Towards Usable and Secure Natural Language Processing Systems

Yasser M. Hausawi and Liam M. Mayron

Department of Computer Sciences
Florida Institute of Technology
Melbourne, FL 32901, USA
{yhausawi@my.,lmayron@}fit.edu

Abstract. Natural Language Processing (NLP) systems must be both secure and usable, but this remains an elusive objective. This work considers the relationship between usability and security in NLP systems. Development and lifecycle practices are discussed with the goal of a more integrated, comprehensive process for NLP system development.

Keywords: Natural Language Processing, Security, Usability, Artificial Intelligence, Human-Computer Interaction.

1 Introduction

Natural Language Processing (NLP) systems are used with increasing frequency by a growing number of people. Such systems interpret text or voice that is generated by a human in a manner interpretable by a machine. They employ a variety of machine learning methods in order to determine the meaning of the original material. Scenarios for usage of NLP systems range from the automated extraction of entities from text or speech and translation to determining the emotion of a human or the relationships between people. In this work, we consider the effectiveness of NLP systems in the context of their usability and security. Despite the widespread usage and potential applications of NLP systems, investigations into their usability are scarce. Furthermore, the security implications of NLP systems merit additional investigation. Perhaps most interesting is the intersection of usability, security, and the capabilities of NLP systems. In terms of usability, an NLP system must be able to satisfy metrics of effectiveness, efficiency, and satisfaction. Security requirements include confidentiality, integrity, and availability. Security and usability requirements can sometimes be in opposition [4], but work towards bridging this gap has been undertaken [7].

2 Usability and Security for NLP Systems

NLP occurs in five main stages: user interface (for example, the input from a microphone or text), recognition and conversion, segmentation and parsing, matching, and processing (Figure 1). In the case of audio input, an Automatic

C. Stephanidis (Ed.): Posters, Part I, HCII 2013, CCIS 373, pp. 109–113, 2013.

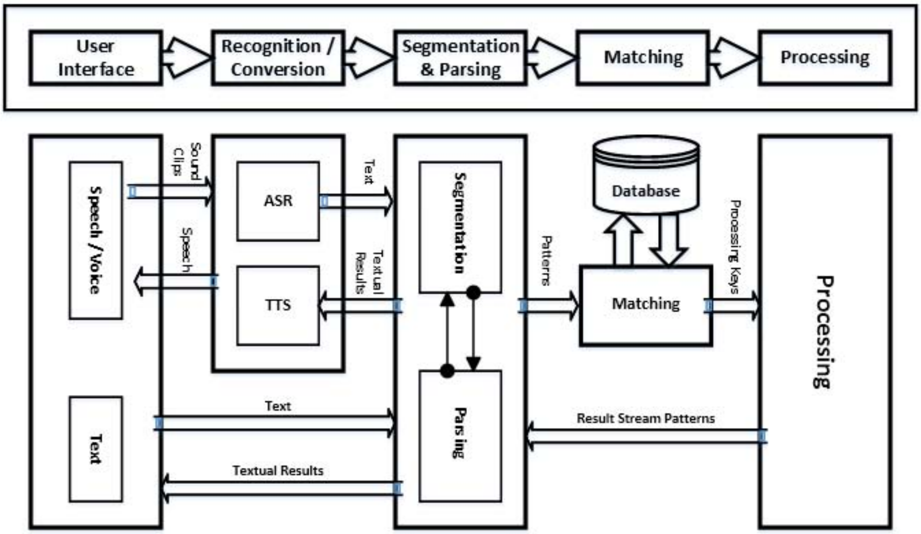

Fig. 1. NLP system architecture

Speech Recognition (ASR) subsystem can be used to recognize sound and covert to textual patterns. After processing, the resulting text is converted back to audio through a Text-to-Speech (TTS) system if the response is to be presented as speech. If the system uses only textual input, the recognition and conversation stage can be eliminated.

The term usability is defined by the International Standard Organization (ISO) as the range in which a product can be operated by legitimate users to satisfactorily perform specific tasks in an effective, efficient, and specified way [6]. The assessment of an NLP system's usability must consider these three factors (efficiency, effectiveness, and satisfaction). An NLP system can only be considered as effective if its users are able to achieve their goal of operating it. An efficient NLP system must complete specific task or process to reach a particular goal within an acceptable amount of time. For a NLP system to be satisfactory, both the vendors and the users must be happy with the system (as determined by their willingness to rely on and reuse the system). Evaluating satisfaction can be challenging due to the difficulty of measuring it. The best way to evaluate system satisfaction is through vendor and user questionnaires, surveys, and interviews [7].

System security is a set of methods and techniques applied to prevent weaknesses from being exploited. At a high level, there are three main security objectives: confidentiality, integrity, and availability [8]. NLP systems, like all other computer systems, have vulnerabilities that need to be discovered and remedied.

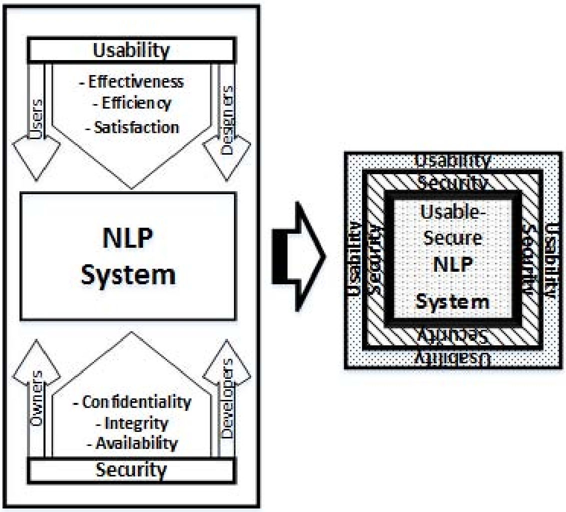

Fig. 2. Usability and security in NLP systems

In order for a NLP system to be considered confidential, it must limit access to its features and services solely to authorized users. Integrity requires that a system protects its contents from unauthorized alteration. Finally, a system must be available for use when needed by authorized users for legitimate purposes.

The interaction between usability and security in NLP systems is illustrated in Figure 2.

3 Developing Secure and Usable NLP Systems

Building a NLP system using the standard waterfall model of software development tends to be linear [9], following the Software Development Lifecycle (SDLC). NLP system development starts from the pre-development planning phase. Subsequently, the requirements phase establishes objectives for the project. The design phase details the requirements and develops a system architecture. Implementation consists of programming and creating functionality. The testing phase evaluates and validates the system. During deployment, the system is delivered and configured. The maintenance phase keeps the system in working order.

Although the SDLC can satisfy functional requirements, the implementations of security and usability benefit from their own processes that occur within the SDLC [1,2,3,5,9,10]. This alignment is shown in Table 1. It can be used as guidance by software engineers in achieving both a usable and secure development process.

Table 1. Usability and security during the software development lifecycle [1,2,3,5,9,10]

Phase	Security Practice	Usability Practice
Planning	Security training	Human-centered
Requirements	Security objectives Security requirements Quality gates Risk assessment Specifications	Context specification Usage scenarios User analysis Task analysis Usability specifications
Design	Attack surface analysis Threat modeling Design review	Concept development Prototypes Interaction design Design review
Implementation	Approved tools Security patterns Static analysis Code review	Approved tools User interface patterns Interface development User interface review
Testing	Dynamic analysis Attack surface review	Expert review Usability evaluation Acceptance testing
Deployment	Incident response plan Security review Release Archive	Surveys and interviews
Maintenance	Incident plan	Usability review

4 Conclusion

NLP has a significant impact on human-computer interaction. There is a strong relationship between NLP systems, usability, and security, as NLP systems must be both usable and secure in order to engender the trust of both users and vendors. NLP systems can be evaluated in terms of both usability and security, and enhanced as needed.

References

1. Costabile, M.F., et al.: Usability in the software life cycle. Handbook of Software Engineering and Knowledge Engineering 1, 179–192 (2001)
2. Cranor, L., Garfinkel, S.: Security and usability: designing secure systems that people can use. O'Reilly Media, Incorporated (2005)
3. Ferre, X.: Integration of usability techniques into the software development process. In: International Conference on Software Engineering (Bridging the Gaps between Software Engineering and Human-Computer Interaction), pp. 28–35 (2003)
4. Fléchais, I.: Designing Secure and Usable Systems. Ph.D. thesis, Citeseer (2005)
5. Howard, M., Lipner, S.: The security development lifecycle. Microsoft Press (2009)
6. ISO, W.: 9241-11, Ergonomic requirements for office work with visual display terminals (vdts). The international organization for standardization (1998)

7. Kainda, R., Flechais, I., Roscoe, A.: Security and usability: Analysis and evaluation. In: International Conference on Availability, Reliability, and Security, ARES 2010, pp. 275–282. IEEE (2010)
8. Pfleeger, C.P., Pfleeger, S.L.: Security in computing. Prentice Hall PTR (2006)
9. Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S., Carey, T.: Human-Computer Interaction. Addison - Wesley (1994)
10. Shneiderman, B., Plaisant, C.: Designing the user interface: Strategies for effective human-computer interaction. Pearson Education (2005)