

امنیت رایانش ابری

تهدیدات، چالش‌ها، معماری امنیتی و استانداردها

تالیف:

دکتر احمد صلاحی

آراد کتاب

عنوان و پدیدآور	: امنیت رایانش ابری، تهدیدات، چالش‌ها، معماری امنیتی و استانداردها /
تألیف احمد صلاحی	
مشخصات نشر	: تهران، آراد کتاب، ۱۳۹۶
مشخصات ظاهری	: ۲۳۰ ص، مصور.
شابک	: ۹۷۸-۶۰۰-۱۸۶-۳۳۹-۴
موضوع	: محاسبات ابری
موضوع	: محاسبات ابری - تدابیر ایمنی
رده بندی کنگره	: ۱۳۹۶ الف۸ص/۵۸۵/ QA ۷۶
رده بندی دیویی	: ۰۰۴ / ۶۷۸۲
شماره کتابخانه ملی	: ۴۹۲۷۹۳۷

امنیت رایانش ابری

تهدیدات، چالش‌ها، معماری امنیتی و استانداردها

تألیف: دکتر احمد صلاحی	ناشر: آراد کتاب
نوبت چاپ: اول	
سال چاپ: ۱۳۹۶	تیراژ: ۵۰۰ جلد
چاپ و صحافی: مهرگان	قیمت: ۲۳۵۰۰۰ تومان
شابک: ۹۷۸-۶۰۰-۱۸۶-۳۳۹-۴	

حق چاپ برای پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) با عنایت به قانون حمایت مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ محفوظ است و متخلفین تحت پیگرد قانون قرار می گیرند.

با همکاری و حمایت پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

مرکز پخش و فروش:

انتشارات آراد کتاب تلفن: ۰۹۱۲۳۰۶۲۴۵۸ - ۶۶۴۸۲۲۲۶ - ۶۶۹۷۵۲۸۵

فروشگاه اینترنتی: www.aradbook.com

تقدیر و تشکر

لازم است از تمام کسانی که در ویرایش، تایپ و رسم اشکال و ترجمه و چاپ کتاب به من یاری رسانده‌اند به خصوص فرزندانم الهام صلاحی که در ویرایش و رسم اشکال و ترجمه با من همکاری کرده؛ آقای بذرافشان مدیر دفتر اسناد علمی، آقای امیر حسین پناهی مدیر گروه امنیت شبکه و آقای دکتر کامبیز بدیع معاون محترم پژوهش و توسعه ارتباطات علمی مرکز تحقیقات مخابرات و سرکار خانم ملیحه مشرقی که تایپ کتاب را به عهده داشته‌اند تشکر کنم.

فهرست مطالب

17	فصل 1- تعریف رایانش ابری
17	1-1- تعریف انستیتوی ملی استانداردها و فناوری (NIST) از رایانش ابری [1]
17	2-1- ویژگی‌های اساسی
17	1-2-1- خود خدمتی بر اساس بر تقاضا
18	2-2-1- دسترسی گسترده به شبکه
18	3-2-1- جمع کردن منابع
18	4-2-1- کشسانی سریع
18	5-2-1- خدمات اندازه‌گیری شده
19	3-1- مدل‌های سرویس
19	1-3-1- نرم افزار به عنوان یک سرویس (SaaS)
19	2-3-1- سکو به عنوان یک سرویس (PaaS)
19	3-3-1- زیرساخت به عنوان یک سرویس (IaaS)
20	4-1- مدل‌های استقرار
20	1-4-1- ابر خصوصی
20	2-4-1- ابر انجمنی
20	3-4-1- ابر عمومی
20	4-4-1- ابر ترکیبی
20	5-1- مروری بر معماری مرجع رایانش ابری (CCRA)
23	1-5-1- مصرف‌کننده ابر
23	2-5-1- ارائه‌دهنده ابر
24	3-5-1- ممیز ابر
25	4-5-1- کارگزار ابر
25	5-5-1- حامل ابر
25	مراجع
27	فصل 2- چارچوب امنیتی برای رایانش ابری [1]
27	1-2- بررسی اجمالی
29	2-2- تهدیدات امنیتی در رایانش ابری [1]
29	1-2-2- تهدیدات امنیتی مشتریان خدمات ابری
29	1-1-2-2- از دست رفتن و نشتی داده‌ها
30	2-1-2-2- دسترسی نا امن به خدمات
30	3-1-2-2- تهدیدات خودی
31	3-2- تهدیدات امنیتی برای ارائه‌دهندگان رایانش ابری (CSPs)
31	1-3-2- دسترسی غیر مجاز مدیریتی
31	2-3-2- تهدیدات خودی
32	4-2- چالش‌های امنیتی برای رایانش ابری
32	1-4-2- چالش‌های امنیتی برای مشتریان خدمات ابری (CSCs)
32	1-1-4-2- ابهام در مسئولیت

32	2-1-4-2- از دست رفتن اعتماد
33	3-1-4-2- از دست رفتن حاکمیت
33	4-1-4-2- از دست رفتن محرمانگی
33	5-1-4-2- غیرقابل دسترس بودن سرویس
34	6-1-4-2- قفل شدن در داخل یک ارائه‌دهنده سرویس ابری
34	7-1-4-2- مصادره مالکیت معنوی
34	8-1-4-2- از دست رفتن یکپارچگی نرم‌افزار
34	2-4-2- چالش‌های امنیتی برای ارائه‌دهندگان سرویس ابری (CSPs)
34	1-2-4-2- ابهام در مسئولیت
35	2-2-4-2- محیط اشتراکی
35	3-2-4-2- ناسازگاری و تضاد مکانیسم‌های حفاظتی
35	4-2-4-2- تضاد حوزه‌های قضایی
36	5-2-4-2- ریسک‌های تکاملی
36	6-2-4-2- مهاجرت و یکپارچگی بد
36	7-2-4-2- عدم پیوستگی کسب‌وکار
36	8-2-4-2- قفل شدن شریک خدمات ابری
37	9-2-4-2- آسیب‌پذیری زنجیره تامین
37	10-2-4-2- وابستگی‌های نرم‌افزاری
37	3-4-2- چالش‌های امنیتی برای شرکاء خدمات ابری (CSNs)
38	1-3-4-2- ابهام در مسئولیت
38	2-3-4-2- مصادره مالکیت معنوی
38	3-3-4-2- از دست رفتن یکپارچگی نرم‌افزار
38	5-2- قابلیت‌های امنیتی رایانش ابری
38	1-5-2- مدل اعتماد
39	2-5-2- مدیریت شناسه و دسترسی (IAM)، احراز هویت، مجوز دهی و ممیزی تراکنش
39	3-5-2- امنیت فیزیکی
40	4-5-2- امنیت واسطه‌ها
40	5-5-2- امنیت مجازی‌سازی رایانش
40	6-5-2- امنیت شبکه
41	7-5-2- جداسازی داده‌ها، حفاظت و حفاظت محرمانگی
41	1-7-5-2- جداسازی داده‌ها
41	2-7-5-2- حفاظت داده‌ها
41	3-7-5-2- حفاظت محرمانگی
42	8-5-2- هماهنگی امنیتی
42	9-5-2- امنیت عملیاتی
43	10-5-2- مدیریت حوادث
43	11-5-2- بازیابی از فجایع
44	12-5-2- ارزیابی و ممیزی امنیت سرویس
44	13-5-2- قابلیت عملکرد متقابل، قابلیت انتقال و قابلیت برگشت پذیری
45	14-5-2- امنیت زنجیره تامین

46.....	6-2- متدولوژی چارچوب.....
48	مراجع
49.....	فصل 3- معماری امنیتی رایانش ابری
49	1-3- معماری امنیتی
51	2-3- ملاحظات معماری [3].....
51	1-2-3- مشکلات عمومی
51	1-1-2-3- رعایت مقررات - انطباق.....
52	2-1-2-3- مدیریت امنیت
53	1-2-1-2-3- کنترل ها.....
53	2-2-1-2-3- اقدامات تکمیلی
54	3-1-2-3- طبقه‌بندی اطلاعات
55	1-3-1-2-3- اهداف طبقه‌بندی اطلاعات
55	2-3-1-2-3- مزایای طبقه‌بندی اطلاعات
56.....	3-3-1-2-3- مفاهیم طبقه‌بندی اطلاعات
57	4-3-1-2-3- معیارهای طبقه‌بندی
58	5-3-1-2-3- رویه‌های طبقه‌بندی اطلاعات
58	6-3-1-2-3- توزیع اطلاعات طبقه‌بندی شده
59	4-1-2-3- خاتمه کار کارمندان
60.....	5-1-2-3- آگاهی امنیتی، آموزش عملی، آموزش
61.....	1-5-1-2-3- آگاهی امنیتی
62.....	2-5-1-2-3- آموزش‌های عملی و تئوری
62.....	2-2-3- رایانش ابری مورد اعتماد
63.....	1-2-2-3- مشخصات محاسبات مورد اعتماد
66.....	3-2-3- ارتباطات و محیط‌های اجرایی امن
66.....	1-3-2-3- محیط اجرایی امن
67.....	2-3-2-3- ارتباطات امن
68.....	1-2-3-2-3- واسطه‌های برنامه‌های کاربردی (APIs)
69.....	2-2-3-2-3- شبکه‌های خصوصی مجازی
70	3-2-3-2-3- VPN‌های دسترسی از راه دور
70	4-2-3-2-3- VPN‌های شبکه به شبکه
71	5-2-3-2-3- تونل زنی VPN
72	6-2-3-2-3- زیرساخت کلید عمومی و مدیریت کلید رمزنگاری
74	7-2-3-2-3- گواهی نامه دیجیتال
75	8-2-3-2-3- دیرکتوری (فهرست) و X. 500
75	9-2-3-2-3- پروتکل دسترسی دیرکتوری سبک وزن
76.....	10-2-3-2-3- گواهی نامه‌های X. 509
78	11-2-3-2-3- لیست‌های ابطال گواهی نامه
78	12-2-3-2-3- مدیریت کلید
79	13-2-3-2-3- توزیع کلید
79	14-2-3-2-3- باطل کردن کلید

79	15-2-3-2-3- بازیابی کلید
80	16-2-3-2-3- تجدید کردن کلید
80	17-2-3-2-3- نابودی کلید
80	18-2-3-2-3- کلیدهای چندگانه
81	19-2-3-2-3- مدیریت کلید توزیع شده در مقابل متمرکز
81	20-2-3-2-3- بررسی و ملاحظات بیشتر
81	3-3- مدیریت شناسه و کنترل دسترسی
82	1-3-3- مدیریت شناسه
82	1-1-3-3- کلمات عبور
83	2-1-3-3- توکن ها
84	3-1-3-3- کارتهای حافظه
84	4-1-3-3- کارتهای هوشمند
84	5-1-3-3- بیومتریکس
86	6-1-3-3- پیاده سازی مدیریت شناسه
87	2-3-3- کنترل دسترسی
88	1-2-3-3- کنترل ها
89	2-2-3-3- مدل هایی برای کنترل دسترسی
89	1-2-2-3-3- کنترل دسترسی اجباری
89	2-2-2-3-3- کنترل دسترسی اختیاری
90	3-2-2-3-3- کنترل دسترسی غیراختیاری
90	3-2-3-3- ورود به سیستم یکباره یا احراز هویت یکباره (SSO)
91	4-3- امنیت خودکار
93	1-4-3- حفاظت خودکار
93	2-4-3- خودبهبود دهنده خودکار
94	5-3- خلاصه
94	مراجع
95	فصل 4- اصول امنیت نرم افزار رایانش ابری
96	1-4- اهداف امنیت اطلاعات ابر
97	1-1-4- محرمانگی، یکپارچگی و دسترس پذیری
98	1-1-1-4- محرمانگی
98	2-1-1-4- یکپارچگی
99	3-1-1-4- دسترس پذیری
99	2-4- خدمات امنیتی ابر
99	1-2-4- تایید هویت
99	2-2-4- مجوز دهی
100	3-2-4- ممیزی
101	4-2-4- مسئولیت پذیری
101	3-4- اصول طراحی مرتبط با امنیت ابر
102	1-3-4- کمترین امتیاز
102	2-3-4- جداسازی وظایف

102.....	3-3-4- دفاع در عمق
103.....	4-3-4- امن نسبت به خرابی
104.....	5-3-4- اقتصاد مکانیسم
104.....	6-3-4- میانگیری کامل
104.....	7-3-4- طراحی باز
105.....	8-3-4- مکانیزم کمترین اشتراک گذاری
105.....	9-3-4- پذیرش روانی
105.....	10-3-4- ضعیف ترین لینک
105.....	11-3-4- تقویت اجزاء موجود
106.....	4-4- الزامات نرم افزار آبر امن
106.....	1-4-4- شیوه های عمل توسعه امن
107.....	1-1-4-4- اداره کردن داده ها
108.....	2-1-4-4- شیوه های عمل کد نویسی
108.....	3-1-4-4- گزینه های زبان
109.....	4-1-4-4- اعتبار سنجی ورودی و تزریق محتوا
109.....	5-1-4-4- امنیت فیزیکی سیستم
110.....	2-4-4- رویکردها به مهندسی الزامات نرم افزار آبر
111.....	1-2-4-4- الزامات امنیتی نرم افزار آبر از دیدگاه منابع
112.....	2-2-4-4- الزامات امنیتی نرم افزار مبتنی بر هدف
113.....	3-2-4-4- نظارت بر الزامات داخلی و خارجی
115.....	3-4-4- پیاده سازی و تجزیه سیاست امنیتی آبر
115.....	1-3-4-4- موضوعات پیاده سازی
117.....	2-3-4-4- تجزیه موضوعات امنیتی حیاتی به الزامات نرم افزار آبر امن
117.....	1-2-3-4-4- محرمانگی
118.....	2-2-3-4-4- یکپارچگی
118.....	3-2-3-4-4- دسترس پذیری
118.....	4-2-3-4-4- تایید هویت و شناسایی
119.....	5-2-3-4-4- مجوز دهی
119.....	6-2-3-4-4- ممیزی
122.....	4-4-4- اصول امنیتی NIST33
123.....	5-4- تست نرم افزار آبر امن
123.....	1-5-4- تست برای تضمین کیفیت امنیت
125.....	1-1-5-4- تست رعایت استاندارد
126.....	2-1-5-4- تست عملکردی
128.....	3-1-5-4- آزمون کارایی
130.....	4-1-5-4- آزمون امنیتی
132.....	1-4-1-5-4- تزریق عیب
132.....	2-4-1-5-4- تزریق عیب کد منبع
133.....	3-4-1-5-4- تزریق عیب باینری
134.....	4-4-1-5-4- تجزیه و تحلیل کد پویا

135.....	5-4-1-5-4-آزمون مبتنی بر ویژگی
135.....	6-4-1-5-4-دیباگ کردن جعبه سیاه
136.....	7-4-1-5-4-آزمون تعامل پذیری
137.....	2-5-4-آزمون نفوذ به آبر
138.....	1-2-5-4-پیامدهای قانونی و اخلاقی
141.....	2-2-5-4-سه فاز قبل از تست
141.....	1-2-2-5-4-ردپا برداری
142.....	2-2-2-5-4-اسکن کردن
142.....	3-2-2-5-4-شمارش
143.....	3-2-5-4-ابزارها و تکنیک‌های تست نفوذ
144.....	1-3-2-5-4-اسکنرهای پورت
145.....	2-3-2-5-4-اسکنرهای آسیب پذیری
145.....	3-3-2-5-4-شکننده‌های کلمه عبور
146.....	4-3-2-5-4-اسب‌های تروجان
148.....	5-3-2-5-4-سر ریز بافر
149.....	6-3-2-5-4-حمله تزریق SQL
149.....	7-3-2-5-4-XSS Cross-Site Scripting
150.....	8-3-2-5-4-مهندسی اجتماعی
151.....	3-5-4-تست رگرسیون (برگشتی)
153.....	6-4-رایانش ابری و برنامه ریزی تداوم کسب‌وکار و بازیابی از فجایع
153.....	1-6-4-تعاریف
154.....	2-6-4-اصول کلی و شیوه‌های عمل
154.....	1-2-6-4-برنامه ریزی بازیابی از فجایع
156.....	1-1-2-6-4-آزمون برنامه بازیابی از فجایع
156.....	2-1-2-6-4-نقش‌های مدیریت
157.....	2-2-6-4-برنامه ریزی تداوم کسب‌وکار
158.....	1-2-2-6-4-ارزیابی اثر کسب‌وکار (BIA)
158.....	2-2-2-6-4-ارزیابی آسیب‌پذیری‌ها
159.....	3-6-4-استفاده از آبر برای BCP/DRP
160.....	1-3-6-4-افزونگی ارائه شده به‌وسیله آبر
160.....	2-3-6-4-دسترسی از راه دور امن
160.....	3-3-6-4-یکپارچه‌سازی در داخل فرآیندهای کسب‌وکار نرمال
161.....	7-4-خلاصه
161.....	مراجع
164.....	فصل 5- چالش‌های امنیتی رایانش ابری [1]
165.....	5-1-پایاده‌سازی سیاست‌های امنیتی
166.....	1-1-5-انواع سیاست‌ها
166.....	1-1-1-5-بیانیه سیاست امنیتی مدیریت ارشد
166.....	2-1-1-5-سیاست‌های تنظیم مقررات
167.....	3-1-1-5-سیاست‌های مشورتی

167.....	4-1-1-5- سیاست‌های آموزنده و آگاهی دهنده
167.....	2-1-5- تیم واکنش به حوادث امنیتی کامپیوتر (CSIRT)
168.....	2-5- مدیریت امنیت مجازی سازی
172.....	1-2-5- تهدیدات مجازی
177.....	1-1-2-5- ریسک‌های هایپرویزور
177.....	1-1-1-2-5- هایپرویزورهای خودسر
178.....	2-1-1-2-5- تعدیل یا اصلاح خارجی هایپرویزور
178.....	3-1-1-2-5- فرار یا گریز ماشین مجازی
179.....	2-1-2-5- افزایش ریسک ممانعت از سرویس
179.....	2-2-5- توصیه‌های امنیتی ماشین مجازی
180.....	1-2-2-5- تکنیک‌های امنیتی بهترین شیوه عمل
180.....	1-1-2-2-5- مستحکم‌سازی سیستم عامل میزبان
181.....	2-1-2-2-5- محدود کردن دسترسی فیزیکی به میزبان
181.....	3-1-2-2-5- استفاده از ارتباطات رمز شده
182.....	4-1-2-2-5- غیر فعال کردن فعالیت‌های پس زمینه
182.....	5-1-2-2-5- به روز کردن و وصله زنی
183.....	6-1-2-2-5- فعال‌سازی دفاع پیرامونی در ماشین مجازی
184.....	7-1-2-2-5- بررسی یکپارچگی فایل ها
184.....	8-1-2-2-5- نگهداری نسخه‌های پشتیبان
185.....	3-2-5- تکنیک‌های امنیتی مخصوص ماشین مجازی
185.....	1-3-2-5- سخت کردن ماشین مجازی
186.....	1-1-3-2-5- سخت‌سازی هایپرویزور
186.....	2-1-3-2-5- امن کردن ریشه مونیتور
186.....	3-1-3-2-5- پیاده‌سازی فقط یک عملکرد در یک ماشین مجازی
186.....	4-1-3-2-5- حفاظت پورت‌های اضافی ماشین مجازی با دیوار آتش
187.....	5-1-3-2-5- سخت‌سازی دامنه میزبان
187.....	6-1-3-2-5- استفاده از کارت شبکه (NIC) انحصاری برای ماشین‌های مجازی حساس
188.....	7-1-3-2-5- قطع نمودن دستگاه‌های استفاده نشده
188.....	2-3-2-5- امن کردن دسترسی از راه دور به ماشین مجازی
190.....	3-5- خلاصه
190.....	مراجع
192.....	فصل 6- استانداردهای امنیت ابر [4]
193.....	1-6- اطمینان از وجود حاکمیت و فرآیندهای انطباق با مقررات ریسک
193.....	1-1-6- ISO 38500 - حاکمیت IT
193.....	2-1-6- COBIT
193.....	3-1-6- ITIL (کتابخانه زیرساخت فناوری اطلاعات)
194.....	4-1-6- ISO20000
194.....	5-1-6- SSAE16
194.....	6-1-6- HIPAA
194.....	7-1-6- PCI-DSS

195.....	<i>Fed RAMP</i> -8-1-6
195.....	<i>FISM</i> -9-1-6
196.....	2-6- ممیزی فرآیندهای عملیاتی کسب و کار
197.....	3-6- مدیریت افراد، نقشها و شناسه‌ها
198.....	1-3-6- شناسه‌های فدرال
198.....	2-3-6- ورود به سیستم یکبارہ یا احراز هویت یکبارہ SSO
198.....	3-3-6- مدیریت شناسه ممتاز
199.....	(RFC 4510) LDAP -4-3-6
199.....	SAML2. 0 -5-3-6
199.....	(RFC 6749) OAuth 2. 0 -6-3-6
199.....	WS-Federation -7-3-6
199.....	OpenID Connect -8-3-6
200.....	SCIM -9-3-6
200.....	XACML -10-3-6
201.....	4-6- اطمینان از حفاظت مناسب داده‌ها و اطلاعات
202.....	5-6- اعمال سیاست‌های حریم خصوصی
203.....	6-6- ارزیابی مقررات امنیتی برای برنامه‌های کاربردی ابری
205.....	7-6- حصول اطمینان از امن بودن شبکه‌های ابری و اتصالات آن
208.....	8-6- ارزیابی کنترل‌های امنیتی در امکانات و زیرساخت فیزیکی
209.....	9-6- مدیریت شرایط امنیتی در توافقات سطح سرویس (SLA)
212.....	10-6- درک الزامات امنیتی فرآیند خروج (از ابر)
213.....	11-6- استانداردهای توصیه شده برای رایانش ابری
217.....	مراجع
218.....	فهرست کوتاه‌نوشت‌ها
224.....	واژه نامه انگلیسی به فارسی

فهرست اشکال

شکل 1-1- مدل مرجع مفهومی رایانش ابری [2].....	21
شکل 2-1- تعامل بین بازیگران رایانش ابری [2].....	22
شکل 1-3- معماری امنیتی ابر	50
شکل 2-3- معماری مرجع رایانش ابری مورد اعتماد	64
شکل 3-3- پیکربندی VPN	69
شکل 4-3- پیکربندی VPN دسترسی از راه دور	70
شکل 5-3- یک پیکربندی VPN شبکه به شبکه	71
شکل 6-3- یک تونل VPN و محموله داده آن	72
شکل 7-3- تراکنش با گواهی نامه دیجیتال	74
شکل 8-3- فرمت گواهی نامه CCITT/ISO X.509	77
شکل 9-3- فرمت لیست ابطال گواهی نامه (CRL) نسخه 2	78
شکل 1-4- اجزاء مهندسی الزامات نرم افزار [28]	110
شکل 2-4- اضافه کردن فرآیند مهندسی الزامات نرم افزار برای ارتقاء نرم افزار امن [28]	111
شکل 1-5- سلسله مراتب سیاست امنیتی	165
شکل 2-5- محیط مجازی شده نوع 1	170
شکل 3-5- محیط مجازی نوع دوم	171
شکل 4-5- آسیب پذیری عمومی سیستم ماشین مجازی	171
شکل 5-5- سرور 3i مربوط به VMware ESX	174
شکل 6-5- زیرساخت VMware	175
شکل 7-5- معماری سرور ESX	176

فهرست جداول

جدول 1-1- بازیگران رایانش ابری و تعریف آن ها [2]	22
جدول 1-2- مثالی از تجزیه و تحلیل چارچوب امنیتی برای ذخیره سازی فایل به عنوان سرویس ...	47
جدول 1-3- لیست کنترل های امنیتی [2]	50
جدول 2-3- طبقه بندی بالا، متوسط و پائین (H/M/L)	57
جدول 1-4- الزامات امنیتی داخلی و خارجی [31]	114
جدول 2-4- استانداردهای کیفیت نرم افزار ISO-9126	124
جدول 3-4- تکنیک های آزمون امنیتی مشترک	132
جدول 4-4- طبقه بندی الزامات چارچوب زمانی بازیابی	155
جدول 1-5- تعریف کدهای جدی بودن آسیب پذیری های برنامه های کاربردی سرور ESX [1]	174
جدول 1-6- لیستی از استانداردهای مهم امنیت ابر	214
جدول 2-6- خلاصه استانداردها و گواهینامه های توصیه شده امنیت ابری	214