

Module 6: Assignment

6-1: Broken SHA-1

Since 2004, security researchers theorized that SHA-1 would be vulnerable to a collision attack in which the same digest from two different plaintexts could be created. In early 2017, security researchers decisively demonstrated that SHA-1 could create a collision from two separate documents. However, this attack was limited, and it was estimated it would cost attackers from \$110,000 to \$560,000 on amazon's Web services (AWS) to carry it out.

In early 2020, researchers unveiled a new attack on SHA-1 that was even more powerful. The new collision attack gives attackers more options and flexibility to produce the same digest for two or more data sets simply by appending data to each of the sets. This attack cost as little as \$45,000 to carry out. This compromise of SHA-1 has rendered it no longer suitable for use.

- How did the researchers do it? Visit the website shattered (shattered.io) to find information about how SHA-1 was breached in 2017.

Read the Q&A section and view the infographic. Try dragging one of your files to the file Tester to see if it is part of the collision attack.

- What did you learn?
- How serious is a collision?
- What is the impact?
- How do conduct research on the 2020 SHA-1 attack?
- How was it carried out?

Write a one-page paper of what you learned.

6-2: Compare Cipher Tools

A variety of online cipher tools demonstrates different cryptographic algorithms. Visit the website cipher Tools (<http://rumkin.com/tools/cipher/>) and explore the different tools. Select three tools, one of which is mentioned in this module (roT13, one-time pad, etc.). Experiment with the three tools.

- Which is easy to use?
- Which is more difficult?
- Which tool would you justify as more secure than the others do? Why?

Write a one-page paper on your analysis of the tools.

6-3: Lightweight Cryptography

Due to the importance of incorporating cryptography in low-power devices, a new “subfield” of cryptography called lightweight cryptography is being developed. This has the goal of providing cryptographic solutions that are uniquely tailored for low-power devices that need to manage resource vs. security constraints. Research lightweight cryptography.

- What are its goals?
- How will it work?
- What are its limitations?
- What are its advantages?

Write a one-page paper on your findings.

6-4: Twofish and Blowfish

Twofish and Blowfish are considered strong symmetric cryptographic algorithms. For example, Blowfish can accommodate key lengths of up to 448 bits (56 bytes). Use the Internet to research both Twofish and Blowfish.

- How secure are they?
- What are their features?
- What are their strengths and weaknesses?
- How are they currently being used?
- How would you compare them?

Write a one-page paper on your findings.

6-5: SHA-3

The hash algorithms SHA-1 and SHA-2 were not created by publicly sourced contests but instead were created by the national security agency (NSA) and then released as public-use patents. Although they are not identical, they share some of the same underlying mathematics, which has been proven to contain some cryptographic flaws. SHA-2 is a safer hash largely because of its increased digest length. SHA-3 is a completely different type of hash algorithm.

- Research SHA-3.
- What were its design goals?
- How is it different from SHA-1 and SHA-2?
- What are its advantages?
- How does its performance in hardware and software compare?
- When will it be widely implemented?

Write a one-page paper on your research.

Module 7: Assignment

7-1: Transport Layer Security (TLS)

Use the Internet to research TLS.

- Who was responsible for developing it?
- When was the first version released?
- What was the relationship between TLS and SSL?
- What are its strengths?
- What are its weaknesses?
- When will the next version be released?
- What improvements are projected?

Write a one-page paper on your research.

7-2: Recommended Crypto-periods

- How long should a key be used before it is replaced?

Search the Internet for information regarding crypto-periods for the hash, symmetric, and asymmetric algorithms.

- Find at least three sources for each of the algorithms.
- Draw a table that lists the algorithms and the recommended time, and then calculate the average for each.
- Do you agree or disagree?
- What would be your recommendation on crypto-periods for each? Why?

Provide your understanding of the above questions.

7-3: Certificate Authorities (CAs)

OSs come packaged with many digital certificates from certificate authorities (CAs). Use the Internet to determine how to view the CAs for the type and version of OS that you are using and view the list.

- How many have you heard of?
- How many are unknown?
- Select three of the publishers and research their organizations on the Internet.

Write a one-paragraph summary of each CA.

7-4: Root Certificate Breaches

Use the Internet to research breaches of CAs.

- What CAs were involved?
- Were they root or intermediate CAs?
- Who was behind the theft?
- How did the theft occur?
- How were the stolen certificates then used?
- Are certificates from these CAs still accepted?

Write a one-page paper of your research.

7-5: Block Cipher Modes of operation

Research block cipher modes of operation. Find information regarding how ECB can be compromised and write a detailed description of that. Then research one of the other modes (CBC, CTR, or GCM) in detail.

- Draw a picture of how this mode functions by turning plaintext into cipher text.
- Write a detailed description of your research.

7-6: Digital Certificate

Costs Use the Internet to research the costs of the different types of digital certificates: domain validation, EV, wildcard, SAN, machine/computer, code signing, and email.

- *Look up at least three providers of each, and create a table listing the type of certificate, the costs, and the length of time the certificate is valid.*