Chapter XXV

Formal Analysis of Security in Interactive Systems

Antonio Cerone
United Nations University, China

Siraj A. Shaikh
United Nations University, China

ABSTRACT

Reducing the likelihood of human error in the use of interactive systems is increasingly important. Human errors could not only hinder the correct use and operation, they can also compromise the safety and security of such systems. Hence the need for formal methods to analyze and verify the correctness of interactive systems, particularly with regards to human interaction. This chapter examines the use of formal modeling and analysis of security properties of interactive systems. The reader is introduced to some basic concepts in security and human-computer interaction, followed by formal modeling of human cognitive behavior and analysis of such systems. Authors highlight the use of model-checking to drive the system development to design secure user actions and sequences of actions. Authors also analyze the patterns of user behavior that may lead to security violation. Finally, particular areas of security protocol design where human interaction plays a key role are discussed.

INTRODUCTION

Reducing the likelihood of human error in the use of interactive systems is increasingly important: the use of such systems is becoming widespread in applications that demand high reliability due to safety, security, financial or similar considerations. Consequently, the use of formal methods in verifying the correctness of interactive systems should also include analysis of human behaviour in interacting with the interface.

The study of human behaviour in operating machines has emerged in the 1980’s, when Human Reliability Assessment (HRA) techniques have
been used in the analysis of safety-critical systems (Kirwan, 1990). These techniques appeared soon to lack objectivity (Svenson, 1989) and failed to cope with the complex behaviours emerging in the human-machine interaction (Kirwan, 1992).

In the 1990s formal methods have started to be introduced aiming at a more objective analysis (Dix, 1991). However, the gain in objectivity was offset by an oversimplified model of the human behaviour, which was actually often modelled as defined by the interface requirements. In reality, the user interacting with the system does not necessarily behave as it was expected while designing the interface, and errors are actually the very result of an unexpected user behaviour that emerges through the interaction.

To best capture such an emergent behaviour, a model of the user must specify the cognitively plausible behaviour, which is all the possible behaviours that can occur, and that involve different cognitive processes (Butterworth et al., 2000). The model must take into account all relationship between user’s actions, user’s goals and the environment. Following this approach, a number of researchers have explored the use of formal models to understand how cognitive errors can affect user performance. Mode confusion is often blamed for human errors in interactive systems, whereby the user’s mental model of how the system works gets out of step with how the system is actually working. This phenomenon has been analysed by developing a plausible (but simplified) mental model such as might represent the user’s understanding of the system and comparing it with a user interface model, to look for sources of cognitive dissonance (Butler et al., 1998; Rushby, 2002). Rushby (2002) models the behaviour of a forgetful user who follows a warning display light or a non-forgetful user without warning lights and checks for emergent mode confusion. Curzon and Blandford (2004) focus on goal-based interactions and model the behaviour of a user who assumes all tasks completed when the goal is achieved, but forgets to complete some important subsidiary tasks (post-completion error). Cerone et al (2005) investigate the application of formal methods to the classification and analysis of task failure caused by systematic recurrence of human errors. This recurrence produces complex patterns of human behaviours, which are the result of bad habits, poor training, deficient mental models, or are associated with cognitive processes such as habituation. The error is modeled by the behavioural pattern itself, rather than by specific error states as for mode confusion and post-completion error. In particular, different categories of behavioural patterns are formally verified to be a sound and complete decomposition of an air traffic control task failure.

These formal approaches all address safety-critical aspects of interactive systems and cognitive behaviour. Only at the beginning of the new millenium, security aspects of interactive systems have been started to be systematically analysed (Cerone and Curzon, 2007; Yee, 2002; Zurko, 2005). In fact, security violations in human-computer interaction may be due to systematic causes such as cognitive overload, lack of security knowledge, and mismatches between the behaviour of the computer system and the user’s mental model (Yee, 2002). The user who causes the violation may or may not be the attacker: the user may either become aware of the violation and exploit it or unwillingly allow a malicious user to exploit it. The latter situation is more complex due to two reasons. First, the violation often emerges as a consequence of a complex behavioral pattern (Cerone et al., 2005). Secondly, the security properties need to capture the conditions which enable a malicious user to exploit the violation (Cerone and Elbegbayan, 2007).

Rest of this Chapter

The rest of this chapter focuses on the use of formal methods in modelling and analysing security properties of interactive system. Concepts will be introduced with references to a few case studies.