استخدام أشجار الأخطاء للنمذجة والتحليل وتكمية الريبة في نظم أمان المحساب

محمد أحمد موسى القواسمي

بحث مقدم لنيل درجة الماجستير في العلوم
(الهندسة الكهربائية وهندسة الحاسبات / هندسة الحاسبات)

إشراف:
أ.د. علي محمد علي رشدي

استخدام أشجار الأخطاء للنمذجة والتحليل وتكمية الريبة في نظم أمان المحساب

محمد أحمد القواسمي

المستخلص

ثمة توجه حديث في دراسة أمان نظم المحساب يتطلب استغلال التشابهات بين علمي المعَّولية وأمان المحساب لتطوير معايير كمية للأمان التشغيلي. وبصفة خاصة، يستعمل نموذج شجرة الأخطاء حاليا لتحليل وتصميم نظم أمان المحساب وأحيانا يعاد تسمية أشجار الأخطاء (بدون أية ضرورة واضحة) كأشجار الهجوم والدفاع في هذا التطبيق الخاص. في هذه الرسالة نقوم بمتابعة استكشاف استخدام التكمية في أشجار الأخطاء وطريقة تأثيرها على مجالات الأمان في أنظمة المحساب. هذه الرسالة تقوم بتكييف منهجية أشجار الأخطاء المستخدمة في هندسة المعَّولية لتستعمل في تكمية العديد من الحالات والمواقف والمناحي في موضوع انتهاك أمان المحساب، ومن ثم اشتقاق تعبيرات رمزية لاحتمال الحدث الأوجي Q (لكل من أشجار الأخطاء سالفة الذكر) بدلالة احتمالات الأحداث الأساسية $\vec{q}$ ، ومن ثم نقوم في هذه الرسالة بمعالجة المسألة مزدوجة العشوائية الخاصة بتقدير الريبة في احتمال الحدث الأوجي بدلالة التباينات في احتمالات الأحداث الأساسية، وفي نهاية المطاف نقوم بهذه الرسالة بالحصول على تقديرات عددية لاحتمالات الأحداث الأوجية وتبايناتها وكذلك ترتيب أحداث الاختراق الأساسية طبقا لأهميتها.

By

Mohammad Ahmad AL Qwasmi

1306501

A thesis submitted for the requirements the degree of Master of Science (Electrical and Computer Engineering / Computer Engineering).

Supervised

Prof. Dr. Ali Mohammad Ali Rushdi

Mohammad Ahmad AL Qwasmi

Abstract

A new trend in the study of computer system security is to exploit similarities between reliability and security to develop quantitative measures for "operational security". In particular, the fault-tree model, a traditional reliability methodology used in the analysis and design of safety-critical systems, is now being considered also in the analysis and design of security systems. Sometimes, fault trees are unnecessarily renamed as attack-defense trees for this particular application. The present thesis constitutes an extended exploration of the possibility of using fault trees in the quantitative assessment of the effect of security breaches on a computer system. The thesis adapts of the fault-tree methodology of reliability engineering to the quantification of a variety of situations or aspects of the security exposure of computer systems. Next, it derives symbolic expressions for the top-event probability Q (for each of the aforementioned fault trees) in terms of the basic event probabilities $\vec{q}$. Then, the thesis handles the doubly-stochastic problem of estimating uncertainty in the top-event probability in terms of the variances of the basic-event probabilities. Finally, the thesis obtains numerical estimates for the top-event probabilities and their variances and also for the importance ranking of the various breach events.