به نام خدا

مبانی امنیت شبکه

مؤلفین:

مهندس رضا حاتمیان

مهندس رامین مولانا پور

سرشناسه	:	حاتمیان، رضا، ۱۳۵۵ -
عنوان و نام پدیدآور	:	مبانی امنیت شبکه/ مؤلفین رضا حاتمیان، رامین مولاناپور.
مشخصات نشر	:	تهران: آتی‌نگر، ۱۳۹۱.
مشخصات ظاهری	:	۱۸۴ص.: مصور، جدول، نمودار.
شابک	:	۷۲،۰۰۰ ریال: 978-600-6004-43-3
وضعیت فهرست نویسی	:	فیپا
موضوع	:	شبکه‌های کامپیوتری -- اقدامات تامینی
موضوع		کامپیوترها — ایمنی اطلاعات
شناسه افزوده	:	مولاناپور، رامین، ۱۳۵۲ -
رده بندی کنگره	:	۱۳۹۱ ۲م۲ح/۵۹/۵۱۰۵ TK
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۲۸۷۰۳۸۸

انتشارات آتی‌نگر

عنوان: مبانی امنیت شبکه

مؤلفین: مهندس رضا حاتمیان، مهندس رامین مولاناپور

صفحه‌آرایی و طراحی جلد: همتا بیداریان

ناشر: آتی‌نگر

تیراژ: ۱۰۰۰

چاپ اول: ۱۳۹۱

قیمت: ۷۲،۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۶۰۰۴-۴۳-۳

تلفن مرکز پخش: ۶۶۵۶۵۳۳۶-۸

آدرس: تهران- خیابان جمال‌زاده جنوبی- روبه‌روی کوچه رشتچی- پلاک ۱۴۴- واحد ۲

فهرست مطالب

فصل سوم: الگوریتم‌های کلید عمومی

فصل چهارم: امضاهای دیجیتال

فصل پنجم: مدیریت کلیدهای عمومی

فصل ششم: امنیت ارتباط

فصل هفتم: پروتکل‌های احراز هویت

فصل هشتم: امنیت ایمیل

فصل نهم: امنیت وب

دشمن	هدف
دانشجو	تجسس و سرگرمی در مورد ایمیل افراد
کراکر	امتحان سیستم امنیتی افراد و سرقت داده‌ها
نماینده فروش	ادعا کردن در مورد نشان دادن تمام اروپا، نه فقط آندورا
شرکت	کشف برنامه بازاریابی استراتژیک رقیب
کارمند سابق	کینه‌جویی به خاطر اخراج شدن
حسابدار	اختلاس پول از شرکت
دلال سهام شرکت‌ها	انکار عهد و پیمان به مشتری به وسیله ایمیل
سرقت هویت	سرقت شماره‌های کارت اعتباری برای فروش
دولت	یادگیری اسرار نظامی یا صنعتی دشمن
تروریست	سرقت اسرار جنگ زیستی

شکل ۱- برخی افرادی که ممکن است مشکلات امنیتی به وجود آورند و دلیل آن.

مسائل امنیتی شبکه می‌توانند به چهار ناحیه تقریباً متداخل تقسیم شوند: محرمانگی، احراز هویت، انکارناپذیری و کنترل صحت. محرمانگی که رازداری هم گفته می‌شود، در مورد حفظ اطلاعات از دستان کاربر غیرمجاز است. این فکر معمولاً هنگامی به ذهن خطور می‌کند که درباره امنیت شبکه فکر می‌کنیم. احراز هویت در مورد تعیین فردی است که قبل از آشکار شدن اطلاعات حساس یا وارد شدن به یک معامله تجاری، با وی صحبت می‌کنید. انکارناپذیری در مورد امضاهاست. چگونه ادعا می‌کنید که مشتری شما واقعاً یک سفارش الکترونیکی داده است (مثلاً سفارشی به قیمت ۸۹ سنت را ادعا نکند که ۶۹ سنت بوده است)؟ یا ممکن است او ادعا کند که اصلاً چنین سفارشی نداده است. بالاخره، کنترل صحت در این مورد است که چگونه می‌توانید مطمئن شوید که پیام دریافتی شما واقعاً پیامی است که ارسال شده، نه پیامی که یک دشمن بدذات در حین انتقال تغییر داده است.

تمام این مسائل (محرمانگی، احراز هویت، انکارناپذیری و کنترل صحت) در سیستم‌های سنتی نیز روی می‌دهند، ولی با تفاوت‌هایی. صحت و محرمانگی با استفاده از پست الکترونیکی ثبت نام شده و قفل‌گذاری اسناد به دست می‌آید. دستبرد زدن به سلسله پست الکترونیکی مشکل‌تر از آنچه در روز Jesse James بود، است.

همچنین، افراد معمولاً می‌توانند تفاوت بین یک سند کاغذی اصل و فتوکپی را تشخیص دهند. به عنوان یک تست، یک فتوکپی از یک چک معتبر بگیرید. تلاش کنید چک اصلی را در بانک خود در روز دوشنبه نقد کنید. حال سعی کنید فتوکپی چک را در روز سه‌شنبه نقد کنید. تفاوت را در رفتار بانک مشاهده کنید. با چک‌های الکترونیکی، اصل و کپی غیرقابل تشخیص هستند. ممکن است مدتی طول بکشد تا بانک کنترل این مسأله را یاد بگیرد.

افراد، افراد دیگر را با ابزارهای مختلف شناسایی می‌کنند، از جمله تشخیص چهره، صدا و دست خط آن‌ها. تأیید امضا به وسیله امضاها روی کاغذ سربرگ، مهر برجسته و غیره کنترل می‌شود. دستکاری معمولاً می‌تواند به وسیله کارشناسان دست‌خط، جوهر و کاغذ تشخیص داده شود. هیچ یک از این گزینه‌ها، به صورت الکترونیکی وجود ندارد. بدیهی است، راه‌حل‌های دیگر مورد نیاز است.

قبل از این که به خود راه‌حل‌ها بپردازیم، صرف اندکی وقت در مورد در نظر گرفتن محلی که امنیت شبکه پشته پروتکل متعلق به آن است، ارزشمند است. حتماً هیچ مکان منفردی وجود ندارد. هر لایه دارای چیزی برای مشارکت است. در لایه فیزیکی، استراق سمع را می‌توان با پوشاندن خطوط انتقال (یا بهتر فیبرهای نوری) در لوله‌های مهر و موم شده حاوی یک گاز ساکن در فشار بالا خنثی کرد. هر تلاشی برای نفوذ به داخل تیوب، باعث آزاد شدن مقداری گاز می‌شود، فشار را کاهش می‌دهد و هشداری را به صدا در می‌آورد. برخی سیستم‌های نظامی از این تکنیک استفاده می‌کنند.

در لایه پیوند داده، بسته‌ها در یک خط نقطه به نقطه می‌توانند هنگام ترک یک ماشین رمزگشایی و در لحظه ورود به ماشین دیگر، رمزگذاری شوند. تمام این جزئیات می‌توانند در لایه پیوند داده مدیریت شوند، بدون اعتنا به آنچه که در لایه‌های بالاتر اتفاق می‌افتد. این راه‌حل هنگامی شکسته می‌شود که بسته‌ها باید چندین مسیریاب را پیمایش کنند، آن‌ها را آسیب‌پذیر رها کنند تا از درون مسیریاب مورد حمله قرار گیرد. همچنین، به برخی جلسات اجازه محافظت شدن نمی‌دهند (مثلاً، آن‌هایی که شامل خریدهای Online به وسیله کارت اعتباری هستند) و دیگران نه. با وجود این، رمزگذاری پیوند[1]، هنگامی که این متد فراخوانی می‌شود، می‌تواند به سادگی به هر شبکه‌ای اضافه شود و اغلب مفید واقع می‌شود.

1- Link Encryption

در لایه شبکه، فایروال‌ها را می‌توان نصب کرد تا بسته‌ها را به خوبی حفظ کرد و بسته‌های بد را کنار گذاشت. امنیت IP همچنین در این لایه عمل می‌کند.

در لایه انتقال، کل اتصالات می‌توانند به صورت انتها به انتها رمزگذاری شوند، یعنی، فرآیند به فرآیند. برای حداکثر امنیت، به امنیت انتها به انتها نیاز است.

بالاخره، مسائلی از قبیل احراز هویت کاربر و انکارناپذیری فقط می‌تواند در لایه کاربردی مدیریت شود.

با توجه به این که امنیت کاملاً در یک لایه منطبق نمی‌شود، در این کتاب هم منطبق نمی‌شود. به این دلیل، نیازمند بیش از یک کتاب مبانی است.

در حالی که این کتاب، فنی و الزامی است، همچنین برای این لحظه تقریباً نامرتبط است. به خوبی مستند شده است که مثلاً بیشتر ناکامی‌های امنیتی در بانک‌ها، وابسته به رویه‌های امنیتی سست و کارمندان نالایق، اشکالات بیشمار پیاده‌سازی که نفوذهای راه‌دور توسط کاربران غیرمجاز را ممکن می‌سازند و حملات معروف به مهندسی اجتماعی که مشتریان در مورد آشکار کردن جزئیات حساب خود فریب می‌خورند، هستند. تمام این مسائل امنیتی شایع‌تر از بزهکاران باهوشی که به خطوط تلفن گوش می‌دهند و سپس پیام‌های رمزگذاری شده را رمزگشایی می‌کنند، است. اگر کسی بتواند به شعبه‌ای تصادفی از یک بانک یا یک ATM برود، او به خیابانی می‌رسد و ادعا می‌کند PIN خود را فراموش کرده و یکی جدید می‌خواهد (به نام روابط خوب مشتری)، تمام روش‌های رمزنگاری در دنیا از این روش سوء استفاده، جلوگیری نخواهند کرد. در این مورد، کتاب Ross Anderson (2008a) چشم و گوش افراد را واقعاً باز می‌کند، زیرا صدها مثال از ناکامی‌های امنیتی را در صنایع بیشماری مستند کرده که تقریباً تمام آن‌ها به‌طور مؤدبانه شیوه‌های ناشیانه کسب‌وکار یا بی‌توجهی به امنیت نامیده می‌شوند. با این وجود شالوده فنی که تجارت الکترونیکی بر اساس آن ساخته شده است، و در آن تمام عوامل دیگر به خوبی انجام شده‌اند، ساخته می‌شود، رمزنگاری است.

به استثنای امنیت لایه فیزیکی، تقریباً تمام امنیت شبکه برطبق اصول رمزنگاری است. به این دلیل، با بررسی رمزنگاری با قدری جزئیات، مطالعه امنیت را شروع خواهیم کرد. برخی از اصول اولیه را بررسی می‌کنیم. برخی از الگوریتم‌ها و ساختمان داده‌های پایه مورد استفاده در رمزنگاری را بحث خواهیم کرد. سپس به‌طور مفصل بررسی می‌کنیم چگونه این مفاهیم می‌توانند برای حصول امنیت در شبکه‌ها استفاده شوند. در نهایت با برخی تفکرات جزیی در مورد فناوری و جامعه کتاب را به پایان می‌رسانیم.

قبل از شروع، یک فکر آخری هم می‌ماند: چه چیزی بیان نمی‌شود. ما تلاش داریم بر مباحث شبکه‌سازی تمرکز کنیم و نه مباحث مربوط به سیستم‌عامل و برنامه کاربردی. هر چند ترسیم این خط همواره مشکل است. مثلاً، در اینجا هیچ چیزی درباره احراز هویت کاربر با استفاده از بیومتریک، امنیت رمز عبور، حملات سرریز بافر، اسب‌های تروا، login spoofing، تزریق کد از قبیل اسکریپت‌نویسی چند سایتی، ویروس‌ها، کرم‌ها و از این قبیل نداریم. حال اجازه دهید سفر خود را شروع کنیم.