しかし、世界をつなぐことは、すべての悪いこととすべての悪い人々をつなぐことを意味し、今ではすべての社会的および政治的問題がソフトウェアで表現されています。  
–ベネディクトエヴァンス自由を求めて運動をしていると、悪い会社で酒を飲んでいることがわかります。  
25.1はじめに  
攻撃の多くは特定のアプリケーションに依存しており、すばらしい研究の多くもそうです。  
私たちのブログソフトウェアがハッキングされると、ボットネットサーバーが1つ増えるだけですが、お金が盗まれる可能性のある他のアプリ、プライバシー保護に依存するアプリ、権力を仲介するアプリ、および殺すことができるアプリがあります。  
この章では、セキュリティ研究の最先端にある4つのクラスのアプリケーションについて簡単に説明します。  
それらは次のとおりです。自律および遠隔操縦車両。機械学習、副次的学習から社会におけるAIのより一般的な問題まで。プライバシー技術;そして最後に、電子選挙。  
人々が同じ道路で他の車を運転しているため、自動運転車は困難です。  
プライバシーは社会における人間の相互作用の豊かさのために難しい。  
これらの問題はすべて、人間が実行できることとマシンが実行できることの間の境界をさまざまな方法で探索します。  
25.2自律および遠隔操縦車両  
その過程で彼と彼の父親エルマーは人工的な地平線を発明しました。  
ジャイロスコープは欠落している基準を提供し、サーボを介してエルロンとエレベーターを駆動することもできます。  
同じ建物のエンジニアは、初期のヘッドアップディスプレイと衛星ナビゲーション装置に取り組んでいました。  
3つすべてを合わせても、1,000万ドルからほとんど変化がなく、人と同じくらいの重さでした。  
精密に設計されたケージに3つの回転する機械式ジャイロではなく、携帯電話にはMEMS加速度計とジャイロを搭載したチップが搭載されています。  
40年間で、コストは6桁、質量は4桁減少しました。  
片手ヨットの先駆者たちは、1920年代から海を渡り、帆を寝かせたり、調理したり、修理したりするための自動操縦装置を開発しました。アマチュアは今、沿岸巡航のためのよりスマートな自動操縦装置を持っています。  
世界の海軍は、水中鉱山、それらを見つけるための自律潜水艦などを開発しています。  
25.2.1ドローン  
これらは1980年代初頭から使用されており、地面の近くを飛行することによって敵のレーダーの下に潜入し、地形の等高線マッチングを使用して慣性航法を更新します。  
1982年にイスラエルとシリアの間の戦争で彼らの最初の大規模な使用を見た。イスラエル空軍は偵察とおとりとしてそれらを使用して、最小限の損失でシリア空軍を一掃した。  
当初は偵察車両として設計されていましたが、中高度で何時間も標的地域に留まり、地面に標的を攻撃するためにヘルファイアミサイルを運ぶように改造されました。  
それは、より大きくより速い死神に取って代わられ、シリアにおけるイスラム国家との戦争の主力となった。  
20世紀を通じて、愛好家は小型のラジコン飛行機を建造しましたが、FAAは2006年に初めて最初の商用ドローン許可を発行しました。  
関心は急速に高まりました。数年以内に私たちの学生は無人偵察機を製造し、間もなくホビーショップで低コストのモデルを購入できるようになりました。  
しかし、武装勢力と犯罪の両方の用途があり、無人偵察機は麻薬と携帯電話の両方を囚人に配達するのに使用され、反乱軍はドローンに武器として使用するための即席の爆発装置を取り付けました。  
25.2.2自動運転車  
2004年に、アフガニスタンとイラクで即興の爆発装置に対する戦闘損失の増加に直面して、DARPAは自動運転車の開発を推進することを決定し、149マイルを超えることができるものを構築した人のための100万ドルの賞品との競争を発表しましたモハベは最速で砂漠化する。  
彼のロボット、スタンレーは、機械学習と確率論的推論を使用して、地形の知覚、衝突回避、滑りやすい起伏の多い地形での安定した車両制御に対処しました[1887]。  
2007年の彼らの次の課題は、砂漠からシミュレートされた都市環境に移りました。競技者は他の車両を検出して回避し、道路の規則に従う必要がありました。以前は、自動車メーカーは、アンチロックブレーキシステム（ABS）から始めて、着実に支援技術を追加していました。  
セクション23.4.1で説明した自動緊急ブレーキ（AEB）  
。  
DARPAの課題に触発されて、Googleはセバスチャンスランを雇い、2009年に完全自動運転車を作ることを目標にプロジェクト運転手を率いました。  
Teslaは、その「オートパイロット」ソフトウェアが高速道路やストップスタートトラフィックを制御できる無線アップグレードとして発売された2014年に、最初に製品を手に入れました。  
TeslaのElon Muskは2018年までに完全自治を予測し、2017年までにGoogleのSergey Brinを予測していました。その後、2016年にGoogleの自動車プロジェクトがWaymoとしてスピンオフされました。  
いつものように、誇大広告のサイクルが過ぎた。  
このサービスは、雨天時や砂嵐のときは利用できず、コントロールセンターで人間がリアルタイムで監視しています。  
どうしたの？  
自動化は、結果として生じる危険のいくつかに対処できます。前の車が突然ブレーキをかけた場合、ロボットはより速く反応できます。  
しかし、ここにも限界があります。  
たとえば、前の車が曲がり角を示して減速し始めたときに、田舎道を運転しているとします。  
しかし、AEBはこれを理解していない可能性があるため、ターンする車に近づきすぎると、AEBがアクティブになり、シートベルトで前方に投げます。  
一部のシステムは、高速道路の速度ではなく都市へのアクティブ化を制限しており、2020年には、すべてがより高価なモデルで利用可能なオプションになる傾向があります。  
2016年以降、保険会社は全体的なリスクを軽減することに満足しています。安全保証については、セクション28.4.1で説明します。  
セバスチャンスランと彼のチームがスタンレーを説明するために書いた論文は、全体的なテクノロジーについての有用な洞察を提供します[1887]。  
スタンリーの同時プロセスは、経路計画、ステアリング制御、障害物回避を処理しました。これは、22mまでのレーザー距離計、それを超えるカラーカメラ、およびそれを超えるレーダーを使用していました（スタンレーは、所定のコースで2000以上のウェイポイントを与えられたため、レースでは使用されませんでした）。  
これらのシステムはそれぞれ、多くの副問題を解決する必要がありました。たとえば、ビジョンシステムは、変化する光の状態や道路の色に適応する必要がありました。  
。  
たとえば、2018年3月に自動運転のUberがアリゾナ州のElaine Herzbergを殺害したとき、NTSBの調査で、Elaineが自転車を押していて、視覚システムが彼女を歩行者と他の何かとして識別することの間でフラッピングしたことが明らかになりましたが彼女は横断歩道にいなかったので、最終的には歩行者として認識されませんでした。  
最終的に、Uberは、残念ながら当時テレビを見ていたセーフティドライバーに依存していました1。  
民間航空の場合でも、オートパイロットが失敗した後、適切に操縦を回復するのに約8秒の飛行時間を要します。  
  
このような理由から、自動車技術者協会は5つのレベルの自動化を定めています。  
部分的な自動化–ソフトウェアはいくつかのモードでステアリングと速度の両方を制御しますが、人間の運転手は環境を監視し、ソフトウェアが混乱した場合にゼロ通知で制御を引き受ける責任があります。 3。  
高度な自動化–ソフトウェアは、人間が介入できると想定せずに、環境を監視し、一部の運転条件で車を運転します。  
完全な自動化–ソフトウェアは人間ができるすべてのことを実行できます。  
、つまりレベル1と2であり、保険業者は、「自律」や「自動操縦」などの単語は、自動車がレベル4で動作していると思い込ませて事故につながる可能性があるため、危険であると見なします。  
レベル4は、コントロールセンターに座って数十台の「自律」車を監視するバックアップドライバーを想定していますが、その場でセーフティドライバーと同じくらい迅速に危険を理解するための帯域幅はありません。  
それは車を運転する（または航空機を着陸させる）ために重要です  
レベル5は、人工的な一般的な知能を発明しない限り、どの程度実現可能でしょうか。  
別の難しいケースは、車がどちらかの側に駐車されている雑然とした郊外の通りです。ここでは、波、うなずき、または単にアイコンタクトを使用して、対向車を最初に誰が先に行くかを永久に交渉します。  
彼らは人間のドライバーよりもはるかに注意深くなり、大きなギャップを待つ必要があり、その背後にある人間のドライバーを困らせます。自動運転車は、警察官からの手信号を検出して停止することはできますか？ベッドを運ぶ8人の生徒やインドの寺院の行列に対処することは言うまでもありませんか？  
テスラは常に静止車両を確実に検出できるわけではありません。ビジョン、ソナー、レーダーを使用しますが、ライダーは使用しません。  
 レンジローバーは舗装道路と芝生の境界を常に検出できるわけではありませんが、4 x 4の優先順位ではなかった可能性があります。  
道路工事は自動車線維持システムで大混乱を引き起こします。塗りつぶされた古い白い線が光沢のある黒になり、光の条件によっては非常に目立つようになり、古いマーキングと新しいマーキングの間で自動車が前後に揺れる場合があります[632]。  
テスラには自動操縦のための「シャドウモード」さえあります。使用されていないときでも、ドライバーが次に何をするかを予測し、後の分析のためにその予測ミスを記録します。  
安全保証についてはセクション28.4.1で説明しますが、2020年の現状は、TeslaとNHTSAが、Teslaの顧客がAutosteerをアクティブにした後のクラッシュは少ないと主張しているのに対し、独立した研究所はもっと多いと主張しています。  
これらはスペクトルの深刻な端にある傾向があります。高速道路での死亡事故の約30％、死亡事故の半分を占めています。  
 そのため、高速道路の車線を維持し、衝突を回避するためにブレーキをかけ、チャイムに反応しない場合は道路の脇で停止するシステムによって、命を救うことができるはずです。  
 リスクサーモスタット、システムのアフォーダンス、およびマーケティングによってもたらされる期待の少なくとも3つの異なる要素を解決する必要があると思います。  
2つ目は、セクション3.2.1で説明したように、アフォーダンスはテクノロジーとの相互作用を条件付けるものであり、ドライバーアシスタンスシステムによって運転が容易になり、安全性が高まると、人々はリラックスして安全だと思います。より多くのリスク。  
Teslaが自動操縦機能を呼び出すには、オートパイロットがドライバーを騙して、テレビを見たり昼寝をしたりできると考えました。  
  
道路車両の電子セキュリティは、前の世紀にセクション14.3で説明したトラックタコグラフとスピードリミッターとセクション4.3.1で説明したリモートキーエントリーシステムから始まりました。  
2008年までに、人々はエンジンコントロールユニットの改ざん防止に取り組んでいました。業界はソフトウェアを使用してエンジン出力を制御し始めたので、あなたの車が120馬​​力であるか150であるかは、人々が自然にハッキングしようとしたソフトウェアスイッチになりました。  
彼らは彼らが不適切に調整された車の環境への影響を懸念していると主張しました、しかしあなたがそれを信じるなら、私はあなたに売りたい橋を持っています。  
車の内部データ通信は、強力な認証を備えていないCANバスを使用しているため、攻撃者は（たとえば）  
2015年、チャーリーミラーとクリスヴァラセクは、ボランティアのジャーナリストを含むジープチェロキーを携帯電話のリンクでハッキングし、車両を減速させて道路から外した[1316]と報道陣の注目を集めました。  
これは最終的に業界の注目を集めました。  
車をチューニングしたい愛好家がいます。サードパーティのコンポーネントやサービスも使用したいガレージがあります。また、セクション24.6で述べたように、ジョンディアのサービス独占にもかかわらず、トラクターを修理したい農家もいます。  
また、黒い帽子もあります。車の乗員と車を盗もうとする泥棒をスパイしたい諜報機関です。  
州の俳優や他の人は、2.2.1で説明した手法を使用して、車に埋め込まれた携帯電話を乗っ取ることができます。  
それで、特に自動車がより自律的になるにつれて、他に何がうまくいかないのでしょうか？  
クライスラージープのようなリモートエクスプロイトはすでにこれを実行している可能性があります。  
それらの1つが破壊された場合、継続的に送信するように再プログラムされる可能性があります。このような「荒れ狂う馬鹿」と呼ばれ、バス全体が使用できなくなります。  
車が高速で移動している場合、重大な事故のリスクがあります。  
ただし、パッチの適用にはコストがかかります。  
これについては、セクション27.5.4で詳しく説明します。  
2017年、エロンマスクは聴衆に次のように語りました。アメリカ ...彼の聴衆は笑い、3年後、彼は完全に冗談を言っていなかったことが明らかになりました。  
もう一方の端では、パフォーマンスアーティストのサイモンウェッカートが2020年2月にベルリン周辺で99台のAndroidスマートフォンを搭載した手押し車を引っ張ったため、Googleマップはどこに行っても交通渋滞を登録しました[1997]。  
また、外部からの攻撃にコンピュータが関与する必要はありません。  
インドと南ヨーロッパの一部の地域では、歩行者は渋滞した車の中を歩き、車に停車を警告します。この振る舞いがロンドンとニューヨークでも同様に現れるかどうかは興味深いことです。  
自動運転トラックの最初の夢はどこか離れているように思われ、複数のトラックが1人の運転手で配車ハブ間を車列で運転するという中間の夢も野心的であるように思われるので、ロビー活動で運転時間の法的制限を緩和することを期待できますか？  
しかし、テクノロジーの正味の効果が同じお金でトラックの運転手により多くの時間を働かせることである場合、それは25.3になります。  
制限された環境であってもレベル5の自動化が発生した場合、Googleが発明したいと考えているrobotaxisを最終的に確認できるようにするには、ソーシャルハッキングを安全性の側面として考える必要があります。  
Uberはこれらの法律を回避しようとしましたが、それはタクシー会社ではなく「プラットフォーム」であると主張しました。ロンドンでは、市長はそれらを禁止し、長年法廷でそれらに準拠させるために戦わなければなりませんでした。  
 責任ゲームもあります。  
しかし、コンピューターが車を運転していた場合、それは製造物責任であり、製造業者が支払う必要があります。  
完全に予測可能です。  
 たとえば、架空の画像を橋や道路に投影して車を混乱させ、クラッシュさせることができますか？  
私の研究室から家に帰る途中の道路の右側の曲がり角に家があり、その所有者はしばしば対向車に向かって車を停めました。  
結局、大型トラックは時間内に曲がらず、結局壁に落ちました。  
 これにより、次のトピックである人工知能、またはより正確には機械学習に進みます。  
25.3 AI / ML  
アランチューリングのような開拓者にとっては、チューリングテストからコンピューターにチェスをするように教える試みまでさまざまでした。  
1980年代には、日本が「第5世代コンピューティング」への大規模な研究プログラムを発表したことにより、研究の急増がありました。その取り組みの多くはルールベースのシステムに費やされ、Prologはコンピューターサイエンスカリキュラムの言語の1つとしてLispに加わりました。  
。  
 およびベイジアン分類子。自然言語処理（NLP）などのアプリケーションによって進歩が推進された  
NLPコミュニティはカスタムメソッドを開発しましたが、支払い詐欺検出器またはスパムフィルターを設計する一般的なアプローチは、大量のトレーニングデータを収集し、カスタムコード25.3を記述することでした。  
2000年代には、検索エンジン最適化企業があらゆる種類のトリックを使用して検索エンジンが依存する信号を操作し、エンジンが次々と反撃し、隠しテキストなどのアンダーハンドトリックを使用するサイトにペナルティを科したり禁止したりするため、検索は非常に敵対的になりました。  
これにより、検索ランキングの機械学習ベースのアルゴリズムのデバッグが困難になりました。  
ダンチレサン、ウエリマイヤー、ジョナサンマスシ、ユルゲンシュミッドフーバーが、人間と同様に手書きの数字と漢字を認識し、交通標識では人間よりも優れた深い畳み込みニューラルネットワークを訓練した2011年に、大きな変化が始まりました[ 435]。  
 120万枚の画像を分類することで記録を破る結果を得る[1098]。  
最も壮観な結果は、David SilverとGoogle Deepmindの同僚がAlphaGoを作成した2016年に発生しました。これは、世界のGoチャンピオンLee Sedol [1737]を破りました。  
それ以前は、機械学習を勉強したいと考えた研究生はほとんどいませんでした。それ以来、他のことを勉強したいと思う人はほとんどいません。  
  
機械学習とセキュリティの相互作用は1990年代半ばにまで遡ります。  
1990年代半ばにインターネットが一般に開放されたときにスパムが到着したことで、スパムフィルターの市場が生まれました。  
アリス・ハッチングス、セルゴ・パストラーナ、リチャード・クレイトンは、そのようなシステムにおける機械学習の使用と、悪者がそれらをだますために巧妙に仕掛けたトリックを調査した[939]。クラシファイアのトレーニングデータを汚染することは、非常に一般的な攻撃です。  
そして、そのような技術の活発な議論が地下のフォーラムで行われています。  
バティスタビジオとファビオロリは、より技術的な背景を提供します。2004年に、スパマーはいくつかの単語を変更することでスパムフィルターの初期の線形分類子を混乱させる可能性があり、そこから軍拡競争が始まりました[241]。  
  
機械学習システムに対する攻撃には、少なくとも4種類あります。  
モデルが使用中に自身を訓練し続ける場合、それを誤って導くことは簡単かもしれません。  
次に、推論フェーズでモデルの整合性を攻撃することができます。たとえば、モデルに間違った答えを与えることにより、  
アイデアは、モデルの予測誤差を最大化する摂動を選択することです。  
決定空間は高次元であるため、数学的に盲点が避けられません[1706]。ニューラルネットワークでは、決定境界が複雑になり、自明ではなくなります。  
マルウェア検出の世界では、SVMやディープニューラルネットワークなどの非線形分類器は、正しく分類されていれば、実際には線形分類器よりも回避するのが難しいことはありませんでした[241]。  
多くの場合、その結果は、ターゲットモデルの模倣として機能します。  
この近似攻撃は、ニューラルネットワークだけでなく、ロジスティック回帰や決定木などの他の分類器でも機能します[1901]。  
 [1900]。  
。  
たとえば、Ilia Shumailov、Yiren Zhao、Robert Mullinsと私は、ニューラルネットワークにキーを挿入して、死角が異なる場所に表示され、異なるキーを持つモデルが異なる敵対的なサンプルに対して脆弱であることを実験しました[1733]。  
AI / MLの原則は、機械学習にも適用されます。  
大規模なニューラルネットワークには多くの状態が含まれており、外れ値を処理する最も簡単な方法は、それらを記憶することです。  
セクション11.3で説明した、機械学習と差分プライバシーを組み合わせる方法は、活発な研究の対象です[1493]。  
Ilia Shumailov氏と同僚は、分類担当者に難問を投げかけることでサービスを拒否できることが多いことを発見しました。  
より複雑な攻撃は、これらのカテゴリにまたがります。  
ただし、これにより、フィルターを回避したり、ページの別の部分を誤ってブロックしたりするために、敵対的なサンプルを使用する広告主に公開されたままになります[1899]。  
 それは私たちがまだ学んでいることですが、私たちが言えることがいくつかあります。  
Webサービスへの入力をサニタイズし、侵入テストを行い、責任ある開示と更新のメカニズムがあるように、MLシステムでも同じことを行う必要があります[659]。  
セクション21.4.2.2で述べたように、MLシステムは実際のネットワーク侵入検知ではほとんど効果がありません。 Robin SommerとVern Paxsonがその理由を最初に説明しました。  
有能な対戦相手を複雑な企業ネットワークから遠ざけるという問題は、人工知能がこれまで得意だった問題ではありません。  
新たな敵対的攻撃が実際の被害を引き起こす可能性を低くしたい場合、状況に応じてさまざまなことができます。  
感度を下げると、なりすましが簡単になりなくなり、レーダーや超音波などの他のセンサーで補完して、ビジョンシステム自体の重要性が低下します。  
AI / MLが停止し、人間が運転するのを待っています。  
これが実際の生活の中での振る舞いです。セクション3.2.5.1で説明したように、祖先の進化環境では、敵対的な意図や部族のタブーの違反などのトリガーを感知するときは、さらに注意する必要があります。  
基本的な問題は、機械学習にコードとデータの境界をぼかし始め、システムがデータ駆動型になると、人々はそれらをゲームにしようとすることです。  
  
2016年以降の機械学習への関心の高まり、および人気のあるマスコミでの「人工知能」としてのその表現は、倫理に関する多くの憶測につながっています。  
しかし、企業はすでにその定義を満たしています！企業の不正行為の歴史は、企業が実際に非常に悪い振る舞いをする可能性があることを示しています（セクション12.2.6でいくつかの例を説明しました）。最も強力なMLシステムは、Google、Amazon、Microsoft、IBMなどの企業に属しています。  
1つの側面は、技術専攻のMLオファリングが独自のプラットフォームになり、特定の現実世界の問題を解決する多くの新興企業で使用されていることです[658]。  
プリンストンのトルコ人研究生であるアイリンカリスカン氏は、トルコ語から英語への機械翻訳が性別による偏見で行われていることに気付きました。トルコ語には文法上の性別はありませんが、トルコ語の文章を英語に翻訳すると、医師は「彼」、看護師は「彼女」に割り当てられます。  
実際、機械学習に基づく多数の自然言語システムは、トレーニングデータの偏見を吸い込みます。  
関連する政策問題はレッドラインである。  
この本の第2版で2008年に私は次のように書いています。「データマイニングテクニックに基づいて侵入検知システムを構築する場合、差別の危険にさらされます。  
不透明なルールはヨーロッパのデータ保護法にも違反する可能性があり、市民は個人データの処理に使用されるアルゴリズムを知ることができます。」 25.3。  
Manish Raghavan氏と同僚は、就職活動のスクリーニングと採用に使用されている「AI」システムを調査し、システムが新規採用者と会社の要件を一致させていると主張する数十の企業を見つけました。  
応募者は、「Ox- ford」または「Cambridge」という単語を白いテキストのCVに挿入するなどして、システムのゲームを習得します。  
機械学習は私たちが理解していない相関関係を見つけることができるため、それは重要なことです。  
「AI」、さらには「ML」は、テクノロジーの全体を表す一般的な用語です。  
そのため、企業はこの誇大広告を悪用し、そのメカニズムが1世紀前の統計的手法を使用していても、「AI」ラベルを販売しているものに平手打ちします。  
MLは、顔認識などの知覚のタスクを真に進歩させました（セクション17.3を参照）  
、スキャンによる医療診断、および音声からテキストへの変換–これらすべてにおいて、熟練した人間の能力を獲得しています。 2。  
これらには、熟練した人間でさえも同意できない多くのハードエッジのケースがあります。  
MLは、従業員のパフォーマンス、学校の結果、将来の犯罪行動の予測など、社会予測のタスクで進展を見せていません。  
これは虚偽の主張であるため、時間の経過とともにどれほど正確であるかがわかります。2030年にこの本の第4版が発行されれば、さらに多くのデータが得られます。  
直感的に、私たちは人々に判断と機械の退屈なことをする仕事をしてもらいたいと思っています。しかし、実際にそれを機能させることは、見た目よりも難しい場合があります。  
いずれにせよ、道路には多くの衝突があり、倫理と政治についての多くの議論があります。  
AI / MLおそらく倫理に取り組む最善の方法はこれです。  
（実際、線形回帰は約1世紀にわたって継続的に使用されてきました。それらは機械学習としてブランド変更されたばかりです。）  
セクション10.4.5.1でレコードベースの健康および社会政策研究の文脈で倫理について議論したとき、IT企業とその顧客が医師、教師、その他が長年にわたって蓄積してきた知識を無視したために、問題の多くが生じていることに気付きました紙ベースの記録を扱う方法。  
どの子供が犯罪に転向する可能性が高いかを予測する場合、そのような指標が非常に非難される可能性があることは何年も前から知られています。  
児童福祉法とプライバシー法の両方が、そのような指標の共有に反対しています。  
 「予測的ポリシング」については、「通常の容疑者を切り上げる」というポリシーをコンピューターに正当化させるためのもう1つの方法である可能性があることが研究により示唆されています[677]。  
 MLテクニックを使用して、容疑者が飛行リスクまたは再犯リスクをもたらすかどうかについての保釈審問、および容疑者が危険かどうかについての判決審問において裁判官に助言するためにML技術を使用する場合にも同様の問題が発生します。  
それでもMLは、監視、プライバシー、検閲などの問題について長年にわたって浮上している均衡の一部を混乱させる可能性があります。これにより、すでに強力な俳優がさらに強力なツールを利用できるようになり、古い虐待を復活させる新しい言い訳が作成されます。  
 セクション17.3で見たように、いくつかの都市（サンフランシスコを含む）セクション11.2.5で、位置情報とソーシャルデータによって匿名化が非常に困難になる方法と、人々のFacebookデータを政治広告のターゲティング用にマイニングする方法について説明しました。  
要するに、機械学習に対するチャージシートは、プライバシーと監視のバランスを監視に向け、権威主義政府を他の方法で促進する一方で、技術専攻の力を定着させるのに役立つ技術の1つであるということです。  
では、私たちが今住んでいるこの電子村でプライバシーを確​​保するために、実際に何ができるでしょうか。  
25.4 PETSと運用上のセキュリティ  
セクション11.2.5では、Facebookのいいね！が4つしかないことで、ほとんどの場合、注意深い観察者がストレートかゲイかを判断できること、およびこの観察結果がとりわけケンブリッジアナリチカスキャンダルにつながったことを示唆する調査について説明しました。有権者の好みが隠されて詳細に文書化された場所。  
これは、内部告発者など、権限に矛盾する人々に問題を引き起こす可能性があります。  
学術的権威の悪用は、教授に対する匿名の学生のフィードバックと会議論文提出の匿名の審判によって対抗されます。  
プライバシーは、言論の自由の必要な先駆けにもなり得ます。  
そして、その懸念がより戦術的であるその日の政府のためにクマのわなを掘る野党政治家がいます。  
内部告発者を保護する法律も制定しています。  
 技術以前の社会では、2人の人が他のすべての人から少し離れて会話をし、会話の内容を明確に示す証拠を残さなかった。  
つまり、多くの通信が拒否されました。  
たとえば、イギリスの訴訟者は、和解を提案する別の人に「偏見なし」のマークが付いた手紙を書くことができ、この手紙は証拠として使用できません。  
それで？  
産業革命が起きるまで、ほとんどの人は小さな村に住んでいました。そして、町に引っ越すことは救いでした-実際には革命でした。  
多くの点で、インターネットの影響は「電子の村」に私たちを連れ戻すことでした。電子通信は距離を縮めるだけでなく、いくつかの点で私たちの自由ももたらしました。  
 もう少し具体的に説明するために、特定のプライバシー問題を抱えている一部の人々について考えてみましょう。  
アンドリューはテキサスの宣教師であり、そのウェブサイトはイランで多くの改宗者を魅了しています。  
彼に接触した人々の一部は本当の改宗者ではなく、背教者を探している宗教警察官であると彼は疑っています。  
彼が改宗者と個人的に通信するためにどのような技術を使用するべきですか？  
ベラはあなたの10歳の娘であり、オンラインで匿名のままであるように先生から警告されています。  
 3。  
以前は、患者が目立たないように訪問できる町のわかりにくい家で練習していました。  
患者のプライバシーを保護するための賢明な方法は何ですか？  
ダイはベトナムの人権労働者であり、独立した労働組合やマイクロファイナンス協同組合などを設立しようとしている人々と接触しています。  
彼女は同僚とどのようにコミュニケーションを取るべきですか？  
エリザベスは、合併について助言している投資銀行のアナリストとして働いています。  
彼女の反対者は他の企業で彼女のような人々です。  
フィロズは、テヘランに住む同性愛者であり、同性愛者は資本犯罪です。  
7。  
彼は将来オフィスに人員を配置する一部の警官がマフィアの給与に含まれることを知っており、潜在的な情報提供者もこれを知っています。  
 8。  
彼のクライアントのほとんどは、中東と北アフリカで戦争や悪政権を逃れています。  
彼はフランス、イギリスなどの同僚と調整する必要があります。  
 9。  
彼女は次のエドスノーデンに着陸することを夢見ています。  
 10。  
アイリーンは喜んで家族の汚れを掘り出しました。彼のメールを読んだり、彼のソーシャルメディアアカウントから人種差別的なツイートを送信したり、彼の選挙運動用の箱を北朝鮮に送ったりしたい人は他にもたくさんいます。  
 プライバシーはメッセージの暗号化だけではありません。  
アンドリューは彼の交通を無害に見せなければなりません–警察が背教者の交通がどんなものであるか知っていても警察が改宗者を見つけることができないように。  
つまり、WickrがSignalやSkypeよりも安全な製品であるかどうかだけでなく、その国で何人がそれを使用しているのかということです。子供にとっての1つのリスクは、後で恥ずかしいかもしれない不注意なことを言うことです。  
あなたの努力のほとんどは彼女を教育することに入るでしょう。  
儀式ではなく、理解を与える必要があります。  
アンドリューとフィロズは散発的な興味だけに直面するかもしれないが、グラツィアーノ、フリスト、ジャスティンはやる気のある対戦相手を持っている。  
彼女は自分を守るために匿名の通信を使用していませんが、まだ警察の注意を引いていない他の人を保護するために使用しています。  
アンドリュー、チャールズ、ダイ、グラツィアーノ、アイリーンは、彼らが対処する脆弱な人々を保護するためにいくつかの問題に行きますが、フィロズが関心を持っているサイトは彼の安全をあまり気にしません。  
ジャスティンの場合、それは不注意な内部関係者です。ロシア人がイレーヌに与えたいジューシーなものは、彼のキャンペーンボランティアの個人アカウント、および組織的な防御に含めるのが難しい友人や家族の個人アカウントに住んでいます。努力。  
フリストが刑務所に入れられるのは、警察が合理的な疑いを超えて彼に対して訴訟を起こした場合のみです。アイリーンは、証拠のバランスについて名誉毀損訴訟を弁護できれば、ジャスティンを解任することができます。エリザベスやフィロズにとって単なる疑惑は悪い知らせかもしれない。  
セクション22.2.1で、通話の追跡を望まない人がプリペイド携帯電話を購入し、しばらく使用して捨てる方法について説明しました。  
では、オンラインでのハードプライバシーの現状について教えてください。  
25.4.1匿名メッセージングデバイス  
人々が電子メール、メッセージングサービス、または昔ながらの電話サービスを使用しているかどうかに関係なく、ソーシャルグラフへのアクセスにより、警察官は友情ネットワークを計画することができます–マーケティング担当者もそれを手に入れられるときにこれを行います[598]。  
現在、ほとんどの人がデフォルトでTLS暗号化されたWebメールサービスを使用しているため、より複雑になっていますが、同じ原則が適用されます。  
HristoがSignalを使用して、ケヴァンがイギリス海峡を横断するスピードボートで8人を連れてくるように手配するとします。  
KevanまたはHristoも自分の電話を使用して家族とチャットする場合、警察がトラフィック分析を使用してネットワークをマッピングするのに役立つ可能性があります。  
同様の問題は、ダイとグラツィアーノの秘密工作員が直面しています。  
 同じように。  
一般に発売された最初の暗号化電話は、おそらく2014年にSilent CircleのBlackphoneで、政府機関、特殊部隊、人権労働者に販売されたと考えられます。  
Ed Caesarは、ドイツのサイバーバンカーから暗号化電話ビジネスを宣伝した人々の何人かについて説明します。ドイツは、2019年9月に襲撃されて閉鎖されるまで、違法Webサイトの最大のホスティング会社でした[364]。  
;マイクとカメラが無効になっている可能性があるため、GCHQがそれらを監視デバイスに変えることはできません。 GPSも無効になっている可能性があります。標準の警察の法医学キオスクでは読み取ることができません。また、電話とメッセージングサーバーの両方で構成されるクローズドシステムの一部であり、電話番号ではなくユーザーIDで相手を識別します。  
市場には、仮想通貨のオペレーターやスパイからマネーロンダラー、麻薬の売人まで、あらゆる種類の人々が含まれています。  
また、密輸業者も麻薬を密輸し、密輸業者が仮想通貨群衆のために働く派手な税理士を必要とするだけのお金を稼いでいるため、ネットワークの影響は、善と悪の両方の理由で州の監視からプライバシーを求めるあらゆる種類の人々を引きずることができます。  
英国人以外の読者の利益のために、左と右の新聞は、やや異なる言葉でフリストと彼の人間の貨物を見るとここで言及するかもしれません。  
それでは、GCHQが背を向けないようにするために、Hristoは何を購入できるでしょうか。  
その年の4月に、オランダとカナダの当局は彼らを襲撃し、サイバーバンカーに関与していた所有者を逮捕しました。  
翌年、オランダの警察は、Iron Chat [792]と呼ばれる暗号電話システムが壊れたと主張しました。  
CEOのVincent Ramosは、世界中の麻薬の売人に電話を供給することに罪を認め、彼の判決聴聞会で、検察官は彼が同僚に送ったメッセージを読みました。  
Cuz私はたくさんのビジネスを閉じました。  
シナロアカルテル、それが問題です」[278]。  
次の市場リーダーであるEncroChatは、改良されたAndroidフォンを使用しました。6月13日、EncroChatはハッキングされたことに気付き、顧客にすぐにスマートフォンを処分するようアドバイスしました[1922]。  
したがって、Grazianoのような警官は、暗号電話システムを停止するための標準的な手引きを持っています。  
実際、PGPが最初に1990年代に登場したとき、それは暫定IRAによって北アイルランドでのイギリスの統治に対する反乱で採用されました。  
PGPは連絡を簡単にしました。  
暗号化された電子メールを自分に送信することで報告することもできます。  
25.4.2ソーシャルサポート  
政府の最新の愚行に豆をこぼしたい上級公務員が彼女に近づいた場合、物語が現れるとすぐに「モグラ狩り」が始まります。  
アイリーンは、リズが識別、発砲、起訴される可能性を最小限に抑えるのにどのように役立つでしょうか？  
大きな問題は信頼の確立であり、それは両面のプロセスです。  
彼女には実話がありますか？  
 それは、彼女が政治ゲームの一部として彼女の大臣の暗黙の承認を得て提供している、半認可されたリークですか？  
 アイリーンや彼女が働いている新聞の信用を落とすことを目的とした挑発なのでしょうか？  
 物語が出たとき、他に誰がそれを漏らしたのだろうか？  
しかし、多くの場合、内部通報者はストーリーが発表されると完全に公開されます。  
したがって、ベストプラクティスは、アイリーンがリズに連絡した後できるだけ早くリズと直接会うことです。  
話が終わった後でリズが容疑者10人のうちの1人であり、首相が治安局長に向かって叫び始めた場合、彼女は彼らすべての既知のデバイスがティータイムによって危険にさらされると考えたほうがよいでしょう。  
その後、多くの新聞は、内部告発者が連絡するための技術的手段、PGPキー、Signalを使用するジャーナリストの携帯電話番号、および人々がファイルをアップロードできるようにするSecureDropと呼ばれる機能を提供するために急いでいます。  
まず、そのようなメカニズムは使いにくい。  
第2に、内部告発者は、適切な運用上のセキュリティ手順を考案するために危険を理解する必要がありますが、通常の新聞では、たとえばこの章のように危険について説明していません。  
（暗号化電話の方が使いやすいでしょうが、アイリーンにはおそらく予算がありません。リズがそれを手に入れたら、景品になる可能性があります。）  
ほとんどの内部告発者はサイズ1の匿名セットであり、それらの開示は国家機密ではなく詐欺と虐待に関するものです。  
しかし、多くの場合、不正行為を明らかにする決定には、発砲したり、非難されるなどの個人的なコストがかかる場合があります。  
ハーヴェイワインスタインにレイプされた数人の女性が発言する勇気を見出して初めて、何十人もの人々が前に出てきたのです。  
精神分析医のチャールズは、彼が患者に提供できるプライバシー（私たちがメアリーと呼ぶかもしれない）が治療の仕事に不可欠であることを知っています。  
 実際のリスクはありますが、プライバシーを両方に理解しにくくし、治療における促進者としての役割を損なうことになります。  
ほとんどの場合、それでも2Evenでは、最新のプリンターがドキュメントに埋め込んだセクション24.4.3で説明したマシン識別コードなど、ジャーナリストが知っておくべきことがもっとたくさんあります。  
恐怖は実際のリスクよりもはるかに大きくなりますが、リスクが本当である場合もあります。彼女はダイ、アイリーン、またはリズかもしれません。  
チャールズは、アイリーンが彼らの最初の会議でリズに与えるかもしれない種類のopsecの詳細な説明との関係を始めることはできません。  
ベラのような子供たちと接するとき、優先事項は、彼らが学び、成長できる穏やかで安心できる環境を提供することです。  
親としてのあなたの使命は、子供たちが権限を与えられた市民に成長するのを助けることであり、架空の怪物から身をかがめるように彼らを訓練することではありません。  
当局は彼女が効果的であることを止めようとしているので、彼女のケースはチャールズのものよりはるかにトリッキーです。  
Daiのような人権労働者は確かにSkype、Tails、Tor、PGPなどの一般的なツールを使用してトラフィックを保護していますが、彼らが受ける攻撃は単なる技術的なものではありません。彼らはスパイ小説のものです。  
彼らは電話を暗号化するとき、秘密警察がその片側（または両方）を取得しているかどうか疑問に思う必要があります  
マイクが隠されていない場合もあります。窓際にショットガンマイクを向けて家の外に堂々と立っている警察の活動家から聞いたことがあります。これの一部は、スパイ映画と同じです。秘密のエントリを検出するためにテルテールを残し、常にノートパソコンを携帯し、バグの発生しにくい場所で機密の会話を行います。  
 法律の違反を回避する必要があり、複数のサポート体制を育てる必要があります。下流の新入社員に秘密裏のサポートを提供するだけでなく、海外のNGOや政府からの明白なサポートを受けます。  
ダイのケースは、チャールズのケースの逆です。彼女が新しい新入社員を取得するとき、トレードクラフトでそれらを訓練することは、導入、社会化、およびサポートプロセスの一部です。  
（スパイや密輸業者はもっと知っているかもしれませんが、彼らは話していません。）  
最も全体主義的な支配者以外のすべての支配者が対抗勢力を疎外、飼い慣らし、または協同しようとする複雑なゲームがありますが、反体制派の動きはそれに応じて進化します。  
最高のopsecを持つグループは最も速く成長することができ、最も過激なグループは最大の信頼性を持つことができます。  
。  
後で熱くなる場合に備えて、彼はいくつかの機能の使用を控えているので、対策を講じていないものを準備しています。  
25.4.3土地に住む  
これを国外での生活と呼ぶかもしれません3。  
すべての国のエリートはたむろする場所を持っているので、上級公務員が著名なジャーナリストに会いたい場合は、誰も何も通知せずにロンドンの紳士クラブまたはバージニア州のカントリークラブでオープンにチャットできます。  
したがって、匿名のコミュニケーションを即興で作ろうとするときに最初に尋ねるのは、すでに共有しているクラブまたはプラットフォームです。  
そこにも、暗号化された通信を持つユーザーコンテンツを利用できるプラットフォームが見つかります。LinkedinとAmazonの書評の2つの例です。  
2つ目は、脅威モデルです。  
大規模な秘密警察でさえ、一度に非常に多くのファイルしか処理できません。  
しかし、メアリーが突然有名人になると、人々は彼女のメンタルヘルスにすぐに興味を持つようになります。  
イランでも、いくつかのopsecが必要です。  
 他の改宗者たちとも話し合うか、宗教警察は偽の改宗者たちからそれを学び、ノックしてくる。  
すべてのユーザーの中で、投資銀行家のエリザベスが最も単純なケースかもしれません。  
Torは注意して使用するとかなり良い匿名性を提供し、リスクは低いです。ターゲットが彼女の興味を疑う場合、3このフレーズは、必要に応じてターゲットの脆弱性を直接利用してシステムを攻撃し、リモートアクセスのトロイの木馬を残さないハッカーにも使用されます。  
彼女は自分の人生ではなく、いくらかお金を失います。  
ジャスティンもハイステークスでプレーしていますが、管理上の問題ははるかに少なくなっています。  
リズは重大なリスクに直面しており、アイリーンから提供されるサポートの質はさまざまです。  
最後に、フォレンジックの問題があります。  
針を見つけたくない場合は、より大きな干し草を作ります。  
そして、カジュアルな検索者がコンテンツにアクセスできないようにするためのアドホックな方法はたくさんあります。修復可能な方法でメモリスティックを損傷したり、物理的に隠したりする可能性があります。  
これはすべてトレードクラフトに戻ります。  
日常的な交通分析に打ち勝つには、受付として1日の仕事を得るだけで十分かもしれません。町の全員が医師の手術に電話をかけた場合、誰かが手術を呼び出したという事実はほとんど情報を伝えません。  
25.4.4すべてをまとめる  
 1。  
彼は改宗者に会ってopsecで訓練することができず、入手可能で目立たないものを使用する必要があります。  
2。  
孫にTorを使わせることを夢見たことはありません。それはただ不気味です。  
子供たちはこれを楽しみ、敵対的思考の芸術をゆっくりと吸収します。  
3。  
彼が患者のメアリーを知るようになると、彼は時々、流れに沿って、彼女を怖がらせるのではなく、彼女に力を与える限り、彼が適切で必要だと思う提案を時々行うかもしれません。  
この環境について交渉するのは難しいかもしれません。インフォームドコンセントは、患者とセラピストの間の非対称なパワー関係のため、治療において困難な問題です。  
4。  
5。  
彼女の主な問題は、それを適切に使用し、ゲームを流さないようにターゲットWebサイトに対して行うクエリの種類に注意を払うことです。フィロズは調子が悪いので、率直に言って、私が彼の状況にあったのなら、私はドイツへの散歩に出発しました。  
彼は、警察に襲撃された場合に何が起こるかを事前に検討する必要があります。  
 7。  
クライアントエンドで1人または2人の裏切り者に対して秘密のネットワークを防御するのは十分に悪いです（Andrewはそうする必要があります）。  
彼の解決策の一部は、セクション10.2で説明したように、仕切り付きの警察の記録保管システムであり、曲がった警官がすべてにアクセスできないようにすることができます。  
8。  
彼の立場から、ダイから、長期的には最高のopsecを持つグループが勝利することを学びました。  
短命のメッセージを含むシグナルなどのチャットアプリを使用し、電話とSIMカードを定期的に変更する場合、どの同僚が懲戒処分を受けているかを確認し、誰を何に信頼するかを決定できます。  
ジャーナリストのアイリーンは、すべての最も困難な仕事の1つを持っています。  
調査ジャーナリストも貿易工芸品を必要としています。  
プライバシー技術について基本的な知識があるだけでは十分ではありません。彼女は、極度のストレスにさらされており、彼らの生命の危険にさらされている可能性のある連絡先に適切な戦術を教える方法を知る必要があります。  
（そして、この仕事がますます重要になり、高度に熟練するようになると、GoogleとFacebookがすべての広告を食い尽くすため、マスコミが利用できる予算は崩壊します。）  
ジャスティンも難しい問題を抱えています。  
しかし、彼はおそらく自分の脆弱性を理解しておらず、最善を尽くすことを期待して、ただ進んでいきます。  
身を隠すために特別な努力をしなかった人々でさえ、追跡できなくなる多くの方法があります。  
また、ISPは不適切なログを保持することが多く、その後トラフィックを追跡できません。  
そして、テクノロジーは常にopsecを難しくしています。  
  
2010年1月に、イアンフレミングとジョンルカーの小説で説明されているような伝統的な諜報機関の貿易品がほつれ始めているという警告を受けました。  
過去にはそのような殺害は秘密にされていましたが、UAE当局は今回、CCTVのすべての映像を収集して調査し、それをエージェントのホテルの滞在や国境通過と関連付けました。  
英国とオーストラリアはパスポート犯罪でイスラエルの外交官を追放した[307]。  
2番目の警告は2013年に来て、レポートは2003年にイタリアのアブオマールと呼ばれるイスラム教の聖職者の誘拐を分析し、それをCIAに固定し、不在のイタリア警察によって多くのエージェントが起訴された[1274 ]。  
個人情報の兵器化は続いています。 2016年の調査権限法により、英国政府は大規模な個人データセットを所持している企業に要求することができ、政府機関は信用記録や医療記録などにアクセスできるようになりました。  
国防総省はスタッフに消費者向けDNAテストキットを使用しないように指示し、中国人はデッドドロップのようなよりローテクなものを支持するように言ったが、防衛および諜報機関はさまざまな方法で対応してきたが、銀の弾丸があることは明らかではない。  
この文脈で、中国の「AI覇権」への入札は懸念されています。  
セクション17.3で顔認識について説明しました。中国の都市はCCTVシステムにまたがっているので、確実に人々をフォローできます。  
 マルチセンサーデータフュージョンアプリケーションでの機械学習の使用は簡単ではなく、この章で前述したように、社会予測でうまく機能しないか、まったく機能しない傾向があります。  
一方で、ジャスティンの事件についての議論が明らかになるように、やや混沌とした民主主義国家では、政治キャンペーンを攻撃から保護することは困難です。  
次に彼らに目を向けます。  
25.5選挙  
投票システムは非常に多様であるため、米国の選挙は何年もの間、投票技術のテストベッドでした。  
また、他のほとんどの旧イギリス植民地が含まれている連邦からの重要な経験もあります。加盟国のすべてが何らかの形で選挙を行っている[329]。  
学校では、現代の憲法をどのように進化させたかという歴史の変種をすべて学びました。  
ギリシア人とローマ人は、議会、評議会、法廷に座る代表者を選択するメカニズムを試しましたが、民主主義が寡頭政治に退化したり、君主制が権力を掌握したりすることがよくありました。ローマ帝国はこれらの実験を終わらせましたが、理想はスイスとイタリアの都市国家を介した教皇選挙と中世ギルドを通して続きました。  
また、17世紀には新世界で最初の集会があり、18世紀にアメリカの革命が起こりました。創設者たちはギリシャとローマのモデルに触発されました。  
早期選挙にはプライバシーがありませんでした。ローマの選挙人は候補者の後ろに並んでおり、公開抗議による投票は19世紀まで標準であり、贈収賄と脅迫につながりました。  
1832年の最初の近代的な改革では、選挙区の変更が導入されました。産業革命で生まれたイギリスの都市のいくつかには議員がおり、他の選挙区には有権者がほとんどなく、MPは地方の地主によって選ばれました。  
最終的に、1872年に秘密投票が導入されました。  
南北戦争は奴隷制度を終わらせ、フランチャイズをすべての人に拡大しました。しかし、復興の失敗後、黒人市民の投票を阻止するために、南軍の元の州は識字テストやその他の法律を考案しました。  
虐待が蔓延していた。今日まで、英国、米国、その他の国の政治家は、公正な手段を用いて、支持者に反対者よりも多くの票を投じさせようとしている。  
25.5.1投票機の歴史  
多くの都市や州には、投票を取り消すだけでなく、それを操作する政治的な「機械」があり、アメリカの選挙はイギリスのように全国的にではなく、州や郡のレベルで組織されているという事実を利用しています。  
これを押し戻すために、発明者は、透明な投票箱から、レバーが引かれたときに機械的カウンターを計時する投票機まで、すべてを思い付きました。  
ルイジアナ州では、ロング兄弟がアザラシを倒し、数を望ましい結果に設定して、州を何年も運営していました。  
機械式投票機には、一般に割りピンやその他の機械的リンクという形で、約100ビットのプログラミング機能があり、誰も理解していませんでした。  
  
発明者らは、ピアノのピアノに触発されて、紙ロールに穴をあける競合タイプの機械を考案しました。打ち抜かれたカードは、集計機やコンピュータによって普及した後、広く使用されるようになりました。  
また、投票箱に落とされると匿名になります（指紋を心配しない限り）  
2000年の米国大統領選挙では、その結果、パンチカードマシンを使用していたフロリダがオンになり、再集計には、投票者がカードから打ち抜いた段ボールの小さな長方形であるチャドに関する議論が含まれました。  
 パンチが貫通していないディンプルはどうですか？  
結局、最高裁判所は再集計を停止し、ブッシュに選挙を与えた。  
 新しい選挙装備の購入に38億ドルを割り当てました。  
これはセキュリティエンジニアを驚かせました。  
政治家は、機械式または紙製の投票システムをできるだけ早く電子機器に置き換える必要があると考えていましたが、セキュリティの専門家は同意しませんでした。  
国立標準局のロイ・ソルトマンによる1988年の報告は、失敗する可能性が高いことの大部分をすでに詳しく述べていた[1641]。  
 19世紀のレバーマシンの子孫であるマシンは、通常、候補者や他の投票オプションを画面に表示し、有権者の入力を記録していました。  
このような「投票のめくり」は、2006年にフロリダ州サラソタで広く報告されており、根本的な原因が使いやすさなのかテクノロジーなのかが不明でした（たとえば、感度の低いタッチスクリーンの分類方法による）。  
いずれにせよ、有権者の3分の1は、レビュー画面での誤った投票を無視しました[991]。  
河野嘉一氏と同僚はそれを分析し、機器が「他の状況で期待される最低限のセキュリティ基準でさえはるかに下回っている」ことを発見しました。有権者は無制限の票を投じ、内部者は有権者を特定でき、外部者もシステムをハッキングする可能性があります[1075]。  
これは騒動につながり、Yoshiの主要な勧告を実装するための法律を要求し、有権者検証可能な監査証跡が存在すべきであると述べました。  
 一部のDREマシンでは、これはすべての投票者の行動を記録する不揮発性メモリカートリッジの形式で提供されますが、これによりプライバシーに緊張が生じます。DRE以外のほとんどの機器は、投票者が記入した投票用紙またはカードを、ペンまたは特別な投票マーキング装置を使用してスキャンし、投票箱に落とす光学式スキャンマシンで構成されていました。  
次の選挙サイクルでは、カリフォルニア州国務長官であるデブラボーエンが、カリフォルニア大学の教授であるデイビッドワーグナー氏とマットビショップ氏が率いる大規模なコンピューター科学者チームに、州の投票システムの徹底的な評価を許可しました。  
彼らが調査したすべてのDRE投票システムには、攻撃者が選挙結果に影響を与えるために悪用できる特定の脆弱性に直接つながる重大な設計上の欠陥がありました。  
カリフォルニアはそのような急進的な行動をとることができました。おそらく2004年に投票した900万人の4分の3が紙または光学式スキャンの投票用紙を使用してそうしたのです。  
オハイオ州も同様で、同様の結論に達しました。  
;バッファオーバーフロー;役に立たない物理的セキュリティ。 SQLインジェクション。改ざんされる可能性のある監査ログ。文書化されていないバックドア[1261]。  
しかし、まだうまくいかないことがたくさんあります。  
ただし、一部のマシンは人間が読み取れるマークと機械が読み取れるマークを別々に作成します。そのようなマシンがハッキングされる可能性がある場合、テキストに「ゴア」と書かれ、バーコードに「ブッシュ」と書かれた投票カードを印刷できます。  
英国では依然としてゴールドスタンダードが手書きの紙の投票用紙ですが、米国では投票用紙マーキングマシンのベンダーが機器を販売するために障害者権利運動家を募集しています。  
トニーブレア首相の政府は、郵便やその他の欠席形式の投票の使用を段階的に拡大しました。これにより、野党は投票の購入と脅迫を容易にしたため、これが批判されました。  
 は、投票者に郵便投票を選択するよう圧力をかけ、投票用紙を収集して記入し、提出することができます。  
最後に、2007年5月の地方政府選挙では、電子投票パイロットが英国中の11の地域で開催されました。  
カウントは紙よりも遅かった。システム（光学式スキャンソフトウェア）  
（プリンターは印刷の途中でインクを交換したため、投票用紙の半分が「間違った黒の色合い」でした。）  
最終的に、全員が家に帰れるように、帰国役員は保証書（その場でベンダーが書いたもの）を受け入れました  
しかし、この演習では、さまざまな関係者の代表が深刻な不安を抱きました。  
選挙委員会はこれに同意しなかった、そしてこの経験は英国に今日まで手で数えられ、印が付けられた紙の投票用紙を使い続けることを説得した。  
   
この経験は、ソフトウェアの独立性の重要性と達成の難しさの両方をもたらしました。投票ソフトウェアの検出されない変更やエラーは、選挙結果に検出できない変化やエラーを引き起こし得ないという特性です[1608]。  
しかし、実際にそれをどのように行うのですか？  
2020年のコンセンサス見解では、システムは、ソフトウェアで問題が発生した結果として発生する不正またはエラーの確率に厳格な制限を課す可能性があるリスク制限監査をサポートするように設計する必要があります。  
カウントが近い場合、または不一致が見つかった場合は、さらに多くのボックスをカウントできます。  
 暗号学者は、投票集計をより検証可能にしようとしました。  
セクション5.7.7でメカニズムを説明しました。匿名性と監査性を同時にサポートする必要があるため、これは興味深い暗号設計の問題です。  
30年以上の研究の後、現在、これについてよく理解されたメカニズムがあります。  
すべての投票用紙が適切に形成され、結果が適切に復号化されるようにするには、もう少し作業が必要ですが、結果はソフトウェアに依存しないカウントです[223]。  
暗号化による投票集計は「エンドツーエンドの検証可能」として販売されていますが、この主張はやや野心的です。  
セクション18.6.1で説明した電子署名デバイスと同様に、信頼できるユーザーインターフェイスがないため、投票マーキングデバイスまたはスキャナーのバグやトロイの木馬について心配する必要があります。  
それでも、有権者登録、投票帳、結果集計、および結果の発表に対する攻撃を心配する必要があります。  
次に、電話のマルウェアや、設計と実装の品質についても心配する必要があります。オランダでは別の興味深い脅威が出現しました。  
彼らはいくつかのテストを実行し、主要ベンダーであるNedapのマシンがテンペスト攻撃に対して脆弱であることを発見しました：単純な機器を使用して、投票所の外に座っているオブザーバーは有権者が選択した当事者を確認できます[785]。  
。  
他の国については、状況は複雑です。  
選挙は、野党候補者を投票用紙から降ろすために偽の刑事告訴を提出する、または単に彼らを誘拐して殺害するなど、より伝統的な方法によって不正が行われている。  
私がこれを書いているニュースは、「ヨーロッパの最後の独裁者」であるアレクサンドルルカシェンコが選挙で投票の80％以上を獲得したと宣言したベラルーシでの選挙後の不安です。投票の70％を実際に獲得しました。  
その後、ルカシェンコは結果として生じたデモを力ずくで鎮圧した[611]。  
近年、人口登録をめぐって多くの問題が発生しています。セクション7.4.2.2で、国民IDカードを再発行し、民族グループがカードを入手しにくくして大統領を支持する可能性を低くすることで、発展途上国が選挙をどのように実施しているかについて説明しました。  
これは非常に古い脚本です。  
2000年のフロリダでさえ、チャドの吊り下げのために投票された投票よりも、登録の乱用の結果として、より多くの有権者の権利が奪われました。  
投票用紙や投票機があまりにも複雑で、教育水準の低い人の権利を剥奪されたかどうかについての訴訟もあった。  
たとえば、ジョージア州は私が2020年に書いているときに完全に混乱しているように見えます。何年も投票を困難にしようと試み、ディーボルド機の既知のフローを修正できず、ロシア人の標的となった後、州政府は裁判所にシステムの交換を命じられました。  
しかし、注目の主な焦点は選挙でのソーシャルメディアの使用に移っています。  
セクション8.5で説明したように、GoogleとFacebookで使用される広告オークションメカニズムは、入札金額に「広告の品質」と呼ばれる係数を掛けます。これは、人々が広告をクリックする確率であり、ソーシャルメディアの場合は、 共有する。  
セクション2.2.3で説明したように、2016年のもう1つの要因はロシアの干渉でした。  
彼らはイリノイ州とフロリダ州（そしておそらく他のいくつかの州）のシステムにハッキングしました  
クリントンが勝利した場合、それらの州のいずれかが彼女に投票した場合、「詐欺」の証拠が彼女の大統領職を弱体化させるために現れた可能性があります。  
 この本のリリースが予定されているため、アイオワ州の民主党予備選挙で結果集約をめぐる大失敗[637]があり、ロシア人が再び扇動派共和党キャンペーンをオンラインで実行している[1619]ことに注意します。  
トランプ氏は、選挙が盗まれた場合にのみ失う可能性があると主張して、共和党全国大会での地位を整えた。  
8月に、主要なテクノロジー企業は選挙操作を行うための同盟を発表しました[963]。  
 政治問題の技術的解決策を探すことに対して私たちに警告するアメリカの政治史の1世紀以上があります。  
。  
しかし、執行は着実に弱まっています。  
Brexitへのロシアの関与は、主に金銭的な貢献とソーシャルメディアでのさらなるキャンペーンの形で行われました。  
 Open Rights Groupの2019年の会議で、私は広告禁止をテレビ広告からFacebook、Twitter、YouTubeのすべての広告に拡大する必要があると主張しました。  
政治家の仕事は、社会のさまざまな利害関係者間の紛争を調停することです。これらのグループが独自のフィルターバブルに陥る場合、政治家は代わりに紛争に火をつけたくなる可能性があります。  
 しかし、それは選挙コンテストをヨーロッパ人が親しんでいる文化的および経済的空間の中でより多く保つでしょう。  
有権者の登録、投票のキャスティング、投票の集計、結果の集計と監査などの個々の問題はすべて合理的に堅牢なソリューションを備えていますが、それらをまとめて堅牢なシステムにすることは簡単ではありません。  
まず、選挙日は不動であり、準備ができているかどうかに関係なく、ソフトウェアを展開する必要があります。  
第三に、選挙の間の長いギャップの中で、経験のあるスタッフが移動し、ノウハウが失われます。しかし、米国で使用されているほとんどの投票機は製造されなくなったので、アップデートはどこから来て、どのようにテストされますか？  
それでは、エンジニアリングから政治まで調べてみましょう。  
4私が書いているように、選挙は「顧客」の編集された部分の解放を強制する試みで敗北側であり、救済の望みがない場合-裁判所を介しても、投票箱を介しても、訴訟は継続します次回–民主主義のメカニズムへの信頼が失敗し始める可能性があります。  
逆に、法律を微調整し、投票機を購入し、地元の政治文化が許容する限り、大小を問わず、彼ら自身の側に多くの利点を生み出すのは、通常、現職者です。  
根底にある社会契約が侵食されると、超党派的環境により、在職者はあえて権力を譲ることをしないと感じる可能性があります。  
  
2020年に最も困難なセキュリティエンジニアリングの問題のいくつかは、ソフトウェアが私たちが使用するサービスと私たちの周りのデバイスに浸透するにつれて、これらのサービスとデバイスの設計が人間社会の根底にある複雑さに直面するという事実に関係しています。  
自動運転車は、空の砂漠の道路に対処できますが、実際の交通を人間のドライバーと見つけるのは非常に困難です。  
プライバシーを強化するツールと技術は、人間の複雑さによるセキュリティへの影響を調査する1つの方法ですが、物事を暗号化して匿名化するためにどのように努力しても、社会構造は何らかの方法で示される傾向があります。  
人の生活がますますオンラインに移行するにつれて、オンラインアプリケーションの重要性と複雑さが同時に高まっています。  
従来のソフトウェアエンジニアリングツールは、開発者が脱落する前に、システムの複雑さの山をさらに遠ざけるのに役立ちました。  
 そして、これはどのように政治と相互作用しますか？  
研究の問題研究の問題の1つの束は、人と自動化の間で責任を分割する方法に関連しています。  
これは飛行制御システムにとって当然のことであり、その選挙に対するミュラー報告を生命維持する。  
大規模なテクノロジー企業が毎秒数百万件のフィルタリングの決定を行っている場合、人間はどのようにして品質管理を行うことができますか？  
 その根底にあるのは、自動化（MLを含む）かどうかについての長い議論です  
MLを含む自動化が普及するにつれて、質問はより広くなる可能性があります。  
次に、メカニズムと社会の共進化に関する世界的な社会的および政治的問題が発生します。  
保護メカニズムのスケーリング方法になります...  
 数十億人のユーザーを抱える社会技術システムの中で。」私は、政府に愛されているマルチレベルのセキュリティなどのルールの単純なシステムは決して自然なものではなく、人々は常に仕事を成し遂げるためにそれらを破らなければなりませんでした。  
 今では、その経験が増えています。いくつかの大規模なテクノロジー企業は10億人を超えるアクティブユーザーがいるシステムを運用しており、数百の企業が1億を超える企業を抱えています。  
。  
これらはどちらもそれだけでは十分ではなく、技術と政治の相互作用によって、政府を選択するメカニズムが損なわれる可能性さえあります。  
この本の3番目のセクションでは、幅広いポリシーと管理に関する質問（監視とプライバシーなど）に取り組みます。  
参考資料カーセキュリティの概要については、まずチャーリーミラーとクリスヴァラセックがジープをハッキングした方法の説明[1316]をご覧ください。次に、技術的な詳細を知りたい場合は、クレイグスミスの「カーハッカー 'ハンドブック」をご覧ください。 1792]。  
機械学習のSVPであるGoogleのジェフディーンは、[528]でAIの公平性に関する同社の研究について説明しています。  
敵対的な国家関係者が直面する個人のプライバシーについては、ツールが両側で進化するにつれて、それは感動的な対立です。  
[458]には、Ben CollierによるTorプロジェクトの組織的および社会的ダイナミクスに関する興味深い説明があります。このプロジェクトは、主要なオンライン匿名サービスを維持しています。  
米国の投票システムの歴史は、ダグラスジョーンズとバーバラシモンズによって伝えられています[991]。  
ごく最近、連邦は、加盟国の非常に多様な経験に基づいて、選挙の電子的安全性に関するガイドを作成し、登録から投票のキャスティング、集計、結果の伝達までの全サイクルをカバーしました[329]。