

به سوی فضای رایانه‌ای امن‌تر

ترجمه:

گروه مترجمان دانشکده و پژوهشکده‌ی پدافند غیرعامل

این کتاب با حمایت مالی سازمان پدافند غیرعامل کشور ترجمه شده است.

دانشگاه جامع امام حسین (ع)

مؤسسه چاپ و انتشارات

مؤسسه چاپ و انتشارات
دانشگاه جامع امام حسین (ع) (پایه)



۱۳۶۵

دانشگاه جامع امام حسین (ع) (پایه)

مؤسسه چاپ و انتشارات

کتاب: ۲۹۶
سری: پدافند غیرعامل - ۴

- عنوان: به سوی فضای رایانه‌ای امن‌تر
- تألیف: گودمن، سیمور ای.
- مترجم: گروه مترجمان دانشکده و پژوهشکده پدافند غیرعامل
- نوبت چاپ: اول ۱۳۸۹
- شمارگان: ۱۰۰۰ نسخه
- نشانی: تهران، بزرگراه شهید بابایی، بعد از پل لشکرک، دانشگاه جامع امام حسین (ع) (پایه) معاونت پژوهش، مؤسسه چاپ و انتشارات، مخزن: ۷۷۱۰۵۷۰۳-۰۴ دورنگار: ۷۷۱۰۵۷۵۲
- مرکز پخش: تهران، میدان فردوسی، فروشگاه و نمایشگاه شماره ۱ مؤسسه چاپ و انتشارات دانشگاه جامع امام حسین (ع) (پایه) مخزن: ۸۸۱۰۲۹۷، همراه: ۰۹۱۲۴۸۷۰۰۱۷

- کلیه حقوق اعم از چاپ و تکثیر، نسخه‌داری، کپی‌برداری، اقتباس برای دانشگاه جامع امام حسین (ع) (پایه) محفوظ است.

سرشناسه	گودمن، سیمور ای، ۱۹۵۳-
عنوان و پدیدآور	به سوی فضای رایانه‌ای امن‌تر / [ترجمه: گروه مترجمان دانشکده و پژوهشکده پدافند غیرعامل]
مشخصات نشر	تهران: دانشگاه جامع امام حسین (ع) (پایه)، مؤسسه چاپ و انتشارات
مشخصات ظاهری	۲۷۵ ص.
فروست	دانشگاه جامع امام حسین (ع) (پایه)، سری پدافند غیرعامل
شابک	۹۷۸-۹۶۴-۴۵۲-۳۰۵-۲
وضعیت فهرست‌نویسی	فیا
یادداشت	عنوان اصلی: Toward a safer and more secure cyberspace, c2007
موضوع	کامپیوترها - ایمنی اطلاعات
موضوع	تروریسم رایانه‌ای - پیشگیری
شناسه افزوده	لین، هریت
شناسه افزوده	دانشگاه جامع امام حسین (ع) (پایه)، مؤسسه چاپ و انتشارات
رده‌بندی کنگره	QA ۷۶ / ک ۹۵ ۱۳۸۹
رده‌بندی دیویی	۰۰۵/۸
شماره کتابشناسی ملی	۲۲۴۹۰۵۵

بسم الله الرحمن الرحيم

«يرفع الله الذين امنوا والذين اوتوا العلم درجات»

خداوند مقام اهل ایمان و دانش مدار عالم را (در دو جهان) رفیع می گرداند.
(سوره مبارکه مجادله - آیه ۱۱)

تمامی ادیان الهی و در رأس آنها اسلام، انسان را موجودی کمال گرا می دانند. از نظر اسلام، انسان همواره در حال تکامل است و به سمت کمال بی نهایت یعنی خداوند تبارک و تعالی است.

یکی از راه های کمال و تقرب به ذات اقدس الهی، علم و دانش است. علمی که - به تعبیر استاد شهید مطهری - زیبایی عقل است؛ علمی که انسان را دایره دین نشانه های معبود را می جوید و می یابد و علمی که هر چه فزون تر می گردد، دارنده آن را به خدا نزدیک تر می کند.

هم از این روست که در نظام مقدس جمهوری اسلامی ایران که شالوده و اساس حاکمیت در آن بر مبنای احکام اسلام است، توجه به علم و دانش و تحقیق و نشر در صدر مسائل قرار دارد.

دانشگاه جامع امام حسین (ع) نیز به عنوان مولود شجره طیبه سپاه پاسداران انقلاب

اسلامی که خود برآمده از عمق ارزش‌های الهی و انقلابی است به عنوان تنها دانشگاه جامع علمی - نظامی کشور، پس از پایان افتخارآمیز حماسه هشت سال دفاع مقدس که خود عرصه‌ای کم‌نظیر برای نمایش لیاقت‌ها و توانمندی‌های علمی- پژوهشی نیروهای مخلص حزب‌اللهی بود، موضوع «جهاد علمی» و تلاش در جهت رشد و شکوفایی هر چه بیشتر در زمینه‌های مختلف را سرلوحه فعالیت‌های علمی خویش قرار داده است. دانشگاه در این راستا از زمان تأسیس، به منظور ترویج و نشر علوم مختلف آثاری عرضه نموده که استیصال اندیشمندان و پژوهشگران مواجه شده است.

امید است این کتاب مورد توجه و بهره‌برداری صاحب‌نظران، محققان و علاقه‌مندان قرار گیرد و ایشان نیز با اعلام نظرات و پیشنهادهای اصلاحی خود، ما را در جهت ترویج و انتشار آثار مورد نیاز - به علمی کشور یاری فرمایند.

و من الله التوفیق

حاونت پژوهش دانشگاه جامع امام حسین(ع)

فهرست مطالب

صفحه

عنوان

پیشگفتار.....	(سیزده)
مقدمه.....	(پانزده)
خلاصه.....	(بیست و سه)
فصل اول: مقدمه.....	
۱-۱ خلاصه گزارش.....	۱
۲-۱ پیشینه‌ی بررسی.....	۳
فصل دوم: چه چیزی در خطر است؟.....	
۱-۲ فناوری اطلاعات منسجم، همه جا و در هر زمان.....	۷
۲-۲ ماهیت آسیب‌پذیری‌های امنیت رایانه‌ای.....	۹
۱-۱-۲ محرمانه بودن.....	۹
۲-۲-۲ تمامیت.....	۹
۳-۲-۲ دسترسی.....	۹
۳-۲ سامانه‌ها و شبکه‌های در معرض خطر.....	۱۲
۱-۳-۲ حمله به اینترنت.....	۱۳
۲-۳-۲ حمله به سامانه‌های محاسبه و کنترل درونی/بی‌درنگ.....	۱۶
۳-۳-۲ تهاجم به امکانات محاسبه‌ی ویژه.....	۱۸
۴-۲ پیامدهای بالقوه‌ی سوءاستفاده.....	۲۰
۵-۲ گستردگی تهدید در برابر فناوری‌های نوین.....	۲۶

۳۱	۶-۲ آینده‌ی شوم
۳۲	۱-۶-۲ تکامل تهدید
۳۹	۲-۶-۲ توانمندی‌ها و اهداف گسترده مهاجمان رایانه‌ای

۵۳ فصل سوم: بهبود وضعیت امنیت رایانه‌ای ملی

۵۳	۱-۳ لایحه‌ی حقوق امنیت رایانه‌ای
۵۴	۱-۱-۱ مقدمه‌ای بر لایحه‌ی حقوق امنیت رایانه‌ای
۵۶	۱-۱-۲ تمهیدهای لایحه‌ی حقوق امنیت رایانه‌ای
۶۲	۳-۱-۲ نظارت‌های پایانی
۶۳	۲-۳ درک چشم‌انداز
۶۴	۳-۳ ضرورت تدبیر
۶۸	۴-۳ اصول شکل‌دهی به ورکار تحقیقات
۶۹	۱-۴-۳ اصل اول: اجرای حقیقت امنیت رایانه‌ای با در نظر گرفتن اهمیت آینده‌ی آن
۸۱	۲-۴-۳ اصل دوم: دفاع در مقابل تهدیدات آینده
۸۳	۳-۴-۳ اصل سوم: تضمین تداوم برنامه‌ریزی شده در دستور کار تحقیقات
۸۵	۴-۴-۳ اصل چهارم: تأکید بر نیاز به گسترش دستور کار تحقیقات
۸۹	۵-۴-۳ اصل پنجم: اشاعه‌ی دانش و محصولات جدید

۹۳ فصل چهارم: گروه ۱- انسداد و محدودسازی رخنه

۹۴	۱-۴ طراحی، توسعه و سنجش امن
۹۴	۱-۱-۴ تحقیقات برای پشتیبانی از طراحی
۱۰۵	۲-۱-۴ انجام تحقیق در پشتیبانی از توسعه
۱۲۳	۳-۱-۴ انجام تحقیق در پشتیبانی از ارزیابی و سنجش
۱۲۹	۲-۴ کاهش و بازیاب مطلوب
۱۳۰	۱-۲-۴ مهار

- ۱۳۲ ۱-۲-۴ بازیاب
- ۱۳۴ ۳-۴ ضمانت سامانه‌ها و نرم‌افزار

فصل پنجم: گروه ۲- پاسخ‌گویی ۱۳۹

- ۱۳۹ ۱-۵ تشخیص هویت
- ۱۴۰ ۱-۱-۵ دقت
- ۱۴۱ ۱-۵-۲ حجت
- ۱۴۱ ۵-۳-۳ دوره / زمان
- ۱۴۱ ۵-۱-۴ پیش‌بینی
- ۱۴۲ ۵-۱-۵ امنیت
- ۱۴۶ ۵-۲ سامانه‌های شناسایی، استفاده و تشخیص حمله (MAD)
- ۱۴۶ ۵-۲-۱ سامانه‌های شناسایی سواستفاده تشخیص حمله مبتنی بر سامانه‌ی میزبان
- ۱۴۷ ۵-۲-۲ سامانه‌های شناسایی سواستفاده و عملیات بی‌هویت شبکه-بنیاد
- ۱۴۹ ۵-۳ مدیریت حقوق رقومی

فصل ششم: گروه ۳- ارتقای کاربرد ۱۵۳

- ۱۵۳ ۱-۶ امنیت قابل استفاده
- ۱۶۳ ۶-۲ بهره‌برداری از اقدامات پیشین
- ۱۶۶ ۶-۳ ماتریس امنیت رایانه‌ای
- ۱۷۹ ۶-۴ اقتصاد امنیت رایانه‌ای
- ۱۸۰ ۶-۴-۱ منافع و انگیزه‌های متضاد بین بازیگران امنیت رایانه‌ای
- ۱۸۵ ۶-۴-۲ ارزیابی احتمال خطر در امنیت رایانه‌ای
- ۱۹۱ ۶-۴-۳ ماهیت و وسعت شکست بازار (در صورت وجود) در امنیت رایانه‌ای
- ۱۹۲ ۶-۴-۴ تغییر رویکرد شرکت‌ها و دگرگونی محاسبه‌های بازار
- ۲۱۰ ۶-۵ خط‌مشی‌های امنیتی

فصل هفتم: گروه ۴- بازداري و پيگرد مهاجمان احتمالي ۲۱۵

۱-۷ مسایل قانونی مرتبط با امنیت رایانه‌ای ۲۱۶

۲-۷ ظرف عمل ۲۱۸

۳-۷ مسائل قانونی ۲۲۱

فصل هشتم: گروه ۵- زمینه‌های میان‌بر تحقیقاتی روشن‌گر مسئله- محور ۲۳۱

۱-۸ امنیت برای سامانه‌های قدیمی ۲۳۱

۲-۸ نقش پنهان‌کاری در دفاع رایانه‌ای ۲۳۶

۳-۸ تهدیدهای از جانب افراد درون سازمان ۲۳۷

۴-۸ امنیت در محدوده‌های رایانه‌ای سنتی و در زمینه کاربردی ۲۴۷

۱-۴-۸ فناوری‌های سلامت ۲۴۷

۲-۴-۸ شبکه برق ۲۴۹

۳-۴-۸ خدمات وب ۲۵۴

۴-۴-۸ سامانه‌های فراگیر و داخلی ۲۵۶

۵-۸ معماری شبکه‌ی امن ۲۵۹

۶-۸ مشخصه‌ی حمله ۲۶۲

۷-۸ مقابله با حملات از نوع بازداري خدمات ۲۶۳

۱-۷-۸ ماهیت مقابله با حملات از نوع بازداري خدمات ۲۶۳

۲-۷-۸ پاسخ به حملات بازداري از خدمات توزیعی ۲۶۵

۳-۷-۸ چالش‌های تحقیق و پژوهش ۲۶۹

۸-۸ مقابله با هرزنامه ۲۷۲

فصل نهم: گروه ۶- تحقیقات نظری ۲۸۱

۱-۹ فعالیت تحقیقات امنیت رایانه‌ای ۲۸۲

۲-۹ رویکردهای زیست‌شناسی به امنیت ۲۸۴

۳-۹ استفاده از تکنیک‌های حمله برای اهداف دفاعی ۲۸۶

۴-۹ تلافی رایانه‌ای ۲۸۷

فصل دهم: نگاهی به آینده ۲۸۹

۱-۱۰ چرا اقدام کافی انجام نشده است؟ ۲۸۹

۲-۱۰ اولویت اقدامات ۲۹۷

۳-۱۰ نظرات پایانی ۳۲۵

پیوست‌ها ۳۲۷

پیوست الف - گزارش‌ها، روش‌های امنیتی رایانه‌ای گذشته ۳۲۷

الف-۱ مقدمه ۳۲۷

الف-۲ فعالیت خط‌مشی امنیت رایانه‌ای از سال ۲۰۰۱ ۳۲۹

الف-۳ شناسایی خطر، اقدامات و روش‌های مناسب ۳۳۴

الف-۴ همکاری، هماهنگی و تشریک مساعی بخش عمومی و خصوصی ۳۴۳

الف-۵ تلاش‌های مهم اخیر در شناسایی دستورکار تحقیقاتی ۳۵۰

الف-۶ چشم‌انداز فعلی تحقیق و توسعه‌ی دولت مرکزی ۳۶۵

فهرست منابع ۳۸۹

پیشگفتار

فضای مجازی رایانه و خطرهای پنهان و آشکار آن همواره به یکی از دغدغه‌های نیروهای نظامی و غیرنظامی تبدیل شده است. زیرساخت‌های حیاتی هر کشور، وابستگی شدیدی به فناوری اطلاعات دارد و اختلال در هر یک از این زیرساخت‌ها می‌تواند آسیب‌ها و خسارت‌های جبران‌ناپذیری را بر جای بگذارد. بنابراین حفاظت از خطرهای موجود در این زمینه می‌تواند باعث کاهش آسیب‌پذیری بالقوه شبکه‌های متکی بر فناوری اطلاعات شود.

هزینه‌هایی که نیروهای مسلح و بخش خصوصی در زمینه امنیت فضای رایانه‌ای شبکه‌های خود صرف نمودند بسیار سنگین و در حال افزایش است. در این زمینه ارتش آمریکا بیشترین سرمایه‌گذاری را از نظر نیروی متخصص و مالی کرده است. اخیراً ارتش آمریکا برای نخستین بار یک ربرال^۱، مسئول رایاورد^۱ یا جنگ‌های رایانه‌ای کرده است، اقدامی که به عقیده‌ی بسیاری، نگرانی‌ها درباره‌ی تسلیحاتی شدن فضای مجازی و اینترنت را شدید می‌کند.

کیت الکساندر، ژنرال چهار ستاره‌ی ارتش آمریکا اکنون مسئول پست جنجالی فرماندهی رایانه‌ای در وزارت دفاع آمریکا است که برای هدایت جنگ‌های مجازی و ایجاد امنیت رایانه‌ای برای بخش‌های مختلف ارتش آمریکا در شبکه‌های رایانه‌ای جهان در نظر گرفته شده است. این انتصاب نشان می‌دهد که پنتاگون به سمت جدیدی روی رایاورد و امنیت شبکه‌های رایانه‌ای باز کرده است. فرمانده جدید را ربرال، تاکنون تنها چند روز پس از آن معرفی شد که نیروی هوایی آمریکا از ماموریت جدید هزاران نفر از نیروهای خود خبر داد. نیروی هوایی این کشور به تازگی اعلام کرد که سی هزار نفر از نظامیان خود را از بخش پشتیبانی فنی به خط مقدم رایاورد منتقل کرده است.

مقام‌های دولت آمریکا اکنون عقیده دارند که دکترین پنتاگون و چهارچوب قانونی موجود نتوانسته عملیات برخط^۲ را سازماندهی کند و واشنگتن در سال‌های گذشته در

1. Cyberwar

2. Online

رایاورد و امنیت شبکه‌های رایانه‌ای نظامی و غیر نظامی خود، یک قدرت ضعیف بوده است. ژنرال الکساندر می‌گوید: تنها شبکه وزارت دفاع آمریکا هر روز با ده‌ها هزار حمله در فضای مجازی روبه‌رو است که امسال (۲۰۱۰) این مسئله به اوج خود می‌رسد.

واقعیت این است که در دنیای امروز میزان حمله‌ها و نبردهای رایانه‌ای هر روز در حال افزایش است. در این میان کشوری مانند چین با در اختیار داشتن گروهی از بهترین رخنه‌گرها^۱ در صف اول کشورهای قدرتمند در رایاورد محسوب می‌شود. چین اکنون از سوی مقام‌های غربی متهم شده است که سال گذشته با حمله‌های رایانه‌ای، شرکت گوگل و بیست شرکت بزرگ دیگر را هدف قرار داده است. آمریکایی‌ها همچنین چین را مسئول مجموعه‌ای از حمله‌های زنجیره‌ای و هماهنگ به شبکه‌های رایانه‌ای دولتی و نظامی آمریکا در سال ۲۰۰۳ می‌دانند. رخنه‌گرهای کره شمالی و روسیه نیز در ردیف‌های بعدی متهمان به حمله‌های گسترده در فضای مجازی هستند.

مسکو نیز متهم است که در پشت پرده حمله گسترده رایانه‌ای به استونی در سال ۲۰۰۷ قرار دارد، حمله‌ای که رومن عملیات بزرگ در فضای رایانه‌ای در تاریخ به حساب می‌آید.

فرماندهی جدید رایاورد ارتش آمریکا برقراری امنیت و دفاع را از شبکه‌های اطلاعاتی این ارتش به عهده خواهند گرفت که بیش از نود هزار نظامی در آن فعالیت می‌کنند.

در فضای مجازی، روش‌ها و تکنیک‌ها آن قدر سریع‌تر و پیچیده‌تر می‌شوند که کسی نمی‌تواند منتظر سیاست‌گذاری دولتی برای مقابله با این تهدیدها باقی بماند. هرگونه غفلت یا بی‌توجهی به امنیت شبکه‌های رایانه‌ای و سامانه‌های متکی به آن، موجب خسارت‌های جبران‌ناپذیری به زیرساخت‌های حیاتی و امنیت ملی هر کشوری خواهد گردید.

مترجم

مقدمه

در چند سال گذشته، امنیت رایانه‌ای، از نگرانی بیش‌تر دانشمندان رایانه و مدیران سامانه‌های اطلاعات به مسئله‌ی اهمیت ملی تبدیل شده است. زیرساخت‌های حیاتی ملی، شبکه‌های برق‌رسانی، سامانه‌های مراقبت پرواز، سامانه‌های مالی و شبکه‌های ارتباطی برای کارکرد خود، به طور گسترده‌ای وابسته به فناوری اطلاعات (IT)^۱ می‌باشند.

نگرانی‌های موجود در مورد آسیب‌پذیری این زیرساخت‌ها، در محیط امنیت‌گرای پس از حمله‌ی مای‌یورده سپتامبر ۲۰۰۱، افزایش یافته است. نگرانی فزاینده سیاست‌گزاران ملی نشان می‌دهد که برخی کشورها متخاصم با پشتیبانی منابع بی‌شماری که در اختیار دارند، آسیب‌پذیری‌های رایانه‌ای زیرساخت‌های حیاتی، بهره‌برداری نموده و در نتیجه تهدیدی را به کشور، وارد می‌کند.

امروزه، درک کافی در مورد آنچه باعث آسیب‌پذیر شدن سامانه‌های فناوری اطلاعات در مقابل تهاجم می‌شود، وجود ندارد. بنابراین، بهترین روش، کاهش این آسیب‌پذیری‌ها و نیز چگونگی انتقال دانش امنیت را به‌ای به اقدام واقعی است.

بر طبق دلیل‌های گفته شده و پاسخگویی به توجه فوری جریه و قضائیه، شورای تحقیقات ملی^۲، کمیته‌ای را برای بهبود تحقیقات امنیت رایانه‌ای در آمریکا، ایجاد نمود. هدف این کمیته توسعه راهبرد تحقیق‌های امنیت رایانه‌ای در قرن بیست و یکم است. برای توسعه‌ی این راهبرد، این کمیته از گزارش‌های تهیه شده قبلی در این زمینه، مانند مخاطره‌های رایانه‌ها^۳ (۱۹۹۱)، اعتماد به رایافضا^۴ (۱۹۹۸) و فناوری اطلاعات برای ضد تروریسم^۵ (۲۰۰۳)، استفاده نمود. اگر چه این‌ها در چند سال گذشته تهیه شده‌اند، ولی

1. Information Technology
2. National Research Council
3. Computers at Risk
4. Trust in Cyberspace
5. Information Technology for Counterterrorism

کمیته دریافت که این گزارش‌ها شامل نکته‌های با ارزش، برای تلاش‌های حاضر هستند. علاوه بر این، کمیته‌ی مزبور، چندین جلسه گفت‌ووشنود و توجیهی را برگزار کرد که اطلاعات خوبی را درمورد نگرانی‌های اخیر و پاسخ به این نگرانی‌ها، فراهم نمود.

گزارش کمیته‌ی مشورتی فناوری اطلاعات ریاست جمهوری در مورد امنیت رایانه‌ای: نقدی بر تعیین اولویت‌ها که دستور کار تحقیقاتی را مطرح می‌کند و توصیه‌هایی را در زمینه‌ی چگونگی پیامدسازی آن‌ها ارایه می‌دهد، نقطه آغاز مفیدی را نیز فراهم آورد.

جول-۱. دارای وظیفه‌های کامل این کمیته است. بررسی‌های کمیته در زمینه‌ی چشم‌انداز تحقیقات، امنیت رایانه‌ای اخیر، در ضمیمه‌ی ب درج شده است.

برطبق وظیفه‌ی حوزه، بخش ب- ۵ نشان‌دهنده‌ی تلاش‌های تحقیقاتی در زمینه‌ی امنیت رایانه‌ای، اعتبار ارزیابی مجموعه‌ی اخیر عنوان‌ها است. بخش ۴ و ب- ۶، سطح تلاش‌ها، حجم کار و منابع اعتباردهی را مورد بحث قرار می‌دهد و بخش ب- ۳ نیز کیفیت را مطرح می‌کند. به ترتیب با زمان بندی تحقیقات امنیت رایانه در بخش ۲-۲-۱۰ مورد اشاره قرار می‌گیرد.

ابعاد ساختاری برنامه تحقیقات امنیت رایانه در بخش ۳-۳ نیز مطرح می‌شود.

در شرح کار این کمیته، به دو موضوع به طور کامل اشاره نشده است. در موضوع اول، با وجود این که بخش ۲ اطلاعات کلی در زمینه‌های مناسب، می‌کند و برنامه‌ای را فراهم می‌آورد، این گزارش، شرح کامل اولویت‌های تحقیق را در این زمینه‌ها، ارایه نمی‌دهد. دلیل این موضوع که در بحث ۴-۴-۳ به طور کامل‌تر شرح داده می‌شود، این است که در ادامه‌ی برنامه‌ها، کمیته‌ی مزبور به این نتیجه رسید که دستور کار تحقیقات امنیت رایانه کشور، باید جامع باشد و هر تلاشی برای مشخص کردن اولویت‌های تحقیق به روش از بالا به پایین، سودمند نخواهد بود.