UNIVERSITY OF GUELPH
School of Computer Science

CIS*6510 **Cybersecurity and Defence-in-Depth** **Fall'24**
Total Marks: 10 **Hassan Khan**

Assignment03

Release date: **Nov 05, 2024**
Due date: **Nov 28, 2024 *1*1:59 pm**

Overview

As we approach the end of the term, we will focus on: (1) good easy to comprehend resources that can teach you more about cybersecurity; (2) emerging areas in cybersecurity; and (3) pressing issues in privacy.

Please use CourseLink for all communication. Ask a private question if necessary.

What to submit? Please provide your responses in a PDF file and name the file as your-first-name_your-last-name.pdf.

Quantum Cryptography [2 marks]

To answer the following questions, you should:

- Read "The cryptopocalypse is nigh! NIST rolls out new encryption standards to prepare" by Dan Goodin on Ars Technica. `https://arstechnica.com/information-technology/2022/07/nist-selects-quantum-proof-algorithms-to-head-off-the-coming-cryptopocalypse/`
- Read "NIST's POST-Quantum Cryptography Standards" post on Schneier on Security: `https://www.schneier.com/blog/archives/2022/08/nists-post-quantum-cryptography-standards.html`.

1. Are symmetric key and public key cryptography methods equally susceptible to threats from quantum computing? Explain your answer [1 mark]
2. How many of the alogorithms failed in the NIST's POST-Quantum Cryptography Standards competition and which round. (Just list the number of rounds and the

algorithms that failed in each round; however, reading the article is important). [1 mark]

State-of-the-Art Malware [2 Mark]

To answer following questions, you should read Mandiant's report on UNC3524. `https://www.mandiant.com/resources/blog/unc3524-eye-spy-email`

1. List all evasion techniques employed by UNC3524 [1 mark]
2. Briefly explain the backdoors employed by UNC3524 and their purpose. [0.5 mark]
3. Why malware authors used SOCKS tunnel? [0.5 mark]

EDR [2 Mark]

To answer following questions, you should watch EDR Evasion Primer at `https://conference.hitb.org/hitbsecconf2022sin/session/edr-evasion-primer-for-red-teamers/` or read Dan Goodin's article summarizing the findings at `https://arstechnica.com/information-technology/2022/08/newfangled-edr-malware-detection-generates-billions-but-is-easy-to-bypass/`

1. How EDR compare with antivirus products (signature or anomaly-based)? [1 mark]
2. Briefly explain the three evasion techniques (explain each technique in 3 lines or less). [1 mark]

Crypto Wars [4 marks]

Listen to Ross Anderson's lecture on the history of Crypto Wars in UK: `https://www.youtube.com/watch?v=LWwaVe1RF0c` (if you are interested in learning about the US, you can consult Schneier's blog). Note that it is important that you follow the whole lecture. There may be questions in the exam.

1. What does Ross predict for the next 20 years of cryptowars (be as brief as possible)? [3 marks]
2. What was NSA's Bullrun program (be as brief as possible)? (note that the details are on Wikipedia and not in the above youtube link) [1 mark]