Questions 4月25日(水)

1. Googleなどのサーバーを使わずに通信をするために全員が独自のサーバーを作るとなるとそれはそれでエネルギーの効率なども悪くなると思うのですがいい設計法などはあるのでしょうか

   ➔ **集約した方が一般的には効率は良くなる。しかし、事故対応は大変になったり。**

2. なお、暗号化の部分について、「平文と暗号文は1対1」という関係は必ず成り立つ、といえませんでしょう。異なる平文は、必ず異なる暗号文は（単射）ですが（復号の条件）、同一平文、key、暗号化関数を使っても、異なる暗号文になることがありえます。Nonce/IV を使って「リプレイアタック」と「複数のメッセージを眺めてパターンを見つけること」を防ぐ場合、Nonce は暗号化のとき、毎回乱数から生成しますため、出来上がった暗号文も異なりますでしょう。

   ➔**One Time Password（使い捨て）と同じですね。これは、公開鍵暗号における セッション鍵ともほぼ同じですね。セッション鍵は、One-Timeでの使い捨て。**

   ➔**平文のシンボルから 複数の暗号化空間のシンボルへの対応を行う方法は不可能ではないけど、逆写像が可能でないとね。**

3. 公開鍵暗号での、秘密鍵方式の暗号化はワンタイムパスワード方式であることを理解した。

4. 今の発展した暗号化技術が生まれる前はインターネットは危険すぎて使い物にならなかったのではないでしょうか。
   ➔ 悪い人が {ほとんど} いない 空間だったかな。
5. 病院のシステムがあまりセキュリティが考慮されていないという話は意外だった。 ➔ とても 酷い 状況なのよ。
6. 安全ではなく安心だという話は、サイバーセキュリティに限った話ではなく、日常会話でもよくあることですね。保守的人種は、一度うまくいったなら次もうまくいくという神話を信じる傾向が強いため、安全とはいえないことでも安心できるからと継続を要求してきますね。さらにタチが悪いのは、彼らはその神話を合理的なものだと勘違いしているため、ただの「安心」だということを認めたがらないのですが、真っ向からそれを指摘すると怒られるので、ほどほどに控えています。

   質問：この2つの言葉(安心 と 安全)の使い分けはサイバーセキュリティの分野では一般的なものなのでしょうか。サイバーセキュリティの分野についてあまり精通していないので、初歩的な質問ですが理解を深めたいと感じました。

7. 漫画村が社会にとって利をもたらしていることは考えもしませんでした。
8. 様々な方向から一様に情報を受け入れるだけでは物事の判別をつけてはいけないのかと改めて感じさせられました
9. 将来的に多くの個人のPCにAI用のチップが載るというような話があった。これは電力の輸送コストよりも情報の輸送コストが小さいことを利用しない例であるように思えて、何か情報を明かさずとも、つまり暗号化した状態でAIを利用できる方法があると便利だろうなと思った。
10. ブロッキングの話題の通信先等の閲覧に関して、サイバー攻撃の捜査的な側面ではどのように考えられているのか興味を持った。
11. セキュリティやプライバシーにおいて何かを守るために行動すると他の何かが危険に晒されてとイタチごっこのような形になってしまう形式は致し方ないものだと思うが、それを完全に防ぐには絶対的正義が必要なのだと思った。しかし、そのようなものないので安心を最大化することに力を入れるしかないという現実が少し悲しくなった。

➔ **絶対的正義 という言葉には 注意が 必要だね。**

12. Googleアカウント等のログインにおいてワンタイムパスワード・2段階認証が必要になったのは最近のことだと認識しています。初めから2段階認証を登録しなかった理由が知りたいと思いました。

➔ **面倒じゃない？**

13.漫画海賊版サイトの規制について、海賊版サイトを規制するためのブロッキングがそれ以外の目的にも使われてしまうのでできない、という点がネットワーク規制の難しい点だと思った。何か１つを規制しようにも一蓮托生で他分野の利用にも関係してしまい実質的に何も規制できない、という現状に対応しないとインターネットはより無法地帯になってしまうと思う。インターネットは現実世界よりもさらに結びつきが強く（ボーダーレスで）規制が難しいですが、どのように規制を行えばよいのでしょうか？

➔ **知恵を絞らないとね。 自由の確保は、大変 難しい 課題。**

14.いつも思うのですが、クレジットカードの裏にセキュリティコードが書いてありますが、クレジットカードを発行する時に書類でコードを送り、裏には載せない方が安全だと思うんですけどなぜ裏にコードを乗せているのですか？

15.節度ある自由のために，秘匿が存在するのだろうか。