Sudan University of Science and Technology

College of Computer Science and Technology

Resolving Network Packet Length Covert Channels

معالجة القنوات السرية المبنيةعلى طول حزمة البيانات في الشبكات

Thesis

Submitted for the degree of

Doctor of Philosophy (PhD) in Computer Science

BY

MuawiaAbdelmagidElsadig

Supervisor

Professor Yahia A. Fadlalla

April, 2018

Abstract

The continuous and rapidly advancing developments in network technology seem to encourage hackers to find new ways to breach a system's security policy; consequently, compromising confidential information. When the interpretation of a security model adopted by a system is violated by a communication between two users, or processes operating on their behalf, it is said that the two users are communicating indirectly or covertly. This thesis deals with detecting and resolving network packet length covert channels. These channels are notoriously known to be risky, invisible, and undetectable. The thesis introduces and develops three new approaches to resolve covert channels. Furthermore, the thesis introduces an approach that accurately detects this notorious type of channels. Combined together, the four (4) approaches form a system that is proven to be successful in detecting and resolving network packet length covert channels. The first approach eliminates covert channels by hiding the true identity of a system's user from the process or processes that represent him or her inside that system. This approach not only completely eliminates the known and potential covert channels, but also those that are unknown, never detected, and/or undetectable by the system. The second approach eliminates network packet length covert channels by altering the covert message in a way that the intended receiver gets an unintended message – a totally different and useless message. Two term-based similarity tests (cosine and dice coefficient similarity tests) were successfully computed and showed zero (0) similarity score while a semantic similarity test (MCS Method) shows 0.0405626 similarity score. These results indicate that this approach effectively resolves any potential covert channel. The third approach is an enhanced version of the previous approach. It reduces its overheads up to 50 %. With this third approach, the term-based similarity tests show zero (0) similarity score and the semantic similarity test shows 0.0674704 similarity score. These results again show that there are no similarities between the covert intended message and its distorted and altered form that was obtained using this approach. The fourth and last approach is a machine learning-based detection approach to detect network packet length covert channels. It attained an

excellent degree of detection accuracy: 98% with zero (0) False Negative (FN) and 0.02 False Positive (FP) classification errors.

الملخص

إن التطور المتسارع في أنظمة كشف إختراق الشبكات وكذلك التطور في شبكات الحاسوب وتقنياتها قد شحذ الهمم عند قراصنة المعلومات والشبكات للبحث عن طرق بديلة يتسنى من خلالها تسريب المعلومات السرية و ذات الأهمية بإسلوب يصعب إكتشافه من خلال أنظمة إكتشاف الإختراقات. نعم قد وجد القراصنة ضالتهم فيما يعرف بقنوات الإتصال السري والتى من خلالها يتم تسريب المعلومات بصورة تنتهك السياسات الأمنية للأنظمة. عندما يتم إنتهاك السياسات الأمنية لنظام شبكات حاسوب ما عن طريق إيجاد قنوات إتصال تسمح بتسريب المعلومات بين مستخدمين - أو إجرائين يعملان نيابة عنهم - غير مخولين بتبادل هذه المعلومات حينها يمكن القول بحدوث ما يسمى بالقناة السرية وهي تعتبر مهدد أمني لأنظمة الشبكات والمعلومات . بصورة أساسية هذه الاطروحة ركزت إهتمامها في دراسة أحد أنواع القنوات السرية في شبكات الحاسوب وهو ما يعرف بالقناة السرية المبنية على أطوال حزم البيانات حيث يمثل هذه النوع من قنوات الإتصال السري مهدد أمني خطير متزايد ومتطور وصعب الإكتشاف.

ساهمت هذه الاطروحة بتقديم وتطوير ثلاثة طرق أو مناهج للتعامل مع مشكلة القنوات السرية ، كما انها قد قدمت منهج رابع يعمل على اكتشافها . هذه المناهج الأربع يمكن تضمينها ضمن نظام واحد يمكن من خلاله معالجة مشكلة القنوات السرية المبنية على أطوال حزم البيانات .المنهج الأول إستهدف القضاء على القنوات السرية عن طريق إخفاء هوية المستخدم عن العملية التي تعمل بالنيابة عنه داخل النظام الحاسوبي. هذا المنهج لا يقضي فقط على القنوات السرية التي تم إكتشافها بل يتجاوزها بالقضاء أيضاً على القنوات محتملة الحدوث والتى لم يتم إكتشافها بعد. المنهج الثاني تعامل مع القنوات السرية المبنية على أطوال حزم البيانات عن طريق تغيير الرسالة المرسلة بطريقة تجعل المستقبل يستقبل رسالة مختلفة تماماً . تم إثبات كفاءة هذا المنهج من خلال قياس نسبة التشابة بين الرسالة الأصلية والرسالة المستلمة من قبل المستقبل. إثنين من أدوات قياس نسبة التشابة والمبنية على قياس التشابه على مستوى المفردات أظهرت صفر نسبة تشابه بينما أداة قياس أخري مبنية على قياس التشابه في المعاني أظهرت نسبة تشابه بلغت 0.0405626 ، وهذا يدل على عدم وجود تشابه وبالتالى كفاءة المنهج . المنهج الثالث هو تطوير للمنهج الثاني حيث يقلل نسبة الأعباء على النظام بـ 50% .وبالتالى فإنه ذو تاثير لا يذكر على أداء النظام . أدوات قياس نسبة التشابه المبنية على المفردات أظهرت صفر نسبة تشابه بينما المبنية على المعاني أظهرت 0.0674704 نسبة تشابه وهذا أيضا يشير إلى عدم وجود تشابه بالتالى كفاءة هذا المنهج. المنهج الرابع قدم طريقة لإكتشاف ذات النوع من القنوات السرية حيث طريقة الإكتشاف بنيت على خوارزميات تعلم الآلة . أظهر هذا المنهج مستوى دقة إكتشاف ممتاز بلغ 98% ، بنسبة صفر خطأ سلبي و 0.02 خطأ إيجابى.