男が長すぎると、眠りに落ちる可能性が高いからです。  
  
–トーマスカーライル  
  
現在、ほとんどのセキュリティエンジニアは電子システムに重点を置いていますが、物理的な保護は無視できません。  
第2に、電気工学またはコンピュータサイエンスの背景を持つ人に、物理的なセキュリティの基礎を他の方法よりも教える方が簡単であるため、物理的保護と論理的保護の相互作用は、通常、管理するシステム担当者次第です。  
情報に基づいた、しかし外交的なアドバイスを提供できる必要があります。  
第5に、最近の多くの機械式ロックは、簡単な隠れた手法である「バンピング」によって完全に危険にさらされています。彼らの製造業者はしばしば彼らの製品が素早く迂回されることを可能にする脆弱性に気づいていないようです。  
 または、機械部品とデジタル部品の統合が不十分なため。  
施設周辺の犯罪発生率をどのようにして減らすことができるかについては、犯罪学と建築学から役立つアイデアがあります。これらのいくつかは、システム設計にも行き渡ります。  
たとえば、盗難警報器を倒すには、警報を停止するか、警備員に信頼性がなくなったと説得するだけで十分です。  
機密性を維持するために設計された軍事メッセージングシステムや記録の真正性を維持することを目的とする簿記システムを見てきたように、監視は信頼できる可用性が必要なシステムの典型的な例を示しています。  
、またはそれが私に言ったのは誰でしたか（したがって、信憑性は大きな問題ではありません）  
歴史的に、コンピュータセキュリティ研究の約90％は機密性について、約9％は信頼性について、1％は可用性についてでした。  
そして何よりも、可用性について教えてくれるのは警報システムです。  
13.2脅威と障壁  
あなたは顧客と合意した基準に従ってそれを評価します。これは、2019年に銀行本部の建物に、5年間のメンテナンスコスト、建物のソフトウェア侵入テスト、およびセキュリティポリシーを規定する仕様があることを意味する場合があります[350]。  
次に、1層以上のバリアとセンサーを備え、偶然の侵入者を排除し、故意の侵入者を検出し、迅速に侵入するのを困難にします。  
バリアには、許可されたスタッフが出入りできるドアがあるので、金属製のキーから生体認証スキャナーまで何でも可能である入り口制御があります。  
たとえば、施設のマネージャーが家族を人質に取られた場合、どのように対処しますか？  
セキュリティの運用面を企業の文化に組み込む必要があります。そうしないと、うまく機能しません。これは、コンピューターの種類だけでなく、物理的なセキュリティにも当てはまります。  
これが、情報セキュリティの専門家として、物理的な側面にも注意を払わなければならないもう1つの理由です。  
13.2.1脅威モデル  
また、ある状況で次々と目にするように、セキュリティはスカラーではありません。  
」という文脈なし：「誰に対して、どの環境でセキュリティを確保しますか？  
•デレクは19歳の中毒者です。  
•チャーリーは40歳で、強盗の7つの有罪判決には不十分です。  
あまり知性はありませんが、彼は狡猾で経験豊富です。彼は内部の呪文の間に多くの「伝承」を拾いました。  
•ブルーノは「紳士犯罪者」です。  
カバーとして、彼は小さなアートギャラリーを運営しています。  
 壁に美術史の大学の学位、そして18年前の強盗の有罪判決。  
彼は自分の過去を知っている諜報機関のために時折「ブラックバッグ」の仕事をしました。  
•Abdurrahmanは12人のエージェントのセルを率いており、そのほとんどが軍事訓練を受けています。  
Abdurrahman自身は、軍事アカデミーで280人のクラスの3番目に来ました。  
彼の機関と政府が考えている可能な任務の1つはプルトニウムを盗むことです。  
したがって、デレクは未熟で、チャーリーは熟練しており、ブルーノは非常に熟練しており、クリーナーなどの未熟練のインサイダーの助けを借りているかもしれません。  
（最近の多くのテロリストがかろうじてチャーリーのレベルにあることは事実ですが、チャーリーがあなたが心配しなければならない最高級の攻撃者であると仮定して、原子力発電所を設計することは賢明ではありません。社会学者はデレクに、犯罪学者はチャーリーに、軍はアブドゥルラフマンに焦点を当てていますが、私たちの関心は主にブルーノにあります。  
しかし、銀行やコンピュータルームの物理的な防御は、ブルーノを念頭に置いて設計される傾向があります。  
13.2.2抑止  
可能であれば、アセットを匿名で目立たなくすることをお勧めします。  
場所は重要です。一部の地区は他の地区よりも犯罪がはるかに少ない。  
所有者が目に見える警報を設置するだけであるならば、彼らは彼らの隣人に犯罪を再分配するかもしれません。しかし、隣に送られるだけでなく犯罪者を捕まえる目に見えない警報は、近隣全体の犯罪を阻止することができます。  
多くの車にロジャックがある町では、車の泥棒がすぐに捕まり、部品のために盗まれた車を解体する「チョップショップ」が閉鎖されます。  
同じことが不動産にも当てはまります。多くの家が警官を静かに呼ぶ高級警報器を持っている近所は、強盗が働くのに危険な場所です。  
しかし、それだけではありません。  
犯罪学者や建築家は、どのデザインが犯罪を多かれ少なかれ可能にするかを知ったので、これの多くは低所得住宅の文脈で進化しました。  
1972年、オスカーニューマンはこれを「防御可能な空間」の概念に発展させました。建物は居住者の「領土とコミュニティの潜在的な感覚を解放する」べきです[1435]。  
同時に、レイジェフリーは、社会学ではなく心理学に基づいたモデルを開発し、したがって、個々の犯罪者間の幅広い違いを考慮に入れています。それは私たちの4つの「モデル」悪役に反映されます。  
ジェフリーの「環境設計による犯罪防止」は効果があり、抑止力に関する昔ながらの多くのアイデアに挑戦しています。  
歩道や駐車場を見下ろす窓のある、文明化された正面の方がよいでしょう。  
活動が頻繁に行われるピクニックシートのある共有エリアは、より大きな抑止効果があります。  
。  
たとえば、CCTVカメラは、1つの出口がある駐車場などの施設でのみ犯罪を抑止することがわかっています[766]。  
手すりが透けて見えるように、手すりは壁よりも優れたバリアを作成できます。  
もう1つの影響力のあるアイデアは、ジョージケリングとキャサリンコールズの壊れた窓の理論です[1029]。  
したがって、問題がまだ小さい場合は修正する必要があります。  
ニューヨークのささいな犯罪と深刻な犯罪の両方が激減しました。  
関連する一連のアイデアは、ロナルドクラークの状況犯罪防止理論にあります。  
その焦点は主に、製品から、日常生活からの犯罪の設計にあります。実用的であり、アプリケーションによって駆動されます[440]。  
このような実証研究は、社会学のバックグラウンドを持つ犯罪学者によって「理論」が不足していると批判される可能性がありますが、影響力を増しており、セキュリティエンジニアが行うことからそれほど離れていません。  
このフレームワークは、必要に応じて他のトピックへの環境制御の拡張に自然に対応します。  
少なくとも、それは従来のアプローチでした。しかし、それは最後の言葉ではないかもしれません。  
これにより、物理的なセキュリティコストのほか、システム管理者の給与や電力を節約できます。  
13.2.3壁と障壁  
最初のタスクは、実際に保護しようとしているものを特定することです。  
したがって、1980年代までに、哲学は「彼が見ることができるすべての現金を彼に与える」ことに移行しました。  
1997年に、スターバックスは、3人の従業員が荒廃した強盗で射殺された事件の後、物理的なセキュリティを見直しました。  
副次的なメリットは、顧客サービスの改善でした。  
車のキーをベッドサイドのテーブルの上に置くのではなく、家の正面玄関のすぐ内側に置いていく人が増えていることに気づきました。  
 第2に、保護目標を決定したら、どのような目的で、どこにどのような境界または境界を設定するかを決定する必要があります。  
しかし、ありふれた脅威を犠牲にして、まれではあるが「刺激的な」脅威に焦点を合わせるのは誤りです。  
このため、NIST、建設業者ハードウェア製造業者協会、保険業者研究所、およびその他の国の同等の組織には、壁、屋根、金庫などのテスト結果と標準が多数あります。  
通常の建築資材では、それほど大きな遅延はありません。ハンマーで空洞のレンガの壁を1分足らずで通り抜け、正面玄関に施した錠の高さに関係なく、SWATチームはドアをバタリングラムでヒンジから外します。そのため、データセンターや銀行の金庫などの設計者は、鉄製のドアフレームを備えた鉄筋コンクリートの壁、床、屋根を好みます。  
イギリスの最大の強盗では、2015年にハットンガーデンの安全な預金会社の20インチのコンクリートの壁に穴を開けた高齢の犯罪者のギャングが、ダイヤモンドを1400万ポンド売り上げました。  
ロック、金庫、金庫室を認証する組織は、攻撃ツールについて時代遅れの仮定を行うことが多いことに注意してください。  
典型的な銀行の金庫室は、10分間の攻撃に耐えることが認定されていますが、地元の消防署は、最新のアングルグラインダーを使用して2分で通過できます。  
もう1つの問題は、ほとんどのバリア材料をすぐに突き破る熱ランスまたはバーニングバーです。安全なエンジニアは、そのようなものを使用して、組み合わせが失われたボールトに侵入します。  
したがって、障壁を単独で見ることはできません。  
  
近年、錠前業界は、多くの低コストの機械式および電子式ロックの脆弱性を露呈した開発によって深刻に動揺しています。  
この技術により、多くの機械式ロックを迅速に開くことができ、今ではすぐに利用できるツールを使用して、熟練していない人が損傷することもありません。  
。  
図13.1：–切断可能なピンタンブラーロック（提供：Marc Weber Tobias）  
通常、各スタックは2つまたは3つのピンで構成されています。  
正しいキーが挿入されると、各スタックの一番上のピンと一番下のピンの間の隙間がプラグの端に揃い、せん断線が作成されます。これでプラグを回すことができます。  
実際の数は、機械的な公差とキーカットの制限のため、少なくなります。  
詳細については、MITロックピッキングマニュアル[1896]、またはマークウェーバートビアス[1891]による論文などをご覧ください。基本的な考え方は、テンションレンチを使用してプラグを少しひねり、ピンをロックピックで操作することです。それらがすべてせん断線に沿って並ぶまで。  
。  
新しい発見は、攻撃者が特別に作られたバンプキーを挿入できることで、そのそれぞれの歯は最も低いピン位置に設定され、その肩はわずかに丸みを帯びています。  
 侵入者は、指先でキーをわずかなねじれの下に置き、ゴム槌でキーヘッドを軽くたたくことができます。  
正味の効果は、マレットを数回タップするだけで、ロックを開くことができることです。  
これは、ロックピッカーのオープン組織（TOOOL）のバリーウェルスとロップゴングリジプによって書かれた2005年のホワイトペーパーによって公表されました。  
。  
専門家の見解は、深刻な結果を招く可能性のある突発的なデスクルのロックピッキングである[1892]。  
オランダの論文とその後の宣伝は軍拡競争を開始し、ベンダーはより複雑なデザインを作成し、アマチュアの鍵屋はそれらの多くに衝突攻撃を報告しました。  
彼らはそれを愛しています！ほぼすべての金属ロックが壊れています。  
、および銀行の最も重要な暗号化キーが保持されているハードウェアセキュリティモジュールを保護するために使用されました。  
Medecoは、キーに切り込みが入れられる角度でセカンダリキーイングを使用します。  
2005年、メデコはm3を導入しました。このm3にも、キーの側面に切り込まれたスライダーの形のシンプルなサイドバーがあります。  
世帯主は何ができますか？  
車で1時間以内に店頭で見つけられた唯一の高セキュリティ製品は、イスラエルのブランド変更されたMul-T-Lockデバイスであることが判明しました。  
そして次に知性のバックグラウンドを持つ誰かが私たちを訪ねたとき、彼はイギリスでは麻薬の売人だけがそのような錠をかけたと述べた。警察が通り過ぎると、私は容疑者として彼らのデータベースに行き着くかもしれません。  
私のホームセキュリティのこの疑わしい改善には、標準製品の20ポンドに対して、200ポンドの費用がかかりました。そして実際には、泥棒は常に窓を破る可能性があるので、私たちの実際の保護は、鉄器よりも私たちの場所と犬に依存しています。  
最も効果的な抑止力は、警報や運転中の車などの占有の目に見える兆候でした[1709]。  
。  
どのロックの設計が衝突に抵抗するかについての知識は存在しますが、それを探す必要があります。  
 したがって、購入者はレモン市場に直面します–とにかく、ほとんどのロックベンダーのマーケティング資料の光沢、ふわふわ、技術的コンテンツの欠如から疑われるかもしれません。実際、Tobiasによる最近のセキュリティアラートは、最も人気のある高セキュリティデッドボルトの1つが、狭いドライバーをキー溝に滑り込ませ、ボルトを最後に留めて、それを回すことで、ロック内の広範なセキュリティ保護を破らなくても機械的にバイパスできることを明らかにしました。  
多くの高セキュリティインストールでは、同様のハードウェアを採用しています。  
これらはしばらくの間、鍵屋にも知られていましたが、改良され、Matt Blaze1によって公開されました。  
より複雑なスキームが一般的です。たとえば、私たちの建物では、システム管理者やクリーナーが私のドアを開ける間に、生徒のドアを開けることができます。  
したがって、上部ピンと下部ピンの間に1つのカットがあるピンの代わりに、一部のピンスタックには中央ピンもあります。  
私のキービッティングが557346で、廊下のマスターキーが232346であるとします。  
論文は[259]です。  
それは機能しません。  
2は最初のピンの有効なビットであるので、これはロックを開き、ユーザーのビット5とは異なるため、そのピンのマスターキーのビットであることがわかります。  
したがって、マスターキーイングは、建物の居住者だけでなく、深刻な強盗にも非常に便利です。  
この攻撃に対抗するマスターキーイングシステムがあります。たとえば、オーストリアのロックメーカーEvvaには、複製が非常に難しい金属キーに埋め込まれた磁石を含むシステムがあります。  
機械的なマスターキーイングシステムの大きな頭痛の種は失効です。  
彼らは自分の鍵のコピーを切り取って、攻撃者に売ったのかもしれません。  
ここではマスターキー攻撃が重要であり、多くの高価なピック耐性のあるロックが実際に問題を悪化させています。  
サイドバーは、建物内のすべてのロックで同じであることがよくあります（マスターキーシステムでは、マスターキーを共有するロックに共通のサイドバーが必要です）。  
したがって、図11.3のように、悪人が私の生徒の1人が所有する本物のキーの写真を撮ることができれば、それをバンプキーに変えて、私のドアを開くことができます。  
しかし、それは間違いなく、攻撃者が襲撃の計画に2年間を費やす可能性のある銀行、金塊のディーラー、宝石商のためのものです。  
したがって、機械式ロックは1つに簡単に変更できますが、1つの建物に何百ものロックを統合するシステムでは、泥棒を敷地外にロックするよりも、建物の所有者をロックベンダーにロックしてしまう可能性があります。  
ツールと知識が広がるにつれ、チャーリーのようなキャリア犯罪者はほとんどすべての家の鍵を法医学的な痕跡を残さずにすばやく開くことができ、ブルーノやアブドゥラマンのようなより専門的な攻撃者はほとんどの商業施設でも鍵を開けることができます。  
サーバールームやその他の資産の物理的な保護があなたの責任に含まれている場合は、それらについて検討を開始します。  
13.2.5電子錠  
彼らは長い間使用されてきました–ホテルは1970年代からカードロックを使用しています。  
それらの多くはさまざまな方法でバイパスすることができ、この本のほとんどの章は、設計、評価、および保証に何らかの方法で適用できます。  
 コンポーネント;しかし、錠前、暗号、電磁メカニズムをシームレスに連携させることは困難です。あなたがそれらをテストするまで、あなたは決して言うことができません。  
しかし、ロックを使用して大規模で複雑な建物を保護する大企業の観点からは、問題はロック自体ではなく、特に世界中に数十または数百の建物がある場合に、建物内の数十または数百のロックをどのように管理するかです。 。  
理想的な世界では、誰がどのドアをリアルタイムで通過したかを知っており、これを情報のセキュリティポリシーに合わせることができます。たとえば、分類された材料が処理されている場合、適切なクリアランスのない部屋に誰かがいると、アラームを鳴らすことができます。  
電子システムは完全に、またはほとんどの場合オンラインであり、取り消しをはるかに容易にします。  
しかし、それは長い道のりになります。  
あるビルドプロジェクトで、ベンダーのプロトコルが理想的に使用したいキットをサポートしておらず、独自のエントリーコントロールシステムをゼロから構築する時間も人もいませんでした。。  
ロックインの主な制限は、システム全体のリッピングと交換のコスト、つまり独自のケーブル接続です。  
同じ組織によって運営されている他の建物がこのシステムを使用し、時刻の関数であるより複雑なアクセス制御ポリシーを許可しました。  
。  
その後、NXP Semiconductorsから販売されているカードシステムであるMifare Classicに対する攻撃が見つかりました。  
Mifare Classicには、弱い乱数ジェネレーターや、エラーメッセージを介してキーストリームマテリアルをリークするプロトコルなど、他のフローがありました。  
Mifare Classicは、2007年にKarsten Nohlと同僚によって部分的にリバースエンジニアリングされました[1450]。ナイメーヘンのフラビオガルシアと同僚は翌年に仕事を終え、チップの完全な分析を公開し、オランダのすべての公共交通機関のチケットで使用されているバージョンがどのように破壊されるかを示しました[747]。  
これらの攻撃によるMifareへの影響は、運送システムに侵入検知システムを配備して、料金ドジャーを検出させることでした。入場管理システムへの影響は、カードキーの複製が容易になったことです。  
さらに、巧妙な攻撃者は偽のロックを配備し、それを通過した人の鍵をコピーする可能性があります。  
非接触式リーダーを胸の高さで保持するコーヒーカップに入れて、ストラップに留めておく人の鍵を複製することもできます。  
あるベンダーは、ロックをホテルにほぼ原価で販売し、1ドルで交換用のカード在庫を販売することで利益を上げることを考えました。  
NXPは、カードにデジタル署名を追加した製品で応答しました。これにより、鍵は弱いキーでしたが、本物の弱いキーであることがロックに通知されました。  
1つ目は、弱いCrypto 1暗号を引き続き使用しながら、初期の攻撃を容易にする実装ミスを修正した「強化された」クラシックカードでした。しかし、根底にある暗号が弱いため、これらも破られました[1316]。  
しかし、デビッド・オズワルドとクリストフ・パールは、即座にDESファイアへのタイミング攻撃を発見しました[1484]。  
 およびBluetooth（NFCチップをApple Payに固定するApple製の電話用）  
他の人は、セクション4.3.1で述べたUWB無線の新しい802.15.4z標準などの新しいテクノロジーを採用しています。  
これによって作成された外部性の一部は、より多くのアラートカードリーダーベンダーによって捕捉されました。  
これが、CISOのセキュリティエンジニアリングチームが物理的なセキュリティにも関心を向ける必要があるもう1つの理由です。  
13.3アラーム  
それらのアプリケーションの範囲は、スーパーマーケットの冷凍庫の温度の監視に及びます（したがって、スタッフは家に持ち帰るための食料を与えられることを期待して冷凍庫を「誤って」オフに切り替えません。）  
ただし、強盗やサーバールーム、銀行の金庫室、アートギャラリーの保護のコンテキストでそれらについて説明すると便利です。  
アラームを作成するための基準は、国によって、またリスクの種類によって異なります。  
私自身の専門的な経験は、現金自動預け払い機に組み込まれたアラームから、宝石店などの大きなリスクのために警報システムで使用される通信のセキュリティまで、銀行のコンピューター室を保護するために使用されるシステムにまで及びました。  
。  
これには、貴重なオブジェクトを保護して表示するという興味深い設計上の問題があります。  
映画脚本家のブルーノに対する見方は、市庁舎の建築計画をじっくりと見つめながら、アラームに対する狡猾な攻撃を組織しているというものです。絵画を盗む方法（1）  
彼は絵をつかみ、床に触れることなく後ろに登り、盗難を依頼した裕福なギャングから支払われました。  
現実はより単純で見知らぬものです。  
  
警報システムを設計する際のよくある間違いは、最新のセンサー技術に魅了されることです。  
現代科学は驚異的ではありませんか？  
これで、Bosunの椅子のチャップが検出されます。  
 それは簡単です。  
 ブルーノは観光客としてやって来て、ほうきの戸棚に隠れています。  
オフはアラームを鳴らしますが、それでなんと！ 1分も経たないうちに、バイクに乗ることになります。  
アラームが建物の入口制御とうまく統合されることはほとんどありません。  
深刻な物理的セキュリティは、人々に対する深刻なコントロールを意味します。  
クレデンシャルには、体重や手の形状などのデータが含まれていました[1747、1751]。ドアを開けたままにしておく人たち。  
（最新テクノロジーへの過度の依存のタイタニック効果は、多くの場合、人々を常識から見えなくします。）  
上で述べたように、物理的保護システムにはいくつかのステップがあります。抑止–検出–アラーム–遅延–応答であり、その重点はアプリケーションごとに異なります。  
Abdurrahmanが核分裂性物質を盗もうとする可能性がある種類のターゲットでは、攻撃はほぼ確実に検出されます。主な問題は、海兵隊が到着するまで彼を遅らせることです。  
したがって、注意深く調べて、より大きな問題が検出、遅延、または応答のいずれであるかを判断する必要があります。  
13.3.2センサーの敗北  
ほとんどのセンサーは回避できます。  
センサーの適切な組み合わせを設計するには、スキルと経験が必要です（後者は常に前者を保証するとは限りません）  
日付が少し古い場合でも、センサーの取り付けに関する基準は[408]です。  
超音波は、セントラルヒーティングインレットなどの移動する空気の近くでは十分に機能しませんが、交通状況によって振動検出器が役に立たなくなることがあります。  
一部の場所では、通常の天候でさえ保護を困難にする可能性があります。侵入者がセンサーを越えて（さらにはフェンスを越えて）滑走できるサイトをどのように防御しますか  
 しかし、アラスカとアリゾナのどちらにいても、保護されているオブジェクトに近づくほど、より厳密に環境を制御できるため、達成可能な誤警報率が低くなります。  
しかし、警備員がそこに到着するのに十分な時間侵入者を遅らせるために、外周は正確に信頼できるセンサーが必要な場所です。  
 したがって、ブルーノの次の攻撃は、暗くて嵐の夜を待つことです。  
または、アラームが本物だったことを示す他の確固たる証拠を残します。  
警備員は出てきて何も見つけません。  
今回は警備員は気にしないので、彼は行きます。  
これらは、アラーム応答部隊に対するサービス拒否攻撃です。  
故意に引き起こされる誤警報は、24時間体制の警備員がいないサイトに対して特に効果的です。  
、彼らは、警報会社または別のキーホルダーがチェックするためにそこにいるまで、もはやスクワッドカーをそこに送りません。  
それらが気象条件や交通騒音などの環境刺激によって引き起こされる割合は、効果的に展開できるセンサーの感度を制限します。  
一般的な戦略は、リモートビデオ監視を第2の防御線として持つことです。これにより、顧客の施設は警備会社のディスパッチャーによって検査できます。多くの警察は、このようにして確認された警報を優先している[979]。  
攻撃者は、同じ通りにある他の建物の照明を無効にしたり、火災を起こしたり、警報を発したりすることができます。  
交通と天候の後、ブルーノの次の味方は時間です。  
したがって、深刻な物理的保護を必要とするサイトには、多くの場合、周囲にいくつかの境界があります。次に、センサーを埋め込んだ芝生、赤外線バリアを備えた内側のフェンス、そして最後に、騎兵がそこに到着するまで悪者を遅らせるのに十分な大きさの建物。  
ほとんどのサイトでは、この種の保護は高すぎるでしょう。  
良い例は、アラームを設置する理由がなかったネイルサロンなどの店舗と壁を共有している小売店を標的としたフロリダの宝石泥棒の集団から来ています。  
とにかく、センサーと物理的バリアの組み合わせは、まだストーリーの半分に満たない。  
13.3.3機能の相互作用  
これらの中で最も明白なのは電気です。  
あまり明白でない相互作用は、火災警報と消火です。  
 ブルーノは観光客としてギャラリーを訪れ、タイマーに煙の手榴弾を置きます。  
（そうでない場合、警報ディスパッチャーは、トラックを現場に運ぶことに集中するため、とにかくそれらを無視します。）  
彼はおそらく一般的な混乱の中でなんとか逃げることができるでしょうが、もし彼がそうでなかったら、彼は火を見て公共の意欲的な傍観者であり、町の貴重な文化遺産を保存するために命を危険にさらしたといつも主張することができます。  
史上最大の強盗–ドレスデンのGr¨uneGew¨olbeからの約10億ユーロに相当する宝物の盗難、アウグストゥスザストロングの宝庫の本拠地、その他数十の貴重な骨董品の部屋が放火された[469 ]。その警備員は最終的にCCTVへの侵入者を見て、警察に電話をかけましたが、間に合うように到着しませんでした。  
原子炉では通常、爆弾が発見された場合、サイトは封鎖され、誰も出入りできません。火災が発生した場合は、スタッフの多くを避難させる必要があるという火災安全規則（さらに、おそらく地元住民の一部も）  
これは、爆弾が爆発した場合にどの規則が優先されるかという興味深い問題を提起します。  
多くのサーバールームには自動消火器があり、これは二酸化炭素で溢れることを意味します。  
窒素ダンプはそれほど壮観ではありませんが、致命的でもあります。酸素レベルの低下は、CO2レベルの上昇のようにパニック反応を引き起こしません。  
  
高度な攻撃者は、少なくともセンサーと同じくらい通信を攻撃する可能性があります。  
絵を盗む方法（5）  
彼はその夜に戻って自分を助けます。  
2006年2月、ケント州トンブリッジにあるSecuritas Cash Managementデポからの英国最大の強盗事件で、強盗はマネージャーと彼の家族を人質に取り、警察官になりすました。  
私が1980年代に銀行で働いていたとき、私達は彼らの家族が人質に取られるのを防ぐためにコントロールがそこにあることを私たちのキャッシュセンターのマネージャーに説明するように気をつけました。  
有能なディフェンダーを備えた価値の高いサイトでは、アラームの保守とテストは1人ではなく2人で行うように要求しています。  
英国で4番目に大きい強盗事件で、暫定IRAは2004年12月にノーザンバンクで2人のキーホルダーを誘拐し、家族を銃を突きつけて翌日に銀行のベルファスト本部に連れ込むよう強制しました。  
もう1つのエッジケースは刑務所システムです。このシステムでは、センサー、ケーブル、および建物の構造そのものへの攻撃が頻繁に行われるため、継続的なテストと検査のプログラムが不可欠です。  
」と「私を奪うことを決めた組織で少数のスタッフが働いていた場合、どうしたらよいでしょうか？」  
アラームセンサーとコントローラー間の通信を保護する昔ながらの方法は物理的でした。各センサーに複数のワイヤーを敷き、それらをコンクリートに埋め込むか、装甲ガス加圧ケーブルを使用しました。  
では、どうやって攻撃するのですか？  
 ブルーノは、彼らの警報を扱う警備会社から来たと主張してライバルのギャラリーに電話をかけます。  
 後輩のオフィスはそうするのに役立ちます。ボックスのシリアル番号が通信を保護する暗号キーでもあることを認識していません。  
これは、そうでない場合でも「すべて順調」を報告し続けます。  
さまざまなアラームコントローラを偽装するブラックボックスが長年にわたって報告されています。  
ニュージャージー州ハッケンサックにある倉庫を保護する警報システムが遮断されました。  
また、セクション13.2.3で、イギリスの最大の強盗がどのようにしてアラーム信号を妨害したかについて述べました。  
ただし、セキュリティプロトコルのトレーニングを受けていないエンジニアが設計を行ったため、設計に欠陥があることがよくあります。  
。  
失敗のさらに頻繁な原因は、全体的な設計の失敗です。  
これは、注文書、請求書、および多くの人が見ることのできるその他の書類によく表示されます。  
これにより、「スパイク」されたものを入手する可能性も低くなります。  
 おそらく、あなたはおそらくアートギャラリービジネスに参加しないことに決めたでしょう。  
これが、盗難警報システムに対する最も強力な攻撃です。  
 センサーを対象とするのではなく、通信に使用します。  
 ブルーノは電話線をライバルのギャラリーまで切り、数百ヤード離れた茂みの中に隠しています。  
2つの数値が等しい場合、カストディアンが言った「まあ、私たちは朝に修正します」、またはそのための言葉は、かなりの推測です。  
これは多かれ少なかれ銀行の金庫室を攻撃する標準的な方法であり、コンピュータのインストールでも使用されています。  
（これが、フェンスをガタガタ音を立てるよりもはるかに強力な理由です。）  
彼らはこの機会を利用して、アメリカの販売業者からLucien Piccardの腕時計を盗みました。卸売価格は210万ドル、小売価格は800万ドルでした。  
3番目に、悪役が電話交換を爆破し、ロンドンのジュエリークォーターにある数十のショップへのサービスを中断しました。電話からブロードバンドへの移行は何も変わっていません。 BT電話回線を切断する代わりに、イギリスの泥棒はBT Openreach DSL回線を切断します。これは同じ銅片ですが、デジタル信号を運ぶようになりました。  
さらに、アラームサービスは多くの場合ブロードバンドプロバイダーと提携しており、センサーを提供する企業は、洗練された何かをするインセンティブがない低コストのボリューム市場で競合しています。  
地元の電話交換所の近くですべてのアラームを鳴らすのではなく（警察でそれを押しつぶすことである程度保護することができます）  
これには、警察の通信や4Gネットワ​​ークへの攻撃が含まれる可能性があります。これらは有線よりも多くの警報通信に使用されているためです。  
長年にわたり、ロンドンの保険市場におけるルール（世界の主要な再保険事業のほとんどを行っています）  
従来のアプローチは、有線通信を使用する1つのアラームと、セルラー無線を使用する1つのアラームでした。 2019年までに、2つの異なる4Gラジオサービスを使用する製品が登場します。  
原子力の世界では、IAEAの規制により、プルトニウムが500gまたはU-235が2kgを超えるサイトには、警報制御センターと施設内に武装した対応部隊の両方が必要であると規定されています[949]。  
あなたと世界をつなぐ1本の繊維が縁石のジャンクションボックスを通過する場合、8インチのコンクリートの壁と屋根を用意しても意味がありません。  
それでも、知識のある相手がホスティングセンターを引き出す最も簡単な方法は、通常、その通信を切断することです。  
クラウドスケールで運用していない場合は、自問してみてください。誰が掘りたいのか、誰がどこにいるのかを知っていますか、そしてそれらをすぐに検出しますか？  
銃器の私的所有が広まっている国では、射手について計画を立てる必要があります。  
13.3.5教訓  
明白な理由よりも多くの理由があります。  
金属製の鍵を写真に撮ったり、3Dプリンターで偽造したり、昔ながらのファイルを作成したりすることもできます。彼らが開くロックは、しばしばぶつかることがあります。  
したがって、アラームは重要です。  
侵入者アラームは、適切な知識と経験を提供します。  
•もう1つは、最も外側の境界の防御は、最も信頼したいものであるが、最も信頼性が低い防御でもあるという観察です。  
•警備員に警戒を怠らないようにすることは、特にほとんどすべての警報が誤報である仕事では大変です。  
彼らは、スクリーナーをシフトごとにチェックポイントごとに数回テストした場合、脅威の約20％しか通過しないことを発見しましたが、1回だけテストすると60〜75％に上昇します[713]。  
犯罪作家が間違っていると考えるものだけでなく、実際に何が悪いのかを知る必要があります。  
警報産業の経験が関連する他のアプリケーションがあります。  
  
セキュリティエンジニアは、物理的な保護だけでなく、コンピュータや暗号化システムにも対処する必要があります。  
「スマートビルディング」への移行とは、エネルギー管理などと統合された入室管理、警報、システムセキュリティを意味します。  
この章では、注目に値するいくつかのことを強調しました。  
次に、ロックは思ったほど安全ではありません。  
最も一般的な製品は1990年代に米国の輸出規制によって侵害され、多くのカードキーシステムも脆弱です。それらをより良いものに置き換えるプロセスは、業界の構造とインセンティブによって妨げられています。  
第3に、すでにかなり自動化されている物理的セキュリティの1つの側面、つまりアラームから学ぶべきことがたくさんあります。  
他の状況でサービス拒否攻撃を処理するときに、それらはいくつかの有用な洞察を与えることができます。  
情報と物理的なセキュリティの境界を探索する人によって、新しい研究課題が見つかることを期待しています。 2020年にプレスを開始する際に浮上した例は、音響サイドチャネルの使用です。  
間違いなく、この種の結果はさらに増えるでしょう。  
これを、他の複雑なエコシステムが主要コンポーネントのセキュリティ障害にどのように対応したかと比較すると、興味深いかもしれません。  
低レベルのメカニズムについては、組み込みシステムのキーを管理するための優れたツールで対処できます。  
 そして、非常に多くの異なるサービス会社がすべての有能な対戦相手がコピーを持っていると想定されなければならない計画にアクセスできるという意味で、スマートビルディングは最終的にオープンになるでしょうか？すべての請負業者は喜んでISO 27001の認証を取得していると主張しますが、ビッグデータの侵害まで所有しているほとんどすべての企業もそうです。  
特定の国のリソースは、米国産業安全保障協会[45]などの業界団体を通じて、または地元の保険業界を通じて入手できることがよくあります。多くの国には、米国のUnderwriters 'Laboratories [1916]などの非営利団体があり、製品、設備、またはその両方を認証する計画があります。  
最新のセンサー技術に関する研究論文は、IEEE Carnahan会議[952]に掲載されています。