امنیت فضای مجازی و دفاع الکترونیکی

جلسه پنجاه و سه

فصل سوم: احکام امنیت فضای مجازی

۹۶/۱۲/۱۰

- امنیت
- امنیت فضای مجازی
- تهدیدهای امنیت ملی

اول: جنگ

۱- جنگ الکترونیکی

۲- جنگ سایبری

۳- جنگ نرم

دوم: تروریسم

سوم: جاسوسی

جـنگ سایبری:چهار نوع کاربرد را در جنگ سایبری از هم تفکیک می‌کنیم:

❑ اول: جنگ واقعی + سامانه‌های سایبری به عنوان تسلیحات جنگی

- ❑ رباتهای هوشمند برای حمله به اهداف تعیین شده،
- ❑ موشکهای هوشمند،
- ❑ بمبهای نصب شده بر روی پهبادها،
- ❑ پهبادهای مسلح

(کرار ایرانی، ماشین درو MQ-9 امریکایی)

- ❑ هواپیماها و تانکهای دارای ابزارهای اطلاعاتی نقطه زن
- ❑ و ...

۲- جـنگ سایبری:

- دوم: استفاده از سامانه سایبری برای یک تخریب فیزیکی مثل زیرساختهای حیاتی- بدون جنگ واقعی

- اما آنچه واقعاً رخ می‌دهد تهدید علیه امنیت ملی به صورت حمله سرزمینی نیست بلکه تهدید تخریبی علیه زیرساختهای حیاتی یک کشور مثل شبکه برق یا سایت انرژی هسته‌ای یک کشور است.

- راهبردهای قابل توجه در این نوع جنگ سایبری:
  - جلوگیری از حملات علیه زیرساختهای حیاتی
  - کاهش آسیب‌پذیری ملی در برابر حملات سایبری
  - کاهش آسیب‌ها و زمان ترمیم حملات سایبری

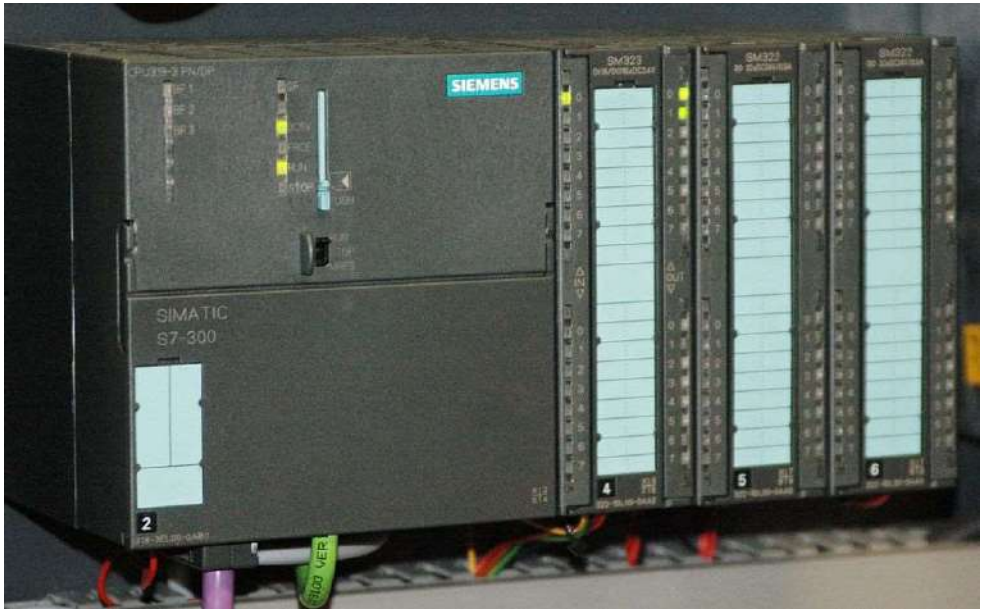
- مرور یک نمونه عینی: ویروس استاکس‌نت

نمونه عینی: ویروس استاکس‌نت: نحوه کارکرد

- استاکس‌نت طوری طراحی شده بود که از طریق یک پورت USB وارد رایانه‌های شخصی شده و طوری برنامه ریزی شده که از طریق شبکه به نوعی خاص از یک سخت‌افزار برسد و مدیریتی خاص روی آن اعمال کند. اگر آن را پیدا نکرد ساکت بماند و اگر پیدا کرد وارد عمل شود و با تغییر سرعت موتور چرخشی سانتریفیوژها موجب اخلال در کار آنها شود. در حالی که اپراتور به صفحه کنترل کننده نگاه می‌کرده ولی ویروس با اختفای خود ردی به جای نمی‌گذاشته در نتیجه همه چیز عادی به نظر می‌رسیده است.

نمونه عینی: ویروس استاکس‌نت: نحوه کارکرد

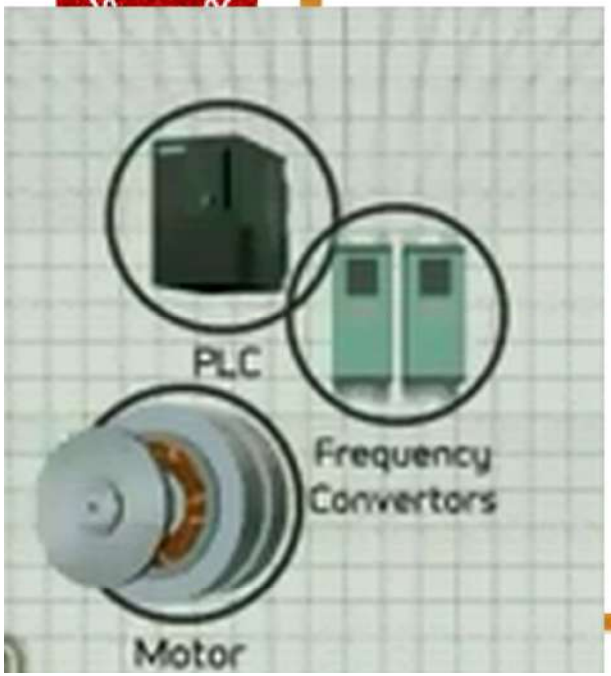
- یک استاد آلمانی (لنگنر): استاکس‌نت برای هدف خاصی طراحی شده بود و آن هدف این بود که بتواند یک قطعه PLC خاص را پیدا کند که دارای مشخصات معینی بود و در تأسیسات خاصی کار می‌کرده و دارای تنظیمات خاصی بوده و اجزاء دیگری نیز بدان متصل بوده مثل مبدلهای فرکانس که در همه دنیا از آن استفاده می‌شود و یک موتور حرکت دهنده است تا سرعت آن موتور را که سانتریفیوژهای ایرانی را به حرکت درمی‌آورد کنترل کند.



نمونه عینی: ویروس استاکس‌نت: نحوه کارکرد

- استاکس‌نت یک ویروس برای دزدی هویت یا رمز عبور یا پول نبود بلکه با خزش در بین یک به یک رایانه‌ها به دنبال نوعی عملیات صنعتی بود که از نوع خاصی از یک قطعه تجهیزات استفاده می‌کرد به نام SIEMENS S7-300 که قطعه‌ای برنامه‌پذیر برای کنترل منطق رایانه‌ای بود. کارکرد این قطعه دستور به ادوات صنعتی برای شروع یا خاتمه کار است و به آن PLC می‌گویند.

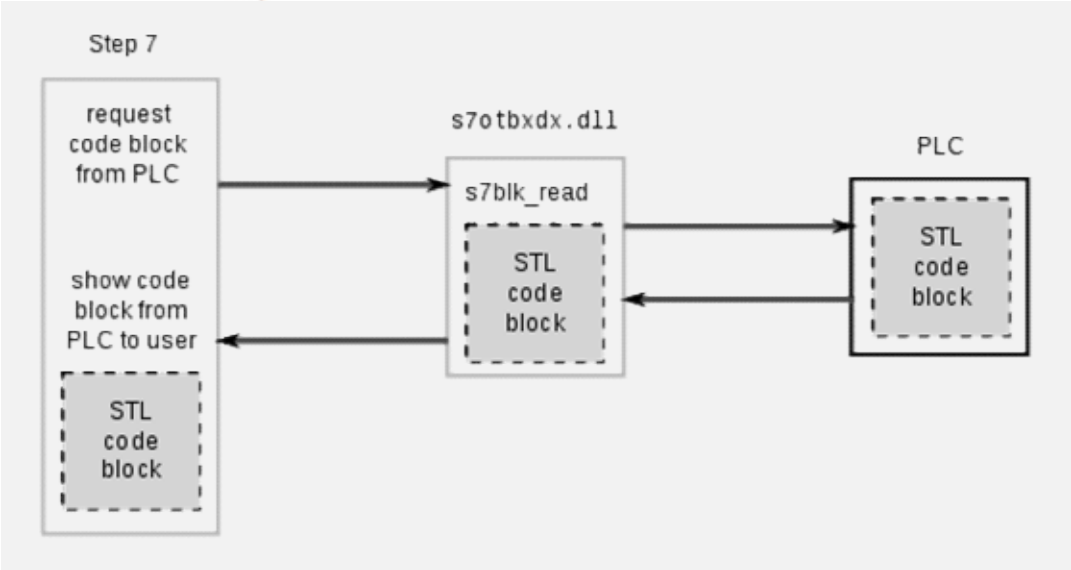
- این قطعه در صنایع بسیار کارآیی دارد از جمله کنترل خطوط تولید صنعتی، کنترل چراغهای راهنما، لوله‌های نفت و گاز، تأسیسات برق و تأسیسات هسته‌ای.

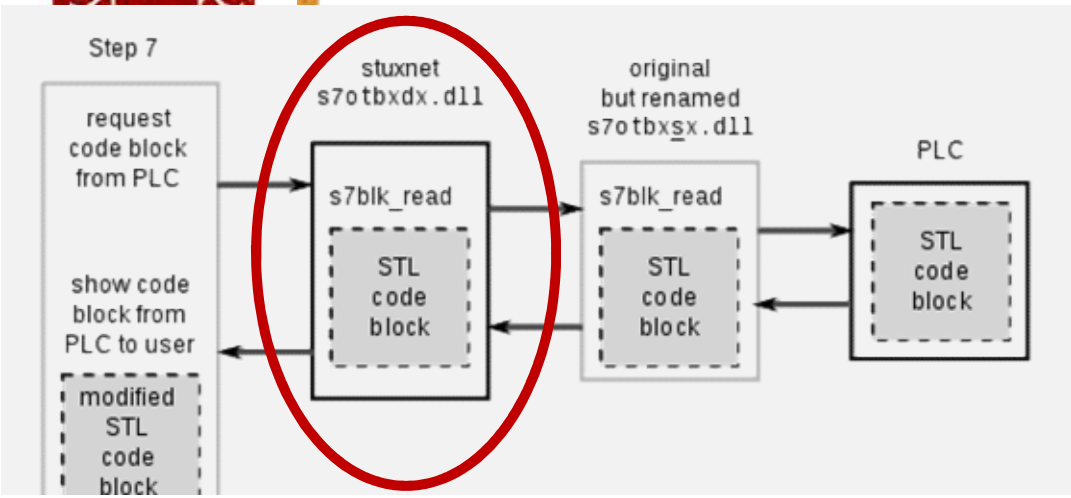


1.mp4

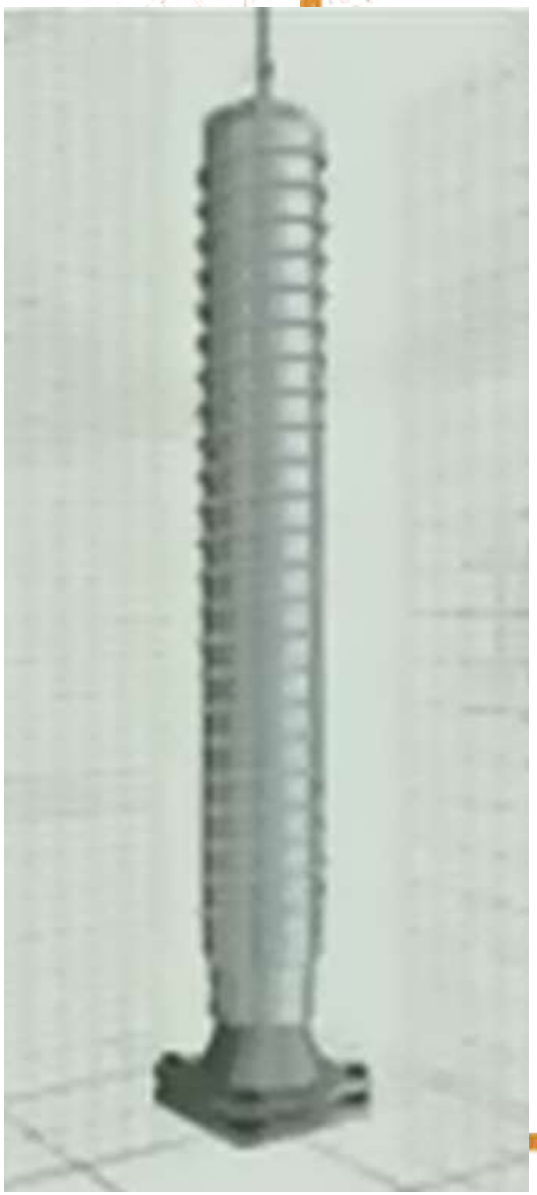
نمونه عینی: ویروس استاکس‌نت: نحوه کارکرد

- یک برنامه نرم‌افزاری به نام (step 7) برای کنترل PLC از سوی شرکت زیمنس عرضه می‌شد که به واسطه یک فایل اجرایی dll سیستم عامل ویندوز مدیریت می‌شد.
- این ویروس در حقیقت یک فایل مضاعف dll بود که خود را پنهان نگاه می‌داشت و مدیریت PLC را برعهده می‌گرفت.





نمونه عینی: ویروس استاکس‌نت



- در برخی از گزارشهای خارجی آمده است: ناظران آژانس بین‌المللی انرژی اتمی گزارش کرده‌اند که بین هزار تا دو هزار سانتریفیوژ به دلائل نامعلومی از صحنه سایت نطنز خارج شده‌اند. از این امر چنین نتیجه‌گیری شد که استاکس‌نت موفق شده صدماتی را وارد کند.
- با مهندسی معکوس ویروس استاکس‌نت معلوم شد که طراحان آن شناخت خوبی از کارخانه و اداوات آن در سایت نطنز داشته‌اند.

نمونه عینی: ویروس استاکس‌نت

- کارشناسان معتقدند در حال حاضر با مهندسی معکوس این ویروس و دانلود کدهای آن، این امکان فراهم است که آن را مجهز کرده و سپس با آماده سازی مجدد، آن را به هر نقطه‌ای دیگر هدفگیری کنند.

- حمله با این ویروس به صورتی طبیعی به معنای تجویز این نوع عملیات از سوی دیگر کشورها بود.

۲- جـنگ سایبری:

- در هر حال این که این نوع دوم را جنگ واقعی بدانیم اختلاف نظر است. به نظر می‌رسد که اثرات این نوع حملات مثل یک بمب‌گذاری منفرد است و جز در مواردی که ملحق به قسم اول گردد جنگ واقعی تلقی نمی‌گردد.
- اما در بسیاری از کاربردها به این نوع تخریب جنگ سایبری اطلاق شده است چون نوعاً بین دولتهای متخاصم رخ می‌دهد.

۲- جـنگ سایبری:

- چهار نوع کاربرد را در جنگ سایبری از هم تفکیک می‌کنیم:
- نوع سوم: اخلال در سامانه‌های الکترونیک خدماتی
- آنست که کشوری با ایجاد اختلال در سامانه‌هایی که خدمات عمومی را به شهروندان کشوری دیگر عرضه می‌دارد، این سامانه‌ها را از کار بیاندازنند.
  - ویروسی کردن سامانه‌ها برای ایجاد کندی یا اختلال در خدمات
  - حملات ردّ خدمات

۲- جـنگ سایبری:

❑چهار نوع کاربرد را در جنگ سایبری از هم تفکیک می‌کنیم:

- نوع چهارم: سرقت اطلاعات ملی و جاسوسی
- آنست که صرفاً اطلاعاتی از کشور مورد حمله را در اختیار گیرد بدون این که تخریب یا اختلالی شکل دهد:
- مثل سرقت اطلاعات ملی یک کشور با جاسوسی از همه شهروندان مثل آنچه در حال حاضر در تلگرام رخ می‌دهد و واگذاری اطلاعات به سازمانهای جاسوسی دولتهای متخاصم مثل اسرائیل.
- مثل هواپیماهای جاسوسی دارای نظام سنجه موقعیت مکانی (GPS) که برای جمع‌آوری اطلاعات بر روی سرزمین دولتی دیگر به پرواز درآید.
- اگر به این نوع حملات نیز جنگ گفته شود مسلماً معنای حقیقی جنگ نیست بلکه در این قسم سوم نوعی جاسوسی محقق شده است.

والحمد لله رب العالمين