ملخص أطروحة الدكتوراه بعنوان

تطوير نموذج أمن متكيف للوصول إلى حلول أمنية للشبكات الحاسوبية بمردود مثالي للكلفة والزمن

اسم الطالب

م. منير محمّد الوزّة

المشرف

أ.د.م سمير كرمان

المشرف المشارك

أ.د. محمد نور شمه

القسم والاختصاص

هندسة الحواسيب والأتمتة

هندسة الحواسيب وشبكاتها

الملخـــــص

أدى التطور التقني والعلمي إلى زيادة كمية المعلومات الموجودة في الأبحاث والدراسات، وللحفاظ على هذه المعلومات من السرقة والاختراق، تعزز دور الاهتمام بأمن المعلومات، بدءاً من تحديد السياسة الأمنية التي تنظم عمل المستخدمين الموجودين على الشبكة وسماحياتهم، فضلاً عن الأجهزة والبرمجيات؛ مثل الجدر النارية، وأنظمة كشف الاختراق ومنعه ، ومصائد مخترقي الشبكات، وبرامج مكافحة الفيروسات، ويؤدي هذا التنسيق بين هذه التقنيات ،وتحديثها المستمر إلى حماية الشبكة من أي اختراق.

ويتمتع المخترقون بميزة التطور الأسرع، وامتلاكهم للأساليب الخبيثة التي يتّبعونها للوصول إلى الشبكات، في حين يكون التطور بطيئاً في الأجهزة والبرمجيات المضادة، إذ يتطلب زيادة في الكلفة وزمن التحديث، ويُعد هذا عبئاً كبيراً على المؤسسات.

ويسعى المهاجمون إلى اختراق شبكات الجامعات والمعاهد للحصول على المعلومات، وسرقة الخصائص الفكرية والأبحاث، مستغلين بعض الثغرات الأمنية الموجودة في هذه الشبكات. وتفتقر الجامعات ومراكز الأبحاث إلى مشاركة المعلومات حول أي هجوم قد تتعرض له مع بقية الجامعات، وقد يكون مفيداً معرفة طبيعة الهجوم وأسبابه، واتخاذ الأساليب التي تسهم في الوقاية منه، أو الحد منه في بقية الجامعات في حال تعرضها لهجوم مشابه.

ولما كنا جزءاً لا يتجزأ من هذا المجال التعليمي، قمنا بتطوير نموذج للبحث وتحليل الاختراقات وكشفها، ويعتمد هذا النموذج على استخدام نظام منع الاختراق القائم على الاستفادة من مصائد مخترقي الشبكات وكشفه، وهو قادر على التقاط الهجمات الإلكترونية وتحليلها، ومشاركة نتائج التحليل مع الشبكات الأخرى وذلك في الزمن الحقيقي مستفيدين من تقنيات تعلم الآلة، ومن الميزة الافتراضية، ومن ثم توفير الكلفة والزمن، لأن مصدر هذه الأنظمة متاح ومجاني.

PhD dissertation summary

Developing an Adaptable Security Model to have Secure Solutions for Computer Networks with Optimal Cost-Time Efficiency

Student Name

Eng.Muneer Mohammad Alwazzeh

Co-Supervisor

Prof.Mohammad Nour Shamma

Supervisor

Prof. Sameer karaman

Department

Computer and Automation Engineering

Summary

Technical and scientific development has led to an increase in the amount of information available in research and studies, and preserving this information from theft and penetration has reinforced the need to pay attention to information security, starting with defining the security policy that regulates the work of users on the network and their permissions, in addition to hardware and software such as firewalls and intrusion Detection and prevention systems, network intrusion traps(honeypots), and anti-virus programs. coordination between these technologies and their continuous updating will protect the network from any intrusion. Attackers have the advantage of developing faster, and have the malicious methods they use to gain access to networks while the development of hardware and anti-software is slow, which requires an increase in cost and update time, and a huge burden on institutions. Attackers seek to penetrate university and institute networks to obtain information and steal intellectual properties and research by exploiting some of the security vulnerabilities in these networks. Universities and research centers lack to share information about any attack they may be exposed to with the rest of the universities, which is useful in knowing the nature of the attack and its causes and taking the methods that contribute to preventing or mitigating it in the rest of the universities in the event of a similar attack. Being an integral part of this educational field, we have developed a model for research, detection and analysis of penetrations that depends on the use of intrusion detection and prevention systems based on taking advantage of the honeypots and capable of capturing electronic attacks and analyzing them and sharing the results of the analysis with other networks in real time, benefiting from the advantage of machine learning techniques, and virtualization and thus Cost and time savings because these systems are open source and free.