بسمه تعالی

موضوع:

امنیت شبکه های کامپیوتری

(network security)

تهیه کننده:

علی علیخانی

مرکز آموزش علمی کاربردی شهرداری

بهار ۱۴۰۱

فهرست

امنیت شبکه (network security) چیست

در حال حاضر ارتباطات و شبکه های کامپیوتری بخشی اجتناب ناپذیر از مباحث حوزه فناوری اطلاعات است. هر زمانی که شبکه و ارتباطات مطرح است **امنیت شبکه** نیز به همراه آن مطرح می شود. طبق بررسی هایی که به عمل آورده ایم مطلب کاربردی و مناسبی در این زمینه بسیار کم است و به همین جهت تصمیم گرفتیم این مقاله را بصورت کاربردی برای شما عزیزان آماده کنیم. در ابتدا باید بدانیم امنیت شبکه چیست و چگونه می توان **امنیت شبکه های کامپیوتری** را تامین کرد.
امنیت شبکه شامل سیاست ها و اقدامات اتخاذ شده جهت نظارت و جلوگیری از دسترسی های غیر مجاز، سوء استفاده و هک شدن می باشد. به عبارتی به هرگونه فعالیتی مبنی بر محافظت از استفاده و یکپارچگی شبکه و داده ها، امنیت شبکه گفته می شود.

شبکه های کامپیوتری می توانند همانند شبکه های شرکتی خصوصی باشند و یا این که به صورت عمومی باشند و در دسترس عموم قرار گیرند.

- شامل فناوری های سخت افزاری و نرم افزاری می باشد.
- تهدیدات مختلف و متنوع را هدف قرار می دهد.
- مانع از ورود و انتشار تهدیدات در شبکه می گردد.
- دسترسی به شبکه را مدیریت می کند

امنیت شبکه چیست

در حالت کلی به مجموعه اقداماتی گفته می شود که به منظور جلوگیری از بروز مشکلات امنیتی در بستر شبکه صورت میگیرد. این مجموعه اقدامات می تواند بصورت راهکارهای متعددی در غالب سرویس های سخت افزاری و نرم افزاری پیاده سازی شوند. لازم به ذکر است که معمولا بسیاری از روشهای تامین امنیت توسط رول ها (Roles)صورت می گیرد.

در بحث Network Security ، رول ها مجموعه دستورها و نقش های وظایفی هستند که در سیستم های نرم افزاری و سخت افزاری قابل تعریف هستند.

عملکرد امنیت شبکه چگونه است؟

امنیت شبکه چندین لایه دفاعی را در لبه (edge) و در داخل شبکه ترکیب می کند. هر لایه امنیت شبکه مسئول پیاده سازی کنترل ها و خط مشی ها می باشد. بنابراین کاربران مجاز امکان دسترسی به منابع شبکه را دارند، اما کاربران غیر مجاز بلاک می شوند و امکان هر گونه سوء استفاده از آن ها گرفته می شود.

خدمات امنیت شبکه

امروزه امنیت اطلاعات و داده ها، به عنوان بزرگ ترین چالش در عصر فناوری اطلاعات شمرده می شود و حفاظت از اطلاعات و شبکه ها، امری ضروری و اجتناب ناپذیر می باشد. خدمات امنیت شبکه در راستای محافظت از زیرساخت های داخلی سازمان و دستگاه های متصل در مقابل دسترسی های غیر مجاز، سوءاستفاده و حملات سایبری طراحی شده اند.

ارائه دهندگان خدمات امنیت شبکه، بررسی کاملی از ساختار شبکه و ارزیابی امنیت اینترنت و اینترانت را انجام می دهند. در مرحله بعد، از این اطلاعات به دست آمده جهت پیاده سازی فایروال یا سایر اقدامات امنیتی متناسب با نیاز مشتری استفاده می نمایند.

به طور کلی جهت ارائه خدمات امنیت شبکه می بایست، موارد زیر را در نظر گرفت:

- بررسی منابع شبکه
- بررسی تهدیدات شبکه
- نیازهای امنیتی
- ایجاد امنیت شبکه
- ایجاد امنیت برنامه های کاربردی
- ایجاد امنیت ارتباطات شبکه
- ایجاد امنیت کاربران
- ایجاد امنیت سازمانی
- تعریف سیاست های امنیتی برای شبکه مورد نظر
- تعریف استراتژی های امنیتی خاص
- مدیریت شبکه
- نظارت بر امنیت

انواع راهکارها در مباحث امنیت شبکه

موارد زیر جزو اساسی ترین مباحث و راهکارهای کنترل امنیت در انواع مقیاس ها است. البته برخی موارد در مقیاس های کوچکتر قابل حذف هستند اما اگر امنیت اهمیت بالایی دارد بهتر است بر روی تمامی موارد زیر کار شود:

Access controlبه معنی کنترل دسترسی

Antivirus and antimalware softwareبه معنی نرم افزارهای مقابله با ویروس و بدافزار

Application securityبه معنی امنیت نرم افزار

Behavioral analyticsبه معنی تحلیل عملکرد و تعیین معیارها

Data loss preventionبه معنی جلوگیری از دست رفتن اطلاعات

Email securityبه معنی امنیت ایمیل

Firewallsبه معنی دیوار آتش (نرم افزاری و سخت افزاری(

Mobile device securityبه معنی امنیت دستگاه تلفن همراه

Network segmentationبه معنی تقسیم بندی شبکه

Security information and event managementبه معنی اطلاعات امنیتی و مدیریت رویداد

VPNمخفف Virtual private network به معنی شبکه خصوصی مجازی

Web securityبه معنی امنیت وب

Wireless securityبه معنی امنیت شبکه بی سیم

کنترل دسترسی هاپ: در هر شبکه کوچک یا بزرگ، عمومی یا خصوصی بهتر است دسترسی ها کنترل و محدود شده باشند. اینکار یک قدم بسیار موثر و بزرگ در جلوگیری از بروز مشکلات امنیتی است. زیرا با اینکار دسترسی عموم به شبکه محدود شده و تنها افراد و دستگاه های مجاز می توانند به شبکه متصل شوند. تعیین محدویت برای اتصال اولیه به شبکه با مواردی مانند IP, Mac Address انجام شده و در بستر شبکه با تعیین دسترسی ها قابل انجام است. یکی از بهترین راهکارهای تکمیلی در این موضوع غیرفعالسازی سرویس ها و پورت هایی می باشد که از آنها استفاده نمی شود.

نرم افزارهای مقابله با ویروس و بدافزار: استفاده از ابزارهایی مانند آنتی ویروس و ضد بدافزار بدون شک در شبکه ضروری است. رول هایی متعددی که در بطن این ابزارها وجود دارد و همواره در حال بروزرسانی و تقویت است موجب دفع و جلوگیری از مشکلات متعدد امنیتی در سطح شبکه می شود. در برخی مواقع بدافزارها و ویروس ها بصورت پنهان وارد عمل شده و ممکن است کل موجودیت شبکه را با مشکل اساسی مواجه نماید. خوشبختانه چنین ابزارهایی به صورت راهکارهای سازمانی و شرکتی برای انواع شبکه های کامپیوتری عرضه شده و می توان از آنها بهره برد.

امنیت نرم افزار: نرم افزارها در ساختار های متعددی وجود دارند. نرم افزارهای تحت وب و نرم افزارهای کامپیوتری در ارتباط با شبکه می بایست طبق اصول امنیتی نوشته شده و مورد استفاده قرار بگیرند. معمولا مشکلات امنیتی نرم افزار بصورت باگ مشخص و راهکار مناسب برای حل آن در نظر گرفته می شود. نمی توان

ادعا کرد که امنیت یک نرم افزار مشکلی ندارد چون امنیت نرم افزار علاوه بر ساختار به عوامل متعددی مانند سرویس ها و فریم ورک ها وابسته است.

تحلیل عملکرد و تعیین معیارها: با مشخص شدن رفتارهای طبیعی و مجاز در سطح شبکه می توان معیارهای متناسب برای کنترل عملکردهای غیر طبیعی و مشکوک را تدوین کرد. پس از اینکار، مانیتورینگ شبکه بصورت مداوم ضرور است.

جلوگیری از درز و انتشار اطلاعات: این موضوع ابعاد بسیار گسترده ای دارد که با استاندارد DLP مشهور است. مبحثی که در این بخش بر روی آن می بایست تمرکز کرد Data loss prevention است. با راهکارهای موجود می بایست این اطمینان برای تیم امنیتی شبکه حاصل شود که اطلاعات محرمانه توسط افراد مجموعه یا سازمان و یا افراد دیگر به بیرون از شبکه درز نشده و امنیت اطلاعات (بخصوص اطلاعات محرمانه) تامین می شود.

امنیت ایمیل: ایمیل به عنوان یکی از روشهای ارتباطی که می تواند راه مناسبی برای نفوذ هکرها باشد می بایست بصورت مناسبی از لحاظ امنیتی پوشش داده شود. با توجه به اینکه امکان حملاتی نظیر فیشینگ، تزریق بدافزار و ویروس بر روی شبکه با ایمیل وجود دارد می بایست راهکار مناسبی جهت تشخیص و مقابله با این موضوع بکار برد.

استفاده از فایروال: یکی از موثرترین ابزارهای برای کنترل ترافیک و درخواست ها در بستر شبکه، فایروال است. این ابزار بصورت سخت افزاری و نرم افزاری و یا ترکیبی از این دو موجود است. البته می بایست توجه داشت که کارکرد مناسب فایروال ها برای بررسی صحیح درخواست ها، تعریف و تعیین رول های کاربردی و بروز است. از جمله مواردی که فایروال در برابر آنها می تواند عملکرد قابل قبولی از خود به نمایش بگذارد مسدودسازی درخواست های مغایر با قوانین و معیارهای سطح دسترسی ها و مقابله با حملات تکذیب سرویس (Dodo's)است.

امنیت دستگاه تلفن همراه: یکی از مواردی که با گذشت زمان اهمیت بیشتری پیدا کرده است دستگاه های موبایل است. به این دلیل که بیشتر پلتفرم ها بر روی گوشی های هوشمند قابل اجراست و چون موبایل یک وسیله شخصی بوده و امکان نفوذ از این طریق برای هکرها نسبت به سطح شبکه آسانتر است عوامل و تیم امنیتی شبکه می بایست راهکاری مطمئن برای جلوگیری از بروز مشکلات امنیتی را بکار بگیرند.

تقسیم بندی شبکه: این موضوع می تواند آسیب های احتمالی از مشکلات امنیتی را کنترل و یا تعدیل کند. به اینصورت که با تقسیم بندی شبکه، چنانچه یک بخش از شبکه مشکل امنیتی پیدا کرد کل شبکه تحت تاثیر آن قرار نمی گیرد.

اطلاعات امنیتی و مدیریت رویداد: سرویس ها و ابزارهایی وجود دارند که اطلاعات لازم برای شناسایی و پاسخ به تهدیدات را برای عوامل تامین امنیت شبکه های کامپیوتری فراهم می کنند. این سرویس ها و ابزارها معمولا توسط شرکتهای فعال در زمینه راهکارهای امنیتی سازمانی و شرکتی ارائه می شوند.

شبکه خصوصی مجازی: استفاده از شبکه خصوصی مجازی با ساختار امن در صورت بهره گیری از قابلیت رمزنگاری اطلاعات و تراکنشهای انجام شده در بستر شبکه می تواند راهکاری مناسب برای تامین امنیت شبکه باشد.

امنیت وب: این راهکار بصورت شناسایی وب سایت های مخرب و مسدودسازی آنها و همچنین تامین امنیت وبسایت به کار گرفته می شود. لازم به ذکر است تامین امنیت وب می بایست بصورت ویژه ای در دستور کار قرار بگیرد.

امنیت شبکه بی سیم: همانطور که می دانید شبکه های بی سیم از محافظتی مانند شبکه سیمی برخوردار نیستند. به همین جهت می بایست نهایت محدودیت و کنترل را در شبکه های بی سیم اعمال کرد.

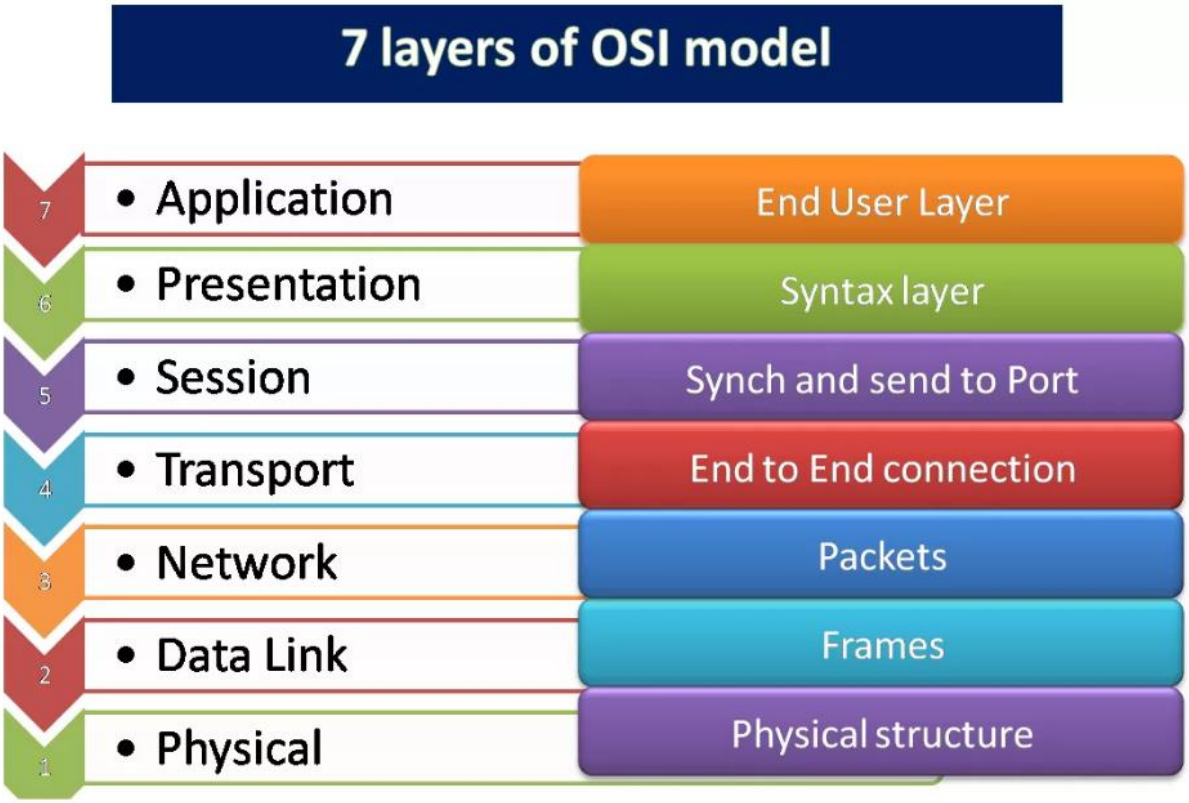
پیشنهاد می شود مطالعه نمایید : جلوگیری از هک وای فای

مفاهیم پایه در شبکه های کامپیوتری

همانطور که در ابتدا قول داده ایم قرار ایت این مقاله بصورت کاربردی مطرح شود. به همین جهت نهایت سعی بر این خواهد بود تا این مطلب بصورت ساده و کاربردی بیان شود. لازم است قبل از وارد شدن به بحث تامین امنیت شبکه، با یکسری مفاهیم و اصطلاحات آشنا شویم تا بتوانیم درک درستی از بحث داشته باشیم.

هفت لایه OSI چیست؟

در سال های اولیه وجود و استفاده از شبکه، ارسال و دریافت دیتا در شبکه سختی های خاص خود را داشت؛ بخاطر آن که شرکت های بزرگی مثلIBM ، Honeywellو Digital Equipment هرکدام استانداردهای خاص خود را برای اتصال و ارتباط کامپیوترها داشتند. این موضوع باعث میشد که فقط اپلیکیشن هایی که بر روی تجهیزات یکسانی از یک شرکت خاص وجود دارند، میتوانند با یکدیگر ارتباط داشت باشند. به همین علت سازنده ها، کاربران و استانداردها نیاز داشتند تا بر ایجاد و اجرای یک ساختار استاندارد واحد که به کامپیوترها این اجازه را بدهد تا بتوانند براحتی با یکدیگر تبادل دیتا داشته باشند. فارغ از هرگونه شرکت و برند مختلف، توافق کنند.در سال ۱۹۷۸، موسسه ISO (International Standards Organization)یک مدل شبکه بنام مدل OSI (Open System interconnection) را معرفی کرد.همانطور که گفته شد برای ارتباط دو کامپیوتر نیاز به الگویی هست که ایندو بتوانند حرف همدیگر را تحت آن الگو بفهمند. این زبان و قاعده مشترک یک استاندارد استکه تحت نام OSI معرفی شده است مجبوریم برای درک بهتر مباحث امنیت شبکه (Network Security) با مفاهیم تئوری شبکه نیز آشنا شویم. مدل OSI یکی از استانداردهای توصیف ساختار شبکه است. به اینصورت که درخواست از سمت کلاینت برای پردازش، هفت لایه را در بستر شبکه طی می کند تا پاسخ مورد نظر را دریافت کند. در ادامه همان مسیر بصورت بالعکس طی می شود تا پاسخ به کلاینت برسد. در زیر بصورت خلاصه ۷ لایه مدل OSI توضیح داده اند



لایه های بالایی نرم افزاری هستند و هرچه بیشتر بسمت لایه های پاین تر پیش برویم، به بُعد سخت افزار نزدیکتر میشویم. بطوری که لایه Physical کاملا سخت افزاری بوده و عملیاتی که در آن تعریف میشود، کاملا در حد تجهیزات سخت ازفزاریست.قانون کلی به این صورت است که در لایه بالایی اطلاعات مورد نظر جهت ارسال، قطعه قطعه شده و هر قطعه (Chunk) اطلاعاتی بصورت مجزا وارد مدل OSI خواهد شد.

در هر لایه یکسری اعمال روی هر Chunk انجام میشود و نتیجه آن عملیات در همان لایه به Chunk اضافه میگردد. به قطعاتی که در هر لایه به Chunk اضافه میگردد، هدر (Header) و Trailer فقط در لایه (Datalink)گویند. هر چیزی که در نهایت در لایه آخر به Chunk اضافه شده است، در کامپیوتر مقصد و در لایه های متناظر یک به یک از Chunk جدا خواهند شد. به عمل اضافه شدن هدر در هر لایه،

Encapsulationگویند.هر لایه با لایه های بالا و پایین خودش توسط یک interface در ارتباط است.

لایه هفتم » لایه کاربردی(Application Layer)

زمانی که بواسطه یک ابزار یا نرم افزار درخواستی را در شبکه انجام می دهیم این لایه کاربردی است که وظیفه درخواست با سرویس مورد نظر را بر عهده دارد. برای مثال اگر آدرس سایتی را در مرورگر وارد می کنیم درخواست مورد نظر که معمولا برای وب سرور و سرویس http یا https است توسط این لایه برای ارتباط درخواست انجام می شود.

معرفی پروتکل های لایه هفتم

1. HTTP (port 80)
2. FTP (port 20, 21)
3. DNS (Port 53)
4. (SNMP UDP port 162(Simple Network Management Protocol): برای مانیتورینگ و ریپورت گیری نود های مختلف شبکه
5. Telnet (Port23): Command promptبرای ریموت به دیوایس دیگر از طریق محیط
6. RDP (Port TCP//UDP 3389) (Remote Desktop Protocol)
7. SMTP (Port TCP 25) (Simple Mail Transfer Protocol) برای ارسال میل استفاده میشود
8. POP3 (Port 110) (Post Office Protocol): برای دریافت ایمیل در نرم افزارهای ایمیل
9. IMAP (port 143) (Internet Message Access Protocol): برای دریافت ایمیل در نرم افزارهای ایمیل

لایه ششم » لایه نمایشی(Presentation Layer)

این لایه وظیفه تفسیر و تعامل درخواست انجام شده در لایه کاربردی با لایه های پایین تر را دارد. به زبان ساده این لایه درخواستها را برای پردازش و اجرا در سطح شبکه آماده می کند. مواردی مانند تفسیر، رمزنگاری، فشرده سازی و نظایر آن توسطه لایه نمایشی در شبکه صورت می گیرد.

لایه پنجم » لایه نشست(Session Layer)

لایه پنجم که به لایه نشست مشهور است وظیفه ترکیب و اعلام درخواست به سرویس مورد نظر را دارد. برای مثال درخواست برقراری ارتباط با سرویس http و یا https بر عهده این لایه می باشد.

لایه چهارم » لایه انتقال(Transport Layer)

درخواست ها در بستر شبکه به انواع سرویس ها به مسیری هدایت می شوند که بصورت مجموعه درخواستهای همزمان در قالب رشته های قابل انتقال تبدیل می شوند. لایه انتقال وظیفه انتقال این رشته ها در سطح شبکه را دارد.

لایه سوم » لایه شبکه(Network Layer)

مثال قابل درکی که می توان برای لایه شبکه بکار برد این است که این لایه وظیفه ای مانند مناطق پستی مدیریت مرسولات را دارد. به اینصورت که درخواست ها را به سرویس مورد نظر رسانده و از آن تاییدیه نیز می گیرد.

لایه دوم » لایه پیوند داده(Data link Layer)

در این لایه اطلاعات هویتی دستگاه های در ارتباط با شبکه به منظور تعیین مقصد پاسخ درخواست مورد استفاده قرار گرفته و پس از وارد شدن به لایه اول به کلاینت تصدیق شده، در مسیر بالعکس درخواست بازگشت داده می شود.

لایه اول » لایه فیزیکی(Physical Layer)

در این لایه نوع اتصال و روش برقراری ارتباط مطرح است. همانطور که می دانید سخت افزارهای مختلف بر اساس نوع عملکرد و ساختار آن دارای مدلهای ارتباطی متفاوتی هستند. در این لایه ارتباط بین سخت افزار و نرم افزار برقرار می شود.

عوامل زیادی همچون نویز، تداخل خطوط و غیره وجود دارند که می‌توانند باعث از بین رفتن داده‌ها در طی انتقال شوند. لایه‌های بالاتر در نمایی تعمیم یافته از معماری **شبکه** قرار دارند و از روش پردازش داده‌ها روی شبکه واقعی اطلاع ندارند. از این رو لایه‌های فوقانی انتظار یک انتقال عاری از خطا بین سیستم‌ها را دارند. اغلب اپلیکیشن‌ها در صورت وجود داده‌های خطادار مطابق انتظار رفتار نخواهند کرد. با این وجود، کاربردهایی مانند انتقال صوت و تصویر ممکن است تا این حد متأثر از خطاها نباشند و در صورت وجود پاره‌ای خطاها، همچنان به درستی کار کنند.

لایه داده-لینک از نوعی مکانیسم کنترل خطا استفاده می‌کند تا اطمینان یابد که قاب‌ها (Frames) (جریان‌های بیتی داده) با سطح معینی از دقت انتقال می‌یابند. اما برای درک چگونگی کنترل خطا می‌بایست با انواع خطاهایی که ممکن است پیش بیایند آشنا باشیم.

انواع خطا ها در شبکه های کامپیوتری:

سه نوع خطا ممکن است در شبکه‌های کامپیوتری رخ دهد:

خطای یک بیت منفرد

در یک قاب، تنها یک بیت وجود دارد که به نوعی از بین رفته است.

فریم در حالی دریافت می‌شود که بیش از یک بیت از بین رفته است .

خطای گسترده

فریم شامل چندین بیت متوالی از داده‌های از بین رفته است.

شناسایی خطا

خطاها در فریم‌های دریافتی به وسیله «بررسی توازن (Parity Check) و بررسی افزونگی چرخه ای Cyclic Redundancy)شناسایی می‌شوند. در هر دو حالت، چند بیت اضافی همراه با داده‌های واقعی ارسال می‌شوند تا تأیید شود که بیت‌های دریافتی در سمت دیگر همان‌هایی هستند که ارسال شده‌اند. اگر بررسی متقابل در سمت گیرنده با شکست مواجه شود، بیت‌ها به صورت از بین رفته تلقی می‌شوند.

بررسی توازن

یک بیت اضافی همراه با بیت‌های اصلی ارسال می‌شود تا در صورتی که توازن زوج وجود دارد، تعداد ۱-ها زوج شود و یا در صورت وجود توازن فرد، تعداد ۱-ها فرد شود.

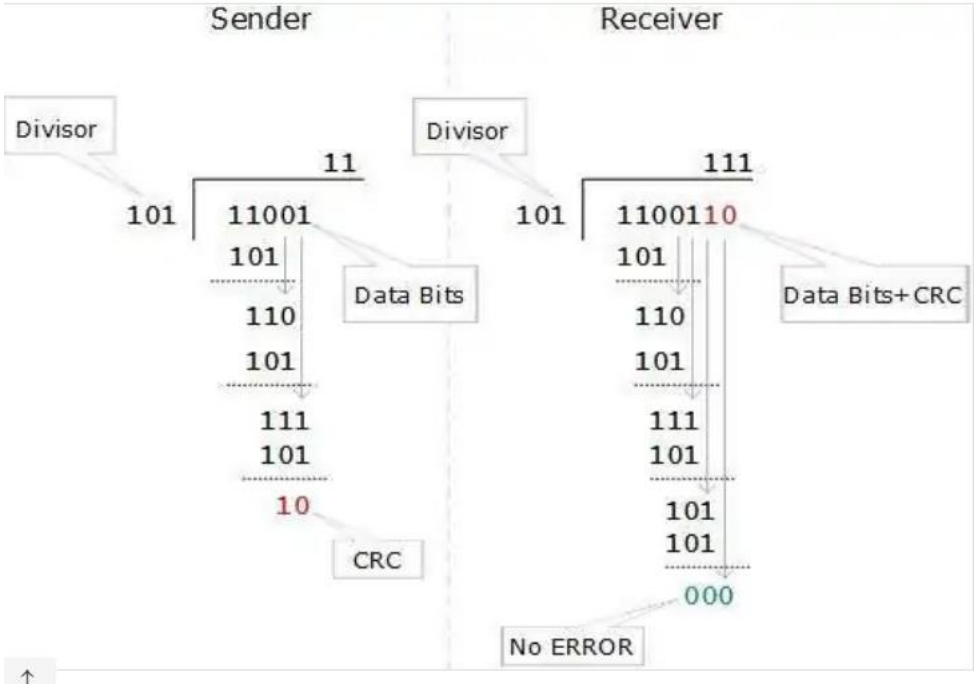
در این روش فرستنده در زمان ایجاد یک فریم تعداد ۱-های داخل آن را می‌شمارد. برای نمونه اگر از توازن زوج استفاده شود و تعداد ۱-ها زوج باشد، یک بیت با مقدار ۰ اضافه می‌شود. بدین ترتیب تعداد ۱-ها زوج باقی می‌ماند. اگر تعداد ۱-ها فرد باشد، برای این که زوج شود، یک مقدار ۱ دیگر اضافه می‌شود.

در این روش، سمت گیرنده تعداد ۱-ها در فریم را می‌شمارد. گر تعداد ۱-ها زوج باشد و توازن زوج برقرار باشد، قاب به صورت سالم تصور می‌شود و مورد پذیرش قرار می‌گیرد. اگر تعداد ۱-ها فرد باشد و توازن فرد برقرار باشد، همچنان فریم سالم محسوب می‌شود.

اگر در زمان انتقال، تنها یک بیت معکوس شده باشد، گیرنده می‌تواند با شماره تعداد ۱-ها این وضعیت را تشخیص دهد. اما زمانی که بیش از یک بیت دارای خطا باشد، در این صورت شناسایی خطا برای گیرنده دشوار خواهد بود.

(CRC) بررسی افزونگی چرخه‌ای

CRCرویکردی متفاوت برای شناسایی سالم بودن داده‌های دریافتی است. این تکنیک شامل تقسیم باینری بیت‌های داده ارسالی است. مقسوم با استفاده از معادله‌های چندجمله‌ای تشکیل می‌شود. در این روش فرستنده عملیات تقسیم را روی بیت‌هایی که قرار است ارسال شوند، انجام داده و باقی‌مانده را محاسبه می‌کند. پیش از ارسال کردن بیت‌های واقعی، فرستنده باقی‌مانده را به انتهای بیت‌های واقعی اضافه می‌کند. بیت‌های داده واقعی به علاوه باقیمانده به نام «کلمه رمز « (Codeword) شناخته می‌شوند. فرستنده بیت‌های داده را به صوت کلمه رمز ارسال می‌کند.



در سمت دیگر، گیرنده عملیات تقسیم را با استفاده از همان مقسوم روی کلمه رمز اجرا می‌کند. اگر باقیمانده کلاً برابر با بیت‌های صفر باشد، داده‌های دریافتی مورد پذیرش قرار می‌گیرند؛ در غیر این صورت داده‌های دریافتی به صورت نوعی داده از بین رفته در زمان انتقال محسوب می‌شوند.

اصلاح خطا

در دنیای دیجیتال، اصلاح خطا به دو روش صورت می‌گیرد:

اصلاح خطای رو به عقب

هنگامی که گیرنده خطایی را در داده‌های دریافتی تشخیص دهد، از فرستنده تقاضا می‌کند که داده‌ها را یک بار دیگر ارسال کند.

اصلاح خطای رو به جلو

زمانی که گیرنده نوعی خطا را در داده‌های دریافتی شناسایی کند، کد اصلاح خطایی را اجرا می‌کند که به بازیابی خودکار و اصلاح برخی از انواع خطا کمک می‌کند.

روش اول که اصلاح خطای رو به عقب نام دارد، آسان است و تنها در مواردی به صورت مؤثر قابل اجرا است که ارسال مجدد داده‌ها مستلزم هزینه بالایی نباشد. برای نمونه فیبر نوری چنین است. اما در مورد روش انتقال بی‌سیم، ارسال مجدد ممکن است هزینه بالایی داشته باشد. در این موارد اخیر، از روش اصلاح رو به جلو استفاده می‌شود.

برای اصلاح خطا در فریم داده‌ها، گیرنده باید دقیقاً بداند که کدام بیت در فریم از بین رفته است. برای موقعیت‌یابی خطا، بیت‌های تکراری به عنوان بیت توازن برای شناسایی خطا مورد استفاده قرار می گیرد.برای نمونه «کلمه» یا ۷ بیت داده را در قالب اسکی دریافت می کنیم سپس می‌توانیم ۸ نوع اطلاعات مورد نیاز خود

را داشته باشیم که ۷ بیت به ما می‌گویند کدام بیت خطا دارد و یک بیت دیگر به ما اعلام می‌کند که خطایی وجود ندارد.

منابع و ماخذ:

۱- کتاب آموزش شبکه و امنیت شبکه و روش پیاده‌سازی استاندارد امنیت اطلاعات نوشته مرتضی معتمدی فر بخش آموزش شبکه
۲- مبانی امنیت اطلاعات و شبکه +SECURITY نوشته احسان امجدی بیگوند
۳- رمزنگاری و امنیت شبکه نوشته بهروز فروزان
۴- مقدمه ای بر امنیت شبکه مهدی حسنی
۵- اینترنت