Thursday 9 January 2014
10h30
INP-ENSEEIHT, Salle des theses

Khalid NASR
Team IRT - IRIT

Performance Analysis of Wireless Intrusion Detection Systems

Jury:

Directeurs de thèse:
M. Christian FRABOUL – IRIT, ENSEEIHT- INPT.
M. Anas ABOU EL KALAM – Lab. OSCARS, UCA/ENSA, Marrakech, Maroc.

Rapporteurs:
M. Abdelmadjid BOUABDALLAH – Professeur, Université de Technologie de Compiègne.
M. Belhassen ZOUARI – Professeur, Sup’Com de Tunis- Université de Carthage.

Examinateur:
M. Frédéric CUPPENS – Professeur, ENST-Bretagne, Campus de Rennes.

Abstract: Wireless network security has a considerable attention in recent years. Several security efforts have been exerted to combat the wireless attacks, but unfortunately complete attack prevention at the first line of defense such as authentication, encryption, and firewall is not realistically attainable. Thus, the emphasis on detecting wireless attacks at a second line of defense, in the form of Wireless Intrusion Detection System (WIDS), has been growing. Despite the importance of WIDSs in wireless network security, their performance is sometimes not satisfying in practice. Thus, WIDSs performance evaluation is a pressing necessity. By evaluation we mean a systematic assessment for measuring the ability of a WIDS to meet the intended operation and expected performance. In this thesis, we have developed a comprehensive evaluation methodology that covers all necessary dimensions for a credible evaluation of WIDSs performance. The main pivotal tasks in our methodology are characterizing and generating the evaluation data-set, defining expressive evaluation metrics, and circumventing the evaluation limitations. Comprehensive and credible evaluation of WIDSs necessitates taking into account all possible attacks. While this is operationally impossible, it is necessary to select representative attack test cases that can be extracted mainly from a comprehensive classification of wireless attacks. Dealing with this challenge, we have developed a holistic taxonomy of wireless security attacks from the perspective of the WIDS evaluator. The second pivotal task in our methodology is defining expressive evaluation metrics. We introduced a new evaluation metric \( E_{ID} \) (intrusion detection effectiveness) for manipulating the drawbacks of the previously proposed metrics for evaluating the IDSs/WIDSs effectiveness. As well, we proposed another metric \( R_R \) (recognizing rate) for measuring the attack type recognizing attribute. As a third important task, we have circumvented the evaluation limitations, caused by the uncontrolled traffic in the wireless open medium, by constructing a RF shielded testbed to take all measurements under our control without any interfering from any outside uncontrolled traffic. Finally, we followed our methodology and conducted experimental evaluation tests of two popular WIDSs, and demonstrated the utility of our proposed taxonomy of wireless attacks and our developed evaluation metrics (\( E_{ID} \) and \( R_R \)), in addition to evaluating the impact of WIDSs on the supervised system resources.