

نشر علوم پایه

مبانی

امنیت فضای رایانه‌ای



شامل:

- مفاهیم اساسی امنیت
- رمزنگاری و نهان نگاری
- گواهی الکترونیک و زیرساخت کلید عمومی
- مفاهیم و پروتکل‌های تصدیق هویت
- مفاهیم و مدل‌های کنترل دسترسی
- فایروال
- رمز عبور

محمد جعفری

کارشناس امنیت شبکه



ISBN 964-453-23-3

مبانی امنیت فضای رایانه‌ای

محمدجعفری

زیرنظر:

مهندس مجتبی جعفری

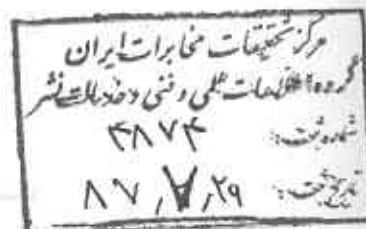
مهندس سیدهادی سجادی

مرکز تحقیقات مخابرات ایران

کتابهای فارسی



1 0 4 8 7 4 I.T.R.C.



QA
۷۶
/۹
۱۴۹۰/۷

جعفری ، محمد ، ۱۳۶۰ -

مبانی امنیت فضای رایانه ای / محمد جعفری ، زهرا جنتی جعفری ،
هادی سجادی ، تهران : علوم پایه ، ۱۳۸۴
۵۳۶ ص ، مصور .

ISBN 964-6432-15-8

فهرست نویسی براساس اطلاعات فیبا

واژه نامه .

کتابنامه .

۱. کامپیوترها -- ایمنی اطلاعات . ۲. شبکه های کامپیوتری --
- اقدامات تامینی . ۳. اینترنت -- اقدامات تامینی . ۴. کامپیوترها -- کنترل
- دستیابی . ۵. فایروال (ایمن سازی کامپیوتر) . ۶. رمزگذاری داده ها .
- الف . جعفری ، مجتبی ، گردآورنده ، ب. سجادی ، هادی ، گردآورنده .
- ج . عنوان .

۰۰۵/۸

QAY۶/۹/الف ج۷

۴۵۰۶۲ - ۸۴ م

کتابخانه علی ایران



عنوان : مبانی امنیت فضای رایانه ای

مؤلف : محمد جعفری

ناشر: علوم پایه

نوبت چاپ : اول تابستان ۸۵

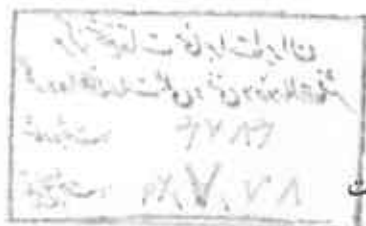
تیراژ : ۲۰۰۰ جلد

قیمت : ۵۵۰۰ تومان

آدرس الکترونیکی : info@opeco.ir

تلفن مرکز بخش : ۸۱۲۸۰۶۴۹

حقوق چاپ و نشر برای مؤلف محفوظ است



به: باقیمانده خدا در زمین...

محمد جعفری

1	کتابخانه
2	پایان نامه
3	مجموعه
4	مجموعه
5	مجموعه
6	مجموعه
7	مجموعه
8	مجموعه
9	مجموعه
10	مجموعه
11	مجموعه
12	مجموعه
13	مجموعه
14	مجموعه
15	مجموعه
16	مجموعه
17	مجموعه
18	مجموعه
19	مجموعه
20	مجموعه
21	مجموعه
22	مجموعه
23	مجموعه
24	مجموعه
25	مجموعه
26	مجموعه
27	مجموعه
28	مجموعه
29	مجموعه
30	مجموعه
31	مجموعه
32	مجموعه
33	مجموعه
34	مجموعه
35	مجموعه
36	مجموعه
37	مجموعه
38	مجموعه
39	مجموعه
40	مجموعه
41	مجموعه
42	مجموعه
43	مجموعه
44	مجموعه
45	مجموعه
46	مجموعه
47	مجموعه
48	مجموعه
49	مجموعه
50	مجموعه
51	مجموعه
52	مجموعه
53	مجموعه
54	مجموعه
55	مجموعه
56	مجموعه
57	مجموعه
58	مجموعه
59	مجموعه
60	مجموعه
61	مجموعه
62	مجموعه
63	مجموعه
64	مجموعه
65	مجموعه
66	مجموعه
67	مجموعه
68	مجموعه
69	مجموعه
70	مجموعه
71	مجموعه
72	مجموعه
73	مجموعه
74	مجموعه
75	مجموعه
76	مجموعه
77	مجموعه
78	مجموعه
79	مجموعه
80	مجموعه
81	مجموعه
82	مجموعه
83	مجموعه
84	مجموعه
85	مجموعه
86	مجموعه
87	مجموعه
88	مجموعه
89	مجموعه
90	مجموعه
91	مجموعه
92	مجموعه
93	مجموعه
94	مجموعه
95	مجموعه
96	مجموعه
97	مجموعه
98	مجموعه
99	مجموعه
100	مجموعه

فهرست

۷	فهرست
۱۱	مقدمه
۱۷	۱. مفاهیم نظری
۱۹	امنیت
۴۷	سیاست امنیتی
۵۹	صحت
۷۳	محرمانگی
۸۳	دسترسی پذیری
۹۱	قلمرو خصوصی
۱۰۱	آسیب پذیری
۱۰۷	حمله
۱۲۳	مهاجم
۱۲۹	امنیت فیزیکی
۱۳۷	رمزنگاری
۱۴۷	تاریخچه رمزنگاری
۱۵۷	رمز بلوکی
۱۶۵	رمز دنباله ای
۱۶۹	رمز متقارن
۱۷۷	پروتکل دیفی-هلمان
۱۸۱	رمز کلید عمومی
۱۸۹	پاکت نامه الکترونیک

۱۹۳	تابع درهم‌ریزی
۲۰۱	امضای الکترونیک
۲۱۱	گواهی الکترونیک
۲۱۵	زیرساخت کلید عمومی
۲۳۱	ابطال گواهی الکترونیک

۲۴۳	نهان‌نگاری
-----	------------

۲۵۱	تصدیق هویت
۲۶۱	پروتکل امنیتی
۲۷۱	پارامترهای متغیر با زمان
۲۷۹	پروتکل‌های تصدیق هویت
۲۸۹	پروتکل‌های نیدهام-شرودر

۲۹۹	حفاظت
۳۰۷	کانال پنهان
۳۱۳	کنترل دسترسی
۳۳۱	مدل‌های کنترل دسترسی
۳۳۹	کنترل دسترسی نقش-محور
۳۴۹	مدل ماتریس دسترسی
۳۵۹	مدل بل-لاپادولا
۳۶۷	مدل دیوار چین

۳۷۳	۲. مفاهیم کاربردی
-----	-------------------

۳۷۵	رمز عبور
-----	----------

۳۹۳	فایروال
۴۰۵	فیلتر بسته‌ها
۴۱۵	دروازه کاربرد
۴۲۱	فایروال شخصی
۴۲۵	تصفیه محتوا

مقدمه

سوئیچ‌های مخابراتی رفته‌رفته از شکل مکانیکی خارج شدند و جای خود را به سوئیچ‌های دیجیتال سپردند. رایانه‌ها کاربرد خود را در سوئیچ‌های مخابراتی نشان دادند و از این رهگذر، سرعت گسترش و توسعه‌ی مخابرات در جهان چندین برابر گردید. رایانه‌ها با تولید و عرضه نرم‌افزارهای پردازش صوت، هنر خود را بیش از پیش برای صنایع مخابراتی نمایان ساختند. گسترش شبکه‌های رایانه‌ای، خصوصاً ظهور اینترنت، موجب شد تا این دو فناوری هرچه بیش‌تر به هم نزدیک شوند و بالاخره پیوند خود را در قالب فناوری ارتباطات و اطلاعات به دنیا معرفی کنند.

با آغاز پردازش تصویر، رایانه‌ها پا را فراتر نهاده و در حوزه فناوری‌های صوتی-تصویری نیز گام نهاده‌اند و عرصه‌ی هنر نیز، از تاخت و تاز آن‌ها مصون نماند. هر روز خبر فتح حوزه جدیدی اعلام می‌شد؛ بهداشت و درمان، اقتصاد و تجارت، بانک‌ها و بیمه‌ها، آموزش و اطلاع‌رسانی و عمومی شدن اینترنت، زمینه را برای نفوذ بیش‌تر این فناوری‌های تازه در عرصه‌های دیگری همچون خدمات مختلف دولت به مردم و تعامل اقشار گوناگون مردم با یکدیگر فراهم ساخت.

گویی رایانه‌ها هم چون ساحری جامعه را جادو کرده و بشر را با فضای جدیدی مواجه ساخته بودند. این فضای جدید، دانشمندان را نیز به شگفتی واداشته بود؛ هر یک از منطری به آن نگریسته، یک یا چند ویژگی آن را مد نظر قرار می‌داد و نامی برای آن انتخاب می‌کرد: جامعه شبکه‌ای، جامعه نظارتی، جامعه اطلاعاتی و ...

آری، جامعه‌ای جدید شکل گرفته بود؛ باید کاری می‌کرد و برای ورود به آن آماده می‌شد. سازمان‌های جهانی به تکیه افتادند (UNESCO، WTO، ITU، WIPO و ...) و برنامه‌هایی آماده‌شد. از تجمیع برنامه‌های بخش‌های گوناگون، برنامه‌ی سازمان ملل متحد شکل گرفت و سرانجام در آذر ماه سال ۱۳۸۲ هجری شمسی (نوامبر ۲۰۰۴ میلادی) جامعه اطلاعاتی از سوی سران کشورها به رسمیت شناخته‌شد.

بدون شک، یکی از مهم‌ترین دلایل عمومیت یافتن شبکه‌های ارتباطی-رایانه‌ای، خصوصاً اینترنت، نقش آن‌ها در افزایش و تسهیل دسترسی به اطلاعات است و به خاطر این مزیت است که آحاد مختلف مردم به استفاده از آن‌ها رغبت نشان می‌دهند. از سوی دیگر، تنها دسترسی به شبکه کافی نیست؛ میزان افزایش اطلاعات کاربران رابطه مستقیمی با مقدار اطلاعات به اشتراک گذاشته در شبکه دارد و هر چه در شبکه‌ها، اطلاعات بیش‌تری ارائه شود، مطلوبیت بیش‌تری می‌یابند. اینترنت، هم دسترسی بالایی ایجاد کرده و هم میزان اطلاعات موجود در آن بالا است و به همین دلیل گسترشی جهانی پیدا کرده‌است.

قطعاً کاربرد این فناوری برای کشورها منافع بی‌شماری به ارمغان می‌آورد. میزان اثر آن بر تولید ناخالص ملی، نقش آن در افزایش آگاهی‌های عمومی، بالا رفتن سطح دانش و تولید علم و رشد کشورها برکسی پوشیده نیست. راه‌گشا بودن آن در رفع بسیاری از تنگناهای اجتماعی-اقتصادی (مثل نقش آموزش از راه دور در حل مشکل کمبود مدرسه، صرفه‌جویی‌های حاصل از حذف کاغذ در مکاتبات اداری و...) تأثیرات شگرف اجتماعی ناشی از افزایش نقش نظارتی مردم بر دولت و مدیران اجرایی بر جریان‌های اداری، تأثیر عدم نیاز به حضور فیزیکی در تعاملات گوناگون بر ترافیک و منافع اجتماعی و اقتصادی ناشی از آن و بسیاری تأثیرات دیگر، موجب آن شد که کشورها در بهره‌گیری و کاربرد بیش‌تر فناوری ارتباطات و اطلاعات گوی سبقت را از یکدیگر برابند و در این راه گام‌ها را با شتاب بیش‌تری بردارند.

این جامعه‌ی نوپا مناسبات سنتی اقتصادی، فرهنگی، سیاسی و اجتماعی، را برهم زده است؛ راه‌های تجارت را تغییر داده و شیوه‌های آموزش، درمان و... را عوض کرده‌است. مرزها را شکسته و حریم‌های امنیتی مردم و اجتماعات کوچک و بزرگ را برچیده و به داخل خانه‌ها وارد شده‌است؛ هنجارهای اجتماعی را دگرگون ساخته، باورها و ارزش‌ها را نشانه‌گرفته است. به همین دلایل، باید مقدمات ورود به این جامعه فراهم شود و آمادگی لازم کسب‌گردد. کارهای زیادی باید صورت پذیرد؛ فرصت کم است و اگر شتاب نکنیم زمان از دست می‌رود. در کنار

ایجاد زیرساخت‌های ارتباطی و اطلاعاتی، برنامه‌ریزی و تأمین نرم‌افزارهای کاربردی مورد نیاز، آمادگی‌های فرهنگی، اجتماعی و وضع قوانین و مقررات نیز از ملزومات است. میزان اطلاعات مردم هر کشور ملاکی برای میزان توسعه‌یافتگی آن محسوب می‌شود و استفاده از فناوری ارتباطات و اطلاعات، میزان اطلاعات تک‌تک مردم را به طرز چشم‌گیری افزایش می‌دهد. این افزایش آگاهی و اطلاعات عمومی، سبب رشد شاخص‌های توسعه‌ی کشورها می‌گردد، پس می‌توان چنین نتیجه‌گرفت که در بین عوامل مؤثر و دلایل تأثیر گسترش کاربرد این فناوری در توسعه‌ی کشورها، اطلاعات به‌عنوان کلیدی‌ترین عامل به‌شمار می‌رود.

اشتراک اطلاعات همان‌طور که مزایای بی‌شماری دارد، می‌تواند مبدأ ورود به حریم خصوصی و تهدید منابع و سرمایه‌های کاربران نیز باشد. باعنایت به این مطلب که کاربران شبکه‌ها لزوماً حتی از نقض حریم خصوصی باخبر نمی‌شوند، باید دقت کرد که چنین مواردی می‌تواند گسترش کاربرد فناوری ارتباطات و اطلاعات را با چالشی جدی مواجه کند و با توجه به کوتاه بودن طول زمان این فرایند، کنترل آن بسیار مشکل خواهد بود.

همان‌طور که پیش‌تر نیز اشاره‌شد، برای گسترش هرچه بیش‌تر کاربرد فناوری ارتباطات و اطلاعات در کشور، تأمین نیازمندی‌ها و ملزومات مختلفی ضروری است و در مقابل این توسعه، چالش‌ها و موانعی وجود دارد که عدم توجه کافی و صرف همت و تلاش برای رفع آن‌ها، این توسعه را با مشکلات بسیار جدی مواجه می‌سازد. در کنار موانع مرتبط با قانون و مقررات و چالش‌های جدی فرهنگی و اجتماعی، یکی از مهم‌ترین چالش‌های پیش روی گسترش استفاده از فناوری اطلاعات و ارتباطات، امنیت فضای مرتبط با آن است. در صورت تأمین سطح مطلوبی از امنیت این فضا، امکانی برای رشد و توسعه‌ی بیش‌تر این فناوری فراهم خواهد و در غیر این صورت، ناامنی به مثابه مانعی در برابر گسترش این فناوری خواهد ایستاد.

شاید بزرگ‌ترین دلیل شکل‌گیری جوامع بعد از نیاز طبیعی انسان‌ها، امنیت باشد. و قطعاً اولین چالش پس از شکل‌گیری هر جامعه - با هر اندازه و گستردگی - امنیت آن است. امنیت سرویسی است که مستقیماً مورد استفاد قرار نمی‌گیرد و لذا تنها در صورت نبود این سرویس، ضرورت آن نمایان می‌شود. امنیت در جوامع سنتی به‌عنوان امری لازم، شناخته شده و ضرورت آن برای همگان به اثبات رسیده‌است و هیچ جامعه‌ای را نمی‌توان یافت که به آن، به‌عنوان امری مهم و اجتناب‌ناپذیر نپرداخته باشد و هزینه‌های فراوانی را به آن اختصاص ندهد.

دهخدا، "امنیت" را "بی‌بیمی" معنا نموده و از این رو نقطه‌ی مقابل آن، بیم، هراس و اضطراب است. همان‌گونه که در جامعه سنتی امنیت امری لازم است و حکومت و تک‌تک اعضای جامعه، خود را در تأمین آن موظف می‌دانند، در فضای رایانه‌ای و جامعه‌ی اطلاعاتی نیز امری ضروری است و تأمین امنیت فضای تبادل اطلاعات بر عهده دولت و آحاد مختلف مردم است. هنوز ابعاد، خطرات و معضلاتی که از این ناحیه می‌تواند جامعه را تهدید کند پنهان است و هرچه حساسیت آن بیش‌تر روشن‌تر شود، تقاضای ایمن‌سازی بیش‌تر و وظیفه‌ی تأمین‌کنندگان، ملموس‌تر خواهد شد.

عمر دانش و روش‌های امنیتی در جامعه‌ی سنتی، با عمر دانش بشری مقایسه می‌شود و به‌همین دلیل بسیار طولانی است -هرچند همه افراد از آن برخوردار نباشند-؛ در حالی که دانش امنیت فضای رایانه‌ای، در عین حال که در محیط‌های نظامی سابقه‌ای نه‌چندان طولانی داشته، اما به شکل فعلی آن، بسیار نواخته و جوان است. امنیت فضای تبادل اطلاعات، به دلیل نیازهای عمومی، خیلی زود از انحصار بخش‌های نظامی خارج شد و به فضای دانشگاه‌ها و مراکز علمی و تحقیقاتی پا گذاشت. به دلیل همین نوپایی، که گسترش‌های چشم‌گیری در انتظار آن است.

در کشور ما -همچون بسیاری دیگر کشورها- کمبود آگاهی عمومی و دانش و نیروی انسانی متخصص در زمینه امنیت فضای تبادل اطلاعات به طرز چشم‌گیری خودنمایی می‌کند. برای حل این مشکل بزرگ، عزمی راسخ در سطح ملی و تلاشی گسترده و در تمامی ابعاد لازم است. گروه امنیت پژوهشکده ارتباطات و فناوری اطلاعات در راستای این وظیفه مهم، پروژه‌های گوناگونی را در این حوزه آغاز نموده‌است، که از آن جمله می‌توان به پروژه فتا (فرهنگ‌سازی و تربیت نیروی انسانی) با مسئولیت دوست عزیزم جناب آقای دکتر رسول جلیلی از اساتید محترم دانشگاه صنعتی شریف اشاره کرد. در قالب این پروژه، مرکز امنیت شبکه در هفت دانشگاه کشور در حال شکل‌گیری است. "آگاهی‌رسانی در زمینه امنیت فضای تبادل اطلاعات" عنوان پروژه دیگری است که مسئولیت آن را دوست و همکار گرامیم جناب آقای مهندس سیدهادی سجادی برعهده دارد. این پروژه در راستای آگاهی‌رسانی امنیتی، پایگاهی به نام "امن" به آدرس amn.itrc.ac.ir ایجاد نموده‌است که حاوی اطلاعات مفیدی در زمینه‌ی امنیت فضای تبادل اطلاعات می‌باشد و کتاب حاضر نیز از محصولات همین پروژه است.

مجموعه‌ای که در قالب این کتاب تقدیم علاقه‌مندان شده‌است می‌تواند مورد استفاده‌ی عمومی و دانشجویان رشته‌های مرتبط قرارگیرد. پس از معرفی عمومی امنیت در فصل اول آن، مطالبی

برای آشنایی عمومی با مفاهیم بنیادی و تئوری امنیت فضای تبادل اطلاعات ارائه شده و ضمن معرفی مبانی امنیت این فضا، تا حد مطلوبی به ابعاد نظری مفاهیم آن پرداخته است. این بخش می‌تواند برای دانشجویان رشته‌های مرتبط بسیار مفید باشد. در بخش دوم کتاب، مفاهیم کاربردی معدودی شرح داده شده که هم برای دانشجویان و هم مهندسانی که دنبال کاربردهای امنیت در فضای رایانه‌ای هستند مفید خواهد بود.

در عین حال، کتاب دارای ساختاری به صورت یک گراف معنایی است که در آن، هر مفهوم یک گره و ارتباطات بین مفاهیم، لبه‌ها را تشکیل می‌دهند. در حقیقت، مطالب این کتاب در قالب تکمیل بخشی از این گراف معنایی تنظیم شده و از این رو جای برخی مفاهیم مطرح در حوزه‌ی امنیت در آن خالی است. به هر روی، ساختار شبکه‌ی معنایی، ویژگی خاصی به آن بخشیده است که می‌تواند به عنوان جلد اول از دایره المعارف بزرگ امنیت فضای تبادل اطلاعات تلقی گردد و در آینده به سوی تکامل هرچه بیش‌تر پیش رود. ابعاد و گستردگی موضوعات، غنا و تعدد مراجع مورد استفاده، نیز از ویژگی‌های دیگر آن است.

در پایان بر خود لازم می‌دانم از دقت و کوشش آقای محمد جعفری در تحقیق و تدوین کتاب و زحمات آقای مهندس اردوان مجیدی در ارائه‌ی طرح گراف معنایی و کوشش‌های آقای مهندس سیدهادی سجادی در هدایت این پروژه‌ی مهم تشکر کنم.

مجتبی جعفری

مدیر گروه امنیت ارتباطات و فناوری اطلاعات

مرکز تحقیقات مخابرات ایران

آبان ۱۳۸۳