企業は数百万ドルを技術保護に費やすことができ、誰かが基本的に電話で誰かに電話をかけ、コンピューターの防御力を低下させるか、求めていた情報を明らかにするためにコンピューターで何かをするように説得できれば、それは無駄になります。  
–クリストファーワイリー電話、それらがサポートするアプリエコシステム、およびそれらが依存する通信ネットワークの保護は、現代世界の中心です。  
 アプリへの象徴として、ビジネスセクター全体が革命を起こしています。の5。  
 第二に、スマートスピーカーから車まで、新世代の接続デバイスは電話によく似ており、多くの場合、同じプラットフォームを使用し、同じ脆弱性を共有しています。  
第4に、モバイルネットワークは他のインフラストラクチャにとって重要です。電力会社は障害を修復するときにエンジニアに指示するために携帯電話に依存しているため、電力供給の数時間後に電話システムがダウンすると、問題が発生します。  
 スマートフォンは、銀行などのサービスへのアクセスを許可することにより、第三世界の貧困層の生活に革命をもたらしましたが、監視と制御も容易にします。  
 通信セキュリティの歴史66822。  
 電話網への攻撃  
各段階で実施された防御策は、さまざまな理由で不十分な傾向がありました。  
 現在、急速に成長している電話ベースの不正取引銀行システム、人々の個人情報を盗む悪質なアプリ、および5Gインフラストラクチャの国家安全保障への影響に関する高い政策論争が見られます。  
1。  
2。  
電話セキュリティは、これらの最初のものがすべてでしたが、今ではほとんどが2番目です。  
1電話ネットワークの攻撃通信の乱用は何世紀も前にさかのぼります。  
迷惑メールは、特に有名な人々にとって大きな問題になりました。そのため、受信者は、手紙を支払う代わりに、手紙を調べて拒否することができました。  
 これを阻止するために規制が導入されましたが、実際には効果的ではありませんでした[1460]。  
初期の光学テレグラフは、セマフォまたはヘリオグラフを使用して機能していました。人々はオペレーターに賄賂を贈ったり、望遠鏡で最後のヘリオグラフステーションを観察して「ローカルループをハッキング」したりして、地元のブックメーカーが勝つ前にどの馬が勝ったかを調べます。  
 電気電信がコストを下げたとき、問題はさらに悪化しました。コミュニケーションの量が増加し、サービスに組み込まれ、サービスに加えられた柔軟性が高まったため、複雑さが増し、乱用が増えました。  
セキュリティエンジニアリング669ロスアンダーソン22。  
 電話網への攻撃22。  
1通話メーターの攻撃初期の通話メーターシステムは、創造的な虐待にさらされていました。  
•最初は、オペレーターはどの電話からの電話かを知る方法がなかったため、電話番号を尋ねる必要がありました。  
 オペレーターが国際電話の番号を確認するために電話をかけ始めたため、人々はソーシャルエンジニアリング攻撃に取り組みました（「これはIBMです。ここではサンフランシスコへの電話を予約したいと考えています。時間差があるため、今夜、私たちのマネージングディレクターが自宅に持ち帰ることができます。 ？彼の番号はxxx-yyyyです）。  
 しかし、英国の実装にはバグがありました。公衆電話からオペレーターに電話をかけた顧客は、簡単にそれを押し下げることができました。すると、彼は（しばしば異なるオペレーターに）再接続され、今回は公衆電話からの呼び出しであるという警告はありませんでした。  
•初期のシステムは、1つまたは複数のパルスによるコインの進入も通知しました。それぞれのパルスは、ラインに抵抗を挿入した後、簡単な開回路が続いています。  
 （この場合の請求書は学生組合に送られましたが、魔法のボタンはそれほど面白くありませんでした。  
 1990年代に、ほとんどの国の公衆電話は公衆電話をコインからチップカードに移動し、コインの収集と破壊行為のコストを削減しましたが、私がセクション18で述べたとおりです。  
他の攻撃には、いわゆるクリップオンが含まれます。サービスを盗むために、電話を誰か他の人の回線に物理的に接続します。  
ノルウェーの電話会社は、ダイヤルトーンが与えられる前に、顧客宅内機器を交換機に認証させました[994]。  
 クラムリントンの家族が発見することになったため、これは時折側副的な被害を引き起こしました。  
 次は、迷惑電話の苦情があったと言った警察の訪問でした。1。  
 家族の法案が調査されたとき、公衆電話であることが判明した番号のクラスターへの呼び出しもありました。これらは、迷惑電話と同時に非常に突然始まりました。  
電話会社のメンテナンスエンジニアからの報告によると、家族の回線は配電キャビネットで改ざんされていたが、これは教義に反しており、会社は後に報告書に誤りがあると主張した。  
家族の代わりに無実の家族の電話回線を使用することで、彼は電話代を節約しただけでなく、警察の監視を回避する可能性が高まりました。  
 ノルウェーの電話会社は、弁護のクリップオンについて証言するための辞任を拒否した。  
コードレス電話から発信音を盗むことも、テーマの別のバリエーションでした。  
 ほとんどの機器は、フランスの会社Alcatelが特許を取得した暗号化を使用するDECTセキュリティメカニズムを使用するのではなく、ハンドセットのシリアル番号を基地局に単純に送信するようです。  
 DECT認証は、弱いブロック暗号に基づいています。 confiden-tialityは、弱いストリーム暗号（セクション5で後述するA5 / 1のやや複雑なバージョン）を使用します。  
1）通常は234e↵ortで破損する可能性があります。弱い乱数ジェネレータがあります。一方、プロトコル障害には中間者攻撃や、サイレントコールを行ってキーストリームを収集し、先に記録したコールを復号化するリプレイ攻撃などがあります。  
 Tewsの業績が公開されて以来、DECT標準は代わりにAESを使用することを推奨していますが、どちらのベンダーが不利になるかは明確ではありません。  
 クリップオン詐欺に関しては、SkypeやWhatsAppのようなサービスが長距離通話を安くして以来、それは大幅に姿を消しました。  
 詐欺師がAT＆Tのふりをしてあなたに電話をかけ、通話カードでペルーに大量の電話をかけたかどうかを尋ねます。  
 これで123-456-7890が電話番号、5678がパスワードとなり、詐欺師が通話料金を請求できるようになります。  
1。  
 実際、人々をだましてプレミアム番号に電話をかけるというビジネスにより、詐欺師はフィッシング攻撃で現在使用している技術を磨くことができました。  
 多くの人々が+1 809は「外国」でより高価であることを知っていますが、ケイマン諸島の+1 345などのカリブ海の市外局番の導入により、そのような詐欺を見つけるのはさらに困難になっています。  
 政府は通常、プレミアムレートのオペレーターを規制しようとするのを避けて、あまりに難しいと主張する弱い規制当局を設立します。そして時々それはすべて爆破します。  
 これらの多くは録音されているため、通話は無駄でした[1323]。  
 最大の詐欺行為がロシアの暴力団ではなく「信頼できる」企業によって実行されることもよくあることです。  
1。  
 1980年代まで、電話会社は、音声を伝送するのと同じ回路でトーンパルスを送信することにより帯域内で機能する信号システムを使用していました。  
 開拓者の1人であるジョーエングレシアは完璧なピッチを持っていて、長距離電話のバックグラウンドで聞いた口調で口笛を吹くことで無料で電話をかけることができる子供であることを発見しました。  
 トリックは、0800番号を呼び出し、遠端の回線をクリアダウンする2600Hzトーンを送信することでした。つまり、交換機に接続されたトランク回線を発信者に残しながら、着信者を切断します。  
 Phonephreakingは、ベイエリアに根付いたコンピューターハッカー文化のルーツの1つであり、パーソナルコンピューターの開発と進化において形成的でした[1222]。  
電話での不正行為は、強力なイデオロギー要素から始まりました。  
 インセキュリティエンジニアリング672ロスアンダーソン22。  
 電話ネットワークへの攻撃アメリカ、AT＆Tは非常に虐待的な独占であり、裁判所は最終的に破綻しました。ヨーロッパのほとんどの電話会社は政府機関でした。  
 あなたの娘を求愛した青年が（あなたには知られていない）彼にかけた電話の代金を支払っていなかった電話の乱暴だった場合、あなたは突然、会社が青年の名前または支払いのいずれかを強要しようとしていることに気付くでしょう。  
多くの国の電話の不法行為は、警察官やスパイが電話を盗聴するためにラインマンを派遣しなくても、自分のデスクの快適さから電話を盗聴できるようにする信号コードまたはスイッチ機能を発見しました。電話会社はカウンターカルチャーのヒーローであり、電話会社は闇の勢力と協力していた。  
 徐々に、地域ごとに、世界はブルーボックス攻撃から閉鎖されました。  
22。  
3スイッチングと構成の攻撃電話交換スイッチがプログラム可能になると、攻撃の第2の波がコンピュータを標的にしました。  
 あまり保護されていないこれらのマシンの1つをハッキングすることにより、フリークはLANを通過してスイッチング機器、またはサブスクライバーデータベースなどの他のセカンダリシステムに侵入する可能性があります。  
これらの手法を使用すると、リストにない電話番号が見つかり、加入者の知らないうちに電話が転送され、あらゆる種類のいたずらが可能になりました。  
彼は有名人のリストにない電話番号を取得したり、ロサンゼルスのラジオ局KIIS-FMからポルシェを獲得したりするなど、ささいなことをしました。  
 彼はまた、違法な盗聴とスパイ活動の容疑で告発された。これらの告発は却下された。  
FBIの機密性は、電話会社のコンピュータへの攻撃がリモートの盗聴を行うために外国の諜報機関によって使用されているという事実を強調しています。  
1。  
 自社の電話交換機を構築するのではなく、電話交換機を輸入している国は、電話交換機がサプライヤーの政府に知られている脆弱性を持っていると仮定しなければなりません。  
 USAFは最初だけを爆撃した。  
 これは、電話会社が追加の電話に対応するための限界コストがゼロの場合はそれほど問題ではありませんでしたが、1990年代に付加価値サービスが急増し、規制緩和により電話会社間の現金支払いが増加したため、深刻になりました[460]。  
部外者に関しては、Poulsen以外の「アーチハッカー」はKevin Mit-nickでした。彼は一連の侵入により逮捕され有罪判決を受け、FBI捜査の標的にもなりました。  
 第3章で述べたように、彼は刑務所からの釈放後、彼の悪用のほとんどすべてがソーシャルエンジニアリングに関係していることを証明しました。  
 議会の証言で、彼はこの章の冒頭の引用を思いついた。「企業は技術保護に何百万ドルも費やすことができ、誰かが基本的に電話で誰かに電話をかけ、コンピューターの防御を低下させるコンピューターで何かをするように彼らを説得することができる場合、それは無駄になります。または彼らが求めていた情報を明らかにする」。  
2020年まで早送りします。心配な開発の1つは、切り替えのエクスプロイトの増加です。  
スイッチファブリックへのアクセスにより、彼らは1980年代にポールセンとミトニックが達成したようなゲームをプレイできます。  
 次に、Googleでアカウントの復元を開始します。これにより、SMSを送信してパスワードをリセットします。  
4。  
7。  
 SS7はまた、サウジアラビアのMNOに悪用され、米国のサウジアラビアの反体制派を追跡している[1054]。  
 そのような合意がある場合、リモート電話会社によってSS7アクセスが与えられた企業は、SMSメッセージを取得するために電話を盗むか、プレミアム詐欺を行うことができます。  
 何千ものケースがある場合、銀行はオペレーターに行く意欲があるかもしれません。  
 つまり、セキュリティエンジニアリング674ロスアンダーソン22を含む攻撃だと私たちは考えていました。  
 電話網への攻撃SS7は国民国家の保護でしたが、もはやそうではありません。  
1。  
カスタマープレミスの留守番電話として実装されているか、現在では一般的なクラウドサービスとして実装されているかにかかわらず、ボイスメールの悪用は数多くあります。  
 最も悪名高い事件は、2002年3月21日のイギリス人女子高生ミリーダウラーの殺害でした。  
 結果として生じた怒りは、新聞の閉鎖、2014年にデビッドキャメロンの広報担当者である元世界ニュース編集者のアンディクルソンの投獄を含むいくつかの刑事上の有罪判決、および基準の報道に対する公的調査につながりました。  
 企業の構内交換機システム（PBX）への攻撃は、1990年代半ばまでに大規模ビジネスになり、ビジネスに数十億ドルの費用がかかりました[467]。  
 会社の営業担当者は0800番号に電話をかけ、PINまたはパスワードを入力してから、大企業が長距離電話で受けることができる低料金を利用して再度電話をかけることができます。  
結果はダイヤルスルー詐欺として知られています。  
 また、多くのPBX設計には、リモートメンテナンスアクセスを可能にする固定エンジニアリングパスワードがあり、賢明な人々は、どのPBXにも少なくとも1つのバックドアがあり、法執行機関や諜報機関に簡単にアクセスできると考えています（これは、輸出ライセンスの条件として言われています）。ある例では、スコットランドヤードのPBXが侵害され、犯罪者が電話をかけるために使用し、ヤードに100万ポンドの費用がかかり、そのために電話設置者を訴えました。  
 犯罪者の動機の1つは、盗聴されないコミュニケーションにアクセスすることです。  
悪名高い事件では、労働市場のラケット攻撃に関与している中国の暴力団–中国福建省から英国への不法移民の密輸–が英国地区評議会のPBXをハッキングし、それを使用して100万ポンド相当の中国への電話をかけました。  
1。  
 評議会は今までに電話代の不一致を発見し、電話会社を返金した。  
 ここでも、ギャングたちはお金を節約するだけでなく、監視を回避することにも興味を持っていました。  
）そのような場合を除いて、ダイヤルスルー詐欺は主にプレミアムレートサービスによって引き起こされ、詐欺師はプレミアムラインオペレーターとの交渉に参加しています。  
 PBXは通常、セキュリティについてほとんど知らない会社の通信管理者によって実行されますが、セキュリティマネージャは電話についてほとんど知らないことがよくあります。  
 世界中のビジネスが受けたPBX詐欺による損失の見積もりは、4ドルから​​減少しました。  
後半の図の約半分が、従来のPBXではなくVOIPとなっている[91]。  
 Red Browserワームが5ドルのSMSをロシアに送信することでキャッシュアウトした2006年に、プレミアムレートのモバイルマルウェアが登場しました[941]。これはAndroidの登場後に拡大しました。モバイルマルウェアについてはセクション22で説明します。  
1。  
 そして今や、電話は投票、アパートの建物への入室の確保、貸し手が仮釈放条件を遵守していることの確認、金融取引の認証などのタスクにますます使用されるようになり、さらに創造的な種類のいたずら、特にハッキングのための動機が生まれています。これは、発信者回線IDを無効にします。  
 これが現実になりました。この章の後半で詳しく説明します。  
1。  
•ワシントン州のクララムベイ矯正センターの受刑者は、コレクトコールの発信のみが許可されていましたが、電話会社（「Fone America」）がコレクトコールを自動的に処理するために導入したシステムの興味深い悪用を発見しました。  
。  
（呼び出し元の名前）。  
。  
囚人は、録音して挿入するマシンの名前を明記することになっていた。  
 受刑者はそうし、自分自身を特定するように求められたとき、「このメッセージを英語で聞きたい場合は33を押してください。  
 ワシントン大学はこの詐欺に何度か襲われました[696]。  
1。  
 また、エンドポイントの識別に依存するメカニズムを無効にするためにも使用できます。  
•電話の転送は、多くの詐欺のソースです。  
今日では、それは専門家と厄介なことができます。  
そのため、銀行のコールバックメカニズムは無効になっています。  
 たとえば、一部の国のフットボールのフーリガンは、試合中に自宅にいることを要求する門限の下に置かれ、発呼者IDを確認する保護観察サービスを呼び出すことによってこれを証明します。  
 保護観察者が群衆の騒音について尋ねた場合、それはテレビであることを彼に伝え、あなたはそれを断ることができない、またはあなたの仲間があなたを殺すでしょう。  
）22。  
6VOIPボイスオーバーIP（VOIP）では、音声トラフィックがデジタル化され、圧縮され、インターネット経由でルーティングされます。  
 今日では、ほとんどの従来の通話はデジタル化され、電話会社に属するIPネットワークを介して送信されるため、技術的な意味では、ほとんどすべての通話が「VOIP」になっています。  
最も人気のあるVOIPプロトコルであるセッション開始プロトコル（SIP）は、脆弱性のシェアをハッシュ化しますが[2069]、ほとんどの場合、多くのアクターが常にスキャンしている貧弱な構成を通じて攻撃されます。 PBXは、内線番号として登録しようとすると、1日あたり100万を超えるメッセージを受信し、発展途上国で高額な番号に電話をかけることができます[1271]。  
1。  
 セキュリティとのより広範な相互作用は複雑です。  
 現在の政治的闘争はロボコールを超えているため、VOIPを経由すると発信者IDをより簡単に隠すことができます。  
 もう1つの規制上の問題は、政府がVOIPサービスを介して行われた緊急通話が確実に機能し、発信者の場所に関する情報を提供することを望んでいることです。  
 そして、VoIPハンドセットは電話のように見え、機能しますが、セキュリティエンジニアリング677ロスアンダーソン22。電話ネットワークの攻撃は、電話のように、電源がオフになった場合にサービスも停止します。  
 したがって、デフォルトの緊急システムであるのは、従来のネットワークではなく、モバイルネットワークです。  
1。  
 古典的な詐欺は密かに行われ、悪意のある電話会社が無意識のユーザーに小額のスロットを請求します。  
 （それはカットを取得するので、それはごまかすためのインセンティブを持っていません。  
 バルセロナでの休暇中に妻のバッグがひったくられたため、私たちは彼女が持っていた電話を呼び出し、キャンセルしました。  
 すべての確率で、スペインの電話会社は、彼らが以前は見たことのない数にいくつかの料金を詰め込んでいただけであり、彼らは通常それを逃れることになるだろうという知識の中で。  
私は、私がアカデミックセミナーで会社のCEOに会い、問題を解決するために彼のプライベートオフィスに連絡をとることができたという理由だけで、この請求から抜け出しました。  
実際、英国の電話会社の苦情への対応は、不正請求に対する顧客の「保険」を提供することでした。  
 多くのバリエーションがあります。米国で800番に電話をかけた場合、会社は「すぐに電話をかけ直せますか？」同意すると、料金を受け入れたと見なされ、プレミアム料金がかかる場合があります。  
もう1つの問題は非難です。つまり、同意なしにサブスクライバーのサービスプロバイダーを不正に変更することです。  
 AT＆Tは最悪の違反者の1つであり、非難だけでなく、加入者の署名を偽造して、サービスに切り替えることに同意したかのように見せかけています。  
さらにもう1つは、プレミアムレートの詐欺に対する国際的な呼びかけの利用です。  
電話会社は、プレミアムレートの数値を国際人に見せかけることでこれを回避しました。  
1。  
 このような詐欺行為は、電話会社が国際的な宛先を選択的にブロックすることを阻止する国際協定（ナイロビ条約）から利益を得ます。  
1。  
 しかし、これらは停止したようです。 2020年のロボコールの広範な研究では、ロボコールの証拠はもう見つかりませんでした[1543]。  
スマートフォンが登場する頃には、電話会社はロンドンのパーキングメーターからフィンランドのフェリーチケットに至るまで、高額なサービス提供の削減に慣れていました。  
 多くの新しいサービスがスマートフォン革命によって可能になり、支払いはSMSからアプリ経由の支払いに移行しました。  
 業界の経済学について考えるために一時停止するかもしれません。  
1。  
 全国規模のネットワークを構築するには何十億もの費用がかかりますが、追加の電話や映画のダウンロードを処理する費用は基本的にゼロです。  
まず、支配的な企業の市場に向かう傾向があります。  
 反トラスト法訴訟後のAT＆Tの解散、およびマーガレットサッチャーによる英国でのBTの民営化の後、世界は規制された競争の異なるモデルに移行しました。  
第二に、競争部門（長距離電話など）では、価格が急速にゼロ近くまで下がっています。  
多くの通信市場で結果は混乱価格です。製品は絶え間なく解約され、低価格のプロバイダーと競合するために新しい導入により寛大な導入割引が提供されますが、料金は後で急上昇します。  
 継続的に価格を確認するのが面倒な場合は、お得な情報を得ることができますが、多くの場合、サービスの質が低下します。  
セキュリティエンジニアリング679ロスアンダーソン22。  
 モバイル化22。  
 2020年までに、私たちは現在50億を超えるサブスクライバーを抱えています。 2019だけで10億台以上のスマートフォンが販売されたと言われています。  
 成長は発展途上国でも急速であり、そこでは有線ネットワークはしばしば老朽化しており、人々は何年も電話サービスを待つために使用されてきました。  
 これは多くの利益をもたらし、新しい犯罪ももたらしました。  
虐待と同様に携帯電話のセキュリティも発達しています。  
 そのため、悪意のあるユーザーは、近所の電話からこれらの番号を取得するデバイスを作成したり、近くにある他の電話からIDを盗んだりするために電話を再プログラムした  
 コールセルのオペレーターは、複製された携帯電話で既知の売り場にぶらぶらし、彼らの顧客は数ドルで電話の家に並ぶでしょう。  
 タンブラーとして知られているこれらは、警察が追跡するのが特に困難でした[944]。  
 シリアル番号の需要は急速に高まり、それを満足させることは、多くの携帯電話がオンになっている空港などの場所でスヌーピングすることでさえ、ますます困難になりました。  
携帯電話は携帯電話です。事業者はサービスエリアをセルに分割し、それぞれを基地局でカバーします。初期のアクティブな攻撃は、通常、フリーウェイブリッジなどの通過交通量の多い場所にある偽基地局で構成されていました。  
詐欺の量を減らすために、さまざまなメカニズムが試みられました。  
 ボーダフォンはまた、RFフィンガープリントを使用しました。これは、携帯電話の無線送信機の製造ばらつきから生じる信号特性を使用して、個々のデバイスを識別し、それらを主張されているシリアル番号に関連付けます[776]。  
セキュリティエンジニアリング680ロスアンダーソン22。  
 モバイル化22。  
1GSM第2世代の携帯電話（2G）はデジタル技術を採用しています。  
 GSMの設計者は、クローン作成やその他の攻撃からシステムを保護することに着手しました。彼らの目標は、GSMが少なくとも有線システムと同じくらい安全であるべきだということでした。  
業界は当初、GSMプロトコルのコアを形成する暗号化およびその他の保護メカニズムを秘密にしようと試みました。  
 ここで簡単に説明します。  
 これらのデータベースにより、着信コールを正しいセルに転送できます。  
 SIMは3つの数字を含むと考えることができます：1。  
 国際的な携帯電話加入者識別情報（IMSI）があります。これは、携帯電話番号にマッピングされる一意の番号です。3。  
ハンドセットのシリアル番号、国際モバイル機器識別（IMEI）もあります。  
1）。  
IMSIは加入者のHLRに中継され、5つのトリプレットを生成します。  
アルゴリズムは、RANDがSIMの認証キーKiで暗号化され、SRESがKc：{RAND} Ki =（SRES | Kc）Security Engineering681Ross Anderson22と連結されていることを示しています。  
 GOINGMOBILEHLR�VLR�BSC�SIM�Mobile�図22。  
とにかく、トリプレットは基地局コントローラ（BSC）に送信され、基地局コントローラ（BSC）は最初のRANDをモバイルに提示します。  
 モバイルはこれをベースステーションに返します。これが正しい場合、モバイルとベースステーションは暗号化キーKcを使用して通信できます。  
2。  
。  
BSC！ SIMRANDSIM！ BSCSRESBSC！ mobile {tra�c} Kc図22。  
 まず、ベースステーションは認証されていないため、盗聴者が偽のベースステーションを使用して通話を傍受するのは簡単です。  
 第2に、ほとんどの国では、基地局とVLR間の通信は暗号化されていないマイクロ波リンクを通過します3。  
GSMの導入により、犯罪のパターンは大きく変化しました。  
 強盗は次の問題であり、子供たちが携帯電話のために強盗されているというメディアストーリーが相次ぎました。  
 盗難の一部はいじめです。子供は小さい子供用の携帯電話を使用しています。一部は、トイレにスマートフォンを落とし、保険が偶発的な損傷をカバーしていないので盗まれたと報告した加入者による保険詐欺です。しかし、強盗が電話を取り、フェンスに売るという強固な盗難の核があります。  
 今日、必要なのは低コストのソフトウェアラジオだけです。  
セキュリティエンジニアリング682ロスアンダーソン22。  
 GOING MOBILEハンドセットのシリアル番号、または海外でハンドセットを出荷する組織犯罪者へのリンクがあります4。  
 2008年までに、プリペイドはメキシコの市場の90％を占めましたが、米国では15％を占めました。  
プリペイド電話も匿名通信を実用的にしました。  
 ただし、プリペイド式の電話は、警察があまり努力しない限り、警察から保護するだけです。  
 すでに述べたように、9/11首謀者の1人は、別のアルカイダメンバーが使用していたものと同じバッチのprepaidSIMを使用したときに捕まった。そして、21/7のロンドン爆撃が失敗した後、1人はローマに爆撃され、すぐに捕らえられました。  
 あなたが世界中の警察を抱えている場合、SIMを変更するだけでは十分ではありません。  
認証に加えて、2Gはさらに2種類の保護を提供することになっていた–位置セキュリティと通話内容の機密性。  
 これは軽量のメカニズムです。異なるネットワークの基地局であるふりをするIMSIキャッチャーによって簡単に打ち負かされます。  
 音声はデジタル化され、圧縮され、パケットに切り刻まれます。各パケットは、暗号化キーKcとパケット番号から生成された疑似ランダムシーケンスでXORすることにより暗号化されます。  
 これは、Comp128と同様に、もともと秘密であったストリーム暗号です。 Comp128と同様、リークされ、攻撃がすぐに見つかりました[248]。  
 電話は、さらに弱いアルゴリズムであるA5 / 2もサポートしました。これは、EU以外の国への輸出が許可されており5、ほぼ瞬時に解読できます。1。  
 世界中の大国の大使館には、地元の電話回線を捕捉するためのアンテナを示す屋根構造があり、スノーデンの論文は、NSA4を確認しています。最近のスマートフォンの設計では、IMEIは変更できないことになっています。一部のAndroidphonesはTrustZoneでそれを保ちます。  
セキュリティエンジニアリング683ロスアンダーソン22。  
 GOING MOBILEは、米国の外交使節団で地元の電話トラフィックを収集します。  
GSMベンダーは、Kasumiと呼ばれる強いブロック暗号に基づいており、第3世代の携帯電話の標準となった、第3の暗号A5 / 3を導入しました。  
 IMSIキャッチャーは、より弱い暗号を使用するようにハンドセットに通知するだけです。  
 携帯電話を使用している容疑者をフォローしている場合は、チャレンジとレスポンスの最初のプロトコル交換を含め、通話を録音します。  
 IMSIキャッチャーは、A5 / 1ではなくA5 / 2を使用するように電話に指示し、キーが正式に設定されます。IMSIキャッチャーは、以前に使用されたチャレンジを送信します。  
 これは現在弱い暗号で使用されているため、すぐに解読され、すでに録音されている会話にアクセスできます。  
 ただし、A5 / 1は最新の機器を使用すると簡単に壊れます。  
 2004-5年、アテネオリンピック中に不明な人（ただしNSAまたはCIA出身であると推定される人）がギリシャ首相の携帯電話をタップし、アテネオリンピック中にその国の政治、法執行機関、軍のエリートを約100名、盗聴設備を破壊しましたボーダフォンのギリシャのネットワーク。  
 同僚と私はこの問題について何年も前に警告し[4]、スノーデンの開示はそれが着実に悪化していることを示唆している。  
とにかく、ネット効果は、2G GSMセキュリティメカニズムがA5 / 1の使用を許可されている国の有線ネットワークよりもわずかに優れた保護を提供するように設計され、他の場所ではやや悪い保護を提供する一方で、今やどこでもやや悪い保護を提供していますサードパーティが工業化できる範囲のエクスプロイトがあるためです。  
2。  
 頭字語3gppは、4G、5G、およびそれ以降の標準化団体で引き続き使用されています。  
 これは主に、人口の少ない農村地域で発生する可能性があり、新しい4Gおよび5Gテクノロジーをインストールすることが経済的でなく、必要なバックホール伝送がはるかに大きくなります。  
6kb / sの標準2Gおよび毎秒数十キロビットの2。  
2。  
 3Gのビジョンは、モバイルTVから、どこでもオンラインになるラップトップまで、あらゆる種類のモバイルサービスを可能にすることでした。  
全体的なセキュリティ戦略は[1976]で説明されており、セキュリティアーキテクチャは[1961]にあります。  
 すべてのキーは128ビットになりました。  
 したがって、ベースステーションまたはマイクロ波バックホールからキーまたはプレーンテキストを取得することは、もはや攻撃ではありません。  
 理論的には、これにより不正な基地局への脆弱性がなくなるため、IMSIキャッチャーは機能しなくなります。  
 3Gには、ローカル傍受のための適切なインターフェイスもあります[1962]。  
 現在、ホームロケーションレジスタはホーム環境（HE）、SIMはUMTS SIM（USIM）として知られています。  
{RAND} K =（RES | CK | IK | AK）HEとUSIMには既知のシーケンス番号SEQもあります。  
チャレンジ、期待される応答、機密性キー、完全性キー、およびマスクされたシーケンス番号は、HEからVLRに送信される認証ベクトルAVを構成します。  
USIM！ HEIMSI（これはオプションで暗号化できます） VLRRAND、XRES、CK、IK、SEQ AK、MACVLR！ USIMRAND、SEQ AK、MACUSIM！ VLRRES図20。  
セキュリティエンジニアリング685ロスアンダーソン22。  
 モバイルを2Gで使用する場合、その設計目標はセキュリティが有線ネットワークのセキュリティと同等であることであり[922]、ネット効果はわずかな改善でした：標的型攻撃ではありますが、高品質のメカニズムによってエアリンクでの大量盗聴が防止されますIMSIによるキャッチャーは、フォールバックを利用することで引き続き機能します。  
22。  
34GF第4世代モバイルネットワークは、2009年に最初にロールアウトされ、ほとんどのモバイルサブスクリプションを占めました（4。  
 回線交換コアネットワークがあった2Gおよび3Gとは異なり、IPthroughoutを使用します。  
データレートが高いため、GoogleマップやSnapchatなどのアプリの動作が大幅に向上し、ビデオストリーミングアプリが可能になりました。  
4Gセキュリティ標準は、ハンドセットとベースステーション間のリンクに暗号化を制限することにより、3Gから戻ってきましたが、ほとんどのアプリは、アプリケーションレイヤーでデータを暗号化します。ハンドセットはUEまたはユーザー機器になり、HE / HLRはホームサブスクライバーサーバー（HSS）になりました。  
 MMEは保護されたスペースに収容するか、少なくとも改ざん防止機能を持たせることができるという考えでした（TPMについて話されているが、オペレーターが実装していないようです）。  
 SS7は、メッセージをオプションで暗号化できる、Diameterと呼ばれる制御プロトコルスイートに置き換えられていますが、オペレーターが互いに信頼し合うため、同じタイプの攻撃の多くに対して脆弱です[426]。  
Rich Communications Services（RCS）は2019年中に広く利用可能になり、Googleのメッセージアプリでのサポートに感謝します。  
 SMS +、+ Message、またはjoynとも呼ばれ、WhatsAppと同じサービスの多くを提供しますが、電話会社がホストする製品であるため、エンドツーエンドの暗号化はありません。  
セキュリティエンジニアリング686ロスアンダーソン22。  
 モバイル化何十年もの間、セキュリティとインテリジェンスコミュニティの要請により、電話のセキュリティは弱く保たれてきました。  
 3Gと4Gのどちらであるか、具体的なエクスプロイトは何であるかについては明らかにしていませんが、2016年12月にオバマ政権がロシアの外交官30名を追い出しました。  
22。  
45G以降5世代ネットワークは2019年にサービスを開始し、帯域幅とレイテンシの点で4Gをさらに大幅に改善することが約束されています。  
 繰り返しになりますが、複雑さがますます高まる標準のファミリが進化しています。  
 本当の興奮は、後に続くスタンドアロンモード（SA）についてです。  
 ネットワークのエネルギー効率とエリアトラフィック容量は2桁増加する可能性がありますが、接続密度、モビリティ、およびデータレートは1桁増加する可能性があります。  
用語が再び変わります。  
 暗号化はデバイスからCUに送られ、そこからIPSecを使用して保護され、MMEボックスに代わるアクセス管理機能（AMF）が使用されます。  
重要な改善点の1つは、デバイスIDがパブリックネットワークで暗号化されてホームネットワークに送信されるため、位置情報のプライバシーが侵害されにくくなることです。また、IMSIキャッチャーは機能しなくなると言われています6。  
ただし、すべての法執行機関のアクセスメカニズムを含め、コアネットワーク全体がクラウドに移行します。  
構成の間違いの1つであり、物事は世界中で判読できる可能性があります。 SGX6のようなものを除いて、以前は3Gでそれを聞いていました：盗聴者は2Gへのフォールバックを強制しただけです。  
セキュリティエンジニアリング687ロスアンダーソン22。  
 GOING MOBILEを機能させることができます。クラウドプロバイダーの政府は、オペレーターではなくワラントに令状を出すことでアクセスできる可能性があります。  
 一方、仕様は複雑で、実装は不安定です。  
 理論的には、トラフィックの編集は編集を行う会社によって署名されますが、それがどのように機能するかはだれも知りません。  
 2020年には、中国でのコロナウイルスの流行と反中国感情の高まり、香港での「1か国2制度」の終了に伴い、英国政府は2020年末からHuaweiに5Gネットワ​​ーク機器の販売を禁止し、2027年までに既存の機器を撤去することを決定しました。  
6Gと7Gはどうですか？通信研究者は、ピーク時の帯域幅、レイテンシ、サービス品質、および電力消費に関するさまざまな要件を持つ多様なアプリをサポートするための、無線アクセスネットワークにおける以前の見え方の進化について話します[1454]。後者は、地球の表面全体に200Mbpsのブロードバンドを展開するための数千のマイクロ衛星を持っています。  
 次に、1990年代後半のドットコムブームにより、ウェブサービスをコアのアクティブプロセスと静的または静的に提供され、残りがCDNにローカルにキャッシュされる残りのアクティブプロセスに分割するように強いられたように、アクティブなstuの一部をホストする必要があります。 ↵ローカルにも。  
2。  
 1つは、携帯電話がサポートする認証機能に対する攻撃が急増していることです。  
1。  
 これらの多くは、セキュリティ経済学を根底に持っています：セキュリティエンジニアリング688ロスアンダーソン22。  
 モバイルへの移行システム内のさまざまなプリンシパル間でインセンティブの不一致がいくつかあります。  
4。  
 これはあらゆる種類の騒乱への扉を開くことができます。個人は、自分のオンラインアカウントを乗っ取る攻撃者によって、自分の人生を捨てられる可能性があります。  
 セクション12で述べたように。  
4、SIMスワップ攻撃は2020年に銀行およびビットコイン取引所の顧客に対して主に使用され、多くの場合、電話会社の内部関係者が関与します。SIMスワッピングを困難にしている唯一の主要な米国MNOは、Verizon [712]です。  
 2003年に最初に行動を起こしたMNOは南アフリカのMTNで、これによりユーザーは2番目のSIMを指定してSIMの交換を許可することができました。不思議なことに、これは2007年の最初のSIMスワップ詐欺事件に関係した電話会社であり、セクション12で説明しました。  
4。  
 セクション22で、電話会社が顧客に対してしばしば対立する態度について話しました。  
8; MNOは、この点で従来の有線電話会社と違いはありません。  
MNOとそのサプライヤーがカスタマーセキュリティを適切に実行できないと感じているもう1つの例は、SIMjackingです。  
 SIMカードは署名されたソフトウェアのみを実行できるため、業界はこれは問題ではないと反論しました[1582]。  
 MNOと顧客との関係は常に幾分敵対的であり、多くの国ではオンデマンドでミドルパーソン攻撃を実行せざるを得ません。  
このようなネットワークインジェクション攻撃は、IMSIキャッチャーを使用して戦術的に実行できますが、MNOで実行する方が便利です。  
 セクション26で、政府の監視と、暗号化戦争以降のセキュリティによって生じた緊張について説明します。  
7。  
MNOの根本的な問題は、MNOがサービスの制御を失ったことです。  
 彼らは最終的には商品化されていた–インフラを維持しなければならないが、かつては独占利益を享受していて、他人にクリーム色にされているビットシフターを見る。  
3。  
3プラットフォームのセキュリティ電話ストーリーの2番目の部分は、アプリのエコシステムです。  
 プログラム可能な電話が2000年代初頭に登場して以来、これはますます懸念されています。  
 簡単に言うと、iPhoneが登場する前は、チップデザイナー、チップメーカー、OSベンダー、携帯電話OEM、MNOがDRMと制御を乱用している間に、セキュリティがサプライチェーンに沿って細分化されていました。  
 アクセスコントロールの章で述べたように、Armは2004年にTrustZoneを立ち上げました。 2007年までに、毎年数百のウイルスとワームがSymbian電話で検出され、ベンダーはアクセス制御、コード署名などで対応しました。  
 まず、顧客との関係を持つOEMのタブーを破りました。  
 第三に、App Storeをプラットフォーム戦略の中心に据え、音楽ダウンロードとソフトウェアの両方を共有することで収益化しました。  
 デバイスは、MNOまたはwifiを介してオンラインになり、必要に応じて2つを簡単に切り替えることができます。  
 Googleは翌年、Androidをローンチしました。戦略は、可能な限りオープンなプラットフォーム7にすることで、誰でもAndroidフォン用のアプリを作成できるようにしました。  
 彼らは、マイクロソフトが1980年代初頭にネットワークエフェクトを好むよりオープンなプラットフォームを提供することでAppleからPCソフトウェア市場の大部分を奪い、iPhoneをニッチ製品として残して、電話で同じことをしたいと考えたことを思い出しました。お金持ち。  
しかし、Appleの収益化戦略により、プラットフォームを維持するインセンティブが向上します。通常、iPhoneには少なくとも5年間パッチが適用され、Android製品には3パッチが適用されます。  
 電話には他に数十のCPUが含まれているため、メインプロセッサはすべてではありません。また、DSPにも複数のOEMの携帯電話に影響を与える可能性のある脆弱性が発見されています[1212]。  
 豊富なセンサーと幅広いアプリケーションの組み合わせにより、プラットフォームレベルでのセキュリティとプライバシーサービスはかなり複雑になります。  
 ただし、これらは、デバイスのRF動作を制御するベースバンドソフトウェアをロックダウンする必要があるとの規制当局の主張を前提とするのではなく、エコシステムとして理解するのが最も適切です。セキュリティエンジニアリング690ロスアンダーソン22  
 プラットフォームセキュリティ保護オプションのリスト。  
 2019年までに、全インターネットアクセスの56％がモバイルデバイスからでしたが、米国では63％、インドでは80％でした[1252]。  
境界を定義することは困難です。  
 モバイルデバイスがブラウザーアプリからアクセスするWebサービスを含めますか？ WhatsApp、Skype、Signalなどのアプリに移行するので、音声通話を含めますか？時計から車まで、モバイルオペレーティングシステムやアプリを実行する他のデバイスはどうですか？アプリファミリから始めるのが最も簡単な場合があります。3。  
 そのプラットフォームセキュリティモデルは、GoogleのRen´eMayrhoferと同僚によって[1252]とセクション6で説明されています。  
8テクニカルアーキテクチャについて説明しました。  
 実装では、従来の\* nixシステムのようにエンドユーザーにユーザーIDを与えるのではなく、Androidは各アプリを個別のユーザーIDで実行します。プライベートアプリディレクトリ内のデータはアプリによって制御されますが、共有ストレージ内のデータはエンドユーザーによって制御されます。重要なシステムデータがルート化されていない限り、プラットフォームによる制御下に維持されるようにするための必須のアクセス制御メカニズムがあります。  
 脅威モデルには、物理​​的な攻撃から盗聴、オペレーティングシステム、ライブラリ、その他のアプリの脆弱性の悪用まで、あらゆるものが含まれます。ユーザーが悪意のあるアプリをインストールするよう誘導されることが想定されています[1252]。  
ただし、Googleはアプリの販売から収益の30％を受け取り、アダルトアプリのホストを拒否しています。  
 2014年以降、GoogleはPlayストア以外のアプリを最初に実行するときにスキャンするためにアップロードすることを義務付けていますが、悪意のあるアプリのリスクは常に存在します。  
 悲しい事実は、ユーザーデータが主要な商品になっていることです。ほとんどのアプリは無料であり、エコシステムは他の何よりも広告収入によって推進されているので、他に期待できることはほとんどありません。  
 （Blackberryでは、ユーザーがインターネットアクセスを拒否することが許可されていました。  
 これが気に入らない場合は、VPNになりすましたファイアウォールアプリケーションを入手し、他のアプリケーションのインターネットへのアクセスをブロックすることができます。  
セキュリティエンジニアリング691ロスアンダーソン22。  
 プラットフォームのセキュリティ22。  
1。  
 Androidエコシステムはオープンであるため、誰でも開発者になることができ、Playストアを通じて作成したソフトウェアを配布できます。  
 Android SDKでフレームワークを使用する必要があるという事実は、開発者を潜在的に有用な方法で制約します。  
ただし、開発者は急速に技術面とビジネス面の両方の複雑さに直面します。  
 しかし、その機能はどの程度均一ですか？ Androidのバージョンをいくつサポートする必要がありますか？何百もの異なるハンドセットでテストする必要がありますか？現在、役立つテストフレームワークがありますが、アプリが多くの最新の電話で豊富なハードウェア機能を使用している場合、断片化は現実的な問題です。  
 別の例は、開発者がバンキングアプリの主要な資料など、本当に機密情報を保護したい場合です。  
 次に、An-droidはKeyStoreを提供しました。これにより、アプリはキーをTrustZoneまたはaSecure Elementまたは利用可能な場合は他の暗号化プロセッサに保存し、他のアプリがそれらを使用できないようにします。  
7。  
ビジネスの複雑さは、アプリケーション自体、またはエコシステムの基礎となる経済性に起因する可能性があります。プラットフォーム企業、デバイスベンダー、アプリ開発者、アプリパブリッシャー（あらゆる種類の広告を追加する）、広告ネットワーク、ツールスミス、エンドユーザーはすべて問題を抱えています。 erentインセンティブ。  
 ユーザーを識別するためのルールは複雑です。ユーザーの同意は、一部のUID（IMEI、IMSI、電話番号、および広告ID）を使用するために必要ですが、MACアドレスやハードウェア指紋などのその他のものは必要ありません。  
3。  
2Bad Androidの実装2010年頃にAndroidが広まったときに明らかになったシステムセキュリティの問題の最初のバンドルは、Androidをライセンスしている多くのOEMによるエンジニアリング作業の質の悪さでした。  
 裕福なユーザーが最新のモデルを購入し、古い電話が販売されてしまうため、中古電話の取引は盛んです。  
 しかし、一般的な電話でフラッシュメモリを構成する方法とのすべてのやり取りがあるため、これを正しく行うのは困難です。組み込みのマルチメディアカード（eMMC）と仮想SDカードがあり、独自のウェアレベリングメカニズムを備えている場合があります。  
3。  
数年間、私はGoogleの自社ブランドのNexusとPixelのスマートフォンを購入し、使用後は決して販売しませんでしたが、多くの人々は契約によって補助金を受け、MNOにロックされます。  
）これらの品質の問題は、さまざまなチップセットベンダーによって実装されているTrustZoneおよびそのTrusted Execution En-vironment（TEE）にも及びます。  
その他の問題は、他の4つのベンダーのTEEへの攻撃を可能にします。信頼できる環境で使用されるソフトウェアセキュリティメカニズムは、ASLRの欠如または弱い、TCBが非常に大きい、デバッグチャネルを介した情報リークなど、最新の技術より数年遅れます。実行防止、複数のサイドチャネル、邪悪なTAや脆弱なTAを無効にする方法はありません。ただし、Android実装の最大のセキュリティ問題は、アフターサービスのサポートが不十分なことです。  
 2015年の調査では、アクティブなデバイスの87％が安全ではなく、2011〜15年の平均でした。これは、既知の脆弱性を含むオペレーティングシステムのバージョンを実行していたためです。  
 これは、2011年までにGoogleによって問題としてすでに特定されていました。同社は、OEMがシステムにパッチを適用することを約束した場合、価格の安いコンポーネントへのアクセスを提供しましたが、これにはほとんど影響がありませんでした。  
 OpenSSLやBouncy Castleの暗号ライブラリに脆弱性が見つかった場合、この修正はLinux、Android、各OEM、そして多くの場合は各モバイルネットワークオペレーターに伝播し、MNOが電話の更新を制御する必要があります。ネットワークにロックされています。  
 これは、調整された開示に関する厄介な問題を引き起こします。これについては、セクション27で説明します。  
7。  
22。  
1。  
Androidの初期のバージョンでは、アプリのマニフェストはアプリが要求するアクセス権を指定しており、ユーザーはアプリを実行するためにインストール時にすべてを承認する必要がありました。  
 すでに2012年の調査では、インストール中に注意を払ったのは17％のユーザーのみで、セキュリティエンジニアリングに回答できるのはわずか3％でした693Ross Anderson22。  
 プラットフォームセキュリティ何が起こっているかに関する基本的な質問[676]。  
 実際、より危険なアクセス許可の漸進的な制限により、プラットフォームの進化が何よりも推進されています。  
Googleは現在数十の権限を提供しており、開発者は他のアプリでサービスを利用できるようにするときに、常にカスタム権限を定義できます。これらの何千ものハードウェアベンダー、MNO、セキュリティファーム、インターネットブラウザーによって定義されています[741]。  
Yasemin Acarと同僚による同意の問題の分析は、ユーザーと開発者の両方による許可の理解と許可への注意に分かれています[10]。  
 略奪的なashlightアプリが私のアドレス帳へのアクセスを求めている理由は十分に明らかです。多くの失敗はより微妙です。  
 開発者の使いやすさは、バグの重大な原因です。これは他の場所でも指摘しています（e。  
 セクション5で。  
 かなりの少数の開発者が、無知や混乱から排除されたものよりも多くの許可を要求します。これは、開発者がよりよく知っているはずのシステムアプリにも当てはまります。  
 これにより、開発者は、stackexchangeなどのフォーラムを介して他の開発者のコ​​ードをコピーするようになりました。  
3。  
4AndroidマルウェアAndroidは誰でもアプリを記述できるオープンプラットフォームであるため、多くの有害なソフトウェアを引き付けています。  
1。  
 ここでの定義は難しいものです。多くのアプリは、一部の人々を少なくとも異なる方法で有害にするためです。ここでは、アプリをインストールしたユーザーの利益に反して秘密裏に機能するアプリに焦点を当てます。  
3。  
6。  
 その量のほとんどは、民間部門のバラエティが豊富で、そのほとんどは定期的な流通チャネルを通じて提供されます。  
 The8Itはまた、Acarと彼女の同僚に開発者の視点からユーザビリティを見るように促し[11]、セキュリティ制御の重要な新しい領域を作成しました。これは、Access Controlの章の最後にあるリサーチの問題のセクションで述べました。  
3。  
 アプリは生まれながらに有害な場合があり、依存しているライブラリが悪くなる場合や、悪意のある人が元の銀行のドメインを取得するのと同じように、失敗したアプリ会社を購入する場合があります。  
 60以上のアンチウイルス企業が異なる基準を使用してアプリにラベルを付け、それらを異なるファミリに分類するため、測定の問題は重要なものです。  
Guillermo Suarez-TanguilとGianluca Stringhiniが分析した2018年の調査1。  
 2012年以降、それらのほとんどは再パッケージ化に関与しており、マルウェアの開発者が正当なアプリ（キャリア）を取得し、有害なコード（therider）を追加しています。  
 ライダーは、永続的なアクセスのために電話をルート化し、通常のPCマルウェアと同じように、コマンドアンドコントロールサーバーの指示でお金を稼ぐことができるリモートアクセストロイの木馬（RAT）を投下しようとします。  
 ライダーの大多数は暗号化などの難読化の手法を使用していますが、これを行うのは無害なアプリの4分の1のみです（Facebookのアプリは、マルウェア、特に開発途上国のRATによって盗まれたユーザーデータとキーに対する防御として難読化を使用しています）。バンキング型トロイの木馬は、より標的を絞った民間セクター向けマルウェアの中でも際立っています。  
 Androidマルウェアはしばらくの間、銀行のSMSを盗んでおり、Googleは承認されたアプリのみにSMSの読み取り権限を許可することで拒否しています。 2020年の最新の動向は、CerberusバンキングマルウェアがGoogleオーセンティケーターCookieも盗むようになったことです[431]。  
 このようなマルウェアは、ルートアクセスを求めますが、スパイウェアを埋め込みます。  
一部の管轄区域では、大量のステートマルウェアにアプリの修正バージョンを義務付けることができます。Skypeは、中国の検閲者によって禁止されている単語をスキャンするために再パッケージしたローカルディストリビューターのTomOnlineを通じてのみ、2005年から中国で利用可能でした。  
セキュリティエンジニアリング695ロスアンダーソン22。  
 プラットフォームのセキュリティアプリが許可フレームワークを打ち負かしながら、電話を応援する手間を省くという技術的な不正行為があります。  
 彼らは、SDカードを秘密チャネルとして使用している2つの中国の大企業、BaiduとSalmonadsを見つけました。これにより、携帯電話のIMEIを読み取ることができる広告が、そうでない場合のためにそれを保存できます。  
22。  
1。  
 このようなサービスは、ユーザーの同意なしでも、複数のアプリにわたってユーザーを追跡できます。  
ある時点で、アプリが更新され、悪意のあるモジュールを含む新しい広告ネットワークが追加されました。  
サードパーティのサービスは、ユーザーには直接見えないため、エコシステムのかなり不透明な部分です。  
 彼らはこれまでに報告されていなかった数百を含む2,000以上の広告および追跡サービス（ATS）をマッピングし、かなりの少数（39％）がデバイスをまたいだ追跡を行っていることを発見しました。上位20社のうち17社は、ウェブとアプリのエコシステムに存在しています。  
 すべての中で最大のものはAlphabetand Facebookでしたが、Chart-boost、Vungle、AdjustなどのATSでビジネス全体を構成している企業は大きなシェアを占めており、ユーザーには比較的知られていません。  
 有料アプリはトラッカーが最も少なく、無料アプリはより多く、無料アプリはアプリ内購入を可能にし、多くの場合プレミアムサービスが最も多い傾向があります。  
 アプリ開発者は、アプリサンドボックスで実行され、その権限を継承するため、広告ネットワークを信頼する必要があります。  
 （PCの世界では以前と同様に、境界は少しあいまいです。スタックのほぼすべてのレイヤーで略奪的な動作があります。  
3。  
 さらに悪いことに、アプリの19％はSDKを使用して個人を特定できる情報を収集しており、これを子供向けアプリで禁止していました[1599]。  
 EUGDPRとそのeプライバシー指令に反する慣行は他にもありますが、ATS産業は米国に圧倒的に基づいており、実質的に目に見えない輸出となっているため、EUの規制当局は関与することに消極的です。  
ほとんどの人は、アプリにお金を払えばプライバシーが保護されることを期待しています。  
 Catherine Hanandの同僚は、同じアプリの無料版と有料版を比較し、有料版の3分の1はデータ収集に関して同じように略奪的であり、6分の1は同じデータの少なくとも一部を収集したことを発見しました。 4分の3が同じ権限を使用しました。そして、ほとんどすべてが同じセキュリティポリシーを持っていました。  
22。  
1。  
 ディストリビューションは通常、ハンドセットOEMとMNO間のパートナーシップを反映しており、さまざまな関連開発者、広告ネットワーク、およびディストリビューターがいます。  
 一部の電話には、悪意のあるアプリによって悪用される可能性のある診断モードまたはサポートモードもあります。  
 FacebookやAccuWeatherなどの個人データを積極的に収集することで知られている企業からの報告もあります。これらの多くは、これらの企業のアプリの公開バージョンではありません。また、多くのプリインストールアプリはモバイルアナリティクスまたはターゲット広告ライブラリを使用しています。  
多くの企業は、企業顧客向けのモバイルデバイス管理、コールブロッキング、VPNサービスなどのタスクを実行するために、機密性の高いカスタム権限を持っています。  
 このようなアプリが最も頻繁にアクセスするドメインは、Alphabet、Facebook、Amazon、Microsoft、Adobeでした。  
22。  
2AppleのアプリエコシステムAppleは、セキュリティの使いやすさを最初からリードしており、Androidよりずっと前にきめ細かなアクセス制御を提供していましたが、そのエコシステムは常により閉鎖されていました。  
3。  
 ビジネスモデルはゲームコンソールとほとんど同じでした。  
 Appleが半分の先進国（そして10代の4分の3）で市場を持っている今、これは反トラスト法の問題になりつつあります。なぜマッチのような出会い系サイトをする必要があります。  
 ルールは特に小規模な企業に大きな影響を与えているようであり、iPhoneアプリを介して予約した場合、パンデミックのためにオンラインで行ったミュージシャン、フィットネスインストラクター、ヨガの教師などの人々に「アップル税」を課しました。  
Appleはまた、ハードウェアとオペレーティングシステムの制御を使用して、権利管理メカニズムを実装し、アフターマーケットの収益を保護しました。競合するアプリストアは許可されていません。  
アプリの審査プロセスは、Googleのテストよりもはるかに困難です。広範な自動セキュリティテストがあり、その後、手動による確認が行われ、アプリが支払い、コンテンツ、不正行為などのAppleのポリシーに準拠していることを確認します。  
 したがって、学術研究者はiOSエコシステムをあまり詳しく調べていませんが、それでもいくつかのことが言えます。  
 確かに、私たちの大学のファイナンス部門がフィッシングから本当に高額なトランザクションを保護する方法についてアドバイスを求めたとき、私のアドバイスは簡単でした：支払いを解放するために銀行の認証アプリを実行するiPadを購入し、支払いにのみ使用する-メント、そしてそれを残りの時間安全に保管してください。  
まず、Androidのように、DRMに異議を唱えたり、Appleの99ドルの税金を払わずに自分のアプリをサイドロードしたりしたいと思った人から始まって、愛好家やその他の「脱獄」Appleデバイスの長い歴史があります。  
 エクスプロイトがデバイスのブートROMの場合など、パッチを適用できない場合があります。たとえば、2019 Checkra1n脱獄は2017年より前に販売されたほとんどのデバイスを解放します[798]。フォレンジック業界は、4SからX [798]までのすべてのiPhoneのブートROMを利用するCheckm8脱獄を使用します。これは、セクション26で説明するように、世界の警察に販売されているフォレンジック「キオスク」で広く使用されています。  
1。  
3。  
2。  
 キャリアロック解除の市場もあります。この市場では、電話が攻撃者の物理的な管理下にあると想定することもできます。  
 セクション2で説明しました。  
4 UAEがこのようなツールを使って反体制派を標的にし、サウジアラビアがイエズベゾスに対してどのように使用したか。 theSaudisは、地域のライバルであるカタール国王もハッキングしました。  
 Appleはそのようなエクスプロイトに常に迅速にパッチを適用するため、何百万ものユーザーがごく一部のターゲットにしかアクセスできません。  
 これにより乱用とスパッツが発生し、アプリがApp Storeのポリシーに違反しなくなるまでFacebookのエンタープライズ証明書が一時停止されました。 iPhone上のGoogleのアプリも同様の経験をし、突然、ポルノ、ギャンブル、スパイウェアアプリによる多くの虐待が明らかになりました。  
 悪意のある俳優の多くは、発展途上国のMNOからのヘルプラインアプリのふりをして、企業の証明書を取得していました[1170]。  
 したがって、iOS向けのファイアウォールアプリも見つかりますが、これはiOSのプライバシーメカニズムがプライバシーを妨げる一方向です。  
マルウェアの問題はAndroidほど深刻ではありませんが、同じ市場の力が適用されるため、依然として広告の乱用が発生します。  
 VPNやアドブロッカーなど、プライバシーの意識が高まると思われる可能性のあるアプリの場合と同じように、Androidエコシステム[1739]のように、埋め込まれた広告ネットワークを通じてプライバシーエクスプロイトが侵入します。  
 また、Apple App Storeの方がGoogle Playストアよりも多くのアプリが支払われます（4ではなく6％）。  
 セクション22。  
1。  
 Appleについても同様の結果が期待できるかもしれませんが、iPhoneは調査を行うのが難しいプラットフォームです。  
 それがあなたの戦略であるなら、あなたは時々リスニングデバイスを兼ねてあなたのPAがあなたのためにそれを運ぶようにするかもしれないとあなたはより良く仮定するべきです。  
2。  
10。  
3。  
 たとえば、iOS13は、インストール時の「許可」から「一度だけ許可」および「アプリの使用中は許可」にジオデータを絞り込み、位置を特定するためのWi-FiとBluetoothの使用を削減し、開発者からの同様の苦情を引き起こします[434]。  
セクション2で説明したように、2つの店は、サウジアラビアの男性が自分の妻、娘、使用人の動きを制御するために使用するアプリを両方許可するなど、いくつかの政治的問題を共有しています。  
4。  
 Appleは「悪い」アプリを削除することに関してGoogleよりも積極的ですが、これはそれらを悪い評判にすることがあります。  
。  
 具体的には、ユーザーが法執行機関を回避することを許可した」一方、GoogleはAndroidのバージョンアップを残しました[1253]。シンガポール政府は2020年2月に、Bluetoothを使用して互いに近くにあった電話を記録するアプリを発表しました。これにより、誰かがウイルス陽性であると検査されたときに、公衆衛生担当者は患者に尋ねるだけでなく、連絡先を自動的に追跡できるようになりました。先週会った。  
 2m離れた場所にいる人が確実に見えるように音量を設定すると、10m離れたところにかなりの数が表示されます。これにより、連絡先トレーサーが処理する必要がある偽警報の数が大幅に増加します。  
 これが4月に報告されたときまでに、英国、フランス、ドイツ、ラトビア、オーストラリアを含む他の国々の多くは、連絡先追跡アプリを開発し始めていました。  
より良いアクセスを求めてGoogleとAppleは拒否し、すべてのアプリがBluetooth連絡先トレースを実行できるかどうかを顧客にプライバシーリスクとして言及しました。  
 これは、選ばれた政治家の仕事である政策決定をすることに対するグーグルそして特にアップルの批判につながりました[955]。  
セキュリティエンジニアリング700ロスアンダーソン22。  
 プラットフォームのセキュリティ22。  
3分野横断的な問題2つのエコシステムの融合により、分野横断的な問題が増加しています。  
 もう1つの注目すべきエコシステムは、おそらくスマートスピーカー製品カテゴリを開始したAmazon Alexaのエコシステムです（このカテゴリは非常に急速に成長し、スマートフォンでは8年ではなく米国の人口の半分に採用されるまでに4年かかりました）。  
セクション22で説明したMNOに起因する問題に加えて、  
5、そして前のセクションで説明した猛烈な広告エコシステムでは、主要な問題は不十分に設計されたアプリです。  
 特定のアプリケーションの問題は、この本の他の多くの章で説明されています。  
 これは、多くのアプリ開発者がよく考えていない問題、つまり失効を示しています。  
 それが本当のエンジニアリングの結論です。サプライチェーンと連携し、カスタマーエクスペリエンスと悪用の可能性のあるケースの両方を通して考えます。  
 さらに多くのケースがありますが、これは十分に設計されていないアプリが安全が重要なシステムを含む他のシステムを公開する可能性があることを示すのに十分です。  
 維持されなくなったアプリに依存する商品の結果は、EUが2019年にGoodsDirectiveの販売を可決したことであり、デジタルコンポーネントを備えた商品のベンダーがこれらのコンポーネントを少なくとも2年間維持することを要求しています。顧客。  
 この本の最後の章でサステナビリティについてさらに議論します。  
4。  
4SummaryPhoneのセキュリティは魅力的なケーススタディです。  
 はじめに、システムは実際にはまったく保護されておらず、請求を回避して通話をリダイレクトすることは簡単でした。  
 これらは、PBXなどの端末機器の不十分な設計と管理によるユーザーへのソーシャルエンジニアリング攻撃から、さまざまな予測が困難な機能の相互作用の悪用までさまざまです。  
モバイルの面では、GSMとその第3、第4、第5世代の後継者を確保しようとする試みが興味深いケーススタディになります。  
彼らの努力は完全に無駄ではありませんでしたが、非常に複雑なグローバルエコシステムにつながり、特に5Gインフラストラクチャの制御を巡る重要な政治的闘争の対象になりました。  
 Androidecosystemは、アプリを主要な国際的なビジネスに組み込んだUberのような企業から、多くの確立されたビジネスや多数の専門ツールによって提供されるアプリを通じて、かなりの犯罪者まで、何十万もの開発者を魅了しています。  
 両方のエコシステムにある明らかに無害なアプリの多くは興味深い方法で悪用される可能性があり、それらが使用する広告ネットワークはプライバシーに対する広範な脅威です。  
 実際、ほとんどのAndroidスマートフォンは最新のパッチが適用されていないため安全ではないため、技術的なプラットフォームセキュリティのレベルではなく、エコシステムのレベルでの大掛かりな作業は行われていません。  
 私たちは、過去10年間、携帯電話アプリのエコシステムにおける問題の多くを調査してきました。そのほとんどは、問題のほとんどが発生するAndroidの部分です。  
 これらの新たに出現するエコシステムの規模が非常に大きいことを考えると、脅威と脆弱性の両方の探索を自動化する革新的な方法が必要です。4。  
さらに読む世界の電話システムに関する情報は、かなり重いと思われる多数の標準ドキュメントに散在していますが、アプリプラットフォームには少なくとも公式ガイド、ホワイトペーパー、開発者コミュニティがあります。  
特定のサブ問題についての良い調査がいくつかあります。これについては関連セクションで引用しましたが、電話のセキュリティシーン全体に関する優れた書籍や調査報告書は知りません。  
セキュリティエンジニアリング703ロスアンダーソン