あなたが望むものであり、ソニーやワーナーやAOLが望むものではありません。  
1はじめに著作権は、デジタル時代の非常に論争の的となっている問題の1つであり、デジタル著作権管理（DRM）の開発を牽引してきました。  
 我々は勝った;音楽や映画業界での力は、EMIやUniversalなどの企業からApple、Spotify、Amazon、Net ﬂ ixなどの企業に渡り、Amazonは書籍で市場を独占しました。最初は物理的に、次に電子書籍でした。  
 この章を第3版から削除し、オンラインで第2版の章を紹介することについて真剣に考えました。技術的な説明はそれほど多くないからです。  
 第9章で説明するマルチレベルの安全なシステムはほとんど時代遅れですが、軍事用コンピュータのセキュリティの発展を促し、今日のセキュリティ環境にさまざまな微妙な影響を与えたので、著作権戦争もその痕跡を残しました。  
 ゲームプラットフォームでも非常によく似た手法が使用されており、プレーヤーがエイムボットを使用するのを難しくしています。 。  
 この73724を節約する私の最終的な理由。  
 はじめに章では、著作権戦争は私たちの共有セキュリティ文化の一部になったということです。若すぎて参加できなかったとしても、時折、私たちの灰色ひげが燃えているものを理解するのに役立つことがあります。  
1709年のアンの定款から始まり、プレス検閲をめぐる18世紀の戦いを経て、啓蒙主義と米国憲法の枠組みに至るまで、近代著作権法の制定を通じて繊細さが続いた。  
 著作権の仕組みは、情報を支払っていない人々の手に渡らないようにするために存在し、検閲者は情報を信頼していない人々の手に渡らないようにします。  
20世紀にわたって、文芸著作権、映画、音楽の所有者に蓄積された莫大な富は、支配に対する強い関心を生み出しました。  
 これらの法律は、フィッシングWebサイトの停止から、プリンターカートリッジの補充や、壊れたデバイスの修理まで、さまざまな目的で使用され、悪用されてきました。  
 ファイルを暗号化してコピー不可にしてから、ユーザーに固有のキーを使用して暗号化されたメディアファイルのキーである「ライセンス」を別途提供するというDRMisの基本的な考え方に加えて、「権利管理言語」の記述についてユーザーはコンテンツを操作できます。  
 また、歴史のクイックツアーを提供し、衛星テレビの暗号化システム、著作権のマーキング、裏切り者の追跡などの興味深い変種について説明します。  
いくつかの深刻な政策問題がこれらすべてに混同されています。  
 コンピュータ業界はDRMに抵抗しましたが、ハリウッドと音楽業界はそれを導入することを強制しました。  
 音楽はもはやUniversalやEMIなどの企業ではなく、AppleやAmazonなどの企業によって運営されています。そしてストリーミングへの移行により、Spotifyなどの新しい企業がパーティーに参加できるようになりました。  
 これまでに聞いたすべての音楽トラックとこれまでに見たすべての映画を知っているMicrosoftのライセンス管理サーバーの代わりに、現在Apple、Spotify、またはNet ﬂ ixのストリーミングサーバーになっています。  
2。  
2著作権著作権の保護は、長年、映画、音楽、書籍出版業界に執着してきました。  
 19世紀に戻ると、写真の発明が本の出版業界を破壊するという警告がありました。 18番目の本の出版社は、公共の貸出図書館を閉鎖しようとしました。彼らが再び気付くまで、彼らは大規模なリテラシーを生み出し、売り上げを伸ばしていました。一方、16世紀には、可動式活字印刷の発明は、王子や司教からクラフトギルドまで、当時のほとんどの権力者によって破壊的であると考えられていました。  
 しかし、最初にソフトウェアの保護について見ていきます。DRMにつながった著作権の問題のほとんどは、1980年代からPCおよびゲームソフトウェア市場で見られたからです。  
2。  
 IBMは1960年代に、ユーザーが作成したプログラムをユーザーが共有できるようにする計画を立てました。  
 しかし、研究で使用されたソフトウェアは広く共有されました。コンピュータを所有するほとんどすべての組織は、大規模で尊敬されていました。彼らのソフトウェアは熟練したメンテナンスを必要とする傾向がありました。  
 そこで、ソフトウェアではなくサービスを購入しました。  
1960年代にミニコンピュータが登場したとき、ソフトウェアのコストはかなり高くなった。  
 そもそも、ハードウェア、ソフトウェア、メンテナンスといった完全に特注のシステムを販売していたため、海賊行為はそれほど問題ではありませんでした。  
 当時最も一般的な著作権紛争は、プログラマーがあなたの会社を辞めて競合他社に加わったときであり、彼らのコードは突然あなたの多くの機能を獲得しました。問題は、彼がコードを一緒に持っていったのか、再実装したのかということでした。  
 たとえば、ソフトウェアがアセンブラで作成されていたため、人々が初期のIBM PCのROMからソフトウェアをコピーしたかどうかをめぐる訴訟により、レジスタがプッシュおよびポップされる順序がオンになりました。  
 詳細1暗号解読者のウィリアム・フリードマンと彼の妻のエリゼベスは、ベーコンがシェイクスピアを書いたかどうかを解明するために、環境大金持ちに雇われました。  
2。  
 Codestylometryはまだ研究の活発な分野です[370]。  
 そのため、在庫管理のためにミニコンピュータを購入した（または、局のサービスに応じて契約した）会社は、管理プログラムを準備するだけでなく、統計プログラムを実行したくなるかもしれません。  
 Sosomeシステムハウスは、施行メカニズムの設計を開始しました。  
 1981年に小売在庫管理システムを販売している会社で働いていたとき、数か月ごとに次のようなメッセージが表示されました。  
 WXYZはライセンスシリアル番号の暗号化されたバージョンでした。発信者がその顧客からのものであると主張した場合、パスワードを提供して、今後数か月間システムを再度有効にします。  
）このメカニズムは、「顧客」が理解できれば簡単に打ち破られた可能性がありますが、実際には問題なく機能しました。ほとんどの場合、障害メッセージを受け取ってオフィスに電話をかけたのは低レベルの店員でした。  
 最初の反応はさまざまでした。  
「それに取り組んだ人々に給料が支払われるかどうかは誰が気にするのですか？」彼は尋ねた。  
「フェアプレーへのアピールはこれまでに至っており、業界は次にミニと初期のマイクロの間のメインディエンスに取り組みました。後者はプロセッサーのシリアル番号がありませんでした。  
1。  
最も単純なのはシリアル番号だけでした。最も一般的に実行されるのは、単純なチャレンジ/レスポンスプロトコルです。一部のトップエンドデバイスは、実際に計算の重要な部分を実行しました。  
 初期の非常に一般的な戦略は、単純なコピーに抵抗する方法でソフトウェアをPCのハードディスクにインストールすることでした。  
 これで、製品が標準ユーティリティを使用してハードディスクからコピーされた場合、不良セクタはコピーされず、コピーは機能しません。  
 [1001]。  
2。  
 ただし、一般的には、コピーの保護とマスターの保護を区別する必要があります。多くの場合、必要に応じてバックアップ用にコピーを作成できるようにする必要がありますが、コピーのコピーを作成することはできません（これはコピー生成制御と呼ばれます）。  
 1988年にライセンスサーバーが登場しました。これは基本的に企業ネットワーク上のすべてのマシンで共有されるドングルとして機能するようにプログラムされたマシンで、企業が最大20台のマシンでプログラムを実行する権利を購入できるようにするなど、より複雑なビジネスモデルをサポートしていました。かつ、複数のソフトウェア会社が同じライセンスサーバーを介して製品のライセンスを取得できるようにします。  
 私が1989年に取り組んだ製品は、PCに指紋を付けました-存在する拡張カード、メモリの量、プリンタの種類-そして、この構成が極端に変化した場合、ヘルプラインに電話するようにユーザーに要求します。  
 したがって、ソフトウェアを特定のマシンフィンガープリントに関連付けることができます。広告トラッカーは、今日と同様の手法を使用しています。  
 多くの愛好家がスポーツのためにこれを行い、発売後できるだけ早くソフトウェア製品の保護されていないバージョンをオンラインに置くことを競いました。  
 重要なコードをコピーできない場所（ドングル、ライセンスサーバー、または最近のクラウドなど）に置くことでこれを止めることができますが、このアームレースは、そのようなことをしないと、デバッガーを備えた子供たちは常にあなたのスキームを常に破壊することを皆に教えました。  
ベンダーは心理的手法も使用しました。これは、偽の名前で登録されたコピーを海賊版で配布することを阻止するものではありませんが、正当なユーザーがカジュアルなコピーを同僚に与えることを阻止します。  
これらは、後で詳しく説明する著作権表示の例です。  
•初期のMicrosoftソフトウェア（Multiplan、Word、またはChart）がデバッガーの下で実行していると思った場合、「悪の樹は苦い実を結ぶ。  
’その後、フロッピーディスクのゼロを追跡し、「rrnt、rrnt、rrnt」に進みます。  
2。  
 ゲーム市場はハードウェア保護に移行し、ソフトウェアが独自のカートリッジで販売されたクローズドアーキテクチャのコンソールが支配的になった。  
 これにより、ハードウェア保護を使用してアフターマーケットを制御するアクセサリ制御が可能になりました。これは、プリンタを販売する企業などに採用されました。  
6。  
 このような製品ではテクニカルサポートが重要な場合が多いため、ソフトウェアとサービスのバンドルとして販売される場合があります。  
•重要なコードの一部を実行するためにドングルハードウェアにお金を費やす準備ができていない限り、マスマーケットソフトウェアのメカニズムは、知的チャレンジの対象となる人々によって打ち負かされ、保護されていないコードは匿名で公開されます。  
 複数のドングルが邪魔になるか、互いに干渉します。  
 （この権利を取得する難しさは、ライセンス管理を使用する多くの企業がFlexlmを使用する理由の1つです。  
 両方の慣行が共通であったため、どちらか一方を非常に困難にするメカニズムが問題を引き起こしました。  
•コンピュータウイルスの到来により、企業のお客様はソフトウェアの衛生に投資する必要が生じたため、カジュアルなコピーはそれほど簡単には容認できませんでした。  
•個人ユーザーに嫌がらせをすることで得られるお金はそれほど多くありませんでした。  
 ツールの海賊版を入手してそれを気に入った人は、通常のコピーを購入するか、雇用主に購入を勧めるでしょう。  
 いつか彼らはそうするでしょう。  
 彼らは一種の中毒になり、次の10年間にどのように収集するかを何らかの方法で考え出します」[755]。  
2。  
 たとえば、ツールの場合、ボーランドは1983年にターボパスカルを発売して業界を揺るがしました。  
 Borlandの製品の価格は49ドルです。  
（それで、他の多くの人々と同様に、それを聞いて、友達からコピーを借りて、それを試して、気に入って、外に出て購入しました。  
その後、業界は法律に目を向けました。  
 詳細は国によって異なりますが、著作権侵害は、商業規模で行われた場合にのみ犯罪になる傾向があります。  
 ただし、大規模なユーザーに対しては、著作権の行使は価値があります。  
1988年、マイクロソフトはIBMの足跡を残して業界をリードし、無許可のソフトウェアの広範な使用を容認していた大企業の注目を集める業界団体（米国のビジネスソフトウェアアライアンスなど）を設立しました。  
業界は、法律が執行のためのツールを提供するだけでなく、制限も設定していることを発見しました。  
 彼らの顧客は、彼のソフトウェアに定期的にロック解除コードを入力する必要がありました、またはフリーズして、データへのアクセスを拒否しました。  
Oceの普及により、Microsoftは企業部門への課税となり、25,000を超えるライセンスを持つ顧客からの収益のほとんどを占めていました。  
 これらはアプリケーションコードを分解することで依然として敗北する可能性がありましたが、コードが大きくなるにつれてこれは難しくなり、いくつかの訴訟が提起されたため、大企業にとって魅力がありませんでした。  
パーソナルソフトウェアでは、オンライン登録に重点が移っています。つまり、製品を設計することになります。SecurityEngineering743Ross Anderson24。  
 COPYRIGHTは、顧客にあなたのWebサイトと対話させる-曲、最新の為替レート、またはセキュリティ更新をダウンロードするかどうか。  
私はこの本の第2版で2008年に書きました：「サービスとしてのソフトウェアは、ソフトウェア（またはオンラインでライブ配信できるその他のコンテンツ）の最終的な著作権保護またはDRMかもしれません。購入することはできません。バージョンを凍結してください。実行中、またはoitineを使用します。  
 それはまさに、ソフトウェア業界が2010年代初頭から収束してきたモデルです。  
5。  
 ソフトウェアはサブスクリプションで販売され、コピープロテクションの問題はなくなります。  
2。  
これは、当初IBMを意味していた当時の主要なプラットフォームを引き続きサポートしていました。ただし、世界中のその他の学者がハードウェア上で実行されるソフトウェアを作成しており、ほとんどがFORTRANのような高級言語で作成されているため、IBMのメインフレームが必要であり、移植は面倒でした。  
1983年、IBMは自社製品のソースコードの提供を停止し、「オブジェクトコードのみ」のポリシーを導入し、他のベンダーがそれに続きました。  
 2年後、MITのエンジニアであるRichard Stallmanは、Xeroxがプリンタードライバーのソースコードを提供しなかったため、新しいXeroxプリンターをローカルメンテナンスの取り決めに統合できなかったときに悩みました。  
 フリーソフトウェアとは、ユーザーがあらゆる目的で実行し、動作を調査して変更し、再配布できることを意味します。これには、改良されたバージョンや変更されたバージョンが含まれます。  
 FSFは、GPLライセンスソフトウェアを適用し、それを利用可能にするには誰もがソースを作成する必要があるという性質を持つGNU General Public License（GPL）を宣伝しました。製品登録を整理すると、マイクロソフトはドイツで販売されているOceのコピーの3分の1が偽造品であることを発見しました、そしてそれらをケンブリッジの私たちから数マイル先の小さな工場まで追跡しました。  
 彼らは彼らの製品を誇りに思っており、彼らの販売員は他のソフトウェア会社からCD複製ビジネスを得ようとするためにそれを使用しました。  
2。  
 1988年、カリフォルニア大学はUnixのBerkeleyディストリビューションを、制限の緩いBSDライセンスの下でリリースしました。これにより、誰もが目的を問わずソフトウェアを使用できるようになります。  
独自のソフトウェアベンダーは、彼らが採用するエンジニアによって書かれたコードの著作権を取得できます3。しかし、ボランティアによって維持されているプロジェクトはどうですか？オープンライセンスは、主張の矛盾を回避するのに役立ちます。  
 Linuxは1991年にGPLの下で最初にリリースされましたが、Berkeley UnixはFreeBSDおよびBSDライセンスの下で利用可能なその他のバリアントを生み出しました。  
 他のフリーソフトウェアライセンスはApacheや他のコミュニティのために開発され、パブリックライセンスはソフトウェアから他のクリエイティブアクティビティに急速に広まりました。たとえば、BSDのバリアントがWikipediaに適合されました。  
 伝統的なミュージシャンは時々新しい曲を作曲しますが、多くの場合、既存の曲を変更します。新しい作曲でさえ、既存の語彙からのフレーズを利用します。  
 小説家は古いストーリーとキャラクターのステレオタイプを再利用し、コメディアンは古いジョークをリサイクルします。  
 したがって、音楽会社はミュージシャンに伝統に従い、古いプレーヤーの最高の曲を採用するのではなく、完全に新しい曲をきれいな著作権で書くように迫るでしょう。  
 他の多くの数学者が他の結果で定理を使用する場合、数学者は有名になり、多くの人々が私たちのソフトウェアを使用する場合、コンピューター科学者は認識を得ます。  
 実際、1970年代以降、多くのコンピューター科学者がFTPサーバーを使用して、コードや出版物をオンラインで自由に利用できるようにしました。  
1994年には、いくつかの出版物が実際に影響を与えました。  
S  
 米国などの一部の国では、従業員が作成したプログラムの著作権を所有していますが、その他の国では、雇用契約でそれを解約する必要があります。請負業者もまた別の問題です。  
 書面による合意があることは本当に賢明です。  
2。  
 出版物が完全にオンラインになり、すべての論文をすべての人が読めるようになった場合、おそらく実際の数学に費やされる量が増える可能性があります。  
もう1つは、より有名なのは、Grateful Deadの作詞家でもあるEFFの創設者John PerryBarlowによる論文です。  
 インターネットが人々を国境を越えてファイルを交換することを可能にしたので、両方の物理的なコンテナのアイデア（本、CD）は管轄と同様に消えていました。  
彼は、情報化時代のきめ細かさと連携するビジネスモデルを開発するよう企業に求めました。  
 彼は他の業界がビットのバンドルを販売するよりもむしろライブパフォーマンスとサービスのモデルを探究することを提案しました[170]。  
 本、雑誌、音楽、および映画についての議論（これから間もなく戻る）とはまったく別のことですが、共有インフラストラクチャおよびツールの必要性の実現が高まっています。  
 たとえば、1994年にNetscapeが最初の人気のあるWebブラウザーを利用可能にした後、Microsoftは独自のブラウザーであるInternet ExplorerをWindowsで無料で提供することで殺し、サーバー側でInternetInformation Serverと呼ばれる製品で独占を確立しようとしました。 1995年。これは、MicrosoftがWebの初期の段階ではリンクの両端を制御できなかったため、賃貸料を引き出すための独自のものに変えることができなかったため、これまでに作成された最も重要なソフトウェアの1つでした。  
 （代わりに私たちは彼らと政策闘争をしているかもしれませんが、その間に多くの革新が起こりました。  
 一部の作家は自分の作品がだれでも使用できることに満足しているため、BSDスタイルのライセンスを選択します。他の人はセキュリティエンジニアリング746Ross Anderson24に彼らの仕事を望んでいます。  
 著作権はクローズドプロプライエタリ製品に組み込まれるのではなく、コモンズに留まるため、GPLを優先してください。学者は通常、クリエイターとして認められている限り、私たちのステューディを使用することを望んでいます。  
 たとえば、ユーザーが他のユーザーと作業を共有できるかどうかを指定できます。商用利用が許可されているかどうか。彼らがあなたに固有の属性を与えなければならないかどうか;彼らがそれに適応して構築できるかどうか、もしそうなら、彼らはオリジナルと同じライセンスの下で貢献を配布しなければならないかどうか。  
 実際、私の学術論文のほとんどはCCライセンスの下で利用可能であり、この本の出版社との私の合意は、原稿が出版のために送信されてから42か月後にすべての章をオンラインで自由に利用できるようにすることを指定しています。  
重要な進展は、1996年に米国のコミュニケーションズ品位法（CDA）のセクション230で発生しました。  
サービス会社は、侵害されていないコンテンツを、そのコンテンツが整理されていない場合は削除することになっています。実際には、境界を取り締まるのは難しく、インセンティブはひどいものです（セクション230が偽造者の広告を掲載するときにそれらを保護します[1830]）。  
したがって、ソフトウェアと人間の創造性を持つ他の製品の両方について、多くの代替ビジネスモデルがあります。  
 （この本がPDFファイルとしてフリーオンラインになったとしても、印刷された本の代金を支払う必要があります。  
 あなたはそれらを組み合わせることができます：あなたの無料の製品にはまって顧客を獲得し、それから彼らにもっとストレージまたは広告なしの体験を販売してください。  
2008年のこの本の第2版では、「ハリウッドの問題の解決策はビジネスモデルの変化にある」と提案しました。  
 ワーナーのハリウッドを率いたスタジオは、通常の金色のパラシュートなしで幹部を雇った。彼らはもはや宇宙のマスターではなく、彼らは電話会社のビデオ制作部門の従業員になっていました。  
 認知できる形で残る唯一のスタジオはDisneyで、サブスクリプションへの移行を早期に管理しました。おそらく、Steve Jobsを筆頭株主およびメインボードディレクターにしたことで、おそらく助けとなりました。  
5、しかし、今度はa Security Engineering747Ross Anderson24を取り上げましょう。  
 メディアコンテンツ保護の世界を巡るCOPYRIGHTquickの歴史ツアー。  
2。  
 小説の発明後、本の大衆市場が出現し、それを提供するために流通図書館が出現した。  
しかし、図書館は本の欲求を刺激し、読者の数は1850年までに500万人に増えました。  
 図書館運動は、印刷業者として最大の役割を果たし、マスマーケット向け書籍のまったく新しい市場を創出するのに役立ちました[1718]。  
 パガニーニは、人々が彼のバイオリン協奏曲をコピーして、リハーサルとパフォーマンスの直前にスコアを自分でオーケストラに配布し、その後それらを再び収集するのではないかと心配していました。  
）著作権収集社会は19世紀半ばから設立され、パリから始まりました。メンバーだった作曲家は、作曲を行うために会場やバンダに料金を請求します。  
 あなたはそれらにプレイリストを提出することができます、そしてあなたがあなた自身のすべての作曲を再生するならば、お金のいくらかは最終的にあなたに戻る方法を見つけるかもしれません。  
 自由文化運動と海賊党は、そのような不正を消去するために著作権を制限または廃止することを提唱しています。一部の欧州諸国では議会の議席を獲得しましたが、彼らは常に世界の舞台で著作権ロビイストによって打ち負かされているようです（この問題については、後でセクション24で返します）。  
1）。  
 技術的な対策も試みられました。  
 多くのレコードプレーヤーはスポイラートーンを拾うための帯域幅を持っていなかったため、実際には機能しませんでした。  
 カセットは、家庭用機器では音質が著しく悪いため、大きな問題ではないことがわかりました。人々は主に車で聴く音楽を録音するためにそれらを使用しました。オーディオを圧縮するためのMP3フォーマットのおかげで、オーディオのコピーは1990年代に再び主要な関心事になりました。  
 ただし、MP3はSecurity Engineering748Ross Anderson24を有効にします。  
 COPYRIGHT人はオーディオトラックを数メガバイトに圧縮し、ブロードバンドはこのサイズのファイルを簡単に共有できるようにします。  
業界の対応は、技術的な修正を推進することでした。  
 それは、デジタルパブリッシングに関する作業と、有料テレビやDVDを保護するために使用されるメカニズムに起源があるため、まずそれらを簡単に見てみましょう。  
2。  
 最初、ハリウッドは恐怖に陥り、ホームビューのために映画をリリースすることを拒否しました。  
 それからハリウッドは、本の出版社が図書館について行っていたのと同じように、ビデオレンタル店について偏執的になりました。  
 VCRとビデオカセットは、ロックスターのおもちゃではなく、大衆市場向け製品となり、2000年までに、事前録音されたカセットの販売がディズニーなどの企業の収入のほとんどを占めました。  
それまでに、世界の十代の若者たちの多くは、親がディズニーカセットのコレクションを自分の友達と同じように作成するように両親に要求しました。そのため、ビデオカセットの海賊は、パッケージをオリジナルのように見せなければなりませんでした。  
 オンライン登録が始まる前の大衆市場ソフトウェア、または今日の香水とスイスの時計と同様に、施行には、製品を購入し、偽造品を探し、サプライチェーンを追跡し、起訴するためのフィールドエージェントの派遣が含まれます。  
有料テレビの登場は、ケーブルまたは衛星のどちらで配信されようとも、ステーションオペレーターがさまざまな方法でチャネルの受信を制限できるようにする条件付きアクセスメカニズムの必要性を生み出しました。  
 ポルノチャンネルの運営者は、厳格な検閲法によりアイルランドなどの国での受信を防ぐ必要がありました。  
24。  
4。  
 1970年代から利用可能になった最初の世代のシステムは、ビデオ信号を時々反転させてセキュリティエンジニアリング749ロスアンダーソン24を妨害するなどのトリックを使用した粗雑なアナログデバイスでした。  
 同期をコピーし、スパイクを挿入してテレビの自動ゲイン制御を混乱させます。  
システムの第2世代は1980年代後半に登場し、アナログ技術とデジタル技術のハイブリッドを採用しました。放送はアナログでしたが、加入者制御はデジタルでした。  
 これには、デバイスのスクランブル解除が含まれます。•サブスクライバースマートカードはデバイスをパーソナライズし、セットトップボックスがデスクランブルできるプログラムを制御します。  
このアーキテクチャは、バルクビデオスクランブリングなどの複雑で高価なプロセスを、製品寿命が長い大量生産のカスタムチップで実行できる一方で、ハックを顧客に低価格で販売した後で変更が必要になる可能性があるキー管理機能を使用できることを意味します交換が簡単なコストトークン。  
基本的なメカニズムは、セットトップボックスが入力データストリームからECMをデコードし、カードに渡すことです。  
 次に、セットトップボックスはコントロールワードを使用して、ビデオストリームとオーディオストリームをデスクランブルします。  
24。  
4。  
 典型的なスキームは、Videocryptで使用されているカットアンドローテートアルゴリズムでした。  
1）：これには、ビデオ信号のアナログからデジタルへの変換、アバファーへの保存、回転後のデジタルからアナログへの変換が含まれていました。このプロセスは、1990年までに低コストのカスタムVLSIチップになりそうでした。  
セキュリティエンジニアリング750ロスアンダーソン24。  
 COPYRIGHTPlain-カットポイント-暗号-図24。  
 これは、1995年にMarkusKuhnによって最初に行われ、大学のスーパーコンピュータを使用してリアルタイムで行う必要がありました。  
図2は、暗号化されたビデオのフレームを示しています。図24は、  
 2000年までに、これをPCで実行できるようになりました[1824]。  
 ハイブリッドシステムは、開発途上国の一部のステーションでまだ使用されています。また、頻繁にキーを変更して海賊を不便にしています。その問題は、顧客が解読したときにキーを顧客に配布することです。  
 これらのデジタルシステムは同じ原理で動作します。暗号化ハードウェアを備えたセットトップボックスと、ECMからコンテンツキーを解読する個人キーを保持するスマートカードです。  
 現在のデジタルビデオ放送システムについては、次のセクションで説明します。  
 ただし、1995年以降の10年間にかなり決定的な攻撃を受けたため、彼らは教えるべき興味深い教訓をいくつか持っているので、間違ったことを簡単に説明します。2 –スクランブルされたビデオフレーム図24。  
2。  
2。  
3ハイブリッドスクランブルシステムでの攻撃コントロールワードのストリームを使用してブロードキャストビデオのスクランブルを解除できるセットトップボックスの数を考えると、次の問題は、有料の顧客だけがコントロールワードを取得できるようにすることでした。  
ただし、使用可能な帯域幅は通常、1秒あたり約10 ECMでした。  
お客様のスマートカードがECMを解釈します。  
 カードを改ざん防止できる場合、準拠したデバイスのみがマスターキーKにアクセスでき、必要に応じて自殺する必要があります。  
 スマートカードから送信されるコントロールワードは、現在プログラムを解読しているすべてのセットトップボックスで同じであるため、スマートカードとセットトップボックスの間にPCを置いてオンラインで投稿することにより、1人の人がコントロールワードのストリームを記録できます。  
 サーバーはこのキーログ攻撃で急増しましたが、業界にとってはわずかな迷惑でした。多くの視聴者は、PCをセットトップボックスに接続するための特別なアダプタを購入または構築する準備ができていました。  
暗号解読もいくつかの機会を与えました。  
 Eurocryptシステムには、31と29の長さの2つの線形フィードバックシフトレジスタがあり、長い線形シーケンスを生成します。  
 出力の連続する各バイトは、スクランブラーの制御バイトになります（図24。  
線形フィードバックシフトレジスタ1 ###（アドレス）マルチプレクサー！ output（select） "" "" "Security Engineering752Ross Anderson24。  
 COPYRIGHT線形フィードバックシフトレジスタ2図24。  
 しかし、暗号にはショートカット攻撃があることが判明しました。  
 （私は1985年にこの攻撃を発見し、それが暗号に興味を持った理由です。  
 したがって、暗号解読を使用して後者を再構築できます。  
おそらく、「アマチュア」攻撃の中で最も強力なものは、マスターキーリークを悪用したものです。中古PCを購入し、好奇心からハードディスクを調べ、有料TVオペレーター1人の完全な加入者管理システムの削除を取り消した人、埋め込まれたマスターキーを含みます。  
とにかく、商業海賊は、マイクロプロービング技術を使用してスマートカードをリバースエンジニアリングすることになりました。  
ただし、ハードウェアの修正は新しいカードの問題に限定されており、オペレーターは新しいカードを1年に1回以上発行することを望んでいません。これは、加入者あたり数ドルの費用がかかり、サブスクリプションは通常月額20ドル未満でした。  
訴訟は1つのルートでしたが、時間がかかりました。  
 業界のロビー活動の筋肉は、ダブリンを無効にするためにヨーロッパの法律で導入するために配備されましたが、これには数年かかりました。  
したがって、1990年代半ばまで、海賊とオペレーターは技術的対策と対策の戦争に従事していました。  
 オペレーターはいくつかを購入して分析し、失敗させるトリックを開発しました。  
 それらのより効果的なものの1つは、パケットの内容がスマートカードによってコードとして実行されたECMでした。このようにして、既存のカードベースをその場でアップグレードし、正規のカードと海賊版カードの実装の違いを利用できます。  
2。  
5：–バイナリー取り消しツリーをMACアルゴリズムにフィードして、海賊カードが無効なコントロールワードを配信するようにします。  
 各加入者スマートカードには、加入者鍵kiが含まれ、加入者鍵を現在アクティブなマスター鍵KMにリンクする中間グループ鍵KGijのバイナリツリーがあります。  
5。  
 最初のパケットは{K0M} KG12で、加入者の半分が一度にK0Mを計算できるようにします。次に、KG11の更新バージョンで暗号化されたaK0Mがあります。{K0M} KG011;次に、この新しいグループキーKG011がGK22で暗号化されます。等々。  
 もちろん、これは完全な解決策ではありません。複数の加入者キーを含む海賊カードを処理する方法と、海賊カードに侵入する手間をかけずに漏洩したキーを特定する方法についても考える必要があります。  
心理学的測定値も使用されました。  
経済的要因も、ここと同様に重要です。  
3か月後に9％の偽造。  
2。  
経済学の理解は、あなたが彼のプラグを抜く前に海賊に実質的なユーザーベースを構築させることが最善であると教えています、これは彼に彼の競争相手を拭く時間を与え、そして彼が確立されたら彼のカードを切り替えると彼の信用をさらに破壊します即時の応答よりも潜在的な顧客。有料テレビ業界は、セキュリティの回復を事前に計画し、最初は使用されなかったが後でアクティブ化できる機能を非表示にすることを学びました5。  
 攻撃者はプロービングステーションでアルゴリズムを読み取るだけでなく、チップ内の数千のゲートをリバースエンジニアリングする必要があったため、攻撃を行うための技術的能力を備えたラボの数を数に減らしました。  
 テントの外に残った人たちは見守られました。  
 業界は、主要な商業用海賊を追い詰め、刑務所に入れられたか、訴訟で溺死させたかにかかわらず、彼らを廃業させました。  
彼は偽造カードが違法ではなかったアイルランドのフロント会社を通して偽造品を販売しました[1368]。  
 イギリス当局は起訴するつもりはなかったため、スカイは私訴を起こし、有罪判決を受けました。  
 それから彼は適切な刑務所に行きました。  
24。  
4。  
 規格は非常に複雑で、IPTVと地上デジタルTV、衛星TV、および無料放送サービスと有料TVに関連しています。  
 最新の標準であるDVB-T2は、2009年にETSIによって公布されました。  
 DVBの条件付きアクセスメカニズムはハイブリッドシステムに似ています。コンテンツは、セクション16で説明したen-5Weです。  
1紙幣印刷業者が何年も前に、必要に応じて一度に1つずつ開示できる一連のセキュリティ印刷機能を組み込むことを学んだ方法。  
2。  
 暗号化にはDVB CommonScrambling Algorithmを使用します。これはNDAでのみ利用可能でしたが、2002年に漏洩しました。  
 スマートカードは標準化されていないため（インターフェイスレベルを除く）、各ブロードキャスターは自分のお気に入りの暗号トリックとサプライヤを使用できます。これまでの海賊行為は、スマートカードのクローン作成に関係しているようであり、有料テレビ事業者がお互いにハッキングを非難したさまざまな訴訟が行われています。  
 それを取り除いたのはNet ﬂ ix、より一般的にはブロードバンドに基づくオンラインサブスクリプションサービスへの移行でした。  
2。  
家庭用電化製品業界は、1996年にデジタルビデオディスク（DVD）を導入しました。  
 そのため、コンテンツスクランブルシステム（CSS）と呼ばれるメカニズムが土壇場で組み込まれました。これに関する議論はDVDの発売を遅らせ、それは急いで設計されました。  
）DVDにはリージョンコーディングがありました：ディスクは、物理的なフィルムプリントの制作コストを最小限に抑えるために、最初にアメリカで、次にヨーロッパで映画をリリースするという伝統的な慣習をサポートするために、指定されたリージョンリストからのプレーヤーでのみ実行されるはずでした、そして映画が爆撃された場合の金銭的損失。  
 したがって、すべてのDVDベンダーは、2番目に安全性の低いプレーヤーを市場に出したいと考えていました。彼らはハリウッドが猛威を振るっている企業になりたくはありませんでしたが、見込み客にプレーヤーのリージョンコーディングがハッキングされる可能性があることを確信してもらいたかったのです。  
 キーの長さが40ビットであるため、機器は米国の輸出規制に違反しませんが、設計は非常に貧弱で、有効なキーの長さはわずか16ビットでした。  
 Industrylawyersはそれをオンラインにした人々に対して差止命令を得ましたが、これらは検閲であると見なされたため、米国外のWebサイト、Tシャツ、歌、および伝統的に憲法保護を享受する他の形式のスピーチで表示され始めました6。  
 彼らの弁護士は、政府を説得して、失敗しました6CSSの完全な説明とこの本の第1版と第2版でそれを破る方法がありました。 DVDが恐竜の道を進んでいるので、私はこの版のためにそれを落としました。  
3。  
 彼は2003年に控訴で無罪となった。  
 DVDコンソーシアムは、リバースエンジニアリングが困難になるように、コードを難読化するためにDVDプレーヤーソフトウェアを作成する人々を必要としました。  
 しかし、このクローズドアプローチは、何百万人もの人々がすでに使用しているオープンソースのPCオペレーティングシステムであるLinuxと衝突しました。  
そのため、CDドライブを搭載したPCが店頭でDVDドライブを搭載したPCに取り替えられ始めたため、LinuxユーザーコミュニティはCSSを壊すか、Windowsを支持してLinuxを使用することを諦めなければなりませんでした。  
とにかく、DVDは通常のパターンに従いました。ハリウッドは驚いて、彼らの最高の映画をリリースすることを拒否しました。コピーを防止するために講じられた技術的措置。その後、訴訟。もちろんコピーはありますが、まだ完全なものではありません。DSLモデムでさえ4Gb DVDムービーを友人に送信するのに数時間かかり、PCのディスク容量も問題です。  
その後、2007年にHD-DVDとBlu-Rayの間でフォーマット戦争が発生し、より短い波長のレーザーを使用して情報をより高密度にエンコードし、最大50Gbのディスクあたり50Gbを提供する、より高密度の光学メディアを売り込む試みがありました。  
 ただし、Blu-Rayを完全に実装したのはPlaystation 3だけで、HD-DVDが本当の牽引力を得ることはありませんでした。  
24。  
 これにより、DRMメカニズムが実際の所有権を反映できるようになったため、私はあなたに写真を売ることができ、レシートを受け取ったらそれを復号化することができます。さらに、それを誰かに渡すと、それがなくなってしまいます。  
 元のアプリケーションには、科学雑誌からの新聞や記事の配布が含まれていました[315]7。InterTrustの特許は、20世紀のコンピュータ関連の特許が4つしかなかったため、9桁の金額が変更され、その他はハーバード仮想メモリの特許でした。 RSA公開鍵特許およびフラウンホーファーMP3特許。  
3。  
基本的な問題は、汎用コンピュータであるPCが原理的に任意のファイルをコピーし、それを他の任意のコンピュータに送信できることです。アナログコピーとは異なり、コピーは完璧なので、1つのオリジナルから何百万ものコピーが作成される可能性があります。  
 音楽業界は、無制限のコピーはビジネスを破壊すると信じていました。コンピュータ業界は、DRMは本質的に汎用コンピュータでは不可能であるため、新しいビジネスモデルを採用するほうがよいと彼らに言いました。  
 その結果、DRMが強く求められました。  
3。  
 MP3プレーヤーのサポートからカラオケの歌詞の同期まで、さまざまな機能で、音楽の再生、ビデオの視聴、写真の表示が可能になりました。  
デジタルメディアを販売するストアは、コンテンツキーを使用して各アイテムを暗号化し、暗号化されたファイルをWebサイトにリンクされたストリーミングメディアサーバーに配置します。  
 ライセンスはライセンスサーバーによって生成され、お客様のWMPアプリケーションによって生成された公開キーを使用して暗号化されます。  
このアーキテクチャは有料音楽の条件付きアクセスに似ています。音楽またはビデオを保護する一括暗号化タスクは、個人に合わせたキー管理タスクから分離されているため、顧客ごとにビデオを新たに暗号化する必要はありません。  
IBX内部は時々リバースエンジニアリングされました[1693]。  
 セクション6で説明しました。  
5 2000年代の初めに、Microsoft、Intel、その他の大手企業がTrusted Computing Groupを形成して、DRMをセキュリティエンジニアリング758Ross Anderson24に適切に構築しようとした。  
 汎用コンピュータのDRMのPCアーキテクチャ。  
マイクロソフトは、DRMを一般ユーザーに拡張することを目的としたWindows Server 2003でInformation Rights Management（IRM）を発表しました。アイデアは、ドキュメントまたは他のデジタルオブジェクトへのアクセス制御がその作成者によって保持されるというものでした。  
 これは、Windowsエコシステム全体のTrusted ComputingMechanismsによってサポートされ、LinuxやGoogleドキュメントなどからの課題に対してエコシステムを便利に強化するというビジョンでした。  
 現在、このような分散使用制御をO�ce365やGmailなどのクラウドベースのシステムに実装することは簡単ですが、そのようなエコシステム全体で作業することは困難です。そのため、Trusted Computingが機能するようになっていた場所からそれほど遠くないところまで到達しました。  
 WMPは、ストリーミングメディアサービスの提供、音楽サブスクリプションサービスのサポート、MLBなどの地理的にリンクされたサービスの提供に最も基本的に使用されます。  
24。  
2Fairplay、HTML5、およびその他のDRMシステムMicrosoftの提供は、権利管理システムのかなり典型的なものでした。  
 曲を購入すると、ランダムなセッションキーで暗号化されたマスターキーと、iTunesプレーヤーのRSA公開キーで暗号化されたセッションキーが顧客に送信されます。  
 Windowsと同様に、保護されたコンテンツのロックを解除する多くのプログラムが時々登場し、AppleがiTunesをアップグレードしました。  
一部の企業の権利管理システムは実に虐待的であり、2005年にソニーのXCPシステムで特に極端な事例が発生しました。マイクロソフトはそれをマルウェアとして分類し、Windows DefenderとMaliciousSoftware削除ツール[1307]によって削除しました。  
2012–14年には、World Wide WebConsortium（W3C）がブラウザでサンドボックスを提供するHTML5を採用してDRMを備えたマルチメディアコンテンツをサポートするかどうか、およびサンドボックス内のソフトウェアの手段としてEncryptedMedia Extensions（EME）を採用するかどうかについて、大きな論争がありました。オンラインライセンスマネージャーと通信します。  
3。  
 2017年以降、ブラウザはNet ﬂ ixなどのサービスをサポートするためにGoogleの「Widevine」DRMソフトウェアのライセンスを取得する必要があります。  
 2020年に、Googleはこの技術のオープンソースブラウザへの提供を停止しました。それ以降は、すべての新しいブラウザが独自仕様である必要があります。これは、2012–4年の討論中にEFFによって予測されていました[571]。  
 Microsoftが運営するDRMがFISA令状で武装したFBIagentがMicrosoftクラウド上のデータにアクセスできないようにするかどうかは興味深い問題です。 nextSnowdenが出たときだけ答えがわかると思います。  
3。  
 逆アセンブラーを使用していて、そのようなトリックを無効にするために時間を費やしている子供たちは、可能な場合、企業はいくつかの重要な機能をクラウド、信頼できるハードウェア、またはその両方に移動します。  
 セクション12で説明したように。  
4、これは、マルウェアによってルート化またはジェイルブレイクされた可能性のある電話上のアプリを保護するために一部のモバイルアプリ開発者が使用する一連の手法です。  
 そして、ヨーロッパ中央銀行からの委任を受けて、RASPはヨーロッパのバンキングアプリ、またはそれらが依存する認証アプリの必須となっています。  
 これは、Windows Media Playerなどの1990年代製品の脅威モデルでもありました。  
 セクション24で説明したように、これらは正しく壊れていました。  
セクション6で説明したように、以前は5でしたが、IntelをTrusted Computingに、最終的にはSGXに移行するように導きました。  
1。  
 ただし、他の不可能性がマルウェア検出のセキュリティなどのセキュリティをもたらすのと同様に、完全な難読化が理論的に不可能であるとしても、実用的な難読化が目的によっては十分であるかどうかという疑問が生じます。  
3。  
マルウェアの作成者も同様の傾向を示しました。  
3。  
 キーサンドヘッダーはすべて異なるため、マルウェアの認識が難しくなります。  
 ただし、そうではない場合がほとんどです。セールスベンダーからのRASPを購入する素朴な企業は、最悪の事態を予想する必要があります。  
 それにもかかわらず、難読化に取り組んでいる小さな研究コミュニティがあり、2020年の認証または復号化のためのエンジンを保護するときの最先端の技術は、奇数の命令セットを持つ仮想マシンを実装することです。この仮想マシンに暗号を実装し、さらに仮想を難読化します。マシン自体（カスタムオペコードは、1990年代のSky-TVスマートカードですでに使用されていました）。  
 RASPtesterが2週間試行しても暗号キーを抽出できない場合、1か月間試行する誰かに対して保証はありません8。  
誰かがこれについて本当のコツを習得しますが、コンプライアンステストラボでは機能しない可能性があります。したがって、レモン市場が期待されます。  
 一部のツールは、Javaバイトコードを縮小および最適化するときに難読化します。その1つであるProGuardは、Android SDKの一部として配布されます。  
24。  
4ゲーム、チート、DRMGamesは、すべての最初のアプリケーションの1つでした–世界で最初の適切なコンピューターであるEDSACが動作可能になるとすぐに、研究生がゲームを作成しました。  
彼らは1970年代のホームコンピューターブームを引き起こし、その結果、PC業界が生まれました。ゲームコンソールは、マイクロプロセッサとメモリチップの巨大な市場でした。また、ゲームは、コンソールでもPCでも、コンピュータグラフィックスの開発を大きく推進してきました[2056]。  
8傷跡は個人的に負担します。  
 ちょうど途中までたどり着いたので、同社は顧客に「ケンブリッジはこれを壊すことができなかった」と自慢しました。  
セキュリティエンジニアリング761ロスアンダーソン24。  
 汎用コンピューターのDRM任天堂がコンソールゲームを家庭に移したとき、彼らはソフトウェアカートリッジや他のアドオンの販売からコンソールに助成金を支給したため、後で説明するように、使用できるアクセサリーの制御に多くの努力が費やされました。 24。  
ただし、オンラインコンピュータゲームへの移行により、これらの懸念は緩和されました。ゲーマーが不正行為を行う方法は非常に多くあります[2057]。  
 現実の世界では、不正行為の申し立ては、結果が正直なプレーで期待できたものよりも優れているかどうかについての見解を持つ経験豊富なプレーヤーの陪審によって聞かれます。  
 オンラインプレイは、統計分析のためのオンラインレコード、多くのプレイヤーが同じカードを使用するオンライントーナメント、および1つではなく多くのパートナーとプレイする新しい形式のプレイがあるので役立ちます。  
 セクション8で説明します。  
8、これらは現在、2020年に、DDoS for-for-hireサービスの最大の市場です。  
3番目のタイプの不正行為は、コンピュータゲームの性質から生まれたものです。  
しかし、ゲームの物理モデルには常に欠点があり、ネットワークレイテンシや、ゲームデザイナーがそれに対処するために使用する最適化によってしばしば導入されます。  
 しかし、多くのゲームクライアントで使用される予測アルゴリズムは近くのプレーヤーに関する情報をキャッシュするため、角を曲がって敵を確認して撃つと、ネットワーク接続が遅いほど、彼があなたに会って反応するまでの時間が長くなります。  
 それ自体は不正行為ではないかもしれませんが、近年、プレイヤーはネットワーク接続を意図的に操作して、他のプレイヤーを遅らせるための着信パケット、または他のプレイヤーが何をしようとしているのかを確認するための発信パケットなど、人工的な遅延を作成しています。  
 人々は、着信ネットワークパケットを傍受し、悪意のある人物を特定し、発信ショットを調べるプロキシを介して、ファイアボタンを繰り返しクリックする単純なルーチン（物理的に発砲できるレートが要因であるゲームをハックする）から、さまざまなツールを作成しました、そして彼らの目的を最適化します。  
 プロキシとしてパケットストリーム、グラフィックスカード、またはクライアントコードにフックできます。  
3。  
 ファーストパーソンシューティングゲームは通常、生の位置情報をゲーム内のすべてのプレーヤーに送信し、ローカルの物理モデルに従ってレンダリングするクライアントソフトウェアに任せているため、このようなハッキングが可能です。  
 PunkbusterなどのGuardソフトウェアは、2000年から使用されており、ウイルス対策技術を使用して、ゲームコードまたはそれが依存するドライバーにフックする試みを検出しています。  
 上記のセクションで説明したように、これは絶え間ない戦いであり、人工ラグなどの一部の手法は完全に処理することが困難です。  
 サーバーはまた、プロの橋トーナメントのように、イベント後の不正行為を検出するための分析機能を備えています。  
3。  
 人々がコンピュータとブロードバンド接続にCDドライブを持っていると、お気に入りのコピーをコピーして共有できます。  
 法的措置を招くファイルを中央に保管するのではなく、Napsterはインデックスを提供して、特定のトラックを探している誰かが他に誰がそれを持っているのかを見つけ、共有株取引の準備ができているようにしました。  
 その後、GnutellaやFreenetなどのシステムは、検閲耐性システムの世界からアイデアを取り入れて、法的攻撃によって閉鎖される可能性のある中央ノードなしでネットワークをセットアップしました[439]。  
私は初期の検閲耐性システムであるEternity Ser-viceの設計者でした。  
ペネ。  
事件の主題となったメッセージには、教会の元首相による、メンバーが完全に開始された後、人類の残りの部分が誤った意識に苦しんでいると伝えられたというダビットが含まれていた;実際には、イエスは悪者であり、ルシファーは善人でした。  
3。  
 彼らは多くの管轄区域でこの議論を回避し、最終的にオランダの裁判所はNGOに「フィッシュマンアダビット」と呼ばれるように発行することを許可することでそれを阻止しました。  
 これの新しいバージョンはPublius9で、検閲に耐性のある匿名の公開メカニズムを提供していました[1974]。  
 裁判所の命令により閉鎖できるサーバーがないことは、音楽業界の執行者にとって興味深い問題です。  
ピアツーピアシステムを攻撃する1つの方法は、変更されたピアを導入し、他の可能な限り多くのピアに接続して、それらを識別することにより、「ネットワークを歩く」ことです。  
 多くの場合、人々は訴訟を起こすのではなく、中止して辞任し、小さなペナルティを支払うことに同意しました。 2007年10月にミネソタ州ダルースの連邦陪審。音楽業界で働いている企業も、損傷した音楽ファイルをスパム送信システムにアップロードしており（通常は合法です）、サービス拒否攻撃も行っていることが疑われました（多くの法域ではそうではありません）。  
Media Defenderのビジネスモデルは、15のP2Pネットワークの1,200万人のユーザーに対する攻撃を含む「保護」のために、アルバムごとに月額4,000ドル、トラックごとに月額2,000ドルを請求することが判明しました[1501]。  
 Comcastは、ケーブルネットワーク経由でTVを視聴することを顧客に好む可能性があるため、広告が表示されますが、申し立てが真実である場合、公共政策の問題が提起されます。  
 これは、何よりも地方の手続き法の機能であると思われます。多くの国では、弁護士は曲がったり、少なくとも米国では読めない9。米国以外の読者の場合：革命家のアレクサンダーハミルトン、ジョンジェイ、およびジェームズマディソンは、連邦紙のコレクションを書いたときに、ペンブリウスというペン名を使用した。 1787–8年にニューヨーク州の新聞に掲載された85の記事は、ニューヨーク州の有権者に米国憲法を批准するよう説得するのに役立ちました。  
3。  
大規模なグローバルエコシステムでは、大きなサービス企業が主流になり、著作権侵害の決定要因は、米国DMCAの下で設定された通知と削除の体制であり、他の場所でも同様の法律が続いています。  
5。  
3。  
 Armのような企業は、アプリケーション固有の集積回路（ASIC）を設計する場合でも、フィールドプログラマブルゲートアレイ（FPGA）を使用する場合でも、カスタムチップを製造する企業にプロセッサやその他のコンポーネントの設計をライセンスすることで生計を立てています。  
 Acamera社は、FPGAにロードされたビットストリームに統合する回路のライセンスを取得し、それが中国の工場で製造した新しいカメラの主要コンポーネントになります。  
 失敗のモードは2つあります。カメラ会社が追加の製品を注文してIP所有者に嘘をついた可能性があります。または、中国の工場がカメラ会社をだましている可能性があります。  
今では、製造後にシリアル番号などを使用して各カメラをパーソナライズするなど、カメラ会社が工場の不正行為を阻止するために使用できる技術的メカニズムがありますが、これによりIP所有者の不正行為が困難になる可能性があります。  
 カメラ会社は、あるモデルのプロセッサまたはフィルターのライセンスを取得し、それを宣言せずに別の安価なモデルに組み込むこともできます。  
 また、FPGAの販売も抑制します。FPGAの製造元は、暗号化されたビットストリームと更新をチップ全体に配布することによって最初の問題に対処するメカニズムを提供します。2番目の問題は、チップ設計ツールが信頼境界内にあるため、より困難です。  
 科学捜査のためのサイドチャネルの使用がいくつかあります。  
 コンポーネントは、電力トレースで適切な信号を生成するように意図的に設計することもできます。  
）これにより、著作権表示の問題が発生します。  
4。  
4Information HidingHollywoodは、1990年代半ばに著作権を保護するための新しいメカニズムを見つけることに関心を示し、軍が邪魔にならない通信に関心を示し、政府の暗号化を制御することへの関心が高まり、情報隠蔽の分野で急速な発展を遂げ始めました。  
ハリウッドは、控えめにデジタルオーディオ、ビデオ、アートワークに埋め込まれた著作権マークの救済を求めました。  
 たとえば、AppleのiTunesミュージックストアからMP3をダウンロードした場合、MP3にはあなたを特定するオーディオに埋め込まれた指紋が含まれていました。  
 （一部の人々は、正直な購入者が作成した法的ハザードのため、指紋が全体的に売上を押し下げたと信じていました。  
）プライバシーの関心はステガノグラフィにあり、その目的はメッセージがカバーメディアに埋め込まれ、その存在自体が検出されないままになることです。  
 アリスとボブは刑務所におり、脱出計画を孵化したいと思っています。彼らのすべての通信は、監視員、ウィリーを通過します。ウィリーが暗号化されたメッセージを検出した場合、彼はそれらを孤独な監禁に投げ込むことによって彼らの計画を挫折させます。  
暗号化の関連分野と同様に、使用されているメカニズムは監視員に知られていると想定しているため、セキュリティは、アリスとボブが何らかの方法で共有した秘密鍵のみに依存する必要があります[1753]。まず、ステガノグラフィがインターセプトの可能性が低い通信であると見なされている場合、著作権マーキングは妨害耐性のある通信に似ています。これはほとんど同じ方法を使用できますが、集中的な攻撃に抵抗するために、ビットレートがはるかに低くなる可能性があります。  
 第2に、もともと電子戦のために開発された直接シーケンススペクトラム拡散などの技術は、情報隠蔽コミュニティで使用されています。  
 一部のテレビ局は、画像の隅に目に見えるが目立たない方法でロゴを埋め込んでおり、私が指摘したように、学術誌のダウンロードでも同様のことが行われます。  
24。  
1透かしとコピー生成管理DVDコンソーシアムは、デジタルビデオまたはオーディオをアナログ形式にデコードしてから再配布できることを懸念しました（いわゆる「アナログホール」）。  
 アイデアは、ビデオまたは音楽トラックがセキュリティエンジニアリング766Ross Anderson24であるかもしれないということでした。  
 情報の非表示、または「決してコピーしない」、または「一度だけコピーする」とマークされている;準拠したプレーヤーは、「コピー禁止」とマークされたビデオを録画しません。「コピー1回のみ」とマークされたビデオを録画すると、マークが「コピー禁止」に変更されます。  
このようにして、消費者が利用できるDVDプレーヤーは、ホームビデオの無制限のコピーとテレビ番組のタイムシフトされた視聴を可能にしますが、商業的著作権侵害のために簡単に悪用されることはありません。  
 各ディスクについて、ランダムな番号であるチケットXに加えて、コピー制御情報に加えて、リードイントラックのウォブルなどの物理メディアに固有の情報を選択します。  
 隠し著作権マークとしてビデオにh（h（X））を埋め込みます。  
準拠デバイスは、Xが指定されている場合のみマークされたトラックを記録します。この場合、h（X）のみが新しいディスクに書き込まれます。  
これは最終的にはBlu-rayになりましたが、市場では失敗し、開発者が作業するのにまったく苦労しました。  
 マーキングメカニズムでアラームレートの低下を見逃すだけでは不十分です。低い誤警報率も必要です[1318]。  
 では、どのような種類のマークが可能であり、偽造、なりすまし、およびその他の攻撃に対してどの程度堅牢か？24。  
2一般的な情報隠蔽手法情報隠蔽は、暗号学よりもさらに遡って、そのルーツを詐称しています。  
 フランシス・ベーコンは、2種類の異なるフォントを交互に使用することにより、1文書につき1ビットで2進数のメッセージを埋め込むシステムを提案しました[1513]。  
 軍事および諜報機関は、トラフィックのセキュリティがコンテンツの機密性よりも重要である場合が多いことを強く認識しており、スパイが使用するマイクロドットから低確率の傍受無線まで、あらゆる種類のテクノロジーを使用しています。  
 著作権マーク、またはステガノグラフィーの場合、埋め込まれたテキストは、マークされたテキストを生成するカバーテキスト、またはステガノグラフィーの場合、ステゴテキストに隠されています。  
4。  
 ここで、「テキスト」という単語は、「オーディオ」、「ビデオ」などに適宜置き換えることができます。  
•多くの人々は、オーディオまたはビデオ信号の最下位ビットにマークまたは秘密のメッセージを隠すことを提案しています。  
 また、非可逆圧縮技術によって深刻な損傷を受けています。  
 これは古典的な中国で最初に発明されました。  
 送信者は空白の紙の上にマスクを置き、穴にメッセージを書き、それを削除して、秘密の埋め込みメッセージの文字を含むカバーメッセージを作成します。  
•これの最新バージョンは、マークをに隠します。  
秘密鍵は、適切な数のピクセルを選択するキーストリームに拡張されます。  
 実際には、画像内の非常に多数のピクセルでさえ、目に見える影響なしに、パレット内の同様のピクセルの色に変更することができます[972]。  
 カバー画像と埋め込み方法が、ピクセルの1％を安全に微調整できるような場合に、より良い結果が得られます。  
 これらは、エラー修正コードを使用して回復できます。  
 紙幣マーキングのために提案されたシステム、パッチワークは反復コードを使用します。キーはピクセルの2つのサブセットを選択します。一方は明度を上げることでマークされ、もう一方は明度を下げることでマークされます。  
 これは、差分電力分析を連想させます。キーテルは、入力データを2つの山に分類する方法を示し、キーが正しかった場合、それらは著しく異なっています。したがって、一般的な手法は、電子戦[1890]から借用した直接シーケンススペクトラム拡散技術を使用することです。  
セキュリティエンジニアリング768ロスアンダーソン24。  
 情報の隠蔽•スペクトラム拡散符号化は、変換空間で行われることが多く、その影響を知覚しにくくし、一般的な形式の圧縮に対してより強固にします。  
•一部の方式は、テキスト行を上下に3分の1インチ移動することにより印刷媒体にマークを付ける方式[315]や、知覚のしきい値[225]未満で音楽に余分なエコーを追加する方式など、特定の媒体の特性を使用します。  
著作権マーキングの進歩は1990年代後半に非常に急速でした。あるシステムが紙幣やAdobeなどのツールで採用されるまで、人々は他の人々が破ったマーキングスキームを発明しました。  
24。  
3著作権マーキングスキームへの攻撃この本を通して、暗号化システムに時々暗号解読を伴う攻撃が見られましたが、多くの場合、誤った仮定、間違ったものの保護、プロトコルの失敗、実装のバグに依存していました。  
 著作権表示はどちらの点でも違いはありません。  
しかし、これは問題ではありません。  
•いつものように、多くの設計者はKerckhoの原則を無視しました。システムのセキュリティは、使用中のアルゴリズムではなく、キーの選択にあるべきであるということです。  
•たとえば、米国で販売されているカラーコピー機は、通貨偽造者を検出する追加の手段として、コピーのビットパターンにMachine IdentificationCode（MIC）を隠しています[2002]。  
 セキュリティエンジニアリング769ロスアンダーソン24。  
 その後、情報隠蔽メカニズムは、EFFが主導するクラウドソースのエフォートでリバースエンジニアリングされました。  
人間の目にはほとんど見えず、A4カラーコピーで約150回繰り返される直径1mm。  
•多くのマークは、信号にノイズを追加するだけです。  
 または、いくつかの既知のコンテンツをマーキングシステムに提供し、その入力と出力を比較します。  
•たとえば、誰でも1つのプリンシパルだけが検出できるマークを挿入したり、1つのプリンシパルだけが挿入できたマークを検出したりできるように、公開キー暗号化と同等のマーキングを開発する試みがありました。  
 後者はもっと難しいようです。  
 第2に、上位ビットまたは顕著な機能だけを認証しようとすると、堅牢性の問題があります。マークを検出するデバイスが与えられた場合、攻撃者は、デコーダーがそれを見つけられなくなるまで、画像に小さな変更を加えることでマークを削除できます[1511 、1168]、独自の署名を適用します。  
•ステガナリシス技術は、ほとんどの埋め込みスキームを打破するために開発されました。  
 最も巧妙な攻撃チームは、ジェシカ・フリドリッチとビンガムトンの彼女の学生でした。ステガノグラフィーに関する彼女の本は、この主題に関する真剣な研究の出発点です[724]。  
 彼らは、画像の所有者が目に見えない指紋を埋め込むためのツールを提供し、マークされた画像を探してWebをクロールし、著作権所有者に報告するボットを持っていました。  
 たとえば、マークされた画像は、Webページにレンダリングされたときに元の画像と同じように見えるが、著作権マークが検出されない小さな画像に切り取られることがよくあります（図24。  
 Digimarcはしばらくの間、ブロードキャストストリームの監視に取り組みました。しかし、時間が経つにつれてAIは改善され、ソフトウェアはどの曲が直接再生されているかを識別できるようになりました。  
 たとえば、ユーロ紙幣のSecurity Engineering770Ross Anderson24にあります。  
 情報の隠蔽図24。  
ジェット写真。  
PhotoshopやPaintshop Pronowなどのソフトウェアパッケージは、マークされた画像の処理を拒否します。  
•知覚できない著作権マーキングスキームに対する最も一般的な攻撃は、適切に選択された歪みを伴います。  
 画像については、学生が開発したStirmarkと呼ばれるツールが、高品質プリンターで印刷してから高品質スキャナーで再度スキャンするのと同じ種類のエラーを画像に導入します。  
著作権マーキングスキームに対する攻撃の詳細については、[724]を参照してください。  
おそらく、著作権マーキングを殺した主な技術的要因は、攻撃ではなく遅延でした。  
 最近、メディアストリーミング標準（DASH、HLS）が更新され、メディアチャンクを完全に記述してから修正する前に、メディアチャンクをダウンロードできるようになりました。これは、代わりに著作権を侵害するコンテンツの直接認識の採用を促進するのに役立ちました。  
5。  
 著作権者は、広告収入の一部を獲得することで動画を収益化するか、ブロックするかを選択できます。  
24。  
 この反応には、アメリカのDigitalMillennium Copyright Act（DMCA）による著作権期間の延長からヨーロッパのIP施行指令への一連の法律が含まれており、技術などの多くの人々が脅迫していると感じた方法で権力をシフトしました。  
 これは、ヨーロッパではなく米国の情報サービス企業の成長を支持した。  
加入者が異議申し立て通知を提出し、著作権所有者の訴訟が起こらない限り14日以内に手続きを戻すようにする規定（「通知と差し戻し」）もありますが、実際には多くのISPが訴訟に関与するのではなく、顧客のサービス。  
Googleへの削除リクエストの半分以上は、上位16の著作権所有者からのものであり、上位3は年間10億以上を生み出しています。それらの多くはGoogleにないリンクにリンクしています。  
これは実際にポリシーに影響を与えます。Nikeになりすましている中国のショップを検閲することと、白人の至上主義者からの苦情に応じてBlack Lives Matter Peckhamを検閲することは別です。  
 たとえば、キッチンを拡張するための計画許可を申請したとき、私は現地の計画の4つのコピーを提出しなければなりませんでした; 10「知的財産」という用語は議論の余地があります。  
セキュリティエンジニアリング772ロスアンダーソン24。  
 ポリシーしかし、私たちの大学図書館の地図ソフトウェアでは、3部しか印刷できません。  
 法的規制はアクセス制御によって補足され、DMCAおよび同等のEU法によってこれらのアクセス制御に与えられる法的特権は、法学者によって「パラ著作権」[532]と呼ばれる新しい権利の束を作成します。  
その結果、著作権ユーザーの権利が侵害されました。  
これは、書籍の物理的なコピーを所有することと電子書籍を「所有すること」の間の大きなギャップを冷静に思い出させるものでした。実際、あなたはライセンスを書いたベンダーからライセンスを購入して、まったく権利をまったく与えないようにしました。  
 かつてはパブリッシャーなどの専門家の関心事でしたが、今では音楽をダウンロードしたり、タイムシフトムービーをダウンロードしたり、個人のWebページを維持したりするすべての人の生活に影響を与えています。  
 たとえば英国では、携帯電話で聴くためにCDをリッピングすることは技術的に違法です。しかし、これが人々が依然としてCDを購入する主な理由の1つであるため、英国のレコード業界（業界団体）は、誰も訴訟を起こさないと優雅に言います。  
 John Tehranianは、典型的な法律の教授が1日に80を超える著作権侵害を犯し、1,000万ドルを超える法的罰則を科していると計算しています[1866]。  
 テクノロジーにより施行が可能になり、著作権をますます少数の企業所有者および収集社会に統合することでロビーが集中し、貪欲が乱用され、摩擦が増大します。  
 私はすでに税制の場に影響を与えず、金持ちのゲットロットと小さな稚魚がそれほど多くない方法で収益を分配する集金社会の問題について述べました。これはストリーミングで悪化しており、支払いはユーザーではなくプレーの機能です。  
 つまり、サブスクリプションの大部分、または技術系企業が何らかの方法で支払わない金額の少なくとも一部が、アリアナ、エドシーラン、レディガガなどのメガスターに送られます。  
 昔は本を買うために本やレコードを現金で買っていました。ダウンロードへの移行は、Google、Spotify、Appleなどの企業が運営するサーバーが、人々が何を視聴したかという記録を持っていることを意味し、召喚状を提出することができます。  
）これらの記録はマーケティングにも使用されます。  
5。  
著作権所有者、または彼らに代わって行動することを主張する大手テクノロジー企業がなぜそんなに離れているのですか？答えはロビー活動のダイナミクスにあります。  
5。  
 歴史はピーター・ドラホスとジョン・ブレイスウェイト[581]によって語られました。要約すると、ファイザーおよび他の製薬会社は、音楽および映画業界（偽造およびコピーを削減したい）、高級品業界（安価なノックオフの数を減らしたい）、およびその他の多くの企業と提携しました。米国のプレーヤー（BusinessSoftware Allianceを含む）は、米国政府に、他の国に圧力を適用して、特許、著作権、および商標に関する法律をアメリカの法律と一致させるように説得しました。本質的にtheUSAとEUは集まり、インドとブラジルのようなホールドアウトをいじめました。  
 米国では、1998年のデジタルミレニアム著作権法により、WIPOが要求する著作権保護メカニズムを回避することが禁じられましたが、欧州連合では、2001年の著作権指令にも同様の影響がありました。  
他にも多くの目立った事件がありました。たとえば、2001年の情報隠蔽ワークショップのプログラム委員会に参加していたときに、アメリカのレコード産業協会（RIAA）が、プログラムの議長にエドフェルテンと彼の学生による著作権マーキングスキームの脆弱性を説明する紙を引っ張らせようとする試みが行われましたデジタル音楽規格[495]。  
皮肉なことに、このスキームのプロモーターは、それを打破するために学者や他の人たちに公の挑戦を出した。  
彼が書いた本は彼の出版社を恐れさせましたが、彼は別の本を見つけました。  
5。  
2。  
2003–4年に1つの転機が訪れました。IPロビーは、IP施行指令であるブリュッセルを通じてさらなる措置を講じようとしていたからです。  
今回の措置の反対者は、措置が大幅に修正されたという対立する利害の十分に強い連合を構築することに成功した。  
IPロビーの過ちは、ヨーロッパのすべての国に、単なる民事問題ではなく、特許侵害を犯罪とするよう強要しようとしたことでした。  
 現在、薬物特許保有者は、「常緑化」によって特許を延長することを試みています。これは、後の特許に、疑わしいデリバティブのクレームを付けて提出するものです。ジェネリックドラッグメーカーは、損害賠償金の支払いに対するディストリビューターの補償を提供することで対処しています。  
 これにより、ジェネリック医薬品メーカーは、スーパーマーケット、自動車部品販売業者、消費者グループとともに、この指令に激しく反対しました。  
 もし特許侵害が犯罪になったなら、彼らはきっと彼らの不満を警察に連れて行くでしょうか？ビルはヨーロッパへのいくつかの将来の旅行で逮捕の危険を冒すでしょうか？特許侵害を犯罪化する試みは、テック企業が彼らの支持を撤回したときに崩壊した。  
 別のリッチでパワフルなロビーが反対方向に押し出されたときに停止します。  
 疑わしい。  
 最初の著作権は18年間、次に35年間、その後50年間であり、その後、クリエイターの生涯に70年間を加えたものでした。  
 （他の皮肉屋は、音楽演奏の著作権期間が、クリク・リチャード卿が当時の首相であるトニー・ブレアの休暇をバルバドスの彼の邸宅で休ませた後、50年から70年に延長されたことに言及した。  
古い原稿のキュレーションと同じように、古い部分のキュレーションにはお金がかかります。実際、映画業界は最近、デジタル作品をアーカイブすると、実際にはマスターコピーを古い塩鉱山に保管しただけの昔、実際に支払うよりもコストがかかることを発見しました。  
5。  
 長期的には、ビットストリングが誰にも属さない場合、その維持費に対して誰が支払うのでしょうか？既存の納税者が資金を提供する預金図書館システムをデジタル資料に拡張できるでしょうか？しかし、そのような組織は通常、理解できないことから、著作権法について守りすぎていることまで、さまざまな理由でデジタル素材の進歩に失敗しています11。  
 グーグルは大学図書館の多くの本をスキャンし、最終的には長い訴訟の後で著者や他の利害関係者との法的和解を得た12。  
 書籍が著作権で保護されている場合、著作権法で許可されているフェアユースとしてスニペットを検索および表示できますが、出版社の同意なしに電子版を販売することはできません。  
）2020年の最新の開発は、本の電子コピーのインターネットアーカイブ貸出を停止するための、本の出版者（この本の発行者であるWileyを含む）による訴訟です[1000]。  
24。  
2セクション8で述べたように、誰にメリットがありますか？  
4、著作権戦争のターニングポイントは2005年に来た。  
彼は、古典的な経済理論では、2つの産業間の技術的リンクは通常、より集中した産業（たとえば、自動車メーカーと自動車部品）に利益をもたらすと指摘しました。  
 音楽業界は傷つきましたが、その年の終わりまでに彼らは傷つきました–その年の秋までに、彼らは英国政府と欧州委員会にAppleに「何かをする」ように強くロビー活動をしました。 FairPlay DRMスキーム。音楽メジャーはApple、Amazon、Spotifyなどの企業に市場の力を失い、Net ﬂ ixはビデオ配信における支配的な地位を確立しました。  
バンドはメジャーを頼りにプロモーションを行っていましたが、今では自分たちのウェブサイトでアルバムを配ることで自分たちでできるようになりました。大英図書館が私たちのNGOのWebページをアーカイブしたいと思ったとき、彼らは著作権で保護されたリリースおよび補償フォームに署名することを望んでいました。  
 それがテクノロジー企業の仕事です。従来の組織は、多くの場合、信頼を寄せていません。  
 他v  
; 2015年10月16日（2D巡回）; 2013年11月14日（SDNY）。  
6。  
 実際、スマートバンドにはインディーズレーベルが加わり、ストリーミングやその他の収益のシェアが大きくなっています。  
24。  
物語は、キングキャンプジレットが使い捨てかみそりの刃を発明し、その後の刃の販売からかみそりに助成金を支払った1895年に始まります。  
ハイテク業界は最初にゲーム機にそれを採用しました。その後、1996年にゼロックスN24（カートリッジチップの歴史については[1822]を参照）から、インクカートリッジからプリンターに助成金を出すプリンターメーカーによって採用されました。  
 2003年に、有効期限とインク使用量の制御が追加されました[1207]。現代のカートリッジは、物理的にインクがなくなるのを待つのではなく、電子的にディスペンスされるインクの量を制限するようになりました。  
他の業界がこのテクノロジーを採用しています。  
いくつかの不満の後、ヨーロッパの規制当局はこれに耐えることを決定しましたが、米国では、問題は法廷で決定されました。  
 彼らは最初は勝ちましたが、2004年に控訴に敗れました[1157]。  
 これは、暗号学者のための自由市場を支持する米国の法律を解決しました。それは、DMCAカメアロン[1647]の前の立場でした。  
さらに多くの例があります。  
 何百もの例があります。私がこの章を改訂しているときに2020年に思いついたのは、GE冷蔵庫の水フィルターでの使用です。  
99。  
 ジャックはハックセキュリティエンジニアリング777ロスアンダーソン24を正式に設定しました。  
 ACCESSORY CONTROLおよびそれを公開した[353]。  
 インクカートリッジに高い利益率があるが、プリンターの市場が競争的である場合、競争によってプリンターの価格が下がり、高価格のカートリッジを補うことができます[1942]。  
その後、気が変わった。  
 たとえば、John Deereは、修理を許可されたディーラーに限定するロックをトラクターに取り付けているため、技術者がスペアパーツを承認するために$ 230のコールアウトと1時間あたり$ 135を支払う必要がある農民の間で大きな憤慨を引き起こしています[1070]。  
 トラクターの場合、修理する権利の法律が必要な緩和策の1つである可能性があります。  
 ウォーターフィルターカートリッジを6か月に1回交換するのが良い例です。約5年間使用しています。  
 「スマート冷蔵庫」を購入した場合のもう1つの一般的な結果は、ベンダーが話しているサーバーの保守を数年後に停止すると、冷ややかなレンガになることです。  
5。  
ロックダウンの早い段階で、一部の病院では集中治療医が使用する呼吸マスク用のバッテリーが不足していたため、時折ではなく24時間年中無休で使用されていました。  
 病院は喜んで200ドルでより多くを購入したでしょうが、中国は前月に工場を国有化しました、そして、3Mは他のコンポーネントサプライヤーにキーをリリースしませんでした。  
 他のサプライヤーの呼吸マスクはより安く、独自のバッテリーを要求しません。一方、サウサンプトンでは、PaulElkingtonと医学部の同僚が独自の呼吸マスクを設計し、世界中の誰もがそれらを作成したいと考えている設計を公開しました[623]。  
 市場管理メカニズムは、将来の持続可能性だけでなく、今日の安全性にも影響を与えます。  
7。  
7要約不正コピーからのデジタルコンテンツの技術的保護は、技術的にも政治的にも厄介な問題です。  
音楽業界自体が犠牲者の1人だったというのは正しかったかもしれませんが、継続する問題を解決するものではありません。  
研究の問題2020年の著作権に関する厳しい問題の多くは、技術的な問題ではなく、政策の問題です。  
ソフトウェアの難読化については、Bjorn De Sutterと同僚[555]が主催した、このテーマに関する2019年のDagstuhlセミナーのレポートから始めることができます。彼らはあなたのPCからどのような情報を収集し、どこに送信しますか？それでも合法ですか？Further ReadingKahnは、いつものように、歴史的背景をよく読んでいます[1001]。  
 情報の非表示については、KatzenbeisserとPetitcolasによる本[1023]とJessica Fridrichの本[724]があります。  
著作権とオープンカルチャーに関するポリシーの問題についての原則的な議論については、Pam Samuelson [1646、1647]とLarry Lessig [1144,1145]から始めることができます。  
 あなたが学者なら、何百万もの科学的な論文をオンラインに置き、出版社の弁護士に拘束された後に自殺したアーディンスワーツの悲劇と、サイハブを巡る長期にわたる戦いについて読んでおくべきです。著作権を無視してすべての科学論文を入手できます。  
 パブセッションで音楽を再生する場合、アイルランド音楽著作権機構に関する論争に興味があるかもしれません。  
 たとえば、ここでは、European DigitalRights（EDRi）の見解を示します。「デジタル環境では、市民は州からの不当な執行措置、セキュリティエンジニアリング779Ross Anderson24からの恣意的な民営化執行措置に直面しています。  
 概要企業と革新的な提供者の欠如。これらすべてが、クリエイターと彼らが住んでいる社会との関係を損なう失敗した違法な法的枠組みの印象を強めます。  
”セキュリティエンジニアリング780ロスアンダーソン