

تهدیدات حریم خصوصی کاربران در شبکه‌های گمنامی

www.ketab.ir

تالیف:

سعید شیروی

سرشناسه: شیروی، سعید، ۱۳۷۱-

عنوان و نام پدیدآور: تهدیدات حریم خصوصی کاربران در شبکه‌های گمنامی/تالیف سعید شیروی.- مشخصات نشر: تهران: انتشارات ماهواره، ۱۳۹۸.- مشخصات ظاهری: ۱۰۸ص.
شابک: ۶۷۷-۰-۴۵۹-۶۰۰-۹۷۸-۹ وضعیت فهرست نویسی: فیا- یادداشت: کتابنامه. موضوع:
شبکه‌های کامپیوتری -- تدابیر ایمنی-موضوع: Computer networks -- Security
measures-موضوع: فضای مجازی -- تدابیر ایمنی-موضوع: Cyberspace -- Security
measures-موضوع: شبکه‌های عصبی (کامپیوتر)-موضوع: Neural networks (Computer
science)-موضوع: فراگیری ماشینی-موضوع: Machine learning- رده بندی کنگره:
TK۵۹/۵۱۰۵- رده بندی دیویی: ۸۲/۰۰۵-شماره کتابشناسی ملی: ۵۹۲۲۵۲۳

تهدیدات حریم خصوصی کاربران در شبکه‌های گمنامی

تالیف: سعید شیروی

ناشر مجوز: تهران، ماهواره

نویسنده چاپ: اول، ۱۳۹۸

تیراژ: ۵۰۰ نسخه

شابک: ۶۷۷-۰-۴۵۹-۶۰۰-۹۷۸

قیمت: ۲۲۰۰۰ تومان

صفحه آرا: امیر حسین اسمعیل خانیان- روژین بشیری

آماده سازی و چاپ: موسسه پژوهشگران امیر کبیر

آدرس موسسه: خیابان آزادی-روبروی ایستگاه BRT دکتر قریب-خیابان بهزاد-روبروی

پارکینگ کاوه-نبش کوچه فرازبان-پلاک ۲۷-طبقه اول واحد ۲-۶۶۵۶۳۱۳

مسئولیت صحت مطالب و پاسخگویی به شکایت‌های حقوق مادی و معنوی کتاب بر عهده مولف است.

کلیه حقوق محفوظ است.

ماده ۲۳ قانون حمایت از مولفان و مصنفان - هرکس تمام یا قسمتی از اثر دیگری را که مورد حمایت

این قانون است به نام خود یا به نام پدید آورنده بدون اجازه او و یا عالماً عامداً به شخص دیگری غیر از

پدید آورنده نشر یا پخش یا عرضه کند به حبس تادیبی از شش ماه تا سه سال محکوم خواهد شد.

فهرست مطالب

صفحه	عنوان
۱	فصل ۱: کلیات
۷	فصل ۲: شبکه‌های گمنامی
۸	۲- مقدمه
۹	۲-۱- سازوکارهای چندجست
۱۲	۲-۱-۱- ضعف شبکه‌های ترکیبی
۱۳	۲-۲- مسیر یاب پیازی تُر
۱۳	۲-۲-۱- معماری شبکه تُر
۱۶	۲-۱-۲- ساخت مدار
۱۷	۲-۳- ابزارهای اتصال به شبکه تُر
۱۷	۲-۳-۱- مرورگر تُر
۱۸	۲-۳-۱-۱- افزونه NoScript
۱۹	۲-۳-۱-۲- افزونه HTTPS Everywher
۱۹	۲-۳-۱-۳- افزونه Tor Button
۲۰	۲-۳-۲- برنامه کاربردی Orbot
۲۰	۲-۳-۳- سیستم عامل Tails
۲۱	۲-۴- حملات تحلیل ترافیک
۲۳	۲-۵- معیارهای ارزیابی
۲۴	۲-۵-۱- معیارهای ارزیابی حملات انگشت‌نگاری وب‌سایت

۲۶	۲-۵-۲ معیارهای ارزیابی روش دفاعی انگشت نگاری وبسایت
۲۸	۲-۶ جمع بندی
۲۹	فصل ۳: یادگیری ماشین
۳۰	۳- مقدمه
۳۰	۳-۱- یادگیری ماشین سنتی
۳۲	۳-۱-۱ نمونه هایی از یادگیری ماشین سنتی
۳۳	۳-۲ شبکه عصبی عمیق
۳۴	۳-۲-۱ آموزش شبکه عصبی عمیق
۳۵	۳-۲-۲ تابع فعال ساز
۳۶	۳-۲-۲-۱ تابع هزینه
۳۶	۳-۲-۲-۲ گرادیان کاهشی
۳۷	۳-۲-۲-۳ انتشار به عقب
۳۷	۳-۲-۳ شبکه عصبی خود کد گذار
۳۹	۳-۲-۴ شبکه عصبی پیچشی
۴۰	۳-۲-۵ شبکه عصبی باز گشتی
۴۲	۳-۳ جمع بندی
۴۳	فصل ۴: مروری بر حملات انگشت نگاری وبسایت
۴۴	۴- مقدمه
۴۵	۴-۱ حملات انگشت نگاری وبسایت روی سازوکارهای تک جست
۴۷	۴-۲ حملات انگشت نگاری چند جست
۴۷	۴-۲-۱ حمله هرمن
۴۸	۴-۲-۲ حمله پانچنکو با استفاده از ماشین بردار پشتیبان

۴۸	۴-۲-۳- حمله وانگ
۴۹	۴-۲-۴- حمله پانچنکو با استفاده از ویژگی تجمعی
۴۹	۴-۳- حملات انگشت نگاری وبسایت با استفاده از یادگیری عمیق
۵۰	۴-۳-۱- حمله ایب و گوتو
۵۱	۴-۳-۲- حمله ریمر
۵۱	۴-۳-۳- حمله سرینم
۵۲	۴-۴- چالش های حملات انگشت نگاری وبسایت
۵۳	۴-۴-۱- توانایی مهاجم
۵۴	۴-۴-۲- شرایط کاربر
۵۴	۴-۴-۳- وبسایت
۵۶	۴-۵- جمع بندی
۵۷	فصل ۵: مروری بر روش های مقابله با حملات انگشت نگاری وبسایت
۵۸	۵- مقدمه
۵۸	۵-۱- مبهم سازی در لایه کاربرد
۵۸	۵-۱-۱- روش مقابله HTIPOS
۶۰	۵-۱-۲- روش مقابله لوله کشی تصادفی HTTP
۶۰	۵-۱-۳- روش مقابله آلبا-کا-لما
۶۲	۵-۲- لایه گذاری
۶۲	۵-۲-۱- لایه گذاری بسته ها
۶۳	۵-۲-۲- لایه گذاری با نرخ ثابت
۶۳	۵-۲-۲-۱- روش مقابله بوفالو
۶۵	۵-۲-۲-۲- روش مقابله تامارا