私たちは皆、世界は私たちの岸で終わったと思っていました。  
電子透かしを理解したくなかった紙幣のインクの化学者、および機密性についてのみ話すことができる暗号学者は、着実に原始化されました。  
 そして、これらは実際の人々によって、そしてしばしば地球規模で使用されているので、私たちの分野は人文科学と社会科学も受け入れています。  
 また、攻撃がハードテクノロジーからそれを使用する人々に移行するにつれて、システムはエラー、ミス、さらには強制に対しても回復力を備えている必要があります。  
 実際のシステムが信頼性を提供する方法はますます多様化しており、保護の目標はアプリケーションに近いだけでなく、微妙で複雑になる可能性があります。  
2001年から、永続的なセキュリティ障害の多くがインセンティブ障害であることに気づき始めました。ボブが失敗のコストを支払う一方で、アリスがシステムをガードすると、トラブルが発生する可能性があります。  
 2008年の第2版では、障害のユーザビリティについても次第に説明されており、その後10年でセキュリティ心理学に関する多くの研究が行われました。  
まず、複雑さ。  
 高速道路や砂漠でうまく運転できるように車をプログラムすることはできますが、予測できない人々がいる雑然とした街並みには対応できません。  
 そして、いじめには限界があります。 「コンピュータはノーと言う」は顧客を失う速い方法です。  
第二に、持続可能性。  
 自動車、ペースメーカー、変電所などの耐久性のある商品では、ソフトウェアを20年または40年も維持しなければならない場合があります。  
 いわゆる「スマート」デバイスは、多くの場合、「コンピュータがノーと言った」ときにすぐに捨てなければならないものです。  
 セキュリティはスカラーではなく、関係です。  
 「コンピュータがノーと言う」ときに誰が負け、誰が得るか？ソーシャルネットワークユーザーはプライバシーを取得しますか、それとも広告主はアクセス権を取得しますか？お金を政治権力に変えるためにどのように使用されますか？また、人々が信頼できるインターネットやサイバー犯罪の発生率が低いなどの公共財が必要な場合、これらをグローバルな世界でどのように提供できるでしょうか？テクノロジーが変化した10年以上にわたるサイバー犯罪の安定性は、テクノロジーに関する根本的な問題ではないことを完全に示唆しています。  
 Facebookが政治的スピーチの裁定者になったとき、AppleとGoogleがコロナウイルスの連絡先追跡に関するポリシーを指示できるとき、そしてAmazon、Microsoft、Googleが顔認識（中国以外）に関するポリシーを指示するとき、私はテクノロジーの人々が政治科学について読み始めるべきだと思う、ならびに経済学および心理学について。  
個人が経験を通じて学ぶことができるのと同じように、私たちの社会も学び、適応します。  
 したがって、エンジニアが貢献できる重要な方法は、政策論争に参加することです。  
セキュリティエンジニアリング951ロス・アンダーソン