管理は、アルゴリズムがないものです。  
–ロジャーニーダム  
市場は資本主義の発明ではありません。  
それは文明の発明です。  
  
14.1はじめに  
また、自宅の前払いユーティリティメーターから前払いの郵便料金ラベルを介して、一部のメータリングシステムの値をオンラインで購入することもできます。  
彼らは長い道のりを戻ります。  
彼の検査官はこれらを時々読み、顧客に使用料を請求しました。  
チケットは、交通機関のチケットからスポーツイベント、クーポンまで、膨大です。私の発券のケーススタディは、ガスと電気に使用される前払いメーターです。  
これらの中で最もよく知られているのはタクシーメーターかもしれませんが、これらは電話アプリに置き換えられているので、主にタコグラフについて説明します。銀行のトラックの出入りを記録します。  
4つ目は、手紙や小包をあざけるのに使用される電子切手メーターです。  
私たちは、デフォルトのパスワードなし、暗号鍵の保護、更新可能なソフトウェア、攻撃対象領域の最小化など、通常の母性とアップルパイの要素をレイアウトするETSI標準草案EN 303 645などのIoTセキュリティの一般的な標準の始まりを持っています。ユーザーが個人情報を削除できるようにする[640]。  
この章のケーススタディで、必要なコンテキストに関する洞察が得られることを願っています。  
メーターはさらに微妙です。  
。  
タクシーの運転手は、メーターが実際に働いた時間よりも多くのマイルまたはより多くの分を読み取ることを望んでいる可能性があるため、過剰測定に操作する場合があります。  
ユーティリティの消費者は、メーターが通過する電気やガスの一部を無視することを望みます。  
このような場合、監視の対象により、デバイスが誤った読み取りを行うか、単に失敗する可能性があります。  
多くの計測および監視システムも証拠に関係しています。  
 または、他の誰かがそうしたと偽って主張することによって。  
。  
郵便局は主に、大量の郵便をシステムに滑り込ませるために郵便局員に賄賂を贈る曲がったダイレクトマーケターなどの卸売詐欺の阻止に関心があります。  
  
ユーザーがトークンの1か所で支払いを行うシステムは数多くあります。マジックナンバーでも、磁気ストリップ付きの段ボールチケットでも、QRコードを表示するアプリでも、充電式のチップカードでも、保存された値を使用します。何処か別の場所。  
主な保護目標は通常、トークンが大規模に偽造されるのを防ぐことです。  
すべてのトークンを一意にし、すべてのデバイスをオンラインにすると、このような詐欺を防ぐことができます。  
したがって、リプレイと偽造の検出は時々オフラインで行われる必要があります。  
私たちのオプションは何ですか？  
フリーライダーは地下鉄の駅でバリアをジャンプできます。電気メーターには、バイパススイッチを配線できます。  
収益を最大化するには、ささいな詐欺は少なくとも少し不便である必要があり、さらに重要なことに、チケットを大規模に偽造しないようにするメカニズムが必要です。  
南アフリカの300万世帯を電化するプロジェクトについて相談できたのは幸運だったので、これを選択しました（ネルソンマンデラが政権を握ったときに作成した中央選挙の誓約）  
この作品は、[93]で詳細に説明されています。  
学んだ教訓のほとんどは、他の発券システムに直接適用されます。  
14.2.1ユーティリティメータリング  
。  
この技術は後発開発途上国、特に南アフリカによって推進され、そこではタウンシップを電化することが国家の優先事項となった。多くの家が非公式に建設され、所有者は住所さえ持っていなかったため（信用格付けはもちろん）  
ネルソンマンデラの大統領任期中に200万メートル以上が設置され、現在では約1,000万メートルが使用されています。  
一般的な先進国では、福祉に従事している、または裁判所に対して判決を下しているため、前払いメーターを使用している世帯の約10％がいる可能性があります。  
南アフリカのメーターのほとんどはマジックナンバーを使用しています。  
トークンは実際には1つ以上の命令であり、メーターに固有のキーを使用して暗号化され、「メーター12345 – 50KWhの電力を分配します！」のようなものです。クレジットがなくなると、メーターは供給を中断します。特別なトークンを使用して価格を変更できます。電力会社が昼間と夜で異なる料金を請求する場合、メーターは相対価格と料金が変更される時間の更新が必要になる場合があります。  
前者はSTS標準を使用しませんが、消費パターン、改ざんの試みなどを電力会社に報告できます。  
現在、ほとんどのEU諸国のすべてのメーターを、無線リンクを介して測定値やその他のデータを報告し、リモートで前払いモードに設定できるスマートメーターに置き換えるプロジェクトがあります。  
後で戻ってきます。  
 前払いは、発展途上国が何百万もの家をすぐに電化できる唯一の方法でした。  
追加の利点は、省エネです。  
  
前払いメーターのセキュリティ要件は簡単なようです。  
通常の戦略は、各トークンを一意のメーターに結び付けて、誰かが2つの異なるメーターで同じマジック番号を使用できないようにし、シリアル番号または乱数を使用して各トークンを一意にして、同じトークンが同じメーターで2回使用しないでください。  
各メーターには、自動販売機からの指示を認証するための暗号キーがあります。  
近隣のマスターキーである販売キーKVがあり、各メーターには販売キーの下でメーターIDを暗号化することによって導出されたデバイスキーKIDがあります。第4章のロットアクセスデバイスで、すべてのトークンがローカルで購入される場所で機能します。  
英国では、電力業界の規制緩和により、数十の電力会社が発電機から電力を購入し、共通のインフラストラクチャを介して家庭に販売しているため、メーターは異なる料金体系の複数の電力会社間の所有権を変更します。  
そこで、メーターを「所有」している販売ステーションから別のステーションに顧客のメーターキーを送信し、ATMネットワークのように、バランシングと決済のために反対方向に販売データを渡すプロトコルから始めました。  
このサーバーは700万人の顧客に直接販売されており、ATMやショップなどの約10,000のオンライン販売ポイントを介して販売されています。  
私たちは、30戸の住宅を供給する可能性のあるフィーダーメーターの読み取り値と、それらの住宅のトークン販売額を比較します。  
調査チームのリードソースとして、また簿記システムの統計チェックとして使用できますが、それはそれだけです。  
このような「ゴーストベンダー」を排除することは、通常、すべてのローカルメーターのキーを変更することを意味します。犯罪組織によって運営されている盗まれた機械がまだいくつかあります。  
残高は販売のたびに減分され、現金が預金された場合にのみ再度クレジットされます。次に、運営会社は、クレジットを使用してチップをリロードするマジックナンバーを送信します。  
ただし、戦略的な方向性は一元化であり、再販業者の管理の労力と費用を節約し、事業者はオフラインの自動販売機を、中央サービスからリアルタイムでトークンを取得するオンライン自動販売機に置き換えました。  
14.2.3何がうまくいかない  
広大な気温範囲は別として（米国の大陸と同様に南アフリカでも変動）  
メーターが落雷によって破壊されたとき、顧客は不満を述べ、まだ使用されていないと述べた価値の信用を得ました。  
トークンスロットの下の回路が破壊された場合、メーターの1種類は無制限のクレジットを提供するため、サービス拒否攻撃は十分に機能し、人気を博しました。  
ソウェトの子供たちは、電圧低下（220ボルトから180ボルトへの電圧の低下）があったときに、特定の種類のメーターが最大のクレジットに達したことに気付きました。  
ブラウンアウトテストが指定されていなかったため、このバグは取り上げられませんでした。  
100,000メートルを引き抜いて再度ROM化する必要があったため、担当会社はほぼ破産しました。  
メーターの1つのメーカーは、指定された量の電気を販売していませんでしたが、そのような速度で非常に多くの電気を販売しています。  
もう1つは払い戻しを許可しましたが、払い戻しされたトークンのコピーは引き続き使用できます。  
他の場所と同様に、実際のセキュリティ違反は、偶然に発見され、非常に日和見的な方法で悪用されたバグや失敗に起因します。私たちが[93]で書いた他の教訓は、次のとおりです。•マーケティングチャネルを管理している限り、前払いは安価で簡単ですが、コンビニエンスストア、銀行、スーパーマーケットなどのサードパーティを通じてトークンを販売しようとすると、費用がかかり、複雑でリスクを伴う可能性があります。 •最初にセキュリティインフラストラクチャを正しく取得しないと、通勤をサポートするために遠隔地の店舗でメータートークンを販売する必要がある場合と同様に、セキュリティインフラストラクチャを変更するとコストがかかる可能性があります。 •可能であれば、テクノロジーをリサイクルします。バグが少なくなる可能性があります。  
通常、1人の専門家だけではすべての問題を網羅することはできません。 •長時間のフィールドテストが絶対に必要です。  
最初の展開後の数年間に学んだ主な教訓は、スケーラブルな詐欺を設計することでした。  
そのため、前払いは古き良き監査、エネルギーのバランスと検査の必要性を完全になくすわけではありません。また、発展途上国における地方の腐敗やより広範な州の占領の問題も完全に解決するわけではありません。  
しかし、1つの妥協案が私たちをかむために戻ってきました。  
現在、ほぼ100か国に6,000万メートルあるため、各顧客にロールオーバーを管理するための特別なキー交換チケットを提供するためにユーティリティに数億ドルの費用がかかることになります。  
 したがって、新しいシステムを設計するときは、持続可能性について考えてください。「このシステムは今後30年間問題ないでしょうか。  
’恥ずかしくなるほど長生きするかもしれません！  
2000年代初頭、メーター業界はスマートメーターのアイデアを販売し始めました。これは、中央サーバーにリアルタイムで通信できるメーターであり、リモートで読み取ることができます。  
自動検針（AMR）  
;後者には双方向通信があるため、コマンドをリモートでメーターに送信できます。  
公益事業に売却された利益には、請求コストの削減と借金の回収の容易さが含まれています。  
市場関係者は「スマートグリッド」について話し、メーターが家庭用電化製品を制御し、リアルタイムの関税を市場と交渉できることについて興奮して話しました。  
メーターベンダーにとってのメリットは、15ドルで50年間続く製品を、少なくとも50ドルで15ほど続く製品に置き換えることでした。  
研究者は最初に、公益事業に行く細かい消費データに関する一般的なプライバシーの懸念を提起しました。メーターが分単位または秒単位で消費を監視するように設定されている場合、ユーティリティは、家にいるとき、食事をするとき、シャワーを浴びるとき、および寝るときの人数を計算できます。  
これにより、測定の時間の細かさ、およびメーターに保持する必要のあるデータの量についての議論につながりました。120桁のトークンの66ビットにすべてを合わせる必要がありました。追加の31年を取得すると、1つの単位ではなく2分の時間単位を意味し、1つのメーターに対して複数のトークンを同時に販売することが難しくなります。  
対中央。  
これは国家安全保障局による争奪につながった。  
公益事業は大量のエネルギーを売ろうとしていますが、政府はそれを節約してピーク需要を減らしたいと考えています。  
 先駆者はイタリアで、2001年にユーティリティENELがスマートメーターの設置を開始しました。  
スマートメーターにより、デフォルト設定者はリモートで前払い制度に切り替えることができました。  
スマートグリッドの概念は、2007年のエネルギー独立および安全保障法で米国の政策となり、オバマ大統領が米国の回復および再投資法の主要な指標として45億ドルを開発に割り当てたとき、強力に注目を集めました。欧州議会は2009年に加盟国に2012年までにスマートメータリングの経済評価を実施することを要求する法律を採用し、彼らがそれが有益であると判断した場合、2022年までに使用を義務付けます（2020年までに80％採用）  
現在、多くの国が、米国または地方のスマートメータープログラムを開始しています。これには、米国のユーティリティが多数あり、成功例もいくつかあります（スペインなど）。  
。  
メーターが配電網のオペレーターに属しているか、小売業者に属しているかは、歴史的な事故の問題です。スペインでは、電力会社はバイヤーのカルテルをセットアップし、すべてのサプライヤーのメーターが他のすべてのサプライヤーのヘッドエンドと連携することを主張したため、e50メートル未満の商品ハードウェアのコストがかかりました。  
インセンティブには深刻な問題があります。スマートメーターがエネルギーを節約することで自己採算をとるのであれば、小売業者の管理下に置くことは意味がなく、エネルギー販売を最大化して利益を最大化します。  
英国は残念ながら先を耕しました。  
据え置きなく、彼らはコスト、利益、電力価格、金利に関する仮定を拡張し、2009年に肯定的な評価を行い、英国に電力だけでなくガス用のスマートメーターの導入も約束しました[883]。  
ニュージーランドではスマートメーターをオプションにしており、計算は大きな家でのみ価値があります。  
州は73の地方配電会社に対処し、すべての検針を収集する中央システムを構築し、小売業者や規制当局が利用できるようにしました。  
2005年に作成されたオンタリオ州の費用便益分析（大臣がプロジェクトを発表した翌年）  
全体として、エネルギー計画は非常に貧弱で、州は最終的に米国に余剰電力を販売し、ミシガン州とニューヨーク州のユーティリティに数十億ドルの助成金を支給しました。  
歴代政府（労働、連合、保守派）  
私の考えでは、エネルギーを節約せずに200億ポンドを浪費し、実際の節約をもたらす可能性のあるより優れたプロジェクトに取って代わることは、あなたが得ることができるのと同じくらいグリーンではありませんでした。  
（プロジェクトは2009年に人々がスマートフォンを使い始めたのと同じように始まりましたが、代わりにアプリの使用に切り替えるには厳格すぎました。）  
第2世代メーターの国家標準に同意するまでに何年もかかり、配備されたメーターシートのほとんどは、互換性のない古いモデルで構成されています。ベンダーは何年にもわたって自社の特許を取得するために戦っていましたが、当局には技術知識や政治的支援がありませんでした。  
プロジェクトの失敗を露呈すると脅迫し、おそらくコストが110億ポンドから230億ポンドに増加した内部告発者は、刑務所で脅迫されました[919]。  
さらに、顧客がサプライヤーを切り替えたときにメーターの70％が機能を失いました（適正な価格を得るために毎年行う必要があるため）。  
政府が全員を第2世代メーターに移動するという宣言された戦略に従っている場合、これらすべての古いものを交換する必要があります。 2019年11月のレポートによると、新しいメーターはわずか2.3mでした。  
エネルギー節約については、兆候はありません。  
 請求以外の目的でデータを使用する人はいません。  
メーターメーカーは2000年代後半に大きなマーケティング活動を行っていましたが、デマンドレスポンスを作成して測定を改善することにより、グリッドを安定させるのに役立つメーターについて息をのむような話がありました。  
発電容量がコア伝送ネットワークに接続された大型のスピニングマシンから、より広い配電システムに組み込まれた数十万の風車やソーラーパネルに移行するにつれて、グリッドは実際に壊れやすくなっています。  
 安全限界を超える周波数の変化率が発生し、さらに負荷が制限され、低電圧およびさらに負荷制限が発生しました。  
要点は、変電所レベルでもスマートメーターが必要なことではなく、システムに慣性が必要なことです。つまり、バッテリーや同期コンデンサを購入する必要があります。  
2019年の停電をめぐるイギリスの政治的怒りの多くは、ロンドンの通勤者が電車に何時間も停車していたことから来ました。  
彼らを再び連れて行くには、ラップトップを持った技術者の訪問が必要でした2。  
スマートメーターが役に立った場所はありません。  
たとえば、スタンバイディーゼル発電機を所有していて、稼働するかどうかを確認するために毎月30分稼働させる必要があるデータセンターのオペレーターは、必要なときに発電機を始動するための支払いを受けています。  
最終的には、電気自動車の充電器も、十分な数になると、これに貢献します。  
エネルギー価格を交渉し、価格の急上昇に応じて炊飯器または給湯器をオフにするホームハブのスマートメーターマーケティングビジョンについては、これは商業的現実とはかけ離れています。英国でスマートメーターが達成したことは、請求書支払者に200億ポンドの費用をかけて、数万台のメーターリーダーを廃止することです。  
2UKの鉄道と鉄道信号は、国家安全保障規則により、鉄道は重要な国家インフラストラクチャと見なされているため、無線によるソフトウェアアップグレードは許可されていません。  
よくできました、MI5！ 14.3。  
14.2.5発券詐欺  
ロンドンの場合、鉄道の規制緩和により、鉄道会社が乗車率の高い駅で予約してチケット販売を操作する際に問題が発生しました。ベンダー間で収益を共有するシステムを設計している場合は、利害関係者が不正行為をするインセンティブを設計するようにしてください。  
実際の詐欺データが存在するチケットの1つのタイプは、航空会社の種類です。  
チケットは、クレジットカードの不正使用から航空会社や旅行代理店の不正なスタッフ、盗まれた飛行距離やハッキングされた予約システムなど、さまざまな方法で取得されます。マーケティングチャネルには、スパム、アフィリエイトマーケティング、移民コミュニティへの販売、人身売買業者への販売が含まれます。  
重要な要素は、地下鉄のチケットとは異なり、飛行機のチケットはそのようなエコシステムが発展するのに十分価値があるということです。そして、一部の顧客は偽のチケットを取得していることを知っていますが、それらの多くは単なる吸盤なので、無効なチケットでフライトに出向くすべての人を逮捕することはできません。  
脅威モデルには、センサー操作、サービス拒否、経理の問題、手続き上の敗北、および運用スタッフの腐敗が含まれます。  
  
リミッター多くのシステムは、車両を監視および制御するように設計されています。  
中古車を購入するとき、車が計時されているかどうか、つまり、表示されている走行距離が減少したかどうかを心配します。  
関連する問題はチッピング、つまりエンジンコントローラーの交換または再プログラミングです。  
第1に、第4章で説明するように、エンジンコントローラーは、ほとんどの現代の車を盗難から保護するリモートキー入力システムのサーバーとして機能します。したがって、キーを盗まずに車を盗む場合は、路上でコントローラを交換するか、車を牽引して後でコントローラを交換または再プログラムすることができます。  
そのため、コントローラーは改ざん耐性を強化するか、少なくとも改ざん防止に努めています。  
現在、多くの車両は14.3の間に製造業者にアップロードされたログを保持しています。  
ゼネラルモーターズは、1990年に衝突データを記録するために、一部の車両にブラックボックスを装備し始めました。  
確かに、自動車の電子セキュリティに賛成投票されたESCAR全体の会議があります。  
他の車両監視システムは製造後に装着され、最もよく知られているのはタクシーメーターです。  
 彼がそれでうまくやれるなら。  
「従量制」の保険を若くてリスクの高いドライバーに販売する保険会社は、午後に田舎道を運転するために保険業者がマイル数マイルを充電できるようにする衛星ナビゲーションデバイスをブラックボックスに取り付けるように要求しますしかし、都心部での夜の運転にはマイルあたり数ドル[1909]。  
  
ここで使用するケーススタディはタコグラフです。  
これにより、そのような機器がどのように機能し、失敗するかについての興味深いデータが得られます。これは、デジタルテクノロジーへの移行によって状況が改善されなかった例です。  
運転者がハンドルで眠りに落ちたことに起因する車両事故は、飲酒の数倍の事故を引き起こします（たとえば、英国の事故の20％対3％）。  
トラックが関係する事故は、トラックの質量のために致命的な怪我につながる可能性が高くなります。  
これらの法律は米国で計量ステーションとドライバーのログブックを使用して施行されていますが、ヨーロッパの国ではタコグラフを使用して車両の速度の24時間の履歴を記録しています。  
;それ以来、デジタルタコグラフが導入され、古いシステムはほとんど廃止されました4。  
アナログシステムは、車両の速度計/走行距離計ユニットの一部であるタコグラフに読み込まれるワックス紙のチャートを使用します。  
3Fullの開示があります。私の研究生の1人はBoschから資金提供を受けています。14.3。  
また、関連する運転時間の規制（通常は1日あたり8.5時間、1日あたりの休憩と1週間あたりの休憩のルール）に準拠していることを証明するために、数日分のグラフを保管する必要があります。  
デジタルの場合は、ドライバーカードを接続する必要があります。カードと車両ユニットの両方が記録を保持します。  
 高速道路で、他の道路では少ない。  
タコグラフチャートは、無許可の廃棄物投棄などの他の犯罪の調査や、燃料の盗難を検出するためにフリートオペレーターによっても使用されます。  
実際、セキュリティエンジニアリングの一般原則として、ターゲットを集約するべきではありません。  
私たちが言わなければならないことのほとんどは、タクシーメーターや他の監視装置にも当てはまります。  
これは実際の改ざん手法にはほとんど影響しません。  
14.3.2何がうまくいかない  
14.3。  
14.3.2.1ほとんどのタコグラフ操作はどのように行われるか  
たとえば、ダンディーとサウサンプトンに施設がある会社では、距離が約500マイルで移動に約10時間かかるため、1日1台の車両を各方向に操作するために4人のドライバーが必要です。毎日行います。  
それで、サウサンプトンから来た運転手は今ダンディーからの車で家に帰ります。  
このようにして、彼はペンリスで隔日過ごしたという合法的な印象を与えることができます。  
ヨーロッパ本土では、ドライバーが月曜日にフランスのデポから、火曜日にベルギーで、水曜日にオランダで運転している可能性があるため、検出はさらに困難です。  
停止すると、ドライバーは近くのミルトンまたはラホヤからスタートしたと主張できます。  
オペレーターがチャートや給与記録、計量ステーションスリップ、フェリーチケットなどの補足文書を作成するように指示された場合、彼のオフィスは都合よく燃え尽きることがあります。  
   
合計の約20％に相当する次に大きい詐欺のカテゴリは、電源とインパルス供給、ケーブルとシールの干渉を含む、タコグラフ機器への供給の改ざんを伴いました。  
最近のアナログタコグラフは、回転式のワイヤーではなく電気ケーブルを使用するという点で「電子式」です。  
これにより、いじくりがはるかに簡単になりました。一般的な攻撃は、センサーを1/10インチほど緩めることです。これにより、車両が静止しているかのようにインパルスが停止します。  
フィッターは、時計回りではなく反時計回りにワイヤーを包むように賄賂を渡されます。これにより、センサーのねじを外すと、ワイヤーが壊れるのではなく緩みます。  
しかし、ほとんどのフィドルはまだずっと単純です。  
（1つのメーカーが14.3。  
多くのドライバーは、安全な車を運転するよりも早く帰宅することを好みました。）  
これらは、電源の遮断を示しますが、距離のトレースに不連続がある場合を除きます。  
  
詐欺の3番目のカテゴリは、タコグラフユニット自体を改ざんすることでした。  
これは違反の約6％に相当しますが、デジタル通信の導入によりケーブルの改ざんが容易になったため、1990年代まで減少しました。  
14.3.2.4ハイテク攻撃  
写真の左側にあるプラスチック製のシリンダーは「電圧レギュレーター-日本製」とマークされていますが、電圧レギュレーターではありません。  
 それはタコグラフケーブルに接続され、リモートコントロールキーフォブを使用してドライバーによって制御されます。  
この種のデバイスは信念の1％未満を占めていましたが、その使用ははるかに広まっていると考えられていました。  
そのような装置が装備されたスピード違反のトラックを止めてそれを見つけることができない警察官は、確信を得るのが困難です。封印され、明らかに正しく校正されたタコグラフは、レーダーまたはカメラからの証拠と矛盾します。  
14.3.3デジタルタコグラフ  
英国では、車両検査官による無作為検査のためにトラックが道端に停車しており、疑わしいトラックは国中に隠されている場合があります。  
イタリアでは、高速道路の料金所のデータを使用して、平均速度が制限速度を超えたドライバーを起訴します（イタリアの料金所の直前に駐車しているトラックをよく見かけます）。  
しかし、運転手は異なる管理体制の間で裁定取引をすることができます。  
英国のシステムの弱点は、車両検査官がトラックを停止して違反の証拠を見つけたときに、検察が約14.3になるということでした。（提供：イギリス、ハンプシャー州警察）  
外国人ドライバーはしばしば現れなかった。  
各ドライバーには、過去28日間の運転時間の記録を含むドライバーカードがあります。  
メカニックがデバイスを調整するために使用するワークショップカードと、法執行官が道端でそれらを読み取るために使用する制御カードもあります。  
私は警官や車両検査官からタコグラフベンダーや事故調査官まで幅広い人々と話をした後、レポートを書きました[64]。  
しかし、いくつかの興味深い新しいひねりも浮上しました。  
プロジェクトに提起された主な異論は、デジタル化が全体の70％を占める手続き上の詐欺と戦うのにどのように役立つかが明確ではなかったということでした。  
新しいシステムに切り替わるまでに14年（トラックの寿命以上）かかりました。その間、曲がった会社が1台の新しいデジタルトラックと1台の古いアナログトラックを走らせることができました。  
これは十分な根拠があることがわかりました。  
タクシーメーター、タコグラフ、トラックスピードリミッターは、簡単に操作できるため、必要になる前にデジタルデバイスをインストールしていた可能性があります。  
もう1つの異議は、詳細な速度と運転時間の情報が失われることにより、施行が困難になることでした。  
したがって、ドライバカードのメモリは限られ、限られた数のアラームイベントしか含めることができません。  
14.3.3.1システムレベルの問題  
ドイツは、デジタルタコグラフデータ、既存の紙の海図からのアナログデータのデジタル化されたバージョン、燃料データ、配送データ、さらには給与を受け取り、それらすべてを調整して、運送会社の管理情報だけでなく、管理情報を提供するフリート管理システムのインフラストラクチャを求めましたしかし、警察の監視データ。  
時間の節約、またはコンプライアンスの実証に熱心な企業のためにこれを分析するサードパーティのサービス会社があります。  
英国は自動ナンバープレートリーダー（ANPR）のネットワークを持っています  
これは、自動車の脱税者の検出に基づいて正当化されましたが、その後、テロから強盗に至るまで、ANPRデータがますます多くの訴追に加わることがわかりました。  
しかし、プライバシーや国の経済的利益についての意見の相違は、EU全体の標準化を妨げていました。  
そして、これを必要とする国の間でも、裁定取引がまだあります。  
したがって、古いアナログシステムでは、アルプスを走行中に、通常自分のマシンにチャートを配置することを気にしなかったイタリア人ドライバーがそうしました。  
正味の影響は、特定の国のすべての運転手が同じレベルの執行の対象となったことでした。  
。  
14.3。  
実際の修正は技術的ではなく合法的であることが判明しました。  
以前は、警察官はトラックまたは運転手の記録に表示される犯罪ではなく、進行中の犯罪に対してのみスポットファインを発行できました。  
  
全体として、アナログからデジタルへの移行は改善ではありませんでした。  
そして、タコグラフがデジタル化することには他にも興味深い問題があります。  
長年にわたり、セキュリティ研究者は「裁判官がXをY乗し、Zと等しいことを発見し、ボブを刑務所に送る」のようなパンチラインで学術論文を書いてきました。現実は違います。  
警察は、証拠を「確保する」ための標準的な手順を適用することで問題を解決しました。  
1つは防御に与えられ、もう1つは控訴のために保管されます。  
第二に、多くのドライバーには複数のドライバーカードがあります。  
EUの移動の自由のおかげで、ドライバーは複数の住所を簡単に持つことができます。トゥールーズのジャンムーランは、アントワープのジャンムーランでもある可能性があります。  
たとえば、運転手は居住国の1つでミドルネームを忘れる場合があります。  
3番目に、新しい種類のサービス拒否攻撃（および従来のギアボックスセンサー、ヒューズなど）があります。  
トラックの運転手はスマートカードに幹線電力を供給することで破壊することができます（トラックの24ボルトでも十分です）  
規制の下で、彼は交換を待つ間15日間運転することが許可されています。  
第4に、タコグラフチャートの詳細な冗長データが失われると、施行が難しくなることを述べました。  
タクシーメーター、タコグラフ、トラックスピードリミッターなどの規制。  
次に、システム内の一部のカード（特に、機器のセットアップに使用されたワークショップカードと、警察や車両検査官が使用した制御カード）それらは不正行為の証拠を消去するために使用できます。  
そのため、一部の国では、手に負えないワークショップカードの数を最小限に抑えるために多大な努力をしています。  
会社のライセンススキームはありません。悪意のある企業は、認可された企業の取締役として行動することをブラックリストに載せることができますが、詐欺師は指名された取締役の後ろに隠れているだけです。  
14.3.3.3復活したアヒルの子、または豆腐  
1990年代後半、EUの規制により、図14.3に示す種類の遮断器の使用を妨げるために、すべてのデジタルタコグラフはギアボックスセンサーから車両ユニットへのパルス列を暗号化する必要がありました。  
しかし、一体どのようにして鍵を配布できるでしょうか？  
フィッターがトラックの運転手と共謀してシステムを打ち負かし、ガレージのスタッフがヘルプラインを悪用して盗難車のロック解除データを入手したり、盗まれたカーラジオのPINコードを入手したりする長い歴史があります。  
これは、卵から出てきたアヒルの子が、音を発する最初に動く物体を母親として認識するという事実にちなんで名付けられました。これは刻印と呼ばれます。  
センサーは電源投入時にこれを行います。  
センサーが故障して交換が必要になった場合は、ワークショップカードを使用して車両ユニットのキーストアを「殺し」、新生児として復活させてから、新しいセンサーに刷り込むことができます。  
（これは少なくとも理論でした。1つのユニットでセンサーのキー再生成のエラーコードが停電のエラーコードと同じであるという点で、実装はやや短くなりました。）  
ワイヤレスLANエクステンダーでも使用されます。これらのデバイスは通常、Homeplug AVと呼ばれるプロトコルスイートを使用して、国内の主電源14.3経由で155Mb / sでデータを送信します。  
近所の人がwifiを使用できないようにするために、各仮想ネットワークは、初めてエクステンダーを差し込んだときに設定されるキーで暗号化されています[1437]。  
インターフェースが制約されたデバイスがモノのインターネットに加わるにつれて、そのようなプロトコルはより広く普及するようになります。  
14.3.4センサーの無効化と第3世代デバイス  
デジタルタコグラフの出荷が始まって以来、インタラプタを提供してくれた人々は今、新製品を持っています。ギアボックスをシミュレートする電磁石と電子機器を含むブラックボックスです。  
これでシステムは以前と同じように動作します。コマンドに応じて、インパルスを忠実に中継するか、それらを破棄するか、またはそれらの一部をフィルタリングします。  
安全な検知は見た目よりも難しいです！これは非常に厄介なものになり、EUは2009年に加盟国に「データの破壊、抑制、操作、変更を意図した、または干渉することを目的としたデバイスのチェックおよびチェックを禁止する」という法律を可決しました。記録機器の構成部品間の電子データ交換の任意の部分、または暗号化の前にそのような方法でデータを禁止または変更すること」[652]。  
14.3.5第4世代–スマートタコグラフ  
規制は広範に施行される方向にさらに進んでいますが、車両ユニットが詳細なGPS履歴を保持することを要求するのに十分に止まります。  
CURFEW TAGS：GPS as POLICEMANプライバシー法によっては、一部の国ではそれが困難になります。有害廃棄物の投棄などの悪質な事件では、当局はいつでもドライバーの携帯電話の履歴を召喚することができます5。  
私たちは、これがすべてうまくいくのを待って、見なければなりません。  
 次のアプリケーションからいくつかの洞察を得ることができます。  
14.4門限タグ：警官としてのGPS  
1999年に英国で導入され、刑務所の人口を削減するために使用されています。  
彼らは、家庭の監視ステーションと通信する足首のブレスレットに門限タグをつけています。  
20,000人の犯罪者がいつでも「オンタグ」である可能性があります。  
より高価なタグにはGPSチップが含まれており、タグの着用者の位置を常に警察に報告しています。  
フランスでは、それらは家庭内暴力事件で導入されている[478]。  
。  
監視は2つの企業が支配的で、通常は1日あたり10ドルで、350ドルが前払いされます。  
 したがって、貧しい被告は借金を抱えるか、不払いで投獄されます。  
米国にはいつでも約100万人が刑務所での裁判を待っているため、これは実際の結果を伴う政策問題です。タグ着用者の数は125,000人を超え、2018年のファーストステップ法以降増加しています。2013–6年、私は多くの門限タグの事件で専門家の証人として関与しました。  
私の被告の事件に関連するログの分析は、多数の誤警報を示しました。これらのいくつかは良い説明がありました（停電など）  
全体像は5でした。ヨーロッパの3.5トン未満のすべての車両には、eCall緊急サービス用の組み込み電話が必要です。業界のロビー活動のため、これは残念ながら大型車には必須ではありません。  
CURFEW TAGS：GPS AS POLICEMANは、無秩序な手順と興味のある競合に囲まれた信頼できない技術です。  
さらに、外出禁止令を破った場合、治安判事の前にあなたを連れて行くのは検察官ではなく、請負業者です。システムの設計に協力した下請業者の1人からの専門家の証拠に依存しています。  
請負業者はすぐに「被告は命令に違反していると感じ続けているが、私は公共の利益のために適切に手続きを中止できるようにするいくつかの要因に注意を向けてきた」と答えた[83]。  
 注文。  
多くの個人に、彼らの動きを制限する命令が出され、コンプライアンスを監視するためにGPSタグが付けられました。  
これは秘密保持命令でカバーされていたため、このパターンが明らかになったのは、3人を代表するロンドンの法律事務所に気づかされたときだけでした。  
]。  
これはマスコミに怒りを引き起こした[1904]。  
彼らは契約を剥奪され、その問題は深刻な詐欺オフィス[1286]に付託された。  
タグの改ざんの容疑で入国管理の拘留されていたさらに別のテロ容疑者の場合、門限タグの信頼性は2014年に裁判にかけられ、彼は否定した。  
容疑者の弁護士は、私と私たちの材料科学部門の同僚に専門家として指示しました。  
裁判所は、私たち2人と研究室にいるサウジアラビアの研究生にGPSタグを付けるよう正式に命じ、加速度計とひずみゲージを取り付けてテストを監視しました。  
この仕様では、50kgの引っ張りに耐えるタグ、および事業会社（G4Sから事業を引き継いだものの、同じ専門の下請け業者を使用していた）が必要でした。  
ただし、政府は「商業的機密保持の理由から」この資料の内容を明らかにすることを拒否しました14.4。  
どんなに;壊れた固定ラグのスライバーをテストしたところ、疲労破壊が実際に発生したのはポリカーボネートでした。  
この容疑者はまた、最終的に裁判所によって解放されました。  
サプライヤは当初、GPSの精度について不正確な主張をしていました（販売員は何かを認めたくないので、完璧ではありません）  
これにより、GPS、またはより一般的にはGNSS（元の米国のサービスだけでなく、ヨーロッパのガリレオシステムとロシアと中国の提供物を含む用語）のセキュリティと信頼性を調査する必要がありました。  
そのようなサービスでは、衛星のコンステレーションがそれぞれ非常に正確な時間信号をブロードキャストし、これらの4つ以上を受信する受信機がその位置と時間を解決できます。  
まず、信号の伝播は電離層の状態に依存します。これは可変であり、これを参照ステーションに対して調整できない場合にエラーが発生します。これは、航空機の航法で使用され、精度2mになる可能性があるオーグメンテーションと呼ばれる手法です。  
まず、可視衛星が密集している場合、精度が低下します。これは、少数の衛星しか可視でない場合に発生する可能性があります。  
（最初のケースの主要な修正については、5つの衛星のみが表示され、予想されるエラーは45mでした。場所と時間の関数としてこれを調べることができるWebサイトがあります。）  
 デバイスを最寄りの道路または小道に自動的に配置するスナップフィットソフトウェアがあります。  
マルチパスとスナップフィットの組み合わせにより、高層ビルのある町を運転または歩いているときに、携帯電話またはナビゲーターが1つの通りから別の通りにジャンプします。  
最近まで、GPS電波妨害は政府が行っていたものでしたが、低コストのソフトウェア無線機の出現により、楽しみが広がり始めています。  
直接または基盤となるマッピングサービスに依存することを問わず、GPSに基づいてビジネスを行う場合は、平均エラーだけでなく最悪のケース、およびそのような外れ値が発生する可能性のある状況を理解することをお勧めします6 。私のポスドクの1つであるRamsey Faragherがスタートアップ（Focal Point Positioning）を行いました  
 関連するブログ（https://www.insidegnss.comなど）をフォローします。  
組織レベルでは、裁判所の事件は、テクノロジーが警察の実務にどのように機能していたかについての洞察を与えました。  
（私たちの最初のケースは、誰かの台所に忍び込んで冷蔵庫からワインのボトルを盗んだとされた男性のケースでした。）  
これにより、警察は、より長い刑期の頻繁な出身者を拘束することにより、犯罪統計を押し下げることができます。リハビリ中または精神科的ケアを受けるべき男性で刑務所を埋める場合、または有能な犯罪者から注意をそらす場合、社会的に最適ではなくなる可能性があります。  
14.5送料メーター  
郵便切手はローランドヒル卿によって英国で1840年に導入され、郵便料金の請求を簡素化し、郵便料金の支払いから特定の税金の支払いや郵便為替の付加価値まで、特定の目的に使用できる特別な通貨に発展しました。  
その最初の商用利用は1903年のノルウェーでした。米国では、1920年にアーサーピトニーとウォルターボウズの使用が承認され、その上に大規模なビジネスを構築しました。  
 手紙、またはテープで小包に貼り付けます。  
各メーターには、物理​​的なシールで保護された機械的な値カウンターがありました。メーターを郵便局に持ち込んで、読み取ってリセットすることがよくあります。  
1979年に、Pitney Bowesは「電話によるリセット」サービスを導入しました。これにより、企業は電話で500ドル相当のクレジットを追加購入できました。実装には機械式のワンタイムパッドが含まれ、メーターには連続した再充電コードのテープが含まれていました[477]。  
再充電コードの一部はバリューカウンターから計算されたため、会社が使用した郵便料金の大きさについて嘘をついた場合、デバイスを再充電できませんでした。  
1990年、ピトニーボウズのJos´e牧師は、切手と証印を印刷されたデジタル署名で置き換えることを提案しました[1497]。  
1つの懸念は、カラースキャナーとコピー機が利用可能になり、スタンプや証印を偽造するのが非常に簡単になるかどうかでした。  
メーターを改ざんして追加の送料を取得します。  
そもそも大量のメーラーは郵便局員の疑いを喚起する危険性があるので、彼らを取り引きに誘惑する誘惑がありました。それから、誘導郵便局が別の場所にあるメータープレートを偽造するのは自然なことでした。  
これにより、郵便料金メーターの改ざん防止プロセッサによって生成されたデジタル署名を使用するメーターの開発プログラムが生まれました。  
基本的な考え方は、機械で読み取り可能な証印には、送信者と受信者の両方の郵便番号、メーター番号、日付、郵便料金、メーターがこれまでに販売した郵便料金の金額、および残りのクレジット金額が含まれているということです。それは、すべてデジタル署名で保護されています。  
このようにして、郵便検査官は仕分けオフィスで大量のメールをサンプリングし、各アイテムがフランクされているだけでなく、見かけ上の発信元から宛先までの論理的なルートにあることを確認できます。  
ドイツとイギリスは次の2004年、カナダは2006年でした。他の国も同様でした。  
FIMマークタウンサークルまたは消印ライセンス郵便局/郵便番号から郵送郵送日（必要に応じて）  
 このような印は、旧式のデバイスのドロップイン代替品である郵便料金メーターによって生成できます。あなたは手紙の重さを量って、それを正直にして、月末に請求されます。  
これは、この章で前述した前払い電気メーターとほとんど同じように機能します。  
この「オンライン郵便料金」は、メーターを購入するのに十分なだけの十分な量のメールを送信していない、小規模な会社や在宅勤務の人々を対象としています。  
また、メールの量と収益性をローカルレベルまで追跡することで、システムをより適切に管理できるようになりました。  
しかし、セキュリティについてはどうでしょうか？  
メーター自体に改ざん防止プロセッサが搭載されているか、オンラインの郵送の場合はウェブサーバーに接続されています。これには値カウンターと暗号鍵があります。  
それぞれの場合にいくつかの追加機能があります。  
 メーターによってこれまでに分配された合計値と降順レジスター（DR）が含まれます  
バランス制御は、AR + DR = TS、「合計設定」、つまり、そのデバイスによって行われた、またはそのデバイスに対して承認されたすべての販売の合計です。完全な脅威モデルには、盗まれた郵便料金メーター、無料の郵便料金を提供するために改ざんされたメーター、許可されていない人が使用する本物のメーター、重量とサービスクラスをカバーするのに不十分な値の証印が付いた郵便物、および有効な証印の簡単なコピーが含まれます。  
機微には、認証済みメールや返信メールなどの機能への対処方法が含まれます。  
オペレーターが実際の経験を積むと、業界はデジタル署名からメッセージ認証コードへと移行し始めました。  
主要な仕分け事務所の機器は、毎分数千通の郵便物を処理する必要があり、郵便局は通常、証印をオフラインのバッチ操作として検証します。  
検証が一元化されると、MACは署名よりも意味のあるものになります。中央サーバーには、ユーティリティメーターと同様に、各メーターのMACキーに分散されたマスターキーを持つハードウェアセキュリティモジュールがあります。  
多くの国では、郵便局がすべての暗号化をメーターベンダーに委託しています。  
また、アーキテクチャの多様性も確認しています。  
（そして、郵便配達員に数トンのジャンクメールをシステムに送り込むように賄賂を渡したい場合、それを行う場所は現在国境を越えています。）  
ドイツの郵便局の「スタンピット」スキームでは、ユーザーは郵便局に連絡して印刷されていることを伝える「スマートPDF」ファイルを購入します。ユーザーやソフトウェアとのやり取りはありません。  
そのため、ユーザーはスタンプをコピーするか、必要に応じてもう一度印刷できるファイルにスタンプをコピーするように手配します。  
構文の違いは微妙です。ドイツのシステムはスタンプを複数回印刷するのを止めようとしましたが、イギリスのシステムはより現実的にそれを複数回使用するのを止めようとしました[884]。  
また、サービスをより多くの顧客に拡張し、郵便局のキャッシュフローとクレジットコントロールを改善するビジネスモデルも促進します。  
  
多くのセキュリティシステムは、環境の何らかの側面の監視または測定に何らかの形で関係しています。  
プリンターカートリッジが特定の数のページを印刷した後、プリンターカートリッジの動作を停止するために使用されるメカニズムなど、後の章でさらにメーターと支払いシステムに出くわします。  
いくつかの再設計は成功しており、他はそれほど成功していません。  
デジタルタコグラフはそれほど印象的ではありません。彼らは単に古いアナログシステムが行ったことと同じことを行いますが、あまりうまくいきません。  
3番目の例である門限タグは、位置監視を車両から人間まで拡張します。  
4番目の例である送料メーターは、競争力のある革新を可能にし、成功を収めました。  
どのようなサービス拒否攻撃が可能であるかについては、じっくりと考えなければなりません。  
システムは、相互に疑わしい多数の当事者に対処する必要があり、多くの場合、可能な限り安価なハードウェアに実装する必要があります。  
また、設計を成功させるには、理解しなければならないあらゆる種類のアプリケーションレベルの機微があります。  
ここで説明するようなケーススタディが役立つ場合があります。  
 支払いネットワーク用に開発されたものは適応可能です  
メータリングアプリケーションは、競合する営利団体だけでなく、あらゆるレベルの不正なスタッフや不正な顧客の存在によって引き起こされる広範な相互不信のために特に有用です。そして、機器のほとんどが攻撃者の管理下にあるという事実。  
既存のメータリングシステムの一部のデジタル変換がうまく機能した理由（ユーティリティ、送料）  
？  
 既存のサプライヤーは、より優れたデジタルシステムへの移行を管理し、ドットコムの新興企業との革新的な競争にもかかわらず存続しましたか？  
タコグラフは[64]で作成されています。輸送に関連する他の論文は、自動車の電子セキュリティに関する年次ESCAR会議に掲載されています。  
ただし、郵便料金メーターのセキュリティに関する最も詳細な解説は、プログラムで主導的な役割を果たしたFrancotyp-PostaliaのGerrit Bleumerによる本です[265]。