実現の恐ろしい「ああ、たわごと」の瞬間がありましたが、それについて何をすべきかをリモートで解決していません。  
– WhitDi�e25。  
lightbluetouchpaper。  
 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アプリ、プライバシーを信頼するアプリ、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、自律的で遠隔操縦される車両です。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。  
2。  
 社会における人間の相互作用の豊かさのため、プライバシーは難しい。  
 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。  
2自動操縦および遠隔操縦の車両航空のパイオニアであるローレンススペリーは、1912年に最初の自動操縦を発明し、1914年にそれを実証し、パリでの「より安全な航空機」競争に裁判官をかわしました。  
 自分のデバイスに任された固定翼航空機は、最終的にはスパイラルダイビングに突入してクラッシュします。パイロットは地平線を基準にして水平に保つことができますが、クラウドで飛行しているとき、その外部参照はありません。  
1975年、私は最初の適切な仕事を得て、高速ジェット慣性航法セットを再設計して、石油産業で使用されている小艦艇を研究しました。  
 これらの機器のそれぞれの重量は約20kgで、コストは250,000ポンド（今日の金額では約300万ドル）です。  
現在、2020年には、3つすべてがスマートフォンに搭載されています。  
 また、衛星ナビゲーション用のGPSチップと、目的地までの徒歩、自転車、車での行き方を表示するGoogleまたはApple Mapsアプリもあります。  
 これにより、海、空、陸の支援技術が急速に進化しています。  
 自律的なプローブが南極の氷の下を泳いで、氷が溶ける速度を測定します。  
25。  
1ドローン空中で、ドイツのV1やV2などの初期の武器はツインジャイロオートパイロットロットを使用していましたが、冷戦は両方の湾岸戦争で使用されていたトマホークの巡航ミサイルを提供しました。  
 その後、1982年にイスラエルとシリアの戦争で初めて大規模に使用されたさまざまな無人航空機（UAV）が続きました。イスラエル空軍は偵察やおとりとしてそれらを使用し、最小限の損失でシリア空軍を一掃した。  
2。  
 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搭載するように設計されていました。  
 それは、より大きくより速い死神に取って代わられ、それは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。  
 関心は急速に失われました。数年以内に学生たちがドローンを作り始め、間もなくホビーショップで低価格のモデルを購入できるようになりました。  
 しかし、ドローンは薬物と携帯電話の両方を囚人に配達するために使用され、反乱軍は即席爆発装置を武器としてドローンに取り付けました。  
2。  
2004年、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、モハベ砂漠の149マイルを横断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。最速。  
 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年の彼らの次の挑戦は砂漠からシミュレートされた都市環境に移りました;競争相手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、前世紀のアンチロックブレーキシステム（ABS）から始まり、セクション23で説明したアダプティブクルーズコントロール（ACC）を通じて進歩する支援技術を着実に追加していました。  
1、自動緊急ブレーキ（AEB）および車線維持支援（LKA）。  
 DARPAの課題に触発されて、Googleはセバスチャンスランを雇って、完全自動運転車を作ることを目標にプロジェクトショーウリン2009を主導しました。  
Teslaは、2014年に最初に製品を手にしたとき、その「オートパイロット」ソフトウェアが、ストップウェイスタートトラックでフリーウェイを制御できる無線アップグレードとして発売されました。  
2。  
 TeslaのElon Muskは2018年までに完全自治を予測し、Googleの自動車プロジェクトがWaymoin 2016としてスピンアウトされる前の2017年までにGoogleのSergey Brinを予測していました。  
 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、雨が降っているとき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。  
 では、何が起こっているのでしょうか。答えの大部分は、他の道路利用者は予測不可能であるということです。  
 アダプティブクルーズコントロールは、ドライバーが疲労を軽減し、十分な車両がそれを使用すると渋滞を解消します。これは、交通による衝撃波の伝播を減衰させるためです。  
 エンジニアが自動緊急ブレーキに技術を拡張したとき、他のドライバーの意図を推測することができないことが制限要因になりました。  
 あなたがそこに着くまでにそれが道路を去ったとあなたが予想しているようにあなたはスピードを維持し、そうでなければあなたは追い越します。  
 2020年のAEBシステムの消費者テストでは、誤警報率と、歩行者のダミーが道路を横切ったときに間に合うように車を停止する機能の両方で、かなりの変動性がまだ示されています。  
 AEBは2022年頃にすべての新車に搭載されるはずです。  
4。  
しかし、新しい支援技術はそれぞれ最適化とデバッグに何年もかかり、それらの数十を自動操縦に組み合わせるのは簡単ではありません。  
 数十のプログラムが緩やかに相互作用し、人間がそのようなタスクを実行する方法の理解を反映します。潜在意識はあらゆる種類のものを見て、注意を危険にさらします。  
 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。  
サブシステムを組み合わせることは妥協を意味し、メインベンダーは設計の詳細を秘密にしていますが、事故による最適化と何が問題であるかについて学び始めています。  
2。  
AEBは車を止めたかもしれないが、「異常な車両挙動の可能性を減らすために」オフにされた-言い換えれば、誤った警報率は迷惑だった[457]。  
人間が緊急事態を引き継ぐには時間がかかることは数十年前から知られています。人間はアラームに反応し、コンソールのアラーム表示を分析し、環境をスキャンし、状況を把握し、光の流れに乗り、そして効果的な制御。  
 あなたは車の安全運転手がはるかに良いことを期待することはできません。  
2。  
 ドライバーアシスタンス–ソフトウェアがステアリングまたは速度を制御し、人間のドライバーが残りの作業を行います。2。  
 条件付き自動化–ソフトウェアは環境を監視し、ステアリングと速度の両方を制御しますが、混乱すると人間が引き継ぐことができると想定しています。4。  
 混乱した場合、道路の脇で止まる; 5。  
これまでのところ、マスマーケットで利用できる車両には高度な運転支援システム（ADAS）、つまりレベル1と2しかありません。保険業者は、「自律型」や「自動操縦」などの単語は、車両がレベルで動作していると思い込ませるので危険であると考えています4、事故につながる可能性があります。  
 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、その場で安全ドライバーと同じくらい迅速に危険を理解するために帯域幅を利用します。  
セキュリティエンジニアリング785ロスアンダーソン25。  
 セクション3で説明したように、安全に車を運転する（または航空機を着陸させる）ために重要な自律および遠隔操縦車両  
1。  
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、または単なる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。彼らはヒューマン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たなければならず、それは背後にあるヒューマンドライバーを困らせます。  
 自動運転車は、警察の警官からの停止信号を検出したり、ベッドを運んでいる8人の生徒やインドの寺院の行列に対処したりすることはできますか？2020年の時点で、レベル2システムには多くの欠点があります。  
（ノースカロライナ州のテスラの運転手1人が静止したパトカーの後ろにぶつかった後に起訴された[1118]。  
 多くの車は、ポットホールやその他の粗い表面は言うまでもなく、小さなラウンドアバウトの問題を抱えています。私が初めて乗り物に乗ったとき、私の歯は私たちが30mph近くでスピードバンプを乗り越えたガラガラでした。  
 マルチセンサーデータフュージョンの優れたアルゴリズムから、意思決定の説明を提供できる駆動アルゴリズムまで、自動車がルートを学習するように、人間と同じように、そのような技術トピックに関する膨大な量の研究があります。  
 これにより、テスラはさまざまな道路状況や気象条件にわたって数十億マイルのトレーニングデータを収集できるようになりました。  
4。  
 セクション14で説明したように、  
1、車で眠りに落ちることは事故の主な原因であり、英国全体の20％を占めています。  
 （それが、私たちが商用ドライバーの時間を制限する法律を持っている理由です。  
 なぜこれが起こっていないのでしょうか？私は、少なくとも3つの異なる要因を明らかにする必要があると思います：リスクセキュリティエンジニアリング786ロスアンダーソン25。  
 自律型および遠隔操縦型の車両サーモスタット、システムの基準、およびマーケティングによって生み出される期待。  
2。  
7義務的なシートベルト法は人々がより速く運転するようにしたので、全体的な効果は、全体の数を減らすのではなく、単に車両の乗員から歩行者や自転車に死傷者を移動することでした。  
2。  
 第三に、業界のマーケティングは、微妙な方法でリスクを最小限に抑えます。  
 飛行機の自動操縦の場合はそうではありませんが、ほとんどの非操縦士はそれを理解していません。  
2。  
3およびセクション4で説明したキー入力システムをリモート化します。  
1。  
 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​​力であったか150であったかは、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があります。  
 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、無線の制御を取得した攻撃者は、このアクセスをエスカレートしてドアロックやブレーキを操作できます[1085]。  
 これにより、クライスラーは1を思い出さざるを得なくなりました。  
 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。  
 すべてが文書化されていれば、私たち全員がより安全だと信じているオープンソースソフトウェア活動家や安全擁護者がいます[1792]。  
現在、車の盗難が主要な脅威モデルであり、セクション4でリモートキーエントリとアラームシステムを無効にするために使用される方法について説明しました。  
1。  
2。  
 電話、ナビゲーション、インフォテインメントセキュリティエンジニアリング787ロスアンダーソン25。  
 自律的で遠隔操作の車両システムは、多くの場合、とにかく設計が不十分です。車を借りたり、中古品を購入したりすると、以前のユーザーの個人情報が表示されることが多く、セクション22で説明します。  
3レンタカーを追跡およびロック解除できるアプリを使用して、車が誰かにレンタルされた後、これを続行できるようにする方法。  
 ChryslerJeep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subverteditである場合、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。そのような「荒れ狂う馬鹿」は、その名のとおり、バス全体を使用できなくします。  
 車が高速で走行している場合、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で詳しく説明します。  
4。  
 2017年、エロンマスクは聴衆に次のように語りました。。  
」。  
 数か月前、ハッカーはテスラの「母性」サーバー全体を制御するサーバーの制御を獲得していました。幸運にも彼は白い帽子で、ハックをテスラに報告しました[1119]。  
 高度なドライバーアシスタンスシステムがクラウドファシリティにますます依存するようになると、このような間接攻撃の範囲が拡大します。  
 自動車システムが歩行者やサイクリストのために自動的に減速し始める場合、それらのいくつかはこれを悪用する可能性があります。  
企業は、可能であれば支援システムを活用します。  
 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、それはセキュリティエンジニアリング788ロスアンダーソン25です。  
 AI / MLbeは憤慨し、おそらく妨害されました。  
 12歳の娘がタクシーを呼んで学校から家に帰る場合、現在、タクシーの運転手に犯罪歴のバックグラウンドチェックを要求する法律の形で保護措置があります。  
 では、保護はrobotaxisでどのように機能しますか？また、責任ゲームもあります。  
 コンピュータ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。  
4。  
完全に予測可能です。  
 私の研究室から家に帰る途中、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い車を停めました。  
 結局、大型トラックは時間内に曲がらなくなり、壁に落ちました。  
25。  
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」への巨大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。そのほとんどはルールベースのシステムに組み込まれ、Prologはコンピュータサイエンスカリキュラムの言語の1つとしてLispに参加しました。  
初期のメカニズムには、ロジスティック回帰、サポートベクターマシン（SVM）、ベイズ分類子が含まれていました。進歩は、自然言語処理（NLP）や検索などのアプリケーションによって推進されました。  
3。  
 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シグナルを操作し、エンジンが反撃し、隠されたテキストなどの裏技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2000年代に激しく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。  
2011年、ダンチレサン、ウエリマイヤー、ジョナサンマスシアン、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中国語の文字を認識し、交通標識の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とき、海の変化が始まりました[435 ]。  
200万枚の画像[1098]。  
 最も壮観な結果は、2016年にGoogle DeepmindのDavidSilverと同僚がAlphaGoを作成したときであり、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。  
25。  
1MLとセキュリティ機械学習とセキュリティの相互作用は1990年代半ばにまでさかのぼります。  
3。  
5。  
2。  
手作りのルールは、大規模なメールサービスプロバイダーには十分に拡張できませんでした。特に、ボットネットが出現し、スパムがメールの大半を占めるようになったため、スパムフィルタリングが大きなアプリケーションになりました。  
 スパムフィルタリングはユーザーフィードバックを真実と捉えているため、スパマーは大手Webメールファームで管理しているアカウントにスパムを送信し、スパムではないとマークする方法を学びました。これを検出するために、他の統計分析メカニズムが使用されています。  
もう1つは、バリューチェーンの弱点を探すことです。航空会社のチケット詐欺師は、無害なチケットを購入し、不正チェックに合格してから、出発の直前にリスクの高い目的地へのチケットに乗り換えます。  
3。  
バティスタビッジョとファビオロリは、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器を混乱させる可能性があることを発見し、そこから軍拡競争が行われました[241]。  
25。  
2 MLシステムへの攻撃機械学習システムへの攻撃には、少なくとも4種類あります。  
 モデルが使用中にそれ自体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、モデルの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り、数学的に盲点を避けられない[1706]。ニューラルネットワークでは、決定の境界が複雑になり、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、線形分類器よりも回避するのが実際には困難ではないことがわかりました[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子でも機能します[1901]。  
 多くの攻撃を1つのモデルで開発してから、同じデータまたは同様のデータ（ブラックボックス攻撃）でトレーニングされた別のモデルに対して実行できます。  
 たとえば、Ilia Shumailov、YirenZhao、Robert Mullinsと私は、ニューラルネットワークにキーを挿入して、盲点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]。  
3。  
機密性攻撃の変形は、機密のトレーニングデータを抽出することです。  
そのため、100万件の医療記録で訓練された分類者が「統計的機械学習」であるため個人データではないと一部の企業が主張する場合は、注意してください。  
3、積極的な研究の主題です[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、フィルタを回避するため、またはページの別の部分を誤ってブロックするために、敵対的なサンプルを使用して広告主に公開されたままになります[1899]。  
 まず、システムのセキュリティアプローチを採用して、問題をエンドツーエンドで検討する必要があります。  
次に、カード詐欺、スパム、侵入検知など、過去20年間の作業トピックの経験を利用する必要があります。  
4。  
2、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。  
 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。  
 新しい敵対的な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は、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するため、ビジョンシステム自体の重要性が低くなります。  
3。  
 言い換えれば、あなたは状況認識を組み込むことに着手しました。  
2。  
1、祖先の進化環境は、私たちが敵対的な意図や部族の違反などの引き金を感じるとき、特別な注意を払うように教えてくれました。  
根本的な問題は、機械学習にコードとデータの境界を曖昧にさせ始め、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しようとすることです。  
25。  
3MLと社会2016年以降の機械学習への関心の高まりと、人気のあるマスコミでの「人工知能」としての表現は、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でいくつかの例を説明しました）。  
6）。  
 ML、ビッグデータ、独占の間の相互作用は、政府が技術を規制する方法を熟考するときに政府がナビゲートする必要がある問題の秘訣を追加します。  
横断的な問題の1つは偏見です。  
 さらなる調査の結果、彼女と彼女の監督者であるジョアンナブライソンとアービンドナラヤナンは、使用されている本質的にすべての機械翻訳システムが単なる性差別的ではなく、人種差別的で同性愛嫌悪であることがわかりました[369]。  
 大きなプラットフォームのMLエンジンが、何百ものダウンストリーム企業が依存しているシステムを通じて偏見をなくすことができる場合、明らかに公共政策上の問題があります。  
保険会社が郵便番号レベルの請求統計を使用して保険料のレベルを決定したとき、多くのマイノリティの地域が高い保険料を免れたか、差別から保護され、差別禁止法に違反していた。ニューラルネットワーク技術を使用している場合、決定の根底にあるルールが何であるかを裁判所に説明する方法がないため、自分を守ることは困難な場合があります。  
”セキュリティエンジニアリング793ロス・アンダーソン25。  
 AI / MLAの2番目の分野横断的な問題はヘビ油であり、AI / MLのゴールドラッシュは何千ものスタートアップを導いており、その多くは製品よりもマーケティングに強いです。  
 ほとんどの人が差別していないと主張していますが、従業員のパフォーマンスに関する包括的でアクセス可能なデータを保持している雇用者はほとんどいないため、そのようなシステムをどのようにトレーニングすればよいのか、さらにはそのようなシステムを使用した企業が差別訴訟をどのように弁護するのかは完全に不明です[1571 ]。  
 賢明な雇用主はより透明なメカニズムを要求し、その結果を検証するための独立した指標を考案します。  
Arvind Narayananは、AIのヘビ油の興味深い分析を行っています[1382]。  
 それらのいくつかは、顔認識のためのDNNや実際にAlphaGoのように、実際に進歩しました。  
 さらに深く掘り下げて、Arvindは、機械学習システムは3つのカテゴリに分類できると主張します：1。  
3）、Shazamなどの製品による曲の認識（セクション24を参照）。  
3）、スキャンからの医療診断、および音声からテキストへの変換–熟練した人間の能力を獲得している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厳しい事例があります。  
 MLは、従業員の成績、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歩を遂げていません。  
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版がある場合は、さらに多くのデータが得られます。  
 直感的に、私たちは人々に退屈な仕事をするために判断と機械を含む仕事をしてほしいと思っています。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は多くの議論があります。  
3。  
 AI倫理のコンテキストで議論されている問題の多くは、数年前に、個人情報のデータベースで従来の統計的手法を使用して行われた研究で生じました。  
）それで、私たちの最初の呼び出しのポートは、既存の法律と政策であるべきです。  
4。  
図1を見ると、IT企業とその顧客が、医師、教師、その他の人々が紙ベースの記録で長年にわたって扱ってきた知識を無視したために、問題の多くが発生することがわかりました。  
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。  
4。  
 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。  
 （セクション14。  
）MLテクニックを使用して、容疑者が飛行リスクまたは再攻撃リスクをもたらすかどうかについて審判で裁判官に助言するために、また容疑者が危険かどうかについての判決ヒアリングで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、検閲などの問題で長年にわたって浮上している平衡の一部を混乱させる可能性があります。これにより、MLは、すでに強力な俳優が利用できるさらに強力なツールを提供し、古い虐待を復活させる新しい言い訳を作成します。  
3、多くの都市（サンフランシスコを含む）が「はい」と答えました。  
2。  
 MLテクニックは、コミュニケーションのパターンを見つけることにより、トラフィック分析をより簡単にします[1719]。実際、警察と諜報機関は、セクション21で説明したソートのトラフィックとソーシャルネットワーク分析にますます依存しています。  
3。  
2。  
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、私たちが現在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？セキュリティエンジニアリング795ロスアンダーソン25。  
 ペットと運用上のセキュリティ25。  
 セクション11。  
5私たちは、4つのFacebookが少ないため、注意深い観察者がほとんどの場合同性愛者であるかどうかを調べることができること、およびこの観察結果がとりわけ、有権者の好みが文書化され、詳細に。4。  
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。  
 学術的権威の濫用は、教授および匿名の会議論文提出の匿名の学生フィードバックによって対抗されます。  
 プライバシーはまた、言論の自由の必要な先駆けとなり得る。  
 そして、当時の政府のためにクマの罠を掘り起こしている野党政治家がいます。彼らの懸念はより戦術的です。  
 内部告発者を保護する法律も制定しています。  
 ボブが国王を批判したとアリスが主張した場合、ボブは常に逆を主張することができました。議会の権限を高めるためのデモを提案したのはアリスであり、忠誠を拒否したのは彼です。  
 もっともらしい否認可能性は、日常生活から知性と外交の最上位まで、今日のいくつかのコミュニケーションの重要な特徴です。  
 しかし、ほとんどの状況にはそのような明確で便利なルールがなく、コミュニケーションの電子的性質は、「1分間外に出るだけ」は選択肢ではないことを意味します。  
 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、ほんとうに革命でした。  
 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持っています。  
セキュリティエンジニアリング796ロスアンダーソン25。  
 ペットと運用上のセキュリティ1。  
 その国は彼らの宗教を変えるイスラム教徒の市民を処刑します。  
 彼は本当の改宗者を別として警官に話すことはできません。  
 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。  
 チャールズは精神分析医であり、私的患者が衰弱、不安、その他の問題に苦しんでいるのを見ています。  
 ロックダウン以来、彼はSkypeやズームなどのツールを使用する必要がありました。  
 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。  
 彼女はどのように同僚とコミュニケーションをとるべきですか？  
 彼女は、テイクオーバーターゲットに興味を持たせずに調査する方法を望んでいます。あるいは、誰もが興味を持っていることを知りさえします。  
6。  
彼はポルノをダウンロードして、絞首刑にされることなく他のゲイの男性に連絡する何らかの方法を望んでいます。  
 グラツィアーノはパレルモの治安判事で、マフィアの活動について人々に当局に連絡するためのホットラインを設置しています。  
 腐敗した警官ができるダメージをどのように制限しますか？8。  
 ほとんどのクライアントは、中東や北アフリカで戦争や悪い政府に反対しています。  
 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。  
 アイリーンは、告発者に彼女に連絡するように誘う戦闘新聞の調査ジャーナリストです。  
 政府が明らかにするために一生懸命努力しようとする主要な情報源から連絡を受けた場合、彼女はどのような準備をすべきですか？  
 アイリーンはご家族のごみを喜んで掘り出しました。彼のメールを読んだり、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、北朝鮮に選挙運動用の箱を配線したりしたい人は他にもたくさんいます。  
4。  
 Andrewが改宗者にWickrをダウンロードして使用するように指示すると、改宗者になりすまして警察のスパイは国のファイアウォールを利用して、それを使用する人物を検出します。  
 数十人だけがウィッカーを使用している場合、警察はドアをすべて壊すことができます。  
そして、技術的な対策はアンドリューの問題の一部を解決するかもしれませんが、ベラの場合にはあまり役に立ちません。  
 もう1つは、子どもの安全についての政治的およびメディア的訓練が彼らの福祉の邪魔になることです。  
 ベラが成長するにつれて、他の仲間のグループが使用するツールに精通する必要があります。そしてすぐに、彼女はあなたよりも彼らからのセキュリティ手順を採用します。  
攻撃の強度は大きく異なります。  
 ダイに関しては、彼女は頻繁に監視下に置かれます。  
根本的に異なるインセンティブがあります。  
 Andrew、Dai、Graziano、Hristoはすべて、不正なインサイダーについて考える必要があります。  
成功と失敗には異なるしきい値があります。  
 失敗にはさまざまなコストがあります。エリザベスが失敗すると、ジャスティンがキャリアを失い、フィロズが人生を失う可能性があるため、いくらかお金を失う可能性があります。2。  
しかし、これらのバーナーは、呼ばれることもありますが、適切に使用するのは困難です。アルカイダでさえ、それを正しく行うことができませんでした。  
4。  
2。  
10、調査官はしばしばトラフィック分析から情報の多くを取得します。  
4。  
 昔は、メールの暗号化は危険でした。あなたが国内でPGPを使用しているわずか20人の1人だったとしたら、それはあなたを疑いました。  
Hristoのような政府の監視下にある人々は、たとえ他の多くの人々が無害な目的でそれらを使用したとしても、WhatsAppやSignalのような通常のプライバシーアプリだけでは十分ではないことを学びました。  
 しかし、王立海軍のカッターがケヴァンを逮捕し、彼が彼の電話でフリストのメッセージを見つけた場合、彼は引き渡しに直面します。  
 ネットワークの追跡を困難にするだけでなく、人々が捕まったときにどのような証拠が押収されるかについての問題があります。  
したがって、暗号化されたメッセージングを提供するだけでなく、運用セキュリティ（Opsec）もサポートしようとする「暗号電話」の市場の発展を見てきました。  
3。  
一般に発売された最初の暗号化電話は、2014年におそらく政府機関、特殊部隊、人権労働者に販売されたSilent CircleのBlackphoneでした。  
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、国の最大の違法ウェブサイトのホスティング会社でした[364]。  
 暗号電話会社は、一部の人々は、ハンドセットに対して1000ドル以上のユーロを支払う準備ができていることを発見しました。また、関連するサービスへの6か月のサブスクリプションについても同様です。  
 ネットワークは秘密のコミュニティにも適用されます。 Hristo、Kevan、および他のギャングはすべて同じシステムを使用する必要があります。  
新たなパターンとして、ネットワークの影響により、十分な数のユーザーが警察の標的になり、当局がそれをバストするまで、1つの暗号電話システムがますます広く使用されるようになっています。  
 一部の移民コミュニティは、Hristoの活動を家族再統合サービスと見なしていますが、保守的なメディアのスティグマティス難民と大臣は、組織化された買収犯罪よりも移民の活動を優先順位を高くしています。  
4。  
 その年の4月、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、IronChat [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提供したことで有罪を認め、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：「私たちは金持ちです。  
。  
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、それがそうです」[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づき、顧客に電話を一度に取り除くようにアドバイスしました[1922]。  
したがって、Grazianoのような警官は、クリプトフォン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年代に発表されたとき、北アイルランドでのイギリスの統治に対する反乱でProvisionalIRAによって採用されました。  
 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。  
4。  
 政府の最新の愚行に豆をこぼしたい先輩の公務員が彼女に近づくと、物語が現れるとすぐに「モグラ狩り」が始まります。  
アイリーンはどのようにしてリズが特定、発砲、および起訴される可能性を最小限に抑えるのを助けることができますか？セクション2で内部告発について簡単に説明しました。  
ここで、技術的なセキュリティは通常、内部告発者が直面する問題の1つにすぎず、多くの場合最も深刻ではないことがわかりました。  
 IrenewillはLizをソースとして評価する必要があります。  
4。  
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、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がベストプラクティスです。  
 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、10人全員が既知のすべてのデバイスをティータイムによって危険にさらす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を提供するために急いで行き、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と呼ばれる機能を公開しました。まず、そのようなメカニズムは使いにくいです。  
2。  
 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、一般的な新聞は、たとえばこの章のようにそれらを議論していません。  
 （暗号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。リズがそれに夢中になったら、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、それらの開示は州の秘密ではなく、詐欺と虐待に関するものです。  
2。  
 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、非難されたりするなど、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勇気を出して発言した数十人が前に出てきたのはそれが初めてでした。  
 精神分析医のチャールズは、私たちがメアリーと呼ぶかもしれない彼の患者に提供することができるプライバシーが治療の仕事に不可欠であることを知っています。  
 メアリーメイトは、彼女の雇用主が彼女がセラピーを受けていることを発見した場合、同僚から非難されるか、昇進のために引き渡されるのではないかと恐れているかもしれません。  
4。  
 彼らは、2016年の選挙でのロシアの干渉を記したNSAの文書を漏らし、63か月の刑務所に通ったNSA内部告発者であるReality Winnerを追跡するために使用されました[174]。  
4。  
 したがって、治療環境は彼女を落ち着かせ、自信を刺激しなければなりません。  
 プライバシーに関するアドバイスがある場合は、残りのサポートと一緒に点滴する必要があるかもしれません。  
 賢明な保護者は、子どもの安全を脅かすことを見逃さないでしょう。子供が見知らぬ人に拉致され殺される率は、年間1,000万人に1人の割合であり、合理的な人々がそれを無視するほど低い率です。  
活動家のダイも、彼女が募集しようとしている人々へのサポートの提供者です。  
 私は彼女が当局に知られ、断続的な監視下にあると思います。  
 Thepoliceは密かに家に入り、パスワードを盗むルートキットを埋め込み、会話を聞くためにバグを部屋に埋め込みます。  
 マイクが隠されていない場合もあります。家の外に公然と立っている警察の活動家から、窓にショットガンマイクを向けていると聞いたことがあります。  
 これの一部は、スパイ映画に似ています。秘密のエントリを検出するためにテルテールを残し、常にラップトップを手元に置いておき、バグの発生しにくい場所で機密の会話を行います。  
また、採用担当者を作るには、断続的な観察下で、疑わしい人物ではない人々と密かに連絡を取る必要もあります。  
トレードクラフトで何が機能し何が機能しないのかを知りたい場合、人権擁護労働者は話し合う人々です。  
）出現しつつある状況は、警察と非暴力の政府反対派の両方の行動が社会の運営方法に組み込まれており、時間とともに進化するというものです。  
 不人気な統治者にとってあまりにも素晴らしくなり始める動きは、信頼性を失い、他の人々に追い出されます。  
 セキュリティエンジニアリング802ロスアンダーソン25。  
 ペットと運用上のセキュリティ非暴力の反対は、オープンな反乱や暴力テロを引き起こす可能性があります（そして、「テロリズム」として非暴力の反対を非難する支配者は、まさにそれを招くかもしれません）。  
 後で熱くなる場合に備えて、彼は一部の機能の使用を控えているため、対策を講じていない予備の準備ができています。  
4。  
 これを土地と呼ぶかもしれません3。  
 どの国の選り抜きにもたむろする場所があるので、上級公務員が著名なジャーナリストに会いたい場合は、誰も何も気付か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にオープンなプラットフォームがあります。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った場合、人々は彼女のメンタルヘルスにすぐに十分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。3番目の要素は、サポートを含む能力とモチベーションです。  
 彼女の仕事は違法であり、彼女にはサポートのためのITチームがあります。  
 このコンテキストでも適切であるようです。  
4。  
 グラツィアーノはより高いリスクに直面していますが、経験豊富な警察組織を背負っています。  
 選挙運動は、規律を守るのが難しく、セキュリティよりも勝利に重点を置いている数十人のボランティアによる募金活動の流れに沿っています。  
 Dai、Firoz、Hristo、およびNurは、有能な技術サポートなしで極端な危険に直面しています。  
 これについては、後でセクション26で詳しく説明します。  
 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。  
 また、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アドホックな方法は多数あります。彼は何らかの修復可能な方法でメモリスティックを損傷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。  
日常的な交通分析を打ち負かすには、受付係として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。  
4。  
 宣教師のアンドリューは、最も安全な通信タスクの1つを持っています。  
 おそらく彼にとって最も簡単な解決策は、SkypeまたはWhatsAppを使用することです。  
 あなたの娘ベラの場合、目標は彼女が有能な大人に成長するのを助けることです。  
 私がしていることは、詐欺、フィッシング、その他の虐待について時々夕食のテーブルで話し合うことです。  
 それはすべて、私たちがプレイするボードゲームと同じ精神です。  
 精神分析医であるチャールズは、リスクと可能な緩和策について基本的な認識を持っている必要があります。  
しかし、彼が治療環境への彼女の信頼を損なうことによって、これが彼が取り組んでいる臨床的方法に反する場合、彼は提案をすることにも消極的かもしれません。  
セキュリティエンジニアリング804ロスアンダーソン25。  
 ペットと運用上のセキュリティ実際には、両方の当事者が関連する知識を欠いている可能性があり、メアリーがチャールズよりもリスクについてより多くを知っていたとしても、彼女は提案を聞くことができないと感じるかもしれません。  
 人権活動家のダイは、すべての最も困難な仕事の1つを持っていますが、彼女は時々秘密の警察に振り落とされ、彼女が経験を共有できる他の活動家と協力して、彼女は時間の経過とともに優れた技術を進化させることができます。  
 M＆Aアナリストのエリザベスは、Torが必要なことをかなりうまく行っていることを知っているかもしれません。  
6。  
 それが不可能な場合は、Torを使用するだけでなく、MacまたはLinuxのボックスを入手して、ポルノサイトのマルウェアにさらされる機会を少なくする必要があります。  
 （おそらく、警察が彼を最初から襲撃しないように、彼は革命警備隊に加わるべきでしょう。  
 グラツィアーノも大変な仕事をしています。  
 セクション10で説明したように、彼の解決策の一部は、区画化された警察の記録保持システムである可能性があります。  
彼はまた、彼らが使うどんなメカニズムを使って情報提供者とチャットするかもしれません。  
 Hristoは暗号化電話を使用することの利点を理解しているかもしれませんが、それがcopscrackすると彼のネットワーク全体を巻き込む可能性があります。  
 だから私はそれに焦点を当て、同僚に交通安全について教育します。  
9。  
 ジャーナリストは、記事を書くだけでなく、人を読み、真実を評価し、リスクを判断するスキルも必要です。  
 今日のジャーナリストが検索エンジンを駆使する方法を知る必要があるように、探偵は彼女の情報源を保護する方法を知る必要があります。  
 つまり、人だけでなく脅威やツールについても理解する必要があります。  
）10。  
 規律を付けるのが難しく、修正不可能な悪質なテクノロジーの習慣を持っている可能性のある熱心なボランティアが立ち並んでいる、短期間で高結果のエフォートを保護することは困難です。  
セキュリティエンジニアリング805ロスアンダーソン25。  
 ペットと運用上のセキュリティリチャード・クレイトンは、サイバースペースにおける匿名性とトレーサビリティに関する論文を書き、ネットワークの匿名性がどのように複雑になったかを分析しました[442]。  
複数の学生が住んでいる家の電話回線やプリペイド式の携帯電話から乱用されたトラフィックが送信された場合、責任を確立することは困難です。  
 しかし、匿名を目指す人が失敗する方法もたくさんあります。最終的に人々は、opsecにどれだけの労力を費やしても、間違いを犯します。  
これは政府のセキュリティおよび諜報機関にも当てはまります。  
4。  
 James BondWeは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トレードクラフトがほつれ始めていた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、エージェントのホテルの滞在や国境検問所と関連付けました。  
英国とオーストラリアはパスポートの出所を求めてイスラエルの外交官を追放した[307]。  
2番目の警告は2013年に来ました。レポートでは、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、CIAにピン留めして、不在のイタリアの警察によって多くのエージェントが起訴されました[1274] 。  
2。  
 個人情報の武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する企業に要求することが可能になり、政府機関は信用記録、医療記録などにアクセスできるようになりました。  
 国防総省は国防総省に消費者向けDNA検査キットを使用しないように指示し、中国はデッドドロップのようなより低技術者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で顔認識について説明しました。  
5。  
 しかし、これは全体的にどれほどうまくいくでしょうか？この章で前述したように、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、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。  
4。  
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、政治的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。  
5選挙私が2020年に書いているように、人々は次のUの行動と信頼性を心配しています。  
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経験も豊富です。すべての加盟国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。  
ギリシャ人とローマ人は、議会、評議会、裁判所に座る代表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の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見られ、18世紀のアメリカ革命につながりました。この地域では、創設者の父親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。候補者の後ろにはロマネクターが並んでおり、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。  
5。  
 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。産業革命で勢力を拡大したイギリスの都市にはMPがありましたが、他の選挙区には投票者が少なく、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、旧南軍は、黒人市民の投票を阻止するために、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試して、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。  
5。  
 多くの都市や州には、投票を勝ち取った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。  
 これに戻って、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式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。  
 ルイジアナでは、ロング兄弟がアザラシを倒し、カウントを望ましい結果に設定し、数年間州を運営しました。  
 機械式投票機には約100ビットのプログラミング機能があり、通常はコッターピンやその他の機械式リンケージの形で、誰も理解していませんでした。25。  
2吊りチャド発明者たちは、ピアノのピアノに触発されて、ペーパーロールに穴をあける競合型の機械を考案しました。パンチされたカードがタブを作成するマシンやコンピュータによって普及した後、それらは広く使用されるようになりました。  
 また、投票箱にドロップされると匿名になります（指紋を心配しない限り）。  
 ハンギングセキュリティエンジニアリング808ロスアンダーソン25でした。  
 ELECTIONSchad ’、まだカードに添付されている、有効な投票？パンチが貫通していないディンプルはどうですか？投票カウントマシンは100,000票を超えて拒否しましたが、ジョージブッシュのアルゴアに対する過半数は537票でした。  
 これはそのような論争を引き起こし、2002年に議会は3ドルを割り当てたヘルプアメリカ投票法（HAVA）を可決しました。  
企業がこの巨大な新しい市場に機械を構築して販売しようとスクランブルを掛けたとき、ゴールドラッシュが続いた。  
 実際、Floridarecountが進行中だったので、私はNewOrleansでのアプリケーションセキュリティ会議に出席しました。その参加者には多くのNSAおよび防衛請負業者が含まれ、私たちは議論を組織しました。  
 大多数が、昔ながらのショーで、電子選挙を信用しなかったと投票しました。  
新製品の中には、19世紀のレバーマシンの子孫であるダイレクトレコーディングエレクトロニック（DRE）マシンがあり、これは通常、候補者や他の投票オプションを画面に表示し、投票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は不明です（たとえば、不感なタッチスクリーンの分類方法によって異なります）。  
2002年の選挙では多くの問題が報告された[806]。次の夏、主要な投票機サプライヤーであるDieboldは、ソースコードをオープンウェブサイトに残しました。  
 ほぼ間もなく、ブッシュ大統領再選キャンペーンに積極的に参加したディーボルトCEOのWalden O’Dellは、「私はオハイオ州が選挙投票を来年の大統領に届けるのを支援することを約束します」[1987]と書いています。  
 （投票研究者のRebecca Mercuriは、1992年にDRE機器は投票者の選択をウィンドウの後ろにある紙のロールに表示し、キャストする前にそれを検証するようにすべきだと主張していました[1295]。  
 他のDREmachineには監査証跡がまったくありませんでした。審査員ができることは、同じ結果をもう一度印刷するよう依頼することだけでした。  
5。  
 光セキュリティ工学809ロス・アンダーソン25。  
 ELECTIONSscanシステムは1980年代から使用されており、学校で多肢選択式テストの採点に使用されるマークセンススキャナーから発展しました。  
報告書は憂鬱な読書をした[306]。  
以前に承認されたすべての投票機（Diebold、Hart、およびSequoia）は、認証を取り下げ、ES＆Swaから提出された遅延システムも認証を解除しました。  
フロリダ州の機器の同様の検査がフロリダ州立大学の科学者によって行われ、2007年7月にディーボルト機器の一連の新しい脆弱性が報告されました[749]。  
評価されたすべての機器に重大なセキュリティ障害がありました。暗号化されているはずのデータは暗号化されていませんでした。暗号化が正しく行われていません（たとえば、暗号文の隣にクリアテキストで格納されているキー）;バイヤーオーバーフロー;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。および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。  
 しかし、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、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、テキストが「ゴア」でバーコードが「ブッシュ」である投票カードを印刷する可能性があります。  
 英国では、依然としてゴールドスタンダードは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、障害者の権利運動家に機器の販売を依頼しています。  
 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用紙の使用を段階的に拡大しました。これは、投票の購入と脅迫を容易にするため、野党によって批判されました。  
 投稿から電子メールおよびテキストへの投票を拡大する計画は、この既存の低品位の悪用を容易にし、潜在的に自動化に開放するために批判されました。  
 私のポスドクのうちの2人は、ベッドフォード選挙で検閲官として行動し、さまざまな米国の選挙で報告されたのと同じ種類の修羅場を観察しました。5。  
 （印刷業者は印刷の途中でインクを交換したため、投票用紙の半分は「黒の間違った色合い」でした。  
 結局、誰もが家に帰れるように、帰国者は結果として投票が誤って数えられることはないと言った保証書（ベンダーがその場で書いたもの）を受け入れました。  
ボランティアを組織したオープンライツグループは、観察された領域の結果に信頼を表明できなかったと報告した[1472]。  
 （英国の選挙は、有権者の登録から選挙後の虐待、選挙資金の上限違反まで、キルチェーンの他の場所で乱用されています。そのため、コンピューターを修正するだけでは問題を解決できません。  
5。  
 投票カウントソフトウェアにはバグがあり、悪意のあるものであると想定する必要があるため、それに依存する必要はなく、手動で再カウントする可能性は重要な緩和策です。  
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詐欺やエラーが発生する可能性を厳しく制限できるリスク限定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、投票の集計をより検証可能にすることを試みました。  
 セクション5。  
7メカニズムについて説明しました。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、今ではこれについてよく理解されたメカニズムがあります。  
5。  
 すべての投票用紙が整形式であり、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で説明した電子署名デバイスと同様。  
1、信頼できるユーザーインターフェイスがないので、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、再集計結果、および結果の発表に対する攻撃について心配する必要があります。  
 次に、電話マルウェア、および設計と実装の品質についても心配する必要があります。  
25。  
5なぜ電子選挙が難しいのかオランダでは別の興味深い脅威が浮上しました。  
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観察者は、党の有権者が選択したものを見ることができます[785]。  
3。  
 活動家たちは彼らが望んだ政治的結果を得た：アムステルダムの地方裁判所はすべてのNedapマシンを認証解除した。  
発展途上国の一部の選挙では、州が野党のウェブサイトを体系的に検閲し、サービス拒否攻撃を実行しています。他の国では（通常、最も後ろ向き）、選挙は、野党候補者を投票用紙に入れる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のより伝統的な方法によって不正が行われます。  
 私がこれを書いているときのニュースは、「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消した[611]。  
近年、人口登録を巡って多くの問題が発生している-セキュリティエンジニアリング812ロスアンダーソン25。  
 選挙;セクション7で。  
2。  
 登録メカニズムがかなり堅牢な場合でも、セクション17で言及されているAadhaar生体認証システムを備えたインドのように。  
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りました。  
 たとえば、ジョージア州は2020年に書いているように完全に混乱しているように見えます。何年にもわたって投票を困難にし、ディーボルトのマシン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。ただし、注目の主な焦点は、ソーシャルメディア選挙の使用にシフトしています。  
 セクション8で説明したように。  
 結果は過激主義の偏りです：炎症性の広告はより安いです。  
2。  
 ロシアのエージェントはトランプのためにキャンペーンを行っただけでなく、とりわけ黒投票を抑制することを目的としたトロールファームやソーシャルメディア広告キャンペーンを実行しました。彼らはクリントンのGmailキャンペーンチェアジョンポデスタをハッキングしました。  
 クリントンが勝利したならば、もしそれらの国のどちらかが彼女に投票したならば、「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かもしれない。  
TwitterとFacebookの両方が、トランプと彼の仲間によるCovid [1030]に関する虚偽の情報を含む投稿を削除しました。彼または他の人がオンラインメディアを使用して選挙プロセスを弱体化させたり、セキュリティエンジニアリング813Ross Anderson25を信用したりする懸念があります。  
 結果の選挙。  
 Zuckerbergは有権者抑制の試みを阻止すると述べているが、彼は右翼をより簡単に乗せるようにしていることをFacebook内で心配しています[1740]。  
しかし、その後の結果についての論争についてはどうでしょうか？政治問題に対する技術的な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。  
 締約国は、より多くのキャンペーンと候補者に対してのみ支出できます。そしてほとんどのヨーロッパ諸国はキャンペーン中に有料のテレビ広告を禁止しています。  
 たとえば、ブレグジットの国民投票中に、両方の休暇キャンペーンが支出制限を超えましたが、£20,000の上限を支払っただけです。  
 そのような悪用を阻止するために何ができるでしょうか？オープンライツグループの2019年の会議で、私はテレビ広告からFacebook、Twitter、YouTubeのすべての広告に広告禁止を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対立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った場合、政治家は代わりに対立に火をつけようとすることができます。  
選挙は依然としてセキュリティエンジニアリングの難しい問題の1つです。  
 選挙人を登録し、投票を記録し、それらを集計するためのコンピュータシステムには、堅牢な設計、実装、テスト、および展開の病理学的事例となる多くの特性があります。  
 次に、地域や国によって要件が異なり、時間とともに変化します。  
 第4に、オペレーティングシステムやその他のソフトウェアは、既知の脆弱性を修正するために更新する必要があり、更新は予期しない方法でセキュリティを破壊する可能性もあります。 Windowsのアップデートにより、EV2000投票機が最後の有権者の選択を強調し、次の有権者に投票しました[991]。  
それでは、エンジニアリングから政治まで見ていきましょう。  
私が書いているように、セキュリティエンジニアリング814ロスアンダーソン25の編集された部分を強制的に解放しようとする訴訟が続いています。  
 要約選挙の「顧客」は負けた側であり、裁判所を通じて、または次回の投票箱を通じて、救済の希望がなければ、民主主義のメカニズムへの信頼は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、大小さまざまな自分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行使しないと感じる可能性があります。  
25。  
4つの例を見てみました。  
 機械学習のメカニズムは、より不利になるだけです。彼らはパターンマッチングには優れているかもしれませんが、理解に欠けているため、スタックのすべてのレベルで悪用の新たな可能性が開かれます。特に、本質的に不適切な社会予測タスクに人々が急いで悪用する可能性があります。  
 そして最後に、選挙があります。現職の支配者が、法の範囲内であれ、範囲外であれ、逃げることができると思うすべてのことを実行する準備ができているとき、テクノロジーと法律の両方の限界について多くを学ぶことができます。  
 なじみのある問題の多くは、これまで扱いにくい形で何度も何度も戻ってきます。  
 実社会の複雑さに対処するには、どのようなツール、手法、ガバナンスプロセスが適切ですか？そして、これはどのように政治と相互作用しますか？これらは、この本の第3部で取り組む予定のトピックです。HCIの第一人者であるベンシュナイダーマンは、人間の制御と広範な自動化が、システムの信頼性、安全性、信頼性を高めるためのスイートスポットであると主張しています[1723]。  
セキュリティエンジニアリング815ロスアンダーソン25。  
 機械の概要ですが、推奨システムやヘイトスピーチ検出などにスケールアップすることは簡単ではありません。  
MLを含む自動化が普及するにつれて、質問はより広範囲に及ぶ可能性があります。  
 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疑問が生じます。  
。  
 保護メカニズムがどのように拡張されるかを示します。  
。  
「政府に愛されているマルチレベルのセキュリティなど、単純なルール体系は決して自然なものではなく、人々は常に仕事を終わらせるためにそれらを破らなければなりませんでした。  
そのようなシステムでは、テクノロジーと動作は互いに適応しますが、システム開発者ははるかに強力であり、異なるインセンティブを持っています（ユーザーはプライバシーを求めているのにデータを求めています）。  
 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、ポリシーと管理に関する幅広い質問（監視とプライバシーなど）、大規模で複雑なシステムの進化をどのように管理および管理できるか、および安全などの社会的目標を達成するためにテクノロジーをどのように規制できるかについて説明しますとプライバシー。  
Nicolas Papernotの「Marauder's Map」は、敵対的な機械学習の急速に進んでいる分野[1493]への現時点での最良の導入かもしれませんが、GaryMcGrawと同僚は、設計原理と、システムのセキュリティに取り組む際に考えるべき事柄のリストを提供しています機械学習コンポーネント[1267]。  
 AIとIAの論争に関する私自身の哲学的立場は、[87]にあります。  
出発点の1つは、EFF Webサイトの[Surveillance Self-Defence]ページ[618]かもしれません。  
6。  
 技術的な詳細については、セクション20を参照してください。  
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、独自の加盟国の非常に多様な経験に基づいて、選挙の電子安全保障へのガイドを作成し、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]。