فرم ت ت-↔ به نام خدا

درخواست تصویب موضوع پایان نامه کارشناسی ارشد

نیمسال: دوم سال تحصیلی: ۹۳-۹۴

↔ مشخصات دانشجو, استاد(ان) راهنما و مشاور		
دانشجو: محمود رمضانی	شماره دانشجویی: ۹۲۷۰۰۵۷۳	رشته و گرایش : مهندسی فناوری اطلاعات – شبکه های کامپیوتری
دوره : پردیس بین الملل	گروه: فناوری اطلاعات	دانشکده: پردیس بین الملل
استاد راهنما(↔):جناب آقای دکتر رضا ابراهیمی آتانی	مرتبه دانشگاهی / تخصص:	از:
استاد راهنما(↕):	مرتبه دانشگاهی / تخصص:	از:
استاد مشاور(↔):	مرتبه دانشگاهی / تخصص:	از:
استاد مشاور(↕):	مرتبه دانشگاهی / تخصص:	از:

↕ عنوان پایان نامه و شرح جزئیات آن

الف- عنوان به فارسی:

طراحی و پیاده سازی یک روش دفاع موثر در مقابل حملات مسموم سازی آرپ به وسیله انتقال داده در لایه کاربرد و رمزنگاری آن

ب- عنوان به انگلیسی:

Design and implementation of an efficient defense mechanism against ARP spoofing attacks by transfering ARP data in Application layer and encryption

ج- کلید واژه به انگلیسی:

ARP Spoofing,Man in the middle attack,Encryption

د- نوع کار تحقیقاتی : نظری ☐ تجربی (عملی) ☐ نیمه تجربی (نیمه عملی) ■

ه- توضیح مختصر مساله، فرضیات و هدف از اجرا:

در دنیای امروز هکر ها به خصوص هکر های تروریست و هکر های جنگ های اینترنتی خطر بسیار بزرگی به حساب می آیند .اما خطری که این گروه می تواند ایجاد کند در مقابل آن گروهی که به ما بسیار نزدیک هستند یعنی حمله کنندگان از درون رنگ خود را می بازد .

خطرات امنیتی که حمله کنندگان از درون ایجاد می کنند به هیچ عنوان یک موضوع جدید نیست .دان پارکر در کتاب جرایم کامپیوتری که در سال ۱۹۷۸منتشر شده است برآورد می کند که ۹۵% از حملات کامپیوتری به وسیله کاربران مجاز سیستم ها انجام می گیرد .البته مسلما این موضوع مربوط به زمان پیش از پیداش اینترنت که در آن حمله کنندگان از بیرون دسترسی به سیستم نداشته اند بوده است اما هنوز این مسأله که کاربران مجاز همیشه قابل اعتماد نیستند همچنان باقی مانده است .مطمئنا قضیه کارمندان ناراضی و خرابکار از زمان پیداش خود تجارت وجود داشته است ,اما قدرت کامپیوتر ها و عدم توانائی ما در امن نمودن آن ها در بهترین شرایط قضیه را در دنیای امروز سخت تر کرده است .

به طور کلی سه نوع حمله در این سیستم ها ممکن است اتفاق افتد : سوء استفاده از دسترسی , دور زدن مواضع دفاعی و شکستن ابزار های کنترل دسترسی.

یکی از شایع ترین حملات مورد استفاده علیه افراد و سازمان‌های بزرگ، حملات Man-in-the-Middle است. این حمله یك حمله استراق سمع فعال است که بوسیله برقراری ارتباط با ماشین قربانی و باز پخش پیغام‌ها بین آن‌ها کار می‌کند. در اینگونه موارد،قربانی بر این باور است که با قربانی دیگر به طور مستقیم ارتباط برقرار کرده است در حالی که در حقیقت ارتباط از طریق میزبانی که این حمله را انجام می‌دهد در جریان است. نتیجه نهایی این است که میزبان حمله کننده نه تنها می‌تواند اطلاعات حساس را رهگیری کند، بلکه می تواند برای بدست آوردن کنترل بیشتر سیستم قربانی‌ها، یك جریان داده را تزریق و دستکاری نماید.معروفترین حملات از این نوع شامل آلودگی حافظه پنهان ARP، جعلDNS ، ارتباط ربایی نشست HTTP و.. می‌شود.

یکی از قدیمی ترین اشکال حملات Man-in-the-Middle آلودگی حافظه پنهان ARPبوده است که اجازه می‌دهد مهاجم در زیر شبکه قربانیان خود، ترافیك بین قربانیان در کل شبکه را استراق سمع نماید. با وجود آن که این روش جز ساده‌ترین راه های حمله است ولی به عنوان یکی از موثرترین حملاتی که بوسیله هکرها انجام می‌شود، مطرح شده است.

به دلیل ماهیت پروتکل ARP هیچ یک از راهکار های ارائه شده برای این حمله بدون تغییر توپولوژی شبکه نمی تواند به صورت کامل قربانی را اثرات آن مصون نگه دارد .راهکار ارائه شده در این پایان نامه تبادل داده های پروتکل ARP بین ماشین های یک شبکه به صورت رمزنگاری شده و در لایه کاربرد است بدین ترتیب عملا بسته های پروتکل ARP در شبکه مورد استفاده قرار نخواهند گرفت و امکان سوء استفاده از این پروتکل نیز از بین خواهد رفت .

و- روش پژوهش و مراحل انجام پایان نامه:

همان طور که گفته شد به دلیل ماهیت پروتکل ARP هیچ یک از راهکار های ارائه شده برای این حمله بدون تغییر توپولوژی شبکه نمی تواند به صورت کامل قربانی را اثرات آن مصون نگه دارد .راهکار ارائه شده در این پایان نامه طراحی پروتکلی در لایه کاربرد است که به وسیله رمزنگاری اطلاعاتی را که قبلا به وسیله پروتکل ARP در لایه دیتالینک منتقل می شدند اینک به وسیله این پروتکل در لایه کاربرد و به صورت امن منتقل می گردند بدین طریق حمله مسموم سازی ARP عملا خنثی می گردد.

⬸ فهرست منابع، مواخذ و سوابق علمی

1. ***An Efficient Solution to the ARP Cache Poisoning Problem***
   Vipul Goyal and Rohit Tripathy
   Published in:
   ACISP'05 Proceedings of the 10th Australasian conference on Information Security and Privacy
   Pages 40-51 ©2005

2. ***Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks***
   Seung Yeob Nam, Sirojiddin Djuraev, Minho Park
   Published in:
   Computer Networks: The International Journal of Computer and Telecommunications Networking archive
   Volume 57 Issue 18, December, 2013
   Pages 3866-3884
   Elsevier North-Holland, Inc. New York, NY, USA

3. ***Design and implementation of an efficient defense mechanism against ARP spoofing attacks using AES and RSA***
   Seungpyo Hong, Myeungjin Oh , Sangjun Lee
   Published in:
   Mathematical and Computer Modelling 07/2013; 58(s 1–2):254–260. DOI: 10.1016/j.mcm.2012.08.008

4. ***LAN attack detection using Discrete Event Systems***
   Neminath Hubballi, Santosh Biswas , S. Roopa, Ritesh Ratti, Sukumar Nandi
   Published in:
   Department of Computer Science and Engineering, Indian Institute of Technology, Guwahati 781039, India.
   ISA Transactions (Impact Factor: 2.26). 01/2011; 50(1):119-30. DOI: 10.1016/j.isatra.2010.08.003

5. ***Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN***
   Seung Yeob Nam, Sirojiddin Jurayev, Seung-Sik Kim, Kwonhue Choi and Gyu Sang Choi
   Published in:
   EURASIP Journal on Wireless Communications and Networking 2012

6. ***Monitoring ARP Attack Using Responding Time and State ARP Cache***
   Zhenqi Wang and Yu Zhou
   Published in:
   DOI: 10.1007/978-3-642-01216-7_75 Conference: The Sixth International Symposium on Neural Networks, ISNN 2009, Wuhan, China, May 26-29, 2009, Proceedings, Part IV

7. ***Spoofed ARP Packets Detection in Switched LAN Networks***
   Zouheir Trabelsi and Khaled Shuaib
   Published in:
   DOI: 10.1007/978-3-540-70760-8_7 Conference: SECRYPT 2006, Proceedings of the International Conference on Security and Cryptography, Setúbal, Portugal, August 7-10, 2006, SECRYPT is part of ICETE - The International Joint Conference on e-Business and Telecommunications

8. ***Insider Attack and Cyber Security Beyond the Hacker***
   Sushil Jajodia
   Published in:
   Insider Attack and Cyber Security: Beyond the Hacker (Advances in Information Security)
   Springer-Verlag TELOS Santa Clara, CA, USA ©2008
   ISBN:0387773215 9780387773216

9. ***THE TCP/IP GUIDE***
A Comprehensive, Illustrated Internet Protocols Reference
by Charles M. Kozierok
Published in*:*
No Strach Press
October 2005, 1616 pp.
ISBN: 978-159327-047-6

10. ***TARP: Ticket-based address resolution protocol***
Wesam Lootah, William Enck, Patrick McDaniel
Published in:
Computer Networks: The International Journal of Computer and Telecommunications Networking archive
Volume 51 Issue 15, October, 2007
Pages 4322-4337

⇢منابع مالی تامین هزینه اجرای پایان نامه، مدت زمان اجرا

هزینه انجام پایان نامه‌های کارشناسی ارشد در هر سال توسط شورای تحصیلات تکمیلی دانشگاه تعیین و توسط دانشکده‌ها قابل پرداخت خواهد بود. در صورتی که بخشی از هزینهٔ انجام پایان نامه از محل‌های دیگر تامین می‌شود، ذکر نام سازمان، مبلغ و مشخصه‌ای از قرار داد، الزامی است.

مدت انجام پایان‌نامه کارشناسی ارشد یک سال تحصیلی است. تمدید این زمان، منوط به موافقت شورای تحصیلات تکمیلی دانشکده حسب مقررات دانشگاه است.

امضای دانشجو	امضای استاد(ان) راهنما	امضای استاد(ان) مشاور
تاریخ	تاریخ	تاریخ

⇡ مراحل تصویب عنوان پایان نامه

گروه درجلسه تحصیلات تکمیلی مورخ با انجام پایان نامه موافقت کرد.

امضای مدیر گروه – تاریخ

دانشکده درجلسه تحصیلات تکمیلی مورخ با انجام پایان نامه موافقت کرد.

امضای مدیر تحصیلات تکمیلی دانشکده – تاریخ

شورای تحصیلات تکمیلی دانشگاه در جلسه مورخ انجام پایان نامه فوق را تصویب کرد.

امضای مدیر تحصیلات تکمیلی دانشگاه – تاریخ