技術的な攻撃に頼る必要はほとんどありませんでした。  
– KEVIN MITNICK  
プライバシーとは隠れることではなく、プライバシーとは人間の成長と仲介です。  
  
まず、iPhoneの発売後10年で、世界はPCやラップトップを介したインターネットへのアクセスから、代わりにスマートフォンを使用するようになり、何十億もの新規ユーザーも追加しました。  
第2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と非常によく似ており、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。電力会社は携帯電話に依存してエンジニアに障害を修復するよう指示しているため、電源システムが停止してから数時間後に電話システムがダウンすると、本当の問題が生じます。  
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は有益です。  
 無料通話を受けるため;その後、電話システムの脆弱性が詐欺師に悪用され、警察の盗聴を回避しました。その後、プレミアムレートの通話が導入され、大規模な詐欺が発生しました。その後、通信市場が自由化されると、一部の電話会社は互いの顧客に攻撃を仕掛け始めました。そして、いくつかの電話会社は互いに攻撃さえしました。  
同じ悪用のサイクルがインターネットでも繰り返されました。アマチュアのハッカーが続いて、盗聴についての議論が続き、企業とユーザーの間の詐欺と争いが続きました。 2つが集まったとき、複雑なやり取りがたくさんありました。  
セキュリティエンジニアはこれをどのようにナビゲートするのですか？  
1。  
2。  
電話セキュリティは以前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。  
22.1電話ネットワークへの攻撃  
ローランドヒル卿が切手を発明する前、切手は受取人によって支払われました。  
人々はすぐに、特派員が拒否した手紙の表紙に短いメッセージを送るための計画を練りました。  
電信によって開発された虐待の2番目のセット。  
ここでも、問題を立法化する試みは失敗でした[1818]。  
電話も例外ではありませんでした。  
22.1.1通話メーターへの攻撃  
•1950年代、一部のシステムのオペレーターは、金属板にコインが落ちる音を聞いて、コールボックスの顧客が支払ったことを知らせなければならなかったため、人々は正しいメモを打つ金属片でコインボックスを叩く練習をしました。  
彼は他の誰かの数を与えることができます–そして、誰が請求されるでしょう。  
 彼の番号はxxx-yyyyです）  
したがって、公衆電話回線には、オペレーターに警告する警告がありました。  
、今回は公衆電話からの電話であるという警告はありません。  
•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。各パルスは、ラインに抵抗を挿入した後、短い開回路が続いたものです。  
（この場合の法案は、魔法のボタンがそれほど面白くなかった学生組合に送られました。）  
ほとんどの国では、1990年代に公衆電話をコインからチップカードに移動して、コインの収集と破壊行為のコストを削減しましたが、18.5節で述べたように、最初はデザインが貧弱で、悪意のある人がそれまで多くの偽のテレホンカードを販売していました修正されました。  
1970年代から1990年代にかけて、国際電話の料金が非常に高かったため、一部の外国人学生は自宅に電話をかけるために電話を住宅用回線に接続し、無防備な家の所有者は莫大な請求書を受け取る可能性がありました。  
英国の電話会社は、ノルウェーの電話会社ほど賢明ではなく、盗聴の可能性を否定し、被害者の世帯から通話料を徴収することを拒否する方針を持っていました。  
彼らが問題を抱えた最初の兆候は、彼らの電話での会話を聞いたことでした。  
申立人は3人の女性で、全員が、この家族が膨大な数の電話をかけたと思われる番号とは異なる1桁の数字を持っています。  
家族が後で電話会社に障害について不満を言ったとき、彼らの接続は再ルーティングされ、これで問題が解決しました。  
麻薬の売人が近くに住んでいたことがわかりました、そして彼が公衆電話で彼の急使に電話するために彼らの電話を盗んだことは合理的な推論であるように思われました。しかし、警察と地元の電話会社はどちらも、ディーラーが今は6年の刑務所にいたとしても、危険すぎると主張して、ディーラーが住んでいた家に入るのを拒否しました。  
結局のところ、加入者は嫌がらせの電話をしたことで有罪判決を受けたが、この事件では正義の流産と広く信じられている。  
1990年代に、これはパリで非常に広まり、フランステレコムは電話会社の伝統に違反し、被害者が違法に輸入されたなりすましが容易なコードレス電話を使用していたとして、そのことを発表しました[1097]。  
これらのメカニズムは独自仕様でしたが、リバースエンジニアリング後のErik Tewsが2012年に文書化したように、複数の弱点があることが判明しました[1871]。  
 これは通常234回の作業で壊れることがあります。弱い乱数ジェネレータがあります。プロトコルの失敗には、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、以前に記録したコールを復号化するリプレイ攻撃が含まれます。  
Tewsの業績が発表されて以来、DECT標準化団体は代わりにAESの使用を提案していますが、いくつのベンダーが気になることがあ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電話を安くして以来、それはほとんど姿を消しました。  
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。  
 いいえ、あなたは言う（本当に警戒心がなければ）  
これで123-456-7890が電話番号と5678がパスワードになり、詐欺師が通話料金を請求できるようになります。  
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。  
 比較的安い米国とカナダ以外の国を含みます。  
電話会社は顧客に「知らない電話番号に電話を返さないでください」とアドバイスしました–しかし、それはどれほど実用的ですか？  
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、規制が厳しすぎると主張して、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。  
 あらゆる種類の番組で、視聴者に電話をかけて投票してもらうことに最終的には満足していた。  
1920年代にラジオ放送が始まって以来、放送局による電話詐欺は世界中で繰り返し発生している問題であり、1950年代にテレビが主流になったときに悪化しました[2050]。  
  
「電話の盗用」という用語は、信号に対する攻撃と純粋な電話詐欺を指します。  
私が聞いた最初の攻撃は、1952年にさかのぼります。1960年代半ばから後半にかけて、アメリカとイギリスの両方の多くの愛好家が、通話を再ルーティングする方法を考え出しました。  
彼のあまり才能のない同僚は自家製のトーンジェネレーターを使用しました。その中で最も一般的なものはブルーボックスと呼ばれていました。  
発信者は、自分が本当に望んでいた番号を入力して、支払うことなく接続できます。  
スティーブ・ジョブズとスティーブ・ウォズニアックは、コンピューターに転用する前に最初にブルーボックスを作りました[722]。  
当時、ほとんどの電話会社は独占的で、大規模で面倒で無反応でした。  
国内の電話回線がサービスの盗難に関与していた人々は、彼らが容疑で立ち往生しているのを発見しました。  
 彼女にかけた電話の代金を支払っていなかった電話の話に、あなたは突然、会社がその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、警察またはスパイが電話を盗聴するためにラインマンを派遣する必要なしに、自分のデスクの快適さから電話を盗むことを可能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。  
  
電話交換スイッチがプログラム可能になると、攻撃の2番目の波がコンピューターを標的にしました。  
これらのあまりよく保護されていないマシンの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、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。。  
KIISは毎週102番目の発信者にポルシェを提供するため、ポールセンと彼の共犯者は、ラジオ局の25の電話回線へのすべての通話をブロックし、自分自身を保存して、102番目の通話を行い、ポルシェを収集しました。  
実際、FBIは彼に降りてきたので、「必要に応じて盗聴で背中を傷つけ、ハッカーの問題を調査します」という言葉に沿って、政府機関と電話会社との不適切な関係の主張がありました。 [690]。  
[388]で言及された攻撃の一部は海外からのものであり、そのようなトリックが情報戦争攻撃のコンテキストで電話システム全体をクラッシュさせるために使用される可能性は、NSAを心配しました[727、1106]。  
（2001年のアフガニスタン侵攻の間、カブールは2つの交換を行いました：古い電気機械的交換と新しい電子的交換です。  
 実際の攻撃の多くは、システムを誤設定して特別な番号を介して無料通話を提供する内部者を巻き込みました。  
Poulsenを連想させるハッキングで、ブリティッシュテレコムの2人のスタッフが、ランダムに選択された1000のコールの1つだけが通過するはずだったテレフォンインオファーからコンコルドのチケットを10枚獲得した後、解任されました[1914]。  
彼らは当初、彼が米国の電話システムを悪用して機密性の高い米国の標的を盗聴している外国人のエージェントであると考えていました。  
彼は古典になる[1325]欺瞞についての本を書いた。  
電話会社は、他の企業と同様に、不注意な内部関係者や悪意のある内部関係者に対して脆弱です。  
たとえば、顧客を認証するために大量のSMSメッセージを送信したい場合など、多くの電話会社がSS7に企業顧客へのアクセスを許可しています。  
たとえば、Gmailアカウントをハッキングしたい場合は、モバイルサービスプロバイダーに、あなたが私のネットワークにローミングしたことを伝えるメッセージを送信します。  
セクション3.4.1と12.7.4で述べたように、これは現在銀行詐欺に積極的に使用されています。銀行の顧客からお金を盗むための最初の使用例は、2016年にドイツで、彼らが知らないうちに別のネットワークに移動したときでした。ロンドンでも同様の詐欺が2019年に発生しました[489]。  
先進国のほとんどの主要電話会社は現在、SS7ファイアウォールを使用しており、ローミング契約に応じてリモートアクセスを許可または拒否しています。  
単一のユーザーからの苦情がある場合、フォレンジックは困難な場合があります。あなたができる最善のことは、ローミング料金を探すことです。  
しかし、銀行とその大規模なSMS請負業者は、SS7アクセスの料金をオペレーターに支払い、以前は閉鎖されていたシステムを開放しています。  
  
最近の電話ネットワークの次の主な脆弱性は、安全でない端末機器と機能の相互作用でした。  
エクスプロイトは、誰かをだまして割増料金の番号に電話をかけさせることから始まり、多くの人が変更することを望まないデフォルトのPINを介してジャーナリストやボイスメールをハッキングする他の人にエスカレートします。  
2011年、ニューズオブザワールドで働いていた捜査官、その後マードック帝国の英国の旗艦がミリーのボイスメールをハッキングし、その過程で警察の捜査を妨害し、彼女のメッセージの一部が削除された可能性があることが判明しました。ミリーの家族が彼女がまだ生きているかもしれないという誤った希望を与えている。  
しかし、安全でないエンドシステムを悪用する非常に大きな詐欺は、大きな電話代を支払う能力があるため、企業や政府部門を標的とする傾向があります。  
 1990年代半ばまでに大企業になり、年間数十億ドルの費用がかかっていました[467]。  
。  
ご想像のとおり、これらのPINは知られ、悪役と取引されます[1352]。  
多くの場合、PINはメーカーによってデフォルトに設定されており、お客様が変更することはありません。  
。  
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ったため、電話設置者を訴えました。  
犯罪者の動機の1つは、盗聴されない通信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ギャングが、中国の福建省から英国への不法移民の密輸を行っており、英国の評議会のPBXをハッキングし、それを使用して100万ポンドを超える中国への電話をかけました。議会は今や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。  
 そのような場合は別として、ダイヤルスルー詐欺は、ほとんどが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密談に巻き込まれています。  
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ー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抱えるPBX詐欺による損失の推定値は、2011年の49億6,000万ドルから2017年の38億8,800万ドルに減少しました。  
プレミアムレートのモバイルマルウェアは、ロシアに5ドルのSMSを送信してRed Browserワームがキャッシュアウトした2006年に到着しました[941]。これはAndroidが登場した後に拡大されました。モバイルマルウェアについてはセクション22.3.1.4で説明します。  
2000年代初頭以降、発信者番号IDのハッキング、SMSスプーフィング、SS7シグナリングへの攻撃が詐欺に使用される可能性があるという警告が出されています。  
  
電話操作には、機能の相互作用が含まれることがよくあります。  
 コレクトコールを自動的に処理するために導入されました。  
...電話の番号3を2回押してください。」囚人は、機械が記録して挿入するために彼らの名前を述べ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。」と言いました。これは、企業のPBXに到達し、オペレーターに外部回線を提供するように指示するのに十分な頻度で機能しました。  
•多くの電話番号照会サービスは、運転中にダイヤルできない運転手のためのプレミアムサービスとして、あなたに提供したばかりの番号にあなたを接続します。  
いたずらっ子は、通話禁止にもかかわらずセックスラインに電話をかけるのに使用し、いたずらな大人は、家族の電話代請求書に恋人の番号が表示されないようにするために使用します[1456]。  
昔は、子供たちが電話会社のオペレーターをソーシャルエンジニアリングして教師の電話をセックスラインに転送するなど、いたずらに使用されていました。  
たとえば、詐欺師は、一連の数字をダイヤルすることにより、被害者に銀行に電話番号を確認するように指示する可能性があります。  
•電話会議は、あらゆる方法で悪用される可能性があります。  
パートナーに保護観察サービスと携帯電話で電話会議を設定してもらいます。  
（そして、彼があなたに電話をかけ直したい場合、あなたはあなたのパートナーに電話を転送させます。）  
22.1.6 VOIP  
、音声トラフィックはデジタル化され、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、ほとんどすべての通話が「VOIP」になっています。  
最も一般的なVOIPプロトコルであるセッション開始プロトコル（SIP）  
セクション22.1.4で述べたように、企業のPBXシステムに対する詐欺のVOIPセグメントは、2017年までに年間約20億ドルでした[91]。  
企業のセキュリティポリシーにより、ファイアウォールがVoIPトラフィックの通過を拒否する可能性があります。  
FCCは2020年に、2021年6月末までに通信事業者がSIPを介して発信者を認証する一連のプロトコルSTIR / SHAKENを実装することを主張することを投票しました[326]。  
しかし、IPパケットストリームはどこからでも送信でき、サービス品質を保証するのに十分なインターネットを所有している人はいません。  
次に、モバイルネットワークにフォールバックする必要があります。  
  
電話詐欺は、電話会社に対して電話詐欺を犯し、電話会社が強化する本当の動機がないというメカニズムを利用して他の顧客を詐欺する詐欺的な顧客の話だけではありません。  
請求は、電話会社が独占的で、通常は国営であった時代に設計されたもので、電話会社が相互に信頼していると想定しています。会社Aが通話データレコード（CDR）を作成した場合  
（切り取られるので、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ので、妻が持っていた電話を呼び出してキャンセルしました。  
おそらく、スペインの電話会社は、彼らが以前に見た数に数回の請求を詰め込んでいただけであり、彼らは通常それを回避す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、彼のプライベートオフィスに問題を解決させ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、詐欺的な請求に対する「保険」を顧客に提供することでした。  
バリエーションはたくさんあります。たとえば、米国で800番に電話をかけた場合、会社は次のように言います。  
通話の進行中に音声プロンプトに応答した場合も同じことが起こります。  
詰め込みや叩きつけは、夜間の小さな飛行士だけで行われていると仮定するのは誤りです。  
彼らはテキサスの加入者の亡くなった配偶者の署名を偽造したときに捕まった。  
国内のプレミアムレート番号の悪用により、多くの国の規制当局は電話会社に加入者にプレミアムレート番号のブロックを提供するように強いました。  
セクション22.1.1でカリブ海の数字を使った詐欺について述べましたが、小さな国の多くの他の電話会社がこの法律に参加しました。  
 電話会社が国際的な目的地を選択的にブロックするのを防ぎます。  
ただし、これらは停止したようです。 2020年のロボコールに関する広範な研究では、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、価値の高いサービス提供の削減に慣れていました。  
スマートフォン革命によって多くの新しいサービスが可能になり、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。  
   
電話会社とケーブル会社は、固定費が非常に高く、限界費用が非常に低いです。  
経済学の章で述べたように、これにはいくつかの意味があります。  
長年にわたり、電話サービスはほとんどの国で「自然な独占」と見なされ、政府によって運営されていました。主な例外は、古いAT＆Tシステムが厳しく規制された米国でした。  
詳細は国によって異なりますが、一般的に、一部のセクター（携帯電話など）は  
 企業は自由に競争できました。その他（ローカルループプロビジョニングなど）  
第二に、競争部門（長距離電話など）  
一部のセクターはアプリによって競争力を高められました。SkypeとWhatsAppは基本的に無料で国際電話をかけました。  
ブロードバンドアクセスには、モバイルサービスとTVの提供が常にバンドルされています。  
ブロードバンドと携帯電話の料金を精査する時間がない場合は、不愉快な驚きが生じることがあります。  
22.2モバイル化  
2020年までに、50億以上の加入者がいます。 2019年だけでも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。  
発展途上国でも急速に成長が進んでおり、有線ネットワークはしばしば老朽化しており、人々は電話サービスを何年も待たなければなりませんでした。  
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。  
 使用されたアナログ信号とハンドセットは、シリアル番号をエアリンク経由でクリアに送信しました1。  
主な顧客の1つは、電話サービスを盗んで安価に再販するコールセル操作であり、多くの場合、移民や自宅に電話したい学生に販売されていました。  
通話販売市場は、匿名通信の犯罪市場によって補完されました。人々は携帯電話をハッキングして、通話ごとに異なるIDを使用しました。  
1G電話は音声トラフィックを暗号化しなかったので、誰もがラジオ受信機で通話を盗聴することができましたが、それでも発信者の匿名性の可能性が犯罪での使用につながりました。  
そのため、価格が上がり、パッシブリスニングと同様に、アクティブな方法が使用され始めました。  
モバイルは、信号が最も強い基地局を使用し、顧客が移動するときに、あるセルから別のセルにコールをハンドオフするためのプロトコルがあります。  
電話が通り過ぎるにつれて、彼らはより強い信号を聞き、シリアル番号とパスワードを送信して登録しようとしました。  
ほとんどのオペレーターは、侵入検知システムを実行して、急激な動きや、通話量や通話時間の急激な増加など、不審な活動パターンに注意しました。  
1米国のシステムでは、2つありました。1つは機器用で、もう1つは加入者用です。22.2.1 GSM  
 デジタル技術を採用。  
 1987年に15社がGSM協会に登録し、EUからの政治的支援を確保したときに設立されました。サービスは1992年に開始されました。  
彼らが何をしたか、どのように成功したか、どこで失敗したかは、興味深いケース履歴になります。  
これは機能しませんでした。一部は最終的にリークし、残りはリバースエンジニアリングによって発見されました。  
モバイルネットワークは無線アクセスネットワーク（RAN）で構成されています  
、および各モバイルネットワークには、ホームロケーションレジスタ（HLR）という2つのデータベースがあります。  
 他のネットワークからローミングしたモバイルの場所。  
ハンドセットは、Subscriber Identity Module（SIM）を使用してパーソナライズされた商品アイテムです。  
SIMは3つの数字を含むと考えることができます：1。  
国際的なモバイル加入者識別（IMSI）がある  
最後に、加入者認証キーKiがあります。これは、そのIMSIを認証するために使用され、ホームネットワークで認識されている128ビットの数値です。  
。  
。  
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と連結されることを意味します：{RAND} Ki =（SRES | Kc）  
とにかく、トリプレットはベースステーションコントローラー（BSC）に送信されます。  
これは、SRESを計算するSIMに渡されます。  
したがって、認証プロトコル全体は、図22.2のように実行されます。  
、...  
まず、ベースステーションは認証されないため、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ずに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。中には、スマートフォンをトイレに落として、保険が偶発的な損傷をカバーしていないため盗まれたと報告した加入者による保険詐欺があります。しかし、強盗が電話を取って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。  
ハンドセットのシリアル番号、または海外に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、警察があまり頑張らない場合にのみ警察から保護します。  
すでに述べたように、9/11首謀者の1人は、別のアルカイダのメンバーが使用していたものと同じバッチからのプリペイドSIMを使用したときにキャッチされました。そして、21/7のロンドン爆撃が失敗した後、1人は爆撃機でローマに爆撃し、そこで彼は即座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–ロケーションセキュリティと通話内容の機密性。  
、そのネットワークでそのアドレスとして機能します。  
2G GSMは、認証と登録が完了すると、受話器と基地局間のトラフィックを暗号化することで、通話内容の機密性も提供します。  
ヨーロッパで一般的に使用されているアルゴリズムはA5 / 1です。  
2000年代半ばまでに、法執行機関のサプライヤは1秒未満で鍵を割り込むデバイスを販売していたため、監視チームがすべてのGSMトラフィックをフーバーして復号化できるため、関心のある会話を見つけることができました。  
上記のセクション22.1.1で述べたように、コードレス電話のDECT標準はいくぶん似ており、弱点もあります。  
5オーストラリアがA5 / 2を使用していることが明らかになったとき、列がありました。  
パッシブバルクコレクションに加えて、ターゲットを絞ったアクティブコレクションはプロトコルトリックを悪用する可能性があります。  
しかし、最初のアルゴリズムネゴシエーションが平文であるという事実を悪用する落札攻撃があります。  
Elad Barkan、Eli Biham、およびNathan Kellerは、これを遡及的に実行できることを認識しました[171]。  
彼が終了したら、IMSIキャッチャーをオンにして、彼に偽のベースステーションに登録させます。したがって、携帯電話は以前と同じ鍵Kcを生成します。  
A5 / 2は廃止されました。 A5 / 1またはA5 / 3を使用できないハンドセットはプレーンテキストで通信します。  
電話会社、機器ベンダー、ISPは現在、地方の法執行機関へのアクセスを提供することを余儀なくされていますが、他の国もしばしばアクセスを望んでおり、傍受施設はしばしば悪用されて悪用される可能性があります[1707]。  
 は、ボーダフォンのギリシャのネットワークに組み込まれた盗聴設備を破壊することで、アテネオリンピック中にギリシャの首相とその国の約100の政治、法執行機関、軍事エリートの携帯電話を利用しました。  
同僚と私は数年前にこの問題について警告し[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、最終的な効果は、2G GSMセキュリティメカニズムが、A5 / 1の使用が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ている一方で、他の場所ではやや悪い保護を提供する一方で、どこでもやや悪い保護を提供しているためです。サードパーティが工業化できるエクスプロイトの範囲。  
22.2.2 3G  
 そして現在、第三世代パートナーシッププロジェクト（3gpp、またはちょうど3G）として  
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テクノロジーと、必要なはるかに大きなバックホール伝送をインストールすることが経済的ではありません。  
、3Gデータレートは数十万ビット/秒です。  
それはスマートフォン革命の基礎を築きました。  
暗号アルゴリズムA5 / 1およびA5 / 2は、Kasumi [1021]と呼ばれるブロック暗号に基づいてA3に置き換えられます。これは、現在20年にわたって公の監視に耐えてきたMistyと呼ばれる松井充による設計に基づいています。 1245]。  
暗号化は、コンテンツの機密性だけでなく、メッセージコンテンツとシグナリングデータの両方の完全性と機密性を保護するために使用されます。保護は、単にローカルの基地局ではなく、ハンドセットからコアネットワークまで実行されます。  
認証は一方向ではなく双方向になりました。  
実際には、対象の受話器に2Gオペレーションにフォールバックするように指示するだけで、問題なく機能します。  
基本的な3G認証とキー合意（AKA）  
ホームロケーションレジスタは現在、ホーム環境（HE）と呼ばれています。  
。  
{RAND} K =（RES | CK | IK | AK）  
MACはRANDとSEQで計算され、シーケンス番号は匿名キーで排他的ORすることでマスクされます。  
次に、VLRはUSIMにチャレンジ、マスクされたシーケンス番号、およびMACを送信します。 USIMは応答とキーを計算し、シーケンス番号のマスクを解除し、MACを検証し、それが正しい場合はVLRに応答を返します。  
 彼 ！ VLR RAND、XRES、CK、IK、SEQ ffi AK、MAC VLR！ USIM RAND、SEQ ffi AK、MAC USIM！ VLR RES図20.4 – 3gpp認証プロトコル3G標準は、IDとロケーションのプライバシーメカニズム、2Gとの下位互換性、HEからVLRへの転送中の認証ベクトルを暗号化するメカニズム、さまざまなオプションの暗号化メカニズムのネゴシエーションなど、他の多くの機能を定めています。  
多くの国では、第3世代の携帯電話は、戦術よりも大きな規模で運用するためにシステムをネットワークオペレーターのシステムと統合する必要があったため、最初の数年は警察が盗聴するのが困難でした。  
22.2.3 4G  
 2019年までに[981]。  
無線アクセスネットワークは、3Gのスペクトラム拡散から周波数ドメインイコライゼーション（FDE）に変更されました  
。  
2010年代に進化した標準のファミリが実際にあり、メガビット/秒から数十メガビットまでの帯域幅をサポートしています。  
認証とキー合意（AKA）  
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。  
基地局機能はEvolved NodeB（eNodeB）に分割されています  
、AKA交換を処理し、アドミッションの決定を行い、基地局にセッションキーを提供し、法執行機関のアクセスを処理します。。  
 引き継ぐことができる人なら誰でも監視できます。ユーザー機器のIDがクリアテキストでネットワークに送信されるか、グローバルユニークテンポラリーID（GUTI）を使用してマスクされること  
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ているため、同じタイプの攻撃の多くに対して脆弱です[426]。  
リッチコミュニケーションサービス（RCS）  
SMSを地理位置情報交換、ソーシャルプレゼンス情報、Voice-over-IPなどの豊富なチャット機能に置き換えることを目的としています。  
電話会社が正しく構成していないため、初期の実装の多くは安全ではありません[1696]。  
それでも、米国のロシアのエージェントがプッシュトゥトーク携帯電話を使用したFBIの諜報活動エージェントの通信を危険にさらしたことが判明したとき、この戦略は打ちのめされました[579]。  
彼らはまた、バージニア州ラングレーにあるCIA HQへの視線を備えた施設を取得することに夢中になっていた。  
22.2.4 5G以降  
現在の主な推進力は帯域幅です。モバイルトラフィックは2018年第3四半期から2019年第3四半期の間に主にビデオから68％増加し、2025年までに25％を超える成長が見込まれており、そのときまでに世界中のトラフィックのほぼ半分が5Gになります[981]。  
初期展開では非スタンドアロンモード（NSA）を使用します  
 しかし、データレートを向上させます。  
 後に続きます。  
。  
可用性は最優先事項です。 2016年のブリュッセル爆破事件の後、警察は渋滞のために電話でネットワークサービスを利用できず、互いに話し合うためにwifiホットスポットを見つける必要がありました。  
各小さな基地局は分散ユニット（DU）になりました  
、これもフィールドにありますが、コアネットワークの一部としてカウントされます。  
、MMEボックスを置き換えます。  
。  
デバイスを前世代のテクノロジにダウングレードする中間者攻撃を含め、偽の基地局によるパッシブおよびアクティブな攻撃は依然として可能であり、エネルギークリティカルなデバイスのバッテリーを使い果たす可能性があります[1712]。  
モバイルネットワークオペレーターは、使い慣れたテクノロジーを守る代わりに、彼らが理解していない新しいテクノロジーに依存し、どれが最も安価なベンダーから購入するだけになります。  
諜報機関はこれを打破するために、ビッグデータキャリアと提携してロビー活動をしていると聞いています。  
コアクラウドネットワークでSDNを使用すると、さらに多くの疑問が生じます。最も厄介な長期的な問題は、5Gが最終的なラウンドネットニュートラルになるかどうかであり、ネットワークオペレーターが各アプリケーションへの提供をパフォーマンス（および価格）でカスタマイズできるようにします）  
一方、仕様は複雑で、実装は不安定です。  
理論上、交通編集は編集を行う会社によって署名されますが、誰がそれがどのように機能するかを知っているようには見えません。  
 重大なサプライチェーンリスクが2010〜19年にかけて発達したことを指摘し、市場の推進力は適切な対応を保証するには不十分であった[1393]。  
長期的な解決策は、「ベルヘッド」と「ネットヘッド」の間の3番目の問題に依存する可能性があります。コンピューター業界では、クラウドに入ると、見えているものすべてを喜んで仮想化します[609]。  
 テレコムの研究者たちは、ピーク時の帯域幅、待ち時間、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これまでの進化について話します[1454]。後者には、地球の表面全体に200Mbpsのブロードバンドを展開するために数千のマイクロ衛星が搭載されています。  
 自動運転車は超低遅延のクラウドサービスの需要を生み出すため、Google、Facebook、Microsoft、Amazonが運営する数十のデータセンターにデータを送信するのではなく、各町にサーバーのクラスターを備えたエッジクラウドが見られる場合があります。 、おそらく古い電話交換機を収容していた建物の中にも。  
  
使用中の無線リンク技術の世代に関係なく、その根本原因が業界の経済性と規制にあるMNOのいくつかの一般的な障害があります。セクション22.1.3で説明したSS7のセキュリティ問題（有線通信会社にも適用される）に加えて、モバイルの世界では、SIMスワッピング、チャネルジャック、認証アプリからのCookieの盗難が発生しています。  
セクション3.4.1で、SIMスワップ攻撃を導入しました。攻撃者は、被害者の電話会社に被害者のアカウントで新しいSIMカードを発行するように説得します。  
セレブリティがターゲット：2019年のアウグストで、TwitterのCEOであるジャックドーシーは1時間アカウントを引き継がれ、人種差別や反ユダヤ主義のつぶやきを送信していたため、コメンテーターはトランプ大統領のTwitterアカウントを乗っ取った誰かが第三次世界大戦を開始するのではないかと考えました1340]。  
しかし、電話会社の反応はせいぜいばらばらです。  
しかし、すべての対策がすべてのユーザーに役立つわけではありません。それらがオプションである場合、会社はそれらを使用しないことを選択した顧客による損失をより簡単に否認できます。  
電話会社は、第2要素SMSへの応答としてIMSIのハッシュを送信することにより、依存パーティがSIMスワップを検出するのを支援することもできます。しかし、そうする人はほとんどいません。  
実際、ほとんどの国のほとんどの顧客は前払いの顧客であるため、状況はさらに悪化する可能性があります。  
2013年、Karsten Nohlは、使用中の多くのSIMは、無線によるソフトウェアの更新を容易にするために組み込まれた機能により、簡単に乗っ取れると警告しました。  
2019年に、政府がこれを監視に使用していたことが明らかになりました[1107]。  
容疑者の携帯電話のブラウザーが暗号化されていないURLにアクセスすると、MNOが代わりに警察マルウェアを提供します。  
この慣行は、あまり発展していない国々で始まりましたが、現在ではドイツ[1443]まで広がっています。  
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ました–インフラを維持しなければならないが、彼らが楽しんでいた独占利益を他人にクリームオフされるのを見ているビットシフター。  
22.3プラットフォームのセキュリティ  
これらはいくつかの問題を修正し、他の問題を引き起こします。最も深刻なセキュリティ問題は、プラットフォーム自体が信頼できるかどうか、またはあなたの電話があなたの利益に反するかもしれないかどうかです。  
裏話については、2007年の現状を説明した私の本の第2版を参照してください。  
MNOは、OEMが顧客と何らかの関係を持つことを拒否しました。  
アップルは一度にいくつかの方法で世界を変えました。  
次に、サードパーティベンダーがアプリを作成するのがはるかに簡単になりました。  
これには、セミクローズドプラットフォームが必要でした。  
その効果は、MNOからAppleにパワーをシフトすることでした。  
彼らは、生態系が成長できるように、最低限の信頼を提供することを目指していました。  
これは最終的には起こりませんでした。現在、いくつかの方法で収束した2つの大きなエコシステムがあります。  
iPhoneとAndroidの両方が、私がAccess Controlの章で説明するセキュリティアーキテクチャでリリースされました。どちらのアプローチも、アプリを互いに分離し、それらがプラットフォーム自体を破壊するのを防ぐことを目的としています。  
画面への直接アクセスが拒否されている場合でも、サイドチャネルの章で、たとえば、スマートフォンの加速度計とジャイロを使用して、別のアプリに入力されたパスワードまたはPINを調べる方法についても説明しました。  
AndroidとiPhoneの両方のセキュリティメカニズムは、時間の経過とともに改良され、より悪質な不正行為をブロックまたは軽減するために追加のコントロールが追加されました。  
このエコシステムは本当に巨大です。  
少なくとも、モバイルデバイスの2つのファミリ自体で実行されるアプリと、それらが依存するバックエンドサービスで構成されます。  
アプリデベロッパーが自社の製品にバンドルする広告エコシステムを含める必要があります。  
 WhatsApp、Skype、Signalなどのアプリに移行するので、音声テレフォニーを含めますか？  
 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。  
22.3.1 Androidアプリのエコシステム  
そのプラットフォームセキュリティモデルは、GoogleのRen´e Mayrhoferと同僚によって[1252]で説明されており、セクション6.2.8で技術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は各ユーザーIDで各アプリを実行します。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あることを保証する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。ユーザーがだまされて悪意のあるアプリをインストールすることが想定されています[1252]。  
。  
これにより、有料アプリとアダルトアプリの多くのベンダーが、OEM契約、サードパーティストア、自社のWebサイトなどの安全性の低い配布チャネルを使用するようになりました[1823]。  
さらに多くのアプリは、たとえハードウェアベンダー、MNO、セキュリティファームなどの立派な立派な企業によって配布されたとしても、多少略奪的です。  
主な結果の1つは、Androidがプライバシーに関する最も重要な権限をサポートしていないことです。つまり、ユーザーはアプリのインターネットアクセスを制御できます。  
 そうしないと多くのユーザーがフラッシュライト/ゲーム/コンパスアプリをインストールしたときにインターネットアクセスをオフにしてしまうため、これは広告会社を喜ばせます。  
しかしもちろん、ほとんどのユーザーはデフォルトのままで、広告エコシステムにほとんどすべてのものを収穫させます。  
22.3.1.1アプリ市場と開発者  
Androidエコシステムはオープンであるため、誰でも開発者になり、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、潜在的に有用な方法で開発者を制約します。  
ただし、開発者は技術面とビジネス面の両方で複雑に直面します。  
しかし、その機能はどの程度均一ですか？  
 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？  
たとえば、コロナウイルス用の連絡先追跡アプリを開発している人々は、さまざまな携帯電話間でのBluetoothパフォーマンスのばらつきに苦労しています。  
Armは、開発者がTrustZoneを使用することを期待していましたが、OEM、ハンドセット、およびソフトウェアバージョン間のバリエーションを考えると、これは非常に困難であることがわかり、ほとんどが難読化に変わりました。  
一部の開発者は、電話を根付かせてアプリのふりをするマルウェアをブロックすることを期待して難読化を好みます。 12.7.4節で述べたように、一部の銀行規制当局はこれを主張しています。  
、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異なるインセンティブを持っています。  
ユーザーを識別するためのルールは複雑です。一部のUID（IMEI、IMSI、電話番号、広告ID）を使用するには、ユーザーの同意が必要です  
  
2010年頃にAndroidが広く普及するにつれ、最初に明らかになった体系的なセキュリティ問題のバンドルは、ライセンスを供与した多くのOEMによるエンジニアリング作業の質の低さでした。  
裕福なユーザーが最新モデルを購入し、古い電話が売られてしまうため、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がどのように構成されているかに関するすべての相互作用があるため、これを正しく行うのは困難です。埋め込まれたマルチメディアカード（eMMC）があるかもしれません  
OEMのエンジニアが安全な削除の実装に手間をかけない場合、あまりにも一般的な結果として、携帯電話を直接購入した人がGoogleマスターCookieを取得し、その携帯電話に関連付けられたGmailアカウントにアクセスできるということです[1757 ]。  
（LDCのAndroidフォンがルート化され、ローカルディストリビューターによってリモートアクセストロイの木馬がインストールされていると想定することは賢明です。）  
、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ます。  
 ホストOSのメモリ領域にマップし、その結果、安全でないTAが敵にデバイスをルート化させる可能性があります。  
これらの問題の調査については、David Cerdeiraとその同僚[403]を参照してください。  
多くのOEMは、現在積極的に販売されているバージョンのみをサポートしています。彼らは、エンジニアが修正を古いバージョンにバックポートすることに時間を費やすことに消極的です。  
多くの場合、OEMはフィックスを利用可能にしませんでした[1880]。  
Googleは現在、ベンダーとアプリの両方に認定プログラムを提供していますが、問題はOEMエンジニアリングの取り組みだけではありません。  
これらの各ステップには数か月かかる可能性があり、商業上の理由から無視できる場合もあります[1880]。  
  
アクセス制御の章で述べたように、同意は最初から邪悪な問題でした。  
ほとんどのユーザーはインストールを完了するために承認をクリックするだけであり、多くのユーティリティアプリがアドレス帳、ブラウザの履歴、およびその他の個人データを収集して再販するためのマシンになったため、これが悪用の拡大につながりました。2015年、Android 6は、最初の使用時にそのようなリソースへのアクセスを承認するAppleモデルに移行しました。  
Android 6では、きめの細かい位置情報へのアクセスも個別の権限になりました。 Android 7は、他のアプリのメタデータへのアプリのアクセスを制限しました。 Android 8はMACアドレスをランダム化し、収益化のために単一の広告IDの使用を義務付けました。 Android 9では、アプリがバックグラウンドモードの場合、センサーへのアクセスが制限され、電話や通話ログへのアクセスが制限されていました。 Android 10では、バックグラウンドモードでの位置情報へのアクセスが制限されています。  
これらはエコシステムをさらにバルカン化し、ユーザー（および開発者）をさらに困難にします  
Yasemin Acarと同僚による同意問題の分析は、それを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解します[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。別の場所でこれを記録しました（例：  
 しかし、開発者が有用な作業を行うためにアプリケーションフレームワークAPIを駆動する必要があるため、適用されるエコシステムでは大きくなります。  
Googleはフェイルセーフのデフォルトを実装できませんでした。 APIはわかりにくく、文書化も不十分です。  
  
Androidは誰でもアプリを作成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集めています。  
多くのアプリは、少なくとも一部の人にとってはさまざまな方法で有害であるため、ここでの定義は困難です。ここでは、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。  
マルウェアは大量に存在する場合もあれば、標的にされる場合もあり、民間の犯罪者や国家関係者に由来する場合もあります。  
Playストアの数百万のアプリと同様に、代替マーケットは、特にPlayストアが検閲されている中国やイランなどの国で広く使用されています。  
マルウェアの最大の単一発生源はPlayストアであり、かなりの数のアプリが有害な場合がありますが、一部の代替市場では、有害なアプリのほとんどが削除されることがあります。  
最近公開された最大の犯罪リングの1つは、Androidアプリを購入し、ユーザーデータを使用してボットを訓練し、その後広告をクリックすることにより、数億ドルの広告詐欺を行いました[1738]。このような詐欺は、他の種類のマルウェアも悪用します。  
一度に数百の家族が活動しています。  
2012年以降、それらのほとんどは再パッケージングに関与しており、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、リモートアクセストロイの木馬（RAT）をドロップしようとする可能性があります。  
収益化戦略は進化しました。 2010年はプレミアムレートの電話をかけることに重点が置かれていましたが、2018年には広告詐欺と個人情報の漏洩に移行しました。  
。  
。  
一般的なアプローチは、マルウェアがユーザーをだましてAndroid Accessibility Servicesの使用を許可するオーバーレイ攻撃です。これにより、オーバーレイを構築できます（例）  
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年の最新の開発は、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、ルートアクセスも要求しますが、スパイウェアを埋め込みます。  
大量のState-actorマルウェアには、管轄区域によっては、アプリの修正バージョンを義務付けることが含まれます。 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Skypeを再パッケージ化した地元のディストリビューターであるトムオンラインを通じてのみ、2005年から中国で利用可能でした。  
技術的な不正行為があり、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きます。  
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を発見しました。  
  
携帯電話アプリは通常、クラッシュレポートからA / Bテストまでの幅広い目的で広告、ソーシャルネットワークの統合、分析をサポートするサードパーティサービスを組み込んでいます。  
問題の原因の例としては、1億人以上がダウンロードしてドキュメントをスキャンおよび管理するアプリであるCam- Scannerがあります。否定的なレビューにより、ウイルス対策研究者が調査を開始し、モジュールがトロイの木馬を人々の電話にドロップしていることが判明しました[796]。  
Abbas Razaghpanahと同僚が行った、11,000人のボランティアが使用するVPNアプリを使用して、電話の送受信トラフィックを監視する調査によって、いくつかの光が当てられました[1586]。  
、これまでに報告されていない数百を含み、かなりの少数派（39％）  
トップ10のうち8つは、プライバシーポリシーにおいて、他の組織とデータを共有する権利を留保しました。  
アプリ開発者は、多くの場合、このようなサービスをいくつか同時に使用します。  
相互信頼の問題は、Yasemin Acar氏と同僚[10]によって議論されています。  
広告ライブラリは、Webサービスから安全でないコードを読み込んだり、ユーザーの個人情報を盗んだりするなど、さまざまな方法でアプリを悪用します。アプリ開発者は、マルウェア開発者と同じように、偽のクリックイベントでネットワークからお金を盗むことで、褒め言葉を返します。  
 米国の児童オンラインプライバシー保護法（COPPA）に反して、児童アプリが保護者の同意なしに個人データを収集する例は多数あります  
さらに悪いことに、アプリの19％は、これを子供向けアプリで禁止するSDKを使用して個人を特定できる情報を収集していました[1599]。  
EU GDPR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 Han氏と同僚は、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がデータ収集に関して同様に略奪的であることを発見しました。別の6番目は、同じデータの少なくとも一部を収集しました。 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。  
  
ジュリアンガンバらは、世界中の200以上のベンダーが配布するファームウェアを研究しました[741]。  
彼らは不十分に制御することができます。マルウェアが侵入する複数のケースがあり、商業的または規制上の理由で大規模なデータ収集を行うソフトウェアもあります。  
プリインストールされているアプリのほとんどはPlayストアで入手できないため、従来のフレームワークの範囲外にあるように見えます。  
さらに、非公開アプリの74％は更新されていないようで、41％は5年以上パッチを当てていませんでした[741]。  
行動分析の結果、プリインストールされたアプリのかなりの部分が、ユーザーIDとデバイスID、構成、および現在地にアクセスして配布できることがわかりました。  
一部のプレインストールアプリ（特に安価な電話）には、ユーザーが簡単に削除できないコンポーネントがシステムパーティションにあり、迷惑な広告を配信したり、トロイの木馬のローダーとしても機能します[1109]。  
22.3.2 Appleのアプリエコシステム  
MacがPCと競合していたとき、それは多くのOEMに対する1つのハードウェアプラットフォームでした。同じパターンがiPodにも続き、Appleは音楽の売り上げの30％を要求し、AppleがiPhoneを発売したときもそれは続きました。  
アップルは唯一のハードウェアベンダーであり、ソフトウェアの収益の30％、およびオンラインの商品やサービスのアプリ内購入の30％を要求しています。  
 これは独占禁止法の問題になりつつあります。  
match.comのような出会い系サイトが売り上げの30％を渡さなければならないのに、Uberは渡さないのはなぜですか？  
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、パンデミックのためにオンラインアプリにアクセスしたミュージシャン、フィットネスインストラクター、ヨガの教師などの人々がiPhoneアプリで予約した場合、「アップル税」が課されました。  
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の審査プロセス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に続いて、アプリが支払い、コンテンツ、不正行為などに関するAppleのポリシーに準拠していることを確認するための手動審査があります。  
そのため、学術研究者はiOSエコシステムを深く掘り下げていますが、それでもいくつかのことが言えます。実際、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価値の高い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：銀行の認証アプリを実行して支払いをリリースするiPadを購入し、それだけを使用してください支払いのために、残りの時間は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Appleデバイスを「脱獄」したという長い歴史があります。  
デバイスのブートROMを悪用する場合など、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年以前に販売されたほとんどのデバイスを解放し[798]、フォレンジック業界は、4SからX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[798]。これは、セクション26.5.1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。  
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2.2.4で、UAEがこのようなツールを使用して反体制派を標的とした方法と、サウジアラビアがJeff Bezosに対してどのように使用したかについて説明しました。サウジアラビアはまた、地域のライバルであるカタール国王をハッキングしました。  
Appleは常にそのようなエクスプロイトに迅速にパッチを適用するため、数百万人がアクセスできるのは少数のターゲットだけです。  
これにより、悪用やスパッツが発生し、Facebookのエンタープライズ証明書は、アプリがApp Storeのポリシーへの違反を停止するまで停止されました。 iPhone上のGoogleのアプリでも同様の経験があり、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。  
悪意のある行為者の多くは、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、企業認定を取得していました[1170]。  
したがって、iOS用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1つの方法です。  
マルウェアの問題はAndroidほど深刻ではありませんが、同じ市場勢力が適用されるため、依然として広告の乱用が発生しています。  
 広告主と多くのデータを共有し、Appleエコシステムで許可されています[1762]。  
1つの例では、広告SDKを使用すると、そのSDKを使用し、300mのiPhoneにインストールされた1,200個のアプリからクリックを盗むことができます。そのコードにはステルス機能があり、アプリレビュープロセスを通過するのに役立つ可能性があります[1314]。  
 そして、人々は、アプリを表示しない有料アプリはあなたを追跡しないと想定しています、そのような期待は両方のエコシステムで楽観的かもしれません。  
Appleで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、あなたはそれが時々リスニングデバイスとしても機能し、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考えたほうがいいでしょう。  
Appleは、Googleと同様に、アプリが必要とする権限を徐々に厳しくしています。  
2020年9月から、iOS14は広告主（IDFA）の識別を変更します  
2つの店はいくつかの政治的問題を共有しています。たとえば、セクション2.5.4で説明したように、サウジアラビアの男性が使用するアプリが妻、娘、使用人の動きを制御できるようにしたなどです。  
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、アプリはユーザーが法執行機関を回避することを可能にしました」、一方GoogleはAndroidのバージョンをアップのままにしました[1253]。  
2020年2月、シンガポール政府は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。この1週間で会った。  
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、コンタクトトレーサーが処理する必要のある誤警報の数が大幅に増加します。  
これが4月に報告された時点で、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でも、連絡先追跡アプリの開発を始めていました。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顧客へのプライバシーリスクを挙げました。  
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]。  
  
2つのエコシステムの収束により、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ーを開始したAmazon Alexaのエコシステムです（このカテゴリーは急速に成長し、スマートフォンでは8人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）。  
これらのデバイスの多くは、アプリのエコシステムをサポートするようにも設計されていますが、数や使用方法は製品によって異なります。  
簡単に言えば、何十億もの人々が彼らの金融生活、彼らの社会生活、そして彼らのセックスライフさえもアプリに委ねるとき、それから不十分に書かれたアプリは本当の害を引き起こすことができます。  
ここでは、状況を説明するために1つの例で十分です。  
実際、支払いアプリの設計を支援する際、セキュリティエンジニアリング時間の約半分を費やして、盗まれた電話にどのように対処するかを詳細に検討しました。さまざまな利害関係者からアラートが届いたときに支払いをすばやくブロックする方法、犯罪の被害者が翌日に店に入って新しい電話を購入した場合、電話店に認証を依頼するか、銀行の請負業者に電話をかけるか、どのようにして電話のOEMに対処したか独自のバックアップおよびリカバリサービス–心のこもった詳細の絶対的な塊。  
十分な注意を払わないとどうなるかという私の例は、レンタカーを追跡、ロック、ロック解除、エンジンを始動できるようにするアプリ、FordPassです。レンタルロット[794]に返却。  
不適切に記述されたアプリからの脅威は、機密性、完全性、可用性のすべての範囲をカバーします。  
2022年1月から、自動車や洗濯機などの耐久財と共に提供される電話アプリは、これらの製品の最後がショールームを出てから10年間維持する必要があります。  
  
電話セキュリティは魅力的なケーススタディです。  
そもそも、システム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のは簡単でした。  
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に対する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にまで及びます。  
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、特に5Gインフラストラクチャの制御をめぐって、重大な政治的闘争の対象となった非常に複雑なグローバルエコシステムにつながりました。  
Androidエコシステムは、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によって提供されるアプリや多数の専門ツールまで、何十万もの開発者を引きつけてきました。  
両方のエコシステムで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おらず、したがって安全ではないため、技術的なプラットフォームのセキュリティレベルではなく、エコシステムのレベルで大掛かりな作業が行われています。  
私たちは、過去10年間、携帯電話アプリのエコシステム、主に問題のほとんどが発生するAndroidの部分で多くの問題を調査してきました。  
これらの新たな新興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。  
さらに読む世界の電話システムに関する情報は、かなり重い作業になる可能性があ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が、関連する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の優れた書籍や調査報告書は知りません。