SURVEY 2 QUESTIONNAIRE

- Article 1
  (1) What measure is effective to improve safety when driving connected cars?
  (2) Every link is a potential point of weakness that attackers will be quick to seize on. Except for phone Bluetooth, what else in the peripheral can lead to the insecure opening?
  (3) What does Tesla provide to address bugs?
  (4) What malicious activity is common in smartphone apps?
  (5) To detect and correct threats before they reach the vehicle, what type should the system be?

  ∗ **Reasons for these questions.** This article introduces the security risks in smart connected cars and proposes some security advice to address them. If they can understand the article and answer the questions correctly, they are considered to be knowledgeable of the security texts and thus become sensitive to potential security threats. It aims to provide users with information about security issues and features of connected cars, such as insecure communication interfaces, and vulnerabilities caused by built-in systems or connected smartphones. This knowledge might improve users' recognition of potential risks in smart vehicles and their security behaviours such as prioritize checking security-related services.
- Article 2
  (1) What did researchers set up to detect the attempt of attackers?
  (2) Via which of the following options could attackers remotely gain administrative access (CVE-2015-7755)?
  (3) What does authentication bypass require?
  (4) Which of the following options is related to the detected VPN vulnerability?
  (5) The vulnerable Dual EC standard is said to be an NSA effort to introduce a backdoored X. Which of the following options is X?

  ∗ **Reasons for these questions.** The article explains the network vulnerabilities such as the one to remotely gain administrative access to a personal device. Technical-savvy people might be benefited from the security concepts training (e.g., understanding how honeypot or network protocol SSH works to address cyberattack). Moreover, normal computer users are the majority of network users for both of their daily life and work. By reading this article, they might comprehend the widely used Dual EC standard can make VPN vulnerable so that they need to be more careful about using and protecting their authentication.
- Article 3
  (1) Which of the following options was discovered only a slight increase during the first half of 2018, but continued to pose a threat to enterprise systems everywhere?
  (2) What made it even worse than fraudulent wire transfers?
  (3) Which of the options incurred a 16 percent increase compared to 2017?
  (4) What could mega breaches cause in a smaller percentage than unintended disclosure of data?
  (5) From this article, before a data breach, what will hacks research victims to support?

  ∗ **Reasons for these questions.** Article 3 introduces the security threats of data breach such as ransomware. Users can learn the severity of the attacks and how attackers perform malicious activities. For example, hackers might research the company's IT systems to exploit vulnerabilities or victim background study to masquerade as benign accounts. They also spread malware through daily used communication channels, e.g., infected links or email attachments. Users with knowledge in mind are believed to be alarmed and take precautions towards unknown information.
- Article 4
  (1) How can criminals hacks the devices through a Wi-Fi network?
  (2) What vulnerabilities do the smartwatches have even with SSL/TLS encryption?
  (3) From this article, what can hackers apply to pass authentication and obtain user account credentials through the cloud and mobile interfaces?
  (4) From the provided authentication methods below, which one indicates unsatisfactory security measures in Two-factor authentication (2FA)?
  (5) What software can you use to scan virus in email attachments?

  ∗ **Reasons for these questions.** This article explains the security vulnerabilities and protection in smartwatches. With the increasing popularity of smartwatches, there is a higher possibility for users to leak their personal information through connected internet. By answering our questions correctly, the users are more knowledgeable in using the wearable devices. For example, they may be more cautious when connecting wifi in public area, and more willing to update their system in time, tending to use complex passwords. They are also educated to understand satisfactory security measures for authentication and use appropriate anti-virus programs towards different security threats.
- Article 5
  (1) Microsoft released security updates to bring X back to normal operation. What is X?
  (2) Security flaws exist in chips made by
  (3) What computer system will cause a blue error screen after a fatal system error?
  (4) What may Microsoft Office 2016 for Mac allows an attacker to send to a user in an attempt to launch a social engineering attack?
  (5) What is appropriate if there exist security threats in Adobe Flash?

  ∗ **Reasons for these questions.** Article 5 reports the vulnerabilities in chips and software, and also provides some security advice to develop good security behaviours to stay users safe online. Users are encouraged to update systems or software i time to avoid cyberattacks. They might also be knowledge at the fatal system in OS and security flaws in hardware but not only in software. Users are also expected to become more sensitive with daily used software such as Microsoft Office, which was attacked by social engineering.

The article also helps users understand the measures against security threats in popular but vulnerable plugins such as Adobe Flash.

- Article 6

(1) Which of the following options is not used to deal with big data remotely?
(2) With which application, attackers can generate a large amount of log data (DDOS) resulting in a temporary lack of security monitoring?
(3) Security log data can be downloaded from cloud based on X. Which option cannot become X?
(4) Except uploading data to the cloud, what does the SIEM product provide for compliance or Data Redundancy purposes?
(5) What can be "SaaS" based on this article?

∗ **Reasons for these questions.** Article 6 introduces the security issues and possible solutions in Cloud Service Providers. As increasing people are using cloud services in their daily life and work, they are suggested to be knowledgeable at potential attacks. Their security awareness and consideration are important in purchasing cloud products since professional instructions are not always available. For instance, SIEM product might help if more security log data is produced in the cloud than the local environment.

- Article 7

(1) Before 2017, what supports two-factor authentication for Google employers?
(2) What password manager is the best to support U2F in Linux operating systems?
(3) By using WebAuthn, what may happen?
(4) Which of the following options is wrong?
(5) Why was the author frustrated towards email applications when using Advanced Protection?

∗ **Reasons for these questions.** Article 7 help users understand Google' security products in authentication such as Google Authenticator and Advanced Protection. Users also can learn the major password managers using multi-factor authentication like Dashlane, and Keepass, to protect themselves from common password stealing attacks like man-in-the-middle attacks. By comprehending the security guide in the article, the users are supposed to be more confident to set up security software correctly to support other applications.

- Article 8

(1) According to the article, which of the following option is not mentioned in threat intelligence?
(2) What do many threat intelligence solutions offer to make it easier than ever to share data across platforms?
(3) Which threat in the following options is not more serious than the same old vulnerabilities that continue to be exploited?
(4) Which of the following options refers to those parts of the internet that are locked away behind secure logins or paywalls?
(5) Which of the following options is not an indicator of compromise?

∗ **Reasons for these questions.** Article 8 identifies the current threat intelligence solutions in different use cases. For example, organisations are suggested to integrate threat intelligence into their security program. They should also prioritize fixing existing vulnerabilities instead of unknown exploits since new threats are always developed from old ones. Sensitive information such as academic reports or medical record can be stored safely with the use of different internet sources such as deep web and dark web. Leveraging monitoring techniques to detect malicious links or profiles is also useful in social media. Lastly, identifying an indicator of compromise such as suspicious addresses can help to defend even before attacking. Organisations or individuals can be benefited from adopting appropriate solutions to secure their data effectively.

- Article 9

(1) The article mentioned some high-profile attacks, in which years did them occur?
(2) Which attack is not used to steal credentials for cryptocurrency wallets and exchanges?
(3) Which of the following options is not attack vector used by the hacker to deliver PowerRatankba?
(4) During an attack, which of the following option is not included in the information about the machine PowerRatankba first sends?
(5) How did RatankbaPOS achieve deployment?

∗ **Reasons for these questions.** Article 9 presents several severe cryptocurrency-related attacks including backdoors and malware. For example, the Bangladesh Bank suffered from fraud and lost $81 million. Users especially financial organisations should understand the attack vectors such as spreading a TinyURL shortener link or exploiting suspicious emails to redirect users to phishing websites. Users should also recognise they are at higher risk of being malware target than they estimated. It can be useful to frequently monitor or update their software applications or devices which are most likely to be exploited by hackers.