امنیت ارتباطات

معرفی تهدیدات وسرویسهای امنیتی

بسم الله الرحمان الرحیم

وفوق کل ذی علم علیم

فوق هر دانشمندی دانشمندتری وجود دارد.

(سوره یوسف)

مقدمه

یکی ازچالشهای مهم عصر اطلاعات

تامین امنیت مطلوب در تبادل اطلاعات با حداقل هزینه ها

تامین امنیت بدون داشتن

تعریف صریح وروشن از آن غیر ممکن است

امنیت را در مقابل تهدید مطرح می شود.

سیستمی امن است که حداقل در مقابل تهدیدات شناخته شده مصون باشد.

فرض کنید دوفرد A,B قصد دارند به تبادل امن پیام بپردازند.

مثال : شبکه اینترنت،تلفن شهری

چه تهدیداتي وجود دارد؟

اطلاعات دیجیتال

اطلاعات آنالوگ

امنیت ؟

امنیت يك مفهوم كلي است به راحتي نمي‌توان آن را تعريف كرد.

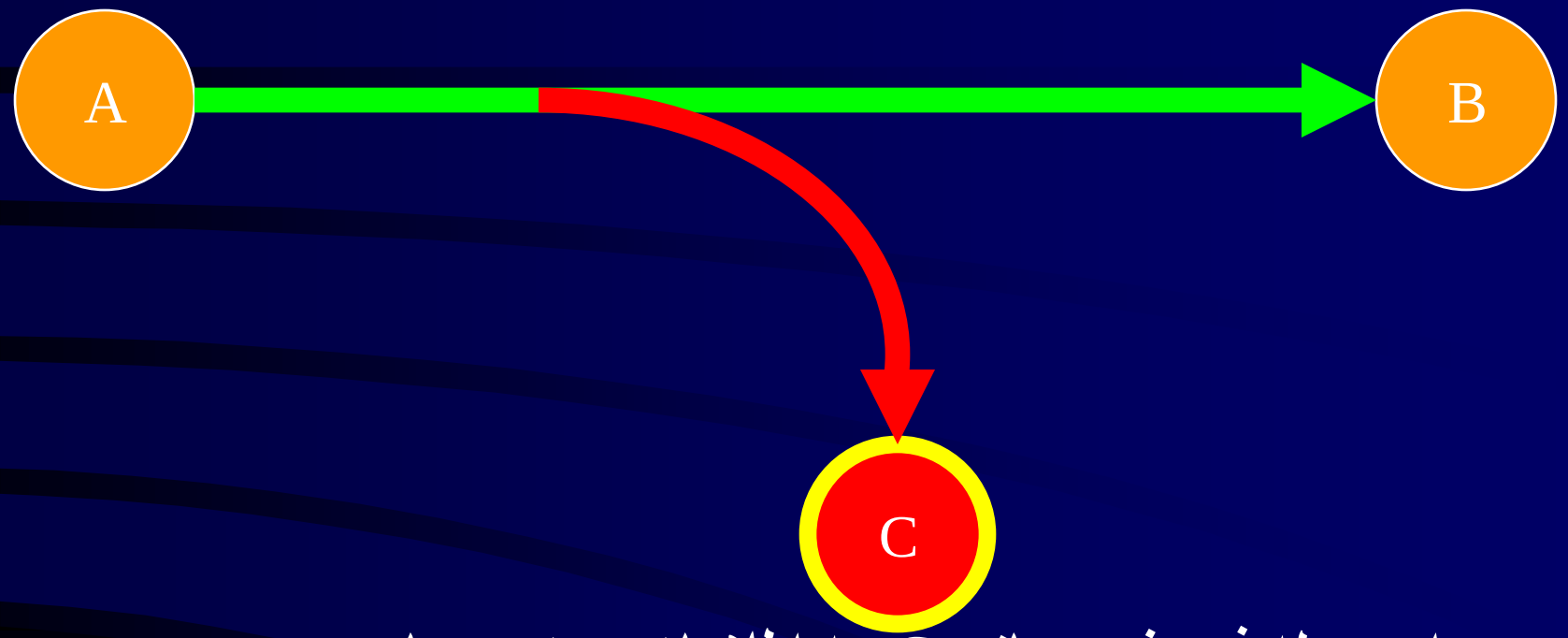
امنیت را درمقابل تهدید مطرح مي كنيم.

تهدید ؟

امنیت نقض شده

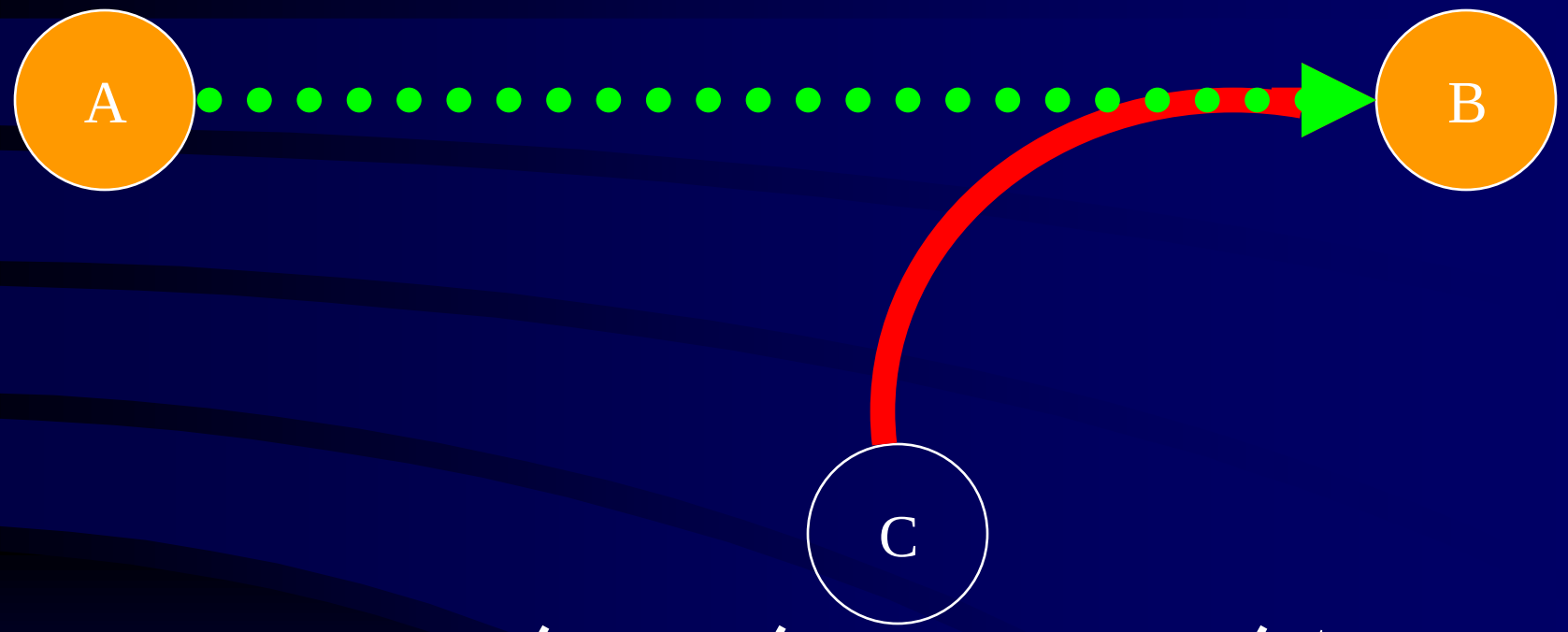
انواع تهدیدات امنیتی قابل تصور

Interception شنود



- در اين حمله فرد غير مجاز C به اطلاعات دست مي يابد.
- مثال : نصب استراق سمع كننده نرم افزاري كه اطلاعات را از طريق شبكه ارسال مي كند.
- اين حمله جزء حملات غير فعال مي باشد و حمله كننده رد پايي از خود بجا نمي‌گذارد وبه همين دليل شناسايي آن مشكل است پس بايد تا حد ممكن از وقوع آن جلو گيري كرد.دراين حمله محرمانگي پيام نقض مي شود.

Fabrication جعل پيام

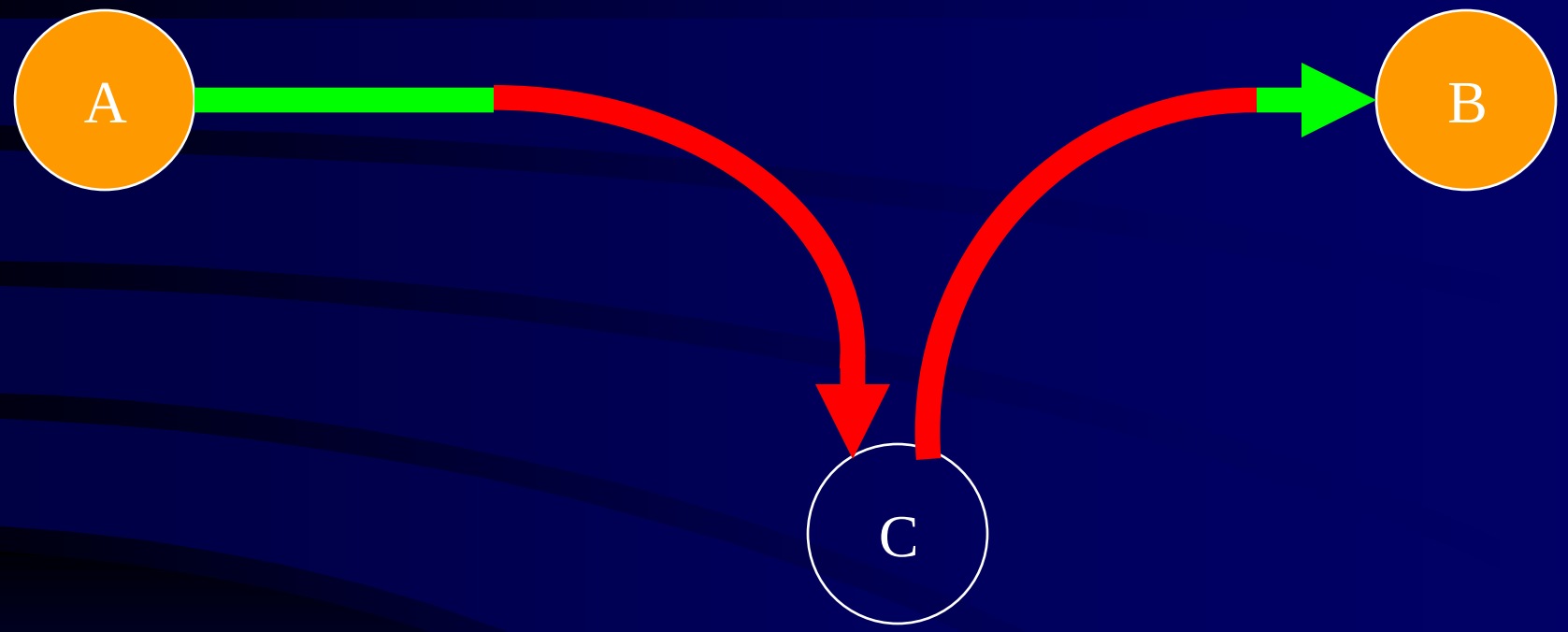


- در اين حمله فرد C خود را بجاي فرد A معرفي مي كند.
- مثال : C امضاي A را جعل مي كند

اين حمله جزء حملا ت فعال مي باشد وجلوگيري از آن مشكل است به همين دليل بايدتا حد امكان به شناسايي آن پرداخت .

دراين حالت اصالت مبدا پيام نقض مي شود.

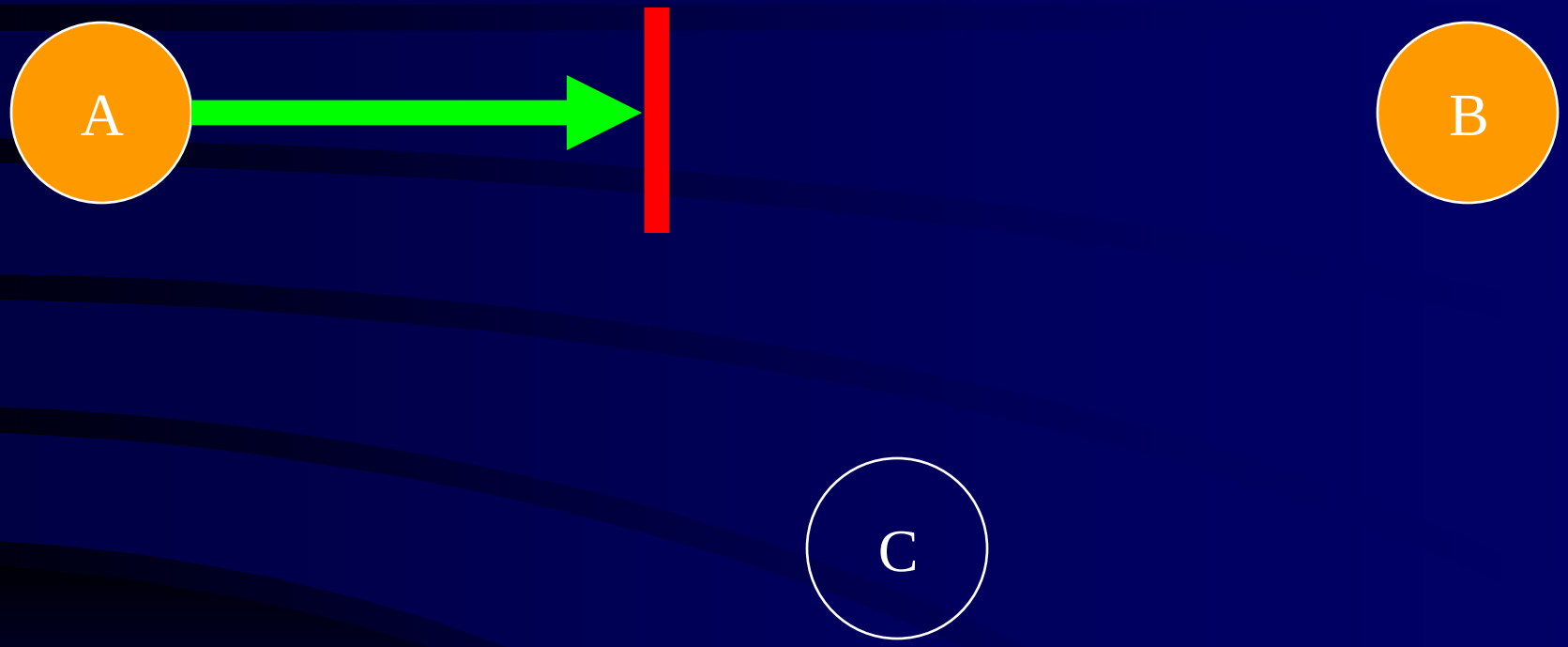
Modification دستكاري پيام



- اين حمله نيز جزء حملا ت فعال مي باشد .دراين حمله صحت پيام يا به عبارتي ديگر تماميت آن نقض مي شود.

- مثال افزودن ركوردي به پيام.

جلو گيري از ارسال Interruption



- اين حمله جزء حملا ت فعال مي باشد.
- مثال ارسال پيام هاي زياد واشباع پهناي باند B

توضيح

تهديد ديگري را كه مي توان مطرح كرد ودر واقع شايد - نتوان آن راتهديد محسوب كرد ولي مي‌تواند مقدمه حملات باشد حمله شناسايي مى باشد

- در اين حمله ترافيک شبكه شنود مي شود واطلاعاتي مانند توپولوژي شبكه ،تعداد وزمان ارسال ودريافت ها نوع سيستم عامل و . . . بدست مي يايد ومي تواند به عنوان مقدمه براي ساير حملات بكار برود.

سرویسهای امنیتی

۱- محرمانگی Confidentiality

۲- تصدیق اصالت مبدا Authentication

۳- صحت Integrity

۴- عدم انکار Nonrepudiation

5- کنترل دستیابی Access Control

6- قابلیت دسترسی Availability

سرویسهای امنیتی

۱- محرمانگی Confidentiality

این سرویس به مااین اطمینان را می دهد که اطلاعات فقط توسط فرد مجاز دریافت می شود.

محتویات پیام را از دسترسی افراد غیر مجاز حفظ می کند.

سرویسهای امنیتی

۲- تصدیق اصالت مبدا Authentication

این سرویس به ما این امکان را می دهد که مبداپیام درست تشخیص داده شود.

سرویسهای امنیتی

۳- صحت Integrity

این سرویس به ما این امکان را بوجود میآورد
که مطمئن شویم که پیام تغییر نمی یابد

سرویسهای امنیتی

۴- عدم انکار Nonrepudiation

این سرویس به ما این امکان را بوجود میآورد
که فرستنده وگیرنده نتوانند ارسال ودریافت پیام را انکار کنند.

سرویسهای امنیتی

5- کنترل دستیابی Access Control

این سرویس به ما این امکان را بوجود میآورد
دسترسی به پیام بصورت کنترل شده باشد وهرکسی نتواند به هر اطلاعاتی دست یابد.

سرویسهای امنیتی

6- قابایت دسترسی Availability

این سرویس به ما این امکان را بوجود میآورد
منابع اطلاعاتی در صورت لزوم قابل دسترسی باشند.