سرویس امنیتی (security service): به سرویس‌هایی گفته می‌شود که امنیت در یک سیستم یا شبکه، سرویس‌های امنیتی اطلاق می‌شود. به طور معمول یک سرویس امنیتی از یک یا چند مکانیزم امنیتی بهره می‌گیرد.

در ادامه نمونه‌هایی از سرویس‌های امنیتی ذکر شده است:

۱- حفظ صحت داده‌ها (Integrity)،
۲- حفظ محرمانگی داده‌ها (Confidentiality)،
۳- احراز اصالت (Authentication)،
۴- کنترل دسترسی (Access control)،
۵- عدم انکار (Non-repudiation)،
۶- دسترس‌پذیری (Availability).

(۱۲) انواع حملات از نظر میزان تأثیر رایی توان در دو رده کلی زیر دسته‌بندی کرد:

۱- حملات فعال (Active attack): به حملاتی اطلاق می‌شود که در آن سعی می‌شود منابع سیستم تغییر کند یا بر عملیات آن تأثیر بگذارد. این دسته از حملات به طور معمول جزء حملات قابل تشخیص دسته‌بندی می‌شوند. برخی از حملات مطرح در این دسته عبارتند از:

- حمله جعل هویت (Masquerade)،
- حمله ارسال دوباره پیام (Replay)،
- حمله تغییر (Modification)،
- حمله منع سرویس (Denial of service).

۲- حملات غیر فعال (Passive attack): به حملاتی اطلاق می‌شود که در آن تلاش می‌شود اطلاعات کسب شود، اما تأثیری روی منابع سیستم و عملکرد آن ندارد. حملات مطرح در این دسته عبارتند از:

- حمله تحلیل ترافیک (Traffic Analysis)

- حمله انتشار پیام (Release of message)

حملات غیرفعال جزو حملات غیرقابل تشخیص رده بندی می شوند زیرا که در روال عادی تغییری ایجاد نمی شود.

(۱۳) حمله جعل هویت (Masquerade attack):

زمانی اتفاق می افتد که یک موجودیت (شخص/ماشین) طوری وانمود کند که موجودیت دیگری می باشد. اگر رویه احراز هویت (Authorization Procedure) در یک سامانه به درستی محافظت نشود، می تواند به طور بالقوه در معرض حمله جعل هویت قرار گیرد.

هدف چنین حملاتی نقض محرمانگی است. نتیجه چنین حملاتی می تواند جعل یا اضافه کردن پیام ها و داده های درسامانه باشد که سوءاستفاده در سامانه یا تخریب داده امکان

را فراهم کند.

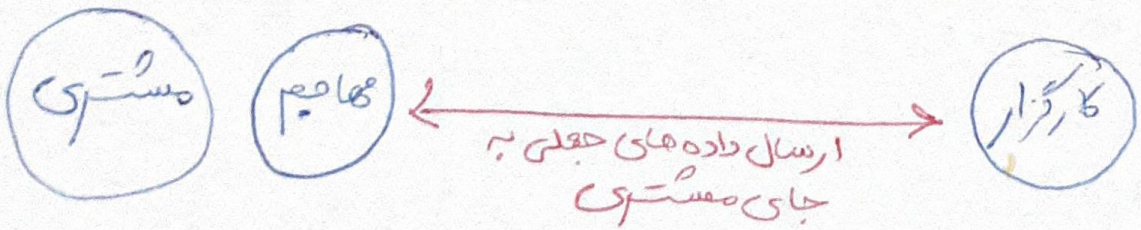
راه های تحقق چنین حمله ای در سامانه عبارت است از:

۱- احتمال فیزیکی به شبکه و دریافت بسته ها

۲- بازارسال بسته های شنود شده پس از اعمال تغییرات مورد نیاز (ارسال بسته های جعلی)

۳- وجود ضعف در مکانیزم احراز هویت و کنترل محرمانگی.

شکل زیر تمایز بین حمله جعل هویت مشتری یا کاربر را نشان می دهد.



در مثال بالا، مهاجم می تواند به جای کارگزار نشسته و با مشتری به تعامل بپردازد.

(۱۴) حمله تکرار (Replay attack):

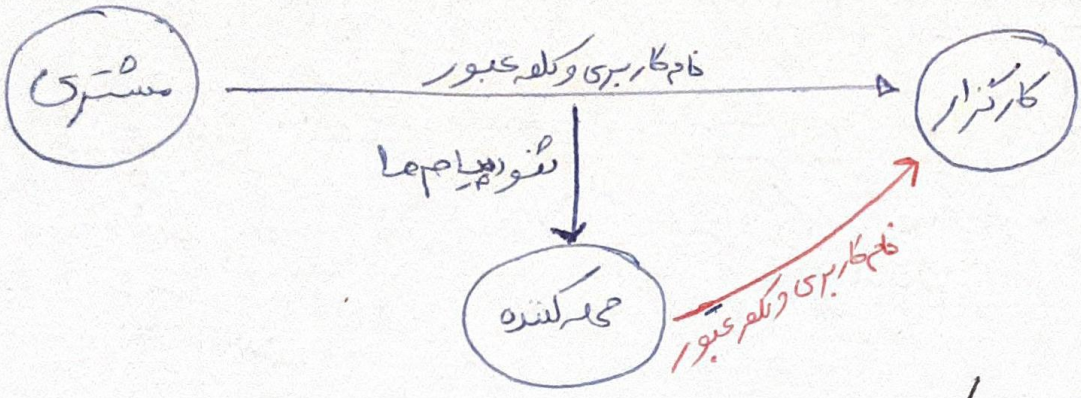
حمله ای است که در آن یک انتقال داده معتبر یا انگیزه بدخواهانه تکرار می شود.

در این نوع حمله، مهاجم داده های در حال انتقال را رهگیری و پس از بدست آوردن

اطلاعات مهم [redacted] آنها را دوباره ارسال

می کند.

شکل زیر یک نمونه از حمله تکرار را به تصویر می کشد.



(۱۵) حمله تغییر یا دستکاری داده (Modification attack):

حمله ای است که با هدف نقض صحت داده ها سامانه صورت می گیرد و منجر به

تغییر غیر مجاز داده ها در سامانه می شود.

برخی راه های تحقق چنین حملاتی عبارتند از:

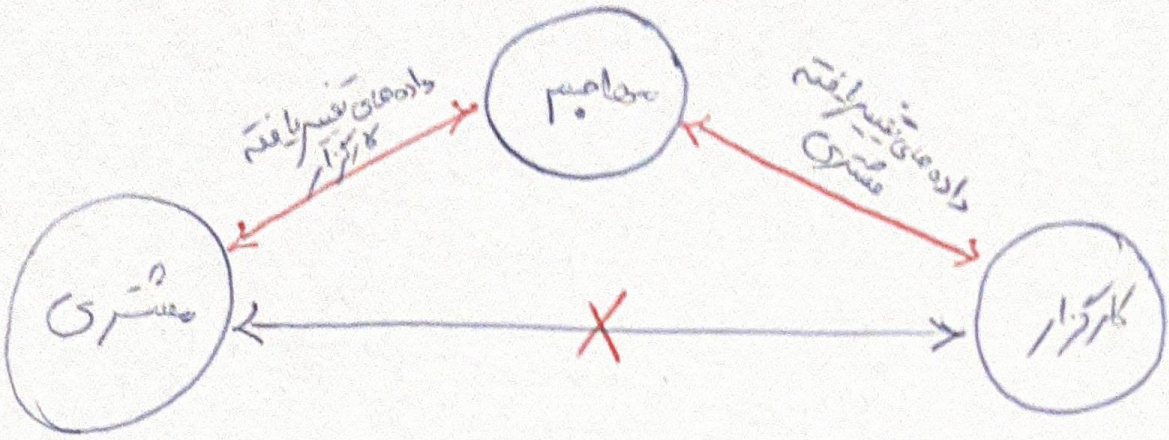
۱- قرار گرفتن در مسیر شبکه و دستکاری و ارسال پیام به گیرنده،

۲- دسترسی غیر مجاز به پایگاه داده و تغییر غیر مجاز در آن،

۳- وجود ضعف و آسیب پذیری در سیستم کنترل دسترسی و صحت سامانه هدف.

شکل زیر حمله تغییر یا دستکاری داده را که حمله مرد میانی (Man in the Middle) نامیده

می شود به تصویر می کشد.

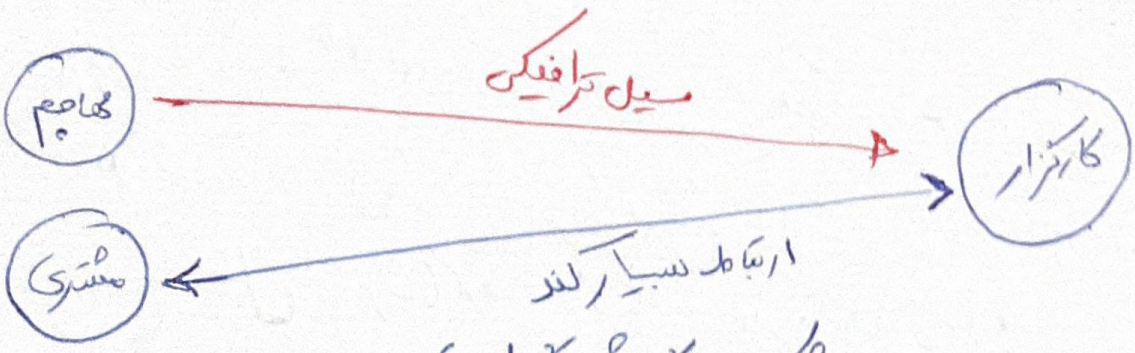


(۱۶) حمله منع سرویس (Deniale of Sewice):

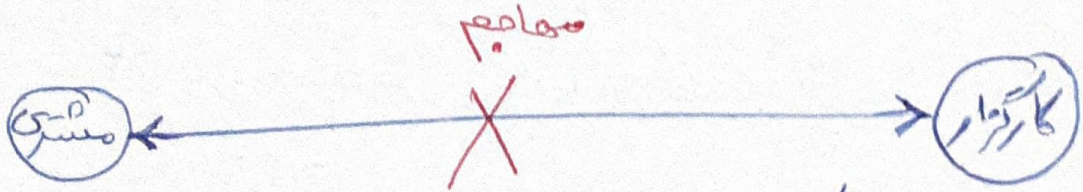
حمله‌ای است که با هدف نقض دسترس پذیری سامانه صورت می‌گیرد و منجر به کاهش کارایی و یا عدم امکان دسترسی کاربران به سامانه می‌شود.

راه اندازی سیل ترافیکی و استفاده از ضعف‌ها و آسیب پذیری‌های سامانه، یکی از مهم‌ترین راه‌های تحقق چنین حملاتی به شمار می‌آید.

اشکال زیر نتایج حاصل از چنین حمله‌ای را به صورت مصورسازی می‌دهد.



شکل - (کاهش کارایی)



شکل - (عدم امکان دسترسی کاربران)

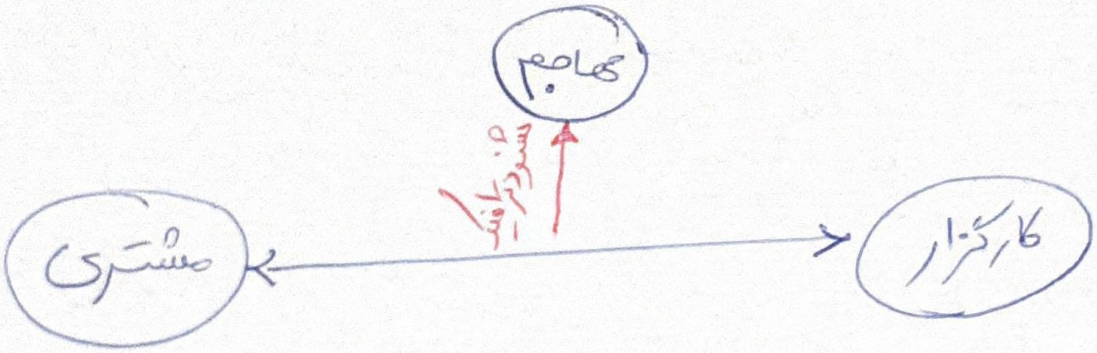
(۱۷) حملات غیرفعال از طریق شنود یا استراق سمع با هدف نقض محرمانگی سامانه و در نتیجه دسترسی غیرمجاز به داده‌های طبقه‌بندی شده صورت می‌گیرد. راه‌های تحقق چنین حملاتی می‌تواند موارد زیر باشد:

۱ انتقال غیرقانونی به شبکه و دریافت بسته‌ها،

۲ دسترسی غیرمجاز به پایگاه داده،

۳ وجود ضعف و آسیب‌پذیری در سیستم کنترل دسترسی،

شکل زیر بیانگر چنین حمله‌ای را نشان می‌دهد.



(۱۸) در سناریو حمل هر ارتباط امن، دو نیاز امنی زیر به طور کلی وجود دارد:

① نیاز به انتقال یک پیام بین طرفین با استفاده از یک کانال ناامن (مثل اینترنت) که به عنوان مسأله ارتباط امن (یا Secure Communication Problem) شناخته می‌شود.

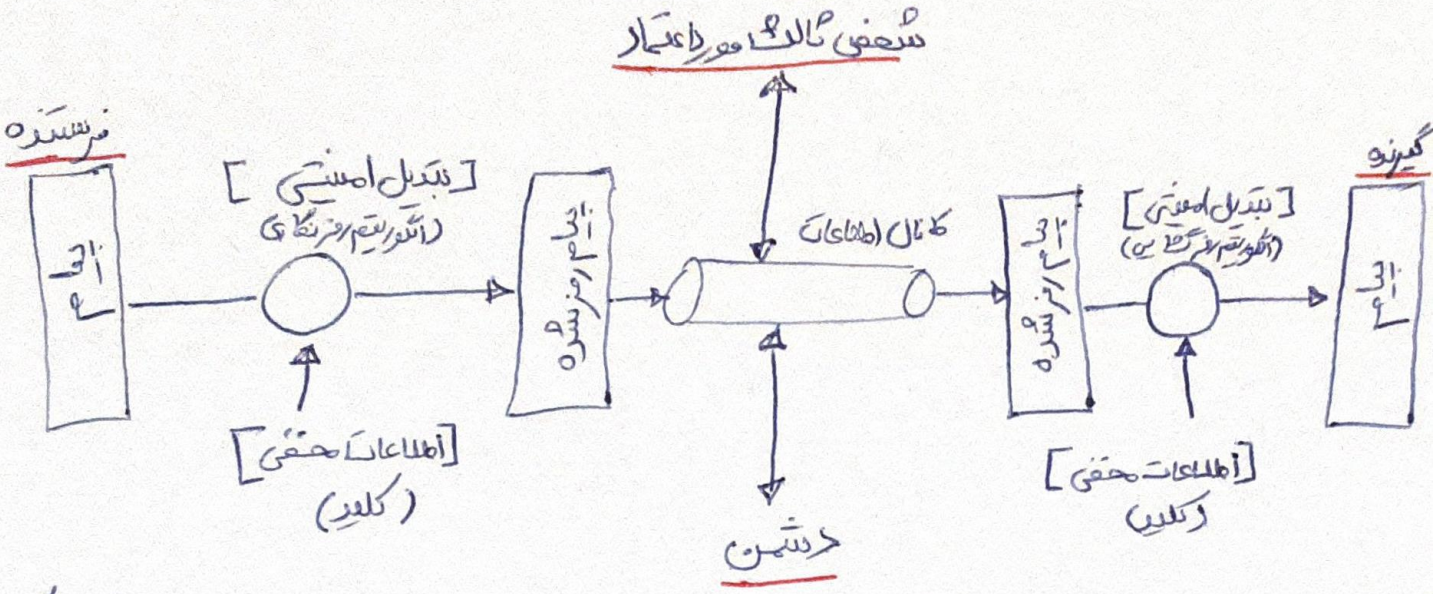
② نیاز به تأمین سرویس‌های امنیتی نظیر محرمانگی، صحت، احراز اصالت و موارد مشابه.

(۱۹) تکنیک‌های مورد استفاده برای ارتباط امن به طور کلی شامل دو مؤلفه زیر هستند:

① تبدیل امنیتی: جهت فراهم آوردن سرویس‌های امنیتی مورد نیاز است، (Security Conversion)

(۲) اطلاعات محفی: در تبدیلات امنیتی مورد استفاده قرار می‌گیرد و به نحوی بین طرفین ارتباط به اشتراک گذاشته شده است. Secret information

(۲۰) شکل زیر یک مدل تعمیم برای ارتباط امن را نشان می‌دهد.



شکل فوق بیانگر آن است که برای فراهم کردن یک سرویس امنیتی به منظور داشتن یک ارتباط امن، می‌بایست نیازهای زیر را فراهم کنیم:

۱. طراحی الگوریتم مناسب برای انجام تبدیل امنیتی مورد نظر،

۲. تولید اطلاعات محفی (کلید) مورد نیاز طرفین،

۳. استفاده از روش مناسب برای توزیع و توافق درباره اطلاعات محفی (کلید)،

۴. طراحی پروتکل مناسب برای ارتباط طرفین و تضمین سرویس امنیتی.