–レオナルドダヴィンチここにはセキュリティはありません–動き続けてください–リチャードクレイトン21。  
 ネットワークセキュリティの多くは実用的なエンジニアリングであるため、これは簡単ではありません。コンピュータサイエンスの純粋主義者は、この分野を別のものの上に積み上げた1つの小屋として見るかもしれません。  
しかし、多くの組織はネットワークセキュリティに注意を払う必要があり、目に見える戦略的傾向がいくつかあります。  
 そして、いくつかの産業には実行可能な代替手段がありません。  
 1990年代の終わりまでに、制御システムエンジニアは、センサーとアクチュエータを安価にIPネットワークに接続していました。そして、センサーのIPアドレスを知っている人なら誰でもそれを読み取れ、アクチュエータのIPアドレスを知っている人なら誰でもそれをアクティブにできることに気づきました。  
 典型的な電気63521。  
 はじめに変電所には、パフォーマンスが重要なLAN上に多数のベンダーの200台のデバイスが存在する可能性があるため、暗号化を改良することは現実的ではありません。しかし、それは外界とのつながりが1つあるため、ここで保護を行う必要があります。  
 内部CANBUSを保護できない車両でも同じアプローチがとられるため、外界との無線インターフェースを保護する必要があります。  
考えられるリーダーの1人はGoogleであり、ゼロトラストセキュリティモデルと呼ばれるファイアウォールなしのアーキテクチャを推進しています。従来のVPNを必要としない場所。  
 特にサービス拒否攻撃に対する境界防御はまだいくつかありますが、それ以外の場合、内部ネットワークには権限がなく、ユーザーとデバイスの厳密な認証と認証の確立に重点が置かれます。各サービスにはインターネットに接続するアクセスプロキシがあります。  
 また、本当に優れたHRデータも必要です。そのため、従業員と請負業者を、使用が許可されているデバイスとサービスに結び付けることができます。  
 家事労働が大幅に増加したため、パンデミックから確実に後押しされるでしょう。  
 たとえば、Iworkが勤務する大学では、境界にいくつかの防御策がありますが、大部分は学部に私たち自身のことをさせています。コンピュータサイエンス部門には、人文科学部門や財務部門とはかなり異なる要件があります。  
 次に、マルウェアを詳しく調べ、次に、フィルタリングや侵入検知などの防御テクノロジーと、防御者がそれらをどのように調整できるかについて見ていきます。  
 最後に、ネットワークアーキテクチャに戻ります。  
 たとえば、さまざまな種類のエンドツーエンド暗号化は、特に一括監視に対して利益をもたらす可能性がありますが、ネットワークセキュリティに必要な監視の邪魔になる場合があります。  
セキュリティエンジニアリング636ロスアンダーソン21。  
 ネットワークプロトコルとサービス拒否21。  
 電信概要は以下のとおりです。  
16。  
93。  
 現在、トラフィックの約10〜15％がIPv6です。多くの国では、新しいブロードバンドサブスクリプションにより、すべての通常の消費者の目的で機能するIPv6アドレスが提供されます。  
 動的ホスト構成プロトコル（DHCP）は、必要に応じてIPアドレスをマシンに割り当て、各IPアドレスが一意であることを確認するために使用されます。  
 そのため、悪意のある処理を行ったマシンを追跡したい場合は、多くの場合、デバイスのMACアドレスをIPアドレスにマップするログを取得する必要があります。  
最も基本的な問題の1つは、サービス拒否（DoS）攻撃の防止と軽減です。  
 対戦相手は、スパムを送信するために、IPアドレススペースの一部または1つ以上のドメインを盗もうとする可能性があります。あなたがそれを取り戻すときでさえ、あなたはそれが広範囲にブラックリストに載っているのを見つけるかもしれません。  
DNSなどのさまざまなオンラインサービスを悪用して、パケットトラフィックの洪水を送信する可能性があります。  
21。  
1BGPセキュリティインターネットは相互接続されたネットワークネットワークです。そのコンポーネントは、ISP、電話会社、大規模組織などの自律システム（AS）であり、それぞれが一連のIPアドレスを制御します。  
ルーター-ネットワーク上でパケットを交換する専用のコンピューター-BGPを使用して、IPアドレスの特定のブロックに到達するために使用できるルートに関する情報を交換し、使用する有効なルートを選択できるようにルーティングテーブルを維持します。  
インターネットの相互接続性は、多くの相互依存層を持つ複雑なエコシステムです。2。  
 ただし、Tier-1プロバイダーの統合の結果として、インターネットは徐々に一元化されており、破壊的な攻撃だけでなく、コモンモード障害（電力カットなど）に対して脆弱です。  
 事故や事故という形ですでにいくつかの警告が出されています。  
 一部の人々は事故に起因すると述べ、他の人々は中国が「サイバー核」をテストしていたと示唆し、その一部は放射性降下物を脱出した。  
中国と（より最近では）ロシアは、国のインターネットを分離可能にすることに取り組んでいるため、理論的には、ローカルサービスや施設に容認できない付随的な被害を与えることなく、大規模な破壊的攻撃を仕掛けることができます。  
 スパマーによるIPアドレス空間のハイジャックから、2018年の8桁の広告詐欺に至るまで、犯罪者の誤用もあり、その犯人は米空軍から盗まれたアドレス空間に隠れていました[791]。  
一歩後退して、インターネットの回復力を定義して測定することは困難です。これは効率に緊張しており、少数の非常に大規模なネットワークが支配的になるにつれて減少する可能性があります。  
 レジリエンスと効率、到達可能性と輻輳、トラフィックの優先順位付け、商業的感度、複雑さと規模の間には、多くの複雑な相互作用があります。  
 ISPと政府の間で蔓延する不信感により、規制は困難になります。  
レジリエンスはこれまで余剰能力と急速な成長に依存してきましたが、それは永遠に続くことはできません。  
現在の主な技術的BGPセキュリティメカニズムは、レジストリが「オートノマスシステムXがIPアドレス範囲Yをアナウンスする」ことを証明できるようにするResourcePublic Key Infrastructure（RPKI）です。  
 すでに脆弱なBGPシステムをより堅牢にして、多くの証明書をセキュリティエンジニアリングに含めるかどうか、ロスアンダーソン21。  
 ネットワークプロトコルとサービス拒否主な見解; 2020年2月にRIPEの証明書が期限切れになったとき、修正されるまで短時間の停止がありました。  
21。  
2DNSセキュリティドメインネームシステム（DNS）では、ross-andersonなどのニーモニック名を使用できます。  
 それは時々攻撃されます：2016年10月にMiraiボットネットがDynDNSを攻撃し、米国東海岸にあるTwitterを5時間攻撃しました。  
ハイジャックは時々、さまざまなレベルで発生します。  
 これはファーミングと呼ばれ、ドライブバイファーミングと呼ばれる変種では、詐欺師は、ホームルーターのDNSサーバーをISPのDNSサーバーから制御下のDNSサーバーに変更するJavaScriptを含むWebページに誘導します[1816]。  
シティバンク。  
 これが、ホームルーターのデフォルトのパスワードを変更する理由の1つです。ネットワーク内からのみアクセスできる場合でも同じです。  
そのような署名を検証することで、レコードサーバーが信頼できるサーバーからのものであり、途中で変更されていないことを確認できます。  
govは署名されることになっています。そして、レジストラが署名されたドメインをより安くしたので、スウェーデンのほとんどのドメインが署名されています。  
 他の企業はDNSSECを避けています。競合他社が「ゾーンを歩き」、すべてのサブドメインを列挙することを望んでいないためです。 NSEC3拡張機能により、企業はハッシュを使用してこれを回避できますが、多くの企業（またはそのサービスプロバイダー）はまだインフラストラクチャを構築していません。  
一般的なテクニックは、アリスがチャーリアのメッセージを送信してボブを攻撃することです。「ねえ、この短い質問に対する非常に大きな答えを教えてくれませんか？あなた、ボブ！」署名されたDNSレコードははるかに大きいため、DDoS-for-hireserviceはDNSSECを増幅器として使用でき、AliceはBobのIPアドレスからのパケットを多くのDNSサーバーに送信し、ターゲットに返信を送信できます。  
govには2つの素晴らしい大きなキーがあります。  
2。  
 メインブラウザーのメンテナーであるChromeとMozillaは、DNSトラフィックをクリアに送信するのではなく、httpsを介してDoHリゾルバーに暗号化することを提案しています。  
 欠点は、多くのエンタープライズセキュリティ製品がDNSを監視して不正行為を検出することです。  
 システム管理者は、DNSハイジャックを監視し、特定のドメインを不適切な作業としてブロックすることも好みます。  
 商業面では、DoHは広告市場でのGoogleの不満を定着させ、アカマイやクラウドなどのコンテンツ配信ネットワークにルーティングや負荷分散などの問題を引き起こします。専門家は、代わりにDNS over TLSを実行することを好んだでしょう。  
2。  
 アリスがボブへのTCP接続を開始し、後続のパケットトラフィックのシーケンス番号を設定するために使用する3ウェイハンドシェイクから始めましょう。  
1 – TCP / IPハンドシェイクこのプロトコルはさまざまな方法で利用されています。  
 アリスは単純に大量のSYNパケットを送信し、応答を確認しません。  
これは、1996年にニューヨークのISPであるPanixを数日間ダウンさせた最初の分散型サービス拒否攻撃の1つで使用されました。  
 そうすれば、ボブはハーフオープンセッションについて多くの状態を保持する必要がなくなります。  
一般的な原則は、あなたが誰でも呼び出すことができるプロトコルを設計しているとき、悪意のあるユーザーが正直な人に作業を強制することを許可しないことです。  
 アリスはボブにパケットを送信しますSecurityEngineering640Ross Anderson21。  
 チャーリーから来たと主張するネットワークプロトコルとサービス拒否。  
21。  
4その他のアンプサービス拒否攻撃では、DNSやTCPよりも多くのプロトコルが使用されています[1503]。  
 AliceがBobからブロードキャストアドレスに来ると主張するICMPパケットを送信した場合、サブネット上のすべてのマシンが応答を送信します。  
 悪意のある人たちは、NTPやDNSなどのプロトコルを使用するように変更しましたが、アンプはまだ見つかりました。  
ICMPやNNTPなどの使用可能な増幅器のほとんどはUDPパケットを使用しますが、SYN反射は使用しません。そのため、2000年代半ばから、ブロードバンドISPは偽造されたソースアドレスを持つUDPパケットのフィルタリングを開始しました。  
 したがって、UDPパケットアンプを悪用する攻撃は、ホスティングセンターのサーバーから実行する必要があります。  
21。  
5その他のサービス拒否攻撃サービス拒否攻撃を作成する巧妙な方法が1つずつ終了しているため、悪意のある人物は感染したマシンから大量のパケットを送信することにより、ますますブルートフォースになりました。  
 現在、ボットネットはあらゆる種類の脆弱性を使用して組み立てられており、アンダーグラウンドマーケットでは、マシンをハッキングし、さまざまな方法で価値を引き出す他のユーザーに販売することに特化しています。  
 TheMiraiボットネットは、この機会を利用するために2016年10月に登場し、それから1000以上の亜種がありました（そのソースコードはHackforumsに投稿されました）。  
ほとんどは学童によって起動されます。通常は、反対側の乗組員のスチームスピークサーバーを停止したいゲーマーです。  
 恐喝の事件がいくつかありました（e。  
 オンラインブックメーカーの）、および政治的反対者を抑制するための技術の使用の増加-開始セキュリティエンジニアリング641ロスアンダーソン21。  
 ネットワークプロトコルとサービス拒否多分キルギスタンの野党のサーバーへの攻撃で、たとえそれらが北米に移転されたとしても[1613]。  
とはいえ、オンラインアクティビズムを忘れてはなりません。  
21。  
6電子メール–詐欺師からスパマーまで電子メールのSMTP標準には、大量の傍受の防止と、不要な大量のメールの防止に関する特定の問題があります。  
PGP / GPGなどのプログラムを使用してメールを暗号化することは可能でしたが、これは小さなコミュニティの外では決して行われませんでした。  
 さらに、少人数のグループだけが暗号化を使用している場合は、当局の注意を引くだけかもしれません。破壊的なグループ、スパイなどには、セクション20で説明したように、機密性だけでなく匿名性が本当に必要です。  
 そのため、PGP / GPGは、システム管理者やアンチウイルス研究者などの専門家によって使用される傾向があります。  
 まず、ほとんどのメールサーバーは、特にSnowdenの啓示以来、メールを交換するときに他のメールサーバーとの暗号化通信を設定するためにstarttlsを使用しています。  
 このような攻撃に対する現在の対策であるMTA Strict Transport Security（MTA-STS）は、Microsoft、Google、Yahoo [1220]によってサポートされています。これにより、メールサービスプロバイダーは、適切な証明書によって認証されたTLSセッション経由でのみメールを配信するように指定できます。あなたは彼らのウェブサイトからダウンロードします。  
 MTA-STSは、以前の標準であるDNSベースのNamedEntitiesの認証（DANE）に取って代わり、starttlsのTLS証明書をメールサーバーのDNSレコードに追加しました1。  
 この場合、電子メールの機密性はTLSによって保証され、証明書の固定と証明書の透明性で強化されます。これについては、後で説明します。大量の不要なメール、つまりスパムには、2つのコンポーネントがあります。  
 マーケティング担当者が面倒に感じる可能性があるため、1DANEはドイツではまだ広く使用されていますが、Googleが信頼できないと見なしているDNSSECに依存しているため、Googleは使用を拒否しました。  
3。  
2つ目は、大部分がボットネットによって送信された、通常は望ましくないトラフィックのフラッドで構成されており、多くの場合、明確な犯罪目的で送信されます。  
これは、4つの主要なメカニズムを持つビッグプロバイダーによって戦われています。  
 ドメインキー識別メール（DKIM）は、送信ドメインのDNSレコードに公開検証キーが保持されている署名キーを使用して署名することにより、送信ドメインに電子メールを結び付けます。  
 あまり変更されていないメールは転送できます。  
2。  
 繰り返しますが、これはドメインDNSレコードのキーに対して検証可能です。  
3。  
4。  
 これは、ユーザーごとに、また時間とともに変化するマーケティング資料のユーザー設定によって、さらに複雑になります。  
 その統計は2000年代半ばから「こぶ」であり、これはより顕著になっています。  
21。  
3。  
 長年にわたって命名法をめぐる宗教戦争がありました。そのため、多くの人々はマルウェアという用語を単に使用することを好みます。  
 ワームは、他のシステムに自身を複製する悪意のあるプログラムですが、他のプログラムのコードに自分自身をフックすることで複製するのはウイルスです。  
 望ましくない可能性のあるソフトウェア（PUS）がオープンにインストールされている可能性がありますが、ユーザーが望んでいないことを実行しています（ユーザーがそれを理解している場合）。  
 たとえば、ストーカーウェア（ある人が別の人の携帯電話の位置を追跡して使用できるようにするソフトウェア）は、秘密にインストールされたか、支配者のいじめっ子パートナーによって、または保釈の条件としてそれを注文した裁判所によって、異なるカテゴリに分類されます。  
マルウェアは通常、ステルス技術を使用して非表示にしますが、最終的には特定され、それを削除するためのツールが作成されます。  
（特に政府機関にマルウェアを販売する企業もあります。  
21。  
1マルウェアの初期の歴史それは1960年代初頭、マシンは遅く、CPUサイクルは割り当てられていました。多くの場合、学生は最後尾にいます。  
 1970年代までに、大学のタイムシェアリングシステムは、トロイの木馬を含むますますいたずらの標的になりました。  
 1978年、Xerox PARCのJohnShochとJon Huppは、ワームと呼ばれるプログラムを作成しました。このプログラムは、ネットワーク全体に自分自身を複製して、アイドルプロセッサを探し、タスクを割り当てることができました[1724]。  
 彼は、システムのソースコードを注意深く検査し、脆弱性がないことがわかっていても、トラップドアを挿入できることを示しました[1883]。  
これが事実であると認識した場合、2無料の試用後に削除するのが非常に困難であったり、不安を招いたりするなど、一部のウイルス対策製品はさまざまな方法でマルウェアのように動作します。  
セキュリティエンジニアリング644ロスアンダーソン21。  
 マルウェアマネージャー–トロイの木馬、ワーム、ラットログインプログラムをコンパイルすると、どのアカウントでも機能するマスターパスワードが挿入されます3。  
 そのため、コンパイラが自身をコンパイルしていることを認識すると、ソースに存在しない場合でも、とにかく脆弱性を挿入します。  
 道徳は、システムを完全に信頼するためには、ソフトウェアエンジニアが「ビルド」という単語を使用する、つまりソースコードからコンパイルするという意味で、システムをすべて構築するだけでは不十分であるということです。  
次にマルウェアはモバイルになりました。  
 1984年にフレッドコーエンはこのトピックについて博士号を取得しました。異なるオペレーティングシステムでの彼の実験は、コードが1つのマシンから別のマシンにどのように伝播するかを示しました。  
4、マルチレベルシステムの1つのコンパートメントから別のコンパートメントへ。  
初期の革新の1つは「クリスマス」ウイルスで、1987年12月にIBMメインフレーム全体に広がりました。  
 それは悪意ではなく、いたずらとして書かれたものです。そして、ネットワーク（IBMのBITNET）を使用して拡散し、ユーザーにそれを実行するように勧めることで、時代を先取りしました。  
3。  
 これは、1988年11月に1つのマシンから別のマシンに拡散するために多数の脆弱性を悪用したRobert Morris Jrによって書かれたプログラムでした。  
4。  
 また、それ自体を偽装するためのステップも実行しました。shと呼ばれ、そのデータ文字列を暗号化しました（Caesar暗号を使用しています）。しかし、バグがありました。  
 その結果、膨大な量のトラフィックが発生しました。これは、当時、Arpanet上の60,000台のマシンの10％しか影響を受けていなかったにもかかわらず、インターネット（正確にはその前身であるArpanet）を完全に詰まらせていました。  
4インターネットが一般に公開される前は、オンラインサービスはほとんどがスタンドアロンでした。掲示板は通常、趣味で運営されていたため、加入者や匿名のユーザーでもダイヤルインして情報やファイルを共有できました。  
3。  
21。  
3マルウェアのさらなる進化1990年代初頭までに、PCウイルスはウイルス対策ソフトウェアの業界全体を生み出すような問題になりました。  
21世紀の初めまでに、主なベクトルはWordなどのマクロ言語の副産物であり、主な送信メカニズムはインターネットになりました[298]。  
 2000年の「Love Bug」は、被害者のアドレス帳の全員に自分自身を送信するワームで、「I love you」という件名で、人々に開かせるように設計されています5。  
 同社は各従業員にアドレス帳の社内ディレクトリのコピーを渡しており、85,000のメールクライアントがそれぞれ85,000のアドレスのそれぞれに「あなたを愛して」と発言しようとしたため、結果はメルトダウンでした。  
次の開発はフラッシュワームで、インターネット全体をスキャンして、エクスプロイトなどに対して脆弱なマシンを探し、それを乗っ取る。 Code RedやSlammerなどの例は、すべての脆弱なマシンを数時間または数分で感染させ、どのような自動防御が時間内に反応するかを調査しました[1821]。  
 スパイウェアは、所有者の許可なしに、またはせいぜい、ユーザーが同意していることを実際には伝えないあいまいなポップアップを使用して、コンピューター（そして現在は電話）から情報を収集して転送します。  
アドウェアは、広告ポップアップでユーザーを攻撃する可能性があり、スパイウェアにバンドルされる可能性があります。  
 一部のスパイウェアは、子供たちが今何をしているのかを見たいと思っている親から、またはパートナーを監視および制御したい虐待的な男性によって、安定した状態を保ちたい企業が意図的にインストールしたものです。  
2004年から6月にかけて、大きな変化が起こりました。  
 それ以来、アンダーグラウンドマーケットや犯罪フォーラムの出現により、1987年の「クリスマス」ワームのより強力な亜種と見なすことができます。  
3。  
 マルウェアの作成者は、ボットネットの遊牧民や他のエクスプロイトに現金で販売できるマシンを募集するために、ソフトウェアにお金を払っています。  
 コードの感染力が不十分な場合、コードは拡散しませんが、コードの感染力が高すぎる場合、数時間以内に世界のウイルス対策ベンダーが製品をアップグレードして、コードを検出して削除します。  
 （主な例外は、パッチを適用できないIoTデバイスを利用する場合です。  
 さまざまなストーリーが使用され、人々がリンクをクリックして、ルートキットを自分のマシンにドロップするトロイの木馬を実行しました。  
最初に本当に大きなものの1つであるStormは、ポンプとダンプのオペレーターと薬局の詐欺師から生計を立てました[1090]。  
 結局、Microsoftによって削除の対象になりました。  
フラッシュワームは、Miraiワームとその亜種で2016年10月から復活しています。  
それ以来、さまざまなIoTデバイスを攻撃するMiraiの亜種が1000以上あります。  
3。  
 ワームは、実行されたときに別の場所に自分自身のコピーを作成するだけです。おそらく、パスワードを推測したりリモートコード実行の脆弱性を使用して別のシステムに侵入したりします（どちらもインターネットワームで使用されていました）。  
ウイルスの2番目のコンポーネントはペイロードです。  
3。  
2。  
9ベルガコムを破壊し、そこにソフトウェアをインストールして、ベルギーを経由して他の国に移動する携帯電話のトラフィックを監視します。•CPUを使用して暗号通貨をマイニングするなど、他の悪質なタスクを実行します。•ルートキットをインストールするか、リモートアクセストロイの木馬で、そのコントローラーが上記のいずれかを実行できるようにし、他のマシン上のマルウェアとの攻撃を調整し、対策に応じて自身を更新します。  
 攻撃者は、ターゲットネットワーク上のデバイスを制御したら、横に移動してネットワークをマッピングし、認証サーバーやメールサーバーなどの主要な資産を見つけて、侵害を拡大し、リモートアクセス型トロイの木馬をインストールして永続的な存在にすることができます。1。  
 今日の良い習慣は、2要素認証を使用して、またはKerberosやSSHなどのプロトコルを使用してこのような攻撃をブロックし、クリアテキストのパスワードがLANを通過しないようにすることです。  
 その他の手法は、ファイルサーバーなどの共有リソースを対象としています。  
Kerberosを使用してクライアントとサーバーを認証する私たちのラボでこれをブロックします。  
3。  
最近、有能な攻撃者が利用できるツールの範囲について知るには、エドスノーデンによってリリースされたNSAの文書と、Vault 7の開示で漏洩したCIAツールキットを参照することをお勧めします。  
重要なのは、ネットワークへの侵入者が他のマシンを乗っ取ることができる容易さは、ネットワークがどれだけしっかりとロックダウンされているかによって決まり、侵害に続く可能性のある損傷は、ネットワーク内の他のマシンが信頼している程度、または侵害されたマシンに対して脆弱です。  
セキュリティエンジニアリング648ロスアンダーソン21。  
 マルウェアマネージャー–トロジャン、ワーム、ラット21。  
5対応策1987年に最初のPCウイルスが流行してから数か月以内に、ウイルス対策ソフトウェアを販売する新興企業が登場しました。  
初期のウイルス対策ソフトウェアは、基本的にスキャナーとチェックサマーという2つのフレーバーで提供されていました。  
 マルウェア開発者はさまざまな方法で対応し、主要な手法は多態性になりました。  
 通常の方法は、コードを暗号化し、復号化コードを含む小さなヘッダーを用意することです。  
最近のマルウェアは、そのようなパッカーを半ダースずつ実行し、実行時に再帰的にアンパックする可能性があります。  
 AVファームは、最後のアンパック操作にハッキングできる限り、少なくともアンパックされたコードをIoCとして使用できます。  
 マルウェア開発者の主な対策はステルスです。これは、このコンテキストでは、マルウェアがチェックサマーによって使用される種類のオペレーティングシステムコールに注意し、チェックが行われるたびに自身を隠すことを意味します。  
DOSベースのファイルウイルスの昔は、すべてのインシデントの中央報告ポイントを提供し、組織のマシンにロードされたすべてのソフトウェアを制御することを学びました。  
 同じ原則が依然として適用されます。  
その理由の1つは、ウイルス対策ソフトウェアの効果が着実に低下していることです。  
ほとんどすべてのエクスプロイトは、最初に起動されたとき（作成者が適切にテストした場合）、現在のウイルス対策製品では検出できず、その多くは、ウイルス対策業界の注意を引くことなく、目的の数のマシンを募集します。  
 つまり、優れたツールサポートを利用し、ネットワークトラフィックをログに記録して、最新の脅威情報に照らして分析します。  
そして今日、多くの攻撃者、特に有能な攻撃者は、マルウェアファイルを放置せず、「土地に住んで」います。彼らは自分のsshkeyをサーバーの1つにある承認済みキーのリストに追加するだけでよいので、好きなときにポップインして、レガシーAVが見つけるものは何もありません。  
4。  
4ネットワーク攻撃に対する防御マルウェアおよびネットワーク攻撃から一般的に防御するために、2008年のこの本の第2版からの見解は、次の3つが必要であるというものでした。システムを最新の状態に更新し、適切に構成するための十分な管理。既知のトロイの木馬とネットワークの悪用を阻止するファイアウォール。侵入検知機能を使用してネットワークとマシンを監視し、侵害の兆候がないかを確認します。これにより、通過した状態を把握し、後でクリーンアップできます。  
 大規模なWindowsショップには次のようなものがあります：1。  
 既知の脆弱性についてネットワークを継続的に調査する脆弱性スキャナー3。  
 リモートで作業するためのSSLゲートウェイ5。  
 会社のドキュメントやコードを削除しようとする従業員を特定するためのデータ漏洩防止（DLP）システム7。  
 最初に妥協が発生したときに戻って、それがどこまで広がったかを調べることができるログ分析ツール; 9。  
これらすべてを連携させるにはシステム統合が必要です。それ以外の場合は、ネットワークセキュリティセンターに何十もの障害が発生し、不正なドメイン、不正なIPアドレス、その他の侵害の指標のリストをツール間でコピーすることになります。  
ITセキュリティに真剣に取り組んでいる組織–彼らは国家の主体（大規模なサービス会社のような）の標的であるか、厳しいコンプライアンス要件を持っているためですセキュリティエンジニアリング650Ross Anderson21。（銀行のように）ネットワーク攻撃に対して防御するか、（軍のように）失うものがたくさんある–すべての脆弱性をソースで阻止することを目指します。  
 しかし、そのような戦略は見た目よりも難しいです。  
 新しいデバイスを登録するために厳格な官僚制度を課す場合、人々は彼らの仕事を成し遂げるためにそれを回避する方法を見つける必要があります。  
 また、勤勉な組織であっても、一度にすべてのセキュリティホールを修正するにはコストがかかりすぎる場合があります。パッチは重要なアプリケーションを破壊する可能性があり、組織の最も重要なシステムは、最も安全性の低いマシンで実行されることがよくあります。  
 第2章と第8章では、愚かな行動によってシステムを公開しないようにトレーニングを行うことの実践と制限について議論しました。  
 これはNSAが2013年に会社を攻撃する標準的な方法であることをEd Snowdenから学びました：彼らは外部トラフィックを監視してシステム管理者を特定し、背景調査を行って個々のターゲットを特定し、説得力のあるフィッシングルアーを作成します。  
疑わしいメールのリンクをクリックしないようにステータスを教育することもできますが、有能な攻撃者は疑わしく見えないメールを作成します。  
 第3章などで、被害者のせいは不適応であると説明しました。セキュリティシステムが使用できない場合は、貧しいユーザーを非難するのではなく、修正する必要があります。  
21。  
1フィルタリング：ファイアウォール、検閲ウェア、盗聴ファイアウォールは、プライベートネットワークとインターネットの間に存在し、有害な可能性のあるトラフィックを除外するマシンです。  
 ファイアウォールは1990年代半ばに登場したときに物議を醸しました。純粋主義者は、企業内のすべてのマシンを保護する必要があると述べたが、ファイアウォールの擁護者は、これは非現実的であると述べた。  
ファイアウォールは、パケットのストリームを検査し、フィルタリングまたはロギング操作を実行するシステムの一例にすぎません。  
 また、ログまたは監査証跡にコピーされる場合もあります。  
 セキュリティエンジニアリングのいずれかの開発651ロスアンダーソン21。  
 ネットワーク攻撃に対する防御これらのフィールドは他のフィールドに影響を与える可能性があります。また、実際のシステムにはオーバーラップping機能がある場合があります。  
 多くのフィルターはログも保持しているため、攻撃後に事実を調査することができます。金融部門の一部では、規制当局がインサイダー取引またはマネーロンダリングの疑いを調査できるように、すべての通信を記録する必要があります。  
21。  
1。  
この機能は、ルーター、Linux、およびWindowsで標準で使用できます。  
 また、「既知の不正」IPアドレスとの間のトラフィックを簡単にブロックすることもできます。  
基本的なパケットフィルタリングは、特定のポート番号に到達する場合を除いて、すべてのトラフィックをブロックするためによく使用されます。  
 高価なルーターを汎用サーバー上のソフトウェアによって制御される安価なスイッチに置き換えるソフトウェア定義ネットワーク（SDN）に移行すると、パケットフィルタリングルールはSDNコントローラー内のアクセス制御ルールにすぎません。  
 たとえば、パケットは、最初のフラグメントがファイアウォールの検査に合格した後、後続のフラグメントによって上書きされ、送信元アドレスがセキュリティポリシーに違反するものに置き換えられるようにフラグメント化できます。  
 たとえば、フィッシング詐欺師は、サイトのIPアドレスが1時間に数回変更されるfast- ﬂ uxのようなトリックを使用します。  
4。  
2サーキットゲートウェイ次のステップは、各TCPセッションのすべてのパケットを再構成して検査するサーキットゲートウェイです。  
 このために使用されるIPSECプロト​​コルについては、この章の最後のセクションで説明します。  
ただし、このようなフィルターは、悪意のあるコードから児童の性的虐待素材まで、アプリケーションレベルで悪いことを排除することはできません。  
セキュリティエンジニアリング652ロスアンダーソン21。  
 ネットワーク攻撃に対する防御21。  
1。  
 例としては、スパムを排除しようとするメールフィルターや、望ましくないコンテンツをブロックまたは削除するWebプロキシがあります。  
 Webベースのメールサービスへの移行とhttpsの採用により、メールフィルターで行う作業が大幅に減り、サービス会社はプロキシを防止するために証明書の透明性などの技術的対策を採用し、エンドポイントへのシフトの必要性をフィルタリングしています。  
 たとえば、中国のグレートファイアウォールは、2000年代を通じて、禁止された主題を参照するメールおよびWebコンテンツをブロックしようとしました[448]。Googleが推進する新しいBeyondCorpモデルでは、プロキシはアプリケーションサーバー自体の前に置かれるため、内部ネットワークを信頼する必要はありません。  
4。  
4IngressとEgressのフィルタリングほとんどのファイアウォールは外側を向いて悪いことを避けようとしますが、中には悪いことをやめようとするものもあります。  
 2005年頃、一部のISPはスパムを検出しようとする送信メールのトラフィックを調べ始めました[442]。現在、ほとんどのコンシューマISPは、顧客が偽装された送信元アドレスでパケットを送信することを禁止しています。  
2020年に最も急速に成長している下りフィルタリングの使用は、データ漏洩防止（DLP）です。  
 ただし、httpsの普及により、DLPシステムは通常、ミドルボックスを使用するのではなく、エンドポイントにソフトウェアをインストールする必要があります。  
4。  
5アーキテクチャ長年にわたり、多くの企業は監査人を満足させるためにファイアウォールを購入しました。  
 反対に、防衛請負業者の深刻なファイアウォールシステムは、非武装地帯（DMZ）としても知られている、外界をスクリーンドサブネットに接続するパケットフィルターで構成されている場合があります。DMZには、メールをフィルターするための多数のアプリケーションサーバーまたはプロキシが含まれています。 Webおよびその他のサービス。  
4。  
 。  
FilterInternetIntranetClassified-イントラネット図21。  
2）。  
 Atour大学では、部署ごとにファイアウォールがありますが、共有ネットワークバックボーンと、ロギングなどの一部の共有中央サービスがあります。  
 各ネットワークを小さく保つことは、あらゆる妥協の範囲を制限し、システム管理者にそれを防御する動機を与えるのに役立ちます。  
まず、ファイアウォールは少数の処理しか行わないため、脆弱性やエラーの原因を簡単に取り除くことができます。  
 一方、同じように構成された数千のPCを備えたコールセンターのようなものを運営している場合は、この構成を堅固に保つことをお勧めします。  
第2に、精巧な中央設置は運用コストが高くなるだけでなく、人々がファイアウォールをバイパスするケーブルモデムなどのバックドアを設置して作業を完了するほどの邪魔になる場合があります。  
 私たちの部門がそうであるように、多くのよく運営されている企業はオープンなゲストネットワークを持っています。常にうまくいくものがなければなりません。  
セキュリティエンジニアリング654ロスアンダーソン21。  
 ネットワーク攻撃に対する防御第3に、ファイアウォールは、人々がそれらを回避する方法を見つけるまで機能します。  
 その後、すべてがWeb 2に移行しました。  
次に、非境界化があります。GoogleのBeyondCorpが指摘しているように、デスクトップコンピューターで使用されていた機能に使用されている電話やPDAの急増、およびビジネス手法の変更により、すべての保護を境界に配置することは着実に難しくなっていますこれには、機能のより多くのアウトソーシングが含まれます–正式に下請け業者に、または情報的には広告でサポートされるWebアプリに。  
g。  
 Webアプリケーションの急増は、便利なことを実行するのが難しくなるため、周辺で実行するインセンティブの鈍化によって補完されます。  
 多くの企業が2000年代初頭にJavaScriptをブロックしようとしましたが、JavaScriptを必要とする人気のあるWebサイトに打ちのめされました。  
そして、私たちの古くからの友人である受信者操作特性またはROC曲線があります。  
 子供が公共図書館のポルノにアクセスするのを停止するためにcen-sorshipシステムを実行している場合、ブロックされたり、写真が通過したときに親や教会を困らせたりしますか？セックス、暴力、悪意のある言語のWebコンテンツをフィルタリングするために使用されるファイアウォールシステムも、無料の音声サイトをブロックする傾向があるという事実により、事態はさらに悪化します（これらの多くはファイアウォールベンダーを批判しています。  
 知り合いの100人が使用する部門ネットワークを管理し、侵入や構成エラーによって引き起こされた混乱を個人的に解決しなければならないシステム管理者は、何千ものマシンを調べている大規模なチームの1人のメンバーである人よりもはるかにやる気があります。 。  
4。  
 発生している悪いことを検出するために使用されるシステムは、総称して侵入検知システム（IDS）と呼ばれます。  
 例：•ボットネットや既知の不良IPアドレスの制御に使用されるIRCチャネルなどの「既知の不良」サービスに接続しようとするマシン、またはセキュリティエンジニアリング655ロスアンダーソン21に接続しようとするマシン。ネットワーク攻撃に対する防御既知の不正なDNS名を解決します。•送信元アドレスが偽造されたパケット-サブネットの外部から発信されたと主張するが、実際にはサブネットから発信されたパケットなど。•ネットワーク内のマシンから送信されたスパム。  
 これは、どのようにしてログが発生し、攻撃者が何に感染した可能性があるかを確認するための調査の最初のステップにすぎません。  
 これは現在、活発な研究分野です。2012年以降のAIのtheboomは、パターンマッチングの問題を探す多くのスタートアップを生み出しています。  
4。  
1侵入検知の種類最も簡単な侵入検知方法は、しきい値を超えたときにアラームを鳴らすことです。  
 より洗練されたシステムは、一般的に2つのカテゴリに分類されます。  
 銀行システムは、ユーザーが3日連続で現金自動預け払い機から最大許容額を引き出した場合に警告を発する場合があります。また、Unix侵入検知システムは、以前にナイーブなユーザーが突然、コンパイラーなどの高度なツールの使用を開始した場合に警告して、ユーザーアカウントの乗っ取りを探す場合があります。  
 これは、データ（マルウェアの特定の部分としてマークする実行可能ファイルの部分文字列など）または動作（既知のボットネットのコマンドアンドコントロールサーバーのIPアドレスにアクセスするマシンなど）のいずれかで明示的です。  
 セクション12で説明したように。  
4、カードの詐欺を検出するために使用されるシステムは、数十の信号を使用します。なぜなら、現代の支払いシステムの規模を活用するには、低い誤警報率が必要だからです。  
 以前に認識およびカタログ化されていない攻撃を検出することが期待されています。  
誤用と異常検出の境界線はややぼやけています。  
4。  
 数字「1」、「2」、.  
。  
 しかし、数値がランダムな自然の情報源に由来し、1桁以上にわたるため、それらの分布がそれらが表現される数体系に依存しない場合、分布は対数的です：10進数の約30％は '1で始まります'。  
別の境界線のケースはハニーポットです-注目を集めるために残されたもの。  
 ネットワークコンテキストでは、ハニーポットは多くのタイプのデバイスをエミュレートするため、攻撃者はインターネットをスキャンして特定のアップグレードステータスのDSLモデムを探して（たとえば）、攻撃するモデムを見つけます。これには、単純なエミュレータ、または最近の設計では、VMで実行されている実際のモデムファームウェアのいずれかが含まれている場合があります[1955]。  
21。  
2。  
 活動家がWebサイトを破壊することを心配している場合は、ページを頻繁にフェッチし、変更があったときにアラームを鳴らすマシンをどこかに設置してください。  
 ウイルスのパイオニアであるフレッドコーエンは、ウイルスを検出すること（プログラムが何か悪いことをするかどうかを決定するという意味で）が問題を停止することと同じくらい難しいことを証明したので、完全なソリューションを期待することはできません[450]。  
 一部の侵入検知システムは、ある種の疑わしい動作をブロックするように構成されています。  
 侵入検知システムは、ログを監視し、疑わしい出来事に注意を引くものとして定義することを好みます。  
 学術機械学習の研究者は、誤った警報率が0になるように分類子を訓練したときに、彼らがうまくいったとよく考えています。  
 しかし、Gmailチームに所属し、毎日自分自身を認証する10億人のユーザーを扱っている場合、それはやりすぎです。  
最後に、機械学習分類子には3つの一般的な問題があります。それらは、新しい攻撃を検出するのがあまり得意ではないという事実、人々がゲーム攻撃をしている、そして彼らがトレーニングデータの偏見を吸い込んでいるという事実です。  
3。  
4。  
3ネットワーク攻撃を検出する特定の問題今、ネットワーク侵入を検出する特定の問題に目を向けると、支払い詐欺よりも発見するのは困難です。  
 実際の侵入を後で検出するのが一般的です。  
4。  
•インターネットは非常に騒々しい環境です–コンテンツのレベルだけでなく、パケットレベルでも。  
 多くの不良パケットはソフトウェアのバグが原因です。その他は、DNSデータが古くなっている、または破損しているという障害です。いくつかは、脱出し、世界中を旅して戻ってきたローカルパケットです[213]。  
 100万セッションあたり10回の実際の攻撃がある場合（これはほぼ確実に過大評価です）、システムの誤警報率が0であってもです。盗難警報器の同様の問題について話しました。これは、HIVのような病気の検査プログラムを実施している医療関係者にとってもよく知られている問題であり、テストの誤り率が病気の有病率を超えています。  
•銀行からの盗難は不正確な状態を引き起こします-間違った場所での金銭と監査証跡の証拠-多くのネットワーク侵入は、例えば、彼らの使命が機密データを漏らすことである場合、これを回避することを目指します。  
•多くのネットワーク攻撃は特定のバージョンのソフトウェアに固有であるため、攻撃シグネチャの大規模で常に変化するライブラリが必要です。  
•暗号化されるトラフィックが増えるにつれ、コンテンツ分析や悪意のあるコードのフィルタリングが簡単に行えなくなります。  
•ファイアウォールのコンテキストで説明した問題は、主に侵入検知にも当てはまります。  
•侵入検知をローカルとグローバルの両方で行う必要がある場合があります。  
現在、侵入検知システムには、ネットワークとエンドポイントデバイスのシートの両方で異なるレベルの複数の監視メカニズムと製品の調整が含まれています。  
4。  
5。  
 したがって、成長分野には、セキュリティインシデントおよびイベント管理（SIEM）、セキュリティオーケストレーションおよびレスポンス（SOAR）、およびメトリックの統合ツールが含まれます。  
5暗号化：不規則な境界ネットワークセキュリティは、さまざまな方法で暗号化と相互作用します。  
 それらはSSHです。 WiFi、Bluetooth、HomePlugによるローカルリンク保護。 VPNで使用されるIPSecメカニズム。 TLS、およびこれらの多くをサポートするために使用される公開キー基盤（PKI）。  
 ネットワークに境界を設定し、ネットワーク内の信頼を変換するために使用するツールは、違いはありません。  
 一方、問題の最も集中化された部分であるPKIは、政府の命令によって破壊されることがよくあります。  
5。  
 そのため、自宅で仕事をしているとき、私のトラフィックは保護されています。また、私のデスクにあるPCからラボ内の別のマシンにログオンするときに、使用するパスワードがLANを平文で渡ることはありません。  
 マシン間の暗号化された接続をセットアップし、ログオンパスワードがネットワーク上を平文で移動しないようにし、その急速な採用につながるその他の便利な機能をサポートします[1617]。  
 秘密鍵は、ユーザーがキーボードで入力するパスフレーズによって保護されます。  
 サーバーにログオンするときは、パスフレーズの入力を求められます。2台のマシンがDi-e-Hellmanキーを設定します。秘密鍵は一時的な公開鍵に署名し、中間者攻撃を阻止するために使用されます。したがって、後続のトラフィックは暗号化され、認証されます。  
Di-e-Hellmanを使用して設定されたセッションキーを認証するか、またはSecurity Engineering659Ross Anderson21を設定するかに関係なく、Kerberosを使用するオプションもあります。  
 暗号化：厳格な境界線セッションキーを直接アップします。  
）考えられる問題には、キーボードで一度に1文字ずつ入力すると、各文字が独自のパケットで送信され、パケットの到着間時間に、入力している内容に関する多くの情報が漏洩する可能性があるという事実が含まれます[1803]。  
 そのため、サーバーが危険にさらされた場合、SSHキーがインストールされている他のすべてのマシンに同じことが起こります。  
 これにより、パスワードを推測する攻撃、および弱いパスワードまたは既知のデフォルトパスワードがある場合に、Miraiおよび類似のツールに基づいてボットネットに募集することが可能になります。  
21。  
2周辺でのワイヤレスネットワーキング多くのネットワークでは、エッジでワイヤレステクノロジーを使用して、最後の数フィートをアクセスポイントからデバイスに、またはデバイスから別のデバイスに移動します。  
 ただし、ほとんどのデバイスは、多くのデバイスにパッチが適用されていないか、ユーザーインターフェイスがないか、またはその両方であるため、完全にブロックすることが困難なローカル攻撃に対して脆弱です。  
5。  
1WiFiWiFiは、電話やその他のデバイスをホームルーターに接続するために自宅で、またはPCだけでなく決済端末や在庫管理デバイスを接続するために企業によってワイヤレスローカルエリアネットワークをサポートします。  
最初に広く使用されたものであるWEP（有線の同等のプライバシー）は、米国の輸出管理が要求する弱い暗号と貧弱なプロトコル設計により、かなり簡単に破られることが示されました[299、1873]。  
 各アクセスポイントのキーは、通常、ルータの背面に収まるカードに印刷されています。  
 英国やアメリカの多くの人々は、ゲストが使用できるオープンなネットワークを用意しておくと便利です。そのため、あなたとあなたの隣人は互いのネット​​ワークをバックアップとして使用できます。インドなど一部の国では、WiFiアクセスポイントをオープンにすることは法律に反しています（2008年にボンベイで攻撃を仕掛けたテロリストが目立たないように自宅に電話をかけました）。  
セキュリティエンジニアリング660ロスアンダーソン21。  
 暗号化：不規則な境界Wi-Fiセキュリティは、依然としてやや脆弱です。  
 しかし、今では多くのデバイスと家庭用アプライアンスに付属のクラウドサービスが付属しています。  
 PINを設定できますが、メカニズムでいくつかの攻撃が見つかりました。  
 2007年3月に、小売チェーンTJMaxxは約45を報告しました。  
、非難することでした[1509]。  
パッチの適用が問題です。  
 おもちゃから家電まで、IoTデバイスの大多数については、パッチが当てられることはありません。  
5。  
2BluetoothBluetoothは、ヘッドセットを電話に、またはポケットの電話を車のハンズフリーインターフェイスにリンクするなど、パーソナルエリアネットワークを目的としたもう1つの短距離無線プロトコルです。  
 WiFiと同様に、プロトコルの最初のバージョンにはフローがあることが判明しました[2015、1713、1101]。  
1（2007年にリリース）では、BluetoothはSecure Simple Pairing [1169]をサポートしています。これは、楕円曲線のDi-e-Hellmanを使用して、パッシブ盗聴攻撃を阻止します。  
 ただし、一方または両方のデバイスにキーボードまたは画面（または両方）がない場合があるため、あるデバイスで番号を生成し、別のデバイスでパスキーとして入力することもできます。中間者攻撃から保護されない「ジャストワークス」モードがあります。  
 ここでも、パッチの適用が問題です。  
 そのため、パッチが適用されていないBluetoothチップを搭載したデバイスを使用している場合は、脆弱性が存在する可能性があります。  
5。  
3HomePlugHomePlugは、主電源ケーブルを介した通信に使用されるプロトコルです。  
6。  
 （関心宣言：私はプロトコルの設計者の1人でした。  
 私たちは、ユーザーがネットワークコントローラーにデバイスラベルに印刷された一意のAESキーを手動で入力するセキュアモードと、認証なしでキーが交換される「シンプル接続」モードの2つの操作モードのみを提供することにしました。  
 ただし、多くのベンダーは「単純接続」モードをサポートしているだけで、セクション14ですでに述べたように、トラストを最初に使用するポリシーが適用されます。  
3。  
他のユーザーは、キーが既にインストールされたエクステンダーとペアを販売しています。  
 ベンダーはまた、競合他社と互換性がないようにさまざまな方法で製品をカスタマイズしました。  
21。  
2。  
 これは、特定のパケットストリームを保護するために使用されるキー、アルゴリズム、およびパラメータの組み合わせとしてのセキュリティアソシエーションを定義します。  
 キーを設定し、パラメータをネゴシエートするためのインターネットキーエクスチェンジ（IKE）プロトコルもあり、これの標準のデフォルト設定（1024ビットDi-e-Hellmanを使用）は安全でないとエドスノーデンの開示から推測できます。  
 個々の従業員のラップトップとhomePCも、適切なソフトウェアを提供するVPNに参加できます。  
21。  
7。  
 当初、政府や電話会社がこれを行うと考えられていましたが、遅すぎました。  
 セキュリティエンジニアリング662ロスアンダーソン21としてゴールドラッシュが続きました。  
 CASとPKIthe CAは互いに購入し、統合されました。投資家は、すべてのデバイスに公開鍵証明書が必要であることを望んでいたため、トースターで証明書を更新するには2年ごとにVerisignに10ドル支払う必要があり、そうしないと冷蔵庫と通信しません。  
 人々がGmailなどのWebサービスに移行すると、セキュリティ機関は中間者攻撃を実行するためのツールを開発し、TLSを使用してパスワードエントリ（およびその後、セッション全体）を暗号化したため、これはCAを作成することを意味しましたwww。の証明書。  
comは、ターゲットのブラウザが受け入れるセキュリティ機関の公開鍵です。  
 この時点で男が聴衆の中で立ち上がって、「どうして私の国を侮辱するのだろう、と勇気を出しました。ツビタクは諜報機関ではありません。それは研究組織です！」Mozillaの男は肩をすくめて肩を落とし、「これでガバナンスの証明がいかに難しいかがわかります。  
 DigiNotarはオランダのCAで、Gmailにワイルドカード証明書を発行したことが判明しました。  
 MozillaとGoogleは、ルート証明書を削除することにより、DigiNotarを即座に死に至らせました。マイクロソフトとアップルがすぐに続きました。  
以前の別のCA、Comodoに対する攻撃があったことが判明しましたが、その会社は、誤って発行された証明書をすべて取り消したと主張しました。「公開（鍵インフラストラクチャ）」と「（公開鍵）インフラストラクチャ」の間には、頻繁に意味上の混乱があります。  
 2つ目ではできません。これをクローズドPKIと呼びます。  
 何百万ものマシンにインストールされているソフトウェアを保守している企業には、コード署名鍵にプライベートCAを使用することをお勧めします。  
 命名は困難であり、証明書に依存するアプリケーションが多いほど、耐用年数は短くなります。  
foo。  
foo。  
「これは、「1つまたは複数の」議論の側面です。  
6。  
 銀行と簿記の章で見たように、機器に別の機器を表示させることで、簡単にメッセージに署名させることができます。  
509プロトコルスイート）は、電話帳の電子的代替物を提供するために開発されたため、openPKIアーキテクチャでは誰もが一意の名前と一意のキーを持っていると想定することから始まりました。  
•何百ものルート証明書の1つをFirefoxから削除すると、Mozillaはそれをサイレントに置き換えます。 Windowsにはさらに多くのルート証明書が付属していますが、それらを完全に削除することはできません。  
•Windowsで認証を取得し、他のブラウザーでは認証を取得していない政府（2014年の軍事クーデター後のタイなど）がMacユーザーに対して異なる監視方法に頼らざるを得ないという興味深い影響がありました[1554]。  
 その結果、ユーザーはセキュリティ警告を無視するように訓練されており、それらに注意を払うために使用されたのはごく少数の少数派だけでした[841]。  
•証明書は会社名をDNS名にバインドしますが、そのベンダーは通常、どちらの権限もありません。彼らは、申請者がそのドメインに送信された電子メールに回答できるか、またはCAチャレンジが記載されたWebページを作成できることを確認した後、証明書を配布します。  
•「認証実務声明」において、CAはすべての責任を否定します。  
 当初のアイデアは、証明書に依存している人は誰でも、CAから証明書失効リスト（CRL）をダウンロードして、依存しようとしている証明書をチェックできるというものでした。  
 さらに、一部のシステム（特に米国政府のもの）のユーザーは、システムを起動するたびに大きなCRLをダウンロードする必要があり、遅延とネットワークの輻輳につながりました。  
この混乱の背後には、いつものように安全保障経済学があります。  
セキュリティエンジニアリング664ロスアンダーソン21。  
 CASとPKI複雑で、SETと呼ばれる重量級のプロトコル。開発者の負担が少ないためです[110]。  
 CAとcertssinceに関するエンジニアリングの多くは、キャッチアップを果たしてきました。  
証明書の最大許容寿命は、メインのブラウザーで受け入れられる場合、8年から3年から27ヶ月に着実に短縮されています。  
 これにより、多くのWebサイトが証明書を更新する必要があります。会社がDNSのすべての証明書をどのように流し出すかを見るのは興味深いでしょう。  
）証明書を購入する必要があったため、以前は証明書を取得することは困難でした。ドメインを制御していることを証明し、証明書を取得してサーバーにアップロードし、構成を変更してから、すべてをテストしました。  
 証明書を無料にすることで、全自動化が可能になり、コストが抑えられます。「LetsEncrypt」CAは、1億ドルのサイトで1億ドルの予算をサポートします。  
 このサービスは、スノーデンの啓示から2年後の2015年に始まりました。  
透明性ログがあり、システムには手動による上書きがないため、証明書の発行を強制されたことはありません。  
）2019年11月には、最大のCAとなり、1億8800万のドメインに1億2200万の証明書が発行されました。上位100サイトの5％が上位100サイトの35％でした。  
21。  
1透明性の証明ComodoおよびDigiNotarへの攻撃に続いて、悪意を持って発行された証明書をブロックするメカニズムの研究が始まりました。  
 Googleは2013年に最初の証明書の透明性ログをリリースし、Chromeは2015年に拡張検証証明書のためにそのようなログを要求し始めました。  
セキュリティエンジニアリング665ロスアンダーソン21。  
 トポロジー21。  
•公益事業には、信頼できるネットワーク上に数十から数百のデバイスを備えた発電機または変電所を含むアイランドがいくつかあり、専用のファイアウォールとVPNを介してネットワークコントロールセンターに接続されています。  
 また、内部ネットワークは信頼できない場合がありますが、ネットワークの場所がアクセス制御の決定に関与しないという意味では、フロントエンドシステムによるDDoS攻撃から保護されている場合があります。ノードがユーザーであり、エッジが互いのアドレス帳に存在する、より複雑なトポロジが見つかります。  
 ソーシャルネットワークは、頂点次数のべき法則分布を持つグラフによってモデル化できます。少数の適切に接続されたノードは、ランダムな障害に対するネットワークの回復力を高め、ナビゲートを容易にします。  
 適切に接続されたノードを削除すると、ネットワークは簡単に切断されます[36]。  
 現在、私たちは定量的モデルを持っています。それらは、革命家が細胞内で組織化する傾向がある理由を説明するのに役立ちます[1373]。十分に接続された少数のオーガナイザーに対して追跡分析を行うことにより、最初の場所のセル構造で反体制派が組織化しない限り、警察は反体制派組織の驚くべき数のメンバーを特定できます[510]。  
8要約ネットワーク経由で起動される攻撃の防止と検出は、最新のCISOの仕事の中核です。  
 それは報道価値のある失敗につながる可能性があります。  
 それぞれの新しい進歩は、心配する新しいことを開きます。たとえば、クラウドサービスは、ネットワークセキュリティタスクの多くをプロバイダーにシフトしますが、構成管理をより重要にします。  
セキュリティエンジニアリング666ロスアンダーソン21。  
 概要ハッキング技術は、一部は主要ベンダーによって偶発的に導入された脆弱性の日和見主義的利用に依存し、一部は信頼できないコードを実行するソーシャルエンジニアの人々への技術に依存しています。  
研究の問題2000年、ネットワークセキュリティ研究の中心は技術的でした。サービス拒否攻撃の可能性が明らかになり始めたため、プロトコルとアプリケーションに対する新しい攻撃を探すのに忙しかったのです。  
 2020年までに、測定基準に関するはるかに多くの作業が行われます。実際に起きている邪悪さを測定し、これを政策論議だけでなく法執行機関にも取り入れます。  
さらに読むインターネットセキュリティに関する初期の古典は、スティーブベロビンとビルチェスウィックによって書かれ、アヴィルビンが第2版[221]に加わっています。  
 BGPのセキュリティについては、2011年のENISAレポートを参照してください。モンティは200ページを超えるページであり、PhDinネットワークセキュリティを始める人向けに設計されていますが、エグゼクティブサマリーも短くなっています[1906]。  
認証局のエコシステムの概要についてはよくわかりません。  
 MicrosoftとNetscapeの最初の目標は、世界中のWebで電子商取引を飛躍的に開始することでした。証明書の使用は、パスワードとソフトウェアの更新に広がり、Javascriptが登場すると、同じ起源の原則が信頼をWebサイトに移しました。  
 技術的なセキュリティ目標と法的目標の間、および監査人と規制当局の間には矛盾があります。  
 詳細については、エコシステムの問題[1785]に関するRyan Sleeviのプレゼンテーションは、技術的および運用上の現在の問題とその背景を掘り下げたいと考えている人々に多くの指針を提供します。