブルの間、多くの新興企業がスマートコントラクトを使用してモノのインターネットをアニメーション化し、分散ストレージなどの新しいサービスを作成することについて話しました。  
これは、2000年代にオンライン市場を支配するようになった大規模なサービス企業からオンラインの世界を遠ざけることを目指す「再分散化」運動に関連しています。また、静的な読み取り専用コンテンツの配布を分散化するための優れたツールはありますが、トランザクションを分散化するための優れた方法がありませんでした[509]。  
 人が介入することなく、ある暗号通貨を別の暗号通貨と交換できるようにします。  
 これは興味深い新しい故障モードにつながりました。  
フロントラン（予測と悪用）によってDEXの非効率性を悪用するアービトラージボットが登場しました  
ボットはイーサリアムでガスと呼ばれる取引手数料を入札します。何億ものこれらの優先ガスオークションがあり、トレーダーは彼らの取引の優先権を得るために急いでいます[508]。  
バグの修正には費用がかかる場合があります。  
攻撃者は契約のフローを悪用して金銭を盗みました13。そしていくつかの議論の後、イーサリアムソフトウェアは盗まれた金銭を回収口座に移動するように変更されました。  
デンマークの研究は、実際のアプリケーションコンテキストでスマートコントラクトを使用することのさらなる問題を示しています。  
意思決定の実行を自動化することで官僚的な足の引きずりがなくなることを期待して、親と控訴委員会の両方がそれらを追跡できるように、Ethereumブロックチェーンに事件文書のハッシュを置くというアイデアでした。  
 地方自治体は頻繁にハッキングされ、ランサムウェアを支払う傾向があります。  
 ブロックチェーンは設計上不変であるため、パッチを適用できません。  
さらに2つの問題には、作業を行うためにルールを曲げなければならないことが多く、プログラマはPythonやCobolなどの一般的な言語ではなく、Solidityなどの不慣れな言語でバグを書く可能性が高いという事実が含まれます。セクション7.3.1.2で説明した新しい言語。  
20.7.4O↵チェーン支払いメカニズム  
これは、身代金の支払いや麻薬のオンライン購入には十分な速度かもしれませんが、EMVと比べると印象的ではありません。  
人々は、サイドチェーン（レイヤー2プロトコルの例）を使用してこれを修正しようとしています。このようなプロトコルは、BitcoinやEthereumなどのレイヤー1プロトコルの外部でトランザクションを行います。  
重要なアイデアは、ハッシュされたタイムロックコントラクト（HTLC）を使用して、暗号通貨を相互にコミットすることです  
このような転送では、ボブはアリスh（R）を送信します  
これにより、チャネルを決済してチャネルを閉じることを決定するまで、署名されたトランザクションを迅速に取引するためのチャネルが開きます。  
アリスとボブのそれぞれが収益からどれだけ取るべきかについて合意しない場合、紛争解決メカニズムが必要です。  
理論的には、これはピアツーピアになる可能性がありますが、実際にはそのようなシステムは、銀行ネットワークのように、常にオープンなチャネルを持つハブに組織化されているように見えます。  
コストには、トランザクションを転送するのに十分な流動性を備えた中間ノードの必要性、すべてのアクティブなプレーヤーがオンラインである必要性が含まれます-その意味は、ホットウォレットの盗難リスクから、ボブがRをブロードキャストするときにマイナーがフロントランニングするリスクまでさまざまです。 、ネットワーク障害後の大規模な崩壊のリスクへ[831]。ここでの制限は流動性にあるように見えます。Lightningチェーン自体は信頼されていませんが、ノードで容量を占有するため、受信者はそれらを受け入れるかどうかを決定する必要があります。  
Lightningの総資本金は数百万ドルにすぎないように見えるため、これにより多少脆弱になる可能性があります。  
  
自分のコインをすべてマイニングすることは不便であり、2010年までに起業家はビットコインを通常のお金と交換する取引所を設立しました。  
2011年までのリーダーは、2011年に1回のハッキングを生き延びた日本のマウントゴックスでしたが、4億6000万ドルでハッキングされたと主張して2014年に破綻しました。  
それだけではありませんでした。  
顧客が正しいパスワードを入力した後、エクスチェンジが秘密鍵に一時的にアクセスできるかどうかに関係なく、顧客のビットコインを別々のウォレットに保持する代わりに、マウントゴックスはすべてのビットコインを独自のウォレットに保持し始め、概念的なアカウントを顧客に示しました彼らがそのウェブサイトを訪れたときのバランス。  
被害者は、ウォレットがホストされた後、許可していない発信トランザクションをどのように見始めたかに関連していました。  
2013年半ばから、あなたが彼らからビットコインを購入したとき、彼らがしたことは、あなたが1つのビットコインの残高があることを示すWebページを表示することだけでした。  
 ビットコインの世界は詐欺でいっぱいで、暗号犯罪の犠牲者の大部分は、破産した、またはハッキングされた、またはハッキングされたと主張する取引所によって取り除かれたようです。  
ビットコイン分析会社であるChainalysisのレポートは、2018年に取引所がハッカーに約10億ドルを失い、ほとんどの窃盗は2人の犯罪組織によって行われたと結論付けました。そのうちの1つは、北朝鮮にリンクされています。  
市場操作もあります。  
ドル、2017ブームの間に[822]、多くの暗号通貨の市場価格が不法な操作の結果である可能性が高いという見方を高めました。  
市場操作はさておき、これまでで最大の単一の暗号通貨詐欺は、PlusTokenと呼ばれるPonziスキームであり、主催者が2019年に逮捕される前に中国国民から約30億ドルを獲得したようです[864]。  
ランサムウェアは、2001年から2015年の間に年間約200万〜300万ドルから年間800万ドルに増えました。この犯罪の種類は着実に増えていますが、身代金はギフトカード経由でも収集されます[1190]。  
その年、世界最大のダークネットの児童ポルノウェブサイトWelcome to Videoは、オペレーターがブロックチェーン上のビットコインのフローを介して追跡された後、閉鎖されたため、仮想通貨の偽名の性質には限界があります[551]。  
定期的な交換はまた、法執行機関にとって生活を困難にします。  
ただし、ビットコインは仮名を使用しますが、ブロックチェーンにはすべてのトランザクションの永続的な記録が含まれています。  
実際のトランザクションとデータにはコンテキストがあり、推論を行うことができます。  
ただし、その場合、ビットコインをマネーロンダリングの試みで汚染します。合計で、ビットコインの10％が少なくとも1回は盗まれたか、マネーロンダリングサービスを通過したと考えられます。  
 例として、オハイオ州の男は、3億ドルを洗浄したそのようなミキサーを操作したとして2020年に起訴されました[553]。  
現在、Moneroは最も強力なプライバシーを提供し、ソフトウェアを使用してコインを採掘できるように設計されています。そのコインの4％以上が他の人のマシンで実行されているマルウェアによって採掘されています[1529]。  
米国財務省の金融犯罪執行ネットワーク（FinCEN）  
 そして、お客様を知っている（KYC）  
一部の政府はさらに進んでいます。  
しかし、これを書いている時点で、最大のプッシュは2019年のFinCENアドバイザリによるもので、10,000ドルを超えるトランザクションを処理する人は送信者と受信者の両方を特定し、疑わしい事件必要に応じて活動レポート。  
ヨーロッパでもさらなる規制が議題になっています。  
イギリス人またはアメリカ人のユーザーがビットコインを別のユーザーに送信する場合、トランザクションがブロックチェーンに近づかない可能性がかなりあります。両方がコインベースの顧客である場合、コインベースはビットコインウォレットのウェブページに表示される残高を調整するだけです。EUでは、電子マネー指令が適用されるように見えるかもしれませんが、英国とドイツの規制当局は、顧客が取引所で持っている従来の通貨残高に関してのみそれを施行します。取引所は、取引需要は投資需要よりもはるかに少ないため、仮想通貨は支払いメカニズムとしてではなく資産として扱う必要があると主張しました。  
 同僚と私が作成した、為替操作と盗まれたビットコインの追跡のメカニズムの分析では、決済サービス指令を適用することを推奨しました。これにより、銀行と同等の消費者保護が取引所の顧客に提供されます[116]。  
暗号通貨の世界における消費者保護は未完成のビジネスであり、ヨーロッパなどの規制当局が取り組んでいます。  
20.7.6許可されたブロックチェーン  
次にCIOは、ビットコインの環境廃棄物、違法なコンテンツ、違法な俳優なしで、有用な作業を実行できるブロックチェーンを作成できるかどうかを調査する必要がありました。  
多くは、作業証明ではなくビザンチンフォールトトレランスに基づいており、スマートコントラクトをサポートできる、許可されたブロックチェーンファブリックを必要とします。  
 提案。  
アプリケーションの例として、JPモルガンは参加銀行がブロックチェーンに住宅ローンを入力できるようにする2015年のシステムに取り組みました。そのスクリプト言語により、トレーダーは任意の複雑さの先物とオプションを作成できるようになります。  
結論の1つは、大多数のアプリケーションでは、ブロックチェーンは必要ないということです。前方に安全な封印されたログで十分です。  
何よりも、ブロックチェーンアプリはレガシーシステムと通信する必要があり、アプリケーションのセキュリティミスやユーザビリティの危険を生み出す可能性が高くなることはありません。  
 ブロックチェーン上で、それが法的に有効であると宣言したところ、誰かがそれをハッキングしてコロナウイルスに関する偽のニュースを公開した[499]。  
おそらく最も物議を醸しているプロジェクトは、その価値を通貨のバスケットに釘付けにした支払いシステムを作成するFacebookの提案であるLibraでしょう。  
  
多くの人々がブロックチェーンに基づく電子投票システムを提案しています。なぜなら、それらは不変であり、暗号を使用してそれらに機能を構築できるからです。  
実際、2017年から8月のビットコインブームの間、一般的な学生プロジェクトの提案は「ブロックチェーンに選挙を実施することにより世界平和を解決する」でした。  
2018年、モスクワ市の3区のシステムは投票集計にイーサリアムブロックチェーンを使用しましたが、選挙直前に2つの暗号化の脆弱性が修正されたため、投票集計とブロックチェーン間のリンクが壊れ、ブロックチェーンは直後に消えました[782 ]。  
Michael Spectre、James Koppel、MITのDanny Weitznerがリバースエンジニアリングを行い、攻撃とは無関係なアプリのブロックチェーンの使用にもかかわらず、攻撃者が投票を公開したり変更したりできる多数の脆弱性を発見しました[1810]。  
ブロックチェーンが選挙の問題を解決できるという考えは、経験豊富なセキュリティエンジニアを絶望させます。  
有権者は規則を絶えず変更し、スタック内のすべてのレベルでテクノロジーを破壊しています。有権者の登録からキャンペーンの資金調達、広告ルール、メディアの検閲、有権者への脅迫、操作可能な投票スキームまでです。  
  
1980年代から、多くの人々が暗号をシステムセキュリティのある側面の信頼できるプラットフォームとして使用しようとしました。  
多くの暗号研究者（私を含む）  
匿名の通信は検閲を停止します。匿名のデジタルキャッシュは私たちのプライバシーを保護します。デジタル投票を行うと、選挙の準備が難しくなります。しきい値署名は、堅牢な内部統制システムの構築に役立ちます。そして、電子オークションは腐敗を押し戻すでしょう。  
一世代後、グローバル化されたテクノロジーの影響について懐疑的なテクラッシュを備えた今こそ、棚卸しする時かもしれません。  
技術的なポイントは、暗号化システムは魔法ではないということです。彼らにはバグがあり、他のようにパッチを当てる必要があります。  
HSMは、機能が破壊されるまでさらに多くの機能を獲得した暗号システムのもう1つの例であり、標的型攻撃をブロックするために他のコンポーネントが必要になりました。すべての中で最も複雑なエコシステムを開発したブロックチェーンについても、ほとんど同じことが言えます。  
繰り返しになりますが、暗号通貨は機能を壊すまで機能を獲得し続けることができ、スマートコントラクトはプロセスを進めるのに役立ちます。  
HSMはサーバーよりもコストがかかります。  
ビットコイン鉱山労働者はニュージーランドと同じ量のCO2を排出します。  
コストがそれだけの価値があるかどうかについての詳細な計算があります。また、この計算は、メンテナンスコストが増加し、システムが技術的負債を負うにつれて、時間の経過とともにさらに悪化する可能性があります。  
成功した場合、彼らは彼らの中心的な目的の一部として、いくつかの規制を満足させたいという欲求か、規制を避けたいという欲求のどちらかを獲得したようです。  
ハードウェアセキュリティモジュールはカード決済システムで必須です。カードスキームルールは、結局のところ、銀行が詐欺の責任を負わないことを望んでいるためです。  
ビットコインとその多くのクローンは、証券および支払法からマネーロンダリング防止法まで、あらゆるものを回避するためのメカニズムになっています。  
暗号通貨に関しては、これまでのところ、極端なボラティリティ、容量制限、予測不可能なトランザクションコスト、ガバナンスなし、透過性の制限がありました。  
法律は、民間企業や個人がクーポンやエアマイルなどのバリュートークンを作成する権利を擁護する必要がありますが、これらが通貨として使用されるようになり、銀行のように振る舞う機関が出現すると、弁護士がそれらをそのように扱うことは合理的です。  
現実の問題を解決するために数学の魔法を適用しようとした40年の経験を要約する必要がある場合、それはおそらくTANSTAAFLでしょう。無料の昼食などはありません。  
分散型プロトコルは化石化する傾向があります。何かを変更するのが難しいため、1990年代初頭からメール、DNS、BGPメカニズムを使用しています。  
ビットコインは別の例を提供します。  
しかし、鉱山掘削装置​​の生産は独占的になり、Bitmainによって制御されていますが、ASICはすべてTSMCから供給されています。  
保管取引所は事実上、規制されていない銀行になった。  
Torではこれはコミュニティですが、暗号通貨の世界では利益のために働いている競合する開発者チームがあります。  
一般に、スマートコントラクトの信頼性はどうですか？  
これに関する文献は増えており、一連のワークショップでさえありますが、メソッドはまだかなり単純なAPIにしか取り組むことができません。  
DEXのセットアップに使用されるスマートコントラクトの多くに、必要に応じて人間の介入を可能にするハードコードされた管理キーがあることは驚くべきことではありません。  
参考資料Torについて理解を深めるには、Tor Projectのドキュメントページから始めるのがよいでしょう。  
集中化とプライバシーの相互作用については、Carmela Troncosoと同僚[1910]を参照してください。  
 [1917]にあります。