Q&A 5月14日 分

インターネット工学概論

1. 回線交換とパケット交換の話で、基本的にはパケット交換の方がメリットが多そうに感じたのですが回線交換のメリットもいくつか教えていただきたいです。
   ➔ もはや ほとんどない ですね。。。。
2. 階層プロトコルによって役割分担をしているという話は、実際の仕事にも通じるものがあり、興味深いと思った。
3. セキュリティの鍵交換の部分で、次の鍵を暗号化して送っても、一度突破されればその後の通信は(鍵もバレていると思うので)全部筒抜けになってしまうような気がしましたが、その点はどういった対策があるのでしょうか？
   ➔対策は、鍵を変えるしかないですね。
   ➔筒抜けになっていた期間のデータによる被害をどうするか。。。。
4. 『070-で始まる電話番号は電話網で回線交換をすることによって高品質な通信が可能になっているものの、震災などで電話局が壊れると通信ができないため、災害時には使わない。その代わり、ラインなどのデータを小包にして送りつけるパケット交換によって情報通信をする場合、中継局が壊れても迂回して通信が継続可能になるため災害時の連絡手段に使われる。』という旨を聞いたとき、なるほどと思い、ハッとしました。
5. プライバシーという主観的な概念が、客観的で二次的な扱いを求められているという点は確かに難しいところだなと感じました ありがとうございました 。

6. 今日の講義では、セキュリティとプライバシーの違いについて学べた。特に「安心」と「安全」の違い、そして共通鍵と公開鍵の違いは興味深いポイントだった

7. 通信プロトコルの階層について、なぜOSIモデルではなくTCP/IPモデルが使用されるようになったのかが知りたい。

   ① 国際標準は、妥協・Deal で、決めることになる。

   ② 理論屋さんが作ったものは、実際には、動かない。

   ➔TCP/IP は、”we believe in running code”で、動くものを最重要視・必須の条件にした。

8. バケツリレーで例えられるのであれば、回線交換方式よりもパケット方式の方が速度がかなり落ちそうだと思いましたが、実際どうなんでしょうか。

   ➔“多少”遅延は大きくなる。 遅延の揺らぎもある。 ＝ 通信品質

   ➔ でも、、ほとんどの コンピュータ アプリケーションは、あまり、気にしないアプリだった。

9. 暗号は、時間を掛ければ解けると言うことですか？安全性が本当に担保されているのか知りたいです。

   ➔ 暗号は、安心しか 提供していません。 安全は、提供していませんし、提供できません

10. クライアントとサーバーの中間(中継)部分を統一することで、エンドとサーバーは物理的・技術的に多様な形態をとることができるという設計思想は面白く、会社同士の取引をアナロジーとする階層構造の話も非常にしっくり来た。 エンドとサーバーが多様な形態をとることを認めるこの形は、ある技術のみに着目したときに、それに特化した方法論をとるよりもどこかで無駄や面倒が生じていると思う。つまり例えば、エンドとサーバーのあいだの通信技術をケーブルによる通信のみに限定すればよりケーブルによる通信に特化・最適化された運用を行えると思う。インターフェース、階層構造という考え方は本当に最適なのだろうか。

    ➔ 局所的な 最適化は、将来の環境変化に 対応することが 難しくなってしまう。短い時間軸では、モジュール化を行わない方法をとりたくなる。 他の 人に邪魔されたくない(新規参入させたくない)場合には、モジュール化をしたくない。 内部(うちわでは)では、モジュールかしていても、これを公開しない。できる ある部分で 優れたものがでてきたら、これを友にしたくない ？

11. 現在、追加のセキュリティ対策としてワンタイムパスワードを利用していますが、今のところ私自身が扱う情報にそれほど重要性を感じていないため、現時点ではセキュリティの強度よりも、ユーザーとしての利便性を重視してしまいます。

    ➔気持ちは、よくわかります。 事故を経験すると、変わります。

    ➔PPAP は、意味ないことは、みなさん ご存知の通り。。。

12. 公開鍵を用いた暗号方式において、公開鍵を渡した人が確かに秘密鍵の保持者であると保証する複数の第三者の存在が大切であることはわかったが、第三者がハッキングなどの攻撃を受けた際その第三者が保証していた人全てに影響を与えてしまう危険性があると感じた。

➔ なので、とても 重要な Trust Anchor Point になります。 これは、1つだと不安ですね。

13. 海底ケーブルによる通信よりも、衛星通信の方がコストパフォーマンスが高いように感じます。それでもなお、海底ケーブルの新設が進められているのはなぜなのでしょうか？

➔衛星の信頼性とコストが小さくなったのは、本当に 最近ですね。

➔さらに、通信容量は、はるかに小さいです。

14. 以前の講義で紹介されたように今後、現在使われている物理的な鍵はインターネットを介したものに変わっていくのでしょうか。現実的にはむしろインターネットを介して他人に鍵を開けられてしまう可能性があり避けられるような気もしますが。

➔ 盗まれる可能性は、どっちが大きいのかなぁ。

15. 暗号が強くても鍵管理の失敗でセキュリティが破られる事例にはどんなものがありますか

➔ フィッシングで、たくさん 被害が出ていますね。

16. 以前ヨーロッパに行った時に、日本で通信している時よりはるかに多くのホームページでcookieの使用を許可するかどうかを選ばされたことに驚きました。自分と関連性のある広告などが表示されるのは便利ですがそれをプライバシーの侵害と考える人もいることを実感しました。
17. 階層構造にすることでデータの物理的運搬法は何でも良いことにすることで新しい技術でも上の階層以降を変える必要をなくしているのはとても未来を見据えた設計を最初にしたんだなと感心した。
18. 規模の大きなシステムを設計するときには、通信システムのように、階層化やモジュール化を行うことが結果としてメリットが大きいと思った。一つ下の階層より下のことを考えないというのは一見すると効率が悪そうに思えるが、このように冗長性を持たせることに意味があると感じた。これに関して、現代の普通のコンピューターでは、例えばpythonのプログラムコードを書くときに、中のハードウェアで物理的にどのような操作が行われているか考えることはないが(階層化されているので)、実機の量子コンピュータを動かそうとするときには、実機では誤り訂正ができず計算に誤差が生じるので、コードを書く時にも実機でどのような操作が行われ、どうすればその誤差を小さくできるかと考えなければならず大変であったと思い出した。

19. ゼロトラストとプライバシーが矛盾しているように感じました。企業のプライバシーポリシーや公開鍵、共通鍵の信用機関とかを信用して安心を得ているのに、自分以外を信じず自衛することになってしまいませんか？企業側は情報漏洩などで信用を失うのを避けるためにきちんと安心を提供するということでしょうか。
    ➔ プライバシー と セキュリティー は、多くの場合、相反することになります。

20. インターネットのネットワークのところで、知能、知性はエンドユーザーに。ネットワークは愚か（simple)でいい。という考え方がありましたが、確かにパケット通信は、データのバケツリレーであり、それらの通信の制御をしているのは、エンドユーザーなので、現在のネットワークの構造をよく表していると思いました。

21. P2Pのスケーリングは素晴らしいが、それこそセキュリティ面で中央集権的なしくみではないと問題が起きるケースがないか
    ➔ ブロック チェーン とか 勉強してみると面白いかもですね。

22. CAの話で、「そもそも最初の認証をどうするのか」がわかりませんでした。証明発行の段階からなりすまされていた場合には、なりすましを抑制できないように思えます。
    ➔はい。そうです。 Trust Anchor Point(s) になります。
    ➔複数存在することが 重要ですね。

23. インターネットの構造を階層構造にしたのは、他の階層に影響を与えないようにするため、と当初から考えられていたのでしょうか。そうだとしたらかなりファインプレーだと思います。あるいは一体系のものが上手くいかなかったという失敗のもとに成り立ったのでしょうか。

    ➔ もちろん、先人の失敗を勉強して、設計を行っています。

24. AmazonやNetflixなどのプラットフォームは、自社サービス内での利用履歴を収集・分析し、個別に最適化されたレコメンデーションサービスを提供しています。この過程で、ユーザーが自覚しないうちに詳細な利用パターンが収集される可能性があります。レコメンデーションの利便性だけに注目するのではなく、プライバシー侵害のリスクや情報自己決定権の観点からも批判的に捉える必要があると思います。

    ➔ はい。そうですね。　データの Sovereign（主権）という問題です。

5月２８日の休講の対応

- Lawrence Lessig の 講演(OSCON 2002) での 講演に関する 内容の簡単な整理と 考察・意見
- 締切： 6月1日(日) 23:55 まで
- 提出方法：ITC-LMS

http://hiroshi1.hongo.wide.ad.jp/hiroshi/lecture/network/03-Lessig.pdf