（また、それらは大きく、維持に費用がかかり、管理が困難であり、環境を汚染します。  
 しかし、それらは十分に普及しており、その制限に基づいてプロトコルを設計する必要があります。  
– BRUCE SCHNEIERMetternichは常に嘘をつき、だれもだましませんでした。Talleyrandはうそをつくこともなく、全世界をだましました。  
1はじめに多くの実際の攻撃は、少なくともテクノロジーと同じくらい心理学を悪用します。  
フィッシングなどのオンライン詐欺は、多くのオンライン保護メカニズムが使いやすくなく、同等の現実世界の詐欺と同じように偽造することが難しいため、類似の現実世界の詐欺よりも実行が簡単で、阻止するのが困難です。  
私たちは何百万年にも渡って社会的および心理的なツールを進化させ、対面での欺瞞に対処する手助けをしましたが、何かをするように依頼するメールを受け取ったとき、これらはあまり効果がありません。  
2。  
 実社会には多くの例があります。ポテトの皮をむくにはナイフよりもアポテトの皮むき器の方が簡単ですが、殺人にははるかに使いづらいです。  
私たちが日常業務で信頼している善悪の非対称性の多くは、簡単に自動化できる正式なやり取りだけに依存するのではなく、物理的なオブジェクト、人の判断、およびサポートする社会的プロトコルのいくつかの組み合わせに依存しています。  
さまざまな種類の詐欺が、オンラインのセキュリティを無効にするために使用される主要なメカニズムになりました。  
 デマと詐欺は常に発生しましたが、インターネットはそれらのいくつかを容易にし、他の人が私たちの既存の制御をバイパスする可能性のある方法で再パッケージ化できるようにします（個人の直感、会社の手順、さらには法律でさえ）。  
 設計者がより簡単な技術的攻撃を未然に防ぐ方法を学ぶにつれて、システムユーザーまたはオペレーターの心理的操作がますます魅力的になります。  
 したがって、セキュリティ経済学の研究がこの本の第1版と第2版の間の見方に大きな変化をもたらしたのと同様に、セキュリティ心理学の研究は、第2版とこの版の間の世界の見方に大きな違いをもたらしました。  
3。  
 コンピュータサイエンスよりもずっと長い間研究されてきましたが、私たちの心の理解は完全ではなく、脳は非常に複雑です。  
 私たちは「心は脳がすること」であることを知っていますが、私たちの自己と個人の歴史の感覚の根底にあるメカニズムは不明瞭なままです。  
 whatSecurity Engineering76Ross Andersonで3。  
 心理学研究からの洞察私は私たちの貿易に非常に関連する心理学研究の3つのテーマのヘリコプターツアーを提供することができます：認知心理学、私たちがどのように覚えているか、どのような間違いをするかなどのトピックを研究します。社会心理学は、グループ内の他の人々と権威にどのように関係しているかを扱います。行動経済学は、測定可能で搾取可能な方法で一貫して不合理な決定をするように導くヒューリスティックとバイアスを研究します。  
2。  
 それは、私たちがどのように考え、記憶し、決定を下し、さらには空想するかを扱います。  
 多くの有名な結果があります。  
 これらの洞察の多くはマーケティング担当者や詐欺師が使用していますが、ほとんどのシステム開発者は誤解している、または単に無視しています。  
しかし、これは正しい結論ではありません。  
メニューサイズの実際の制限は、10の選択肢を提供する可能性のある画面サイズと、平均的なユーザーが3つまたは4つ以上を扱うことが困難な率直なメニューです[1544]。  
 これは、7 +/- 2のようなBroadideaが危険である理由を示しています。詳細を確認する必要があります。  
その結果、HCIの研究者は、知覚、運動制御、記憶、問題解決など、人間のパフォーマンスをモデル化して測定するだけではありません。また、ユーザーのシステムのメンタルモデルの仕組み、開発者のメンタルモデルとの違い、および人々がどのように使用および理解するかを調査するために使用できる手法（タスク分析や認知ウォークスルーなど）についても理解を深めました。システム。  
 低ハンギングフルーツがあります。たとえば、安全研究コミュニティは、機器を操作するときに人々が犯すエラーを研究することに多くの努力を注いでいます[1589]。  
 人、音、コンセプトを認識するためのスキーマ、オーメンタルモデルsoSecurity Engineering77Ross Anderson3。心理学研究からの洞察コンピュータよりもはるかに優れており、間違ったモデルがアクティブになったときに脆弱になります。  
•実行されるアクションはスキルの問題になることがよくありますが、手動のスキルが失敗した場合（たとえば、間違ったボタンを押すなど）はスリップする可能性があり、間違ったスキルを使用することもできます。  
 スリップは、人気のあるドメインと同様のドメインを登録し、タイプミスを犯した人々を収穫するタイプミスキャターによって悪用されます。他の攻撃は、人々が「OK」をクリックしてポップアップボックスを表示し、作業を完了するように訓練されているという事実を悪用します。  
 また、エラーは通常、中断や知覚の混乱の後に発生します。  
 より多くの人々は彼らに最初にお金を与えそして2番目にカードを戻すATMにカードを置き去りにします。  
 情報過多などのさまざまな状況により、人々は、最善のルールではなく、知っている最も強力なルール、または最も一般的なルールに従う可能性があります。  
シティバンク。  
com –ほとんどの人にとって、名前を探すことは、その位置を解析するよりも強い規則です。  
 セキュリティの使いやすさに関する論文、Alma WhittenとDoug Tygarの「WhyJohnny Ca n't Encrypt」は、暗号化プログラムPGPは、ほとんどの大学生が使用するのが非常に難しいことを示しました。公開鍵、暗号化、署名の性質[2018]。  
アクセス制御メカニズムとセキュリティAPIはどちらも、理解しにくく、また使いにくいものです。多くの場合、セキュリティテストツールはそれほど優れていません。  
 次に、エンジニアは相互にコードをコピーしたり、オンラインのコード共有サイトからコードをコピーしたりするため、誤解やエラーが広く伝播します[11]。  
セキュリティエンジニアリング78ロスアンダーソン3。  
 心理学の研究からの洞察これすべての背後にあるいくつかの重要な科学があり、ここに2つの例があります。  
 人々は、他の人に特定の方法で行動するように誘導する環境を作成する優れたスキルを開発しました。ペンサンドソードを作る[762]。  
 まったく同じ方法で、ユーザーの選択をトレーニングおよび条件付けするためのソフトウェアアーティファクトを設計します。そのため、使用するシステムの順序は、あらゆる方法で私たちの考え方に影響を与えることができます。  
ギブソンは、クリストファー・ロングエット・ヒギンズによってさらに開発された光の流れのアイデアも思いついた[1185]。  
 光学視差のエレガントな数学的理論がありますが、私たちの目はそれをさまざまに扱います。それらには、このフローフィールドの特定の側面に対するレセプションが含まれており、その中のオブジェクトが剛体であると仮定し、回転および並進コンポーネントを解決できるようにします。  
 飛行機の着陸や車の運転などの重要なタスクに使用します。  
 それはますますコンピュータの人間の相互作用の研究と結びついています。  
2。  
 しかし、悪用可能なエラーを引き起こす可能性のある知的な攻撃者がいる場合、セキュリティは安全よりも難しい場合があります。  
 これらを探すには、コードのウォークスルーを使用してソフトウェアの脆弱性を検索できるのと同じように、攻撃ポイントの特定を目的とした認知的なウォークスルーを試す必要があります。  
 したがって、すでに機能している攻撃に注意することが重要です。  
）3。  
2性別、多様性、対人関係の変化多くの女性は、医療検査や技術が患者を男性であると想定しているため、またはエンジニアが車を設計するときに男性の衝突試験ダミーを使用しているために死亡します。スポーツウェアからスタブベスト、宇宙服まで、防護具はデフォルトで男性用に仕立てられています[498]。  
 この実現により、セキュリティエンジニアリング79ロスアンダーソン3の研究につながりました。  
 心理学研究からの洞察性ジェンダーHCI –女性が思想的に使用できるようにソフトウェアを設計する方法について。  
アメリカ人女性プログラマーの作業は、彼らが男性よりもいじくり回すのではなく、より効果的に行うことを提案しました[202]。  
ジェンダーは心理学の研究で物議を醸すトピックとなっています。  
 ほとんどの男性は体系化でより高いスコアを示し、ほとんどの女性は共感でより優れています。  
バロンコーエンの研究は、アスペルガーおよび自閉症スペクトラム障害に関するもので、これは彼が男性の脳の極端な形であると見ています。  
 私たちがそのように生まれていれば、それは間違いではありません。  
これは、女性がアメリカとイギリスでCSの約6分の1を占めているのに、男性が女性よりもコンピューターサイエンスに興味を持っている理由を説明しているのでしょうか。しかし、ここで問題が発生します。ソフトウェアの男性優位もかなり最近の現象です。  
 これは、関連する差異が遺伝的または発達的というより文化的であることを示唆しています。  
そして、これらの機能は画像で見ることができますが、それがすべてが生まれたときに置かれるという意味ではありません。私たちの脳には多くの可塑性があります。  
 おそらく、ジェンダーアイデンティティ、性的嗜好、攻撃性、共感性などの違いがあり、私たちの周りに見られるような変化があったとしても、他に何も期待されていなかったかもしれません。  
 （一部の人は、1980年にインドが家庭用コンピュータブームを脱し、ゲームへの進化を遂げたため、女性はインドでのコンピューティングで働くのが幸せであると信じています。  
2。  
おそらく結果として、男性は個人的な賞賛に対してよりよく反応し（「それは本当にあなたの頭が良かった！」）、女性はパフォーマンスの称賛によってよりよく動機付けられます（「あなたは地獄の大いなる努力をしたに違いない」）。  
 さらに、同様のメカニズムが、非学術的であるとシグマ化された民族グループの貧弱な学術的パフォーマンスの根底にあるように見えます。  
 細胞と回路を含む、遺伝子と培養の間にはいくつかの層があります。  
 この調査については、Gina Rippon [1605]を参照してください。  
 たとえば、車の方が高速か安全か。これは社会的価値観と絡み合っています。  
 米国の調査では、白人と男性によってリスクが低いと判断されており、より詳細な研究では、白人男性の約30％がリスクを非常に低いと判断しているためです。  
 アジアの男性は、自動車などのいくつかの危険に対して同様に低い感度を示します。  
もちろん、私たちのエンジニアは、教育システムや実際に私たちの文化のバイアスが少なかった場合のようにではなく、そのまま世界と連携する必要があります。しかし、コンピューターシステムは、自動車や宇宙服のように男性によって男性のために構築されているため、コンピューターシステムが区別する可能性に注意する必要があります。  
 誰もがジェンダーとセキュリティのユーザビリティに多くの作業を行ったようではないので、機会があります。  
 多くのシステムは、白人またはアジア人であり、直接遭遇しないさまざまな形の偏見や障害についてまったく考えられない、またはまったく考えられない若いフィットストレートの賢い男性によって設計され続けます。  
 開発チームのトークンオタク少女が新製品をテストするだけでは十分ではありません。虐待的関係を負っている高齢者、子供、女性を含めて、あまり教育を受けていない、脆弱な人々についても考える必要があります（これについては後で詳しく説明します）。  
 コーポレートガバナンス、市場調査、製品設計、ソフトウェア開発、テストにおいて多様性が重要です。  
 ユーザーを理解する必要があります。また、力と文化が不均衡にどのように影響するかを理解することも重要です。  
2。  
3。  
3社会心理学これは、個人の思考、感情、行動が、実際の、想像された、または暗示された他者の存在によってどのように影響を受けるかを説明しようとします。  
 それを地図に載せた結果は、権威の濫用と、宣伝、尋問、攻撃性との関連性を理解するための基礎を築いた3つの初期の論文でした。  
3。  
3。  
 被験者は実際には実験者のバカである他のグループメンバーから間違った意見を聞いて、線の長さを判断しました。  
スタンレーミルグラムは、ナチス戦争犯罪者のアドルフ・アイヒマンの1961年の裁判に触発され、実験者のせいで「学習者」の役割を演じる俳優に激しい電気ショックを与える準備ができた被験者の数を調査しました。 「教師」の場合-「学習者」がひどい痛みを感じ、被験者に止めるように頼んだときでさえ  
 ほとんどがそうでした–ミルグラムは一貫して60％以上の被験者が彼らに言われたら実に不道徳なことをするであろうと発見しました[1312]。  
3番目はスタンフォード囚人実験であり、通常の人々は命令がなくても邪悪な行動をとることができることを示しました。  
 実験の目的は、看守（そしておそらく囚人）が自己選択していたために、刑務所での虐待が起こったかどうかを発見することでした。  
 この実験も今では物議を醸しています。今日、リピートが倫理的な承認を得ることはまずありません。  
1995年から2005年の間に、自分のことを「O.cerScott」と呼ぶいたずら電話は、32の米国州（少なくとも17のマクドナルドの店舗を含む）にある68を超える米国の店舗とレストランのマネージャーに、窃盗とストリップサーチの疑いで若い従業員を拘束するように命じましたそれら。元刑務所の警備員セキュリティエンジニアリング82ロスアンダーソン3。  
 心理学研究からの洞察警察の警察になりすまそうとしたが無罪となった。  
 マクドナルドは、いたずら電話のパターンが確立されてから数年たっても、店長を適切に訓練しなかったとして訴えられました。そして2007年10月、陪審は彼らに6ドルを支払うよう命じた。  
 彼女はボーイフレンドの監護の店長によって彼女に残されたので、それは厄介な事件でした、そして、彼女はそれから彼女へのさらにいやらしい暴行を犯しました。  
 マクドナルドは、気づかなかったために彼女が受けたいかなる損害についても彼女がデマであったことに責任があり、店長は常識を適用できなかったと主張しました。  
 店長はまた、デマを警告するための会社の過失の別の犠牲者であると主張して訴訟を起こし、1ドルを手に入れました。  
 したがって、米国の雇用主は、権力の乱用に抵抗するように従業員を訓練することに失敗した場合、大きな損害を被る危険性があります。  
2。  
2傍観者の影響1964年3月13日、ニューヨークのクイーンズにある彼女のアパートの外の通りで、キティジェノベーゼと呼ばれる若い女性が刺されて死亡しました。  
 これらの報告は後に誇張されたものであることが判明しましたが、犯罪は全国的な911緊急電話番号をもたらし、また傍観者がしばしば関与しない理由の調査にもつながりました。  
 彼らは、一人の傍観者が85％の時間を助けるだろうが、他の4人が犠牲者を見ることができると思った人は31％の時間しか役に立たないことを発見した。グループサイズは他のすべての影響を支配しました。  
 責任の分散は、他の多くの状況で目に見える影響を及ぼします。  
 もちろん、セキュリティは通常、他の人々が対処するものと見なされます。  
 Lasse Liebst、Mark Levineなどは、過去10年間にいくつかの国で行われた多くの公衆紛争のCCTV映像を調査しました。10件中9件のケースで、1人以上の傍観者が介入して、格下げをエスカレートし、より多くの傍観者が介入すればするほど、彼らは成功する[1163]。  
3。  
4詐欺の社会的脳理論私たちの2番目の大きなテーマは、同じく社会心理学にも当てはまり、詐欺に関する研究の増加です。  
2。  
 それまで、人類学者たちは、より良いツールを作るために私たちがより大きな脳を進化させると考えていました。  
 旧石器時代全体を通して、私たちの脳はチンパンジーから人間のサイズに進化しましたが、同じシンプルな石の軸を使用しました。  
 それで、ニックハンフリーに尋ねた理由は、大脳がまだ必要ないのに、進化したのでしょうか。ケージに入れられた霊長類と野生の霊長類の両方の行動を観察することに触発され、彼の仮説は知性の主要な機能は社会的であるというものでした。  
 これは現在、増え続ける証拠によってサポートされており、心理学を学問として変容させてきました。  
 ほとんどすべてのインテリジェントな種は社会的文脈で発達した。  
）その後、霊長類学者のアンディホワイトンは、戦術的欺瞞の初期の証拠の多くを収集し、社会知性をマキャベリの脳仮説として作り直しました。私たちは他人をだますために賢くなり、中傷も検出できるようになりました[360]。  
 しかし、HugoMercierとDan Sperberは最近、現代の人間の脳が他の何よりも議論するための機械であるという証拠を集めました[1294]。  
社会知性仮説からの2番目のスレッドは、理論の考え方です。これは、1978年にDavid PremackとGuyWoodru↵によるアイデアですが、1983年の古典的な実験でHeinz WimmerとJosef Pernerによって開発され、子供が最初に誰かがだまされたことを知ることができる時期を決定しました。 [2029]。  
 アンはその後部屋を出て、サリーを別のカップの下に置くように切り替えます。  
 通常の子供は、およそ5歳から正解を受け取ります。これは、彼らが他者の信念と意図を識別する能力を獲得したときです。  
多くのコンピューター科学者やエンジニアはある程度その範囲にいるようであり、私たちは一般的に神経型の人々ほど欺瞞が得意ではありません。  
 ああ、そして地下市場が邪悪な目的のためにそれを使用できる詐欺師や詐欺師と一緒に邪悪なコードを書くことができるオタクをまとめる前に、はるかに少ないサイバー犯罪がありました。  
 しかし、これは複雑な分野です。  
2。  
 そして、他の種類の共感的な赤字が多くの犯罪に関与しています。  
 過激化については、後でセクション26で詳しく説明します。2。  
 Robert Triversは、他者をよりよく欺くために、私たちが自分を欺く能力を進化させたと主張します。「動物のコミュニケーションにおいて、詐欺が基本的なものである場合、強力な選択tospot欺瞞があり、これは、ある程度の自己を選択する必要があります。欺瞞、いくつかの事実と動機を無意識にレンダリングして、裏切らないように-自己認識の微妙な兆候によって-欺瞞が実践されている」[904]。  
 正直なギークから、製品を完全に信じる魔法の能力を持つ偉大なセールスマンまで、さまざまな自己欺瞞能力があるかもしれません。  
 たとえば、トニーブレアが2003年にイギ​​リスに戦争に行くことを説得したときに、イラクが大量破壊兵器を持っていると本当に信じていた場合、それは実際には嘘でしたか？誠意をどのように定義しますか？どのように測定できますか？そして、彼らがあなたにうそをつくことができないと予想したならば、あなたは国家指導者を選ぶことさえしますか？ [904]には長い議論があり、議論はやる気のある推論に関する他の研究と関連しています。  
 この一連の調査は、不快な情報の拒否に関するさまざまな側面を説明したジークムントフロイトにまでさかのぼります。その中には、私たちが行う悪いことに対する罪悪感を最小限に抑え、他人を非難する方法などがあります。  
 人々は自分の信念とバイアスを確認する他の人に耳を傾けることを好み、これは情報の快楽的価値の観点から分析することができます。  
 もう1つのリンクは、HugoMercierとDan Sperberの議論の機械としての脳に関する研究です。これについては、前述しました。  
 敵意の検出は、私たちの先祖代々の進化的環境において重要なことでした。州の前の社会では、おそらく男性と少年の4分の1が殺人で死亡し、さらに私たちの祖先の多くは動物の捕食者によって殺されました。  
その結果、テロなどの敵意を伴う脅威に対する防御に費やしすぎており、セキュリティエンジニアリング85ロスアンダーソン3に対する防御には十分ではありません。  
 心理学研究からの洞察より多くの人々を殺す流行病、またはさらに多くを殺すことができる気候変動。  
 暗号化では、信念のロジックを使用して認証プロトコルのセキュリティを分析し、「アリスは、チャーリーがキーKを制御しているとボブは信じている」などのステートメントを処理します。これについては、次の章で説明します。  
 ダンデネットは、哲学における意図的なスタンスを導き出し、推論の際に使用する命題の態度（信念、欲望、および認識）は、人や動物の意図に帰着すると主張しました。  
 ワソンのテストでは、被験者には、片側に文字の等級があり、もう一方に数字のコードがあるカードを検査するように指示され、「生徒がカードの前面にグレードDを持っている場合、背部はコード3”でマークする必要があります。  
 しかし、進化心理学者のレダコスミデスとジョントゥービーは、ルールを「ビールを飲んでいる場合、彼は20歳でなければならない」に変更すると、同じ問題が容易になることを発見しました。歳と16歳。  
 CosmidesとToobyは、論理とおそらく算術を実行する私たちの能力は、社会的交流を規制する手段として進化したと主張しています。  
 私は、詐欺に陥った白人がアフリカ人を愚かであると考えているナイジェリアの詐欺師に言及したので、彼らはそれに値する。詐欺師が外国の標的を公正なゲームと見なしている例はもっとたくさんあります。  
 雇用主が給料を下回っているため、費用をまかなうのは当然だとか、税金をだまし取ったときに州が福祉のためにお金を浪費していると人々は感じるかもしれません。  
DDoS-for-hireservicesを運営する子供たちは、「ウェブストレッサー」サービスを提供することは合法であることをお互いに安心させ、そのサービスは合法的な目的にのみ使用できるとウェブサイトで述べました。  
 UK NationalCrime Agencyは、ウェブストレッサーサービスを検索しているすべての人がDDoSが犯罪であるという社会的警告を確実に目にするように、Google広告を購入しました。  
最後に、社会的文脈の喪失は、オンラインの脱抑制の要因です。  
 富裕層はパートナーを見つけることができますが、悪質な火炎戦争も見られます。2。  
これがすべての主導権を握るのは、オンライン詐欺の性質と規模が適切な相互作用設計によって調整できるということです。  
 彼らは、WhatsAppによってサポートされているグループなど、パフォーマンスを刺激するための有名人もトローリングを促進するための匿名性もないクローズドグループを警戒しました。  
3。  
5ヒューリスティックス、バイアス、行動経済学2000年代中頃からセキュリティ研究者によって適用されてきた心理学の1つの分野は、心理学と経済学の境界に位置し、人々が使用するヒューリスティックスとそれに影響を与えるバイアスを研究する意思決定科学です。意思決定をするとき。  
 初期の先駆者は、初期のコンピューター科学者でありノーベル賞を受賞したエコノミストでもあるハーブサイモンでした。その理由は、古典的な合理性は、計算の選択がどれほど難しいかに関係なく、期待される実用性を最大化することを意味するということです。  
3。  
5。  
 彼らは最初にリスク選好度をモデル化するプロスペクト理論を開発しました。多くの状況で、100ドルを失うことを嫌う人々はすでに100ドルを勝つことを評価する以上のものを持っています。  
'私たちは確率の計算にも長けており、あらゆるヒューリスティックスを使用して決定を下します。•多くの場合、最初の推測または比較に基づいて判断し、必要に応じて調整します–アンカー効果;•推論に基づいています例を思い浮かべるのは簡単です– 50,000年前のライオン攻撃では問題ありませんでしたが、マスメディアがテロのイメージで私たちを攻撃したとき、誤った答えを出します。•私たちは、私たちのことについて懐疑的です。私たちが見たものよりも聞いたことがあります。おそらく、ニューロン処理のビジョンが多いためです。•非常に起こりそうもないが非常に悪い結果をもたらすイベントについて心配しすぎています。セキュリティエンジニアリング87ロスアンダーソン3。  
 心理学の研究からの洞察•言われたことよりも、自分のために自分たちが考え出したことを信じる可能性が高くなります。  
 多くの人々がテロリズムを伝染病、交通事故、さらには食中毒よりもはるかに深刻な脅威であると認識しています。これは間違っていますが、行動経済学者にはほとんど驚くことではありません。  
 （テロについて議論する際にパートIIIで検討する要因は他にもあります。  
 心理学者ダニエルギルバートは、挑発的に「同性愛者のみが地球温暖化を引き起こした場合」と題した記事で、テロリズムに対する恐怖と気候変動に対する恐怖を比較しています。  
 第二に、地球温暖化は誰の道徳的感受性にも違反しません。第3に、それは明確で現在の危険というよりは長期的な脅威であり、第4に、スロートーンではなく環境の急激な変化に敏感です[764]。  
 私たちはまた、満足感を味わっています。これは、特に小規模な取引の場合、確率を完全に計算しようとするのではなく、「十分に良い」代替案を選ぶことを意味します。  
）だから、手の中の鳥は茂みの中では2匹の価値があると言う人々から始めて、私たちはリスクに対する人々の態度を理解してモデル化するのに役立つ非常に多くの機械を開発することができます。  
2。  
2現在の偏見と双曲的割引セントオーガスティンは有名に「主よ、私を貞節にするように祈りましたが、まだそうではありません。  
 この現在のバイアスにより、多くの人々が更新を拒否するようになり、これは長年オンラインでの技術的な脆弱性の主な原因でした。  
 リマインダーにより、無視率が約90％から約34％に削減され、全体のコンプライアンスが最終的に2倍になる可能性があります[726]。  
セキュリティエンジニアリング88ロスアンダーソン3。  
 心理学研究からの洞察双曲線割引は、現在のバイアスを定量化するために意思決定科学者が使用するモデルです。  
 このようなモデルは、プライバシーのパラドックスを説明しようとするために適用されています-なぜ人々は調査でプライバシーを気にしているがオンラインでは行動しないと言うのですか？  
6。  
 まとめると、無料で入手できるという即効性のある明確な有用性は、個人情報を過度に開示したり、疑わしいWebサイトに開示したりする将来のランダムなコストを上回ります。  
2。  
3デフォルトとナッジこれはデフォルトの重要性につながります。  
 2009年、Richard ThalerとCass Sunnsteinはこれを探るベストセラー「ナッジ」を書き、政府が適切な障害を設定するだけで個人の自由を侵害することなく多くの政策目標を達成できることを指摘しました[1876]。2つ目の例は、ドナーが積極的に同意しなければならないイギリスよりも、死者の臓器が反対されない限り法律で許可されているスペインでは、移植可能な臓器がはるかに多いということです。  
 ユーザーが行わなければならない一連の選択、それらが行う順序、および何もしない場合のデフォルトは、選択アーキテクチャと呼ばれます。  
デフォルトはセキュリティにおいても重要ですが、多くの場合、敵を倒すために敵によって設定されます。  
 これは危険なデフォルトだけでなく、制御のパラドックスも悪用します。制御の幻想を提供すると、人々はより多くの情報を共有するようになります。  
 行動経済学者のジョージ・ローウェンシュタインは、「プライバシー管理の設定により、人々は首を絞めるためのロープをより多く与えることができる」と述べています。  
」[1533] 3。  
5。  
 発生生物学の研究は、幼い頃から、社会現象（両親や兄弟の認識など）と物理的セキュリティエンジニアリング89ロスアンダーソン3には異なる精神処理システムがあることを示しています。  
 心理学研究からの洞察現象。  
 子どもたちは物理学を使って見ているものを説明しようとしますが、理解が足りないときは、意図的な行動の観点から現象を説明します。  
 ブルームはそれが興味深い側面を持っていることを示唆しています：それは人間に体と魂が異なると信じるようにさせます、そしてそれゆえに宗教的信念の基礎を築きます。  
 ただし、セキュリティエンジニアにとっては関連性があるかもしれません。  
 第2に、インターネットのgorydesignの詳細についてユーザーに教えることでフィッシングを抑制しようとする試み（たとえば、銀行から送信されたように見えるURLの電子メールを解析するようにユーザーに指示すること）は、戸惑うと価値が限定されます。  
 安全なデフォルトの方が良いでしょう。  
2。  
5影響ヒューリスティックメカニズムではなく意図の観点から考えるように人々に指示すると、ポールスロビックと同僚[1787]が調査した影響ヒューリスティックを利用できます。  
 したがって、マーケティング担当者や詐欺師は、感情に訴えるようにすることで、理由ではなく感情を使用し、計算ではなく発見的方法を使用して、質問に答えてもらうことができます。  
したがって、多くのマルウェアをインストールするためにポルノのWebサイトが使用されていることを誰もが驚かないでください。教会のWebサイトは、維持管理が不十分で、ハッキングが容易です。  
意図的に物事を説明する私たちの傾向を強化することができる他の要因には、脳の合理的な部分が単に疲れる認知過負荷が含まれます。  
 したがって、多忙なウェブサイトを構築している銀行は、より多くの生命保険を販売できる可能性がありますが、顧客をフィッシングに対してより脆弱にする可能性もあります。  
3。  
2。  
6認知的不協和社会心理学のもう1つの興味深い問題は、認知的不協和理論です。  
 現実的な結果の1つは、物事がうまくいかなかったという証拠が山積しているにもかかわらず、人々は間違った行動方針を継続的に続けることができるということです[1863]。  
 セキュリティ専門家は「騒ぎを感じる」必要があります。つまり、最近確立された社会的手がかりと期待により、通常は予約していることに対して「ただやる」よう圧力をかけられる状況に注意する必要があります。  
 しかし、これを知覚するように人々を訓練することは十分に困難であり、平均的な人に社会の流れを打ち破り、「やめろ！」と言わせることは困難です。  
 そのようなトレーニングを主流化することの問題は、そのために利用できるお金が、ビジネスモデルが顧客を混乱させることになる企業のマーケティング予算よりも桁違いに少ないことです。  
2。  
7リスクサーモスタット人々がリスクへのエクスポージャーを管理する方法について、いくつかの興味深い実証的研究が行われました。  
 シートベルトはドライバーに安全性を感じさせるものであり、彼らは彼らの知覚されるリスクを以前のレベルに戻すために速く運転します。  
 教訓は、テストには生態学的妥当性が必要であることです。可能な限り現実的な設定で、提案された介入の影響を評価する必要があります。  
3実際の欺瞞これは私たちを理論から実践へと連れて行きます。  
 セールスエグゼクティブは、休日のアパートのファイナンスプランの提供者に夢中になるかもしれませんが、警官は、彼らの存在によって、より慎重に運転するようにあなたを誘惑するかもしれません。パークレンジャーは、キャンプ場を注意深く消火してクマに餌をやらないようにあなたに指示するかもしれません。そして、企業の弁護士はあなたのウェブサイトから何かを削除するようにあなたを脅すかもしれません。しかし、エコノミストは、そのようなテクニックの利他的な使用は、セルフィッシュのテクニックよりも一般的であると考えたことはありません。  
3。  
 スタンフォード大学の説得テクノロジーラボは、人々を画面に夢中にさせる技術を開発する最前線にあり、卒業生の1人である元Google社員のトリスタンハリスは、批評家になりました。  
 電話やその他の画面はメニューを提示し、したがって選択を制御しますが、それ以外にもそれ以上のものがあります。  
 しかし、コンピュータに先行する多くの古い技術があります。  
3。  
著名な作家は、貿易のトリックを文書化するために中古車から住宅改修、生命保険まですべてを販売する夏の仕事をとった心理学の教授であるロバート・チャルディーニです。  
これらは：1。  
 コミットメントと一貫性：一貫性がないと感じた場合、人々は認知的不協和音を訴える; 3。  
 これは、メンバーであるグループ内の他のメンバーをフォローすることを意味し、グループが小さいほどプレッシャーが強くなります。4。  
 権威：ほとんどの人々は権威のある構成に敬意を払っています（上記のミリグラムの研究を思い出してください）; 6。  
これらはすべて心理学的現象であり、継続的な研究の対象となっています。  
 すべては、私たちが常に遭遇する広告やその他のメッセージで繰り返し使用されます。  
3。  
 ウィルソンは、最も一般的な詐欺「The Real Hustle」について、9シーズンのテレビ番組を調査して登場しました。そこでは、疑いを持たない公衆のメンバーに詐欺が行われ、彼らは返金され、報告され、使用されるビデオ映像の許可を求めました。テレビで。  
1。  
 これはほとんどの魔法のパフォーマンスの中心です。  
 社会的コンプライアンス–社会は、権威を持っているように見える人々に質問しないように私たちを訓練し、銀行や警察から来たふりをするconmenに対して脆弱な人々を残します。  
 群れの原則–周りの誰もが同じリスクを共有しているように見えるとき、人々は警戒を怠ります。  
4。  
多くの人々は「違法だからあなたは善意を得る」という考えに魅了され、詐欺で入手した飛行機のチケットの転売などの詐欺家族全体がこれを有効にします。  
 優しさ–これは不正直さのフリップ面であり、Cialdiniの相互主義の適応です。  
6。  
 良い詐欺師は、マークが夢を夢見るのを助け、これを使って搾乳することができます。  
 時間的プレッシャー–これにより、人々は考えるのをやめるのではなく、内臓的に行動するようになります。  
Cialdiniの原則との関係は明白であるはずです。  
 多くの不動産業者が同じ手法を使用しているため、オンラインの宿泊施設詐欺を調査したところ、検出器のコーディングは困難でした。  
 （これらは、通常のマーケティング資料の他の場所にもあります。  
 Onegood識別子は技術的なようです：マルウェアは多くの小さなセキュリティエンジニアリング93ロスアンダーソン3によって配布されます。  
 逮捕のリスクがあるためにボットネットは偽装しているが、PUPはほとんど1つの大きなネットワークによって配布されている[954]。  
ウェブ検索で1位にランクされた企業の73％が悪かった4。  
 悪質な企業は、WebサイトでTRUSTeプライバシー証明書などの安価な信頼信号を表示する可能性も高かった。  
そして、「合法」ビジネスの不正なマーケティング慣行があります。  
 これらのうち少なくとも183は明らかに欺瞞的だった[1242]。  
 詐欺の起訴の閾値をわずかに下回る詐欺からのこの一定の圧力は、一般に信頼に冷酷な影響を及ぼします。  
 また、ソフトウェアの更新に対する信頼が失われることさえあります。調査によると、セキュリティパッチよりもセキュリティプラス機能のアップグレードを適用する可能性は低いと言われていますが、アップグレードに関するフィールドデータには差異がありません（1591）。  
3。  
 軍事組織と諜報機関は常にお互いの状態を狙っています。古いソビエト連邦のインテリジェンスの成功のほとんどはこの種のものでした[118]。  
調査ジャーナリスト、私立探偵、および詐欺師は、20世紀後半に、偽の口実の電話を産業プロセスと芸術形式の間の何かに発展させました。  
 国に国民健康サービスがあり、全員が登録している場合、秘訣は、あなたがターゲットであると思っていた地域の管理システムにアクセスできる誰かに電話をかけ、保健サービスの他の誰かになりすまして尋ねることでした。彼らは、週に約30件の偽口実の呼び出しを検出しました。これは、英国全体で週6000aまたは年間300,000に拡大します。  
 本当の修正はプライバシー法の施行ではなく、管理者が電話に出るのをやめただけです。  
 それを持っていると聞いて、conmanは言いました「私達はそう考えました。  
セキュリティエンジニアリング94ロスアンダーソン3。  
 不正行為の疑い今すぐPINを教えてください。システムにアクセスしてカードをキャンセルできます。  
アートフォームに関しては、これまでに出版された最も不安なセキュリティ本の1つは、ケビンミトニックの「Art of Deception」です。  
 彼の典型的なハッキングは、電話会社の従業員に同僚であるふりをして、パスワードなどの「助け」を求めていました。  
 嫌がらせを受けたシステム管理者は、CEOのパーソナルアシスタントであると主張する誰かによって、雑談で1回または2回呼び出されます。このアイデアが受け入れられると、発信者は上司に新しいパスワードを要求します。  
ソーシャルエンジニアリングは、2006年9月にヒューレットパッカードの会長であるパトリシアダンが彼女に不審な他の理事と彼女が敵対的であると考えたジャーナリストの電話記録を入手するためにプリテキストを使用した私立探偵を雇ったことを訴えたとき、世界の見出しニュースとなりました。  
探偵は詐欺の有線通信で有罪判決を受け、社会奉仕を行うように宣告された[138]。  
ソーシャルエンジニアリングに関する知名度が高まる中、2007年に税務管理の財務総監によるIRSの監査があり、そのすべてのレベルで102人のIRS従業員を呼び出し、ユーザーIDを求め、パスワードを既知の値に変更するように指示しました; 62人がそうした。  
 それ以来、多くの監査事務所がソーシャルエンジニアリングをサービスとして提供してきました。彼らはクライアントをフィッシングして、それがいかに簡単かを示しています。  
ソーシャルエンジニアリングは、個人情報の盗用に限定されません。  
 この章の冒頭にあるブルースシュナイアーの引用は、株式詐欺の報告書に出ており、偽のプレスリリースでは、会社のCEOが辞任しており、その業績は修正されると述べています。  
 この種の偽のニュースは永遠に出回っていますが、インターネットによって宣伝が容易になり、ソーシャルメディアが普及しているようです。  
4。  
セキュリティエンジニアリング95ロスアンダーソン3。  
 実際の欺瞞3。  
3フィッシング電話ベースのソーシャルエンジニアリングは20世紀の人気の戦略でしたが、オンラインフィッシングが21世紀の主要な戦略に取って代わったようです。  
 それはあなたの状態を訓練するのに十分困難です。平均的な顧客のトレーニングはさらに困難です。  
 そして、単純に平均のために設計することはできません。  
 したがって、システムを使用する最も簡単な方法は、最も安全であるべきです。  
 それまでに、スパムを送信するために電子メールアカウントをクラックする試みは、AOLのWebページに「パスワード要請の報告」ボタンを配置するのに十分一般的になりました。また、「パスワードフィッシング」への最初の言及は1990年に行われ、人々がUnixログオンパスワードを収集するように端末のファームウェアを変更している[443]。  
 そのうち138人が有効なパスワードを返しました。  
しかし、そのほとんどが当局に電子メールを報告していませんでした[812]。  
 初期の攻撃は銀行のWebサイトを模倣したものでしたが、粗雑で貪欲なものでした。攻撃者はATM PINなどのあらゆる種類の情報を要求し、彼らの電子メールも貧弱な英語で書かれていました。  
2008年頃までに、攻撃者はより良い心理学を使うことを学びました。彼らはしばしば、URLが変更されただけの本物の銀行のメールを再利用したり、「PayPalアカウントに新しいメールアドレスを追加していただきありがとうございます」のようなメールを送信して、顧客にログオンして彼らがそうではなかったことを訴えました。  
ペイパル。  
 その時までに、フィッシングは国家の俳優によっても使用されていました。セクション2で説明しました。  
2 2008年のオリンピックの間に、中国の情報機関がダライラマのプライベートビジネスをどのように侵害したか。  
詐欺による損失は急速に拡大しましたが、2015年頃には安定しました。  
 フィステルマンが顧客クレデンシャルを盗むことと、アカウントを使用して盗まれた資金をロンダリングすることの両方の観点から、フィッシャーマンはいつでも各国で最も簡単なターゲットに当たるという競争の激しい状況でした。  
 それ以来、大規模なセキュリティエンジニアリング96ロスアンダーソン3を見てきました。  
 Amazonのような非金融企業への攻撃のスケール; 2000年代後半に、詐欺師はメールと住所を変更し、クレジットカードを使用してワイドスクリーンテレビを注文します。前の章で述べたように、フィッシングは、ボットマスターが新しいマシンをボットネットに募集するために大規模に使用されます。また、特定の方法で特定の人や企業を狙うこと、および諜報機関によってフィッシングが使用されます。  
 標的のラップトップまたは電話にインストールされているクライムウェアが同じ厩舎からのものである場合でも、使用されるルアーサンド技術は異なります。  
 結局のところ、私たちがコンピューターに依存していること、すべてのコンピューターが安全ではないこと、そして常に攻撃が行われていることを考えると、文明は崩壊していないのですか？サイバー犯罪は見た目ほど簡単ではありません。  
我々は、悪意のある人がトニー・グリーニングの1995年のフィッシング詐欺に追いつくのに7年かかったことを指摘しました。  
この本の第2版と2016年に私たちはそれを実際に目にしたことを引用しました：ギャングが米国とオーストラリアの銀行のトロイの木馬を使って何十万ものフィッシングを、LinkedInから明らかに名前と役職を付けて、会社の金融部門で働く個人に送りました[1297]。  
 私たちが見る他のパーソナライズされたバルク詐欺は、被害者が自分の個人情報が侵害されたと主張し、パスワードまたはクレジットカード番号の最後の4桁を証拠として含むと主張する電子メールを取得する恐喝の試みですが、そのような詐欺からの収量は低いようです。  
 2020年に、若者のグループがTwitterをハッキングしました。1,000人以上の従業員が内部ツールにアクセスして、ユーザーアカウントを制御できるようにしました。ギャングはビルゲイツ、バラックオバマ、エロンマスクなどの有名なユーザーのアカウントからビットコイン詐欺のつぶやきを送りました[1292]。  
4。  
7。  
 詐欺師の間でのこのような「譲渡可能なスキル」の広がりは、主流のテクノロジーの採用と多くの点で似ています。  
3。  
3。  
 未公開の財務データ、まだ特許を取得していない産業調査、軍事計画など、本当に価値のある秘密を保護することは、アクセスできる人の数を制限すること、そして誰とどのように話し合うことができるかについての教義にも依存します。  
 私たちの医療プライバシー事件では、口頭での電話について医療サービスを教育し、厳格なコールバックポリシーを設定しました。発信者からではなく、医療サービスの内部電話帳から取得した番号に電話をかけない限り、電話で医療記録について話し合うことはありません。  
もう1つの例は、シリコンバレーの大規模なサービスファームから来ています。これは、部外者がキャンパス内の建物に停泊しているときに侵入を試みていたためです。  
 解決策は、誰かがあなたのために建物のドアを開いたままにしたときに、あなたに彼らにあなたのバッジを示すという社会的ルールを作成して埋め込むことでした。  
多くの場合、教育するのが最も難しいのは最年長者です。コンサルタント会社は、匿名の招待状の一部として、上場企業500社のファイナンスディレクターに「生涯のパーティーに参加するチャンスのために」とUSBメモリスティックを送り、46％がそれをコンピューターに入れました[1031]。  
機密性の高い紙をゴミ箱に捨てないなど、いくつかの運用上のセキュリティ対策は常識です。  
 UK首相のトニーブレア首相から送信されたように見え、当初は「ハッカー」のせいにされた恥ずかしいメールの漏洩が、私立探偵の自宅のゴミ箱から私立探偵[1208]によって流されたことが判明しました。  
 調査によると、企業はコンプライアンス予算が非常に多く、つまり、目標の達成に明らかに貢献していないタスクに1年に何時間も費やす準備ができているだけです[196]。  
 情報を開示するために騙されたくない情報がある場合は、システムがそれを開示できないように、または少なくとも他の情報メンバーと話したり、他のフープを飛び越えたりできるようにシステムを設計する方が安全です。  
 多くのSecurity Engineering98Ross Anderson3もあります。  
 PASSWORDSお客様がビジネスプロセスの脆弱性を見つけたときに試行する小さな詐欺。  
3。  
5欺瞞研究最後に、欺瞞研究についての言葉。  
ポリグラフは、心拍数と皮膚コンダクタンスを介してストレスを測定します。これは1920年代から使用されており、米国の一部の州では刑事捜査で使用されています。また、連邦政府が最高機密のクリアランスを探すために連邦政府を利用しています。それは熟練した尋問者の手に渡る効果的な小道具になることができますが、重要な要素は小道具ではなくスキルです。  
 皮膚のコンダクタンスを介してストレスを測定するだけでなく、目の動きと上半身の動きによる罪悪感を使って気晴らしを測定できます。  
 ただし、そのようなテクノロジーは、質問者のスキルを最大限に高めることができ、それらがうまく機能することをジャンクサイエンスとして扱う必要があると主張しています。  
詐欺に対処するための2番目のアプローチは、実際の顧客の行動について機械学習分類子を訓練することです。  
 たとえば、Noam BrownとTuomas Sandholmは、テキサスホールデムの10,000ハンドの12日間のマラソンで12人のエキスパートプレーヤーを倒したPluribusと呼ばれるポーカープレーイングボットを作成しました。  
 相手の顔のジェスチャーやボディランゲージなどの「テル」にアクセスせずに、常にエキスパートを倒すことができること自体が語っています。  
3。  
 パスワードは、おそらく1970年代以来、セキュリティエンジニアが直面する最大の実用的な問題の1つです。  
問題の状況を説明するために、設定を求められるほとんどのパスワードは、Security Engineering99Ross Anderson3ではありません。  
 パスワードはあなたの利益のために、他の誰かのために。  
そのため、コメントを残す必要があると非常に不愉快なニュース記事をポイントすると、登録する必要があることがわかります。  
 フォームにメールアドレスを入力して送信します。  
 メールのリンクをクリックすると、別の広告のあるページが表示されます。  
 そのような状況では、ランダムなガベージを入力して、ブラウザにそれを記憶させる方がよいでしょう。それ以上なら、気にしないでください。  
 この生態系は、Ryan Holiday [913]によって詳細に説明されています。  
1。  
 ログオンするたびに、後でこのパスワードを尋ねます。  
 通常はセキュリティに関する質問をしたり、プライマリメールアカウントを使用したり、SMSを携帯電話に送信したりして、忘れたパスワードや侵害されたアカウントに対処できるようにする回復メカニズムがあります。  
 この背後にあるのは、パスワードチェックの技術プロトコルメカニズムです。通常、ノートパソコンや電話でパスワードを入力するときにパスワードを暗号化し、ローカルの暗号化された値と比較するか、リモートサーバーにアクセスしてチェックします。  
 多くの場合、複数のプラットフォーム間でパスワードを同期するプロトコルメカニズムがあるため、ラップトップでパスワードを変更した場合、新しいパスワードを入力するまで、スマートフォンでそのサービスを使用できません。  
5。  
6。  
下から上に向かっていきましょう。  
 したがって、「アイデンティティ管理」をアウトソーシングすることは、ビジネスに意味があります。  
 パスワードを悪用しようとする主な原因は、企業がハッキングして何百万もの電子メールアドレスとパスワードを開示したことです。これはbadSecurity Engineering100Ross Anderson3です。  
 PASSWORDSみんなが他の場所で試します。大きな企業はこれをすぐに見つけますが、小さな企業はそうではありません。  
 繰り返しますが、あなたが小さなウェブサイトであるか、人々があまりアクセスしないウェブサイトであるなら、それをするのは難しいです。  
 これはパスワードの回復をもたらします。  
4。  
 スタッフなどの知っている人がパスワードを忘れた場合、その人を知っている管理者またはマネージャーと対話させることができます。  
 また、大規模なサービス会社は毎日数万のアカウントを回復するため、大多数のケースで人間の介入なしにそれを実行する方法が必要です。  
 このようなほぼ公開された情報は、多くの場合簡単に推測できるため、パスワード自体を推測するよりも簡単にアカウントに侵入できます。  
 セレブリティの場合、または以前の親しいパートナーによる虐待の場合、使用可能な秘密がない可能性があります。  
 これらは両方とも公開情報でした。  
 これは2013年にピークを迎えました。これを修正するための対策は、常に口座の変更を郵送で受取人に通知することでした。  
 たとえば、攻撃者は19を得ることができます。  
 37％の人が間違った答えを出しました。  
 安全ではないことに加えて、「セキュリティの質問」は使いづらいことがわかりました。英語を話す米国のユーザーの40％は、必要なときに回答を思い出せませんでしたが、SMSリセットコードを使用して2倍のアカウントを回復できました[291]。  
 しかし、誰かがその電子メールアカウントを侵害した場合、依存しているすべてのアカウントを取得することもできます。  
4。  
これは通常、SMSによって携帯電話に送信されるコードです。コードを暗号化して特定のハンドセットに関連付けることができるアプリを使用することをお勧めします。Googleの調査によると、SMSはボットによるすべてのバルクパスワード推測、96％のバルクフィッシング、76％の標的型攻撃を阻止します[574]。  
 2020年の問題は、SMS認証コードのインターセプトに基づく攻撃の急増であり、これは主にSIMスワップに関与しているようであり、攻撃者はあなたをあなたの携帯電話会社に装ってアカウントの代わりのSIMカードを入手します。  
 SIMスワップ攻撃については、セクション12で詳しく説明します。  
4。  
 このような攻撃については、電話と銀行の章で詳しく説明します。  
 標的型攻撃については、アリアナミリアンによる他の研究とUCSDおよびGoogleの同僚がオンラインで「ハッキングフォーハイヤー」サービスを宣伝しているギャングにアプローチし、Gmailパスワードのフィッシングを依頼しました。  
 これはまだ未熟な犯罪市場ですが、そのような攻撃を阻止するには、アプリまたは認証トークンを使用する方法があります。  
 myGmailでハードウェアセキュリティキーを使用する場合、回復メカニズムとして金庫に2つ目のキーが必要ですか？ （恐らく。  
7。  
）メール通知は、疑わしいログイン試行だけでなく、コードの助けを借りて成功した新しいデバイスへのログインを人々に知らせるためのデフォルトです。  
 次に被害者がどのように回復するかが次の問題です。  
しかし、そのようなシステムを設計するときは、それが最も弱いフォールバックメカニズムと同じくらい強力であることを忘れないでください。それは、制御できないメールプロバイダーによる回復メールループ、SIMスワッピングやモバイルマルウェアに対して脆弱な電話コード、または開いている人間などです。ソーシャルエンジニアリングに。  
4。  
4。  
2で説明したように、パスワードとパスワード回復の質問を推測することで、オンラインアカウントに常に侵入するボットネットがあります。  
1。  
そして人々が新しいサービスを発明し、それらにパスワードを設定すると、パスワード推測者は新しいターゲットを見つけます。  
 一方、パスワードを忘れたため、数十億ドル相当の暗号通貨が失われました。  
 ユーザーは十分に高い確率でパスワードを正しく入力しますか？  
 ユーザーは、誤って、故意に、または詐欺の結果として、パスワードを第三者に開示することにより、システムのセキュリティを破りますか？3。  
3信頼性の高いパスワード入力の困難最初の人的要因の問題は、パスワードが長すぎるか複雑である場合、ユーザーがパスワードを正しく入力できない可能性があることです。  
 お客様がソフトウェア製品のアクティベーションコードを入力するのが困難な場合、これによりサポートデスクへの高額な通話が発生する可能性があります。  
 これは、3語または4語のパスフレーズなど、より長く単純な秘密に向けて人々を駆り立てる要因の1つです。  
 顧客はお金を販売代理店に渡し、20桁の番号をレシートに印刷します。  
 STSの設計者は、人口の多くが文盲であり、数字を入力する途中で人々が迷子になる可能性があるため、システムが使用できなくなる可能性があることを心配しました。  
 最大の問題は入力エラーであり、これは最初の行に4桁の3つのグループが続き、2番目の行に2つが続く[93]で、20桁を2行に印刷することで対処されました。  
2。  
これらは、12桁の10進数のみで構成されています。  
 実験では、12桁がSecurity Engineering103Ross Anderson3の最大値であることが示唆されました。  
 そのような状況では、パスワードを確実に伝えることができます。  
2。  
4。  
 12桁から20桁は電報またはメーターのチケットからコピーするのは簡単ですが、顧客がパスワードを覚える必要がある場合は、攻撃者が推測しやすい値を選択するか、書き留めるか、またはその両方を行います。  
問題はコンピュータへのアクセスに限定されません。  
 ホテルに着いたら、フロントマシンでクレジットカードをスワイプし、数値アクセスコード付きのレシートを受け取って、部屋のドアのロックを解除します。  
 よくある失敗モードは、真夜中に起きてトイレに行き、アクセスコードを忘れて、レシートをまだ持っていないことに気づいたことです。  
パスワードの覚えやすさは、5つの主要な見出しの下で議論できます：ナイーブチョイス、ユーザーの能力とトレーニング、設計エラー、操作の失敗、ソーシャルエンジニアリング攻撃に対する脆弱性。  
4。  
1ナイーブな選択1980年代半ば以降、人々はどのような種類のパスワードを選択するかを調査し、配偶者の名前、単一の文字を使用するか、単に改行を押して空の文字列をパスワードとして与えていることさえわかっています。、/。  
 FredGramppとRobert Morrisの1984年のUnixセキュリティに関する古典的な論文[805]は、パスワードが6文字以上で文字が1つ以上ないソフトウェアが利用可能になった後、20の最も一般的な女性名のファイルを作成し、それぞれに1つの桁。  
 当時、Unixシステムはすべてのシステムユーザーが読み取れるファイル/ etc / passwdに暗号化されたパスワードを保持していたため、どのユーザーも他のユーザーのパスワードの推測を検証できました。  
1990年、ダニエルクラインは25,000のUnixパスワードを収集し、プーチンの量によっては21〜25％のパスワードが推測される可能性があることを発見しました[1056]。  
4％、4％の一般的な名前、ユーザー名とアカウント名の組み合わせ2。  
4％）およびスポーツ用語（0。  
 他のパスワードは、ユーザー「Daniel V」に属するアカウント「klone」を取得するなど、使用されたパターンを推測します。  
4。  
 翌年、AlecMu↵ettは「クラック」というソフトウェアをリリースしました。これは、マングリングルールのセットによって派生した辞書とパターンを使用してUnixパスワードを総当たりするソフトウェアです。  
 彼はまた、スタンドアロンシステムでも、攻撃者が1つのシステムから収集したパスワードを使用して別のシステムでアカウントをクラックする場合でも、パスワードの推測可能性に使用する最適なメトリックを算出しました[289]。  
3。  
4。  
 パスワードチェッカーは、数字と文字を含むより長いパスワードを使用するように彼らを訓練し、それらを使用しないWebサイトに波及します[444]。  
 実際、調査によると、パスワードルールの適用はリスクのある価値の関数ではなく、Webサイトが独占的であるかどうかです。  
企業環境や軍事環境では、パスワード選択ルールやパスワード変更ルールを適用したり、ランダムなパスワードを発行したりできます。  
 したがって、パスワードは保護するデータと同じように扱われると主張できます。銀行のマスターパスワードは一夜にして金庫に保管されますが、軍の「トップシークレット」パスワードは封筒、金庫、占有されていないときにロックされている部屋に封をする必要があります。警備員がパトロールした建物の中。  
 ただし、優秀な人材を採用して維持したい場合は、もう少し慎重に考えてください。  
 国内の同等品は、wifiルーターの背面にあるカードとパスワードです。  
e。  
 私が見つけた最も近いものは、さまざまなタイプのパスワードの想起率、忘却率、および推測率の調査でした[345]。これは、ユーザーにさまざまな種類のアドバイスを与えることの実際の影響を私たちに教えませんでした。  
4。  
 したがって、「12時で空腹です」は「I'S12＆IAH」になります•黄色のグループは、与えられたテーブルから8文字（アルファベットまたは数字）のランダムを選択し、書き留めて、1週間後にこのメモを破棄するように指示されました彼らがパスワードを覚えていたら1つか2つ。  
 しかし、それは私たちが見つけたものではありません。  
したがって、パスフレーズとランダムなパスワードはほぼ同等に効果的であるように思われました。  
 パスワードを覚えるのが難しい（または書き留めた）かどうかを生徒に尋ねたところ、黄色のグループは他の2つのパスワードよりもかなり多くの問題を抱えていました。しかし、赤と緑の間に大きな違いはありませんでした。  
•指示に従うユーザーの場合、ニーモニックフレーズに基づくパスワードは、両方の世界で最も優れています。  
•次に、問題はユーザーコンプライアンスの1つになります。  
したがって、軍が兵士にランダムに選択したパスワードを与える場合、その価値は、パスワードがランダムであるという事実からではなく、パスワードの割り当てがユーザーのコンプライアンスを強制するという事実からもたらされます（ニーモニックフレーズも同様です）。  
サービスを一般に公開する場合、顧客は競合他社と同じインターフェースを広く提示することを期待しています。  
 （GCHQは、オンラインパスワードダンプで最も一般的に見られる100,000個のパスワードの「不正なパスワードリスト」を使用することを推奨しています。  
 カード所有者の半数以上がランダムなPINを保持していますが、約4分の1は、ランダムなPINよりもエントロピーが低く、異なるカードで同じPINを持つ子供の誕生日などのPINを選択します。  
1234などの一般的な選択を禁止する銀行は、オッズを18分の1に増やすことができます[295]。  
4。  
4。  
3設計エラーパスワードを覚えやすいものにしようとすると、重大な設計エラーが頻繁に発生します。  
 驚くほど多くの銀行、政府機関、その他の組織が依然としてこの方法で顧客を認証していますが、今日ではパスワードではなく、パスワードを回復するための質問になりがちです。そして、銀行に電話をかけて、母親の旧姓をYngstromからyGt5r4ad（またはスミスさえ）に変更することを決定したと伝えたら、幸運を祈ります。  
一部の組織では、コンテキストセキュリティ情報を使用しています。  
 理論的には、これは役立つ可能性があります。誰かが電話でトランザクションを行っているのを耳にした場合、それは長期的な妥協ではありません。  
 このシステムが最初に導入されたとき、小切手を書いたばかりのサプライヤが私になりすましているかどうか疑問に思い、最後の3つの小切手の値を尋ねるほうが安全だと結論付けました。  
 年次監査の会計士に小切手帳を渡したので、銀行と話すことができませんでした。  
現在、パスワードを要求するアプリケーションの数は、人間の記憶力を超えています。  
5つのパスワード。それぞれが3で共有されます。  
 Bonneauは、2012年にさらに詳細な統計を公開しました[289]が、それ以降、スマートフォンのおかげで、ユーザーパスワードの入力頻度は低下しています。  
4。  
 しかし、多くの人々は多くの異なる目的で同じパスワードを使用しており、銀行、ソーシャルメディアアカウント、電子メールなどの高価値のログオンに対処するための特別なプロセスを考えていません。  
 （http：// haveibeenpwned。  
）最も一般的で永続的なエラーの1つは、ユーザーにパスワードの定期的な変更を強いることです。  
 ただし、2003年、NISTのBillBurrは定期的な更新を推奨するパスワードガイドラインを書きました[1096]。  
4。  
 一方、セキュリティユーザビリティリサーチャーは、毎月の変化が最適ではないことを示した調査の後に調査を行いました。  
 最終的に調査は、ユーザビリティの第一人者であるロリー・クラノールがFTCの主任技術者である間に[492]、執筆し、学術研究によって裏付けられました[1505]。  
 イギリスのGCHQfollowedやMicrosoftなどの他の政府機関は、2019年4月からWindows 10でのパスワード有効期限ポリシーの終了を最終的に発表しました。  
2020年の現在の方法は、3つ以上のランダムな辞書単語のパスフレーズを選択するようにユーザーを招待することです。  
 しかし、経験的調査によると、実際のユーザーは実際に辞書からランダムに選択した場合よりもはるかに少ないエントロピーで複数の単語のパスフレーズを選択します。彼らは一般的な名詞のバイグラムを探し、3つまたは4つの単語にすばやく移動する傾向があります収益の減少[296]。  
3。  
4。  
 これは、1980年の初期のダイヤルアクセスシステムがいたずらな学童から注目を集めて以来、慢性的な問題でした。  
 モノのインターネットでは、このようなデバイスがますます増えています。彼らはその運用生活に対して脆弱なままです。  
わかりやすいパスワードは、付箋や電子的に同等のものであるかどうかに関係なく、別の長期的な問題です。  
 彼らは後で電話をかけたところ、ウェルカムスクリーンにメンテナンスパスワードが表示されていました。  
 感銘を受けなかったため、監査委員会の議長に新しい監査人を任命するように頼み、最終的にはそれが起こりました。  
4。  
 この凶悪な犯罪は、検察が裁判所に若者を有罪とするよう説得することに失敗したとき、イギリスの議会がその最初のコンピューター誤用行為を可決したことを確立に衝撃を与えました。  
 ウェブサイトで設定することを余儀なくされているパスワードのほとんどは、マーケティング上の理由からです。メールアドレスを取得したり、「クラブ」に所属しているような感覚を与えたりするためです[294]。  
4つ目は、悪質なパスワード管理システムです。パスワードをまったく暗号化しないものもあり、企業のハッカーがバックドアをパスワード管理ライブラリに持ち込んだという報告がときどきあります[427]。  
3。  
4。  
 たとえば、NSAには色の異なる内線電話と外線電話があり、部屋の外付け電話がオフフックの場合、分類された資料は部屋で話し合うことすらできず、電話では話せません。  
フィッシングは蔓延しているため、メールのリンクをクリックして銀行にログオンするのは賢明ではないため、常にブラウザのブックマークを使用するか、URLを手動で入力する必要があります。  
 実際、マーケティング業界の多くは、人々がリンクをクリックできるようにすることに専念しています。  
 銀行の顧客は、悪事を行うようによく訓練されています。  
 Bank of Americaからのスパムにより、英国の顧客はmynew-cardに誘導されました。  
アメリカ銀行。  
ドメインを無視し、証明書の警告を無視し、リンクを陽気にクリックする[582]ことにより、顧客を訓練して安全でないコンピューティングを実践する大手銀行の例は他にもたくさんあります。電話でセキュリティ情報を身元不明発信者に提供することは賢明ではありません。それでも、セキュリティ情報を要求する銀行のスタッフから電話がかかってきます。  
4。  
 （運転中に銀行のセキュリティチームが電話をかけたため、カードがブロックされました。ハンズフリーモード以外で通話に対処することは法律に違反し、安全な場所はありませんでした。  
 どうしたの？お察しの通り、オーストラリアの顧客に「セキュリティアップグレードの一環として」ウェブサイトにログオンし、カード番号とATMPIN [1087]を使用して認証するよう依頼するメールを送信しました。  
 その後、学生はISPに連絡して不正行為を報告し、URLとサービスが本物であることがわかりました[1241]。  
3。  
4。  
 これは、一部はリスクの軽減ですが、一部はリスクのダンピングです。指示を理解していない、または指示に従えない顧客は、結果として生じる損失の責任を負う可能性があることに気づきます。  
当初、アドバイスは「英語をチェックする」でしたので、悪意のある人は英語を書くことができる誰かを騙したか、単に銀行の所有する電子メールを使い始めましたが、URLは変更されました。  
 一部の銀行は、顧客の口座番号の下4桁を電子メールに入れ始めました。フィッシャーマンは最初の4つを入力することで対応しました（これらは特定の銀行およびカード製品で一定です）。  
 アドバイスは、リンクの上にマウスを置いて、リンクが実際にどこに行くかを確認することでした。次に、悪意のあるユーザーは、印刷されない文字をURLに挿入してInternet Explorerが残りを表示しないようにするか、（多くの銀行もそうであるように）管理できないほど長いURLを使用しました。  
 国の対策は非常に複雑で直観に反するようになり、ますます多くのユーザーを混乱させます–まさにフィッシング担当者が必要としているものです。  
セキュリティエンジニアリング110ロスアンダーソン3。  
 パスワード3。  
4。  
 最新のブラウザーは、内部でさまざまなメカニズムを使用して、邪魔なURLに警告します。  
次に、期限切れの証明書やその他のコンプライアンスエラーを探すためのロジックがあります（これらのアラートの大部分は誤警報であるため）。  
 私たちはそれらの多くを見ており、そのほとんどは無関係であり、多くは誰かにリスクを私たちに移すように設計されています。  
 それはあなたを詐欺するためにあなたの銀行口座とクレジットカードの詳細を盗むように設計されたマルウェアであなたのコンピュータを感染させようとするでしょう[1327]。  
 これらの要素を最適化すると、コンプライアンスが約35％から約50％に向上します[675]。  
ファイアウォールでそれらをブロックするか、ブラウザでブロックする必要があります（ChromeとFirefoxの両方で、異なるタイプの証明書エラーが発生するため、21でこの問題について説明します。  
1）。  
4。  
 いくつかは、いくつかのより広範なシステムの問題とともに、パスワードの入力と保存を行うための技術的なメカニズムを伴います。  
 セキュリティエンジニアは、（ATM PINのように）推測が制限されている場合はパスワードシステムを「オンライン」と呼び、そうでない場合は「オフライン」と呼びます（元々は、ユーザーがパスワードファイルを取得して推測を試みることができるシステムを意味していました）。特権ユーザーを含む他のユーザーのパスワード）。  
 一部のオンラインシステムではできない物理的な改ざん防止を使用して3つのPIN推測に制限する支払いカードなど、一部のオフラインシステムは推測を制限できます。  
 ここで最も一般的なトラップは、通常はパスワードの推測を制限するシステムですが、ハッキングされて一方向の暗号化されたパスワードファイルが暗号化キーと一緒にリークされると、突然それが失敗します。  
パスワードの推測可能性は、最終的には選択したパスのエントロピーに依存します。セキュリティエンジニアリング111ロスアンダーソン3。  
 PASSWORDSwordsと許可される推測の数ですが、これは特定の脅威モデルのコンテキストで機能するため、防御しようとしている攻撃のタイプを考慮する必要があります。  
1つのアカウントに対する標的型攻撃：侵入者は特定のユーザーのパスワードを推測しようとします。  
特定のターゲットに属するアカウントへの侵入を試みます。敵は、所有しているアカウントをどこでもハッキングし、他のアカウントを乗っ取ったり、直接害を及ぼす可能性のある情報を入手しようとします。  
 これは、標的となる銀行の口座をハッキングして、お金を不正利用できるようにすることを狙った典型的な事件です。例としては、侵害されたアカウントからスパムを送信できるようにオンライン電子メールサービスのパスワードを推測しようとする悪者や、標的となる企業のドメイン内の任意のランダムなマシンへのログオンを望んでいる標的型攻撃者があります。  
サービス拒否攻撃：攻撃者は、1人以上の正当なユーザーがシステムを使用するのをブロックしたい場合があります。  
この分類法は、パスワードシステムを評価するときに関連する質問をするのに役立ちます。  
4。  
 銀行は、3つの間違ったPINの後でカードを凍結することがあります。しかし、不正なパスワードを3回入力した後でオンラインアカウントが凍結されると、サービス拒否攻撃を受ける可能性があります。  
 現在、多くの商用Webサイトでは、ロックアウトではなくスロットルを使用しています。  
 この場合、保護的な監視が推奨されるオプションとなる可能性があり、危機的状況にある場合はレート制限を放棄する計画があります。  
 彼らは、人気のある成長している有能なサイトは、支払いサイトと同様に、より安全である傾向があることを発見しましたが、Security Engineering112Ross Anderson3。  
 PASSWORDSコンテンツサイトは最悪です。  
3。  
7自分自身または他者を保護しますか？次に、システムはユーザーとサブシステムを互いにどの程度保護する必要がありますか？携帯電話システムや現金自動支払機システムなど、誰でもアカウントを取得できるグローバルシステムでは、攻撃者が既に正当なユーザーであると想定し、だれかが他人の費用でサービスを利用できないようにする必要があります。  
 これには、個人的な側面とシステム的な側面の両方があります。  
5。  
システム側では、サブシステム間の相互認証に使用されるあらゆる種類のパスワード、サーバー/サーバー環境でパスワード品質を実施するためのメカニズムがほとんどないこと、および多くの既知の問題（たとえば、Javaの信頼できるキーストアファイルのデフォルトパスワードは'それを変更'）。  
4。  
4。  
 しかし、これには実際のお金がかかり、お金だけが問題ではありません。  
 その結果、サーバーのパスワードはスクリプトやその他のプレーンテキストファイルに表示されることが多く、最終的にDropboxやSplunkに保存される可能性があります。  
 後の章では、Kerberosやsshなどのプロトコルについて見ていきます。とりあえず、典型的な大企業をハックするのは簡単だったというエドスノーデンの発言を思い出してください。システム管理者をスピアフィッシングして、あなたの道に鎖でつないでください。  
3。  
パスワード入力の攻撃パスワード入力の保護は不十分であることがよくあります。  
4。  
4。  
1インターフェース設計思慮のないインターフェース設計はあまりにも一般的です。  
 キーボードは、設計した男性には適度な高さであったかもしれませんが、数インチ短い女性が露出しています。  
 特にスーパーマーケットのキューにいて、友人が近くに立っている場合、PINは不信感の信号であるため、多くの人がPINを不快にシールドしています。  
3。  
8。  
 偽のターミナル攻撃は、時分割コンピューティングの黎明期にまでさかのぼります。  
疑いを持たないユーザーがこれを行った場合、パスワードを保存し、「申し訳ありませんが、間違ったパスワード」と返信してから消え、正規のパスワードプログラムを呼び出します。  
 これが、Windowsに安全なアテンションシーケンスがあった理由です。 ctrl-alt-delを押すと、本物のパスワードプロンプトが表示されます。  
ATMスキマーは、ATMの喉に座ってカードの詳細をコピーし、顧客のPINを記録するカメラを備えたデバイスです。  
 詐欺師は不正なPIN入力デバイスも配備し、銀行の支店の端末にパスワードを盗むハードウェアを取り付けたとしても投獄されています。  
 いずれの場合でも、端末に悪意のあるハードウェアまたはソフトウェアが含まれている可能性がある場合、パスワードだけでは十分ではありません。  
4。  
3パスワード再試行カウンターの技術的な敗北多くの子供たちは、自転車のコンビネーションロックは通常、緩い順に各リングを解くことで数分で壊れることがあることに気付きます。  
 PDP-10 TENEXオペレーティングシステムは、一度に1文字ずつパスワードをチェックし、そのうちの1つが間違っているとすぐに停止しました。  
 AnSecurity Engineering114Ross Anderson3。  
 最初の文字のPASSWORDSerrorはほぼ一度に報告され、2番目の文字のエラーは報告するのに少し時間がかかり、3番目の文字のエラーは少し長くなる、というようになります。  
 （30年後には、現在構築しているシステムに残っている可能性があるのは、よりニュース価値の高いセキュリティ障害の記憶であることに注意してください。  
1台のリモートカーロックデバイスでは、キーフォブから誤ったバイトが送信されるとすぐに、レシーバーの赤い表示ライトが点灯しました。その理由は、間違ったPINによってPIN再試行カウンターが減少し、このカウンターを保持するEEPROMメモリに書き込むと数ミリアンペアの電流サージが発生したためです。これは、書き込みが完了する前にカードをリセットするのに間に合うように検出できました[1105]。  
 次の章で詳しく説明するように、タイミングチャネルは暗号化を実装する人々にとって深刻な問題です。  
 MycolleagueのSergei Skorobogatov氏は、iPhoneは機密データをフラッシュメモリに暗号化して保持し、暗号化されたメモリの内容を保存し、PINを数回試みた後でそれらを元の状態に復元できるアダプターを構築したと述べています。  
3。  
9パスワード保存の攻撃パスワードは、保存されている場所で脆弱であることがよくあります。  
 ソフトウェアのバグのため、2つのエディタ一時ファイルが入れ替わり、ログオンした全員にパスワードファイルのコピーが表示されました。 [476]。  
PINの処理手順では、銀行の誰も自分のPIN以外のPINにアクセスできなかったため、何千もの顧客カードが出荷されるまで、バグは発見されませんでした。  
5これは、当時のFBIディレクターであるJames ComeyがiPhoneはハッキングできないため、バックドアを作成したオペレーティングシステムのアップグレードを作成するようにAppleに命令する必要があるという主張を弱体化させるために行われました。セクション26を参照してください。  
8。  
4。  
 システムが失敗したパスワードを試行時にログに記録する場合、ユーザーは「ユーザー名、パスワード」シーケンスのフェーズを取得するため、ログには通常、多数のパスワードが含まれます。  
3。  
9。  
パスワードは、入力されると一方向の関数を介して渡され、ユーザーは以前に保存された値と一致する場合にのみログオンします。  
 これを行う正しい方法は、歴史的にこのコンテキストでソルトとして知られているランダムキーを生成することです。低速で暗号学的に強力な一方向関数を使用して、パスワードとソルトを組み合わせます。塩とハッシュの両方を保存します。  
4。  
2パスワードクラッキング暗号化されたパスワードファイルを使用する一部のシステムは、広く読み取り可能にします。  
 したがって、ユーザーはそれをフェッチして、辞書内のすべてのパスワードを暗号化し、それらをファイル内の暗号化された値と比較することにより、パスワードを解読しようとする可能性があります。  
4。  
1この目的のために人々が長年使用してきた「クラック」ソフトウェア。  
 ただし、たとえば、忘れたパスワードを使用してOceドキュメントを暗号化した場合に役立つパスワード回復ツールはまだあります[1674]。  
資格証明の方法もあります。システムがハッキングされてパスワードが解読されると（または暗号化されていないことが判明した場合）、それらは他のシステムで試され、再利用された多くの人々を捕まえます。  
そのため、パスワードのクラックには、まだ注意が必要です。  
 ハニーポットシステムを使用して、誰かがログオンした場合、システムのハニーポットアカウント、またはパスワードカナリア–正規のアカウントの偽の暗号化されたパスワード[996]を警告することができます。  
4。  
3リモートパスワードチェック多くのシステムは、暗号化プロトコルを使用してリモートでパスワードをチェックし、転送中のパスワードを保護します。パスワードセキュリティとネットワークセキュリティの相互作用は複雑になる場合があります。  
4。  
 これについては、次の章のセクション4で説明します。  
4;暗号化されたトラフィックを盗聴できる相手から弱いパスワードを常に保護するわけではありません。  
7。  
 サーバーがハッキングされた場合、TLSはユーザーを保護しません。  
 これについても後で説明します。  
 2006年からTwitterによって開発され、現在では、Google、Microsoft、Facebookなどのメインサービスプロバイダーによって、メディアやその他のサイトにログオンできるようになっています。認可サーバーは、目的のためにアクセストークンを発行します。  
 付随するリスクはクロスサイト攻撃です。現在（2019年）、OAuthが作家とイタリアの国の国家主体によって、地元の人権擁護家をフィッシングするために使用されているのを見ています。  
 ターゲットが応答した場合、最終的にMicrosoftのWebページが表示され、データへのアクセスをアプリに許可するよう求められます[46]。  
4。  
 軍のシステム管理者は、ランダムなパスワードを発行することを好むため、パスワードを推測する攻撃の確率を管理できます。  
このような「証明可能なセキュリティ」の原則には、攻撃者の目標から始まる問題があります。  
 これを止めたい場合は、すべてのアカウントだけでなく、すべてのアカウントに対してレート制御を行う必要があります。CVCNCVCNなどの子音、母音、数字を覚えやすいように設計された固定テンプレートを使用してランダムに選択されたパスワードを発行するために使用されていた英国政府システム（e。  
 fuR5xEb8）。  
52。  
 したがって、攻撃者が1秒間に100個のパスワードを推測できるとしたら、おそらくセキュリティエンジニアリング117ロスアンダーソン3でしょう。  
 パスワードは、ネットワーク上の何百ものマシンの10,000アカウントに分散されており、アラームを鳴らさないようにしています。アクセスするには約500万秒、つまり2か月必要です。  
 失敗したログオンの試行をカウントして分析することもできます：ボットネットを使用した攻撃者、または他の侵入の試みを示唆する一連の推測はありますか？また、気づいたら何をしますか？システムを終了しますか？サービス拒否の世界へようこそ。  
これは、1億のアカウントを持つWebサービスでは大したことではないかもしれませんが、それでも、産業規模のパスワード推測攻撃のソースを特定することは試みる価値があります。  
4。  
 自動推測攻撃が続く場合は、CAPTCHAを使用して対処します。これはセクション3で説明します。  
3。  
11パスワードマネージャーの使用1980年代以降、企業は複数のアプリケーションのパスワードを記憶するシングルサインオンシステムを販売してきました。1990年代半ばにブラウザーが登場し、人々が数十のウェブサイトにログインし始めると、パスワードマネージャーはマスマーケットになりました。製品。  
ランダムなパスワードを選択し、ブラウザにそれらを記憶させることは、実用的な操作方法になる可能性があります。  
 ブラウザーでは、マスターパスワードを設定できます。マスターパスワードは、個々のサイトのすべてのパスワードを暗号化し、ブラウザーの更新時にのみ入力する必要があります。  
 これは、ブラウザを使用する場合の特定の問題であり、もう1つは、マスターパスワードが常にデフォルトであるとは限らないため、多くのユーザーが設定しないことです。  
）ブラウザを使用する利点は、電話のブラウザとラップトップのブラウザの間でパスワードを同期できる場合があることです。  
（ブラウザを使用すると、これはラップトップまたは電話全体をバックアップすることになります。  
 欠点は、多くの製品が本当に恐ろしいことです。いくつかのハードウェアパスワードマネージャーがすべての秘密を平文で保存し[130]、上位5つのソフトウェア製品は、オートコンプリートからサブドメインを無視することまで、深刻かつ体系的な脆弱性があります[389] ]。  
4。  
 Banksthinkを使用するとセキュリティが向上しますが、確信はありません。  
 銀行は、オートコンプリートを殺すと、次のデバイスの盗難が難しくなると主張し、マルウェアがブラウザーまたはパスワードマネージャーのデータベースからパスワードを盗むのを阻止するかもしれませんが、その製品によって提供されるフィッシング防御は無効になり、平均的な顧客に大きなリスクをもたらす可能性があります[1355] 。  
 人々はあらゆる方法でリスクを管理します。  
 しかし、ほとんどの人はそれほど慎重ではありません。  
ノートパソコンが故障するとどうなりますか？あなたの電話が死んだとき？誰かがあなたの電話会社をあなたの電話番号を彼らのSIMにリンクするように説得したとき？あなたが死んだとき、またはあなたが病気になり、パートナーがあなたの状態を管理する必要があるとき？彼らはマスターパスワードをどこで見つけるか知っていますか？本（およびあなたのエグゼキューター）が覚えなければならないすべてが169ページ、大きな期待であるならば、それらを本に書き留めることは意味があります。  
 これをすべて正しく行う人はほとんどいません。  
4。  
 キーボードを持たないIoTデバイスの急増により、何らかの目的でキーボードを使わなくて済むようになります。  
 一例は、アプリを介して排他的に動作するオンライン銀行Monzoです。  
 ただし、アップグレードや新しい電話を購入する人の認証にトップトロントの電子メールを使用しているため、アカウントの乗っ取りには電話の乗っ取り、またはパスワードの推測やパスワード再設定用の質問が含まれます。  
 これがもっと普及することを期待しています。そのため、SIMスワップからAndroidマルウェア、SS7、RCSハッキング、単純な物理的な盗難に至るまで、電話の乗っ取りに基づく攻撃が増えます。  
 したがって、物事は見かけよりも変化が少ない場合があります。  
 認証システムを評価できる基準は数多くあります。ここでは、盗難、物理的な観察、推測、マルウェアやその他の内部的な侵害、他の検証者からの漏えい、フィッシング、標的型のなりすましに対する耐性を強化しました。4。  
 彼らは、純利益に関連するスキームのほとんどがシングルサインオンのバリアントであると結論付けました。OpenIDは確かに広く普及しており、明らかなプライバシーコストにもかかわらず、多くの人々がGoogleまたはFacebookを使用して新聞にログインしています。  
Bonneauの調査では、CAPリーダーなどの物理認証トークンに高いセキュリティ評価が与えられました。これにより、人々は銀行カードを使用してオンラインバンキングにログオンできます。銀行規制当局はすでに多くの国で二要素認証を義務付けています。  
 GoogleやMicrosoftなどの州レベルの攻撃者の標的である企業は、現在、あらゆる種類の認証トークンをすべての状態に提供しています。  
 3番目のオプションであるバイオメトリクスは、ハイエンド携帯電話が指紋リーダーを提供し始めて以来、広く使用され始めています。  
 バイオメトリクスについては、本の後半の独自の章で説明します。  
 したがって、パスワードは、多くの情報セキュリティが構築されている（不安定な）基盤のままです。  
 ますます一般的になっている1つのアプローチは、最初の使用時の信頼です。これは、孵化した後、最初に動く動物にアヒルの子が結合するという事実から、「復活したアヒルの子」としても知られています。  
最後に、データ保護法に基づいて個人情報のコピーを要求する権利を行使する顧客または他の人々を認証する方法について、一生懸命に考える必要があります。  
 86の企業は、政府が公共サービス用のシングルサインオンを設定するための情報を持っていることを認めたが、2020年に閉鎖された英国の「検証」プログラムにより、成功率は低下した[1392]。  
 また、既存の企業が享受しているネットワークの影響により、他の民間企業が競争することも困難でした。  
 したがって、privacyono↵erの品質と性質は、他の動機のために戦う戦いの副次的影響になっています。  
7これは、Monzoのような支店のない銀行では機能しません。しかし、彼らはあなたが登録したときにあなたのビデオを撮って、後でコールセンターがあなたを認識できるようにします。  
5。  
しかし、約4分の1が認証としてメールアドレスまたは電話番号を受け入れる準備ができていました。さらに16％が簡単に偽造可能なIDを尋ねました。  
 彼女がこれまで操作したことのない脅威インテリジェンス企業から、侵害されたアカウントとパスワードのリストが送信されました。  
 あなたがパスワードを廃止し、かつての顧客が彼らの電話が盗まれたと主張した場合、あなたは何をしますか？また、顧客になったことがない人の個人データを保持している場合、どのようにしてそれらを特定しますか？3。  
 これらは、ブログに投稿したり、無料のオンラインアカウントに登録したり、パスワードを回復したりするために解決しなければならないことが多い小さなビジュアルパズルです。  
CAPTCHAは、2003年にスパマーがスクリプトを使用して無料の電子メールサービスで数千のアカウントを開くのを防ぎ、攻撃者が多数の既存のアカウントのそれぞれでいくつかの単純なパスワードを試行することを困難にするために、2003年に大きな方法で最初に使用されました。  
 テストは、コンピュータが人間と機械の違いを判別できるように、方向転換されます。  
 CAPTCHAを壊すことはAIの問題を解決することと同等であり、攻撃者は実際に手作業で行わなければならない、またはコンピュータサイエンスの真の革新を考え出す必要があるという考えです。  
 見た目よりも難しいことがわかりました。  
初期のシステムによってもたらされた画像認識の問題の多くは、賢い人々が一生懸命それらを解決しようとしても、それほど難しくないことが判明しました。  
 この間もなく、スパマーは、CAPTCHAを次々に解いて女性の服を脱ぐゲームを作成しました[191]。  
 さらに数人の内で、人間の視覚システムに触発された信号処理技術を使用した一般的な攻撃は、少なくともサブセットを解決するのにかなり効率的でしたSecurity Engineering121Ross Anderson3。  
 ほとんどの種類のテキストCAPTCHAの要約[746]。  
2014年から、CAPTCHAはルイスフォンアンの発明のもう1つであるReCAPTCHAに取って代わられました。  
 このサービスは当初、OCRソフトウェアを混乱させたGoogleの本のテキストの一部を文字起こしするように人々に求めていました。最近では、「店頭を含むすべての画像をクリックしてください」と尋ねる8枚の絵のパズルが表示されます。これは、Googleがそのビジョン認識AIシステムをトレーニングするのに役立ちます8。  
CAPTCHAの実装は、多くの場合、軽率なものであり、視覚障害のあるユーザーにとってはアクセシビリティの問題があります。6要約心理学は、欺瞞のため、そして使いやすさのために、セキュリティエンジニアにとって重要です。  
 さまざまな種類のフィッシングが主要な国家安全保障上の脅威であり、サイバー犯罪インフラストラクチャを開発および維持するための主要な手段であり、オンラインバンキングシステムに対する主要な脅威の1つです。  
救済策の一部はセキュリティの使いやすさですが、この分野の研究は長い間見過ごされてきましたが、暗号やオペレーティングシステムほど魅力的ではないと見なされています。  
 2010年代半ば以降、私たちは一般のプログラマーにとっても物事を容易にする必要があることにも気づき始めました。実際のシステムが壊れたセキュリティバグの多くは、安全でないデフォルトを使用する暗号化APIからCプログラミング言語に至るまで、使用するのが難しすぎるツールの結果です。  
この章では、詐欺や人々が犯す種類のエラーに関連する心理学の研究を通してホイッスルストップツアーを行い、ケーススタディとして認証に取り組みました。  
 We8 ReCAPTCHAが「ヘリコプターを含むすべての画像をクリックしてください」と言っていて、軍事AIの研究に協力したくないというユーザーからの反発がありました。  
 しかし、他のユーザーはまだ無料でGoogleで働くことに反対しています。  
セキュリティエンジニアリング122ロスアンダーソン3。  
 要約推測可能性、記憶可能性、ユーザーのトレーニング可能性など、ラボで測定できるものだけでなく、実際のシステムがどのように破壊されるか、実際の攻撃の規模、インセンティブなどの分野でのみ観察できる要因に関するデータも増えています異なるプレイヤーに直面すると、安全でない均衡につながります。  
 「私たちは皆同意する」と彼は言った、「人々はテロリズムにあまりにも多くの注意を払い、サイバー犯罪には十分ではない。  
 空港で人々をもっとリラックスさせたい場合は、タンクと銃を取り除き、スピーカーにnicesofasとモーツァルトを入れれば、人々はすぐにリラックスできます。  
 しかし、コンピューター業界がコンピューターを以前よりもはるかに恐ろしく見えないようにするために、コンピューター業界がその道を行くので、それは起こりません。  
 ですから私たちは人々に間違った合図を出し、私たちのお金を間違ったものに費やします。  
研究の問題セキュリティ心理学は2020年のホットなトピックの1つです。  
セキュリティのユーザビリティも規律となっており、毎年有効なプライバシーとセキュリティに関するシンポジウムが開催されています。私たちはワークショップを開催して、人類学者、心理学者、哲学者など、リスクに取り組み、人々がどのように対処するかについてセキュリティエンジニアを集めています。  
 最初の例は安全なユーザビリティです。車から医療機器までの安全性が重要な製品は、ソフトウェアやインターネット接続だけでなく、複雑なインターフェースや独自のアプリさえも取得するので、偶然に人々に害を及ぼさないように設計するにはどうすればよいでしょうか。または悪意の結果として？2番目の例、およびセキュリティと人間の行動に関するワークショップのテーマは、人類学および心理学から社会学、歴史および哲学に至るまで、人々がリスクに対処する方法を研究する学問から学べるものです。  
 パンデミックは、建築家と協力する必要があるかもしれないことを示唆しています。  
 コードをハッキングするだけでなく、設計する必要があります。  
6。  
 一方、ソーシャルエンジニアリングに関する最も優れた本は、ケビンミトニックの「The Art of Deception」[1325]です。  
社会心理学がマーケティングでどのように使用され、悪用されるかについて、必読の本はTim Wuの「注目の商人」で、広告の歴史を物語っています[2050]。  
 次に、[1544]などの標準のHCIテキストがあり、セキュリティの使いやすさに関する初期の論文は[493]と表示され、フィッシングについては[976]と表示されました。  
 自律走行車に関する同様の調査によると、人格が与えられた場合、人々はそのような乗り物をより信頼し、乗客はルートを選択したり、単に停止するように命令したりするなどの戦略的制御を与えられます。  
 より技術的な詳細については、その直前にダニーエディットがトムギロビッチとデイルグリン[769]と共に執筆した大量の論文、または彼が後に書いたポップサイエンスの本「思考、高速、低速」[1005]があります。  
 政府や他の場所でのこの理論の適用については、標準的なリファレンスはディックターラーとキャスサンスタインの「ナッジ」[1876]です。パスワードと関連メカニズムの詳細な履歴、および多くの経験的結果と、推測可能性と再現率の両方を測定するための統計的手法の分析については、ジョーボンノーの論文[289]を強くお勧めします。  
拷問者の聖書として知られ、囚人を尋問し、洗脳するときの感覚遮断、薬物、催眠、社会的圧力などの相対的な効果を説明しています。  
セキュリティエンジニアリング124ロスアンダーソン