アルゴリズムがある場合、それは管理です。  
 それは何世紀にもわたって存在しています。  
– MIKHAIL GORBACHEV14。  
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、顧客にロイヤリティを請求しました。  
 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、チケットの発行は膨大です。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ベタクシメーターですが、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。銀行トラックの行方。  
 私の4番目は、手紙and45714を率直に使用する電子切手メーターです。  
 前払いメーターパッケージ。  
 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、攻撃面の最小化、ユーザーの許可など、通常の母性とアップルパイのようなレイアウトを行うETSI規格EN 303645ドラフトなど、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。個人情報を削除する[640]。  
 この章のケーススタディで、必要なコンテキストの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。  
 しかし、多くの計測システムは、物理的にはるかに露出されています。  
 タコグラフを使用すると、それは逆になります。トラックの運転手は、通常、制限速度を超えて運転したり、危険な時間をかけて作業したりするため、タコグラフで一部の運転を無視します。  
 刑事被告人と仮釈放者は、門限令を回避したいと思うかもしれません。  
 さまざまな種類の悪用の地下市場もあります。  
対戦相手は、通信を操作する（古いメッセージを再生するなど）ことによって、または誰かがそうしたと誤って主張することによって、利点を得ることができます。  
 そして、私たちは真の脅威を理解する必要があります。  
 システムは外部からの不正を阻止するように設計されているように見えますが、実際の焦点は内部にあります。  
2前払いメーターユーザーがトークンに対して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、磁気ストリップ付きの段ボールチケット、QRコードを表示するアプリ、さらには充電式チップカードなど、どこかに保存されている値を使用します。  
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。  
2。  
 したがって、リプレイや偽造品の検出は、オフラインで行う必要がある場合があります。  
私たちのオプションは何ですか？ほとんどの発券システムでは、手続き上の詐欺は簡単です。  
 しかし、ほとんどの人は、誰かがそれを工業化することによってそれを簡単かつ安全に見えるようにしない限り、だましません。  
最初に説明する例は、前払い電力メーターです。  
 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。  
2。  
1）。  
このテクノロジーは後発開発途上国、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の優先事項になりました。家の多くは非公式に建設され、所有者は住所さえも持っていませんでした（信用格付けはもちろん）、前払いが唯一の方法でした。  
 インドネシアで最大の設置数は3,500万であり、アフリカ、アジア、ラテンアメリカ、および一部の先進国では一般的です。北アイルランドのほとんどのメーターは前払いです。  
顧客は店に行ってトークンを購入します。トークンは、カード、磁気ストリップ付きの段ボールのチケット、または20桁のマジックナンバーです。  
 これは顧客にとって便利です。チケットはスーパーマーケットのレジ、ATM、電話またはオンラインで購入できるからです。  
 一部のトークンにはエンジニアリング機能もあります。  
セキュリティエンジニアリング459ロスアンダーソン14。  
 前払いメーター英国の電気メーターの約2倍は、磁気チケットの2倍のスマートカードを使用しています。  
 磁気チケットメーターとマジックナンバーメーターには、このようなバックチャネルはありません。  
 スマートメーターはすでに他の国に設置されており、結果はまちまちです。  
図14。先進国では、主なインセンティブは不良債権やその他の管理コストの削減でした。  
 ほとんどのメーターが前払いされている地域では、その費用が世帯主にとってより顕著になるため、電力消費量は最大10％削減されます。  
2。  
 トークンは偽造が容易ではないはずですが、正規のトークンは間違ったメーターや正しいメーターで2回機能するべきではありません。  
 しかし、この単純なアイデアを堅牢なシステムに発展させるには、驚くほどの経験が必要でした。  
2。  
 初期のシステムでは、通常は地元の店舗で、各地区に1つずつありました。  
 しかし、実際の生活は通常より複雑です。  
 南アフリカでは多くの人が長距離通勤をしているので、働く場所で切符を買いたいと思っています。  
 2007年にオンライン販売を導入しました。中央サーバーにはすべての販売キーを備えたハードウェアセキュリティモジュールがあり、顧客はインターネットまたは携帯電話でマジックナンバーを購入できます。  
統計バランスは、非技術的な損失、つまりメーターの改ざんまたは電源ケーブルへの不正接続による電力の盗難を検出するために使用されます。  
 しかし、顧客はチケットを読んだり、メーターのリーダーがメーターを読むときにうそをついたりするため、その差異はノイズの多いシグナルです。  
自動販売機が盗まれ、公益事業者との競争でトークンを販売する場合がありました。  
 その対策は、自動販売機のセキュリティチップにクレジットバランスを維持し、ベンドキーと外部メーターキーも保護することでした。  
 したがって、ユーティリティのサーバーに保持されている元帳データではなく、販売時点でのバリューカウンターによって実施される会計システムがあります。  
14。  
3何が問題になっているのか盗難警報と同様に、環境の堅牢性が重要です。  
2。  
メーターが雷で破壊されたとき、顧客は不満を述べ、まだ使用されていないと述べた価値に対する信用を得ました。  
 トークンスロットの下の回路が破壊された場合、Onemakeのメーター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信用を得たことを確認しました。  
 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。  
 責任ある会社は、100,000メートルを引き抜いて再度ROM化しなければならなくなった後、ほぼ破綻しました。  
 メーターの1つのメーカーは、特定の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、払い戻したトークンのコピーを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、偶然発見され、かなりの日和見的な方法で悪用されたバグや失敗に起因します。  
[93]で書いたその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、高価になり、複雑で、リスクが高くなります。•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、遠くの店でメータートークンを販売し、通勤者をサポートする必要がある場合と同様に、交換に費用がかかる可能性があります。•テクノロジーをリサイクルするバグが少なくなる可能性があるためです。  
 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。また、最高のものでさえも見逃してしまいます。•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。  
2。  
 したがって、前払いは、古き良き監査、エネルギーの均衡化、検査の必要性を完全になくすわけではありません。また、地方の腐敗や発展途上国におけるより広範な州の占領の問題を完全に解決するものでもありません。  
 しかし、1つの妥協点がbiteus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、持続可能性を「このシステムは次の30年間は問題ないでしょうか？」ではなく、「これは次の100年は問題ないでしょうか？」と考えてください。 。4スマートメーターとスマートグリッド2000年代の初めに、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。  
 自動メーター読み取り（AMR）は、高度なMeteringinfrastructure（AMI）に置き換えられました。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。  
 Mar-keters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、市場とリアルタイムの変動を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ドルでおそらく15続く製品に置き換えることでした。  
 研究者は最初に、公益事業に送られる細か​​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があるデータの量についての議論が生じました1 20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が、カウンターに余分なビットを追加して余分なデータを取得することを考えました31年ということは、1単位ではなく2分の時間単位を意味することになるため、1メーターで複数のトークンを同時に販売することは困難でした。  
セキュリティエンジニアリング463ロスアンダーソン14。  
 中心的に前払いメーター。  
 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。  
 彼らの主な懸念は、特にイタリア南部での、電力の盗難でした。そこでは、非支払っている顧客を切断するために送られた取締りが暴力団によって脅迫されました。  
 これは成功と見なされ、ロビイストは働き始めました。  
アメリカの回復と再投資法の主な指標としてのその発展への50億;欧州議会は、加盟国にスマートメーターの経済的評価を2012年までに実施することを要求する2009年の法律に従い、2022年までに使用を義務付け（2020年までに80％採用）[652]。  
Sユーティリティ、および成功（スペインなど）と失敗（イギリスとオンタリオを含む）のいくつかの経験があります。  
 メーターが流通ネットワーク事業者または小売業者に属しているかどうかは、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で機能することを主張したため、商品ハードウェアの価格はe50メートル未満でした。  
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場合、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。  
 英国は残念ながら耕作されています。  
 据え置きなく、彼らはコスト、利益、電気料金、金利についての仮定を拡大し、2009年に肯定的な評価を導き出し、英国に電気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がオプションになり、計算は大きな家でのみ価値があるとされています。  
2。  
 州は73の地方配電会社に対処し、すべてのメーターの読み取り値を収集して小売業者や規制当局が利用できるようにする中央システムを構築しました。  
 2005年（大臣がプロジェクトを発表してから1年）に作成されたオンタリオの費用便益分析では、費用が最大で8億8,800万ドルであったときに、利益が6億ドルと過大評価され、費用は20億ドルに膨れ上がった。デバイスとそれらをサポートするシステムを測定します。  
英国では、スマートメータリングが、最大の市民活動プロジェクトの災害に発展しました。  
 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、節約をもたらす可能性のあるより優れたプロジェクトを置き換えることは、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、古い互換性のないモデルで構成されています。ベンダーはそこで独自の特許を取得するために何年にもわたって闘い、社会関係者は技術的な知識や首をつなぐ政治的支援を持っていませんでした。  
 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]。  
5分は完了しましたが、39分はまだ完了していません[1391]。  
 政府が宣言された戦略に従って全員を第2世代のメーターに移動させる場合、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、2。  
 2020年代を通じて、業界は古き良き時代遅れのメーター、いくつかのタイプの廃止されたスマートメーター、およびニュースマートメーターをサポートする必要があるため、コスト削減はほとんどありません。  
 （政府は、メーターを使用して全員を前払いに移動した場合、多くのエネルギーを節約することができましたが、それは議題には含まれず、はるかに安価なキットで実行できた可能性があります。  
 そして現在の人々は知りたくないだけです。NAOレポートの言葉を借りれば、「現在、国防総省は、セキュリティエンジニアリング465ロスアンダーソン14以降、消費者との関わりを続ける計画はありません。  
 前払いメーターロールアウトが完了しました。  
 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、何十万もの風車やより広い配電システムに埋め込まれた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。  
 いずれの場合も複雑な要因は、多くの発電能力が人々の屋上に埋め込まれているため、負荷を減らすことが以前ほどうまく機能しないことです。  
 また、インフラストラクチャの残りの部分を停止に対してより寛容にする必要があります。  
 48ではずれたはずの60のSiemens Desiroクラスの列車が49Hzでつまずいたので、これは起こりました。  
 彼らを再び連れて行くには、ラップトップ2を持った技術者の訪問が必要でした。  
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があり、それらが引き続き確実に機能するように毎月30時間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、更新されたときにそれらを起動するために支払いを受けます。  
 最終的には、電気自動車用の充電器が十分にあれば、これも貢献します。  
エネルギー価格を交渉し、価格の急上昇に対応し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、商業的現実から離れています。  
 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、数万人のメーターリーダーを使用できなくすることです。  
2UKの列車と鉄道信号は、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を行うことはできません。  
 よくできました、MI5！セキュリティエンジニアリング466ロスアンダーソン14。  
 タクシーメーター、タコグラフ、トラック速度リミッター14。  
5Ticketing fraudTransportの発券は公共料金のメーターよりも大きなアプリケーションですが、電車、バス、地下鉄のチケットの故障モードに関する深刻で公に利用可能な調査については知りません。  
 セクション13で説明されているMifareクラシックの中断後の恐怖もありました。  
5;ロンドンの交通機関は不正を検出するために侵入検知システムを追加するためにスクランブルをかけました。  
 2010年代には、不正に入手された航空券とそれらを再販するためのチャネルのエコシステムが出現しました。  
 これはすべてAlice Hutchings [936、937]によって文書化されています。  
次に、電力計よりも攻撃がより深刻で長期にわたるアプリケーションのクラスを見ていきます。  
 この模範的な研究分野は、車両監視システムです。  
3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、その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、最新の自動車のほとんど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、彼らはコントローラーの改ざん耐性を高めるか、少なくとも改ざん防止を試みます。  
多くの車両は現在、セキュリティエンジニアリング467ロスアンダーソン14の間に製造業者にアップロードされるログを保持しています。  
 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サービス。  
 伐採が1999年に公開されるまでに、数百万台の車が装備され、その開示はプライバシー活動家からの抗議を引き起こしました[1938]。  
 自律運転への関心が高まっているため、2019年には車両のセキュリティが再び話題になっています3。  
 タクシーの運転手は、メーターを操作して、逃げることができる場合、より多くの走行距離（または待機時間）を表示するインセンティブを持っています。  
 若くてリスクの高いドライバーに「従量制」の保険をかける保険会社は、午後に田舎道を運転するために保険会社が数ペニーを1マイル充電できる衛星ナビゲーションデバイスを備えたブラックボックスを取り付けるよう要求します。都心部での夜の運転[1909]のマイルは1マイルです。  
14。  
1タコグラフ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、そのような機器の動作に関する興味深いデータが得られ、失敗する可能性があります。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。  
ドライバーがハンドルで眠りに落ちたことに起因する車両事故は、飲酒よりも数倍多い事故を引き起こします（たとえば、英国では20％対3％の事故）。  
 したがって、ほとんどの国では、トラックの運転者の労働時間を規制しています。  
 2005–6年まで、これは円形のワックスペーパーチャートに記録されました（図14。  
まず、ベースラインとして古いアナログシステムを見てみましょう。ヨーロッパの道路では、古いトラックやバスでまだ使用されています。  
 24時間に1回回転する計器内部のターンテーブルでゆっくりと回転し、速度計に接続された細かいスタイラスによって速度履歴が記録されます。  
4 2004年8月以降に英国で登録された車両はデジタルシステムを装備する必要があり、2005年6月以降はドライバーカードが発行され、2006年8月には新車でのデジタルシステムの使用が義務付けられました。他のEU諸国では日付が若干異なります。  
3。  
2：–タコグラフチャートの例外は私たちに関係する必要はありません。タコグラフがない限り、ヨーロッパでトラックを運転するのは当たり前です。アナログの場合は、チャートをインストールし、開始時刻と場所を書いておく必要があります。  
1日5時間、休憩時間と休憩日は1週間あたりのルール。  
欧州の法律では、高速道路ではトラックを時速100 km（時速62マイル）に制限し、他の道路ではトラックを制限しています。  
 タコグラフチャートは、無許可の廃棄物投棄などの他の影響の調査や、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、ターゲットをタグ付け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その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を与えません。  
3。  
セキュリティエンジニアリング469ロスアンダーソン14。  
 タクシーメーター、タコグラフ、トラック速度リミッター14。  
2。  
たとえば、施設がダンディーとサウサンプトンにある会社では、距離が約500マイルであり、旅程が約10時間かかるため、1日1台の車両を各方向に運転するには4人の運転手が必要です。これは、1人の運転手が毎日行うことは違法です。 。  
それで、サウサンプトンから来た運転手は、ダンディーからの車両で今帰宅します。  
 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、運転手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命令された場合、オペレーターは都合よく燃え尽きることがあります。  
）14。  
2。  
初期のタコグラフでは、1980年代初頭まで車の速度計と同様に、回転ワイヤーケーブルを使用していました。トラックの走行距離計を詰まらせた場合は、ケーブルを剪断する可能性が非常に高くなります。  
 入力はギアボックス内のセンサーから送られ、プロペラシャフトが回転すると電気インパルスを送信します。  
 これを防ぐために、センサーはワイヤーとリードのシールで固定されています。  
 アザラシが個々のフィッターではなくワークショップに発行されるという事実は、検察を複雑にします。  
 ドライバーはケーブルをショートさせるか、タコグラフヒューズを切れたヒューズと交換します。  
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。  
2：11A前後。  
、外側のトレースに示された速度が突然ゼロから100 km / hを超える場所がいくつかあります。  
 そこで、ユニットは開いていました。  
3。  
3計器の改ざん第3カテゴリーの詐欺は、タコグラフユニット自体の改ざんでした。  
これは全体の約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。  
3。  
4ハイテク攻撃調査時の改ざん技術の現状は、図14の機器でした。  
 写真の左側のプラスチックシリンダーには「VoltageRegulator-Made in Japan」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。  
）タコグラフケーブルに接続され、リモコンの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、確信を得ることが困難です。封印された、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。  
3。  
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蔽されている可能性があります。  
 イタリアでは、高速道路の料金所のデータを使用して、平均速度制限を超えたドライバーを起訴します（多くの場合、イタリアの料金所の直前に駐車されているトラックを見ることができます）。  
たとえば、フランスとオランダの間で運転しているトラック運転手は、オランダの車両検査官がそこに行くことができないフランスの倉庫に彼の書類を保管できます。  
3。  
3：–ラジオキーフォブを使用してドライバーが制御するインタラプタ付きタコグラフ。  
 外国人ドライバーはしばしば姿を消しました。  
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。  
 機械工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、法執行機関が道端で読み取るために使用する制御カードもあります。  
警察官や車両検査官のタタコグラフベンダーや事故調査官など、幅広い人々と話をした後、私は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議は、goingdigital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のに14年かかりました-トラックの寿命よりも長い-その間、曲がった会社は1つの新しいデジタルトラックと1つの古いアナログトラックを実行できました。  
 これは、十分な根拠があることがわかりました。  
3。  
 2020年には、ドライバーは複数のカードを所有しています。  
 1998年に、Germanshadはドライバカードをメモリデバイスにして、詳細なレコードを含めることを望みました。フランス人はスマートカード業界からのロビー活動のおかげで、スマートカードを強く要求しました。  
14。  
3。  
 ドイツは、デジタルタコグラフデータ、既存の紙のチャート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、配達データ、さらには給与を受け入れ、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、警察。時間を節約したい、または単にコンプライアンスを実証したい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。  
英国には自動ナンバープレートリーダー（ANPR）カメラのネットワークがあり、当初はIRA爆撃攻撃を困難にするためにロンドン周辺に設置されています。 1997年の聖金曜日の合意がその脅威を終わらせた後、ANPRは廃止されずに全国的に拡大されました。  
 運転時間の強制の場合、戦略はANPRデータベースに対してログに記録された旅行のサンプルを検証することです。不一致が見つかった場合は、会社の業務をより綿密に調査します。  
 トラックからデータをダウンロードして分析することをトラック会社に要求するかどうかは、個々の国次第です。  
 たとえば、ドイツの警察は、イタリアの警察よりも運転時間の規制を実施することにはるかに積極的です。  
 一方、ドイツのトラックの運転手が別の方向に進んで、彼のチャートを取り出しました。  
 しかし、運転データがイタリアの運転手カードからアップロードされ、ローマのトラック会社のPCに保存されていた場合、イタリアのレベルの執行の対象となりました（または、ローマの警察がドイツの事故を気にしていなかったとしても）。 。  
セキュリティエンジニアリング473ロスアンダーソン14。  
 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英国では、立ち止まり、治安判事の裁判所に出頭するように命じられた外国人ドライバーは、立ち向かわないことがよくありました。  
 2018年3月、イギリスは法律を変更し、路上でスポットファインを許可しました。  
 この変更により、10倍近くの増加が見られました[924]。  
3。  
2その他の問題全体として、アナログからデジタルへの移行は改善されませんでした。  
 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。  
審査員は、デジタル署名が車両ユニットから印刷された小さなチケットに16進数の文字列として提示され、検証のための承認された装置がないため、難しいと判断しました。  
 彼らが危険なトラック輸送会社を襲撃したとき、彼らはPCのディスクドライブをイメージし、証拠バッグに密封されたDVDにコピーを取ります。  
 コピーを文書化したペーパーログは、彼らの崇拝者が車両ユニットからの印刷物とともに検査するために利用できます。  
 これはどこにでもありますが、それだけでは止まりません！ドライバーは、たまにしか使用しない友人からそれらを借ります。たとえば、通常3歳未満のトラックを運転しているためです。  
 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、ドライバーは居住国の1つでミドルネームを忘れる場合があります。  
第3に、新しい種類のサービス拒否攻撃（ギアボックスセンサーやヒューズなどの従来の攻撃）があります。  
 規定により、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上の詳細な冗長データが失われると、施行が困難になると述べました。  
3。  
 これは他の執行タスクに波及します。たとえば、記録された速度履歴はしばしば検査官にトラックのルートについての良い考えを与えたので、アナログチャートは、違法な有毒廃棄物の投棄の証拠を収集するためにしばしば使用されました。  
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。  
 したがって、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、認可された企業のディレクター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ます。  
3。  
3復活したアヒルの子、または豆腐タコグラフの世界からの興味深いスピンオウがあります。  
3、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ますか？ガレージが呼び出すことができるホットラインを設定しただけでは、悪用される可能性があります。  
1つの解決策は、復活したアヒルのセキュリティポリシーモデルによって与えられます。同様に、シュリンクラップから取り外されたばかりの「新生児」車両ユニットは、秘密鍵を送信する最初のギアボックスセンサーを所有者として認識できます。  
 このキーを受け取るとすぐに、車両ユニットは新生児ではなくなり、残りの「寿命」の間、ギアボックスセンサーに忠実なままになります。  
 虐待をより困難にするために、復活の各行為は車両ユニットに消えずに記録されます。  
）キー管理の復活したアヒルの子モデルは、もともとはデジタル温度計やその他の医療機器を医師のタブレットやベッドサイドモニターに安全に刻印するために開発されました[1819]。  
3。  
近所の人があなたのWi-Fi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セットアップされるキーで暗号化されています[1437]。  
 制約のあるインターフェースを備え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。  
3。  
 デジタルタコグラフが出荷され始めてから、インタラプタを持ってくる人たちは新製品を手に入れました。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。  
 システムは以前と同様に動作します。コマンドに応じて、インパルスを忠実に中継するか、または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困難です。これは非常に厄介なものになり、EUは2009年に特に禁止し、加盟国に「データを破壊、抑制、操作、または変更することを目的としたすべてのデバイス、またはこれは、記録機器の構成部品間の電子データ交換の一部を妨害することを目的としているか、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を目的としています」[652]。  
3。  
 規制はさらに広範に施行される方向に進んでいますが、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。  
4。  
 一方、ベンダーは、自動侵害チェックを備えたフリート管理システムを提供し、これにより責任が最小限に抑えられることを企業に保証します。  
しかし、絶え間ないGPS監視を必要とする実用性は何でしょうか？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。  
4Curfewタグ：警官としてのGPS監視と計測の3番目のケーススタディは、犯罪容疑者とパロルされたオーディエンスが動きを抑制および監視するために足首に着用する門限タグです。  
 ほとんどの犯罪者は、刑期の半分を務めた後に釈放され、仮釈放期間の一部を門限の下で過ごします。これは、通常、午後7時から午前7時まで家にいる必要があることを意味します。  
 他の人は、外出禁止令で、刑務所の代わりにコミュニティ刑を受け取ります。  
外出禁止令のタグは他の多くの国にも広がっています。  
 英国では、これらのデバイスは、外出禁止令が学校の近くに行くことを禁止している性犯罪者、一部の警察地域の常駐者、およびテロ容疑者が着用しています。  
 米国では、彼らは保釈の条件として裁判前に多くの容疑者に提供されています（その中で最も有名なのはHarvey Weinsteinであった可能性があります）。  
モニタリングは、通常$ 1日1日10ドル、前払いで350ドルを請求する2つの企業が支配しています。  
）したがって、貧しい被告は借金をするか、不払いで投獄される。  
 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、これは実質的な結果を伴う政策問題です。タグ装着者の数は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ケースの専門家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。これらの一部には説明がありましたが（停電など）、多くはそうではありませんでした。  
eCallemergencyサービス用の組み込み電話を使用するには、ヨーロッパで5トンが必要です。残念ながら、これは大型車では必須ではありません。業界のロビー活動のためです。  
4。  
 タグ付けの請負業者であるSercoは、タグとバックエンドシステムだけでなく、コールセンターと裁判所システムへのインターフェイスも提供しました。  
 私たちは裁判所に、事件のタグへのアクセスと、テスト、システム仕様、誤警報統計および監査報告のための一連のタグ付け装置を要求しました。数か月後、「テロ行為防止および調査措置」（TPIM）の命令の対象となった複数の男性が関与する事件がありました。  
 多くの個人に、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、このパターンは、3人を代表するロンドンの法律事務所によって通知されたときにのみ明らかになりました。  
 数日後、彼らの1人はロンドンのモスクでniqabを着用し、女性として去ることによって監視を回避しました。  
 翌月、英国の2つの主要な門限タグ請負業者（SercoおよびG4S）が政府を大規模に詐欺していたことが判明しました。これは、無罪または刑務所にいる、海外にいる、または死んでいる犯罪者にタグ料金を課すことにより、そして、これは2005年に契約が始まって以来ずっと続いていた。  
 Sercoは最終的に19ポンドの罰金を科されました。  
700万の費用;その会計士であるデロイトは£4を支払いました。  
門限タグの信頼性は、タグの改ざんの容疑で入国管理の拘禁されていたさらに別のテロ容疑者の場合、2014年に裁判にかけられ、彼は否定した。  
 容疑者の弁護士は、私と私たちのマテリアルサイエンス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人と研究室のサウジアラビア人研究生にGPSタグを付けることを正式に命じ、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。  
 50kgの引っ張りに耐えるようタグに要求する仕様であり、運営会社（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）は、タグの素材には疲労骨折の責任がないと主張しました。  
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、疲労破壊が実際に起こっている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の正確さについて不正確な主張をしており（営業担当者は、完璧ではないことを認めたくない）、いくつかの試行があった。  
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。  
 第1に、信号の伝播は電離圏の条件に依存します。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はエラーにつながります。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と、精度が低下します。これは、少数の衛星しか見え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つの衛星しか見えず、予想される誤差は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。  
 3番目に、さらに大きなエラーはマルチパスから発生する可能性があります。通常、建物から反射された信号が直接信号と競合する場合です。  
 最後に、さまざまな種類の妨害があり、それは単にサービスを拒否する弾幕妨害から、おとりが別の場所で観測された無線スペクトルをデコイが再送信して、代わりにその場所にあるとGPS機器に信じ込ませるようなより洗練された戦略までさまざまです。  
 私が暴力団だったら、メコンを使ってアリバイを提供することができます。それは、私が実際に出かけて誰かを撃った間、私が家にいたことを警察に伝えます。  
 業務用機器を使用する場合でも、巧妙な信号処理を使用する場合でも、市販の機器よりも優れた性能を発揮できます。  
insidegnss。  
セキュリティエンジニアリング479ロスアンダーソン14。  
 郵便料金メーター7。  
 強盗のかなりの割合は、「多忙な持続性のある犯罪者」によって犯されています。通常、男性は薬物やアルコールの問題を抱えており、軽度の罪で数十の有罪判決を受けています。  
）警察が彼らの「頻繁な警備員」に門限を取り付けた場合、強盗が報告されたとき、彼らはそれらのいずれかが100ヤード以内にあったかどうかを確認し、そうであれば車を送って拾います。  
14。  
 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、郵便為替の金額の補充まで、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。アメリカでは、アーサーピトニーとウォルターボウズが1920年に使用を承認され、大規模なビジネスを構築しました。  
 証印には日付があり、古い証印を剥がして再利用することはできませんでした。  
 不正防止は、ユーザーがメールをローカルの郵便局に持っていくことに依存していました。店員は日付とメーターのシリアル番号を確認できます。  
 1981年、これはDESベースのシステムにアップグレードされ、メーターを任意の金額で再充電できるようになりました。  
しかし、これらのメーターはまだインクされたしるしを作り出しました。  
 これは、米国郵政公社の注意を引いた。米国郵政公社は、暗号化がより良い郵便料金メーターの作成に役立つかどうかを調査するプログラムを開始した。  
 Doug Tygar、Bennett Yee、Nevin Heintzeが彼らのために行った脅威分析では、大きな問題は切手の偽造やコピーではなく、完全な開示ではないことが明らかになりました。私は会社に投資しました。  
5。  
 大量の郵便物が郵便サービスの従業員を汚し、トラックに大量のジャンクメールを支払うことなくシステムに挿入しました[1912]。  
 1990年までに米国郵政公社の損失は9桁になり、1990年代を通じて、メーターを操作して数百万ドルの無料の郵便料金を手放したばら積み郵便業者の目立たない多数の有罪判決がありました[265]。  
 これは、複数の競合メーカーが利用できるオープンスタンダードに発展しました。  
 秘密署名キーはメーターのプロセッサに保存され、対応する公開署名検証キーはメーターのシリアル番号で索引付けされた郵便サービスディレクトリに保存されます。  
米国は2000年にこの技術を導入し、Pitney Bowesなどの伝統的なサプライヤーが、スタンプなどの新興企業に伝統的なメーターを販売しています。  
 ドイツとイギリスは2004年に、カナダは2006年に続きました。他の国も同様に続きました。  
以下の4。  
32 FIRST-CLASS 1998年3月31日、オプションの広告アート領域図14。  
5。  
 ただし、クレジットメーターの場合はインターネットを介して行うことができるため、メーターを読み取る必要はありません。前払いメーターを購入する場合は、コールセンターに電話してマジックナンバーを購入することで補充できます。クレジットカード。  
Indiciaは、送信者と宛先の郵便番号を指定するだけで、インターネットで購入することもできます。  
 従量制とオンラインの両方の郵便料金は、配布する切手よりも安価です。  
 つまり、デジタルポストは、ユーザーと郵便サービスの両方に高い柔軟性をもたらします。  
 メーター自体に改ざん防止プロセッサー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。  
 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、権限の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ため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。  
 主要な仕分け場所にある機器は、毎分数千通の郵便物を処理する必要があり、郵便サービスは通常、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備えた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、郵便局はすべての暗号化をメーターベンダーに委託しています。  
6。  
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持ち込むことを買収したい場合、それを行う場所は現在国境を越えています。  
 ドイツの投稿オフィスの「スタンピット」スキームでは、ユーザーは自分や自分のソフトウェアとのやり取りなしに、印刷されていると投稿オフィスに連絡する「スマートPDF」ファイルを購入します。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の印刷を複数回停止しようとしましたが、イギリスのシステムはより現実的に複数回の使用を停止しようとしました[884]。  
 また、サービスをより多くの顧客に拡張し、ポストオフィス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。  
14。  
 それらは、ユーティリティメーターからタクシーメーター、タコグラフ、郵便メーターまでさまざまです。  
世界がアナログ技術からデジタル技術に移行するにつれて、多くの監視、計測、支払いシステムが再設計されました。  
 デジタル前払い電力メーターは、発展途上国の公益事業会社が、信用格付けだけでなく、住所さえ知らない何億人もの人々に電力を販売できるようになり、成功を収めました。  
 成熟した業界が既存の安全法に準拠することを目的としていたため、多くの定着した利害関係者と破壊的なプロセス変更の機会がないため、彼らのゆっくりとした進化はおそらく避けられませんでした。  
 技術的なベンダーの監視は新しい産業であるため、これはいくつかの革新をサポートしています。また、大規模で複雑なシステムでGPSを使用する場合の制限についても教えてくれます。  
盗難警報と同様に、監視システムの保護は信頼性と結びついています。  
6。  
 鍵管理は、特に一元的な鍵管理機能を提供したり、十分な信頼できる人を雇ったりすることができない、低コストで分散されたシステムでは問題になる可能性があります。  
 監視装置の多くは対戦相手の手中にあります。  
研究の問題「モノのインターネット」について多くの話がありますが、研究者が考えるための具体的な例はほとんどありません。  
支払いネットワーク用に開発されたメカニズム（および製品）は適応させることができますが、設計作業の多くはやり直す必要があり、最終結果にはしばしば脆弱性があります。  
繰り返しになりますが、セキュリティのエコノミストやイノベーションの学者に質問があります。  
 タコグラフは[64]で記述されています。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]。