Effect of Human Factors in Security Threat Analysis- Replication package

Start of Block: Informed Consent

Q49 You are invited to participate in a study on security risk analysis. Your answers will be processed anonymously for research purpose. You can read the consent form here.

The first part of the survey contains a scenario and a questionnaire. You will be asked to read a scenario and evaluate the recommended solution for the identified security threat. In the second part, we will ask you some general questions as well as some background information.

Please, use only the survey buttons to navigate the survey (do not use the browser buttons). This is a forward-only survey.

- ○ By clicking this button I agree to participate in this study. (1)

End of Block: Informed Consent

Start of Block: Identification questions

SurveyName E0_Survey

Fill in your first name, last name, and student ID.
Example
First Name: John
Last Name: Doe
Student ID: 1234567

- ○ First Name (6) _____
- ○ Last Name (4) _____
- ○ Student ID (5) _____

End of Block: Identification questions

Start of Block: Introduction

Q1
CONTEXT

Digitalization of business processes is a continuous process that relies on building new software products. However, software products may contain security holes that can be maliciously exploited.

In order to deal with or prevent these risks, organizations often perform an analysis of security threats and risks to their software systems. Security threat and risk analysis is a systematic way of finding potential cyberthreats before a software is implemented (during the planning stage) with the aim of solving security issues before they actually occur. If issues are anticipated, trade-offs between different solutions to mitigate risk can be analyzed, allowing for an informed final choice for a security solution.

End of Block: Introduction

Start of Block: The Careless Web Host

Q2 Please read the scenario carefully.

SCENARIO
Web hosting organization MaxxUpload is a company that provides hosting services for client websites. For a fee, clients can choose a domain name (e.g., www.myfirstsite.com) and upload their website files to MaxxUpload's server. From there, MaxxUpload takes care of all the internet traffic. MaxxUpload has the slogan: "Cheap, with a guaranteed content delivery, no matter what".

It turns out that a large portion of MaxxUpload clients are hackers who upload malicious programs, which are able to send spam emails containing links. These links redirect users to MaxxUpload servers where the attacker has previously prepared another malicious program. This program exploits a vulnerability on the users' browser. The attacker can then access user files (like certificates or private photos) which they can threaten to leak if the user does not transfer a large amount of money to an off-shore account.

Despite repeated requests from other international internet service providers, MaxxUpload refuses to intervene with the "hacker clients", referring to their "no matter what" guarantee to their customers. Furthermore, MaxxUpload is based in a country whose laws do not prohibit such hosting activities. As MaxxUpload is operating internationally, this poses a threat.

End of Block: The Careless Web Host

Start of Block: Randomised vignettes

Q3 Several international security experts were called in to study the case of the security threat and provided suggestions about how to approach the issue of MaxxUpload's services being used for malicious hacking.

You may optionally consider the appendix at the bottom of this page, which the analyst attached for their suggested solution as well as an explanation of how hackers may use MaxxUpload to spread malicious programs.

Please read the suggestion below and answer the questions.

Q4
Anna, Senior Analyst at a large cybersecurity consulting firm suggests engineering a computer program which brings down part of MaxxUpload infrastructure to stop behavior that resembles "hacker" activity.

Q5
Frank, Senior Analyst at a large cybersecurity consulting firm suggests engineering a computer program which brings down part of MaxxUpload infrastructure to stop behavior that resembles "hacker" activity.

Q6
Anna, Junior Analyst at a large cybersecurity consulting firm suggests engineering a computer program which brings down part of MaxxUpload infrastructure to stop behavior that resembles "hacker" activity.

Q7
Frank, Junior Analyst at a large cybersecurity consulting firm suggests engineering a computer program which brings down part of MaxxUpload infrastructure to stop behavior that resembles “hacker” activity.

Q8
Anna, Senior Analyst at a large cybersecurity consulting firm, suggests to blacklist (i.e., “block”) some of the incoming traffic from MaxxUpload servers.

Q9
Frank, Senior Analyst at a large cybersecurity consulting firm, suggests to blacklist (i.e., “block”) some of the incoming traffic from MaxxUpload servers.

Q10
Anna, Junior Analyst at a large cybersecurity consulting firm, suggests to blacklist (i.e., “block”) some of the incoming traffic from MaxxUpload servers.

Q11
Frank, Junior Analyst at a large cybersecurity consulting firm, suggests to blacklist (i.e., “block”) some of the incoming traffic from MaxxUpload servers.

Q12 Overall, I found the suggested solution to be acceptable

- ○ Strongly disagree (1)
- ○ Disagree (2)
- ○ Neutral (3)
- ○ Agree (4)
- ○ Strongly Agree (5)

Q13 The proposed solution is effective from __

	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly agree (5)
My objective perspective (1)	○	○	○	○	○
The perspective of MaxxUpload (2)	○	○	○	○	○

Q15 I found the suggested solution to be __

	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
Ethical (1)	○	○	○	○	○
Reliable (2)	○	○	○	○	○
Responsible (3)	○	○	○	○	○
Trustworthy (4)	○	○	○	○	○

Q16 I found the Analyst to be ___

	Strongly disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly agree (5)
Competent (1)	○	○	○	○	○
Skillful (2)	○	○	○	○	○
Knowledgeable (3)	○	○	○	○	○
Moral (4)	○	○	○	○	○
Trustworthy (5)	○	○	○	○	○

Q60
Appendix

Q18

Justification

Frank's proposed solution is a reactive type of solution. It entails coordinating the web browsers (such as Chrome, Mozilla, Safari, etc) with blacklists which block any incoming traffic from MaxxUpload servers. The browsers apply the blacklists by default, unless a legitimate MaxxUpload client makes an explicit request to whitelist their specific address. A possible outcome is that all MaxxUpload clients are blocked, and legitimate clients may struggle to reach blacklist maintainers to request that they whitelist their services.

Q47

Justification

Frank's proposed solution is a corrective type of solution. It entails engineering a computer "worm", otherwise known as a malware computer program that replicates itself in order to spread to other computers and impact their functionality. Though this solution may work, the worm may target MaxxUpload's legitimate clients as well, leading to unnecessary loss of data.

Q46 **Justification**

Anna's proposed solution is a reactive type of solution. It entails coordinating the web browsers (such as Chrome, Mozilla, Safari, etc) with blacklists which block any incoming traffic from MaxxUpload servers. The browsers apply the blacklists by default, unless a legitimate MaxxUpload client makes an explicit request to whitelist their specific address. A possible outcome is that all MaxxUpload clients are blocked, and legitimate clients may struggle to reach blacklist maintainers to request that they whitelist their services.

Q19 **Justification**

Anna's proposed solution is a corrective type of solution. It entails engineering a computer "worm", otherwise known as a malware computer program that replicates itself in order to spread to other computers and impact their functionality. Though this solution may work, the worm may target MaxxUpload's legitimate clients as well, leading to unnecessary loss of data.

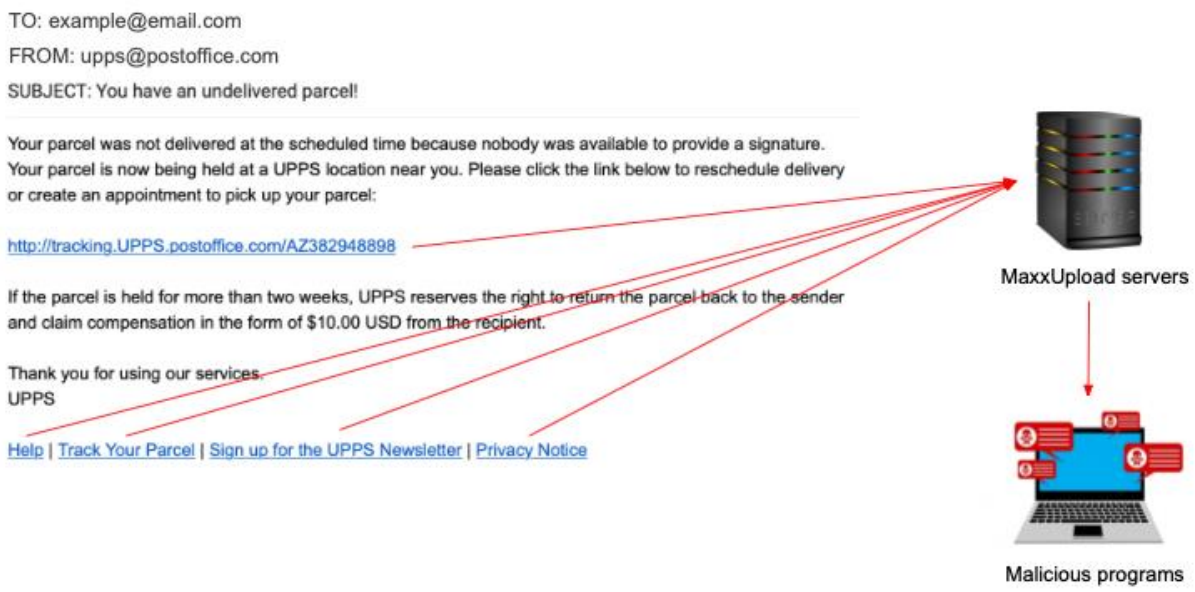
Q61

Appendix

An instance of how a hacker may spread malicious programs is exemplified in Figure 1, in

which a deceptive spam email appears as if it is sent from a legitimate organization or company, but actually is not. The email contains URLs that, when clicked upon, redirects the victim to the malicious programs via MaxxUpload's servers.

Figure 1: Illustration of spam email redirecting the user to malicious programs.



End of Block: Randomised vignettes

Start of Block: Demographics

Q21 Thank you for answering the questions thus far. Next, we will ask you some questions about your personal background.

Q22 What is your sex (as assigned at birth)?

- Male (1)
- Female (2)

Q23 What is your age?

- Under 18 (1)
- 18 - 20 (2)
- 21 - 24 (3)
- Above 25 (4)

Q24 What is your Nationality? Choose the country that coincides with your ethnic/cultural background

▼ Afghanistan (1) ... Zimbabwe (1357)

Q25 Please indicate your study program:

- Artificial Intelligence (1)
- Bioinformatics and Systems Biology (2)
- Computer Science (3)
- Information Science (4)
- Computer Security (5)
- Other (please specify) (6) _____

End of Block: Demographics

Start of Block: Control Questions

Q30 I understood the scenario description about the MaxxUpload activities.

- Strongly disagree (1)
- Disagree (3)
- Neutral (4)
- Agree (5)
- Strongly agree (6)

Q31 Do you agree with MaxxUpload's decision to host any client, even malicious ones?

- Strongly disagree (1)
- Disagree (2)
- Neutral (3)
- Agree (4)
- Strongly agree (5)

Q32 How would you rate your understanding of the following?

	Strongly disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly agree (5)
I understood the proposed solution (1)	○	○	○	○	○
I understood the consequences of the proposed solution (2)	○	○	○	○	○

Q34 I read the analysts' justification and appendix in detail.

- Strongly disagree (1)
- Disagree (2)
- Neutral (3)
- Agree (4)
- Strongly agree (5)

Q35 I understood the appendix.

- Strongly disagree (1)
- Disagree (2)
- Neutral (3)
- Agree (4)
- Strongly agree (5)

Q36 The appendix was helpful in answering the rest of the scenario questions.

- Strongly disagree (1)
- Disagree (2)
- Neutral (3)
- Agree (4)
- Strongly agree (5)

Q38 Do you have any further questions or comments?

_____

End of Block: Control Questions