Questions 5月2日(水)

1. 英小文字だけ使用したときと比べて、大文字や数字、記号を使用すると、同じ文字数だと仮定するとどれほどパスワードの強度は上がるのでしょうか？目安を教えていただきたいです。

   ➔ **Brute-force attack（総当たり攻撃）で計算してみたら？**

2. 個人的にはオープンソース主義の考えを持っていますが、オープンソースで強靭なセキュリティーを実現するためにはきちんと会社が持続可能な仕組みを作ることが不可欠だと感じました。例えばブルーチームとレッドチームもそうですが、自社の脆弱性を探して貰う人の中に悪質なハッカーが存在した場合、そこをターゲットとした攻撃が可能になり、可能な限りオープンソースにしつつ適度に最新の脆弱性はクローズドにすべき二面性が存在すると思いました。

   ➔ **Double edge（諸刃の剣）ですね。**

3. 尖閣諸島中国漁船衝突映像の流出について、正義感に則って映像をインターネットにアップロードしたのは素晴らしいことのように一見感じられるが、海上保安庁の指針に逆らっていることは確かであり、ヒーローのように扱う世間の風潮には違和感を感じた。

4. 今動いているならそのままでいいという保守的な姿勢ではサイバーセキュリティの観点ではよくないことが分かった.

近年，AIの発展に伴い，AIを用いた攻撃や逆にAIを用いた防御が行われ始めているが，いつどこでサイバー攻撃にあうかわからないため，保守的になりがちな日本の企業も，これまでの受動的な対策だけでなくアクティブ・サイバー・ディフェンスを取り入れたり，最新の動向をチェックしてそれに応じた対策を行っていくべきだと感じた．また，サイバーセキュリティ方面での改善を図るにあたり，まだ日本ではサイバーセキュリティ分野に詳しい人材がそれほど多くないので，企業としても今後はそういった人材をもっと重宝して，人材不足を解消するべきだと思った.

➔ Active Cyber Defense は、悪い相手に対して ①事前、②事後 で、＜攻撃可能＞ と 言っている人・組織が 存在します。しかし、Active Cyber Defense は、Re-active(発生への対処)だけではなく、＜Pro-activeな対処＞を行うことを意味しています。 ＜攻撃はしない＞です。攻撃できないように 対処するなのです。 隠れる(見えないようにする)。＜戦争しない＝戦わずして勝つ＞のが、一番の戦争上手(兵法の基本 by 孫子)

Active Cyber Defense (ACD), also known as adaptive security, is a rapidly emerging branch of cybersecurity. It integrates and enhances several cyber intelligence, cyber protection, and cyber analytics technologies to proactively and predictively combat cyber attacks and protect data assets. Rather than passively waiting for cyber attacks to occur, ACD takes an active and proactive approach. Here are some key points about Active Cyber Defense:

- Proactive Defense: ACD focuses on actively defending against cyber threats rather than merely reacting to them. It aims to prevent attacks before they happen by collecting information about potential threats in advance and enhancing defense capabilities.
- Threat Intelligence: ACD involves gathering intelligence about cyber threats, including attack patterns, tactics, techniques, and procedures (TTPs). By understanding the methods used by attackers, organizations can better prepare their defenses.
- Preemptive Measures: ACD includes monitoring network traffic during normal operations to detect early signs of cyber attacks. If suspicious activity is detected, organizations can take preemptive measures to neutralize threats or even launch countermeasures.
- Government Initiatives: Countries like the United States and the United Kingdom have been actively working on ACD initiatives. Government expert panels have emphasized the need to strengthen defensive capabilities through ACD.
- In summary, Active Cyber Defense aims to thwart attackers' objectives by actively and proactively defending against cyber threats. It's a crucial strategy in today's rapidly evolving threat landscape

5. 予測していない問題が起きたときどう対応するかが重要だというのがまさにそうだと思いました。Googleが事後策(Re-active) を対策している話を聞いて、日本の会社は事前策 (Pro-active) ばかり対策していて、事後策についてはあまり対策していないように感じました。
6. 授業で触れられたオープンソースソフトウェアには、悪意のある機能を追加することで脆弱性を作られてしまう可能性があると思いましたが、実際にそのようなことは起こっていますか。
7. フリーソフトウェアの導入等で、セキュリティの観点から望ましい手順が紹介されていたが、自分のPCでこれを常に実践するのは難しく感じた。まともな企業ではこのような手順が正しく行われているものなのでしょうか。
8. ディズニーが現れてから著作権の年数が年々伸びた話やビルゲイツの話を聞いて，これらは著作権の本来の目的である「著作者の権利を守る」を悪用した例であると感じた．世間ではクリーンなイメージの会社でも権利を悪用して競合他社に勝利していることから，権利を悪用するものはいつでも現れるので過度な規制を行うのは安易な判断だと感じた．

9. ブラックリストに比べホワイトリストの方が安全そうに思えるので、ブラックリストを用いるメリットが気になりました。実用上の問題でしょうか。

10.ファイアウォールは本来endユーザーが自分で実施するべきセキュリティを自動化している側面があると知りその保護能力が限定的であることが理解できた。

11.Firewallは間にルータとサーバを差し込むことにより内と外が直接繋がらないようにして安心を作っているという話でしたが、このシステムがうまく働きすぎると逆にセキュリティへの意識が下がるというデメリットも紹介していただきました。これはあまり公助を充実させると具合が悪くなるので公助はほどほどにしておき、自助を促した方が良いということでしょうか。

12.フリーソフトをダウンロードするときに、バイナリファイルとテキストファイルのいずれをダウンロードするか選べるようになっているのは、ユーザがチェックできるようにするためだったのだと理解した。

しかし、そのプログラムに用いられる言語をある程度理解できたり、コンパイルする環境を用意するなど、ハードルの高さも感じた。

13.セキュリティの対策として事後策にこそ意思決定の能力が問われるとおっしゃっていましたが、そのためには事故が発生した場合の意思決定の系統をきちんと整えておく、という事前策が必須であると考えました。

14.最近よくネット上でVPNで自分の個人情報を守ろうみたいな広告見かけます。このVPNは擬似的IPを使える道具としか考えていなかったが、実際どこまでどうセキュリティー保護できるのかを教えていただきたいです。

➔ 通信路の安心のみですね。

15.ウィンドウズが悪のOSとのことでしたが、MacOSはいかがでしょうか

➔ 今では、どちらも、似た UNIXベースの OS です。

16.アカウントの二段階認証で数字6桁のワンタイムパスワードで行われるものがよくある気がしますが、数字6桁だと少し弱いのではと思っています。

17.パスワードの話をしている際に、パスワードがsuper userからしか見えないようにするとおっしゃっていましたが、super userのパスワードがバレてしまうと全てバレてしまうのではないかと感じました。いかがでしょうか。

➔ はい。基本的には、そうなります。 対策を考えたら？

18. 権限を書き換えようとする悪いファイルがあるという話を聞いて、コンピュータは内部からの攻撃に弱いという去年のコナンの映画にあったセリフは結構的を射ていると感じました

19. 社内でいきなり事故を起こしてセキュリティーの事後対策を行ってるGoogleの話を聞いて、実践的なことを行わないとプロでも実際に起こったらすぐには対処できない難しいことなのだと感じた。

20. 私が入っている自動車保険のアプリで、交通マナーの記事を読むとポイントがもらえるという機能があった、授業を聞いてそういうことだったのかと思った。

21.著作権の話をたまにされていたとおもいますが特許はどこから始まったのかなと気になりました。

➔ ルネッサンスの時と言われていますね。

22.童話には著作権が適用されないからディズニーが著作権を無視してる訳では無いけどいい気はしないと思った。当時から童話は著作権が適用されなかったのか、それともディズニーがあとからだいぶ昔の物語なんだからいいだろと童話の著作権をなくしたのか気になる。

23. 丁寧なご講義ありがとうございます。ローレンス・レシシング氏の講演は非常に思慮深い内容でした。

過去と創造との関係や、またその構図を「支配」や「制限」から述べられるのはとても新鮮で、「全体的な進歩のためにアイデアや作法を公開する」や「創造者本人の権利を守る」は矛盾的なものであり、現代では法律の形で調和していますが、その取り決まりによっても社会では様々な違った反応をするでしょう。

よく「オープンソース」の考え方はしばしば例に上がりますが、それはやはり創造物の形に「コード」という制限があるためにもたらす特例でしょうか。

➔ Programは、著作物ではなく、「表現(expression)」と扱う考え方もあります。アイデアを表現しているだけ。 アイデアには、Intellectual Property（知的財産権）が存在可能であるが、表現には、IPはない(?)。。。。

Code とは、Programを意味することが多いですが、Codeとは、ルールを指す場合も 少なくありません。 Codeには、Intellectual Property が存在する場合はありますね。

「創造物」だけど、アイデアでないのであれば、、、、、(?)