امنیت اینترنت اشیاء

شانکانگ لی | لی دا شو

مهندس فاطمه حسینی صفا

۱۳۹۸

سرشناسه: لی، شانکانگ Li, Shancang
عنوان و نام پدیدآور: امنیت اینترنت اشیاء/ شانکانگ لی، لی‌دا شو؛ [مترجم] فاطمه حسینی‌صفا.
مشخصات نشر: قم: آتریسا، ۱۳۹۸.
مشخصات ظاهری: ۱۴۷ ص.: مصور، جدول، نمودار.
شابک: ۳۸۰۰۰۰ ریال: ۲-۱۵-۸۷۵۴-۶۰۰-۹۷۸
وضعیت فهرست نویسی: فیپا
یادداشت: عنوان اصلی: .Securing the internet of things.[2017]
یادداشت: چاپ قبلی: آتی‌نگر، ۱۳۹۷.
یادداشت: کتابنامه: ص.[۱۳۹] - ۱۴۷.
موضوع: اینترنت اشیاء
موضوع: Internet of things
موضوع: کامپیوترها -- ایمنی اطلاعات
موضوع: Computer security
شناسه افزوده: شو، لی دی.، ۱۹۴۵ - م.
شناسه افزوده: Xu, Li D .
شناسه افزوده: حسینی صفا، فاطمه، ۱۳۵۸-، مترجم
رده بندی کنگره: ۸۸۵۷/TK۵۱۰۵
رده بندی دیویی: ۶۷۸/۰۰۴
شماره کتابشناسی ملی: ۵۸۸۳۲۲۰

نام کتاب: امنیت اینترنت اشیاء

نام مؤلف: **فاطمه حسینی صفا**
سال چاپ: پاییز ۱۳۹۸
ناشر: **انتشارات آتریسا**
نوبت چاپ: اول
چاپ: ولیعصر/ صحافی: معمایی
تیراژ: ۲۰۰ نسخه
قیمت: ۳۸۰۰۰ تومان
شابک: ۹۷۸-۶۰۰-۸۷۵۴-۱۵-۲
مرکز پخش: قم انتشارات آتریسا ۰۹۱۲۶۶۵۹۲۴۶

فهرست مطالب

عنوان ..... صفحه

مقدمه مترجم ۷
درباره نویسندگان ۹
۱-۱ مقدمه ۱۱
۱-۱-۱ مرور کلی ۱۱
۱-۱-۲ پیشینه پژوهش ۱۲
۱-۱-۳ الزامات امنیت ۱۴
۱-۲ الزامات امنیت در معماری IoT ۱۵
۱-۲-۱ لایه حسگر و گره‌های انتهایی IoT ۱۷
۱-۲-۲ لایه شبکه ۱۹
۱-۲-۳ لایه سرویس ۲۱
۱-۲-۴ لایه کاربرد-واسط (Application-Interface Layer) ۲۳
۱-۲-۵ تهدیدهای بین لایه‌ها (Cross-Layer Threats) ۲۵
۱-۲-۶ تهدیدهای ناشی از نگهداری IoT ۲۵
۱-۳ امنیت در فناوری‌های فعالساز (Security In Enabling Technologies) ۲۶
۱-۳-۱ امنیت در فناوری‌های تشخیص هویت و ردیابی ۲۶
۱-۳-۲ امنیت در ترکیب شبکه حسگر بی‌سیم و RFID ۲۷
۱-۳-۳ امنیت در ارتباطات ۲۷
۱-۳-۴ امنیت در شبکه‌ها ۲۹
۱-۳-۵ امنیت در مدیریت سرویس ۲۹
۱-۴ نگرانی‌های امنیت در کاربردهای IoT ۳۰
۱-۴-۱ نگرانی‌های امنیت در سیستم‌های SCADA ۳۰
۱-۴-۲ نگرانی‌های امنیت در سیستم‌های اطلاعات سازمانی ۳۱
۱-۴-۳ نگرانی‌های امنیت در IoT اجتماعی ۳۲
۱-۴-۴ محرمانگی و امنیت در مراقبت بهداشتی مبتنی بر IoT ۳۳
۱-۵ خلاصه ۳۴
۲-۱ مقدمه ۳۵
۲-۲ الزامات امنیت در IoT ۳۶
۲-۲-۱ چالش‌های امنیت داده در IoT ۳۷
۲-۲-۱-۱ محرمانگی داده ۳۸

۲-۲-۱-۲ حریم خصوصی..... ۳۸
۲-۲-۱-۳ اعتماد..... ۳۹
۲-۲-۲ امنیت در لایه حسگر..... ۳۹
۲-۲-۳ امنیت در لایه شبکه..... ۴۰
۲-۲-۴ امنیت در لایه سرویس..... ۴۱
۲-۲-۵ امنیت در لایه واسط..... ۴۱
۲-۲-۶ چالش‌های ایمن سازی IoT..... ۴۲
۲-۳ احراز هویت و صدور مجوز ناکارآمد..... ۴۳
۲-۳-۱ احراز هویت در IoT..... ۴۳
۲-۳-۲ صدور مجوز (Authorization)..... ۴۳
۲-۳-۳ احراز هویت و صدور مجوز ناکارآمد..... ۴۴
۲-۳-۳-۱ افراد..... ۴۵
۲-۳-۳-۲ حوزه تجارت..... ۴۵
۲-۳-۳-۳ توانایی دسترسی به IoT..... ۴۵
۲-۳-۴ احراز هویت ناکارآمد دستگاه در IoT..... ۴۶
۲-۴ کنترل دسترسی ناامن..... ۴۶
۲-۴-۱ سیستم‌های کنترل دسترسی مبتنی بر نقش..... ۴۷
۲-۴-۲ سیستم‌های کنترل دسترسی مبتنی بر لیست..... ۴۷
۲-۴-۳ دسترسی مبتنی بر توانایی (Capability-Based Access)..... ۴۸
۲-۴-۴ چالش‌های کنترل دسترسی..... ۴۹
۲-۵ تهدیدهای کنترل دسترسی، حریم خصوصی و دسترس پذیری..... ۵۰
۲-۵-۱ تهدیدهای لایه شبکه..... ۵۲
۲-۵-۲ تهدیدهای لایه سرویس..... ۵۳
۲-۵-۳ تهدیدهای بین لایه‌ها و نگهداری IoT..... ۵۴
۲-۶ حملات مختص IoT..... ۵۶
۲-۶-۱ دسترسی فیزیکی..... ۵۶
۲-۶-۲ حملات محلی روی WiFi..... ۵۷
۳-۱ محرمانگی و ظرفیت کلید مخفی..... ۵۹
۳-۲ احراز هویت/ صدور مجوز برای دستگاه‌های هوشمند..... ۶۲
۳-۳ رمزگذاری انتقال..... ۶۶
۳-۳-۱ امنیت لایه انتقال..... ۶۷
۳-۳-۲ لایه سوکت‌های امن (Secure Sockets Layer)..... ۶۸

۳-۳-۳ HTTPS ۶۸
۳-۳-۴ امنیت انتقال در IoT ۶۹
۳-۴ واسط امن ابر/وب ۷۰
۳-۵ نرم افزار/میان افزار امن ۷۱
۳-۶ امنیت لایه فیزیکی ۷۳
۳-۷ خلاصه ۷۶
۴-۱ اهداف امنیت در IoT ۷۸
۴-۲ احراز هویت بر مبنای کلید عمومی ۷۹
۴-۲-۱ رمزنگاری متقارن ۸۱
۴-۲-۱-۱ AES-CCM ۸۳
۴-۲-۲ رمزنگاری کلید عمومی ۸۴
۴-۲-۳ زیرساخت کلید عمومی ۸۵
۴-۳ اعتبارسنجی مبتنی بر هویت، رمزنگاری و امضای دیجیتالی ۸۷
۴-۳-۱ اعتبارسنجی مبتنی بر هویت ۸۷
۴-۳-۲ امضای دیجیتالی ۸۹
۴-۳-۳ کلید عمومی خام (Raw Public Key) ۹۱
۴-۳-۴ گواهینامه‌های X.509 ..... ۹۲
۴-۴ اتصال IP ۹۴
۴-۴-۱ امنیت لایه انتقال دیتاگرام (Datagram Transport Layer Security) ۹۵
۴-۴-۲ پروتکل کاربرد محدود (Constrained Application Protocol) ۹۷
۴-۵ رمزنگاری سبک (Lightweight Cryptography) ۹۷
۴-۵-۱ کارآمدی ارتباطات انتها به انتها ۹۸
۴-۵-۲ قابلیت بکارگیری روی دستگاه‌هایی با منابع کمتر ۹۸
۴-۶ راهکارهای فعلی امنیت IoT ۱۰۰
۴-۷ خلاصه ۱۰۱
۵-۱ مقدمه ۱۰۳
۵-۱-۱ چالش‌های امنیت در محیط IoT ۱۰۵
۵-۱-۲ لایه حسگر و گره‌های انتهایی IoT ۱۰۶
۵-۲ لایه شبکه ۱۰۸
۵-۳ لایه سرویس ۱۱۰
۵-۴ لایه کاربرد-واسط (Application-Interface Layer) ۱۱۲
۵-۵ تهدیدهای بین لایه‌ها (Cross-Layer Threat) ۱۱۴

۶-۵ تهدیدهای ناشی از نگهداری IoT ۱۱۵
۶-۱ امنیت در فناوری‌های تشخیص هویت و ردیابی ۱۱۶
۶-۱-۱ تشخیص هویت ۱۱۷
۶-۱-۱-۱ ردیابی ۱۱۷
۶-۲ امنیت در ترکیب شبکه حسگر بی‌سیم و RFID ۱۱۸
۶-۳ امنیت در ارتباطات ۱۲۱
۶-۴ پروتکل‌های امنیت و مسائل حریم خصوصی در پشته 6LOWPAN ۱۲۳
۶-۵ امنیت در مدیریت سرویس ۱۲۳
۷-۱ امنیت داده و حریم خصوصی ۱۲۴
۷-۲ محرمانگی داده و مدیریت کلید ۱۲۵
۷-۳ مرور ادبیات ۱۲۹
مراجع ۱۴۰

مقدمه مترجم

عبارت اینترنت اشیاء (IoT) برای نخستین بار در سال ۱۹۹۹ توسط کِوین اَشتون مورد استفاده قرار گرفت و بواسطه آن جهانی را توصیف کرد که در آن هر چیزی از جمله اشیای بی‌جان برای خود هویت دیجیتال داشته باشند و امکان سازماندهی و مدیریت اشیاء توسط کامپیوترها فراهم باشد. اینترنت در حال حاضر همه مردم را به هم متصل می‌کند ولی با اینترنت اشیاء تمام اشیاء به هم متصل می‌شوند. امروزه تقریباً اکثر اشیاء مجهز به حسگر هستند و توسط کنترلر کنترل می‌شوند. اینترنت اشیاء با توانایی جاساز کردن پردازنده، حافظه و منابع انرژی درون اشیاء تقریباً همه چیز را با استفاده از برنامه‌ها به شبکه متصل می‌کند. با تعبیه کردن هوشمندی در اشیاء مورد استفاده روزانه، آن ها به اشیاء هوشمندی تبدیل می‌شوند که می‌توانند از هر جای جهان کنترل شوند. این دستگاه‌ها می‌توانند با مبادله داده در میان خود با یکدیگر یکپارچه شوند. اتصال چنین دستگاه‌هایی به تلفن‌های مبایل یا کامپیوترها از طریق اینترنت می‌تواند حوزه‌های پژوهشی بسیاری را فراهم نماید.

اینترنت اشیاء می‌توانند در حوزه‌های بسیاری از جمله صنعت رسانه، نظارت بر محیط زیست، مدیریت زیرساخت‌ها، ساخت و تولید، مدیریت انرژی، اتوماسیون خانگی، حمل و نقل، پزشکی و مراقبت بهداشتی و غیره مورد استفاده قرار گیرد. هر یک از کاربردها دارای الزامات امنیتی مخصوص به خود هستند. گستردگی کاربردهای اینترنت اشیاء و حساسیت‌های متفاوت هر کاربرد، ناهمگونی تجهیزات مورد استفاده و به تبع آن تعارض استانداردهای ساخت تجهیزات، دسترس پذیری دستگاه‌ها و آسیب‌پذیری‌های مختلفی که برای هر یک از لایه‌های معماری اینترنت اشیاء وجود دارد، موضوعات پژوهشی بسیاری را در زمینه ایمن سازی اینترنت اشیاء ایجاد کرده است. البته الزامات امنیتی اینترنت اشیاء و آسیب‌پذیری‌های آن هنوز هم به طور کامل شناسایی نشده‌اند. در هر حال راهکارهای ارائه شده در زمینه اینترنت اشیاء باید امنیت را در تمام سطوح معماری IoT لحاظ نمایند.

کتاب مرجع که در سال ۲۰۱۷ به چاپ رسیده است به مسئله ایمن سازی اینترنت اشیاء می‌پردازد و تهدیدها و آسیب‌پذیری‌های امنیت را در لایه‌های مختلف معماری IoT تحلیل و بررسی می‌نماید. همچنین راهکارهای ارائه شده در زمینه امنیت IoT را تا سال ۲۰۱۷ ارائه می‌نماید.

هدف از ترجمه این کتاب، ارائه یک منبع فارسی مناسب برای دانش پژوهان در زمینه امنیت IoT است. در ترجمه این اثر اهتمام بسیاری بر بیان شیوای مطالب و حفظ امانت شده است که امیدوارم مورد تأیید پژوهشگران و اساتید حوزه امنیت واقع شود و نیازی به مراجعه به متن اصلی مشاهده نشود.

پیشاپیش از محضر اساتید و دانش پژوهان محترم بابت خطاهای احتمالی در ترجمه مفاهیم کتاب پوزش می‌طلبم و امید دارم که با انتقادات و راهنمایی‌های شما بزرگواران بتوانم به تصحیح اشکالات و نکات مبهم موجود بپردازم.

فاطمه حسینی صفا
شهریور ۱۳۹۸
fhoseinisafa@gmail.com

درباره نویسندگان

شانکانگ لی مدرس ارشد گروه علوم کامپیوتر و فناوری‌های خلاقانه در دانشگاه West of England است. شانکانگ قبلا به عنوان مدرس در دانشگاه Edinburg Napier و به عنوان پژوهشگر امنیت در گروه رمزنگاری دانشگاه بریستول فعالیت می‌کرد، بطوریکه مباحثات مبایل/دیجیتال را در طیف وسیعی از صنایع و فناوری‌ها رهبری نموده است. سابقه فعالیت ایشان در زمینه امنیت شامل تست نفوذ در شبکه، امنیت بی‌سیم، امنیت مبایل و پزشکی قانونی دیجیتال است.

لی دا شو یک عضو IEEE و عضو آکادمی مهندسی روسیه است. وی استاد برجسته دپارتمان «فناوری اطلاعات و علوم تصمیم گیری» در دانشگاه Old Dominion واقع در ایالات متحده است. ایشان در سال ۲۰۱۶ توسط تامسون رویترز به عنوان پژوهشگر برتر معرفی شد. بر اساس گزارش تامسون رویترز پژوهشگران برتر سال ۲۰۱۶ برخی از تاثیرگذارترین ایده‌های علمی را ارائه کرده‌اند.

ایشان رئیس موسس کمیته فنی انجمن IEEE SMC در سیستم‌های اطلاعات سازمانی و سردبیر موسس مجلات مطرحی همچون «یکپارچگی اطلاعات سازمانی»، «یکپارچگی و مدیریت صنعتی»، «سیستم‌های اطلاعات سازمانی» و مدیر مسئول «مرزهای مدیریت مهندسی» و مجله «تحلیل‌های مدیریت» است.

علاوه بر این موفقیت‌های قابل توجه، ایشان برنده جایزه Chnagjian Chair Professor در وزارت آموزش و پرورش چین است. دکتر شو وابسته به موسسه تکنولوژی محاسبات، آکادمی علوم چین، دانشگاه علوم و فناوری چین، دانشگاه Shanghai Jiao Tong، مرکز تحقیق و توسعه شورای ایالتی چین و دانشگاه Old Dominion است.

وی در فعالیت‌های اولیه آکادمیک علمی و آموزشی در زمینه مهندسی سیستم شرکت داشته است. پروفسور شو همکاری گسترده‌ای با دانشمندان پیشگام نظیر West Churchman West ، John Warfield و Qian Xuesen داشته است. بعلاوه ایشان از پیشگامان فعالیت‌های تحقیقاتی و آموزشی در زمینه سیستم‌های اطلاعاتی و سیستم‌های سازمانی بود که در سال ۱۹۸۰ آغاز شد.

بسیاری او را به عنوان یکی از بنیانگذاران رشته نوظهور «مهندسی یکپارچه‌سازی اطلاعات صنعتی» می‌شناسند. ایشان نویسنده کتاب «یکپارچه‌سازی سازمانی و معماری اطلاعات» است و نویسنده همیار کتاب «رویکردهای روش شناختی علوم سیستم» است که توسط گروه Taylor & Fracis منتشر شد. بسیاری از دانشمندان مشهور از جمله Qian Xuesen در تحقیقات اصلی خود به کار وی اشاره داشته‌اند.