

آگاهی وضعیتی سایبری

تألیف:

علی جبار رشیدی

کوروش داداش تبار احمدی

بهزاد نظرپور

سرشناسه:	رشیدی، علی جبار، ۱۳۴۹ -
عنوان و نام پدیدآور:	آگاهی وضعیتی سایبری / تألیف علی جبار رشیدی، کوروش داداش تباراحمدی، بهزاد نظریور.
مشخصات نشر:	تهران: دانشگاه صنعتی مالک اشتر، ۱۳۹۶
مشخصات ظاهری:	م، ۳۷۱ ص: مصور(رنگی)، جدول، نمودار(بخشی رنگی).
شابک:	۹۷۸-۶۰۰-۷۷۳۶-۲۱-۰
وضعیت فهرست‌نویسی:	فیا.
یادداشت:	واژه‌نامه
یادداشت:	کتابنامه: ص. [۳۲۸]-۳۵
موضوع:	ترورسم رایانه‌ای - پیشگیری
موضوع:	جنگ اطلاعاتی
موضوع:	فضای مجازی - تدابیر ایمنی.
شناسه داده:	داداش تباراحمدی، کوروش، ۱۳۵۵ -
شناسه روده:	نظریور، بهزاد، ۱۳۶۰ -
شماره افز:	دانشگاه صنعتی مالک اشتر. انتشارات.
رده‌بندی کنگره:	۱۳۹۶ هـ ۴/۱۵/۶۷۷۳ HV
رده‌بندی دی‌سی:	۳۶۳/۳۱
کتابشناسی ملی:	۴۹۷۶۵۳۴



دانشگاه صنعتی مالک اشتر

مجموعه فناوری اطلاعات و ارتباطات و امنیت

عنوان کتاب:	آگاهی وضعیتی سایبری
تألیف:	علی جبار رشیدی - کوروش داداش تباراحمدی - بهزاد نظریور
ناشر:	انتشارات دانشگاه صنعتی مالک اشتر
طرح روی جلد:	فریناز عسگری
لیتوگرافی، چاپ و صحافی:	دانشگاه صنعتی مالک اشتر
صفحه‌آرایی رایانه‌ای:	امین پژوهش
ویراستار ادبی:	امین پژوهش
شمارگان:	۱۰۰۰ جلد
نوبت چاپ:	اول، پاییز ۹۶
قیمت:	۲۷۰.۰۰۰ ریال

ISBN: 978-600-7736-21-0

کلیه حقوق چاپ برای ناشر محفوظ است.

نقل مطالب فقط با ذکر مشخصات کامل کتاب و با اشاره به نام ناشر مجاز است.
آدرس: تهران، لویزان، دانشگاه صنعتی مالک اشتر، معاونت پژوهش و فناوری، مدیریت دانش
انتشارات. تلفن: ۲۲۹۳۲۸۹۱

پیشگفتار

افزایش بی سابقه حملات سایبری به شبکه‌های سازمانی و افزایش پیچیدگی این حملات سبب شده تا انگیزه پژوهش در زمینه آگاهی وضعیت سایبری روز به روز گسترش یابد. پژوهش‌هایی که تاکنون در این حوزه انجام گرفته بیش‌تر بر چگونگی درک راهبردهای پنهان مرحله‌ای و پیچیده حملات و همچنین پیش‌بینی اقدامات آینده حمله متمرکز بوده است. هر چند این تلاش‌ها، ایده‌هایی نویدبخش و جدید برای حوزه آگاهی وضعیت سایبری به همراه داشته است اما ارزیابی میزان اثربخشی آن‌ها مغفول مانده است. نبود فرآیندهای استاندارد، داده‌های استاندارد و قابل رجوع برای ارزیابی ابزارهای آگاهی وضعیت سایبری، نیز یکی دیگر از مشکلات این حوزه است که آن هم بی دلیل نیست؛ چرا که تولید مجموعه داده‌ای واقعی که بتواند حملات چند مرحله‌ای روی پیکربندی‌های متنوع و بزرگ شبکه به همراه طیف کامل مهارت‌های نفوذ و حمله را فراهم نماید کار بسیار پرهزینه و زمان‌بری است.

هدف اصلی این کتاب که بر مبنای مطالعات و پژوهش‌های چندساله نویسندگان آن نگارش شده است ارائه، تحلیل، نقد و تدوین اطلاعات و دسترسی و کاربردی در زمینه آگاهی وضعیت سایبری است؛ به گونه‌ای که بتوان از این کتاب به شکل موثری در سطوح مختلف از جمله آموزش در مقاطع تحصیلات تکمیلی و پژوهش استفاده نمود.

در این کتاب مفاهیم، نظریه‌ها، مدل‌ها، معماری‌ها و کاربردهای آگاهی وضعیت سایبری و تجربیات موجود در این زمینه مورد مطالعه و بررسی قرار می‌گیرد که ساختار محتوایی فصل‌ها و بخش‌های آن به‌طور خلاصه در ادامه آمده است.

در فصل اول، اهمیت فضای سایبر و تعاریف مربوط به آگاهی وضعیتی در این فضا مورد بحث قرار گرفته، و در ادامه مدل‌های مربوط به آگاهی وضعیتی سایبری به همراه الزامات و چالش‌های پیش‌رو در زمینه سامانه‌های آگاهی وضعیتی سایبری مورد بررسی قرار می‌گیرند. در نهایت معیارهای ارزیابی کارایی در سامانه‌های مذکور تشریح می‌شوند. در فصل دوم، مفاهیم و تعاریف کلی مقوله آگاهی وضعیتی تبیین شده و انواع مدل‌های ادغام اطلاعات که در سامانه‌های آگاهی وضعیتی کاربرد دارند، به همراه آگاهی وضعیتی سایبری مبتنی بر ادغام اطلاعات چندحسگری به‌طور مفصل تشریح می‌شوند.

در فصل سوم، فرآیند درک و فهم حملات سایبری که نقش بسزایی در سامانه‌های آگاهی وضعیتی سایبر ایفا می‌کند، در قالب فرآیندهای همبسته‌سازی هشدار و تولید سناریوهای حملات مورد بحث قرار گرفته و مفاهیم نوظهوری نظیر موتور ادغام اطلاعات در ردگیری حملات سایبری، مبانی هوشمندسازی این موتورها مورد تحلیل قرار می‌گیرد. در فصل چهارم، مقوله حس و پیش‌بینی حملات سایبری بر اساس مولفه‌هایی نظیر قابلیت، فرصت و نیت مبهم مورد مطالعه قرار می‌گیرد و نحوه تجسم حملات سایبری مبتنی بر ادغام اطلاعات سطح بالا و همچنین پیش‌بینی حملات سایبری بر اساس یادگیری الگوها و رفتارهای حمله با استفاده از رویکردهایی نظیر مدل مارکوف تشریح می‌شود. در ادامه مفاهیمی نظیر مبهم‌سازی و تأثیر آن بر مدل‌سازی حملات سایبری و دادگان مورد نیاز برای استفاده در آگاهی وضعیتی سایبری پیشگویانه مورد بررسی قرار می‌گیرد. در فصل پنجم، سامانه‌های تعاملی نظیر صحنه نبرد سایبری، شبیه‌ساز و مصورساز حملات سایبری و همچنین نقش و ارتباط آن‌ها در یک سامانه جامع آگاهی وضعیتی سایبری مورد مطالعه و بررسی قرار می‌گیرد.

با این توصیف کتاب حاضر، افزون بر این که بخشی از نیازهای پژوهش‌گران این شاخه علمی را برطرف می‌نماید، می‌تواند به عنوان مرجعی برای دوره‌های مختلف تحصیلی محسوب شود.

هر چند نویسندگان اهتمام زیادی در نگارش این کتاب داشته اند، با این حال از پیشنهادها و اصلاحاتی که پژوهشگران و خوانندگان کتاب ارائه نمایند استقبال کرده و در ویراستهای آینده از آن استفاده خواهد شد.

علی جبار رشیدی، کوروش داداش تبار احمدی، بهزاد نظربور

www.ketab.ir

فهرست مطالب

فصل نخست: مقدمه‌ای بر آگاهی وضعیتی سائیری ۳

۱-۱- مقدمه ۳

۲-۱- آگاهی وضعیتی ۸

۱-۲-۱- علت نیاز به آگاهی وضعیتی ۱۴

۲-۲-۱- سازوکارهای شناختی آگاهی وضعیتی ۱۷

۳-۲-۱- آگاهی وضعیتی و تصمیم‌گیری ۲۵

۴-۲-۱- مدل مرجع آگاهی وضعیتی ۲۷

۵-۲-۱- مدل فرآیندی آگاهی وضعیتی ۳۶

۳-۱- الزامات سامانه‌های آگاهی وضعیتی ۴۰

۴-۱- آگاهی وضعیتی سائیری ۴۱

۱-۴-۱- نیازمندی‌های آگاهی وضعیتی در عملیات سائیری ۴۲

۲-۴-۱- چالش‌های آگاهی وضعیتی در عملیات سائیری ۴۷

۱-۲-۴-۱- هم‌بندی پویا و پیچیده سامانه‌های سائیری ۴۷

۲-۲-۴-۱- سرعت تغییر فناوری‌ها ۴۸

۳-۲-۴-۱- نرخ پایین سیگنال به نویز ۴۸

۴-۲-۴-۱- حملات مخفی و بمب‌های ساعتی ۴۹

- ۴۹-۱-۲-۵- تهدیدات چندوجهی با تغییرپذیری سریع.....
- ۵۰-۱-۲-۶- سرعت رویدادها.....
- ۵۱-۱-۲-۷- ابزارهای غیر یکپارچه.....
- ۵۱-۱-۲-۸- وفور داده و کمبود معنا.....
- ۵۲-۱-۲-۹- خودکارسازی و کاهش آگاهی وضعیتی.....
- ۵۲-۱-۲-۱۰- خلاصه‌ای از چالش‌های آگاهی وضعیتی سایبری.....
- ۵۳-۱-۲-۱۱- عدم قطعیت در آگاهی وضعیتی سایبری.....
- ۵۴-۱-۲-۱۰- راه‌های تحقیق و توسعه برای آگاهی وضعیتی سایبری.....
- ۵۵-۱-۳-۱- تئوری بازی‌ها و تمرکز بر صحنه نبرد سایبری.....
- ۵۹-۱-۳-۲- مصورساز، شبکه‌های بزرگ مقیاس، پیچیده و پویا.....
- ۶۰-۱-۳-۳- پشتیبانی از تصمیم‌دهی آگاهی وضعیتی.....
- ۶۰-۱-۳-۴- تیم‌های هم‌افزای ماشین-انسان.....
- ۶۲-۱-۳-۵- ارزیابی و اعتبارسنجی موفقه و.....
- ۶۳-۱-۳-۶- کنترل فعال.....
- ۶۴-۱-۴-۴- آگاهی وضعیتی و زیرساخت‌های ملی.....
- ۶۸-۱-۴-۱- حملات، آسیب‌پذیری‌ها و تهدیدات سایبری سطح ملی.....
- ۷۲-۱-۴-۲- نقش آگاهی وضعیتی در حفاظت از زیرساخت‌های ملی.....
- ۷۴-۱-۵-۵- آگاهی وضعیتی فیزیکی و سایبری.....
- ۷۵-۱-۶-۶- ارزیابی کارایی و اثربخشی سامانه‌های آگاهی وضعیتی.....
- ۷۶-۱-۶-۱- معیار اعتماد در ارزیابی سامانه آگاهی وضعیتی.....

- ۱-۶-۲- معیار خلوص در ارزیابی سامانه آگاهی وضعیتی ۷۷
- ۱-۶-۳- معیار بهره‌وری هزینه در ارزیابی سامانه آگاهی وضعیتی ۷۹
- ۱-۶-۴- معیار به موقع بودن در ارزیابی سامانه آگاهی وضعیتی ۸۰
- ۷-۱- جمع‌بندی و نتیجه‌گیری ۸۰

فصل دوم: مفاهیم، مدل‌ها و کارکردهای آگاهی وضعیتی سایرین ۸۶

- ۱-۲-۱- مقدمه ۸۶
- ۲-۲- تعاریف و مفاهیم مطرح در حوزه آگاهی وضعیتی ۸۹
- ۱-۲-۲- سطوح آگاهی وضعیتی و مفاهیم آن‌ها ۹۳
- ۳-۲- آگاهی وضعیتی و ادغام اطلاعات ۹۸
- ۱-۳-۲- انواع مدل‌های ادغام اطلاعات در سامانه آگاهی وضعیتی ۹۹
- ۱-۳-۲-۱- مدل ادغام JDL ۱۰۰
- ۲-۳-۲-۱- مدل اصلاح شده ادغام آبشاری ۱۰۸
- ۳-۳-۲-۱- مدل ادغام کسب آگاهی مبتنی بر چرخه ۱۱۰
- ۳-۳-۲-۴- مدل حلقه کنترلی بویلد ۱۱۱
- ۳-۳-۲-۵- مدل ترکیبی ادغام اطلاعات ۱۱۳
- ۳-۳-۲-۶- مدل ادغام DFIG ۱۱۵
- ۳-۳-۲-۷- مدل ادغام گذار حالت (STDF) ۱۱۸
- ۳-۳-۲-۸- مدل ادغام CECA ۱۲۱
- ۳-۳-۲-۹- مدل ادغام ترکیبی JDL و CECA ۱۲۴
- ۳-۳-۲-۱۰- مدل ارزیابی وضعیتی ۱۲۶

- ۱۲۷-۲-۴- آگاهی وضعیتی سایبری مبتنی بر ادغام اطلاعات چندحسگری.....
- ۱۲۸-۲-۴-۱- آگاهی وضعیتی در امنیت شبکه.....
- ۱۲۹-۲-۴-۲- نظریه شواهد دمپستر- شافر در ادغام اطلاعات حسگری.....
- ۱۳۰-۲-۴-۳- چارچوبی برای آگاهی وضعیتی شبکه.....
- ۱۳۱-۲-۴-۱- پیش‌پردازش در آگاهی وضعیتی شبکه.....
- ۱۳۱-۲-۴-۳- ادغام داده دمپستر- شافر.....
- ۱۳۲-۲-۴-۳- ارزیابی وضعیت.....
- ۱۳۵-۲-۴-۳- تجزیه و تحلیل.....
- ۱۳۹-۲-۵- مدل‌سازی آگاهی وضعیتی سایبری مبتنی بر ادغام اطلاعات.....
- ۱۴۴-۲-۶- ارزیابی وضعیت امنیتی مبتنی بر ادغام اطلاعات.....
- ۱۴۵-۲-۶-۱- مولفه‌های وضعیت شبکه.....
- ۱۴۵-۲-۶-۱-۱- قوانین مولفه‌های وضعیت امنیت شبکه.....
- ۱۴۶-۲-۶-۱-۲- همبسته‌سازی در فرایند تجزیه و تحلیل وضعیت امنیتی.....
- ۱۴۷-۲-۶-۲- معماری همبسته‌سازی مولفه‌های وضعیت شبکه.....
- ۱۴۹-۲-۶-۳- الگوریتم ارزیابی و تجزیه و تحلیل وضعیت.....
- ۱۴۹-۲-۶-۳-۱- ایجاد فرایند حمله توسط شبکه پتری.....
- ۱۵۰-۲-۶-۴- ارزیابی وضعیت مبتنی بر تئوری دمپستر- شافر.....
- ۱۵۰-۲-۶-۴-۱- آزمایش‌ها و تجزیه و تحلیل.....
- ۱۵۲-۲-۷- آگاهی وضعیتی سایبری و حوزه‌های کاربرد.....
- ۱۵۴-۲-۷-۱- آگاهی وضعیتی سایبری برای سامانه‌های کنترل صنعتی.....

- ۲-۷-۲- آگاهی وضعیتی سایبری برای مدیریت بحران ۱۵۶
- ۳-۷-۲- ابزارها، معماری‌ها و الگوریتم‌های آگاهی وضعیتی سایبری ۱۵۶
- ۴-۷-۲- مصورسازی در آگاهی وضعیتی سایبری ۱۵۸
- ۵-۷-۲- تعامل انسان و رایانه برای آگاهی وضعیتی سایبری ۱۵۹
- ۶-۷-۲- آگاهی وضعیتی سایبری در مقیاس بزرگ ۱۵۹
- ۷-۷-۲- تبادل اطلاعات در آگاهی وضعیتی سایبری ۱۶۰
- ۱-۷-۲- آگاهی وضعیتی سایبری نظامی ۱۶۱

فصل سوم: درک و فهم حملات در آگاهی وضعیتی سایبری ۱۶۲

- ۱-۳- مقدمه ۱۶۷
- ۲-۳- درک حملات سایبری با کاربرد سامه‌های تشخیص نفوذ ۱۶۹
- ۳-۳- فهم حملات سایبری مبتنی بر همبسته‌سازی هشدارها ۱۷۱
- ۱-۳-۳- همبسته‌سازی هشدارها و تولید سناریوی حملات سایبری ۱۷۲
- ۱-۱-۳-۳- فرآیند همبسته‌سازی ۱۷۴
- ۲-۱-۳-۳- مؤلفه‌های همبسته‌سازی و نتایج تحلیل ۱۷۶
- ۳-۱-۳-۳- فراهم‌سازها در فرآیند همبسته‌سازی هشدارها ۱۷۷
- ۴-۱-۳-۳- یک نمونه از تولید سناریوی حمله ۱۷۹
- ۵-۱-۳-۳- نرمال‌سازی هشدار در فرآیند همبسته‌سازی هشدار ۱۸۱
- ۶-۱-۳-۳- پیش‌پردازش هشدار ۱۸۲
- ۷-۱-۳-۳- ادغام هشدار ۱۸۴
- ۸-۱-۳-۳- تأیید هشدار ۱۸۶

- ۱۹۱ ۳-۱-۹- بازسازی رشته حمله
- ۱۹۲ ۳-۱-۱۰- بازسازی نشست حمله
- ۱۹۵ ۳-۱-۱۱- همبسته سازی چند مرحله ای
- ۱۹۶ ۳-۱-۱۲- تحلیل اثر
- ۱۹۷ ۳-۴- نقش موتور ادغام اطلاعات در فهم بهتر حملات سایبری
- ۲۰۰ ۱-۴-۱- انواع موتورهای ادغام اطلاعات
- ۲۰۰ ۳-۴-۱-۱- موتور ادغام اطلاعات برای تصمیم گیری بی درنگ
- ۲۰۲ ۳-۴-۱-۱- موتور ادغام اطلاعات دافنی
- ۲۰۵ ۳-۴-۱-۱- موتور ادغام اطلاعات اورسا
- ۲۰۷ ۳-۴-۱-۴- موتور ادغام اطلاعات تدفی
- ۲۰۸ ۳-۴-۱-۵- مقایسه موتور ادغام اطلاعات
- ۲۱۰ ۳-۴-۲- موتور هوشمند ادغام اطلاعات
- ۲۱۲ ۳-۴-۳- موتور ادغام اطلاعات برای ردیابی حملات سایبری

فصل چهارم: پیش بینی و تجسم حملات در آگاهی وضعیتی سایبری ۲۱۹

- ۲۱۹ ۴-۱- مقدمه
- ۲۲۳ ۴-۲- مدل سازی در تجسم حملات سایبری
- ۲۲۶ ۴-۳-۱- تجسم حملات با برآورد قابلیت، فرصت و نیت مهاجم
- ۲۲۷ ۴-۳-۱- تجسم حملات سایبری مبتنی بر قابلیت
- ۲۲۹ ۴-۳-۲- تجسم حملات سایبری مبتنی بر فرصت
- ۲۳۰ ۴-۳-۳- تجسم حملات سایبری مبتنی بر نیت

۴-۴	تجسم اثرات حملات سایبری مبتنی بر ادغام اطلاعات سطح بالا.....	۲۳۳
۴-۴-۱	تجسم تهدید و ارزیابی اثر.....	۲۳۴
۴-۴-۲	مدل سازی و شبیه سازی تجسم حملات سایبری.....	۲۳۶
۴-۵	پیش بینی حملات مبتنی بر یادگیری الگوها یا رفتارهای حمله.....	۲۳۷
۴-۵-۱	رویکرد مدل مارکوف با طول متغیر در پیش بینی حملات.....	۲۳۷
۴-۵-۱	سایر رویکردها برای یادگیری الگوها یا رفتارهای حمله.....	۲۴۱
۴-۶	فناوری های کنه نی و آتی در حوزه پیش بینی حملات سایبری.....	۲۴۲
۴-۶-۱	تا مه سازی، در مدل سازی حمله.....	۲۴۳
۴-۶-۲	تولید مدل حمله مبتنی بر دارایی.....	۲۴۸
۴-۷	دادگان مورد نیاز در اسامی وضعی سایبری پیشگویانه.....	۲۵۷
۴-۸	خلاصه.....	۲۶۰

فصل پنجم: آگاهی وضعیتی سایبری و سامانه های عاملی..... ۲۶۵

۵-۱	مقدمه.....	۲۶۵
۵-۲	صحنه نبرد سایبری.....	۲۶۷
۵-۲-۱	اهداف و ویژگی های صحنه نبرد سایبری.....	۲۶۸
۵-۲-۲	مأموریت و اجزای صحنه نبرد سایبری.....	۲۷۳
۵-۲-۲-۱	میزبان ها، سرور، خوشه میزبان و زیر شبکه.....	۲۷۳
۵-۲-۲-۲	سرویس ها، سطح دسترسی ها و آسیب پذیری ها.....	۲۷۴
۵-۲-۲-۳	مسیریاب، سوئیچ، حسگر و دیواره آتش.....	۲۷۶
۵-۲-۲-۴	پیوندهای فیزیکی و بی سیم.....	۲۷۷

- ۲۷۸ ۵-۲-۲-۵ کاربران
- ۲۷۹ ۳-۲-۵ الگوریتم‌های صحنه نبرد سایبری
- ۲۷۹ ۱-۳-۲-۵ تشخیص حمله موفق
- ۲۸۱ ۲-۳-۲-۵ رایانه‌های آسیب‌پذیر مشابه
- ۲۸۲ ۴-۲-۵ مدل‌سازی صحنه نبرد سایبری
- ۲۸۳ ۱-۴-۲-۵ مدل‌سازی صحنه نبرد سایبری با گراف‌های حمله
- ۲۸۵ ۲-۴-۲-۵ مدل‌سازی صحنه نبرد سایبری با درخت آسیب‌پذیری
- ۲۸۷ ۳-۵ شبیه‌سازی حملات سایبری
- ۲۸۹ ۱-۳-۵ پرس و پرس و مدل شبیه‌سازی
- ۲۸۹ ۱-۱-۳-۵ مدل‌سازی حملات سایبری
- ۲۹۳ ۲-۳-۵ مدل‌سازی در شبیه‌سازی مبتنی بر شی گرای
- ۲۹۸ ۳-۳-۵ شبیه‌سازی حملات و تولید هشدهای حسگرهای تشخیص نفوذ
- ۳۰۰ ۴-۳-۵ نقش ادغام اطلاعات در شبیه‌سازی حملات سایبری
- ۳۰۳ ۵-۳-۵ شبیه‌سازی سناریوی حملات سایبری چند مرحله‌ای
- ۳۰۴ ۶-۳-۵ شبیه‌سازی و صحنه نبرد سایبری
- ۳۰۶ ۷-۳-۵ استخراج سلسله مراتب آسیب‌پذیری برای شبیه‌سازی
- ۳۰۹ ۸-۳-۵ شبیه‌سازی مبتنی بر مدل رفتاری حمله
- ۳۱۳ ۹-۳-۵ الگوی راهنمای تولید سناریوی حمله
- ۳۱۶ ۱۰-۳-۵ پیکربندی شبکه هدف نمونه در شبیه‌سازی حملات سایبری
- ۳۱۹ ۱۱-۳-۵ نمونه شبیه‌ساز حملات سایبری

- ۳۲۲ ۵-۴- مصورسازی حملات سایبری مبتنی بر ادغام اطلاعات
- ۳۲۶ ۵-۴-۱- کاهش تعداد هشدارهای خام مبتنی بر ادغام داده
- ۳۲۶ ۵-۴-۱- نمایش آگاهی وضعیت سایبری
- ۳۲۹ ۵-۴-۲- معماری پیشنهادی برای مصورسازی در آگاهی وضعیتی سایبری
- ۳۳۰ ۵-۴-۲-۱- مدل مرجع آگاهی وضعیتی در سنجش وضعیتی و ارزیابی اثر
- ۳۳۷ ۵-۵- جمع بندی

۳۳۸ مراجع

- ۳۵۲ اصطلاحات مفهومی
- ۳۵۶ واژه‌نامه انگلیسی به فارسی
- ۳۶۴ واژه‌نامه فارسی به انگلیسی