



به نام خدا

امنیت رایانش ابری

مؤلفان:

ابراهیم فوقی

سید ابراهیم موسوی پور



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گیرند.

◀ عنوان کتاب: امنیت رایانش ابری

◀ مولفان: ابراهیم فوقی - سید ابراهیم موسوی پور

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ ویراستار: مهدیه مخبری

◀ صفحه آرای: فرنوش عبدالهی

◀ طراح جلد: داریوش فرسایی

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۴۰۲

◀ چاپ و صحافی: صدف

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۲۹۴۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۲۲-۲۱۸-۶۹۸-۲

◀ نشانی واحد فروش: تهران، خیابان انقلاب، خیابان دانشگاه

◀ تقاطع شهدای ژاندارمری - پلاک ۱۵۸ ساختمان دانشگاه -

◀ طبقه دوم - واحد ۴ تلفن ها: ۶۶۹۶۵۷۴۹-۲۲۰۸۵۱۱۱

◀ فروشگاه‌های اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagaran-tehran.com

نشانی اینستاگرام دیبا dibagaran_publishing نشانی تلگرام: @mftbook

هر کتاب دیباگران، یک فرصت جدید علمی و شغلی.

هر گوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتهای دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

فهرست مطالب

فصل ۱ / مقدمه‌ای بر رایانش ابری..... ۱۷

- ویژگی‌های رایانش ابری ۱۹
- مدل‌های رایانش ابری ۲۱
- مدل‌های استقرار ۲۳
- خدمات و فناوری‌های ابری ۲۵

فصل ۲ / مفاهیم اساسی رایانش ابری..... ۲۸

- مقدمه ۲۹
- عناصر محاسبات ابری ۲۹
- رایانش ابری ۲۹
- خدمات ابری ۳۱
- نرم‌افزار به‌عنوان یک سرویس ۳۲
- پلتفرم به‌عنوان یک سرویس ۳۳
- زیرساخت به‌عنوان یک سرویس ۳۳
- سایر خدمات ابری ۳۳
- سرویس XaaS؛ همه چیز به‌عنوان یک سرویس ۳۵
- مدل‌های استقرار ابر ۳۶
- معماری مرجع محاسبات ابری NIST ۴۰
- بازیگران رایانش ابری ۴۱
- اجزای معماری ارائه‌دهنده ابر ۴۴
- معماری مرجع محاسبات ابری ITU-T ۴۴
- بازیگران رایانش ابری ۴۵
- معماری لایه‌ای ۴۶
- معماری مرجع تابعی محاسبات ابری ITU-T ۴۷
- الزامات شبکه برای رایانش ابری ۴۸

فصل ۳ / اصول امنیت رایانش ابری ۵۱

- مقدمه ۵۲
- مروری بر امنیت کامپیوتر ۵۲
- آسیب‌پذیری‌ها و حملات ۵۳
- سطح کاربردی ۵۳
- لایه سیستم عامل ۵۵
- هایپروایزر، ذخیره‌سازی، سخت‌افزار و شبکه ۵۶
- مکانیسم‌های امنیت ابری ۵۷
- امضای دیجیتالی ۵۸
- هش کردن ۵۹
- امنیت مجازی‌سازی ۶۰
- حریم خصوصی و امنیت در خدمات ذخیره‌سازی ابری ۶۰
- مدل‌های حفاظت از داده‌های ابری ۶۱
- اجرای سیاست‌های کنترل دسترسی در فضای ابری ۶۳
- سایر دلایل احتمالی نشت داده در فضای ابری ۶۴
- حریم خصوصی و امنیت در چند ابر ۶۶
- ویژگی‌های امنیت و حریم خصوصی مورد نظر در چند ابری ۶۷
- تضمین امنیت، حریم خصوصی و قابلیت اطمینان در چند ابری ۶۸
- حسابداری ابری ۶۹

فصل ۴ / خطوط پایه امنیت، حریم خصوصی و اعتماد ابری ۷۱

- مقدمه ۷۲
- درک تهدیدها ۷۴
- طبقه‌بندی و اقدامات متقابل ۷۶
- زیرساخت‌ها و تهدیدات میزبان ۷۶
- بلاایای طبیعی که می‌تواند به زیرساخت‌های حیاتی آسیب برساند ۷۶
- دسترسی فیزیکی غیرمجاز به امکانات یا تجهیزات ۷۶
- آموزش ناقص / سهل‌انگاری کارکنان ۷۷
- Dumpster Diving ۷۷
- حدس زدن رمز عبور ۷۷
- دسترسی غیرمجاز به داده‌ها یا سیستم‌های فناوری اطلاعات ۷۷

- به خطر افتادن گزارش‌های امنیتی عملیاتی ۷۸
- شبکه قطع می‌شود ۷۸
- افزایش امتیاز ۷۸
- حذف ناامن یا ناکارآمد داده‌ها ۷۸
- اسکن یا مشاهده مخرب ۷۹
- رمزنگاری ناامن یا منسوخ ۷۹
- انکار اقتصادی خدمات (EDoS) و فرسودگی منابع ۷۹
- خرابی جداسازی ۸۰
- تقلب در صورتحساب ۸۰
- ثبت و نظارت کافی ۸۰
- خرابی یا خاتمه سرویس ابری ۸۰
- شکست تأمین‌کنندگان شخص ثالث ۸۱
- قفل کردن ۸۱
- مشکلات انطباق ۸۱
- ارائه داده‌های ابری، مدیریت متادیتا و داوری ۸۲
- اصلاحات زیرساخت ۸۲
- پردازش داده‌ها ۸۳
- تغییرات اداری و مالکیتی ۸۳
- انکار خدمات به مستأجرین به دلیل قضاوت نادرست یا تخصیص نادرست منابع ۸۳
- احضاریه و E-Discovery ۸۴
- تهدیدات ارائه‌دهنده خدمات ۸۴
- بازپخش حملات ۸۴
- رهگیری داده‌ها ۸۴
- امنیت مرورگر ۸۵
- برچسب‌گذاری آلمان امضا XML ۸۵
- آسیب‌پذیری‌های تزریق ۸۵
- سهل‌انگاری مشتری و امنیت ابری ۸۶
- قرارگرفتن در معرض رابط مدیریت ۸۶
- از دست دادن حاکمیت ۸۶
- تهدیدات عمومی ۸۶

- حملات مهندسی اجتماعی ۸۶
- انکار سرویس توزیع شده (DDoS) ۸۷
- قرار گرفتن در معرض یا از دست دادن کلیدهای رمزگذاری ۸۷
- قرار گرفتن در معرض موتور سرویس ۸۷
- بد افزار ۸۷
- ارزیابی تهدیدها ۸۸
- اعتماد به ابر ۸۹
- الزامات GDPR برای ارائه‌دهندگان ابر ۹۱
- محدوده مادی و سرزمینی ۹۱
- اصول حفاظت از داده‌ها ۹۱
- رضایت ۹۲
- فرزندان: رضایت والدین ۹۲
- داده‌های حساس و پردازش قانونی ۹۲
- اطلاعیه‌های اطلاعاتی ۹۲
- دسترسی، تصحیح و قابل حمل بودن موضوع ۹۳
- حق اعتراض ۹۳
- حق پاک کردن و حق محدودیت پردازش ۹۳
- پروفایل و تصمیم‌گیری خودکار ۹۳
- پاسخگویی، امنیت و اطلاعیه نقض ۹۴

فصل ۵ / زیرساخت به عنوان یک سرویس (IaaS) ۹۵

- اجزای یک زیرساخت ابری ۹۶
- کامپوننت را محاسبه کنید ۹۶
- مفاهیم امنیتی ۹۷
- شبکه ۹۸
- مفاهیم امنیتی ۹۸
- ذخیره‌سازی ۹۸
- رویکردهای اساسی ۹۸
- مفاهیم امنیتی ۹۹
- پایگاه‌های داده ۹۹
- رویکردهای اساسی ۱۰۰

- مفاهیم امنیتی..... ۱۰۱
- مدیریت ۱۰۱
- مفاهیم امنیتی..... ۱۰۱

فصل ۶ / مدیریت کلید رمزنگاری برای حفاظت از داده‌ها ۱۰۳

- مقدمه ۱۰۴
- زمینه ۱۰۴
- چرخه عمر مدیریت کلید ۱۰۵
- انتخاب‌های طراحی سیستم مدیریت کلیدی ۱۰۶
- درایورها برای طراحی مدیریت کلید ابری ۱۰۷
- چالش‌های مدیریت کلید ابری ۱۰۸
- استراتژی‌های مدیریت کلید ابری ۱۱۰
- داده‌ها را به حداقل برسانید تا رمزگذاری شوند ۱۱۰
- متن رمز را از کلیدها جدا کنید ۱۱۰
- به حداکثر رساندن جدایی بین متن رمزی و کلیدها ۱۱۰
- ایجاد اعتماد در Cryptomodule ۱۱۰
- از تکنیک‌های تقسیم کلید استفاده کنید ۱۱۱
- نیازهای امنیتی لایه‌ها ۱۱۱
- رابط کاربری لایه ۱ ۱۱۲
- نرم‌افزار کاربردی لایه ۲ ۱۱۳
- سیستم عامل سرور میزبان لایه ۳ ۱۱۵
- سخت‌افزار و شبکه زیرساخت میزبانی لایه ۴ ۱۱۷
- بهبود در همه سطوح ۱۱۹
- احراز هویت چند سطحی ۱۲۰
- رمزگذاری ۱۲۱
- مدیریت رمز عبور ۱۲۱
- سرورهای توزیع شده ۱۲۲
- کنترل دسترسی کارآمد با اجرای کلید ۱۲۳
- رمزگذاری بیش از حد ۱۲۵
- محدودیت‌ها ۱۲۵
- طرح اصلی ۱۲۶

- ساختار دو هدر ۱۲۷
- ابطال دسته‌ای ۱۲۸
- به‌روزرسانی‌های سیاست کنترل دسترسی ۱۲۸
- اعطای امتیازات ۱۲۹
- لغو امتیازات ۱۳۰
- تجزیه و تحلیل عملکرد ۱۳۱
- سربار برای اعطای امتیازات ۱۳۱
- سربار برای ابطال ۱۳۲
- تجزیه و تحلیل امنیتی ۱۳۲
- طراحی سیستم ۱۳۳
- مدل پایه ۱۳۳
- مشتری ۱۳۴
- سرور ۱۳۵
- عملیات رمزگذاری شده ۱۳۵
- مدیریت کلیدی ۱۳۶
- سیاست‌های جریان کلیدی ۱۳۷
- مقایسه دو نوع رمز ۱۳۷
- قوانین به‌روزرسانی کلیدی برای Stream Cipher ۱۴۰
- پیاده‌سازی ۱۴۰
- بهبود سرور ۱۴۲
- به‌روزرسانی ویژگی‌ها ۱۴۲
- آزمایش حذف‌های تصادفی ۱۴۸

فصل ۷ / معماری و ملزومات امنیت محاسبات ابری ۱۵۱

- مقدمه ۱۵۲
- تعریف محاسبات ابری ۱۵۳
- معماری مرجع محاسبات ابری ۱۵۵
- ملزومات امنیت رایانش ابری ۱۵۶
- تقسیم مسئولیت‌های عملیاتی ۱۵۹
- دید و اعتماد به اکوسیستم ابر ۱۶۰
- مرزها در یک اکوسیستم ابری ۱۶۱

- ۱۶۲ مرز داده کاربر
- ۱۶۳ مرز خدمات
- ۱۶۴ IaaS امنیتی
- ۱۶۵ PaaS امنیتی
- ۱۶۷ SaaS امنیتی
- ۱۶۸ مرز ارکستراسیون اکوسیستم
- ۱۷۰ مرز استقرار
- ۱۷۱ مرز اعتماد
- ۱۷۲ تعریف ریشه اعتماد شما
- ۱۷۳ مدیریت احراز هویت و مجوز کاربر

فصل ۸ / معماری محاسبات ابری و مفاهیم امنیتی ۱۷۶

- ۱۷۷ مقدمه
- ۱۷۷ ویژگی‌های خدمات محاسبات ابری
- ۱۷۸ مشتریان ابری
- ۱۷۹ مشتریان نرم‌افزار
- ۱۸۰ مشتریان تین یا وب اپلیکیشن‌ها
- ۱۸۲ برخی از نگرانی‌های بالقوه ذخیره‌سازی ابری
- ۱۸۲ سرورهای ابری
- ۱۹۲ اقدامات احتیاطی امنیتی

فصل ۹ / معماری امن ابری ۱۹۴

- ۱۹۵ مقدمه
- ۱۹۶ پروفایل امنیت ابری
- ۲۰۳ کنترل‌های امنیتی در زیرساخت‌های فیزیکی

فصل ۱۰ / قفل کردن سرورهای ابری ۲۰۶

- ۲۰۷ مقدمه
- ۲۰۷ مسئولیت‌ها و مالکیت
- ۲۰۸ جنبه‌های نظارتی قانونی و صدور مجوز
- ۲۰۹ تعریف مناطق مرکز داده و مناطق دسترسی
- ۲۱۱ طراحی امنیتی Hypervisor
- ۲۱۴ گزینه‌های رمزگذاری سرور ابری

- رمزگذاری ذخیره‌سازی ابری ۲۱۴
- مدیریت کلید رمزگذاری در ابر ۲۱۵
- رمزگذاری و احراز هویت برای دسترسی اداری ۲۱۶
- معماری امنیت شبکه ۲۱۷
- طراحی امنیت ابری خصوصی مجازی ۲۱۷
- تشخیص نفوذ شبکه و کنترل سوءاستفاده ۲۱۸
- امنیت اتصال ابر مشتری ۲۲۰
- دروازه‌های VPN ۲۲۰
- خطوط اجاره‌ای و اتصال مستقیم ۲۲۱
- اتصال اینترنت HTTPS ۲۲۱
- هویت ابری و مدیریت دسترسی ۲۲۲
- اقدامات امنیتی عمومی سرور ابری ۲۲۴

فصل ۱۱ / تضمین یکپارچگی ارائه‌دهندگان شخص ثالث برای برون‌سپاری داده ۲۳۱

- مقدمه ۲۳۲
- مدل‌ها ۲۳۵
- طراحی راه‌حل عملی حسابرسی سه‌جانبه ۲۳۶
- مشخصات فنی و آپشن‌ها ۲۳۶
- اجرای طرح حسابرسی سه‌جانبه ۲۳۷
- بررسی یکپارچگی داده از راه دور برای تنظیمات ایستا ۲۳۸
- الزامات برای طرح‌های RDIC ۲۳۸
- طرح‌های اولیه RDIC ۲۳۹
- دارا بودن داده‌های قابل اثبات ۲۴۰
- مدل خصمانه ۲۴۱
- طرح PDP ۲۴۲
- دستیابی به استحکام ۲۴۴
- ملاحظات ۲۴۵
- مدارک بازیابی ۲۴۵
- دارا بودن داده‌های قابل اثبات پویا ۲۴۷
- اثبات‌های دینامیکی قابلیت بازیابی ۲۴۸
- سیستم‌های کنترل نسخه قابل بازرسی ۲۵۰

- ۲۵۲ برون‌سپاری محاسبات مبتنی بر ابر
- ۲۵۳ محاسباتی که می‌توان آنها را به ابرها واگذار کرد
- ۲۵۳ عملیات جبری
- ۲۵۴ مقایسه رشته‌ها
- ۲۵۴ MapReduce
- ۲۵۵ توان مدولار
- ۲۵۵ برون‌سپاری محاسبات ایمن به ابرها
- ۲۵۵ مدل خصمانه
- ۲۵۶ ویژگی‌های برون‌سپاری محاسبات ایمن
- ۲۵۷ چالش‌ها
- ۲۵۷ عدم شفافیت
- ۲۵۷ چند اجاره‌ای
- ۲۵۸ آسیب‌پذیری در معماری ابری
- ۲۵۸ مسائل مربوط به مقررات و انطباق
- ۲۵۹ راه‌حلی برای ایمن برون‌سپاری محاسباتی
- ۲۵۹ محاسبه ایمن توابع دلخواه
- ۲۵۹ مدارهای پیچ‌خورده
- ۲۶۰ رمزگذاری کاملاً هممورفیک
- ۲۶۱ معماری برای برون‌سپاری محاسبات ایمن
- ۲۶۳ عملیات جبری
- ۲۶۴ برنامه‌ریزی خطی
- ۲۶۴ معادله خطی
- ۲۶۵ عملیات ماتریسی
- ۲۶۶ محاسبات نقشه‌برداری
- ۲۶۹ عملیات رشته
- ۲۶۹ مشکلات باز
- ۲۶۹ رعایت مقررات
- ۲۷۰ مسائل حقوقی

فصل ۱۲ / فناوری محاسبات مورد اعتماد ۲۷۱

- ۲۷۴ گروه محاسباتی مورد اعتماد
- ۲۷۵ مروری بر وظایف امنیتی TPM
- ۲۷۶ فناوری اجرای مورد اعتماد اینتل
- ۲۷۷ زنجیره ایستا از اعتماد
- ۲۷۷ زنجیره دینامیک اعتماد
- ۲۷۸ ثبت پیکربندی پلتفرم
- ۲۷۹ اندازه‌گیری استاتیک PCR
- ۲۷۹ اندازه‌گیری دینامیک PCR
- ۲۸۰ مورد استفاده محاسباتی قابل اعتماد
- ۲۸۱ موتور قابل مشاهده دوزنقه‌ای
- ۲۸۳ معرفی
- ۲۸۵ پیشینه فن‌آوری
- ۲۸۶ محاسبات مورد اعتماد - مفاهیم کلیدی
- ۲۸۷ برخی انتقادات از محاسبات مورد اعتماد
- ۲۸۷ برخی از موارد استفاده TEE
- ۲۸۸ پیاده‌سازی‌های Tpm
- ۲۸۸ ARM Trustzone
- ۲۸۹ پردازنده امن AMD
- ۲۹۰ اینتل SGX
- ۲۹۲ محاسبات قابل اعتماد و ابر
- ۲۹۳ عناصر امن در ابر
- ۲۹۵ شبیه‌سازی کارت میزبان
- ۲۹۷ کانتینرها به‌عنوان یک راه‌حل امنیتی

فصل ۱۳ / فناوری محاسبات مورد اعتماد و پیشنهادات برای حل مشکلات امنیت رایانش ابری ۲۹۹

- ۳۰۰ معرفی
- ۳۰۰ تکنولوژی محاسباتی قابل اعتماد
- ۳۰۰ پلتفرم مورد اعتماد
- ۳۰۱ ماژول پلتفرم مورد اعتماد
- ۳۰۵ گواهی از راه دور

- محدودیت‌ها ۳۰۶
- تأیید از راه دور ماشین‌های مجازی ۳۰۷
- TPM مجازی ۳۰۷
- چارچوب کلی ۳۱۱
- معماری Keylime ۳۱۲
- پروتکل مشتق کلید سه‌جانبه ۳۱۶

خط‌مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی با کیفیت عالی است که بتواند
خواسته‌های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.
هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و سرعت توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه، نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش برجسته نموده است.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران و محققان در زمینه‌های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهد.

کتابی که در دست دارید تألیف "جناب آقایان ابراهیم فوقی-سید ابراهیم موسوی پور" است که با تلاش همکاران ما در نشر دیباگران تهران منتشر گشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات و خواسته‌های خود، به ما کمک کنید تا بهتر و دقیق‌تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم. برای رساندن پیام‌هایتان به ما از رسانه‌های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره‌های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
dibagaran@mftplus.com

تو من بودی و من می دانستم...
تقدیم به آن نگاهی که تمام هستی و دلم فدای اوست.

مقدمه مولف

این کتاب راهنمای جامع به عنوان یک مرجع حرفه ای برای کامل ترین و مختصرترین نمای امروزی امنیت رایانش ابری عمل می کند و پوشش عمیقی از تئوری، فناوری و عملکرد رایانش ابری امنیت را ارائه می دهد زیرا آن ها به فناوری های جا افتاده و همچنین پیشرفت های اخیر مربوط می شوند. بنابراین در این کتاب راه حل های عملی برای طیف گسترده ای از مسائل امنیتی رایانش ابری را بررسی می کنیم. فصل های جداگانه در این زمینه تألیف شده و به چالش های فوری و بلندمدت در حوزه های تخصصی مربوطه می پردازد.

مخاطبان اصلی این کتاب، مهندسين و علاقه مندين به نظارت و تجزيه و تحليل محيط هاي امنيتي محاسبات ابري هستند، کتاب امنیت شبکه های ابری همچنین برای امنیت و حرفه ای های مرتبط و علاقه مند به نظارت تاکتیکی و طبقه بندی و ردیابی اهداف امنیتی محاسبات ابری مفید خواهد بود.

افراد دیگری که علاقه مند به استفاده از امنیت رایانش ابری برای درک محیط های خاص هستند کسانی که در دانشگاه، دولت و صنعت هستند.

هر شخصی که به دنبال بهره برداری از مزایای فناوری های امنیتی رایانش ابری، از جمله ارزیابی معماری ها، اجزاء، عملیات و ابزارهای رایانش ابری است و هر کسی که در جنبه های امنیتی رایانش ابری دخیل است و دانش مقدماتی از رایانش ابری یا تجربه ای معادل آن دارد.

این کتاب می تواند بعنوان مرجع جامع برای دانشجویان در مقاطع کارشناسی و کارشناسی ارشد در بحث امنیت رایانش ابری نیز ارزشمند خواهد بود.

در پایان از خوانندگان عزیز خواهشمندم که انتقادات سازنده و پیشنهادهای خود را به نشانی الکترونیکی ebrahimfoghi@outlook.com ارسال نمایند.

ابراهیم فوقی

بهار ۱۴۰۲