

جنگ سایبری

ایجاد پایه و اساس علمی



مؤسسه آموزشی و تحقیقاتی صنایع دفاعی

حوزه نوآوری آرایه‌های دفاعی

دارای مجوز سازمانی نشر از شورای سیاست‌گذاری و نظارت بر انتشارات

مؤسسه آموزشی و تحقیقاتی صنایع دفاعی

کلیه‌ی حقوق محفوظ و متعلق به مؤسسه آموزشی و تحقیقاتی صنایع دفاعی است.

هر نوع تکثیر یا نشر تمام یا بخش‌های مستقلی از این کتاب، منوط به اجازه کتبی ناشر است.

عنوان و نام : جنگ سایبری (ایجاد پایه و اساس علمی) // نویسندگان سوشیل جاجودیا ...
پدیدآور [و دیگران]؛ مترجم حوزه نوآوری آرایه‌های دفاعی.
مشخصات نشر : تهران: مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، حوزه نوآوری آرایه‌های
دفاعی، ۱۳۹۶.

مشخصات ظاهری : ۵۳۷ ص.

شابک : ۹۷۸۶۰۰۸۷۹۳۲۶۷

عنوان اصلی : Cyber Warfare Building the Scientific Foundation, c2015

موضوع : شبکه‌ای کامپیوتری -- تدابیر ایمنی -- تروریسم رایانه‌ای -- ایمنی
اطلاعات -- پیشگیری -- فضای مجازی -- امنیت ملی

شناسه افزوده : جاجودیا، سوشیل ۱۹۴۱ - م. Jajodia, Sushil

شناسه افزوده : مؤسسه آموزشی و تحقیقاتی صنایع دفاعی. حوزه نوآوری آرایه‌های دفاعی

رده بندی کنگره : ۱۳۹۶ ج۹/TK ۵۱۰۹/۵۹

رده بندی دیویی : ۰۰۵/۸ شماره کتابشناسی ملی: ۵۰۸۷۰۶۳

عنوان: جنگ سایبری، ایجاد پایه و اساس علمی

مترجم: حوزه نوآوری آرایه‌های دفاعی

ناشر: مؤسسه آموزشی و تحقیقاتی صنایع دفاعی - حوزه نوآوری آرایه‌های دفاعی

آماده‌سازی و نظارت بر ترجمه و چاپ: مدیریت دانش حوزه نوآوری آرایه‌های دفاعی

نوبت چاپ: اول - زمستان ۱۳۹۶

شمارگان: ۵۰۰ جلد

قیمت: ۴۰۰۰۰ تومان

نشانی: بالاتر از میدان نوبنیاد، پاسداران شمالی، نبش کوهستان هشتم، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی،

نمابر: ۲۲۸۰۸۷۷۴

تلفن: ۲۲۸۰۸۷۰۷

پیش‌گفتار نویسنده

وابستگی هرچه بیشتر و امن‌تری به شبکه‌های کامپیوتری، گوشی‌های هوشمند و اینترنت هدف جدید در زمان درگیری‌ها فراهم ساخته است. درواقع، جنگ سایبری^۱ به عنوان بخشی از سیاست‌های کشور از قبل شکل گرفته است. برای درک آثار آشکار شده این حوزه در جریان شمشادخت کافی است سرخط اختیار رادیو و تلویزیون و تیتراژ درشت روزنامه‌ها را در جریان جنگ روسیه و گرجستان در زمینه‌های استاکس‌نت^۲، آئورورا^۳ یا حملات سایبری مورد توجه قرار دهیم.

در حالی که ما شاهد بسیاری مفاهیم پیشرفته مهندسی (مانند ایجاد دیوارهای آتش، ابزار متا اسپلویت) یا حتی بدافزارهای پیشرفته مانند «Stuxnet» که به‌طور مستقیم بر روی جنگ سایبری تأثیر می‌گذارند، هستیم، تمامی این مفاهیم‌ها براساس بهترین تجربیات، قانون کلی، فنون سعی و خطا توسعه یافته‌اند. هرچند که این اختراعات تأثیر زیادی دارند و از اهمیت بالایی برخوردارند، تاریخ به‌طور مکرر به

1 Cyber Warfare

2 Stuxnet

3 Aurora

ما آموخته است که استقرار اصول علمی منجر به پیشرفت سریع و قابل توجه خواهد شد.

از این رو، این کتاب برای استقرار پایه و اساس علمی برای جنگ سایبری طراحی شده است. در این کتاب مجموعه‌ای از آخرین نتایج تحقیقات در این زمینه که حاصل کار چندین محقق برتر در گوشه‌کنار جهان است، گردآوری شده است. در این کتاب، بسیاری از جنبه‌های مهم درگیری‌های سایبری که شامل استفاده از بات‌نت‌ها، موقعیت‌یابی کندوهای عسل، انکار و فریب، عامل انسانی و مشکل انتساب می‌شود، مورد بررسی قرار می‌گیرد. افزون بر این، در این کتاب تلاش شده است که تنها بر روی جنبه‌های ساده و مختلف از جنگ سایبری تمرکز نشود، بلکه به بسیاری از فنون علمی گسترده‌ای که می‌تواند برای حل کردن مشکلات موجود در این حوزه مورد استفاده قرار گیرند پرداخته شود. فصل‌های این کتاب به مسائلی مانند نظریه بازی، مدل‌سازی شناختی، بهینه‌سازی، برنامه‌ریزی منطقی، تجزیه و تحلیل داده‌های عظیم و چندین مورد دیگر می‌پردازد.

امیدواریم که این کتاب الهام‌بخش محققان برای ایجاد دانش‌های بیشتر در حوزه جنگ سایبری گردد و در نهایت بتوان اینترنت را امن‌تر و قابل اعتمادتر نمود.

درباره کتاب

سه فصل اول این کتاب بعضی از دیدگاه‌ها و اصول جنگ سایبری را معرفی می‌کنند. در فصل اول، تأثیر استفاده از حملات سایبری به عنوان تسلیحات راهبردی کلیدی در درگیری‌های بین‌المللی بررسی می‌شود و مدل‌های تئوری مبتنی بر بازی برای حل مشکلات موجود در زمینه جنگ سایبری ارائه می‌شوند. در فصل دوم، قابلیت جدیدی بر اساس مدل‌سازی چند فرمالیسمی ارائه می‌شود و سپس این قابلیت تجزیه و تحلیل می‌شود و تأثیرات حملات سایبری در زمینه هماهنگی برای

تصمیم‌گیری در سازمان‌ها گفته می‌شود. در فصل سوم، توضیح داده می‌شود که چگونه مهاجمی که از برتری سایبری برخوردار است دارای مزایای خوبی در به دست آوردن اهداف مأموریتی خود می‌باشد.

فصل‌های بعدی فریب سایبری و رویکردهای مبتنی بر بازی را بررسی می‌کنند. در فصل چهارم، یک چارچوب نظریه بازی برای برنامه‌ریزی در زمینه ایجاد طرح‌های موفق برای فریب دشمن در فضای سایبر ارائه می‌شود. در فصل پنجم، استفاده از نظریه بازی برای امنیت شبکه بررسی می‌شود و چندین مدل برای نظریه بازی ارائه می‌شود که بر روی استفاده از تله‌های عسل^۱ برای امنیت شبکه تمرکز دارند. در فصل ششم، مبارزه با فریبکاری سایبری توضیح داده می‌شود و اینکه چگونه می‌توان آن را در دفاع سایبری برای شناسایی و مقابله با مهاجمان سایبری به کار برد. در فصل هفتم، چالش‌های یافتن دشمنان سایبری از طریق نظارت بر شبکه توضیح داده می‌شود، حتی وقتی که دشمنان از عملیات فریبکاری برای پنهان‌سازی فعالیت‌ها و نیت خود استفاده می‌کنند. در فصل هشتم، یک سیستم مبتنی بر استدلال رسمی که به تحلیل‌گر در زمینه انتساب حملات سایبری کمک می‌کند (حتی در زمانی که اطلاعات در دسترس، متناقض و یا نامشخص هستند) ارائه می‌شود.

در فصل‌های ۹ تا ۱۲ جنبه‌های رفتاری و اجتماعی امنیت سایبری و جنگ سایبری بررسی می‌شوند. در فصل نهم، نقش عامل انسانی در امنیت سایبری (هم برای مهاجمان و هم برای مدافعان) بررسی می‌شود. در فصل دهم، یک مدل معروف، چندعاملی و شناختی برای تصمیم‌گیری (که از طریق تجربه و مطالعه رفتاری به دست آمده است) ارائه می‌شود. در فصل یازدهم، مشکل یافتن گره‌های پنهان در

شبکه‌های اجتماعی برای انجام حملات سایبری بررسی می‌شود. در فصل دوازدهم، الگوریتم‌هایی که ساختار جامعه را درون شبکه‌ها کشف می‌کنند و آن‌ها را با یکدیگر مقایسه می‌کنند بررسی می‌شوند.

فصل‌های سیزدهم و چهاردهم بر مبنای فیلد داده‌های مقیاس بزرگ از میان میلیون‌ها میزبان واقعی می‌باشند. در فصل سیزدهم، نتایج مطالعات تجربی انجام شده در رمنه امنیت جهان واقعی با استفاده از داده‌های جمع‌آوری شده از ۱۰ میلیون میزبان واقعی ارائه شده است. در فصل چهاردهم، تکنیک‌های استفاده از کاوش گراف در مجرعه‌های فیلد داده بزرگ برای حل مشکلات امنیت سایبری بررسی می‌شوند. نهایتاً در فصل پانزدهم، توضیح داده می‌شود که چگونه پیشرفت در زمینه زبان برنامه‌نویسی می‌تواند مشکلات سایبری و امنیت کامپیوتری را حل کند. همچنین در این فصل توضیح داده می‌شود که تکنیک‌های تحقیقاتی کنونی برای ضمانت امنیت ناکافی هستند.

فهرست مطالب

فصل اول: بازی‌های جنگ سایبری: رقابت راهبردی در بین دشمنان سنتی	۲۱
۱-۱- مقدمه	۲۲
۲-۱- جنگ سایبری	۲۵
۳-۱- نظریه بازی	۳۰
۱-۳-۱- نظریه بازی در روابط بین‌الملل	۳۳
۴-۱- تدوین مشکل	۳۵
۵-۱- نتیجه‌گیری	۴۵
منابع	۴۶
فصل دوم: جایگزین‌هایی برای جنگ سایبری: بازدارندگی و تضمین	۴۹
۱-۲- مقدمه	۵۰
۲-۲- به‌کارگیری چندین مدل برای بازدارندگی سایبری	۵۴
۳-۲- مدل‌سازی چند فرمالیسمی	۵۸
۴-۲- مدل سازمانی تصمیم‌گیری	۶۰
۵-۲- اقدامات	۶۳

۶۸.....	۶-۲- مدل شبکه‌ای
۶۸.....	۷-۲- مدل‌سازی حملات سایبری
۶۹.....	۸-۲- شرح کوتاهی از «Pacifica»
۷۰.....	۸-۲-۱- مدل سازمانی
۷۶.....	۸-۲-۲- مدل شبکه‌ای و حملات سایبری
۷۸.....	۹-۲-۱- نمایش محاسباتی و نتایج آن
۸۳.....	۹-۲-۱- نتیجه‌گیری
۸۴.....	منابع
۸۷.....	فصل سوم: تسخیر به برداری از برتری سایبری برای بات‌نت‌ها
۸۸.....	۳-۱- مقدمه
۹۰.....	۳-۱-۱- مشارکت
۹۱.....	۳-۲- مفهوم برتری سایبری: یک مثال
۹۷.....	۳-۳- انواع مأموریت
۹۹.....	۳-۴- شناسایی برتری سایبری
۱۰۰.....	۳-۴-۱- بررسی اجمالی مفهوم
۱۰۱.....	۳-۴-۲- توصیف اثربخشی
۱۰۲.....	۳-۴-۳- توصیف مخفی‌کاری
۱۰۳.....	۳-۴-۴- یافتن برتری بهینه‌ی سایبری و ساختار C2
۱۰۶.....	۳-۵- شبیه‌سازی و نتایج
۱۰۶.....	۳-۵-۱- توصیف مورد کاربرد
۱۰۹.....	۳-۵-۲- نتایج
۱۱۵.....	۳-۵-۳- نقاط خلاصه
۱۱۶.....	۳-۶- برتری دفاعی

۱۲۰.....	۷-۳- نتیجه‌گیری
۱۲۱.....	منابع
	فصل چهارم: انتساب، وسوسه و انتظار: چارچوب رسمی دفاع توسط فریب دشمن
۱۲۵.....	در جنگ سایبری
۱۲۶.....	۱-۴- مقدمه
۱۲۶.....	۱-۱-۴- چالش‌های جنگ سایبری
۱۲۷.....	۱-۱-۴- پایه و اساس فریب سایبری
۱۲۹.....	۱-۴-۳- فریب، گشت‌نگاری مهاجم: یک مطالعه موردی
۱۳۲.....	۲-۴- انگشت‌نگاری مدافع: سستی
۱۳۳.....	۱-۲-۴- دوره زمانی بازی انگشت‌نگاری
۱۳۵.....	۲-۲-۴- تست‌های انگشت‌نگاری
۱۳۹.....	۲-۲-۴- جستجوهای انگشت‌نگاری
۱۴۱.....	۴-۲-۴- محاسبه بهره اطلاعاتی
۱۴۲.....	۳-۴- فریب انگشت‌نگاری: مدل بازی
۱۴۶.....	۱-۳-۴- مدل راهبردی
۱۵۰.....	۲-۳-۴- مدل منفعت
۱۵۲.....	۳-۳-۴- مدل بازدهی
۱۵۶.....	۴-۴- تجزیه و تحلیل بازی انگشت‌نگاری
۱۵۶.....	۱-۴-۴- روش تجزیه و تحلیل: بازی بایزی کامل
۱۵۷.....	۲-۴-۴- بازی انگشت‌نگاری: نتایج
۱۵۸.....	۵-۴- ساز و کار بازی فریب
۱۵۹.....	۱-۵-۴- ساز و کار انتخاب راهبرد
۱۶۰.....	۲-۵-۴- مسائل پیاده‌سازی

- ۴-۶- ارزیابی ۱۶۰
- ۴-۶-۱- بررسی کارایی و ویژگی‌ها ۱۶۰
- ۴-۷- کارهای مرتبط ۱۶۶
- ۴-۸- خلاصه ۱۶۶
- منابع ۱۶۷
- فصل پنجم: بنای نظریه بازی برای استفاده راهبردی از کندوهای عسل در امنیت سایبری ۱۷۱
- ۵-۱- مقدمه ۱۷۲
- ۵-۲- پیش‌زمینه ۱۷۵
- ۵-۲-۱- نظریه بازی ۱۷۵
- ۵-۲-۲- بازی‌های امنیتی ۱۷۸
- ۵-۲-۳- بازی‌های فریب‌کاری ۱۸۱
- ۵-۳- کندوهای عسل ۱۸۳
- ۵-۴- بازی انتخاب کندوی عسل ۱۸۵
- ۵-۵- انتخاب کندوی عسل با جستجوهای مزاحم ۱۹۰
- ۵-۶- راهبردهای کندوی عسل برای بازی‌ها در گراف -حمله ۱۹۴
- ۵-۷- بحث ۱۹۹
- ۵-۸- نتیجه‌گیری ۲۰۵
- منابع ۲۰۶
- فصل ششم: مقابله با فریب‌کاری در فضای سایبر: چگونگی شناسایی انکار و فریب‌کاری ۲۱۱
- ۶-۱- انکار و فریب‌کاری چیست؟ ۲۱۲
- ۶-۲- مقابله با فریب‌کاری چیست؟ ۲۱۳

۲۱۶.....	۳-۶- فریب کاری متقابل چیست؟
۲۱۸.....	۴-۶- مقابله فریب کاری سایبری چیست؟
۲۲۴.....	۵-۶- مؤلفه های مقابله با فریب کاری کدامند؟
۲۳۲.....	۶-۶- زنجیره های حمله مهاجم سایبری و عملیات نفوذ
۲۳۷.....	۷-۶- زنجیره های فریب کاری مدافع سایبری و عملیات فریب کاری
۲۴۰.....	۸-۶- اعمال مقابله با فریب کاری در فعالیت های فریب کاری
۲۴۱.....	۹-۶- مدل پردازش مقابله با فریب کاری سایبری
۲۵۸.....	۱۰-۶- بازی جنگ، کار، فریب کاری سایبری و مقابله با فریب کاری سایبری
۲۶۰.....	۱-۱۰-۶- مبانی حمله
۲۶۴.....	۱۱-۶- آینده ی مبارزه با فریب کاری سایبری در دفاع سایبری فعال
۲۷۴.....	منابع
۲۸۵.....	فصل هفتم: پرو فایل سازی به صورت خودکار
۲۸۶.....	۱-۷- مقدمه
۲۸۸.....	۲-۷- هستی شناسی دشمن
۲۹۱.....	۳-۷- تولید فرضیه دشمن
۲۹۳.....	۴-۷- پیش بینی اقدامات دشمن
۲۹۵.....	۵-۷- استنباط از مشاهدات مورد انتظار
۲۹۶.....	۶-۷- برآورد کردن احتمال دشمن
۲۹۷.....	۷-۷- نتیجه گیری
۲۹۸.....	منابع
۳۰۱.....	فصل هشتم: انتساب حملات سایبری: یک رویکرد مبتنی بر استدلال
۳۰۲.....	۱-۸- مقدمه
۳۰۴.....	۲-۸- دو نوع مدل

- ۳۱۰..... ۸-۲-۱- مدل محیطی
- ۳۱۵..... ۸-۲-۲- مدل تحلیلی
- ۳۲۷..... ۸-۳- چارچوب «InCA»
- ۳۳۲..... ۸-۴- پرس وجوهای انتساب
- ۳۳۵..... ۸-۵- سؤالات مطرح
- ۳۳۵..... ۸-۵-۱- یادگیری قواعد
- ۳۳۵..... ۸-۵-۱- اصلاح باور
- ۳۳۷..... ۸-۵-۲- استدلال زمانی
- ۳۳۷..... ۸-۵-۴- پرس وجوهای استنتاج حدسی
- ۳۳۸..... ۸-۶- نتیجه گیری
- ۳۳۹..... منابع
- فصل نهم: عامل انسانی در امنیت سایبری: تقویت سازی و دفاع هوشمندانه ۳۴۳..
- ۳۴۴..... ۹-۱- مشکل سایبری
- ۳۵۰..... ۹-۱-۱- خرید آنلاین از خانه و اداره
- ۳۵۳..... ۹-۱-۲- کنترل ترافیک هوایی
- ۳۵۴..... ۹-۱-۳- بازارهای بورس
- ۳۵۵..... ۹-۱-۴- نگرانی های اطلاعاتی
- ۳۵۶..... ۹-۱-۵- عنصر انسان
- ۳۵۶..... ۹-۲- بررسی اجمالی: رویکرد مقابله با مشکل
- ۳۵۸..... ۹-۳- مشکلات سایبری فراگیر شده اند
- ۳۵۹..... ۹-۳-۱- خطرات
- ۳۶۱..... ۹-۳-۲- کاربران ناآگاه
- ۳۶۳..... ۹-۳-۳- منشأ بدافزار، تعمیر و فریب کاری

۳۶۴.....	۹-۳-۴- منشأ تهدیدات
۳۶۷.....	۹-۴- محیط سایبری پیچیده
۳۶۷.....	۹-۴-۱- لایه‌های سایبری
۳۶۸.....	۹-۴-۲- عامل‌های مخرب
۳۶۹.....	۹-۴-۳- رسانه اجتماعی
۳۶۹.....	۹-۵- رویکردهای مهندسی
۳۶۹.....	۹-۵-۱- ملکه سرخ
۳۷۰.....	۹-۵-۲- سرزنس کاران
۳۷۰.....	۹-۵-۳- تکیه بر فداکاری
۳۷۲.....	۹-۵-۴- آسیب‌پذیری کاربر
۳۷۴.....	۹-۶- دشمنان هوشمند
۳۷۴.....	۹-۶-۱- تغییر ابزارها و تکنیک‌ها
۳۷۴.....	۹-۶-۲- استفاده از فریب‌کاری برای دفاع
۳۷۵.....	۹-۷- تحقیق کنونی
۳۷۵.....	۹-۷-۱- نظریه
۳۷۷.....	۹-۷-۲- انتساب
۳۷۸.....	۹-۷-۳- ساختارهای شناختی
۳۸۰.....	۹-۷-۴- سؤالات امنیت سایبری
۳۸۱.....	۹-۷-۵- نظریه وابستگی متقابل
۳۸۷.....	۹-۷-۶- ارتباطات میان تیم‌ها
۳۸۹.....	۹-۷-۷- خلاصه
۳۹۲.....	۹-۸- نتیجه‌گیری
۳۹۸.....	منابع

فصل دهم: بازی جنگ سایبری: الگویی برای درک چالش‌های جدید در جنگ

سایبری	۴۰۹
۱-۱۰- مقدمه	۴۱۰
۱۰-۲- افزایش مقیاس: از نظریه فردی به نظریه بازی رفتاری	۴۱۲
۱۰-۳- بازی جنگ سایبری	۴۱۸
۱۰-۱-۱- یک مدل شناختی از یک جنگجوی سایبری	۴۲۲
۱-۳-۲- تحقیق کنونی بر روی بازی جنگ سایبری	۴۲۴
۱۰-۴- خلاصه و نتیجه‌گیری	۴۳۰
منابع	۴۳۱
فصل یازدهم: جستجوی فعال‌های پروفایل‌های پنهان در رسانه‌های اجتماعی با	
استفاده از بدافزار	۴۳۷
۱۱-۱- مقدمه	۴۳۸
۱۱-۲- پیش‌زمینه و کارهای مرتبط	۴۴۰
۱۱-۲-۱- شبکه اجتماعی تروریست‌ها	۴۴۰
۱۱-۲-۲- انتشار و همه‌گیری شبکه‌های اجتماعی	۴۴۲
۱۱-۲-۳- بازیابی اطلاعات از دست‌رفته در شبکه‌های اجتماعی	۴۴۴
۱۱-۳- مشکل انتشار متمرکز در شبکه‌های اجتماعی	۴۴۶
۱۱-۴- راهبردهای جای‌گذاری دانه	۴۴۹
۱۱-۵- ارزیابی راهبردهای جای‌گذاری دانه‌ها	۴۵۳
۱۱-۶- خلاصه	۴۶۰
منابع	۴۶۱
فصل دوازدهم: بررسی الگوریتم‌های تشخیص اجتماع بر اساس تجزیه و تحلیل نیت	
۱۲-۱- مقدمه	۴۶۶

۴۶۸.....	۱۲-۲- تجزیه و تحلیل نیت
۴۷۱.....	۱۲-۳- رویکردهای شناسایی اجتماعی شبکه‌ای
۴۷۲.....	۱۲-۳-۱- الگوریتم‌های مبتنی بر سلسله‌مراتب
۴۷۲.....	۱۲-۳-۱-۱- روش‌های تقسیم‌کننده
۴۷۹.....	۱۲-۳-۱-۲- روش‌های متراکم‌شونده
	۱۲-۳-۳- الگوریتم‌های مبتنی بر سلسله‌مراتب، با در نظر گرفتن
۴۸۳.....	تجزیه و تحلیل نیت
۴۸۴.....	۱۲-۳-۲- رویکردهای مبتنی بر مدل تهی
	۱۲-۳-۲-۱- الگوریتم‌های مبتنی بر مدل تهی، با در نظر گرفتن
۴۹۱.....	تجزیه و تحلیل نیت
۴۹۲.....	۱۲-۳-۳- الگوریتم‌های مبتنی بر استنباط آماری
	۱۲-۳-۳-۱- الگوریتم‌های مبتنی بر استنباط آماری، با در نظر گرفتن
۵۰۲.....	تجزیه و تحلیل نیت
۵۰۲.....	۱۲-۳-۴- الگوریتم‌های مبتنی بر گروه
۵۰۵.....	۱۲-۳-۴-۱- الگوریتم‌های مبتنی بر گروه، با در نظر گرفتن تجزیه و تحلیل نیت
۵۰۵.....	۱۲-۴- نتیجه‌گیری
۵۰۸.....	منابع
	فصل سیزدهم: درک چرخه آسیب‌پذیری برای ارزیابی خطر و دفاع قابل حملات
۵۱۵.....	سایبری پیشرفته
۵۱۶.....	۱۳-۱- مقدمه
۵۲۰.....	۱۳-۲- کارهای انجام‌شده‌ی پیشین
۵۲۴.....	۱۳-۳- منابع داده‌ای
۵۲۹.....	۱۳-۴- توصیف چرخه‌ی حیات آسیب‌پذیری

- ۱۳-۴-۱- فراوانی و مدت زمان حملات روز صفر ۵۲۹
- ۱۳-۴-۲- آسیب پذیری های روز صفر بعد از افشاء شدن ۵۳۷
- ۱۳-۴-۳- نسبت بهره برداری از آسیب پذیری ها ۵۴۰
- ۱۳-۵- گفتگو ۵۴۵
- ۱۳-۵-۱- سؤالات مطرح ۵۴۸
- ۱۳-۶- نتیجه گیری ۵۵۰
- منابع ۵۵۱
- فصل چهارم: روش گراف برای امنیت سایبری ۵۵۹
- ۱۴-۱- مقدمه ۵۶۰
- ۱۴-۲- کارهای مرتبط انجام داده ی پیشین ۵۶۲
- ۱۴-۲-۱- انتشار ویروس ۵۶۳
- ۱۴-۲-۲- فرآیند انتشار در گراف ۵۶۵
- ۱۴-۲-۳- داده کاوی برای امنیت ۵۶۷
- ۱۴-۳- کاوش آبشاری ۵۶۸
- ۱۴-۳-۱- نظریه: نکات اصلی و رقابت ۵۶۹
- ۱۴-۳-۱-۱- گلوگاه های همه گیری برای گراف های شبکه ای ۵۶۹
- ۱۴-۳-۱-۲- همزیستی با ویروس های رقابتی ۵۷۰
- ۱۴-۳-۱-۳- همزیستی ویروس ها ناسازگار ۵۷۰
- ۱۴-۳-۲- الگوریتم ها: امن سازی، جای گذاری یال، یافتن مجرمان ۵۷۱
- ۱۴-۳-۲-۱- امن سازی کسری ۵۷۱
- ۱۴-۳-۲-۲- امن سازی کامل و جای گذاری یال ۵۷۲
- ۱۴-۳-۲-۳- یافتن مجرمان سایبری ۵۷۳
- ۱۴-۳-۳- مطالعات تجربی: ایجاد روش های بهتر ۵۷۴

۵۷۵.....	۴-۱۴- مجموعه‌های داده‌ای
۵۷۶.....	۱-۴-۱۴- دورسنجی ضدویروس
۵۷۷.....	۲-۴-۱۴- شهرت دودویی
۵۷۹.....	۵-۱۴- توصیف انتشار فایل
۵۷۹.....	۱-۵-۱۴- الگوهای انتشار زمانی
۵۸۲.....	۱-۵-۱۴- مدل «SharkFin»
۵۸۳.....	۲-۵-۱۴- بائیرات نمونه‌گیری
۵۸۵.....	۶-۱۴- گفتگو
۵۸۷.....	۱-۶-۱۴- سؤالات مطرح
۵۸۹.....	۷-۱۴- نتیجه‌گیری
۵۸۹.....	منابع
۵۹۷.....	فصل پانزدهم: امنیت نظری زبان برنامه‌نویسی در جهان واقعی: یک سراب یا آینده؟
۵۹۸.....	۱-۱۵- مقدمه
۶۰۳.....	۲-۱۵- مطالعات موردی
۶۰۳.....	۱-۲-۱۵- شرکت «HBGray»
۶۰۶.....	۲-۲-۱۵- شرکت «RSA»
۶۰۸.....	۳-۲-۱۵- خون‌ریزی قلبی
۶۰۹.....	۴-۲-۱۵- نرم‌افزارها دارای مشکل هستند
۶۱۰.....	۳-۱۵- اجرای امنیت از طریق زبان‌های برنامه‌نویسی
۶۱۸.....	۴-۱۵- موردی علیه تقویت‌سازی امنیت از طریق زبان‌های برنامه‌نویسی
۶۲۱.....	۵-۱۵- ملاحظات عملی
۶۲۳.....	۵-۱۵- نتیجه‌گیری
۶۲۴.....	منابع