Automatic Generation of Security-Centric Description for Cyber Threats

Tingmin Wu, Swinburne University of Technology / CSIRO's Data61
Supervisors: Prof. Yang Xiang, Dr. Sheng Wen, Dr. Cecile Paris and Dr. Surya Nepal

End users are increasingly concerned with the privacy of their data and security of their devices. Users receive a multitude of security information in written articles to protect their security and privacy. However, prior research suggests that these delivery methods, including security awareness campaigns, mostly fail to increase people's knowledge about cyber threats. It seems that users find such information challenging to absorb and understand. Yet, to raise users' security awareness and understanding, it is essential to ensure the users comprehend the provided information so that they can apply the advice it contains in practice. The security-centric descriptions generated by recent automatic techniques do not always address users' concerns as they are generally too technical to be understood by ordinary users. Moreover, different users have varied linguistic preferences, which do not match the text. Motivated by this challenge, we propose to generate security-centric descriptions for cyber threats.

Motivation

- Education in understanding security texts is critical to the improvement of users' ability in making correct security decisions. However, it was revealed that less than 25% of security advice was easy to understand.
- Most users are not security experts, even if they are technically savvy. The majority of users underestimate the extent of cyber harms, and only around 10% can explain protective measures correctly.
- Developers usually sidestep security risks in their textual descriptions, and there exist variations between existing texts and the real functionality of the software.
- Formal security education or training is time-consuming and requires users' undivided attention, and one-size-fits-all trainings hardly keep people engaged as they might have different learning preferences or background knowledge. Compared to certification programs, online cybersecurity texts give internet users easier access.
- **The aim**: to design a system that automatically learns users' security concerns and linguistic preferences to generate personalised security-centric descriptions on different platforms to improve users' security awareness.

Research Questions

Main Question: How can we design security-centric description to improve the security awareness of end users?

1. How do the end users understand security texts and how can we improve their understanding?
2. How can we generate accurate and useful security-centric descriptions to raise users' security awareness?
3. How can we personalise security descriptions to meet the requirement of different users?

FOR FURTHER INFORMATION
Tingmin (Tina) Wu
Tina.Wu@data61.csiro.au

Research Approach and Methodology

Step 1

Automatic Generation of Personalised Security-Centric Descriptions for Android Apps

- We develop the prototype system that
  - incorporates Big Five personality traits classification and NLG,
  - learns users' concerns and linguistic preferences,
  - generates personalised security descriptions.
- Experiments results and user studies show significant improvement of our generated descriptions in readability and user awareness.

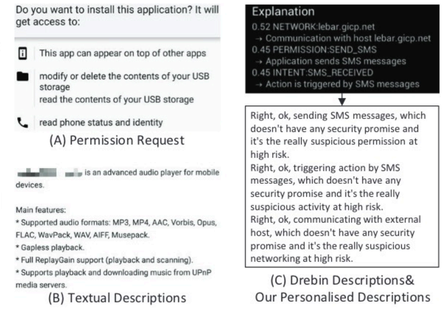

Figure 1: Existing descriptions vs.. our personalised descriptions before app installation.

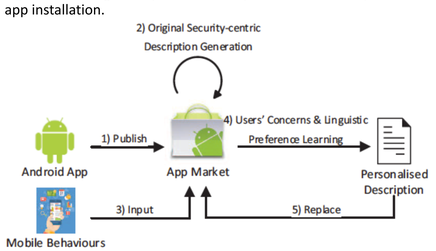

Figure 2: Deployment of our prototype system that generates security descriptions for Android Apps.

Step 2

Analysis of Trending Topics and Text-based Channels of Information Delivery in Cybersecurity

- We build a large collection of cybersecurity texts (187,319 articles) from three online sources: news, security blogs, and websites.
- We propose a semi-automated classification and identify 16 security categories to analyse the security issues.
- We conduct an empirical study to analyse the comparison and evolution of the security categories over the last decade as well as across the sources to shed light on the trends of security issues.
- Interesting findings
  - The impact reflected from cybersecurity texts strongly correlates with the monetary loss caused by cybercrimes.
  - Webpages deliver security information without caring about timeliness much, compared to news and security blogs.

Step 3

An Empirical Study on Users' Understanding of the Terms Used in Security Texts

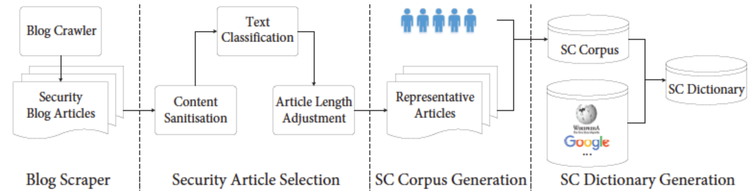

Figure 3: Overview of our framework to build the Security-Centric (SC) Dictionary.

- We study how users comprehend security texts.
  - 61% of technical terms are considered to be hard.
  - 65% of participants would like to have a dictionary-based explanation for technical terms.

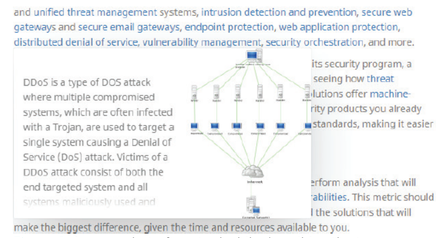

Figure 4: A screenshot of our tool while describing the term 'distributed denial of service'.

- We build a user-oriented security-centric dictionary and develop a tool as a service using the dictionary.
  - Our tool can help users understand security articles significantly better.
  - Users with IT background perform better in understanding security texts than those without, but only when using our tool.

Automatically Extending Security-Centric Dictionary

- We propose a pretrained language model based on Bert for modelling cybersecurity texts to recognise new security terms.

Future Directions

- Improving description generation (Shortened or refined descriptions; visual aids, e.g., infographics).
- Cyber attack prediction based on our analyses.
- More psychological methods to deliver the cyber security knowledge and enhance user behaviour.