

تشخیص نفوذ در شبکه با استفاده از یادگیری عمیق

نویسندگان:

Kwangjo Kim
Muhamad Erza Aminanto
Harry Chandra Tanuwidjaja

ترجمه:

مهندس حسین کاردان مقدم
عضو هیأت علمی دانشگاه صنعتی بیرجند

دکتر مجتبی تاجری



ناشر چهار درخت

تشخیص نفوذ در شبکه با استفاده از یادگیری عمیق

سرشناسه: کیم، کوانگجو Kim, Kwangjo
عنوان و نام پدیدآور: تشخیص نفوذ در شبکه با استفاده از یادگیری عمیق نویسندگان [کوانگجو کیم، محمدارضا آمیناتو، هری چان تانوویدجاجا]؛ ترجمه حسین کاردان مقدم، مجتبی تاجری.

مشخصات نشر: بیرجند: نشر چهار درخت، ۱۳۹۹.

مشخصات ظاهری: ۱۲۹ ص.

شابک: ۹۷۸-۶۲۲-۷۰۲۳-۲۴-۴

وضعیت فهرست نویسی: فیبا

یادداشت: عنوان اصلی: Network intrusion detection using deep learning : a feature learning approach, 2018.

موضوع: ماندهای تشخیص نفوذ (ایمن سازی کامپیوتر)

موضوع: Intrusion detection systems (Computer secur.)

موضوع: شبکه های کامپیوتری — تدابیر ایمنی

موضوع: Computer networks — Security measur.

موضوع: فراگیری ماشین

موضوع: Machine learning

موضوع: شبکه های مصنوعی

موضوع: Neural network Computer science

شناسه افزوده: آمیناتو، محمد ارضا

Aminanto, Muhammad Erza

شناسه افزوده: تانوویدجاجا، هری چان

Tanuwidjaja, Harry Chan

شناسه افزوده: کاردان مقدم، حسین، ۱۳۶۱

شناسه افزوده: تاجری، مجتبی، ۱۳۵۹ — مترجم

رده بندی کنگره: TK ۵۹/۵۱۰۵

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۶۱۶۹۰۵۷

حقوق این اثر متعلق به مؤلفان است

ترجمه: مهندس حسین کاردان مقدم، دکتر مجتبی تاجری

نویسندگان: Kwangjo Kim, Harry Chan, Tanuwidjaja, Muhamad Erza Aminanto

ناشر: نشر چهار درخت

چاپ اول: ۱۳۹۹

شمارگان: ۵۰۰ نسخه

محل نشر: بیرجند

چاپ و صحافی: مهرنگ

شابک: ۹۷۸-۶۲۲-۷۰۲۳-۲۴-۴

قیمت: ۴۰۰,۰۰۰ ریال

بیرجند، خیابان معلم، قدس شرقی، جنب اداره راه و شهرسازی، ساختمان باران

تلفن: ۰۵۶ - ۳۲۴۵۶۲۱۳ همراه: ۰۹۱۵ ۵۶۱۷۱۵۵

4derakht@gmail.com



نشر چهار درخت

فهرست مطالب

فصل اول: مقدمه.....	۹
چکیده.....	۹
فصل دوم: سیستم‌ها، تشخیص نفوذ.....	۱۷
چکیده.....	۱۷
تعریف.....	۱۷
طبقه بندی.....	۱۸
معیار.....	۲۲
متریک عملکرد (Performance Metric).....	۲۲
مجموعه داده عمومی.....	۲۴
فصل سوم: یادگیری ماشین کلاسیک و کاربردهای آن در امنیت.....	۲۹
چکیده.....	۲۹
طبقه بندی یادگیری ماشین.....	۲۹
یادگیری نظارت شده.....	۲۹
دستگاه بردار پشتیبان.....	۳۰
درخت تصمیم گیری.....	۳۱
یادگیری نظارت نشده.....	۳۱
خوشه بندی کی مینز (K-Means Clustering).....	۳۲
دسته بندی مورچه.....	۳۲
کدگذار خودکار (پراکنده).....	۳۳

۳۷.....	یادگیری نیمه نظارتی (Semi-supervised Learning)
۳۸.....	۱- فرض یکنواختی نیمه نظارتی
۳۸.....	۲- فرض خوشه
۳۸.....	۳- فرض چندگانه
۳۹.....	یادگیری با نظارت ضعیف
۳۹.....	یادگیری تقویتی (Reinforcement Learning)
۴۰.....	یادگیری ماشین تخصصی
۴۱.....	سیستم‌های تشخیص مزاحم مبتنی بر یادگیری ماشین
۵۱.....	فصل چهارم: یادگیری عمیق
۵۱.....	مولد (یادگیری نظارت نشده)
۵۲.....	کدگذار خودکار بسته ای (پراکنده)
۵۴.....	دستگاه بولتزمن
۵۵.....	شبکه‌های حاصل جمع
۵۵.....	شبکه‌های عصبی بازگشتی
۵۷.....	متمایز (Discriminative)
۵۸.....	ترکیبی
۵۸.....	شبکه‌های مولد تخصصی (Generative Adversarial Networks (GAN))
۶۳.....	فصل پنجم: سیستم‌های تشخیص نفوذ مبتنی بر یادگیری عمیق
۶۳.....	چکیده
۶۴.....	تولیدی
۶۴.....	شبکه عصبی عمیق
۶۵.....	شبکه عصبی عمیق پرشتاب
۶۶.....	یادگیری خودآموز
۶۷.....	کدگذار خودکار کاهش نویز دسته ای (Stacked Denoising Auto-Encoder)

۶۹.....	شبکه عصبی تکرارشونده با حافظه بلند و کوتاه مدت
۶۹.....	متمایز
۷۰.....	شبکه عصبی عمیق در شبکه‌های نرم افزار تعریف شده
۷۱.....	شبکه عصبی بازگشتی (Recurrent Neural Network)
۷۲.....	شبکه عصبی پیچیده
۷۳.....	شبکه عصبی بازگشتی حافظه طولانی کوتاه مدت
۷۳.....	شبکه عصبی بازگشتی حافظه طولانی کوتاه مدت استادمیر (LSTM-RNN Staudemeyer)
۷۴.....	شبکه عصبی بازگشتی حافظه طولانی کوتاه مدت برای تشخیص بی نظمی گروهی (LSTM-RNN for Collectively Anomaly Detection)
۷۴.....	جی آر یو آی اینترنت اشیا (GRU in IoT)
LSTM.....	شبکه عصبی بازگشتی حافظه طولانی کوتاه مدت برای انسداد سرویس توزیع شده (LSTM-DoS)
۷۵.....	ترکیبی (RNN for DDoS)
۷۵.....	شبکه‌های تخصصی
۷۶.....	یادگیری تقویتی عمیق (Deep Reinforcement Learning)
۷۷.....	مقایسه
۸۱.....	فصل ششم: یادگیری ویژگی عمیق
۸۱.....	چکیده
۸۲.....	انتخاب و استخراج ویژگی عمیق
۸۲.....	روش شناسی
۸۸.....	ارزیابی
۸۸.....	پیش پردازش مجموعه داده ها
۹۰.....	نتیجه آزمایش
۹۹.....	یادگیری عمیق برای دسته بندی
۱۰۲.....	روش شناسی

ارزیابی.....	۱۰۴
مقایسه.....	۱۰۷
فصل هفتم: خلاصه و چالش‌های بیشتر.....	۱۱۳
چکیده.....	۱۱۳
ضمیمه الف.....	۱۱۷
بررسی تشخیص بدافزار بر مبنای یادگیری عمیق.....	۱۱۷
الف-۱ تحلیل خودکار رفتار بدافزار با استفاده از یادگیری ماشین.....	۱۱۷
الف-۲ یادگیری عمیق برای طبقه‌بندی زنجیره‌های درخواست سیستم بدافزار.....	۱۱۸
الف-۳ تشخیص بدافزار با شبکه عصبی عمیق با استفاده از رفتار پردازش.....	۱۱۹
الف-۴ تحلیل بدافزار با یک درآمد بر اساس رفتار شبکه با استفاده از یادگیری عمیق.....	۱۲۰
الف-۵ طبقه‌بندی خودکار بدافزار تشخیص بدافزار جدید با استفاده از یادگیری ماشین.....	۱۲۱
الف-۶ دیپ ساین (DeepSign): یادگیری عمیق برای طبقه‌بندی و تولید خودکار امضا بدافزار (Deep Learning for Automatic Malware Signature Generation and Classification).....	۱۲۲
الف-۷ انتخاب ویژگی‌ها برای طبقه‌بندی بدافزار.....	۱۲۴
الف-۸ تحلیل تکنیک‌های یادگیری ماشین به کار رفتاری سیستم تشخیص بدافزار رفتار محور.....	۱۲۵
الف-۹ تشخیص بدافزار با استفاده از تحلیل مبتنی بر یادگیری ماشین در ازای الگوهای دسترسی حافظه مجازی.....	۱۲۶
الف-۱۰ تشخیص بدافزار زیرو-دی (Zero-Day).....	۱۲۷