– FRANCIS BACON最大の欠点は、私が言わなければならないことですが、どれも意識しないことです。  
1はじめに今日、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、電気工学や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教える方が他の方法よりも簡単なので、物理的保護と論理的保護の間のやり取りは通常、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。  
 5番目に、最近の多くの機械式ロックは、簡単な隠れた手法である「バンプ」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。  
物理的なセキュリティの多くは単なる常識ですが、いくつかの自明ではないひねりがあり、技術には最近大きな進歩がありました。  
 そして、盗難警報装置に関する非常に興味深い事例研究があります。  
2。  
 これにより、サービス拒否攻撃に対する新しい視点が与えられます。  
 私の銀行の金庫室に強盗がいる場合、私は他に誰と知り合うのか（したがって、機密性については心配していません）、または誰が私に言ったのか（それほど真正性は大きな懸念ではない）をあまり気にしません。しかし、私に教えようとする試みが妨害されないように、私は非常に気にします。  
 実際の攻撃と企業の情報セキュリティへの支出は、正真正銘と機密性を組み合わせたものよりも可用性に費やされるため、多くの場合その逆になります。  
13。  
 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が5年間の維持費、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設定する仕様を持ってい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配置し、偶然の侵入者の侵入を阻止し、意図的な侵入者を検出し、侵入が困難になるようにします。  
バリアには、許可された駅が出入りできるドアが付いているので、金属製の鍵から生体認証スキャナーまで何でも可能である入口制御があります。  
 たとえば、ファシリティ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？前述したように、従業員がデュアルコントロールを受け入れ、それらを職場の文化に統合する方法の1つは、これらのコントロールがそれらを保護することです。資産を保護するだけでなく  
 物理ドメイン、ビジネスドメイン、情報ドメイン全体で統一された運用セキュリティを確保することも重要です。悪意のある人物がシステムに誤った配達注文をこっそり持ち込み、宅配業者を選んでピックアップする場合、1億ドルのダイヤモンドを含む金庫を​​保護するために1,000万ドルを費やす意味はほとんどありません。レセプションからダイヤモンドをアップ。  
2。  
13。  
1脅威モデル重要な設計上の考慮事項は、攻撃者のスキル、装備、および動機のレベルです。  
 コンテキストなしで「デバイスXは安全ですか？」と尋ねることは意味がありません：「誰に対して、どの環境で安全ですか？」「国際標準の強盗」がない場合、私が知っている最も近い作業分類が開発されたものです米陸軍の専門家による[173]。  
 彼は次の修正のために売ることができるものを盗むためのリスクの低い機会を探しています。  
彼は過去25年のうち17年を刑務所で過ごしました。  
 彼は小さな店や郊外の家から盗み、地元のフェンスに売ることができると思っているものは何でも持って行きます。  
 彼のビジネスは主にアートを盗むことです。  
 彼は壁に（偽造された）大学の学位を取得しておらず、18年前に強盗の有罪判決を受けた。  
 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、軍事学校で280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が、アブドゥラマンは非常に熟練しているだけでなく、かなりのリソースを持っています。  
 （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する必要がある最高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、私たちの懸念は主にブルーノにあります。  
2。  
 しかし、銀行やコンピューター室の物理的な防御は、ブルーノを念頭に置いて設計される傾向があります。  
2。  
 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の場合、彼らは隣人に犯罪を再配布するかもしれません。しかし、犯罪者をすぐ隣に送るのではなく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。多くの家が警察を静かに呼ぶハイグレードな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の可能性を多かれ少なかれ可能にするかを学んだので、これの多くは低所得者向け住宅の文脈を発展させました。  
 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。建物は住民の「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、RayJe↵eryは社会学ではなく心理学に基づいたモデルを開発し、したがって個々の提案者間の幅広い差異を考慮に入れました。それは私たちの4つの「モデル」悪役に反映されます。  
Je↵eryの「環境デザインによる犯罪防止」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。  
2。  
 ピクニックシートのある共用​​エリアでは、活動が頻繁に行われ、抑止効果が大きくなります。  
 アクセスも重要です。防御可能なスペースには単一の出口ポイントが必要です。これにより、潜在的な侵入者がトラップされるのを恐れます。  
 通過する車両を使用して現場の視認性を高めることから、窓の下にイバラの茂みを植えることまで、長年にわたって開発された多くのトリックもあります。  
 これらに関するアドバイスは、[324]などの最新の標準にあります。  
 彼らは、修理されていない壊れた窓が建物にある場合、すぐに破壊者がさらに壊れ、おそらくは不法占拠者の麻薬の売人が入居するだろうと述べました。ごみが歩道に残っていると、最終的には人々がゴミを捨て始めます。  
 ケリングは、破壊された地下鉄の清掃を支援するコンサルタントとして雇われ、公共の酒飲み、スキーヤーの男性、その他の迷惑行為を取り締まった警官のウィリアムブラットンのゼロトレランス運動に影響を与えました。  
犯罪学者たちは、この落ち込みがゼロトレランスに起因したのか、それとも人口統計[1151]や持ち込み権[1188]などの他の同時変化に起因したのかについて、まだ議論しています。  
これはJe↵eryとNewmanの研究に基づいており、単なる財産犯罪ではありません。それは一般的にリスクとエフォートを高め、報酬と挑発を減らし、言い訳を取り除くことによって犯罪を減らすための多くの原則を提案します。  
 特定の脅威の詳細な調査が含まれます。たとえば、車の盗難はさまざまな問題であると考えられています。たとえば、未成年者の喜び、夜間に家に帰るための盗難、海外での車の解体や販売のためのプロのギャング集団による盗難などです。これらの脅威には、まったく異なる対策が最も効果的です。 。  
 この本で説明されているメカニズムの多くは、アプリケーションレベルの機会削減のフレームワークに簡単に適合します。  
 したがって、標的型攻撃に対する防御策としてホスティングセンターの匿名性を計画している場合は、それらの前提がどこにあるかを知っている人の数をどのように制限するかについて考える必要があります。  
 多くの企業が完全にサードパーティのクラウドサービスに移行しており、ホスティングセンターはもうありません。  
セキュリティエンジニアリング438ロスアンダーソン13。  
 脅威と障壁13。  
3壁と障壁Derek orCharlieがサイトに侵入しようとするのを阻止するために使用する環境機能と、Brunoが侵入するべきサイトを見つけるのをどのように困難にするかを決定したら、問題が発生します。物理的な障壁の設計。昔、銀行は強盗のために本当に厳しい生活を送るために長い時間を費やしていましたが、これには限界があります。強盗は常に顧客を撃つと脅すことができます。  
この哲学は他の小売業にも広がっています。  
彼らは金庫を店長から店の正面に移動することを決め、これらの金庫を、駅、顧客、通行人だけでなく、CCTVを介して制御室にも目立つようにしました。  
 新しい設計は、多くの米国の場所でテストされ、売り上げの増加と損失の削減により、良好な投資収益率が得られました[505]。  
誰かがあなたの車を盗むために夜に家に侵入した場合、あなたは本当に彼らを手にした戦闘に従事させたいですか？2番目に、あなたの保護目標を決定した後、あなたはあなたが持つであろう境界または境界を決定しなければなりません目的と場所。  
 しかし、ありふれた脅威を犠牲にして、珍しいが「エキサイティングな」脅威に焦点を合わせるのは間違いです。  
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。  
 通常の建築材料は、それほど大きな遅延はありません。ハンマーで空洞レンガの壁を1分足らずで通り抜け、正面玄関にかけた高価なロックに関係なく、SWATチームはバタリングラムでヒンジのドアを壊します。  
 したがって、データセンターや銀行の金庫室などの設計者は、鉄筋コンクリートの壁、床や屋根、鋼製のドアフレームを好んで使用しています。  
 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あけた高齢の犯罪者の集団が、1400万ポンドのダイヤモンドを売り出しました。  
セキュリティエンジニアリング439ロスアンダーソン13。  
 脅威と障壁ロック、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想定を行うことが多いことに注意してください。  
 典型的な銀行金庫は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。  
 障壁は孤立して見ることはできません。  
13。  
4機械式ロック近年、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、錠前業界は深刻な混乱を引き起こしています。  
 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、今すぐ入手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はありません。  
1）。  
図13。  
 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。  
 MechanicalSecurity Engineering440Ross Anderson13のため、実際の数は少なくなります。  
 脅威と障壁許容範囲とキーカット制限。  
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Marc Weber Tobias [1891]による論文などを参照してください。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軽くねじってから、ピンをすべてロックピクンティルで操作することです。せん断線に沿って並べます。  
 最近まで、ロックピッキングは、投資銀行や大使館などの高価値のターゲットに対してのみ脅威であると一般的に考えられていました。  
 （このようなキーは、すべての歯が最も低い位置、つまり噛み合い、つまり9番にあるため、「999」キーとも呼ばれます。  
 衝撃によりピンが上方に跳ねます。加えられたねじれにより、スプリングが押し下げられたときにそれらがくっついてしまいますが、シリンダーエッジにギャップがあります。  
このトリックは何年も前から知られていましたが、より優れたツールとテクニックにより、より効果的になりました。  
 TVの取材により、メッセージが幅広い視聴者に広まった。  
 たとえば、米国の国内市場の70％でピンタンブラーがロックできるように、米国のメールボックスのロックは簡単に開けられることがわかっています。私たちの研究室にはロックピッキングキットが用意されているので、学生はオープンな日も一緒に遊ぶことができます。  
 私が銀行で働いていたとき、Medecoからのロックは取得できないと考えられ（そのように認定されていても）、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ていました。  
 Medecoは、キーに切り込みが入れられる角度で二次キーイングを使用します。  
 2005年に、Medecoはm3を導入しました。これは、キーの側面に切り取られたスライダーの形の単純なサイドバーも備えています。  
世帯主は何ができますか？実験として、私は自分のフロントドアロックを交換しました。  
 インストールを2回試みて、初めて妨害しました。その後、家族がより複雑なデッドボルトを使用する方法を学ぶのに約1週間かかりました。  
 不注意に操作すると、脅威とバリアが開きません。  
 錠がすり減った。数年後それはstickingopenを始めました、そして私がそれを取り外したとき、私はいくつかのボールベアリングが出てきたことに気付きました。  
 確かに、Yochanan Shachmuroveらは、コネチカット州グリニッジの居住者を調査し、予防策に応じて、国内の強盗がどのように変化しているかのモデルを構築しました。ロックやデッドボルトシャッドは、ウィンドウなどのエントリの代替手段が常にあったため、本質的に影響を与えません。  
商業企業の状況は少し良くなっています（しかしそれほどではありません）。  
30、ピッキングとドリルへの耐性を指定しますが、バンピングへの耐性は指定しません。そして、耐ピックロックは一般的にバンプするのがより困難ですが、これは保証ではありません。  
 （トビアスの論文、およびwww。  
orgは良い出発点です。  
 そして、高価な耐ピックロックでさえ、多くの場合、ビルダーやOEMによる設置が不十分です。 Medecoロックを備えた暗号化プロセッサに侵入しなければならなかったとき、ホワイトメタル製のカムが回転し、レバーを開けようとすると簡単に曲がることに気づきました。  
この設計は20年以上前から存在しており、脆弱性は開示前は製造元に知られていませんでした。  
最近の2番目のクラスの問題は、マスターキー攻撃です。  
 マスターキーシステムは、建物の各ドアの個別キーに加えて、それらをすべて開くトップレベルのマスターキーが存在できるように設計されています。たとえば、クリーナーが使用できます。  
 ピンタンブラーロックでは、このようなスキームは、一部のピンスタックに余分なカットを設けることで実装されます。  
マスターキー攻撃は、余分なカットを1つずつ検索することです。  
 興味深い回答がありました：「数日間、私の電子メールの受信トレイには鍵屋からの熟練者がいっぱいでした。そのほとんどが私が独り言だということを言っていました。この方法は公開するには危険すぎるので、私は無責任だと指摘しました。」  
セキュリティエンジニアリング442ロスアンダーソン13。  
 脅威と障壁a噛み応えのある157346のキー、そしてロックで試してください。  
 次に、最初の位置を257346まで下げます。  
 私は各ピンに対して平均4つのビッティングを試す必要があります。3つのピンがマスターキーである場合、約12のテスト後にマスターキーを取得します。  
 メタルキーがまだ残っているほとんどの大規模な商業施設ではマスターキーイングを使用するため、これは重要です。  
 しかし、ほとんどのフィールドシステムは脆弱であるように見え、3D印刷の発明によりさらに脆弱になっています。  
 キーホルダーは去ります、そして、不正直であるか不注意であるかもしれません。  
 または、誰かが自分のキーの写真を撮り、それを使用してコピーを印刷した可能性があります。  
 それらは、サイドバーなどの2次キーイングメカニズムに依存することがよくあります。キーは、図11に示すように、2つの通常のピンタンブラーキーが溶接されたように見えます。  
 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には、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）。  
3。  
 しかし、それは間違いなく、攻撃者が襲撃の計画に2年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組み込んだシステムでは、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るようになります。サーバールームやその他の資産の物理的な保護を含む責任がある場合は、それらについて検討を開始します。  
2 –サイドバーロックのキー図11。  
2。  
2。  
 彼らは長い間利用されてきました–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。  
 このようなロックは、単純な金属製のロックやカードロックよりも費用がかかるだけでなく、興味深い方法で失敗することがよくあります。彼らへの攻撃に関する文献はすべてある[1839、1291]。  
新しい建物では、複数のセンサーを使用し、物理的なアクセス制御と論理的なアクセス制御を統合することで、誰がどこにいるかを認識し始めています。  
 建物はオブジェクトだけでなく人も監視できます。このラボでの実験では、人とデバイスの両方が位置追跡用のアクティブなバッジを持ちます[1982]。  
 セキュリティポリシーを適用するだけでなく、スマートビルディングは、照明を回してエネルギーを節約することや、居住者の存在に合わせて空調を調整することなど、他の利益をもたらす可能性があります。  
私が働いていた1つの組織で判明した実際的な問題の1つは、大規模な進入管理システムを販売している企業が数社しかなく、カスタマイズが難しいということです。  
 レガシーエントリーコントロールベンダーは、他のシステムハウスと同じように機能します。彼らは、錠前から（経済的ではなく）ロックインから収益を得ています。  
ロッキーニの主な制限は、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。  
 同じ組織が運営する他の建物は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。  
 組織は、セキュリティエンジニアリング444ロスアンダーソン13に期待していました。  
 脅威と障壁は、適切な価格のドアロックなどの適切なシステム統合を可能にする種類のコンポーネントを入手できれば、より完全な電子システムに間に合います。  
 これは、Crypto-1と呼ばれる独自の暗号を使用しました。その鍵は、私が26で議論した1990年代の暗号戦争中に課された輸出規制の結果として48ビットに制限されていました。  
7。  
 主に輸送の発券に使用されますが、何万もの建物の設置ベースもあり、いくつかの主要な建物の入場管理ベンダーによってサポートされていました。  
NXPは裁判所にこの調査を抑圧するよう求めましたが、失敗しました。  
 鍵を一時的に所有している適切な機器を持っている人なら誰でも、従来のメタルキーと同じように作業コピーを作成できます。  
 これには、建物のすべてのロックを開くキーを持つクリーナーと、会社のすべての建物のすべてのロックを開くキーを持つセキュリティパトロールステーションが含まれます。  
一部のロックベンダーはひどい打撃を受けました。  
Mifareのブレイクは、台湾の競合他社が互換性のある株を数セントで売り、ビジネスモデルを破壊する可能性があることを意味しました。  
共通のsta↵カードで運営されているMifarelocksを使用している数十の建物を持つ組織の結果は、より安全なロックに移行するには、すべてのロックとカードを一度に交換するか、NXPに固執する必要がありました。カード。  
 2番目の製品ラインでは、DESキーカードなど、より優れたアルゴリズムを使用しました。たとえば、2キーのトリプルDESを使用しました。  
 この問題は、複数の製品ラインに対応できるカードリーダーの製造を開始した起業家的なロックベンダーによって部分的に軽減されました。 Mifareだけでなく、NFC（Androidフォンの場合）とBluetooth（Apple製の電話機の場合、NFCチップをApple Payに固定する）にも対応します。  
15。  
3。  
セキュリティエンジニアリング445ロスアンダーソン13。  
 警報要するに、NXPは顧客を新製品に移行することにより、ある程度のコストをかけてロックインの多くを維持することができました。  
しかし、全体の分野は、建築家または建築サービスマネージャーであった従来のロック購入者にとっては、非常に複雑になりました。  
13。  
それらのアプリケーションは、スーパーマーケットで冷凍庫の温度を監視すること（つまり、持ち帰り用の食料が与えられることを期待して冷凍庫を「偶然」に切り替えないでください）から、しばしば侵入者が罠にかけられる危険なゾーンの即席爆発装置に至るまで、さまざまです。 。アラームは、ゲームから電子戦争までのあらゆる問題である、サービス拒否攻撃のより広範な問題の根拠にもなります。  
 ロックと同様に、この種の作業には通常、専門の会社を使用します。ただし、技術的な問題に注意する必要があります。  
サーバールームのアラームは、（少なくとも部外者による）改ざんから十分に保護されています。  
 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。  
 ブルーノに対する映画脚本家の見方は、市庁舎の建築計画をじっくりと見て、アラームへの巧妙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）ピカソは「最新の状態」のギャラリーから盗まれますカーペットの下のプレッシャーマットをアクティブにしないように、ダースのルーフィングタイルを取り除き、ロープを下に降ろした泥棒によるアートの警報システム。  
マスコミはこの種の仕事を愛しており、それは時々起こります。  
 脅威のシナリオを体系的に見ていきましょう。  
3。  
3。  
 保護されたオブジェクトの周りをループできる光ファイバーケーブルや、ケーブルが100 nm未満（1万分の1ミリ）しか伸ばされなかったり緩んだりすると警報が鳴る光ファイバーケーブルなど、市場には多くの印象的な製品があります。  
 それは、ボスーン様式のチャップを検出します。  
絵を盗む方法（2）ブルーノは観光客として来て、ほうきの戸棚に隠れます。  
 O↵は警報を出しますが、それでなんと！ 1分も経たないうちに、彼はバイクに乗ります。  
アラームが建物の入口制御と統合されることはめったにありません。  
 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。  
 信任状には、体重や手の形状などのデータが含まれていました[1747、1751]。  
さらに、アラーム応答プロセスは、多くの場合、十分に検討されていません。  
）したがって、アラームメカニズムを単独で考えてはなりません。  
 対戦相手がデレクまたはチャーリーである場合、私たちは主に抑止力に関心を持ちます。  
 ブルーノは、彼を締め出すために費やす軍事予算がないため、最も興味深い事例であり、防御側がアブドゥルラーマンよりもブルーノを心配している施設がたくさんあります。  
セキュリティエンジニアリング447ロスアンダーソン13。  
 警報13。  
2センサーの敗北強盗警報は、次のようなさまざまなセンサーを使用します。•振動検出器、フェンスの外乱、足音、ガラスやその他の建物や周辺への攻撃、•ドアと窓のスイッチ、•体の熱を検出するパッシブ赤外線デバイス、•モーション超音波またはマイクロ波を使用した検出器;•マイクロ波または赤外線ビームの目に見えないバリア;•カーペットの下の圧力パッド。極端な場合、床全体に広がり、各タイルの下に圧力トランスデューサーがあります。•ビデオカメラ、最近では動き検出器、さらには自動的にアラームを発する、または監視センターにライブビデオフィードを提供するディテクターに直面します。•地震計を介した単純なタイダウンケーブルから光ファイバーのループに至るまで、機器の動きセンサー。  
 フェンス外乱センサーは、フェンスをアーチ型にすることで無効にすることができます。非常にゆっくり動くことによるモーションセンサー;壁を突破することでドアと窓のスイッチ。  
 センサーの取り付けに関する基準は、日付が若干古い場合でも[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、振動検出器は、トラフィックによって役に立たなくなる可能性があります。  
 一部の場所では、通常の天候でも保護が困難になる可能性があります：侵入者がセンサー（さらにはフェンス）を滑走できるサイトをどのように防御できますか？2しかし、アラスカとアリゾナのどちらにいても、保護対象のオブジェクトに近づくほど、環境をより厳密に制御できるという主要なジレンマ。それにより、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だけ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。  
 HesetsはCCTV2に巻き込まれないように注意しながらアラームをなんとかします。アスノーゾーンの原子力発電所の侵入者検知の有益な作業例については、[173]を参照してください。  
3。  
 数百ヤード離れて茂みに隠れます。彼は30分待ってから再び警報を設定します。  
誤警報–故意に引き起こされたかどうかに関係なく–は業界の悩みの種です。  
 電子戦の経験では、約15％を超える誤警報率はレーダーオペレーターのパフォーマンスを低下させます。そして、ほとんどの侵入者アラーム応答は、このしきい値をはるかに超えて動作しています。  
多くの警察は、特定のサイトからの特定の数の誤警報（通常は1年に3〜5回）の後、警報会社または別のキーホルダーがチェックするまで、そこにクワッドカーを送りません。  
 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によって検査されます。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に照明を無効にしたり、火災を起こしたり、警報を設定したりできます。  
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、境界がいくつかあります。酔っぱらいや野生生物を入れないための外側のフェンス。次に、埋め込みセンサーで芝生を水平にし、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巨大な建物です。  
ほとんどのサイトでは、この種の保護は高すぎます。  
 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、センサーと物理的なバリアの組み合わせは、まだストーリーの半分以下を占めています。  
3。  
3。  
これらの中で最も明白なのは電気です。  
 それほど明白ではない相互作用は、火災警報と消火です。  
 それは朝に1つでオフになり、火災警報を設定します。これにより、盗難警報がパッシブ赤外線センサーからの信号を無視します。  
）ブルーノは火の出口を通り抜け、ピカソをつかみます。  
 警察は彼を信じていないかもしれませんが、彼を有罪にするのは難しいでしょう。  
 近くの建物の敷地にある火災により、地元の変電所が無効になり、地元の街灯と博物館の電源がオフになりました[1045]。  
火災と侵入の相互作用は常に困難です。  
 これは、爆弾が発射された場合にどのルールが支配す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、これは多くの場合、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。  
13。  
4通信の攻撃高度な攻撃者は、センサーと同じくらい通信を攻撃する可能性が高いです。  
3。  
絵を盗む方法（5）Brunoはアートギャラリーに入り、状況が混乱している間、窓のスイッチからワイヤーを切断します。  
また、あなたの従業員の1人またはクリーナーが買収され、誘惑者が強要されて脆弱性を作成する可能性もあります。  
 彼らはそれから彼にそれらを入れるように強制し、£53,116,760を取りました。 5人の強盗が捕まったと投獄されたが、他の強盗は脱出し、お金のほとんどは回収されなかった。  
 知識が豊富で意欲的なディフェンダーがいることは素晴らしいことですが、デュアルコントロールの防御は徹底的に実行する必要があります。  
 それでも、特に対戦相手がブルーノではなくアブドゥラマンである場合は、デュアルコントロールでは必ずしも十分ではありません。  
 テロリストは26ポンドで脱出した。  
 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、テストと検査の継続的なプログラムが不可欠です。  
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いて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、どのようにそれらを攻撃しますか？絵画を盗む方法（6）Brunoは、警報を処理する警備会社から来たと主張するライバルギャラリーに電話をかけます。ブルーノは同じコントローラを200ドルで購入し、ライバルの電話回線に接続する機能的に同じユニットを持っています。  
セキュリティエンジニアリング451ロスアンダーソン13。  
 アラーム偽のアラーム機器、またはそれを模倣するコンピューターの代用は「スプーフィング」として知られています。  
 1981年には、泥棒は$ 1で稼いだ。  
 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停止しました。  
 そして、セクション13で言及しました。  
3英国最大の強盗は、警報信号の妨害を伴いました。  
 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。  
そうでない場合でも、ブルーノは疑似ランダムシーケンスを記録して少しゆっくりと再生できるため、月曜日の早朝までに5分の「スラック」が蓄積されて雷撃をカバーできた可能性があります。  
 1つは、暗号鍵をデバイスのシリアル番号と同じにすることです。  
 （アラームコントローラを現金で購入することをお勧めします。  
 しかし、大企業はしばしばこれを行うのが困難です。  
 しかし、私は最後まで最善を尽くしました。  
 これは（3）の変形ですが、センサーを対象とするのではなく、通信に使用します。  
 彼は到着した青い制服を着た男性の数と出発した数を数えます。  
 彼は数時間働くことができることを知っています。  
 手口は、単にトラックを電話会社の縁側のジャンクションボックスに入れ替えるだけでなく、異なる施設で複数の警報を同時に発生させて地元の警察を圧倒しようとする高度な試みまでさまざまです。  
）1つのケースでは、ニュージャージーの泥棒が3つの主要電話線を切断し、3つの警察署とハッケンサックメドウランズの何千もの家庭や企業で電話と警報装置をノックアウトしました。  
3。  
100万卸売り、おそらく800万ドル小売り[861]。  
 3番目に、悪者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何十ものショップへのサービスを妨害しました。  
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。これは銅と同じ部品ですが、現在はデジタル信号を伝送しています。  
 さらに、アラームサービスはブロードバンドプロバイダーと提携していることが多く、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。  
 ローカルの電話交換機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によってある程度保護することができます）、同じアラーム会社によって監視されているすべてのアラームを数千に設定することが可能かもしれません。応答チェーン内の他のコンポーネントを攻撃する。  
 脆弱なコンポーネントの数を最小限に抑える1つの方法は、アラーム通信を匿名にして、サービス拒否攻撃を標的にできないようにすることです[1423]。  
従来のアプローチは、有線通信を使用するアラームと携帯電話を使用するアラームでした。 2019年までに、2つの異なる4g ra-dioサービスを使用するサービスが見られます。  
2。  
 核の世界では、IAEAの規制により、500gを超えるプルトニウムまたは2kgのU-235を含むサイトには、警報制御センターと施設内の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]。  
 世界にあなたをつなぐ単一の繊維が縁石のジャンクションボックスを通っている場合、8インチのコンクリートの壁と屋根があることにはほとんど意味がありません。  
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、コミュニケーション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、自分で考えてみてください。誰が掘りたいのか、どこを知っているのか、そしてそれらをすぐに検出できるのでしょうか？職場–配偶者かどうか、元セキュリティエンジニアリング453ロスアンダーソン13。  
 アラーム従業員または顧客。  
13。  
5教訓学習者は依然として、本質的にコンピューターシステムのセキュリティについての本が、壁、錠、警報システムを説明する数ページを費やすべき理由を尋ねるかもしれません。  
•ほとんどのロックは無効にできます。  
 カードキーは、あなたが近くにいることができれば、しばしば複製することができます。•サービス拒否攻撃への対処は、多くの安全なシステム設計の最も難しい部分であり、多くの場合最も重要です。  
•非常に一般的な教訓の1つは、抑止から検出、警報、遅延、応答まで、システム全体を見なければならないということです。  
•ミスアラームレートと誤アラームレート（レシーバーの動作特性）の間のトレードオフも、セキュリティエンジニアリングの一般的な問題です。  
 典型的な例は空港でのスクリーニングで、物理的に、またはX線装置のソフトウェアを使用して、米国運輸保安局がテストガンをスーツケースに入れます。  
•脅威モデルを理解していない-チャーリーのために設計し、ブルーノを排除することを望んでいる-ことは、多くの現実の失敗を引き起こします。  
•そして最後に、重要な作業は常に亀裂の間に落ちるので、セキュリティ工学プロジェクトの技術的な側面を専門の下請業者に任せることはできません。  
 後の章で、改ざん防止プロセッサに侵入しようとする試みを検出し、すべての暗号化キーマテリアルを破壊することによって応答するように設計された耐タンパープロセッサについて説明します。  
4。  
4SummarySecurityのエンジニアは、物理的な保護だけでなく、コンピューター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年代に米国の輸出管理によって侵害され、それらをより優れたものに置き換えるプロセスが業界の構造とインセンティブによって妨げられているため、多くのカードキーシステムも脆弱です。  
第3に、物理セキュリティの1つの側面、つまり、かなりよく自動化されたアラームから学ぶべきことはたくさんあります。  
 他のコンテキストでサービス拒否攻撃に対処するときに、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。  
 私は、情報/物理的セキュリティの境界を探索する人々によって、新しい研究課題が見つかることを期待しています。私たちが2020年にプレスするつもりで浮上した例は、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ているかと比較するのは興味深いかもしれません。  
4。  
 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より優れたツールで対処できます。  
参考資料警報システムに関する古典的なリファレンスは[173]ですが、一部のシステムの問題は[1423]で説明されています。  
 ロックバンピングと関連トピックの進捗状況については、Tooolグループ、Marc Weber Tobias、およびMatt Blazeを監視します。マットはまた、安全なクラッキングについて書いています[261]。  
 最後に、核兵器管理条約の遵守を監視するために使用されるシステムは、[1748]に記述されています。