امنیت سایبری:

تجزیه وتحلیل‌ها، فناوری و اتوماسیون

(جلد اول)

نویسندگان:
Martti Lehto • Pekka Neittaanmäki

۲۰۱۵

مترجم:
مهندس علیرضا زحلی

عنوان و نام پدیدآور : امنیت سایبری: تجزیه و تحلیل‌ها، فناوری و اتوماسیون/ویراستاران[مارتی لهتو ، پکا نیتانماکی]
مترجم علیرضا زحلی.
مشخصات نشر : تهران: بوستان حمید، ۱۳۹۴.
مشخصات ظاهری : ۲۲۴ ص.
شابک : ۹۷۸-۶۰۰-۶۴۱۲-۴۹-۸
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی Cyber Security: Analytics Technology and Automation 2015
موضوع : فضای مجازی-- تدابیر ایمنی
موضوع : شبکه‌های کامپیوتری-- تدابیر ایمنی
شناسه افزوده : لهتو، مارتی، ویراستار
شناسه افزوده : Lehto, Martti
شناسه افزوده : نیتانماکی، پکا، ۱۹۵۱ - م.، ویراستار
شناسه افزوده : Neittaanmäki, P (Pek...)
شناسه افزوده : زحلی، علیرضا، ۱۳۵۹-، مترجم
رده بندی کنگره : HM۸۵۱/...
رده بندی دیویی : ۳۰۳...۸۳۱
شماره کتابشناسی ملی : ...۳۸۲۱

انتشارات بوستان حمید

عنوان: امنیت سایبری: تجزیه وتحلیل‌ها، فناوری و اتوماسیون
ویراستاران متن اصلی: مارتی لهتو- پکا نیتانماکی
مترجم: مهندس علیرضا زحلی
ویراستار ادبی: محمد صادق اسکندری
ناشر: بوستان حمید
چاپ: اول- بهار ۱۳۹۵
شمارگان: ۱۰۰۰
قیمت: ۱۵۰۰۰ تومان

تلفن ناشر و پخش کتاب: ۳۳۷۰۰۹۲۷ ۰۹۱۲۳۳۷۵۰۳۹ ۰۹۱۲۷۷۵۷۸۳۸
پست الکترونیکی ناشر: boostanhamid.publication@gmail.com

پیش گفتار

فضای سایبر جهانی متشکل از شبکه‌های اطلاعاتی پیچیده و چندلایه‌ای است که شبکه‌های ارتباطی بخش دولتی، جامعه‌ی کسب وکار، مقامات امنیتی و سیستم‌های نظارتی و کنترل را که در زیرساخت های حیاتی[1] و صنعت کاربرد داشته و در اینترنت، یک شبکه‌ی جهانی را خلق می‌کنند، را دربر می‌گیرند.

پردازش و بهره برداری از داده‌های تخیلی، که نشأت گرفته از نیاز شهروندان و جامعه‌ی کسب‌و کار است از مهم‌ترین عناصر یک جامعه‌ی رو به پیشرفت می‌باشند. اطلاعات و دانش[2] به کالاهای کلیدی در جامعه تبدیل شده و با کمک فناوری اطلاعات از آنها می توان بطور مؤثرتری بهره گرفت. سرویس‌های الکترونیکی تعاملی مختلف، صرفنظر از زمان و مکان، در حال در دسترس هستند. در حالیکه بخش دولتی، اقتصاد، جامعه‌ی کسب وکار و شهروندان از سرویس‌های شبکه‌ی جهانی بهره می‌برند، جامعه‌ی فناوری اطلاعات دیجیتال، آسیب پذیری‌های ذاتی دارد که برای شهروندان، جامعه‌ی کسب‌و کار یا کارکردهای حیاتی جامعه می تواند مخاطرات امنیتی را درپی داشته باشد.

جامعه بتدریج درحال تبدیل شدن به یک فرهنگ خدمات مبنی بر اطلاعات است که در سطحی بسیار گسترده‌تر، خدمات دیجیتال عمومی و تجاری را به شهروندان ارائه نموده، و شبکه‌های فناوری اطلاعات و ارتباطات الکترونیکی[3] و سرویس‌های دیجیتال، نقشی حیاتی را در عملکرد جامعه ایفا می‌کنند.

---

1 critical
2 Know-How
3 Electronic ICT networks

محیط عملیاتی علاوه بر روندهای کلی تغییر، پیشرفت‌های فناوری و استفاده از اینترنت، شدیداً تحت تأثیر ماهیت جهانی این بخش درحال گسترش، تغییر عادات، شیوه‌ی زندگی کاربران و چالش‌های مربوط به قابلیت اطمینان[1] و امنیت می‌باشد.

مخاطرات[2] مربوط به امنیت سایبری روز به روز معمولی‌تر می‌شوند. مخاطراتی که زمانی غیرممکن تلقی می‌شدند، امروزه بطور مرتب ظاهر می شوند.این روند، شکل های جدیدی از ابزارها و روش های مورد استفاده در حملات، آسیب‌پذیری‌های روزافزون و انگیزه‌ی بیشتر مهاجمین را بوجود می‌آورند.

اثر فزاینده‌ی حملات سایبری مستلزم راه‌حل‌های جدید، خلاقانه و مبتکرانه برای کاهش مخاطرات است.در گذشته، مهاجمین، افراد خاص یا گروه‌های کوچک هکری بودند ولی امروزه سازمان‌های مختلف تحت حمایت دولت با استفاده از سلاح‌های سایبری پیشرفته و مدل حملات هدفمند را انجام می‌دهند. تمرکز این تهدیدهای پایدار پیشرفته (APT[3]) برروی اهدافی است که با دقت انتخاب شده‌اند؛ توسعه این تهدیدها نیازمند تخصص ویژه و منابع زیادی است.

یکی از روندهای جهانی این است که سرویس‌ها به سمت اَبر[4] حرکت کنند. مقامات دولتی، شرکت‌ها و شهروندان هرچه بیشتر به **سمت ذخیره‌سازی ابری و رایانش ابری پیش می‌روند. رایانش ابری معرف تغییر در نگرش است**؛ سرویس‌ها در یک اَبر ارائه می‌شوند، جایی که کسی از جزئیات فنی آن آگاه نبوده و کاربران سرویس قادر به کنترل آن نمی‌باشند.رایانش اَبری[5] مدل جدیدی از تولید، استفاده و ارائه‌ی خدمات فناوری اطلاعات و ارتباطات را به نمایش می‌گذارد که شامل منابع مجازی قابل مقیاس پویا بصورت خدمات ارائه شده روی اینترنت می‌باشد. برطبق روند متداول، سازمان‌های دولتی روز به روز داده‌های زیرساخت فناوری اطلاعات بیشتری را به

---

1 reliability
2 Risk
3 Advanced Persistent Threats
4 cloud
5 Cloud computing

سمت اَبر حرکت می‌دهد و در نتیجه، چالش‌های جدیدی در رابطه با امنیت سایبری مطرح می‌شود.رایانش اَبری و سرویس‌های اَبر، پیوند کاملی با اَبر داده[1] دارند که از آن، در یک بستر برای خلق خدمات جدید برای کاربران نهایی استفاده می‌شود.این موضوع به نوبه‌ی خود نشان دهنده نیاز به همکاری نزدیک بین سرویس‌دهندگان اَبر و ارائه‌دهندگان راهکارهای امنیت سایبری است.در آینده، خدمات اَبری روی تولید راه‌حل‌های خاص امنیت سایبری و حفاظت از هویت و حریم خصوصی و راه‌حل‌های متفرقه‌ی مربوط به رمزگذاری داده‌ها، متمرکز خواهد بود.

اینترنت اشیا نشان دهنده ی تبدیل صنعت است؛ که محصولات صنعتی و تولید صنعتی از اینترنت، حسگرهای نانو و کل بخش فناوری اطلاعات و ارتباطات بهره می‌گیرد. **اینترنت اشیاء به اشیاء یا «چیزها» هویت قابل تشخیص داده و می توانند در شبکه‌ی جهانی فناوری اطلاعات و ارتباطات با هم ارتباط برقرار کنند.** تجهیزات جدید از قبیل ربات‌های مختلف صنعتی و خدماتی و حسگرهای گردآوری اطلاعات، در فضایی که به سرعت در حال رشد است، با این شبکه‌ها متصل می‌شوند.آخرین گام این توسعه، شامل انواع مختلف خودروها مثلاً ماشین‌ها، بارکش‌ها و اتوبوس‌ها و انواع مختلف ماشین‌آلات سنگین می‌باشد.

خودروهای امروزی وسایلی هوشمند بوده و اکثر سیستم های آنها توسط رایانه کنترل می‌شوند. ارتباط میان خودروها، سیستم‌های کنترل ترافیک و وسایل کاربری (مثلاً تلفن هوشمند) نیز رو به افزایش است. در حالیکه سیستم‌های اطلاعاتی-سرگرمی[3] سرویس‌های متعددی را به راننده ارائه نموده، همچنین می‌توانند حواس راننده را کم‌کننده باشند. **این ترافیک اطلاعات می‌تواند مخاطرات فنی یا خطاهای کاربر را به دنبال داشته و یا** حتی حملات از راه دور به خودرو را امکان پذیر نمایند.

---

1 Big Data
2 Internet of Things (IoT)
3 Infotainment

برای حل این چالش‌های جدید به تحقیقات سایبری میان-رشته‌ای و جامع نیاز است. با توجه به پیچیدگی این حوزه، **تحقیقات بایستی منطبق با چهار الگوی اساسی علمی شامل: رویکردهای محاسباتی نظری[1]، عملی[2]، مبتنی بر مدل و مبتنی بر داده، صورت گیرند.**

علوم محاسباتی سومین الگوی علوم هستند، که از رایانه‌ها برای شبیه‌سازی پدیده‌ها یا موقعیت‌هایی استفاده می‌شود که هنوز در واقعیت وجود ندارند. پیشرفت‌های سریع در فناوری اطلاعات و صلاحیت روش[3]، معرفی مدل‌های محاسباتی واقعی و پیچیده برای حل تحقیقات مربوط به مسائل را تسهیل نموده است. هنگام جست‌وجوی راه‌حل برای موقعیت‌هایی که در آن ها روش های سنتی قادر به تولید نتایج به حد کافی دقیق نیستند، با موفقیت می توان روش های علوم محاسباتی را بکار گرفت. یک رویکرد محاسباتی می تواند آگاهی را میان بخش‌هایی از امنیت سایبری که برای جامعه حائز اهمیت هستند، ارتقاء دهد. رویکرد محاسباتی نه تنها تحقیقات میان-رشته‌ای و چند-رشته‌ای را تقویت می‌کند بلکه توسعه محصول را نیز تسهیل و تسریع می‌نماید. در عین حال، به کاهش موانع بین زمینه‌های تحقیقاتی در هر دو بخش دولتی و خصوصی نیز کمک می‌نماید. همچنین، نوآوری را تقویت نموده و باعث پیشرفت‌های جدید در تحقیقات و توسعه محصول می گردد.

در بسیاری از موارد، شبیه‌سازی‌ها در مقیاس بسیار همراه با چالش‌هایی در محاسبات متمرکز بر داده است. غلبه بر چالش‌های محاسبات متمرکز بر داده مستلزم بهینه‌سازی جابجایی داده در سطوح مختلف سلسله مراتب حافظه می باشد. زمانی که خود را برای محاسبات در مقیاس وسیع آماده می‌کنیم، این ملاحظات بیش از پیش اهمیت می‌یابند.

---

1 theoretical
2 experimental
3 methodological competence

حجم اطلاعات و داده‌های بایگانی شده در دنیای دیجیتال بسیار وسیع است.با ترکیب هوشمندانه‌ی اطلاعات بلادرنگ، که از منابع مختلف گردآوری شده‌اند، امکان خلق انواع کاملاً جدیدی از اطلاعات بوجود خواهد آمد که می توانند به از میان برداشتن موانع بین بخش‌ها کمک کنند.

امنیت سایبری نقشی اساسی را برای تمامی کاربردهای نوع اَبَرداده [1] ایفا کرده و یکپارچه‌سازی سلول های اطلاعاتی [2] که بواسطه‌ی داده‌کاوی [3] تولید شده‌اند مستلزم نرم‌افزار سطح بالا و صلاحیت [4] فناوری اطلاعات و ارتباطات می‌باشد.توسعه‌ی روش های تحقیقاتی اَبَرداده فرصت‌های بهتری را برای دانشمندان در زمینه(رشته)های مختلف فراهم آورده تا بتوانند تحقیقات را در زمینه‌های مختلف انجام داده و راه‌حل‌هایی را برای سوالات خود بیابند. علاوه بر توسعه در متدولوژی اَبَرداده ها، توجه به همکاری چند-رشته ای [5] و میان-رشته‌ای [6] از جمله بین ریاضیدانان، دانشمندان فناوری اطلاعات و علمای اجتماعی بسیار حائزاهمیت می‌باشد.

امنیت جامع مبتنی بر حداکثر رفع مؤثر تمامی تهدیدها در زندگی افراد می‌باشد.این روزها فناوری اطلاعات و ارتباطات و راه‌حل‌های امنیت سایبری مربوط به آن، نقشی حیاتی در حراست از امنیت جامع ایفا می کنند.امنیت در شکل های مختلف به ویژه امنیت سایبری، زمینه‌ای است که فقط برای کسب صلاحیت و فرصت‌های کسب وکار رشد خواهد کرد.

صلاحیت امنیت سایبری در بخش‌های مختلف و حوزه های مختلف آموزشی رسوخ کرده است.تخصص سطح بالا در امنیت سایبری یکی از ملزومات تولید و بهبود آگاهی نسبت به موقعیت در امنیت سایبری، برنامه‌های مؤثر احتیاطی در برابر

---

1 Big-Data
2 morsels of information
3 Data mining
4 competence
5 multidisciplinary
6 Cross-disciplinary

تهدیدهای سایبری، خلق سیستم‌هایی که از زیرساخت‌های حیاتی دفاع کنند و توسعه‌ی راه‌حل‌های کارکردی امنیت سایبری می‌باشد.

فهرست مطالب

جلد دوم

بخش۳ فناوری امنیت سایبری

بخش۴ امنیت سایبری و اتوماسیون

1 Clustering
2 Log