مقاله اول: کالبدشکافی جاسوس‌افزار استاکس‌نت[1]

تاریخ گزارش: ۳۱ مهر ۱۳۹۸

مقدمه

در سری مقالات کالبدشکافی جاسوس‌افزار استاکس‌نت قصد داریم به کالبدشکافی و تحلیل پدیده‌ای در دنیا پر پیچ‌وخم بدافزارها بپردازیم که وقتی برای اولین‌بار کشف و شناسایی شد، مدت طولانی به عنوان عجیب‌ترین و وحشتناک‌ترین بدافزار نظر رسانه‌ها و متخصصان امنیت سایبر جهان را به خود جلب کرد. این بدافزار که استاکس‌نت نام گرفت، اولین بدافزاری بود که به عنوان یک جنگ‌افزار سایبری در جهان شناخته شد که بر خلاف دیگر بدافزارها توانایی تخریب تجهیزات فیزیکی / صنعتی را داشت.

شاید ذکر این مورد دور از واقعیت نباشد که تحولات امنیت سایبر در جهان را می‌توان به دو موج پیش از شناسایی استاکس‌نت و بعد از شناسایی استاکس‌نت تقسیم‌بندی کرد، زیرا با شناسایی بدافزار استاکس‌نت دیگر تهدیدات سایبرنتیک محدود به دیفیس سایت‌های استاتیک، سرقت اطلاعات از سایت‌های دینامیک، جاسوسی یا خرابکاری‌های نرم‌افزاری یک سری مجرم سایبری نمی‌شود.

بعد از شناسایی استاکس‌نت بود که خیلی از کشورها پتانسیل پنهان در ساختار امنیت فضای سایبر خود را کشف کردند که هیچگاه نه با محوریت دفاع و نه حتی با محوریت تهاجم به آن توجه‌ای نداشته بودند. همین مسئله در ادامه موجب شد، کشورهای بسیاری از جمله روسیه به صورت جدی وارد این حوزه شوند و بخش‌های مضاعف دیگری در نهادهای امنیتی خود با عنوان واحد امنیت سایبر (در کنار واحدهای جنگ الکترونیک و مخابرات) به منظور صیانت و دفاع از مرزهای سایبری خود تشکیل بدهند[2]. برخی از کشورها حتی پای خود را فراتر از واحدهای سایبری گذاشتند و حمله سایبری را اکنون معادل با اعلان جنگ به خود قلمداد می‌کنند[3] و این حق را برای خود و متحدین خود محفوظ می‌دانند که به منظور دفاع نسبت به تهدیدات خارجی در فضای سایبر حتی از تسلیحات نظامی (جنگ تمام عیار) نسبت به متخاصم بهره ببرند[4].

---

[1] Stuxnet
[2] Russia's Approach to Cyber Warfare by Michael Connell and Sarah Vogler
[3] A cyber-attack in Japan could now bring the US into war By Daniel Wolfe
[4] http://bit.ly/2IT8E0L

استاکس‌نت اثبات کرد که یک فایل باینری مخرب دیگر تهدیدی محدود به یک کامپیوتر یا یک شبکه محدود از کامپیوترها نیست، زیرا یک بدافزار پتانسیلی دارد که می‌تواند در تخریب تجهیزات فیزیکی مانند تجهیزات درون یک نیروگاه اتمی، نیروگاه برق یا یک پالایشگاه نفت و گاز قدرتی معادل یک موشک را داشته باشد.

از همین روی، در این مقاله به جزئیات این بدافزار از نگاه فنی و همچنین راهبرد امنیت ملی خواهیم پرداخت که این بدافزار برای چه و توسط چه کسانی توسعه داده شد و همچنین چگونه وارد ساختار هسته‌ای ایران شد و در نهایت با هدف قرار دادن موفق تجهیزات غنی‌سازی اورانیوم واقع در نطنز چه تغییراتی در ساختار راهبردی امنیت سایبر و همچنین امنیت ملی کشورها ایجاد کرد.

شایان ذکر است، برای اینکه به شکل صحیح و درستی ساختار و انگیزه اصلی طراحی بدافزار استاکس‌نت را متوجه شویم، نیازمند هستیم که قبل از تحلیل ساختار باینری این بدافزار، دلیل اصلی توسعه استاکس‌نت توسط اتحادیه ۵ چشم، شیوه استقرار این بدافزار در سامانه‌های ایزوله، ساختارهای صنعتی، معماری کنترلرهای برنامه‌پذیر، معماری شبکه‌های ایزوله و بسیاری از موارد پایه دیگر را مورد بررسی قرار بدهیم تا بتوانیم ساختار استاکس‌نت را به شکل صحیح تجزیه و تحلیل کنیم.

در مقاله اول، از سری مقالات کالبدشکافی حمله استاکس‌نت به زیرساخت هسته‌ای ایران، تلاش شده است که دلایل اصلی که موجب طراحی و پیاده‌سازی حمله این بدافزار به زیرساخت هسته‌ای ایران شد، مورد بررسی قرار بگیرد.

در مقاله دوم، تلاش خواهیم کرد زیرساخت حیاتی و صنعتی با محوریت کشور جمهوری اسلامی ایران را مورد بررسی قرار بدهیم که چطور بدافزارهای خانواده استاکس‌نت می‌توانند تهدیدات جدی برای این محیط ایجاد کنند.

در مقاله سوم، به طراحی و پیاده‌سازی یک بدافزار (در قالب اثبات‌کننده ادعا) برای محیط‌های صنعتی و زیرساخت حیاتی پرداخته خواهد شد تا با نقاط ضعف این محیط‌ها در محیط عملیاتی آشنا شویم.

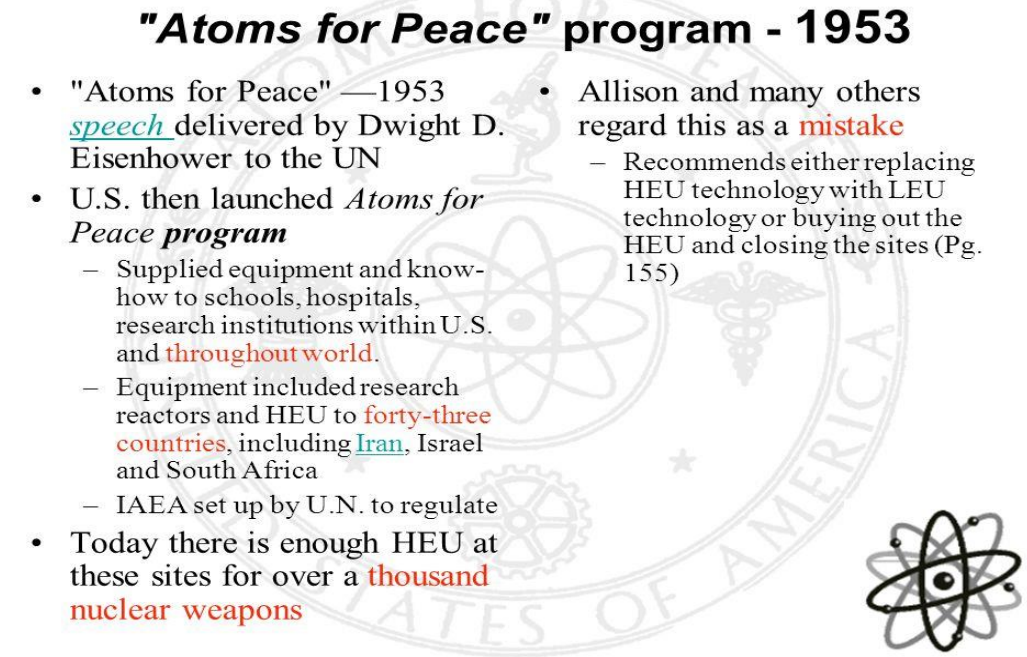
در مقاله چهارم، که مقاله نهایی از سری مقالات کالبدشکافی استاکس‌نت است، به تحلیل خود استاکس‌نت و ماژول‌های آن خواهیم پرداخت که به شکل عمیق‌تری این حملات را درک کنیم تا در ادامه بتوانیم رویکردهای امنیتی صحیح و دقیقی برای محافظت از زیرساخت کشور خود با محوریت امنیت ملی ارائه بدهیم.

میلاد کهساری الهادی (kahsari@kaipod.ir)

فهرست

فعالیت هسته‌ای ایران

پس از آزمایش هسته‌ای هند با عنوان لبخند بودا در ۱۹۷۴[1] و همچنین دستیابی پاکستان به فناوری هسته‌ای در سال ۱۹۷۷[2]، موجب شد حاکم وقت ایران، محمد رضا پهلوی تصمیم بگیرد مانند هند و پاکستان به زنجیره فناوری هسته‌ای دست یابد. در همان سال، قراردادهایی با فرانسه، آمریکا و آلمان غربی برای راکتورهای هسته‌ای امضا شد. اگرچه برخی متعقد هستند، برنامه هسته‌ای ایران در طول دوره جنگ سرد بین ایالات متحده آمریکا و شوروی به دلیل مقابله با تهدید اتمی شوروی تحت دکترین اتم برای صلح آیزنهاور توسط ایالات متحده آمریکا طرح‌ریزی و آغاز شده بود[3].



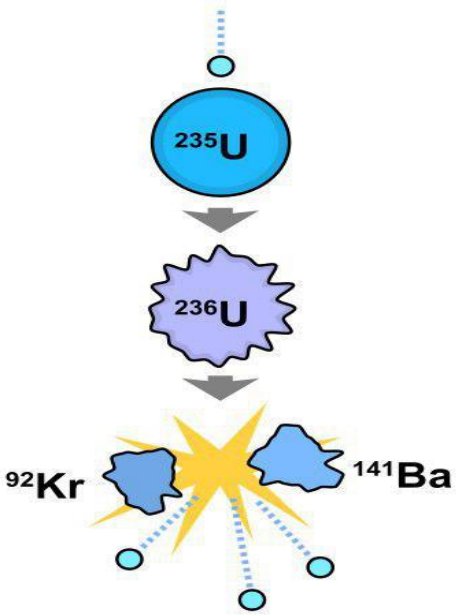
تصویر ۱: طرح اتم برای صلح آیزنهاور

با توجه به تصمیم راهبردی که محمدرضا پهلوی گرفته بود، فرانسه مقرر به تامین ۵، آلمان غربی ۲ و آمریکا ۶ راکتور هسته‌ای شدند. همچنین در سال ۱۹۷۴، فرانسه ضمانت داد تا اورانیوم غنی‌شده مورد نیاز راکتورهای هسته‌ای ایران را تامین کند. از همین روی، ایران ۱۰ درصد از سهام یورودیف (شرکتی که در سال ۱۹۷۳

[1] http://bit.ly/2mBs6Hg
[2] http://bit.ly/2mD5wOl
[3] http://bit.ly/2lQj9cG

برای ساخت نیروگاه‌های اورانیوم غنی‌شده‌ی بزرگ با استفاده از پخش گاز تاسیس شده بود) را خریداری کرد. طی قرارداد ایران، یورودیف مقرر شد حدود ۲۷۰ تن اورانیوم غنی شده تا ۳ درصد U-235 را برای ایران تامین کند.

نکته: یکی از اصول طراحی بمب‌های اتمی، بحث شکافت هسته[1] اتم یک عنصر ناپایدار است. از همین روی، کشورهایی که قصد حرکت به سمت تولید بمب اتم را دارند، در گام ابتدایی خود باید به شکلی اورانیوم ۲۳۵ یا عنصری با خاصیت ناپایداری دسترسی پیدا کنند. در طبیعت تنها عنصرهایی که ویژگی هسته ناپایدار را دارند، پلوتنیوم و اورانیوم هستند. به عنوان مثال، عنصر اورانیوم ۲۳۵ دارای ۹۲ پروتون و ۱۴۳ نوترون است، کافی است در یک عملیات بمبارات نوترونی[2]، یک نوترون دریافت کند تا بتواند به دو اتم دیگر تبدیل شود. در این حالت یک اتم اورانیوم ۲۳۵ به دو اتم دیگر تقسیم می‌شود و دو، سه یا بیشتر نوترون آزاد می‌شود (در تصویر ۲ این شکافت هسته‌ای نمایش داده شده است).



تصویر ۲: شکافت هسته عنصر اورانیوم

---

[1] Nuclear fission
[2] Neutron Bombardment

نوترون‌های آزاد شده خود با اتم‌های دیگر اورانیوم ۲۳۵ ترکیب می‌شوند و آن‌ها را تقسیم کرده و به همین منوال یک واکنش زنجیره‌ای از تقسیم اتم‌های اورانیوم ۲۳۵ تشکیل می‌شود. انجام عمل تقسیم باعث آزاد شدن انرژی می‌شود، بگونه‌ای که جمع انرژی حاصل از تقسیم زنجیره اتم‌های اورانیوم ۲۳۵ بسیار قابل توجه می‌شود. این انرژی آزادسازی شده عظیم چیزی است که در ساخت بمب اتم اهمیت دارد.

به گفته‌ی روزنامه‌ی نیویورک تایمز، شاه ایران دنبال تکنولوژی هسته‌ای بود، نه فقط یک یا دو راکتور برای تولید برق، بلکه تمامی دامنه‌ی تجهیزات، تکنیک‌های علمی و دانش هسته‌ای مورد نیاز برای تبدیل ایران به یک ابرقدرت هسته‌ای و صنعتی را می‌خواست[1]. از همین روی، برنامه ایران در سال ۱۳۵۳ (۱۹۷۴) این بود که در عرض بیست سال، چرخه کامل سوخت را بومی‌کرده و بیست و سه هزار مگاوات برق را از طریق ۲۲ نیروگاه هسته‌ای تأمین نماید[2].

بعد از انقلاب، تمامی شرکت‌های غربی درگیر در توسعه زیرساخت هسته‌ای ایران، ادامه همکاری خود را متوقف کردند. اگرچه حاکمیت جدید به این نتیجه رسیده بود به نیروگاه هسته‌ای نیاز دارد اما تلاش‌ها برای مذاکره با آلمان غربی و فرانسه بی‌فایده بود. ایران تصمیم گرفت تا با شکایت از آلمان غربی آن‌ها را وادار به ادامه‌ی ساخت نیروگاه هسته‌ای بوشهر کند اما با شروع جنگ و بمباران نیروگاه بوشهر آلمان غربی از پروژه انصراف داد.

بعد از انقلاب ایران، در تاریخ ۲۰ بهمن ۱۳۸۱ محمد خاتمی، رئیس‌جمهور وقت ایران، خبر از تهیه سوخت هسته‌ای توسط متخصصین ایرانی برای نیروگاه‌های هسته‌ای ایران داد و در فروردین ۱۳۸۵ محمود احمدی‌نژاد رئیس‌جمهور وقت ایران، اعلام کرد که با توجه به تحریم‌ها ایران موفق به غنی‌سازی اورانیوم به میزان ۳/۵ درصد شده است. در تاریخ ۲۶ بهمن ۱۳۹۰ ایران از ساخت میله سوخت هسته‌ای ۲۰ درصد غنی شده و بارگذاری آن در رآکتور تحقیقاتی ۵ مگاواتی تهران خبر داد.

---

[1] https://nyti.ms/2mAc6Fj
[2] https://amzn.to/2mBHP94

با انتشار اخبار متناوب از فعالیت‌های هسته‌ای در ایران و پس از دامنه‌دار شدن اختلافات میان ایران و نهادهای بین‌المللی نظیر شورای امنیت سازمان ملل متحد[1]، این اختلافات منجر به صدور چندین قطعنامه[2] علیه برنامه هسته‌ای ایران گردید. علاوه بر قطعنامه‌ها، تحریم‌های وسیعی علیه ایران از طرف آمریکا، اتحادیه اروپا و سایر کشورهای جهان صورت گرفت.

منازعه اطلاعاتی مسئله هسته‌ای ایران

منازعه اطلاعاتی و امنیتی بین ایران و کشورهای غربی از سال ۸۱ به صورت پنهان آغاز شد، زیرا در مرداد ۱۳۸۱ گروهک شورای ملی مقاومت ایران (شاخه‌ای از مجاهدین خلق ایران – منافقین)[3] اقدام به انتشار گزارشی نمود که در آن از وجود تأسیسات غنی‌سازی نطنز و آب سنگین اراک[4] اطلاعاتی منتشر شده بود. با آنکه نخستین بار این گروه خبر فعالیت پنهانی مراکز هسته‌ای ایران را به جهان مخابره کرد، اما نیویورک تایمز می‌نویسد که تلاش‌های سرویس‌های اطلاعاتی آمریکا، انگلیس، و اسراییل منجر به کشف این مرکز در سال ۱۳۸۱ شده بود[5].

بعد از گزارش فعالیت هسته‌ای ایران توسط گروهک شورای ملی مقاومت ایران جنگ اطلاعاتی و امنیتی بین ایران و سرویس‌های جاسوسی و امنیتی ایالات متحده آمریکا و هم پیمانان آن در قالب اعضای اتحادیه ۵ چشم[6] به همراه رژیم صهیونیستی آغاز شد، زیرا این کشورها، جمهوری اسلامی ایران دارای فناوری هسته‌ای را تهدید جدی بر علیه ماهیت خود می‌دانستند و به هیچ شکل این فعالیت را مشروع قلمداد نمی‌کردند و البته هنوز هم در زمان نوشتن این مقاله (مورخ ۲۵–مهر–۱۳۹۸) فعالیت اتمی ایران را نپذیرفتند.

از آنجایی که کشورهای غربی مخصوصا ایالات متحده آمریکا و رژیم صهیونیستی حق داشتن فعالیت هسته‌ای را برای ایران به رسمیت نمی‌شناختند، تمامی برآوردها و تحلیل‌های راهبردی اندیشمندان و اندیشکده‌های

---

[1] United Nations Security Council
[2] Resolution
[3] http://bit.ly/2m1iftr
[4] http://bit.ly/2kQYaWK
[5] https://nyti.ms/2krSYse
[6] http://bit.ly/2kngHcW

نظامی جهان راه‌حل مشکل فعالیت هسته‌ای ایران با غرب را در دو مورد خلاصه می‌کردند: تقابل (جنگ) یا مذاکره[1].

در این مقاله، قبل از اینکه به تحلیل فنی بدافزار استاکس‌نت بپردازیم، ابتدا نگاهی به این دو راه‌حل خواهیم کرد و این مسئله را مورد بررسی قرار خواهیم داد که چرا جنگ تمام عیار نظامی با ایران ممکن نبود و آمریکا رویکرد دیگری را در قالب راه حل سوم دنبال کرد.

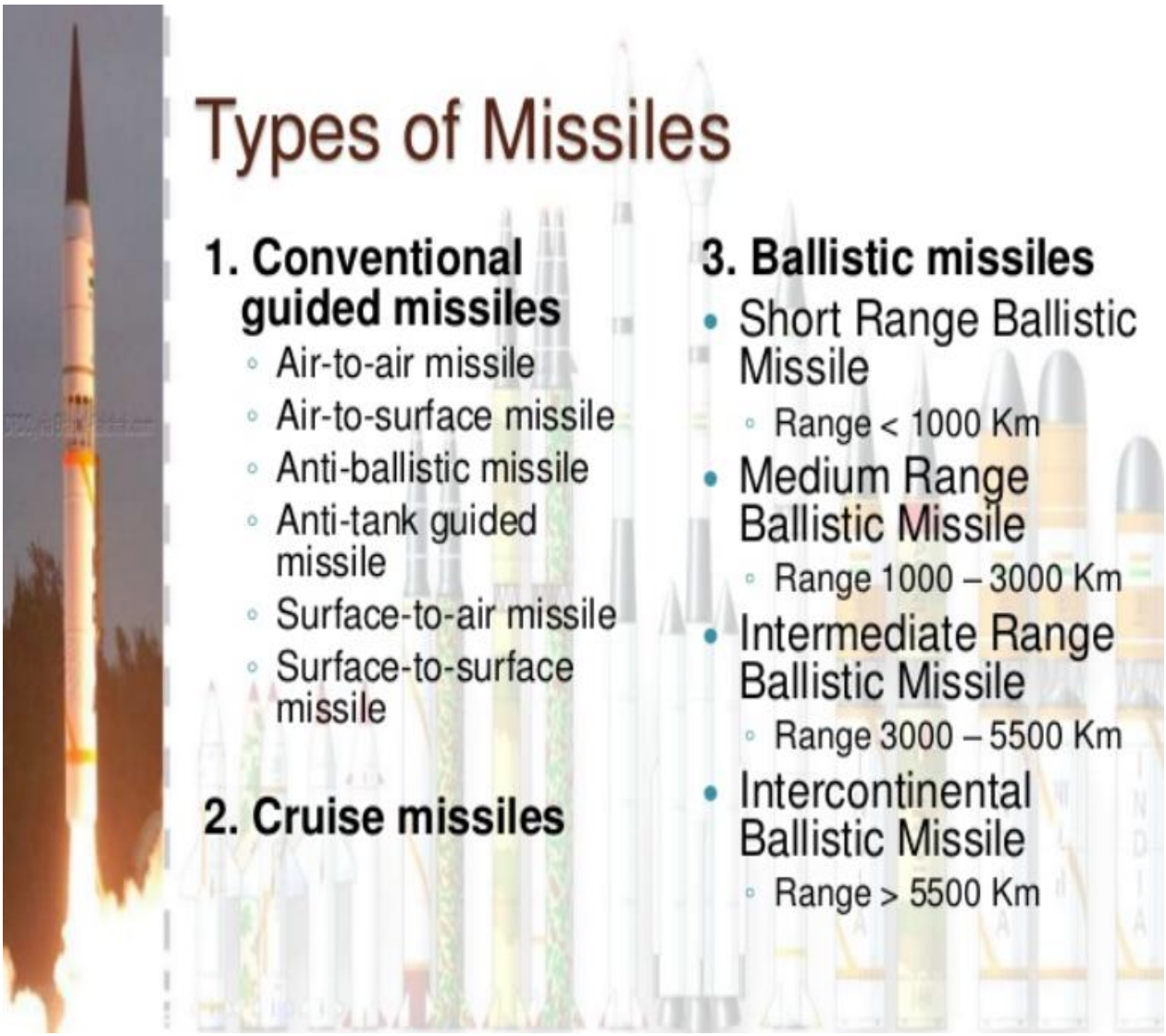
راه‌حل سوم – فشار حداکثری اقتصادی و تهاجم سایبری

همانطور که پیش از این ذکر شد، راه‌حل مشکل فعالیت هسته‌ای ایران با توجه به گزارش و تحلیل اندیشمندان و اندیشکده‌های راهبردی مطرح دنیا تقابل یا مذاکره بود. اما وقتی در مورد تقابل و جنگ صحبت می‌شود، تحلیل و پیش‌بینی آن ساده نیست زیرا متغیرهای بسیار زیادی وجود دارد که اگر هر یک از آن‌ها در نظر گرفته نشود، ممکن است فاجعه به بار بیاورد مخصوصا وقتی در مورد کشوری مانند ایران صحبت می‌شود که پتانسیل‌های پنهان و آشکار بسیار زیادی دارد.

به همین دلیل، گزینه نظامی ایالات متحده آمریکا با ایران از همان ابتدا به نظر غیرممکن بود چون ایران مانند کویت و ویتنام و عراق و ... کشوری کوچک با جمعیت کم نیست که آمریکا بتواند با صرف نیمی از توان نظامی خود با آن روبه‌رو شود و در مدت زمان کوتاهی هم مسئله آن را حل کند.

علاوه بر اینکه ایران وسعت بسیار زیادی دارد، کشوری با ساختار غیرمسطح و کوهستانی، ساختار فرماندهی واحد، دارای نیروهای رزمی نیابتی در منطقه جنوب غربی آسیا (حزب‌الله و حماس و حشدالشعبی و حوثی‌ها ...)، زنجیره متنوعی از موشک‌های بالستیک و کروز و هدایت‌پذیر (همانطور که درتصویر ۳ تشریح شده‌اند) با بردهای چند هزار کیلومتری، تسلیحات پدافندی قدرتمند، انواع ناو و زیردریایی و جنگنده‌های رزمی است که به این کشور توانایی بسیاری بر روی زمین و هوا و دریا می‌دهد.

[1] Dealing with Iran: Confrontation or Negotiation? By Jstor Publication



تصویر ۳: انواع موشک‌های تهاجمی

باید به این مسئله هم اشاره کرد که ایالات متحده آمریکا، با هدف قرار گرفتن پهپادهای فوق پیشرفته خود مانند RQ170[1]، ScanEagle[2] و در مورد اخیر MQ-4C[3] که در تصویر ۴ نمایش داده شده‌اند، و همچنین انهدام اهداف داعش در سوریه توسط نیروی هوافضای سپاه[4] این پتانسیل را به عمل مشاهده کرده است.

[1] http://bit.ly/2kScUo6
[2] http://bit.ly/2kG5jt2
[3] http://bit.ly/2m0hmla
[4] http://bit.ly/2kFZvzL

تصویر٤: پهپادهایی که توسط ایران منهدم شدند

ایالات متحده آمریکا واقف به این مسئله است که اطلاعات مذکور تحلیل نیستند، بلکه فرمی از اینتلیجس می‌باشند که واقعیت‌هایی را ابراز می‌کنند. در کنار این مسائل، مشکلات ایالات متحده آمریکا با قدرت گرفتن چین را هم باید در نظر گرفت که یکی از عمده‌ترین دلایل خروج آمریکا از جنوب غربی آسیا و رفتن به دریای جنوبی چین برای مهار قدرت روز افزون و تهدید این کشور بود[1].

به همین دلایل و البته هزاران دلیل دیگر، عموم تحلیلگران خبره نظامی جهان جنگ آمریکا با ایران را غیرممکن قلمداد می‌کردند چون علاوه بر مشکلات آمریکا در تقابل و رقابت با قدرت‌های نوظهور مانند چین و روسیه، اقتصاد جهانی توانایی تحمل یک جنگ تمام عیار در منطقه قلب جهان[2] را ندارد.

به عنوان مثال، یاکو کدمی که یکی از تحلیلگرهای معروف مسائل نظامی و سیاسی است، هنگام مناظره در مورد جنگ احتمالی ایالات متحده آمریکا با ایران می‌گوید اگر عرب‌ها یا آمریکایی‌ها با ایران وارد جنگ شوند، ایرانی‌ها هستند که پیروز جنگ خواهند بود. او در ادامه دلایل مختلفی از قبیل موقعیت راهبردی، توان دفاعی، شرایط ایالات متحده آمریکا با قدرت گرفتن چین و ... را توضح می‌دهد که چرا با در نظر گرفتن این مسائل

[1] http://bit.ly/2mfybZg
[2] http://bit.ly/2lTxbKr

جنگ بین ایران و آمریکا ممکن نیست[1]. از همین روی گزینه اول یعنی جنگ تمام عیار محتمل به نظر نمی‌رسید.

راه‌حل دوم هم مذاکرات سیاسی بود که از ابتدای فعالیت هسته‌ای ایران به صورت پنهان و موردی شروع شده بود و ایران چندین سال درگیر مذاکره با قدرت‌های جهانی بود تا به یک توافق جامع برد برد برسند، به شکلی که ایران فعالیت هسته‌ای صلح‌آمیز خود را ادامه دهد بدون اینکه به بمب اتمی دست پیدا کند و همچنین تحریم‌های اقتصادی بر علیه ایران هم برداشته شود، که این راه‌حل هم به نظر در سایه عدم اعتماد طرفین به یکدیگر غیرممکن به نظر می‌رسید.

به همین دلیل، آمریکا راه‌حل سوم را دنبال کرد چون نه حق غنی‌سازی اورانیوم را برای ایران مشروع می‌دانست و نه اینکه دنبال امتیاز دادن اقتصادی به ایران بود (مبتنی بر یادداشت‌های فصل هجدهم کتاب هر روز یک موهبت است، نوشته جان کری، وزیر امور خارجه وقت ایالات متحده آمریکا در فرآیند توافق برجام[2]).

راه‌حل سوم ترکیبی از جنگ و مذاکره بود که ایالات متحده آمریکا و هم پیمانان خود دنبال کردند تا بدون اینکه امتیاز زیادی بدهند، فعالیت هسته‌ای ایران را به صورت کامل برای مدت طولانی متوقف کنند و همچنین اقتصاد ایران را به سمت ورشکستگی سوق بدهند تا در نتیجه ایران در مسائل منطقه‌ای و همچنین سیاست‌های کلان تسلیم قدرت‌های جهانی شود. در راه‌حل سوم، همانطور که اکنون در زمان نگارش این مقاله مشخص شده است، آمریکا با مذاکره برای خود وقت خرید تا با دقت بیشتری به اهداف خود یعنی فشار حداکثری بر روی اقتصاد ایران دست پیدا کند.

در حقیقت مذاکره پیرامون فعالیت هسته‌ای ایران وسیله‌ای بود برای اینکه اطمینان حاصل کنند، ایران دارای بمب اتمی نیست و در مدت مذاکره هم به این سمت نمی‌رود که بمب اتمی بسازد تا با اطمینان خاطر بیشتری تحریم‌های اقتصادی ایران را هدفمندتر اعمال کنند، جایگزین تامین انرژی ایران در بازار جهانی شوند و همچنین در صورت ممکن (بهترین تحلیل) فعالیت اتمی ایران را هم به شکل کامل متوقف سازند تا در صورت منازعه سخت، ایران توانایی به کارگیری تسلیحات غیرمتعارف را بر علیه متحدین منطقه‌ای آمریکا از جمله اسرائیل نداشته باشد.

---

[1] https://www.aparat.com/v/X8xoT
[2] https://amzn.to/2kDtWqd

ایالات متحده آمریکا، با انجام مذاکرات تا حد ممکن دستیابی احتمالی ایران به بمب اتمی را غیرممکن کرد و در همین حین که مذاکرات در حال انجام بود، تلاش کرد که به منظور فشار حداکثری به اقتصاد ایران، این کشور را در بازار انرژی (فروش نفت) حذف و خود جایگزین آن در زمینه صادرات نفت شل[1] شود که این هدف را با موفقیت توانست در دوره چهل و پنجم ریاست جمهوری ایالات متحده آمریکا توسط دونالد ترامپ[2] به سرانجام برساند.

همچنین در حین اینکه مذاکرات در حال ادامه بود، ایالات متحده آمریکا با همراهی سرویس‌های امنیتی دیگر کشورهای غربی توانست با جنگ سایبری زیرساخت‌های هسته‌ای ایران را تا حدودی (یک پنجم سانتریفیوژهای عملیاتی IR-1) از بین ببرد و برای اینکه اطمینان حاصل کنند به مدت طولانی ایران توانایی بازگشت به نقطه اول فعالیت‌ها و بازسازی زیرساخت هسته‌ای خود را هم ندارد، به ترور دانشمندان کلیدی صنعت هسته‌ای ایران هم اقدام کرد که در نتیجه این عملیات ۵ دانشمند کلیدی صنعت هسته‌ای ایران توسط موساد و منافقین ترور شدند.

تصویر ۵: نسل‌های متنوعی از سانتریفیوژهای ایران (ساخت ایران)

[1] http://bit.ly/2ku8yUc
[2] http://bit.ly/2kTxOU1

حذف ایران از بازار انرژی، تخریب زیرساخت هسته‌ای ایران با حمله سایبری استاکس‌نت، جنگ رسانه‌ای و همچنین ترور دانشمندان کلیدی این صنعت و تحریم هدفمند زیرشاخه‌های مهم اقتصاد ایران نوید این را می‌داد که ایالات متحده آمریکا بدون حتی شلیک یک گلوله به تمامی اهداف خود در ارتباط با مسئله تقابل و منزوی کردن ایران رسیده است. از همین روی، می‌توان راه‌حل سوم ایالات متحده آمریکا و هدف قرار دادن زیرساخت ایران با جنگ‌افزارهای سایبری را هنرمندانه‌ترین منازعه نرم در تاریخ بشر تاکنون دانست.

در این مقاله قصد ما فقط این است که به بخش جنگ سایبری در راه‌حل سوم ایالات متحده آمریکا بپردازیم که چگونه جامعه اینتلیجنس ایالات متحده آمریکا[۱] از قبیل آژانس امنیت ملی (NSA)[۲]، آژانس اینتلیجس مرکزی (CIA)[۳]، با کمک سرویس اینتلیجس مخفی (SIS یا Mi6)[۴]، اینتلیجنس نظامی (Mi5)[۵]، ستاد ارتباطات دولتی (GCHQ)[۶] بریتانیا و سازمان اطلاعات و وظایف ویژه (Mossad)[۷]، واحد ۸۲۰۰[۸] و مرکز سامانه های اطلاعاتی و محاسباتی (Mamram)[۹] رژیم صهیونیستی توانستند این سلاح مخوف سایبری با عنوان استاکس‌نت را طراحی کنند که اکنون به عنوان اولین جنگ‌افزار سایبری دنیا شناخته می‌شود.

---

[1] http://bit.ly/2kvCmQm
[2] http://bit.ly/2kJQHsC
[3] http://bit.ly/2kw6CdW
[4] http://bit.ly/2kw6GKI
[5] http://bit.ly/2m5Mfo3
[6] http://bit.ly/2kTfp9K
[7] http://bit.ly/2kJM7dW
[8] http://bit.ly/2kqryTp
[9] http://bit.ly/2kT4jBJ

تکامل جنگ‌افزارها

در گذشته وقتی یک کشور بر علیه کشور دیگری اعلان جنگ می‌کرد، یا تصمیم به کشورگشایی می‌گرفت از تسلیحات موشکی، جنگنده‌ها، هلیکوپترها و انواع بمب‌ها (شیمیایی و هسته‌ای و خوشه‌ای)، زیردریایی و کشتی و ... بر علیه دشمنان خود استفاده می‌کرد تا با از بین بردن زیرساخت‌های تدافعی کشور مقابل در سطوح مختلف به سرعت خاک آن را اشغال کند.

به هر صورت، در جنگ‌ها و منازعات سخت گذشته تمامی برخوردها یا بر روی زمین، یا دریا، یا هواوفضا صورت می‌گرفت که برای تهاجم و دفاع در هر کدام از این سه محیط ابزارهایی توسعه داده شده است که پیش از این برخی از آنها نام برده شد. ولی به هر صورت، از منظر تاریخی تکامل جنگ و منازعات انسان‌ها جالب است که چطور این بازی رقابت و تهدید در سطح امنیت ملی موجب توسعه بخش‌های متنوع اجتماعی بشر شده است.

به همین دلیل، قبل از اینکه به بدافزار استاکس‌نت و جنگ‌افزارهای جدید در فضای مجازی/سایبرنتیک بپردازیم، و همچنین در مورد این مسئله صحبت کنیم که استاکس‌نت موجب چه تغییراتی از منظر امنیت ملی و مسائل نظامی‌گری شد، باید یک نگاهی گذرا به تاریخچه منازعات سخت بشر و همچنین فناوری‌های به کار رفته در آن منازعات داشته باشیم.

نسل اول: تسلیحات گرم

به صورت کلی می‌توانیم تکامل منازعات بشر را به چهار نسل تقسیم کنیم که در هر کدام از آن دوره‌ها بشر با دستیابی به مجموعه‌ای از فناوری‌ها توانست برتری نسبت به رقیبان خود به دست آورد. اولین نسل از فناوری‌های نظامی، دوره‌ای بود که انسان به دانشی رسید که توانست سلاح‌های انفرادی گرم، توپ‌های سرپُر، و بمب‌های دستی طراحی کند و دیگر با شمشیر و نیزه و سپر به منازعه نپردازد.

همچنین، هر کشور یا امپراطوری که توانست زودتر به فناوری سلاح‌های انفرادی گرم و سلاح‌های سنگین مانند توپ‌های سرپُر برسد، و کشتی‌های جنگی دارای توپ بسازد، در ادامه موجب شد مانند امپراطوری‌های اولیه از جمله بریتانیا و فرانسه و اسپانیا و پرتغال و ... با سهولت بیشتری کشورگشایی انجام بدهد، چون به آن کشور برتری بر روی زمین و دریا را می‌داد.

نسل دوم: هواپیما و زیردریایی

در جنگ جهانی اول، ساختار نظامی دچار تغییر و تحول اساسی شد. چون علاوه بر زمین و دریا، منازعات سخت با استفاده از جنگنده‌های نسل اول (دارای موتورهای پیستونی) به هوا و با زیردریایی (دارای موتورهای دیزلی–الکتریکی) به زیردریا رسید و همچنین تمامی تسلیحات از نظر قدرت تخریب و عملکرد به‌روزرسانی و توسعه داده شده بودند و همچنین برای اولین بار ماشین‌های جنگی مانند تانک و نفربر و ... مورد استفاده وسیع قرار گرفتند. در جنگ جهانی اول، کشوری توانایی داشت که در مقابل تمامی تهدیدات از خود مقابله کند که علاوه بر نیروی زمینی و نیروی دریایی، نیروی هوایی و همچنین زنجیره متنوعی از تسلیحات شناسایی، دفاعی و تهاجمی در سطوح مختلف دارا بوده باشد وگرنه کشور متخاصم می‌توانست در مدت کوتاهی تمامی استحکامات دفاعی آن را نابود کند.

تصویر ٦: جنگنده **Eindecker** فوکر آلمان در جنگ جهانی اول

در جنگ جهانی دوم، این مسئله به شکل جدی نمایانگر و به اوج خود رسید. چون وارماخت[1] یا همان ارتش آلمان نازی با تکیه بر نیروی زمینی[2] و هوایی[3] و دریایی[4] قدرتمند مجهز به زنجیره تسلیحاتی متنوع خود توانست به سرعت در خاک اروپا شروع به پیشروی کند. البته همین مسئله در ادامه موجب شد، کشورهای

[1] Wehrmacht
[2] Heer
[3] Luftwaffe
[4] Kriegsmarine

دیگر مانند اتحاد جماهیر شوروی سوسیالیستی[1]، انگلیس و آمریکا از ترس قدرت روز افزون وارماخت تحت امر هیتلر و حزب نازی آلمان تسلیحات دفاعی خارق‌العاده‌ای در بخش پدافند، توپخانه، رادارها، سونارها و ... خلق کنند تا بتوانند در مقابل تهاجم آلمان نازی از خود دفاع کنند.

تصویر ۷: جنگنده Bf 109 آلمان نازی در جنگ جهانی دوم

به عنوان مثال وقتی جنگ جهانی دوم آغاز شد، آلمان‌ها دارای یک کلاس زیردریایی از خانواده Uboat با عنوان یو-۴۸۰ بودند که به پنل‌های پلاستیکی حباب‌ساز برای محافظت از شناسایی توسط امواج سونار مجهز شده بود که اولین زیردریایی مخفی کار شد و توانست برای مدتی در کانال انگلیس مخفی بماند و چند فروند کشتی متفقین را غرق کند[2].

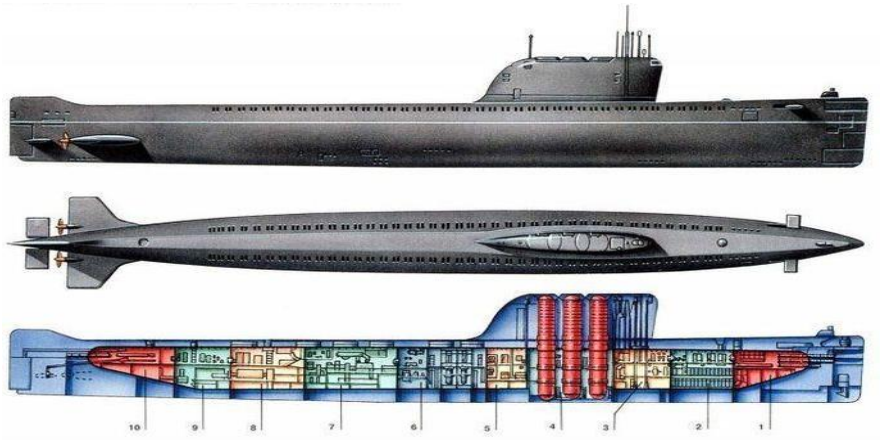
تصویر ۸: زیردریایی U480

[1] http://bit.ly/2m3XHR5
[2] http://bit.ly/2m3qxRy

این کلاس از زیردریایی نازی‌ها فناوری حباب‌سازی در اطراف ساختار بدنه خود داشت که سیگنال‌های صوتی ارسال شده توسط سونارها را به خود جذب می‌کرد و این مسئله موجب می‌شد که این زیردریایی‌ها توسط سونارهای ASDIC بریتانیا[1] قابل شناسایی نباشند چون بعد از برخورد سیگنال‌های صوتی ارسال شده توسط سونار به حباب‌های اطراف بدنه زیردریایی دیگر بازگشت داده نمی‌شدند، و همین مسئله موجب می‌شد سونار نتواند موجودیت و موقعیت این زیردریایی‌ها را حدس بزند. به هر صورت، دانشمندان انگلیسی در ادامه توانستند با پژوهش قدرتمندترین و خلاقانه‌ترین سونارهای جهان را طراحی کنند که در نتیجه بتوانند زیردریایی‌های یو-۴۸۰ آلمان‌ها را که با ایجاد حباب در سطح خود امواج صوت شناسایی سونارها را جذب می‌کردند، شناسایی و در نهایت منهدم کنند.

نسل سوم: عصر فضایی و موشک‌های بالستیک

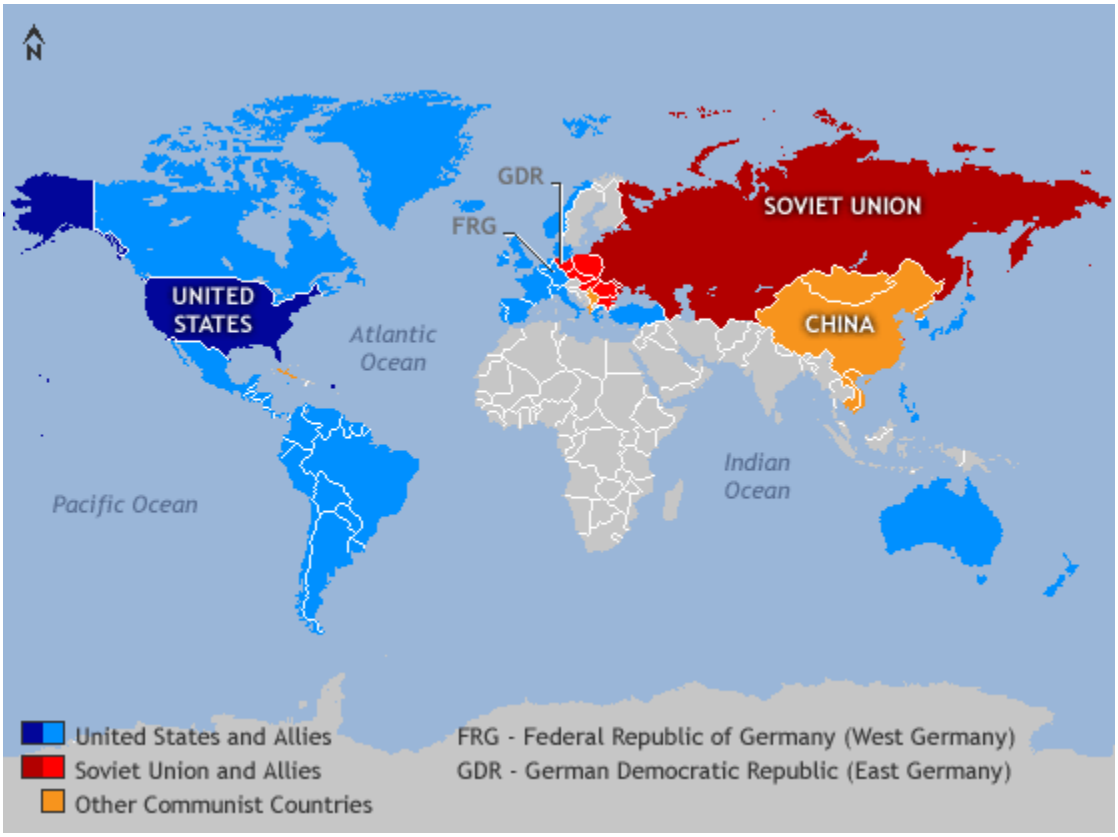
نسل سوم تسلیحات، و البته عمده‌ترین پیشرفت‌های مبتنی بر فناوری در دوره جنگ سرد[2] بین شوروی و ایالات متحده آمریکا رخ داد. در این دوره بود که انسان‌ها به فضا رسیدند، شبکه‌های کامپیوتری را طراحی کردند، مخابرات همراه، موشک‌های بالستیک و کروز و هدایت‌پذیر، تسلیحات شیمیایی-میکروبی، زیردریایی‌های هسته‌ای، زیردریایی هدایت‌پذیر از دور، هواپیماهای بمب افکن، برتری هوایی و جنگنده، و سامانه‌های پدافندی ضدهوایی طراحی شدند، ارتباطات فضایی شکل گرفت و بسیاری از پیشرفت‌های دیگر که امروز به شکلی زندگی ما متکی به آن‌ها است.



تصویر ۹: زیردریایی هسته‌ای K19 شوروی

[1] http://bit.ly/2lWvsnC
[2] http://bit.ly/2koDIfx

بعد از جنگ جهانی دوم، اروپا به شکل کامل نابود و جهان بین دو قطب قدرتمند شوروی و ایالات متحده آمریکا تقسیم‌بندی جناحی شده بود. مابقی کشورها به شکلی از نظر اندیشه‌ای سیاسی، اقتصادی و اجتماعی یا به سمت بلوک شرق یعنی شوروی (سوسیالیسم[1] – کمونیسم/لنینیسم[2]) یا به بلوک غرب یعنی آمریکا (کپیتالیسم[3] – لیبرالیسم[4]) گرایش داشتند.



تصویر ۱۰: دسته‌بندی کشورها در دوره جنگ سرد

در این دوره، بین بلوک شرق با رهبری شوروی و بلوک غرب با رهبری ایالات متحده آمریکا رقابت‌های گسترده‌ای هم وجود داشت از قبیل رقابت فضایی[5] که به دلیل سفر موفق یوری گاگارین توسط فضاپیمای وُستوک–۱ به فضا صورت گرفت. ایالات متحده آمریکا برای اینکه در رقابت فضایی از شوروی عقب نباشد، با استفاده از فضاپیمای آپولو ۱۱ و فرماندهی نیل آرمسترانگ و باز آلدرین با موفقیت به ماه سفر کردند (اگرچه

[1] http://bit.ly/2m3snlq
[2] http://bit.ly/2lYwnno
[3] http://bit.ly/2lX0FqG
[4] http://bit.ly/2lYGKaZ
[5] http://bit.ly/2ktQdGS

هنوز بسیاری از تحلیلگران آن را دروغ می‌دانند). این رقابت موجب شد عصر سفرهای فضایی انسان در دوره جنگ سرد شروع شود.

علاوه بر رقابت فضایی، بین ایالات متحده آمریکا و شوروی رقابت تسلیحاتی (موشک‌های بالستیک برد بلند حامل کلاهک هسته‌ای[1]) هم بود و به دلیل دستیابی دو کشور به این نوع تسلیحات، هم دیگر را به حمله اتمی تهدید می‌کردند، به شکلی که شوروی در کوبا و ایالات متحده آمریکا در ترکیه پایگاه نظامی و موشکی ایجاد کرده بودند. در این جنگ لفظی که دو کشور یکدیگر را تهدید به حمله اتمی می‌کردند، مسئله حفظ ارتباطات حتی در حین حمله اتمی اهمیت فراوانی داشت. این مسئله در ادامه موجب شکل‌گیری شبکه‌های کامپیوتری و توپولوژی‌های مختلف ارتباطی–مخابراتی شد تا حتی اگر یک ایالات آمریکا توسط شوروی مورد تهاجم اتمی قرار گرفت (مانند اتفاقی که برای ژاپن رخ داد) تمامی ارتباطات از بین نرود و خطوط فرماندهی حفظ شود.

شایان ذکر است، پیش از آمریکا، شوروی با همین محوریت و البته ساخت جامعه سایبرنتیک طراحی ساختار ارتباطی OGAS[2] را آغاز کرده بود که به دلایل مشکلات اقتصادی شوروی این پروژه متوقف شد اما ایالات متحده آمریکا توانست به شکل صحیح این ساختار ارتباطی که ما اکنون به عنوان Computers Internetworking یا Computers Network[3] می‌شناسیم را با کمک دانشگاهیان و برخی پژوهشکده‌های تحت نظر دارپا[4] ایجاد کند.

در این دوره بود که ارتباطات و جاسوسی فضایی هم شکل گرفت. چون شوروی به توانایی در ساخت رادار رسیده بود که دیگر ایالات متحده آمریکا با هواپیماهای جاسوسی خود مانند U2 توانایی جاسوسی از آسمان شوروی را نداشت[5]، همین مسئله در ادامه موجب شد ایالات متحده آمریکا به سمت جاسوسی با استفاده از ماهواره‌های سری KH تحت برنامه جاسوسی فضایی کرونا[6] برود.

همچنین با استفاده از پایگاه‌های شنود–جاسوسی که در شمال ایران (مانند سایت جاسوسی ایالات متحده آمریکا واقع در بهشهر) ایجاد کرده بود، به جاسوسی از فضای فرکانسی و ارتباطی شوروی بپردازد. این رویکرد

---

[1] http://bit.ly/2m38dbf
[2] http://bit.ly/2mqpyvj
[3] http://bit.ly/2kRre08
[4] http://bit.ly/2m1tna4
[5] http://bit.ly/2knbAJK
[6] http://bit.ly/2kkM73A

فضایی دو کشور ابرقدرت جنگ سرد در ادامه موجب شکل‌گیری نظارت و ارتباطات ماهواره‌ای و همچنین فناوری‌های مرتبط با آن مانند موقعیت‌یابی ماهواره‌ای از قبیل سرویس GPS ایالات متحده آمریکا و GLONASS[1] شوروی شد.

تصویر ۱۱: مرکز جاسوسی سیا برای رهگیری سیگنال‌های الکترونیکی شوروی در صفی‌آباد بهشهر، ایران

به صورت خلاصه، همانطور که در این قسمت مورد بررسی قرار گرفت، رقابت بین ایالات متحده آمریکا و شوروی در زمان جنگ سرد، اساس بسیاری از فناوری‌ها و پیشرفت‌های بشر شد و تغییرات بسیاری در مسائل نظامی، ارتباطی، رفاهی و ... صورت گرفت اگرچه مسئله رقابت با محوریت امنیت همواره وجود داشته است. مثلا وقتی یک کشور به فناوری دست پیدا می‌کند که به او برتری در یک سطح مخصوصا با محوریت مسائل امنیت ملی می‌دهد، کشورهای دیگر به سمت شناسایی فناوری‌هایی می‌روند که با به کارگیری آن‌ها برتری کشور دیگر را حداقل نسبت به خود خنثی کنند.

همین روند در ادامه موجب می‌شود همواره بشر در سطح فناوری و مخصوصا هنگام منازعات سخت به سرعت در سطوح مختلف پیشرفت کند. البته گاهی اوقات این موضوع می‌تواند دردسر آفرین هم باشد، مانند رقابت در زمینه توسعه جنگ‌افزارهای هسته‌ای و جنگ‌افزارهای سایبرنتیک که اکنون تبدیل به یک مسئله جدی برای امنیت و صلح پایدار شده است.

[1] http://bit.ly/2kFkaE1

نسل چهارم: جنگ‌افزارهای سایبری در راه

بعد از جنگ سرد بین شوروی و ایالات متحده آمریکا که اساس بسیاری از فناوری‌ها در آن شکل گرفت و بشر تغییرات گسترده‌ای در تمامی جنبه‌های اجتماعی خود تجربه کرد، در سال ۲۰۱۰ اتفاق دیگری در جریان بود که نوید یک تغییر بنیادی دیگر را تجربیات زندگی بشر می‌داد.

در این سال بود که تمامی خبرگزاری‌های جهان مات و مبهوت اتفاقی بودند که از تاسیسات غنی‌سازی اورانیوم واقع در نطنز کشور ایران مخابره می‌شد. اتفاقی نادر که پیش از این در هیچ کجای دنیا تجربه نشده بود و بسیاری از کشورها را دچار شوک کرده بود. در این سال بود که برای اولین بار خبر از کشف بدافزاری گزارش شده بود که توانایی تخریب تجهیزات فیزیکی در ساختارهای صنعتی را داشت و همچنین با موفقیت توانسته بود این کار را در تاسیسات غنی‌سازی اورانیوم ایران با انهدام یک چهارم از سانتریفیوژهای عملیاتی انجام بدهد.

تصویر ۱۲: نقشه آلودگی به بدافزار استاکس‌نت

گزارشات اولیه از تجزیه و تحلیل این بدافزار توسط متخصصان Symantec و Kaspersky و McAfee نشان می‌داد که با پدیده‌ای رو به رو هستیم که آن را دیگر نمی‌توان یک بدافزار خطاب کرد. شاید ظاهری مانند یک بدافزار داشته باشد، اما پیلود آن دیگر جاسوسی یا تخریب‌های جزیی در سطح شبکه‌های کامپیوتری نبوده است. این بدافزار عملیاتی شده است تا تخریبی مانند یک سلاح جنگی را داشته باشد.

این بدافزار که استاکس‌نت نام گرفت، امنیت ملی کشورها را وارد فاز جدید دیگری کرد زیرا نشان می‌داد دیگر تهدیدها محدود به زمین، دریا و یا حتی هواوفضا نیستند، بلکه اکنون تهدید می‌تواند در گوشی همراه، لپ‌تاپ و دیگر تجهیزات الکترونیکی شما باشد. شناسایی استاکس‌نت، به صورت کامل مرزها برای شناسایی تهدیدها را از بین برد، چون هر لحظه ممکن است تهدیدی از فضای سایبر به شما هجوم ببرد و تمامی زیرساخت‌های شما را نابود کند.

در گذشته اگر جنگی بین دو طرف اعلام می‌شد، بخش بزرگی از این جنگ‌ها هدف قرار دادن زیرساخت‌های انرژی و اقتصادی و ... کشورها بود، از همین روی شما باید از تسلیحات متنوع نظامی استفاده می‌کردید، اما از آنجایی که امروز بسیاری از زیرساخت‌ها الکترونیکی–کامپیوتری شده است، این تخریب را اکنون یک بدافزار چندکیلوبایتی هم می‌تواند فقط با ایجاد تداخل در سطح سیستم‌های کنترلی انجام بدهد، مانند اتفاقی که در تهاجم استاکس‌نت به زیرساخت غنی‌سازی اورانیوم ایران رخ داد.

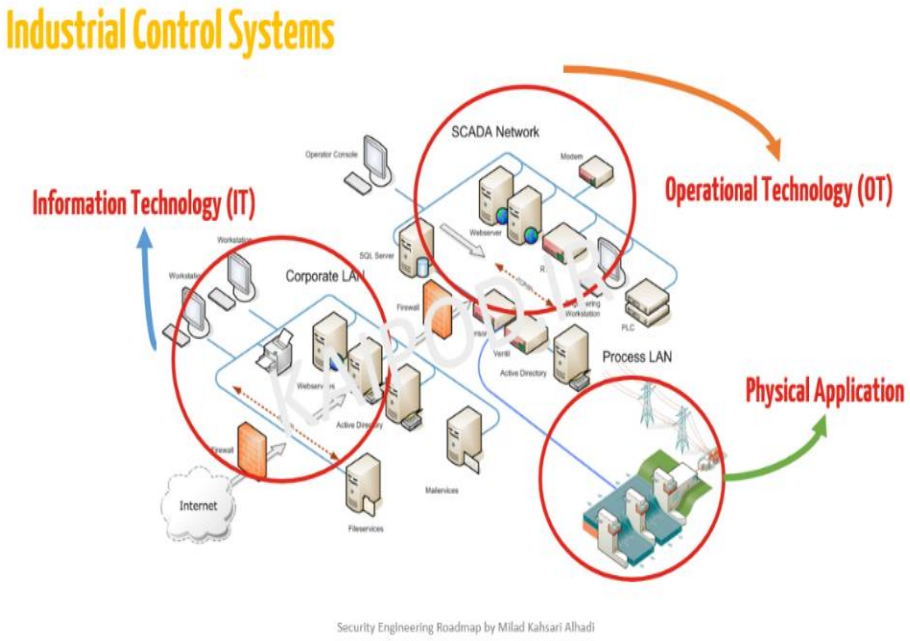
البته این پایان ماجرا نیست، بعد شناسایی و کشف استاکس‌نت و بدافزارهایی مشابه آن مانند Flame و Duqu و ... همچنین نمایان شدند که به دلیل کارآمدی توسعه این نوع تسلیحات با محوریت تهاجم برای کشورهای ابرقدرت دنیا بود.

به عنوان مثال، همانطور که ایالات متحده آمریکا با همراهی اعضای اتحادیه پنج چشم و رژیم صهیونیستی اقدام به توسعه بدافزار استاکس‌نت برای انهدام تجهیزات غنی‌سازی اورانیوم ایران کردند، در اقدامی مشابه روسیه هم با توسعه بدافزار BlackEnergy اقدام به انهدام زیرساخت انرژی اوکراین کرد. این مسئله نشان می‌داد که به زودی، تسلیحات سایبرنتیک با روی آوردن کشورهای بیشتر به آن، شکل جدی‌تری به خود بگیرند.

ساختار مورد هدف استاکس‌نت

تا به الان با سیر تحولات و پیشرفت‌هایی که در فناوری و صنایع نظامی / امنیتی رخ داده است، آشنا شدیم. فهمیدیم که اکنون در عصر چهارم تحولات هستیم که یک برنامه کامپیوتری می‌تواند نقش مخربی مانند یک سلاح فیزیکی را داشته باشد. از آنجایی هم که این مسئله در گذشته با واسطه استاکس‌نت تجربه شده است، دیگر یک نظریه نیست بلکه در عمل این تهدید تجربه شده است.

اما قبل از اینکه به تجزیه و تحلیل بدافزار استاکس‌نت و کلا این گروه از تهدیدات بپردازیم، ابتدا باید زیرساخت‌های صنعتی را مورد بررسی و کالبدشکافی قرار بدهیم که توسط این بدافزار (و بدافزارهای مشابه به آن) مورد حمله قرار گرفت. شایان ذکر است، سامانه‌های صنعتی دارای اهمیت بسیار فراوانی برای ما هستند، چون در بخش‌های متنوعی از زیرساخت ارتباطی و زیرساخت حیاتی مانند بخش انرژی، اقتصاد و حتی تجهیزات نظامی مورد استفاده قرار می‌گیرند.



تصویر ۱۳: معماری شبکه تجهیزات صنعتی

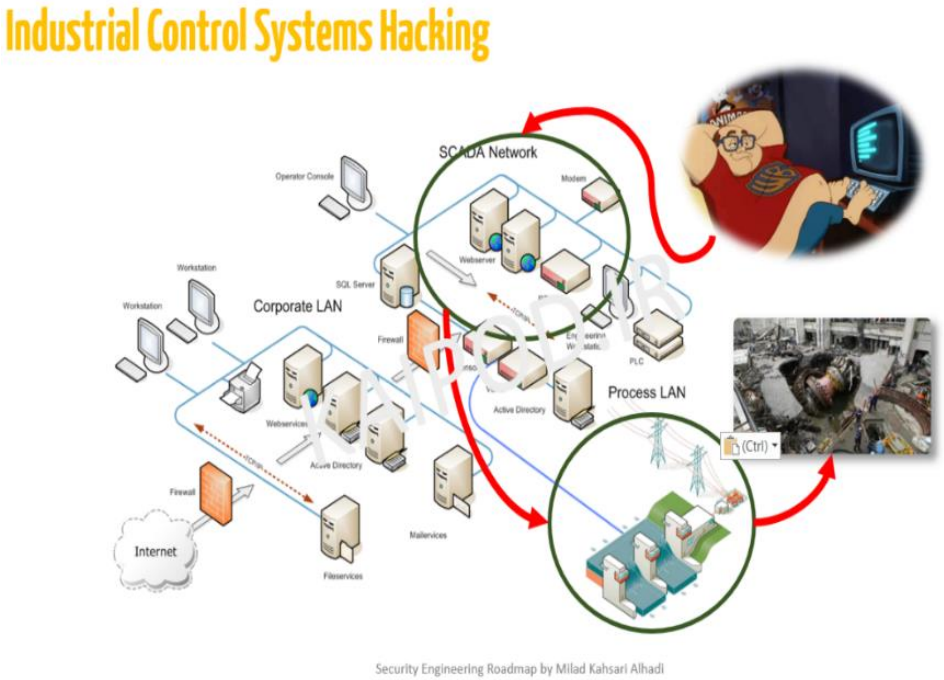
همانطور که در تصویر ۱۳ نمایش داده شده است، یک زیرساخت صنعتی به صورت کلی از سه بخش عملیاتی در ظاهر مجزا تشکیل می‌شود که تمامی این بخش‌ها به صورت ایرگپ با یکدیگر مرتبط هستند. این سه بخش در قسمت زیر تشریح شده‌اند:

۱. **بخش فناوری اطلاعات**[1]: بخش فناوری اطلاعات، در حقیقت شامل ابزارهای نرم‌افزاری مانند ایستگاه‌های کاری[2]، اکتیو دیرکتوری[3]، سرورها، نرم‌افزارهای کنترلی و ... می‌شوند. این بخش از منظر نفوذگری اهمیت فراوانی دارد، چون با نفوذ به این قسمت می‌توان عملیات خرابکاری را آغاز کند.

[1] Information Technology
[2] Workstations
[3] Active Directory

۲. **بخش فناوری عملیاتی[1]:** بخش فناوری عملیات، شامل تجهیزات کنترلی مانند کنترلرهای برنامه‌پذیر منطقی و سنسورها[2] و ... می‌شود. این بخش از منظر خرابکاری اهمیت فراوانی دارد، چون اگر مهاجم بعد نفوذ به شبکه صنعتی بتواند تجهیزاتی که در این بخش عملیاتی هستند را مورد دستکاری قرار بدهد، فاجعه صورت خواهد گرفت.

۳. **بخش تجهیزات فیزیکی[3]:** این بخش دقیقا قسمتی است که تجهیزات فیزیکی مانند سانتریفیوژها[4]، رآکتورها[5]، دریچه‌ها[6]، دیگ بخار[7] و ... قرار دارند که توسط اکتوترها[8] و کنترلرهای برنامه‌پذیر منطقی باید تحت نظارت بلادرنگ و کنترل قرار بگیرند.



تصویر ۱٤: تخریب تجهیزات فیزیکی

شایان ذکر است، این سیستم‌ها در حالیکه تا ۳۰ سال پیش به صورت فیزیکی از مابقی سیستم‌ها مجزا شده بودند، امروزه تمامی آن‌ها و سیستم‌های زیرساخت کنترلی می‌توانند به اینترنت متصل شوند که متصل شدن

---

[1] Operational Technology
[2] Sensors
[3] Physical Application
[4] Centrifuges
[5] Reactors
[6] Valves
[7] Steam Boilers
[8] Actutaors

هرکدام از این سیستم‌های صنعتی به اینترنت یا در حالت کلی به شبکه می‌تواند یک خطر امنیتی بزرگ برای آن‌ها ایجاد کند زیرا اگر یک شخص بتواند وارد ساختار صنعتی شود و همانطور که در تصویر ۱۴ نمایش داده شده است، در ادامه بتواند در منطق عملیاتی بر روی تجهیزات کنترلی و نظارتی تغییرات اعمال کند، این تغییرات منجربه نابودی بخش فیزیکی خواهد شد.

متاسفانه هنگامی‌که به مکانیزم‌های امنیتی موجود برای محافظت از اطلاعات سیستم‌های صنعتی در سطح پروتکل‌های شبکه صنعتی یا مکانیزم‌های نرم‌افزاری / سخت‌افزاری می‌نگریم، متوجه می‌شویم برخلاف سیستم‌های کامپیوتری که تعداد زیادی مکانیزم و پروتکل امنیتی برای آن‌ها به منظور ایمن‌سازی ارتباط سیستم با شبکه و همچنین یکپارچگی عملیات خود سیستم تعریف و پیاده‌سازی شده است، در سیستم‌های صنعتی و سامانه‌های عامل بلادرنگ[1] اینگونه نمی‌باشد و مکانیزم‌های امنیتی موجود در آن بسیار ناچیز یا برخی از آن‌ها بدون مکانیزم امنیتی هستند.

به هر صورت، سیستم‌های زیرساخت حیاتی می‌توانند یک سیستم بزرگ مانند یک شبکه توزیع و انتقال برق هوشمند[2] یا یک واحد اندازه‌گیری فاز[3] در یک شبکه انتقال برق یا یک کنترلر سیستم بخار یا سرما در یک نیروگاه برق یا یک واحد اندازه‌گیری راه دور/حسگر در یک کارخانه باشد. یکی دیگر از مهم‌ترین قسمت‌های سیستم‌های حیاتی بخش کنترل آن است که سیستم کنترل صنعتی[4] خوانده می‌شوند. شایان ذکر است، یک زیرساخت صنعتی از زیرسیستم‌های زیر تشکیل شده است:

۱. **معماری شبکه‌بندی تجهیزات:** وقتی در مورد ساختار ارتباطی تجهیزات صنعتی صحبت می‌کنیم، با یک مدل خاص از ارتباطات روبه‌رو هستیم که به عنوان ارتباطات ایرگپ یا ایزوله شناخته می‌شوند. در این نوع شبکه‌بندی، ارتباطات به صورت محلی است و هیچ کدام از تجهیزات صنعتی اتصال به اینترنت ندارند.

۲. **واسط انسان و ماشین[5]:** دستگاهی است که نحوه پردازش داده را به یک اپراتور انسانی نشان می‌دهد و از این طریق، اپراتور انسانی عملکرد ماشین را نظارت و کنترل می‌کند.

---

[1] Real-time Operating Systems
[2] Smart Grid Networks
[3] Phasor Measurement Unit
[4] Industrial Control System
[5] Human Management Interface

۳. **واحدهای خروجی راه دور:** این واحدها به سنسورها متصل شده است، سیگنال‌های سنسور را به داده‌های دودویی تبدیل کرده و داده‌های دودویی را به سیستم نظارتی ارسال می‌کنند.

۴. **کنترل‌کننده‌های منطقی قابل برنامه‌نویسی[1]:** این سیستم‌ها مانند مغز متفکر ساختارهای صنعتی هستند و کارهای اساسی را انجام می‌دهند، زیرا آن‌ها اقتصادی، تطبیق‌پذیر و انعطاف‌پذیر بوده و دارای قابلیت پیکربندی بهتری نسبت به واحدهای خروجی راه دور با هدف خاص هستند.

۵. **پروتکل‌های صنعتی[2]:** پروتکل‌های خاص ارتباطی بی‌سیم یا سیمی در سطح شبکه صنعتی هستند که برای اتصال تجهیزات صنعتی به صورت بهینه طراحی شده‌اند.

البته در یک ساختار صنعتی، فقط زیرسیستم‌های ذکر شده در قسمت بالا وجود ندارند، ولی از نظر امنیتی اهمیت واسط انسان و ماشین (HMI)، کنترل‌کننده‌های منطقی قابل برنامه‌نویسی (PLC) و معماری شبکه ساختارهای صنعتی دارای بالاترین اهمیت هستند. از همین روی، در این مقاله، به این مولفه‌های صنعتی نگاه خواهیم کرد تا بتوانیم با درک نسبتا بهتری وارد مبحث تحلیل بدافزار استاکس‌نت و همچنین چالش‌های طراحی آن شویم.

[1] Programable Logic Controller
[2] Industrial Protocols

معماری شبکه ایزوله / ایرگپ

اولین مولفه‌ای که در ساختارهای صنعتی باید مورد بررسی قرار بگیرد، نوع معماری شبکه‌بندی سامانه‌های کنترل صنعتی است. برخلاف معماری ارتباطی سامانه‌های اداری و سازمانی، شبکه‌بندی سامانه‌های کنترل صنعتی به صورت ایزوله یا ایرگپ هستند، به این معنا که تجهیزات درون شبکه صنعتی، ارتباط مستقیم به اینترنت جهانی ندارند.

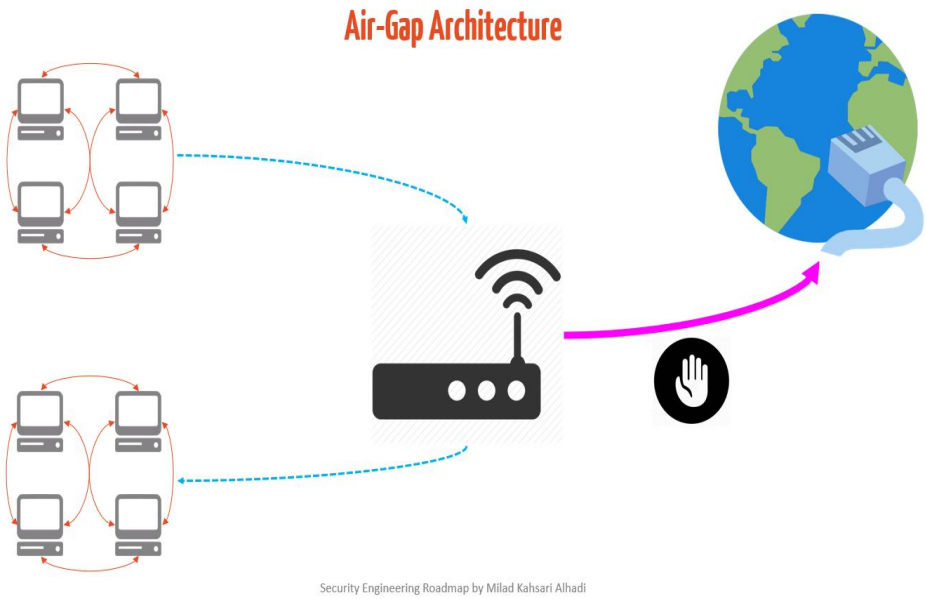
همانطور که در تصویر ۱۵ نمایش داده شده است، ارتباطات تجهیزات درون شبکه صنعتی به صورت محلی است، و این سامانه‌ها به صورت مستقیم امکان دسترسی به اینترنت جهانی را ندارند و فقط می‌توانند در قالب شبکه‌های محلی یک شبکه‌کاری را تشکیل دهند.

مقدمه‌ای بر معماری شبکه‌بندی ایزوله/ ایرگپ

یکی از دلایل مهم پیکربندی شبکه صنعتی به صورت ایرگپ اهمیت ساختارهای صنعتی است زیرا به هر دلیلی اگر شخصی بتواند از راه دور به این تجهیزات و کلا شبکه زیرساخت حیاتی / صنعتی دسترسی بگیرد و یا با بهره‌برداری از آسیب‌پذیری‌های روزصفرم به آن‌ها رخنه کند، و پروسه کنترل یک شبکه صنعتی و لاجیک بارگزاری شده بر روی تجهیزات کنترلی را تغییر دهد، فاجعه صورت خواهد گرفت.

دلیل اینکه با دستکاری در سامانه‌های کنترلی و نظارتی فاجعه رخ خواهد داد این است که در طراحی ساختارهای صنعتی کوچک‌ترین تداخل در پروسه کنترل و عدم تصمیم‌گیری بلادرنگ تجهیزات کنترلی برای نظارت یک دستگاه فیزیکی ممکن است به طور کامل دستگاه تحت کنترل را نابود کند. به همین دلیل، ارتباط تجهیزات کنترلی درون شبکه‌های صنعتی به صورت ایرگپ پیکربندی می‌شود تا جلوی این نوع فجایع در بخش زیرساخت‌های حیاتی گرفته شود.

به صورت خلاصه، از آنجایی که در این نوع معماری شبکه‌بندی، تجهیزات صنعتی مانند کنترلرهای برنامه‌پذیر منطقی (PLC)، سامانه‌های نظارتی و سامانه‌های ایستگاه–کاری به اینترنت جهانی دسترسی ندارند، تصور می‌شود نسبت به تهدیدات خارجی مانند اکسپلویت‌های راه‌دور ایمن هستند، چون از بیرون شبکه صنعتی کسی امکان برقراری ارتباط با آن‌ها را ندارد.



تصویر ۱۵: معماری شبکه‌های ایزوله

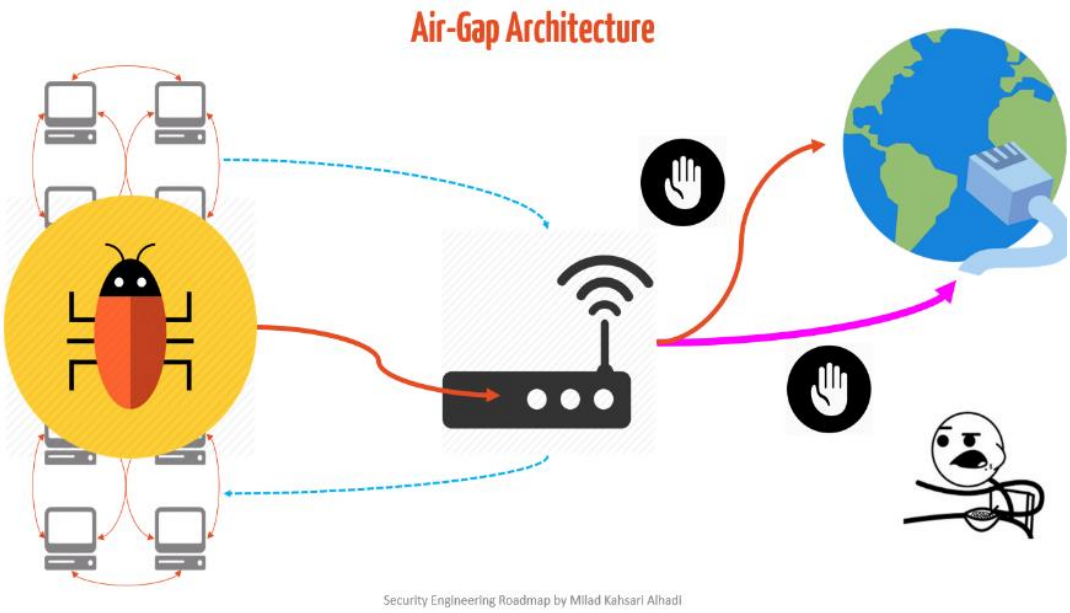
البته این فقط یک فرضیه است که به دلیل طراحی معماری شبکه‌بندی ایزوله هیچ سامانه‌ای به اینترنت دسترسی ندارد، اما گاهی اوقات مشاهده شده است که این فرض اشتباه است و به دلیل طراحی نادرست شبکه ساختار صنعتی برخی گره‌ها به اینترنت دسترسی دارند.

یک اشتباه در طراحی شبکه‌بندی ایزوله ممکن است کل اکوسیستم امنیتی ساختارهای صنعتی را ناکارآمد کند، زیرا یک مهاجم خواهد توانست فقط با دسترسی به گره دارای ارتباط با اینترنت بتواند از طریق آن گره به دیگر گره‌ها نفوذ کند و به همین صورت کل ساختار شبکه را پیمایش کرده تا به دیگر تجهیزات درون شبکه صنعتی مانند کنترلرها و ایستگاه‌های کاری برسد.

اما اگر معماری شبکه‌بندی ساختار صنعتی به درستی ایزوله / ایرگپ پیکربندی شود، حتی در صورت آلودگی سامانه‌ها به بدافزار از طریق هدف قرار دادن زنجیره تامین تجهیزات[1] یا تهدیدات داخلی[2] (یک نفوذی)، به دلیل اینکه ساختار ارتباطی سیستم‌ها به صورت ایرگپ و محلی است، ارتباط بین بدافزار در تجهیزات آلوده با سرور کنترل و فرماندهی خود ممکن نیست. از همین روی، بدافزار نه امکان سرقت اطلاعات از روی سیستم‌ها را دارد و نه اینکه می‌تواند فرمانی را از سرورهای کنترل و فرماندهی خود دریافت کند. این مسئله در تصویر شماره ۱۶ نمایش داده شده است.

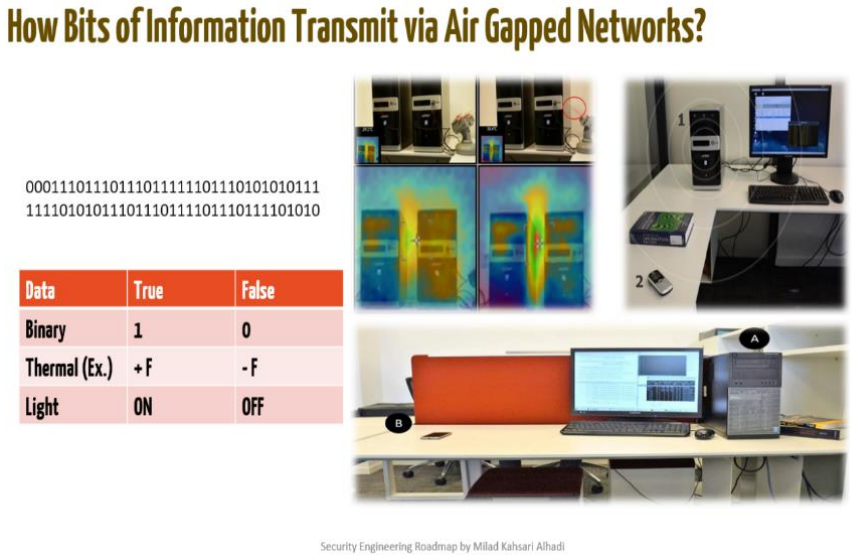
---

[1] Supply Chain Infection
[2] Insider Threat



تصویر ۱۶: عدم توانایی ارتباط بدافزار با اینترنت

اگرچه اکنون تحقیقاتی در دانشگاه بن‌گورین و تل‌آویو رژیم صهیونیستی صورت گرفته است که نشان می‌دهد معماری شبکه‌بندی ایرگپ یا ایزوله را می‌توان به واسطه کانال‌های جانبی دیگری مانند گرما، الکترومغناطیس، صوت، و ... که در تصویر ۱۷ نمایش داده شده است، دور زد تا در نتیجه بتوان اطلاعات را بین دو سیستم مجزا از یکدیگر انتقال داد[1].



تصویر ۱۷: کانال‌های جانبی برقرار ارتباط بدون سیم

[1] https://cyber.bgu.ac.il/air-gap/

شایان ذکر است، معماری ایرگپ فقط می‌تواند ارتباط مرکز کنترل و فرماندهی با بدافزار در زیرساخت را غیرممکن یا سخت کند، اما طراحی بدافزاری مانند استاکس‌نت نشان داد، طراحان حرفه‌ای بدافزار با جمع‌آوری اینتلیجس و اطلاعات به صورت پسیو یا اکتیو نسبت به محیط عملیاتی زیرساخت مورد نظر خود می‌توانند بدافزاری طراحی کنند که حتی بدون ارتباط با مرکز کنترل و فرماندهی عملیات خود را با موفقیت انجام بدهد که در ادامه این مسئله را در نمونه استاکس‌نت به صورت کامل و عمیق بررسی خواهیم کرد.

در هر صورت، با اینکه ساختار و معماری شبکه‌بندی سیستم‌های صنعتی به صورت ایرگپ و ایزوله طراحی شده‌اند، اما این به معنای امنیت ۱۰۰ درصد نیست، چون راه‌های بسیار دیگری وجود دارد که بتوان یک بدافزار را در یک سیستم ایزوله وارد کرد، و با آن از طریق کانال‌های ارتباطی دیگر مانند صوت، الکترومغناطیس، نور و ... ارتباط موثر برقرار کرد. از همین روی، این فرض که معماری شبکه‌بندی ایرگپ می‌توان از نفوذ به شبکه صنعتی جلوگیری کرد، ایده کاملا صحیحی نیست زیرا اکنون موارد نقض آن نمایش داده شده است.

مقدمه‌ای بر حملات ایرگپ

در قسمت قبل به صورت خلاصه با معماری شبکه‌بندی ایرگپ یا ایزوله آشنا شدیم، و همچنین فهمیدیم که دلیل طراحی معماری شبکه‌بندی یک ساختار صنعتی چیست. همانطور که تا به الان مشخص شد، مسئله مهم و بسیار حیاتی که در طراحی و پیکربندی یک شبکه به صورت ایزوله وجود دارد، عدم امکان دسترسی به تجهیزات از بیرون ساختار و شبکه به تجهیزات کنترل و نظارتی صنعتی است.

همین مورد در ادامه موجب خواهد شد به شکل قابل توجه‌ای تهدیدات سامانه‌های کامپیوتری-کنترلی نسبت به زیرساخت‌های صنعتی کاهش قابل توجه‌ای داشته باشند زیرا کسی نمی‌تواند با آن تجهیزات مهم و حیاتی ارتباط برقرار کند و در نتیجه نخواهند توانست در صورت وجود آسیب‌پذیری بر روی تجهیزات درون شبکه صنعتی، آسیب‌پذیری مذکور را مورد بهره‌برداری یا پروسه اکسپلویت کردن قرار بدهند اما مواردی هم مشاهده شده است که طراحی نادرست شبکه به صورت ایزوله موجب رخنه نفوذگران و در نتیجه خسارت فراوان شده است.

اگرچه وقتی یک زیرساخت به صورت ایرگپ یا ایزوله طراحی می‌شود، دلیل نمی‌شود که استدلال کنیم دیگر به هیچ روشی امکان دسترسی به آن تجهیزات وجود ندارد، چون اکنون روش‌های حمله‌ای مانند آلوده‌سازی

زنجیره تامین تجهیزات و همچنین تهدیدات داخلی (نفوذی‌ها) معرفی شده‌اند که به سادگی می‌توانند این رویکرد امنیتی را بی اثر کنند.

همچنین علاوه بر روش‌های حمله مانند آلوده‌سازی زنجیره تامین تجهیزات و تهدیدات داخلی، اکنون رویکردهایی ارائه شده است که به سادگی معماری شبکه‌بندی ایزوله یا ایرگپ را بی‌معنا می‌کنند. این نوع حملات که به صورت ویژه معماری ایرگپ را هدف قرار می‌دهند، به عنوان حملات ایرگپ[1] شناخته می‌شوند که در ادامه برخی از این حملات را مورد بررسی قرار خواهیم داد، اگرچه پیش از بررسی این نوع حملات باید مفاهیم پایه مخابرات و شبکه را مورد بررسی قرار بدهیم تا به شکل صحیحی این نوع حملات را درک کنیم.

مفاهیم پایه مخابرات و الکترونیک

قبل از اینکه متوجه شویم در حملات ایرگپ چه رخ می‌دهد، ابتدا باید نحوه برقراری ارتباط بین دو گره و در یک مقیاس کامل‌تر نحوه ارتباط بین دو ماشین را به صورت ساده مورد بررسی قرار بدهیم. به عنوان مثال، یک پیام از کامپیوتر A به کامپیوتر B چطور ارسال می‌شود؟ هنگامیکه این مسئله را مورد بررسی قرار دادیم، سپس می‌توانیم به این مورد بپردازیم که آیا راه دیگری به منظور انتقال اطلاعات وجود دارد یا خیر؟

در حالت کلی، انتقال پیام و اطلاعات میان دو یا چند نقطه (با فاصله کم تا زیاد) در قالب سیگنال‌ها[2] یا نشانه‌ها رخ می‌دهد. در زمان‌های گذشته، برای ارسال سیگنال از دود، طبل، سمافوریا (مخابره به وسیله پرچم)، هلیوگراف (مخابره به وسیله نور خورشید)، تلگراف (با ساختار کدگذاری مورس) استفاده می‌شد، اما اکنون به دلیل پیشرفت مهندسی برق با ارسال سیگنال‌های الکتریکی امکان انتقال اطلاعات با فاصله بسیار زیاد از طریق کانال‌های ارتباطی سیمی یا حتی بی‌سیم ممکن است.

سیگنال خود در اصل یک مقدار متغیر با زمان است که نوعی از اطلاعات را منتقل می‌کند. در مهندسی برق مقداری که متغیر با زمان است، معمولا ولتاژ (در غیر این صورت، جریان) است. بنابراین وقتی از سیگنال الکتریکی صحبت می‌کنیم، آن‌ها را می‌توانیم ولتاژهای متغیر نسبت به زمان در نظر بگیریم که در ادامه خصوصیت‌های این نوع سیگنال را مورد بررسی قرار خواهیم داد.

---

[1] Airgap Attacks
[2] Signals

شایان ذکر است، در سامانه‌های مدرن امروزی با دو نوع سیگنال رو به رو هستیم. نوع اول سیگنال‌ها را با عنوان سیگنال‌های آنالوگ یا پیوسته می‌شناسیم که در سطح مدارهای الکتریکی با حالت‌های نامتناهی وجود دارند، و نوع دوم را به عنوان سیگنال‌های دیجیتالی می‌شناسیم که نمایش گسسته‌ای از سیگنال‌های آنالوگ هستند. فارق از اینکه سیگنال آنالوگ باشد یا دیجیتال، این سیگنال‌ها بین دستگاه‌ها معمولا از طریق سیم یا باندهای فرکانسی رادیویی/ فیبر نوری برای ارسال و دریافت اطلاعات جابه‌جا می‌شوند.

سیگنال‌های آنالوگ و دیجیتال[1]

همانطور که پیش از این ذکر شد، در مباحث کامپیوتری و الکترونیکی، دو کلمه آنالوگ و دیجیتال اغلب با مفهوم سیگنال و همچنین سیستم به کار گرفته می‌شوند. به عبارت دیگر، یک سیستم یا با سیگنال‌های آنالوگ یا سیگنال‌های دیجیتالی در سطوح مختلف کار می‌کند.

به زبان خیلی ساده، همانطور که در تصویر ۱۸ نمایش داده شده است، یک سیگنال، موجی با مشخصه‌هایی از قبیل فرکانس[2]، دامنه[3]، و فاز[4] است که با استفاده از قواعد مدولاسیون و دمدولاسیون[5] در مخابرات می‌توانیم پیامی را کدگذاری و در یک کانال ارتباطی بی‌سیم[6] یا سیمی[7] به واسطه سیگنال‌های مخابراتی ارسال کنیم. در قسمت زیر مشخصات یک سیگنال به تفکیک تشریح شده‌اند:

۱. **فرکانس:** بَسامَد یا فرکانس معیار اندازه‌گیری تعداد تکرار یک رخداد (تغییر ولتاژ) در واحد زمان (مثلاً ثانیه) است. برای محاسبه فرکانس بر روی یک بازه زمانی ثابت، تعداد دفعات وقوع آن حادثه را در آن بازه می‌شماریم و سپس این تعداد را بر طول بازه زمانی تقسیم می‌کنیم.
در سیستم واحدهای SI، فرکانس به احترام فیزیک‌دان آلمانی هاینریش رودولف هرتز، با هرتز اندازه‌گیری می‌شود. یک هرتز به این معنی است که یک رویداد (در بحث سیگنال‌های الکتریکی این رویداد تغییر ولتاژ یا جریان است) یک‌بار در هر ثانیه رخ می‌دهد.

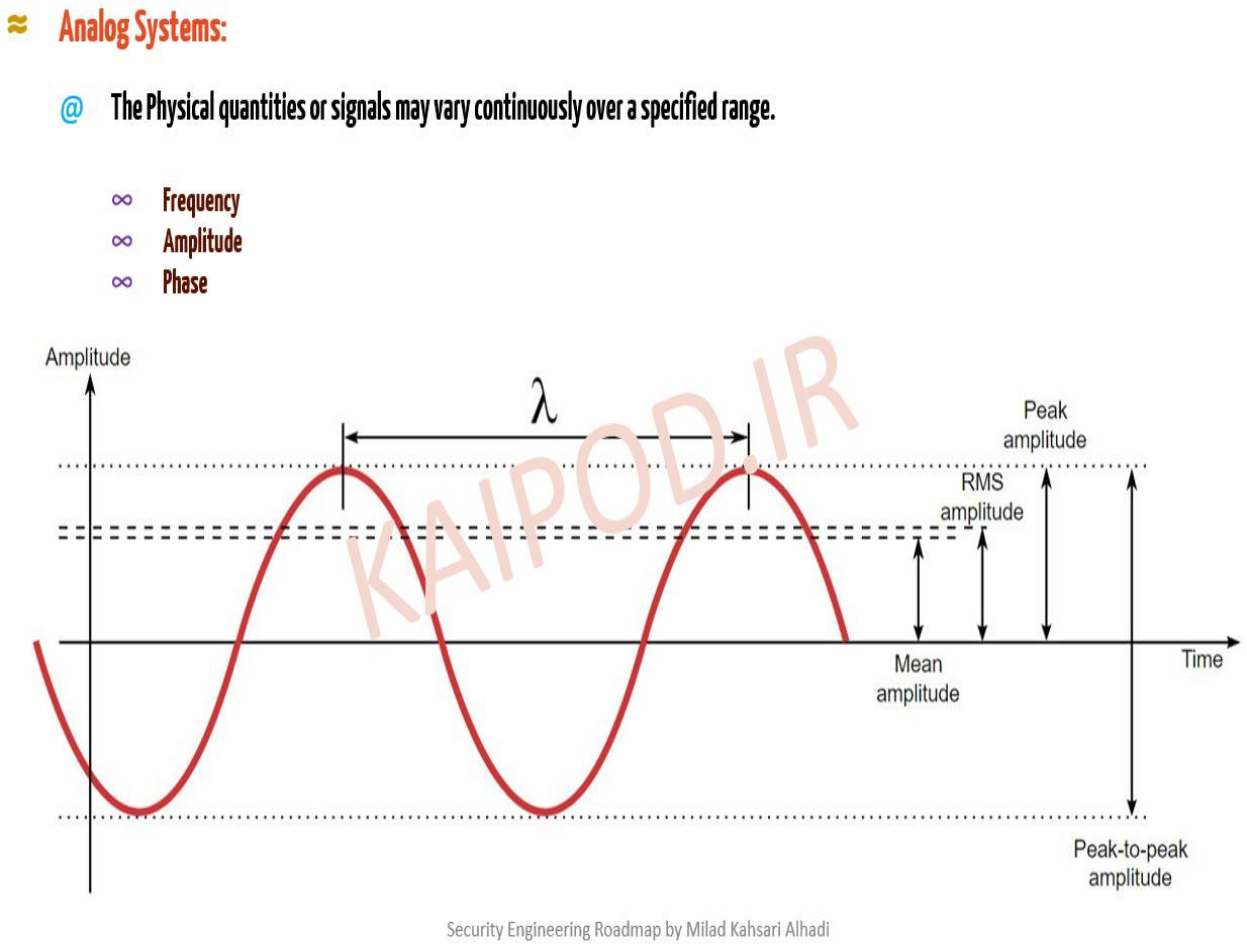
---

[1] Analog and Digital Signals
[2] Frequency
[3] Amplitude
[4] Phase
[5] Modulation and Demodulation
[6] Wireless
[7] Wired

۲. **دامنه یا حوزه:** همانطور که پیش از این ذکر شد، هر سیگنال آنالوگ تابعی از زمان است و مطابق شکل ۶ می‌تواند بر حسب ولت بیان شود. به عبارت دیگر دامنه یک سیگنال آنالوگ مقدار ولتاژ آن در هر لحظه است. در سیستم واحدهای SI، ولتاژ با ولت اندازه‌گیری می‌شود.

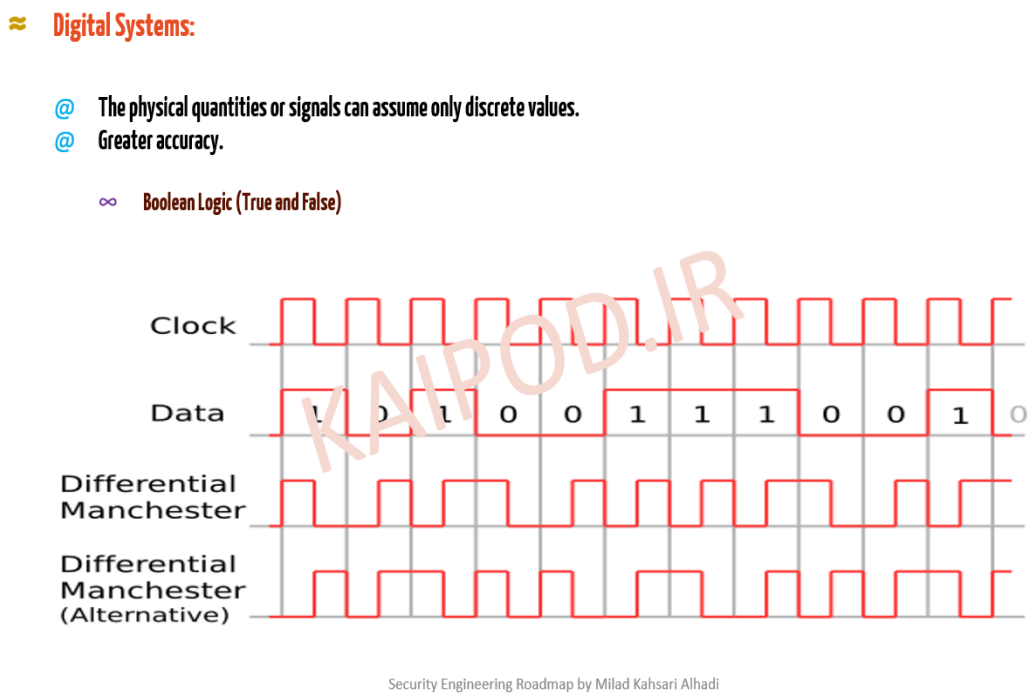
۳. **فاز:** دو سیگنال با فرکانس یکسان می‌توانند دارای اختلاف فاز باشند. یعنی یکی از سیگنال‌ها در لحظه‌ای متفاوت با دیگری شروع می‌شود. این تفاوت را می‌توان برحسب درجه از ۰ تا ۳۶۰ درجه بیان کرد.

شایان ذکر است، در تصویر شماره ۱۸ یک سیگنال آنالوگ نمایش داده شده است که در زمان و دامنه پیوسته است، به همین دلیل می‌تواند بی‌نهایت حالت داشته باشد. این نکته قابل ذکر است، تغییرات داده‌هایی که سیگنال‌های آنالوگ حمل می‌کنند اغلب با تغییر منبع ولتاژ مشخص می‌شوند.



تصویر ۱۸: مشخصات یک سیگنال الکتریکی / مخابراتی

اما برخلاف سیگنال‌های آنالوگ، سیگنال‌های دیجیتالی در زمان پیوسته ولی در دامنه ناپیوسته هستند (حالت محدود دارند)، به همین دلیل در دیجیتال فقط دو حالت صفر یا یک می‌توانند وجود داشته باشند. چون ۰ و ۱ فقط دو حالت هستند، یعنی یک سیگنال دیجیتالی در لحظه فقط می‌تواند یکی از این دو حالت صفر یا یک را داشته باشد.



تصویر ۱۹: سیگنال‌های دیجتالی

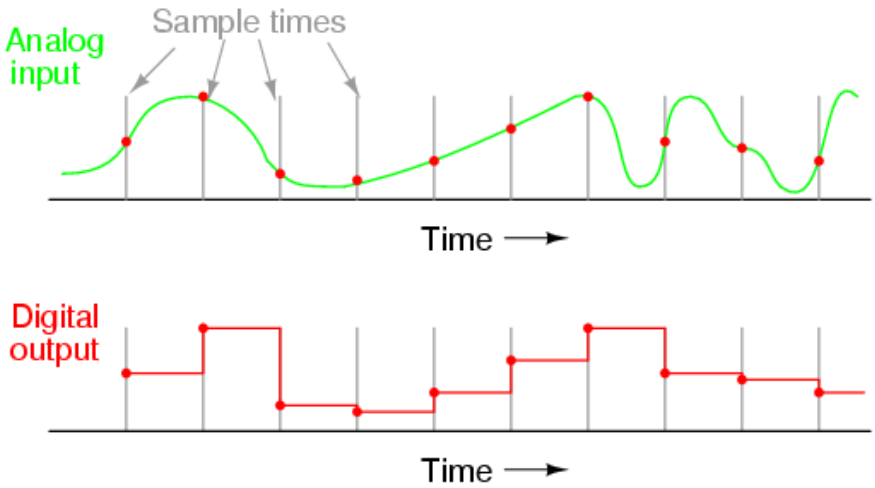
در تصویر ۱۹، ساختار یک سیگنال دیجیتال نمایش داده شده است که در بردار زمان پیوسته و در بردار دامنه ناپیوسته است. همچنین در تصویر ۱۹ کدگذاری سیگنال دیجیتال با روش منچستر و منچستر تفاضلی هم نمایش داده شده است که مبحث کدگذاری سیگنال‌ها محل بحث ما در این مقاله نیست.

تبدیل سیگنال‌های آنالوگ به دیجیتال

سیگنال‌های دیجیتالی در حقیقت از نمونه‌برداری[1] و کوانتیزه‌سازی[2] سیگنال‌های آنالوگ با استفاده از تراشه‌های مبدل آنالوگ به دیجیتال (A/D) استخراج می‌شوند. شایان ذکر است، نمونه‌برداری، یکی از مهم‌ترین مراحل فرایند تبدیل سیگنال آنالوگ به دیجیتال است. در پردازش سیگنال اثبات می‌شود که حداقل فرکانس

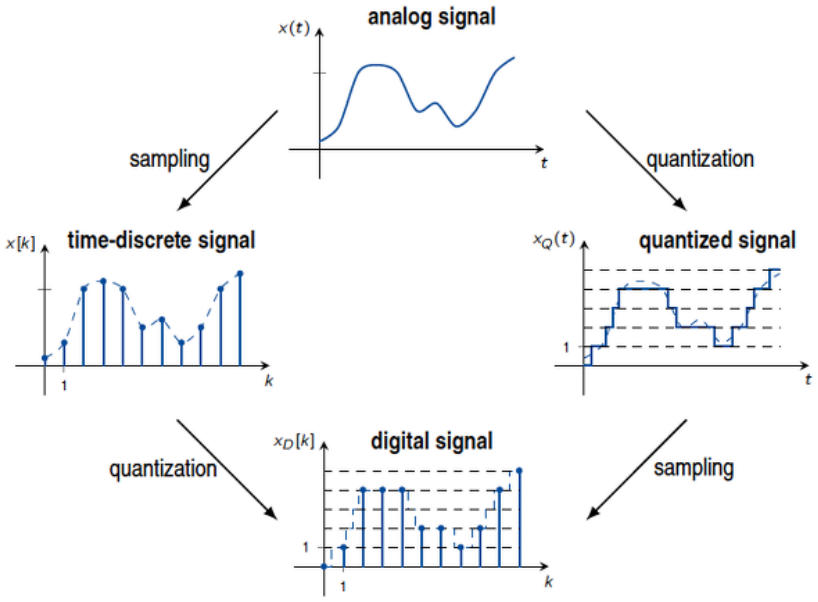
[1] Sampling
[2] Quantization

نمونه‌برداری می‌بایست دو برابر پهنای باند فرکانسی سیگنال نمونه‌برداری شده باشد تا بتوان سیگنال پیوسته را از سیگنال نمونه‌برداری شده بازسازی نمود. در تصویر ۲۰، نمونه‌برداری از یک سیگنال آنالوگ نمایش داده شده است.



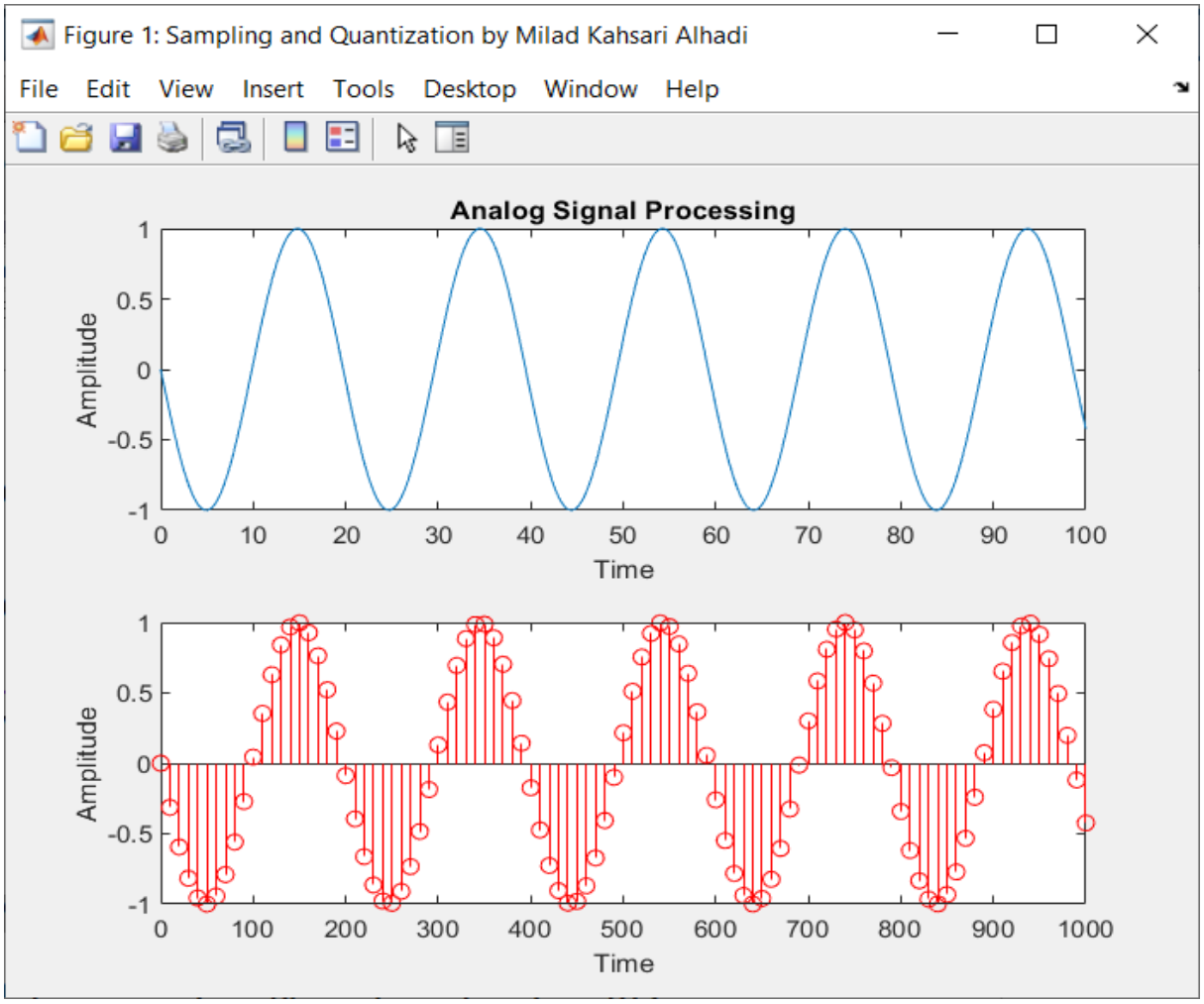
تصویر ۲۰: نمونه‌برداری از سیگنال آنالوگ

همچنین برای اینکه بتوان سیگنال گسسته را دیجیتال‌سازی کرد، باید به مقادیر خاصی آن را محدود ساخت. به عملیات محدودسازی سیگنال گسسته کوانتیزه‌سازی یا کمینه‌سازی گویند. دلیل کوانتیزه‌سازی یک سیگنال گسسته آن است که دستگاه‌های کنونی قدرت تشخیص صددرصد یک سیگنال و ذخیره‌سازی آن را ندارند.



تصویر ۲۱: نمونه‌برداری و کمینه‌سازی سیگنال و تبدیل آن به دیجیتال

در تصویر ۲۲، نمونه‌برداری و کمینه‌سازی و در نهایت تبدیل یک سیگنال آنالوگ به یک سیگنال دیجیتالی در محیط متلب نمایش داده شده است.



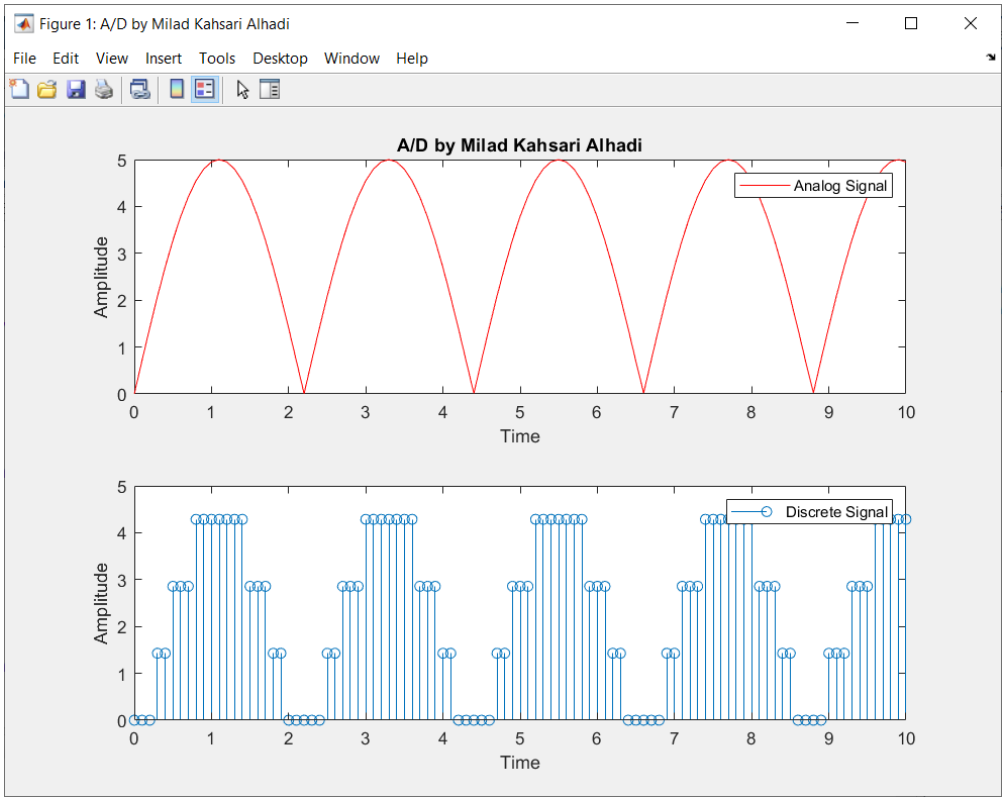
تصویر ۲۲: نمونه‌برداری از سیگنال آنالوگ

در ادامه بعد از استخراج سیگنال دیجیتال از سیگنال آنالوگ با استفاده از تکنیک‌های نمونه‌برداری و کمینه‌سازی، صفر و یک منطقی در سیگنال‌های دیجیتال با تعیین ولتاژ پایین و بالا در سطح مدارهای الکتریکی مشخص خواهند شد. حال اینکه ولتاژ پایین و بالا چیست در ادامه به آن پرداخته‌ایم.

ولتاژ پایین و بالا[1]

در هر کدینگ دیجیتالی، یک محدوده مشخص به دو قسمت تقسیم می‌شود. قسمتی به نام ولتاژ بالا (HV) و قسمتی به نام ولتاژ پایین (LV) شناخته می‌شود. اگر ولتاژ سیگنال در محدوده ولتاژ بالا باشد، حالت آن سیگنال به عنوان یک منطقی و اگر در محدوده ولتاژ پایین باشد حالتش صفر منطقی خواهد بود.

در تکنولوژی‌های مختلف مدارات دیجیتالی[2]، قراردادی که برای ولتاژ بالا و ولتاژ پایین تعیین کرده‌اند، متفاوت است، مثلاً در مدارات نیم‌رسانای اکسید–فلز مُکمِّل[3] که در کامپیوتر استفاده می‌شوند، محدوده ولتاژ پایین از صفر ولت تا ولتاژ منبع تغذیه تقسیم بر ۲ و محدوده ولتاژ بالا از ولتاژ منبع تغذیه تقسیم بر ۲ تا خود ولتاژ منبع تغذیه است، یعنی اگر ولتاژ تغذیه ۵ باشد، از ۰ تا ۲.۵ ولت به عنوان صفر منطقی و از ۲.۵ تا ۵ ولت به عنوان یک منطقی شناخته خواهد شد.



تصویر ۲۳: مدل‌سازی یک سیگنال آنالوگ

[1] Low and High Voltage
[2] Digital Circuits
[3] Complementary Metal-Oxide Semiconductor, CMOS

در تصویر ۲۳، مبحث کدینگ سیگنال‌های دیجیتال نمایش داده شده است. در این طرح شماتیک، سیگنال‌هایی که دارای ولتاژی مثبت ۲.۵ ولت هستند، به عنوان یک و سیگنال‌های دارای ولتاژ پایین‌تر از ۲.۵ ولت به عنوان صفر در نظر گرفته می‌شوند.

برای درک بهتر نحوه عملکرد این دو نوع سیگنال، فرض کنید که قصد ضبط صدا، ذخیره و پخش صدای ذخیره شده را داشته باشیم. برای ضبط صدا از یک میکروفون استفاده می‌کنیم که بسته به ضربه صوتی که به آن زده می‌شود، سیگنال‌های آنالوگی را تولید می‌کند که برابر صدای دریافتی است. ما نمی‌توانیم آنالوگ را بر روی حافظه‌های جانبی کامپیوتر ذخیره کنیم چون مثلاً دیسک سخت، در هر مکان ذخیره داده مثل یک آهنربا دو حالت دارد: صفر یا یک.

در حافظه‌های فلش نیز چنین است یا ترانزیستورها به اصطلاح باز یا بسته هستند، یعنی یا صفر یا یک هستند. حافظه‌های جانبی می‌توانند داده‌های دیجیتالی را ذخیره کنند اما ورودی ما آنالوگ است، در این میان یک مبدل آنالوگ به دیجیتال[1]، داده‌های آنالوگ را معادل‌سازی کرده و در قالب دیجیتال به حافظه جانبی می‌فرستد و در آن‌جا به عنوان صفر و یک‌های منطقی ذخیره می‌شوند.

در هنگام پخش صدا نیز داده‌های باینری از روی حافظه خوانده شده و به چیپی که وظیفه تبدیل داده‌های دیجیتالی به آنالوگ[2] را دارد، تحویل داده می‌شود. حال که داده‌هال آنالوگ صدا در اختیار ماست، کافیست با استفاده از یک تقویت کننده صدا را بلندتر کرده و به اسپیکر یا هر خروجی صدای دیگری ارسال کنیم. در اسپیکر هم لرزاننده هوا با توجه به قدرت سیگنال آنالوگ در لحظه، به هوا ضربه وارد کرده و در نتیجه به گوش ما می‌رسد.

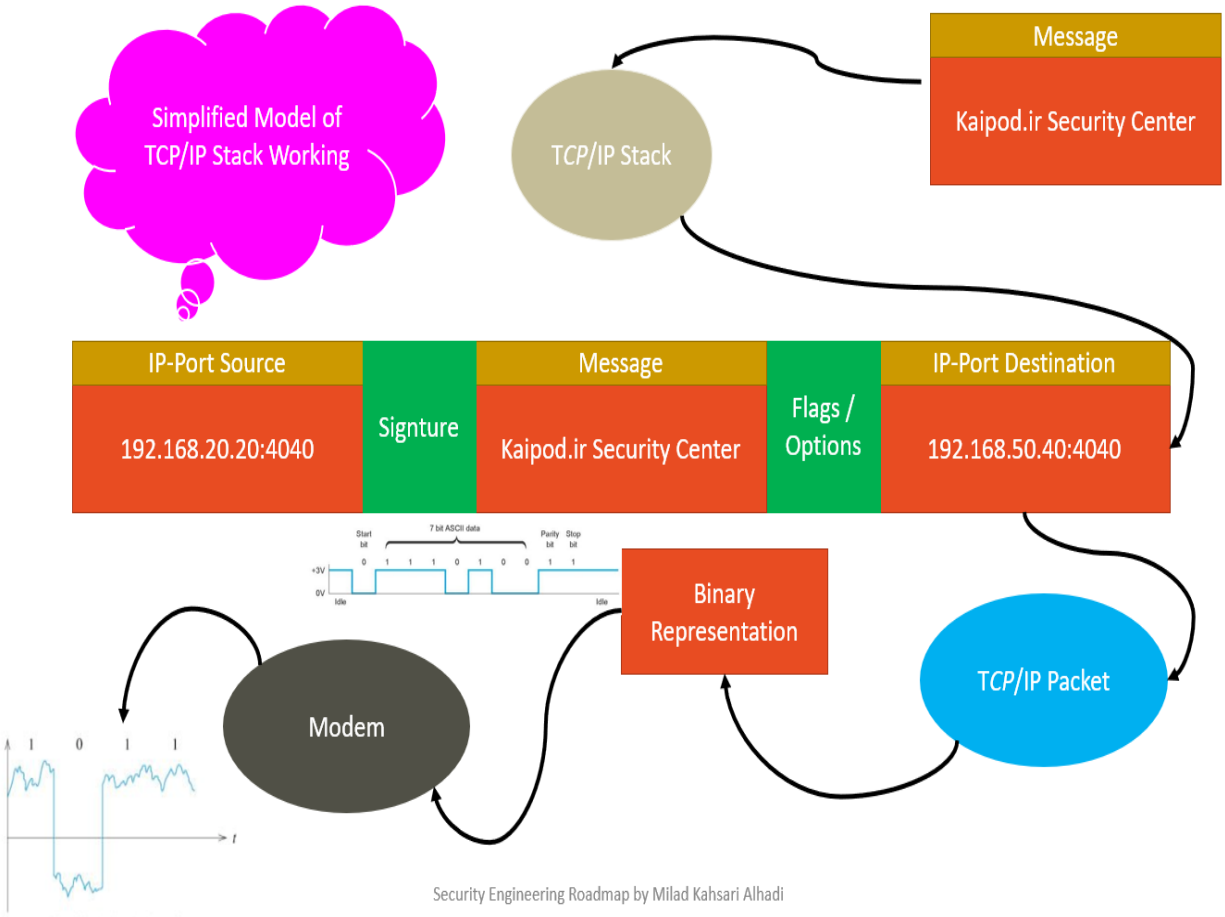
پشته پروتکل شبکه[3]

تاکنون متوجه شده‌ایم که در سامانه‌های کامپیوتری مدرن سیگنال چیست و چه خصوصیت‌هایی دارد. همچنین در مورد تبدیل سیگنال‌های آنالوگ به سیگنال‌های دیجیتال اندکی صحبت کردیم. مسئله‌ای که در این قسمت به آن خواهیم پرداخت، ارسال سیگنال‌ها از طریق یک کانال رسانای مخابراتی است.

---

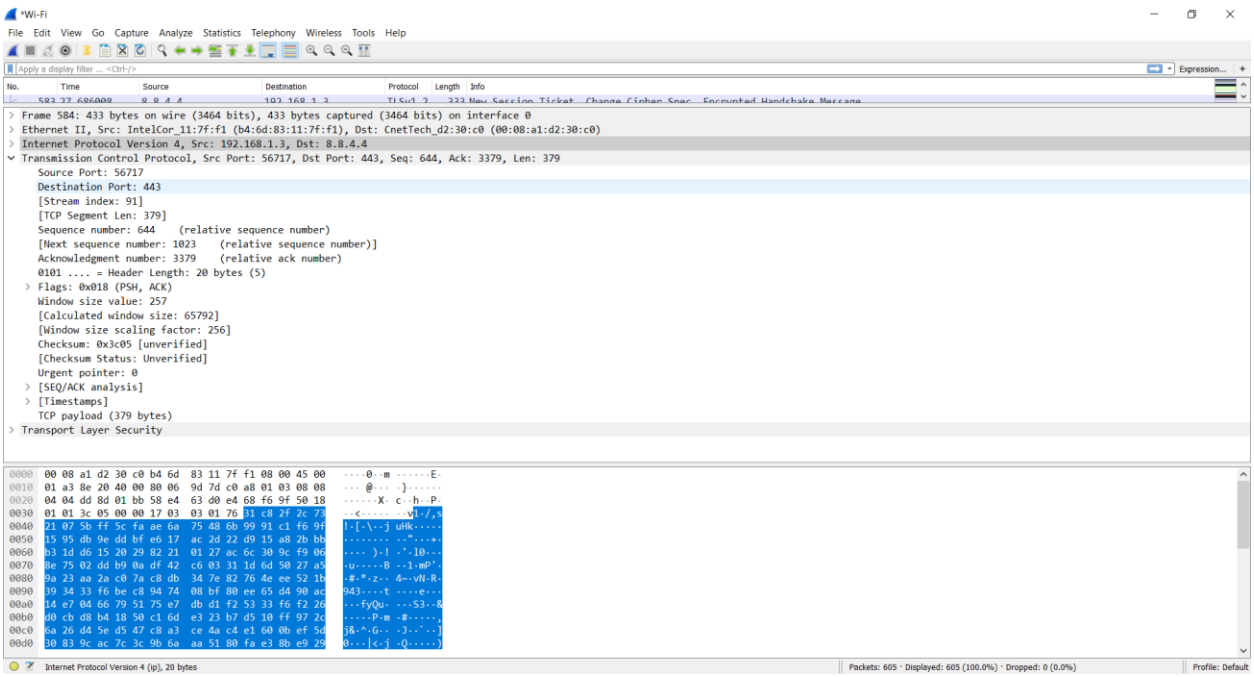
[1] A/D
[2] D/A
[3] Network Protocol Stack

در تصویر ۲۴، به صورت خیلی ساده مراحلی که یک پیام بعد از ایجاد در یک سیستم کامپیوتری باید طی کند که آماده ارسال توسط یک مودم به یک گره دیگر شود، نمایش داده شده است. البته این مدل با هدف نمایش ساده‌سازی شده است تا فقط حامل مفهوم انتقال اطلاعات باینری در سطح کامپیوترها باشد، در حالیکه اصل انتقال اطلاعات در سامانه‌های کامپیوتری بسیار پیچیده‌تر است.



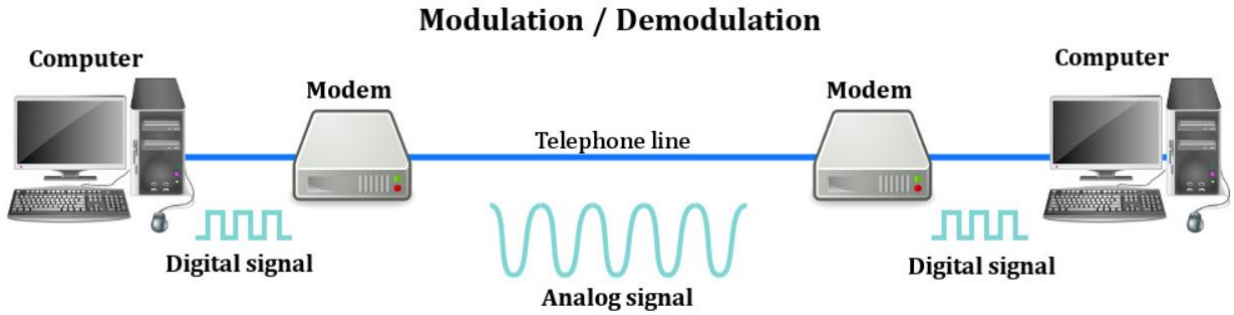
تصویر ۲٤: مراحل آماده‌سازی یک پیام برای ارسال

در تصویر ۲۴، یک برنامه کاربردی پیامی با محتوای (Kaipod.ir Security Center) ایجاد کرده است. این پیام برای اینکه آماده ارسال به ماشین دیگر شود، باید از لایه‌های پشته TCP/IP بگذرد، و در هر لایه اطلاعات تکمیلی به آن از قبیل آدرس ماشین مقصد، درگاه پذیرنده پیام ماشین مقصد، نوع برقراری ارتباط، اندازه پاکت، شماره پاکت‌ها و ... افزوده شود تا در نهایت یک پاکت شبکه مبتنی بر استاندارد TCP/IP شکل بگیرد.



تصویر ۲۵: نمای کلی یک پاکت شبکه **TCP** به صورت باینری و تفسیر شده

پس از اینکه پاکت شبکه TCP/IP ایجاد شد، و اطلاعات ماشین مقصد و دیگر اطلاعات مورد نیاز برای مسیریابی و اعتبارسنجی پاکت شبکه به آن افزوده شد، پاکت شبکه به مودم انتقال داده می‌شود و در نهایت پاکت شبکه توسط مودم تبدیل به سیگنال‌های الکتریکی آنالوگ خواهد شد و از طریق کانال مخابراتی (خطوط شبکه PSTN یا باندهای فرکانسی LTE) و تجهیزات شبکه میانی مانند مسیریاب‌ها[1] و سوییچ‌های[2] شبکه به ماشین دیگر مسیریابی و ارسال می‌شود.



تصویر ۲۶: نمای کلی از عملکرد مودم

[1] Routers
[2] Switches

انواع حملات ایرگپ

در قسمت قبل به شکل ساده مبحث سیستم‌های کامپیوتری و اصول مخابراتی را مورد بررسی قرار دادیم. در این قسمت به این مسئله خواهیم پرداخت که در حملات ایرگپ چطور مهاجمین می‌توانند تبادل اطلاعات انجام بدهند، بدون اینکه بین دو ماشین رابط یا کانال ارتباطی سنتی وجود داشته باشد.

همانطور که تاکنون متوجه شدیم، وقتی یک پیام از ماشین A به ماشین B بخواهد ارسال شود، باید مراحل پشته TCP/IP را طی کند، تا در هر مرحله اطلاعات تکمیلی به آن پیام اضافه شود که در نهایت بتوان آن را به ماشین مقصد ارسال و مسیریابی کرد. ولی اگر دو ماشین با یکدیگر راه ارتباطی نداشته باشند، به عنوان مثال یکی از طرفین به شبکه PSTN متصل نباشد، ارتباط صورت نخواهد گرفت چون بین دو ماشین کانال ارتباطی برای رفت و آمد سیگنال‌های آنالوگ الکتریکی وجود ندارد.

در حملات ایرگپ همین مسئله مورد پژوهش قرار گرفته است که آیا امکان انتقال اطلاعات بین دو ماشین که هیچ نوع ارتباطی با هم ندارند، ممکن است یا خیر. در این پژوهش‌ها مبتنی بر اصول مخابراتی اثبات شد که تنها راه ارتباطی بین دو ماشین فقط خطوط PSTN یا باندهای فرکانسی LTE/GSM و ... نیستند، بلکه ما می‌توانیم پاکت‌های شبکه (در قالب باینری) را از طریق کانال‌های دیگر مانند ارسال سیگنال‌های نوری[1]، سیگنال‌های صوتی[2]، سیگنال‌های الکترومغناطیسی[3] و ... به شکل پخش همگانی[4] ارسال و توسط گیرنده‌های مخصوص دریافت کنیم. در جدول ۱، این پژوهش‌ها به صورت خلاصه آورده شده‌اند.

نوع	متد	مقاله
الکترومغناطیس	متد AirHopper – استفاده از فرکانس رادیویی FM	لینک[5]
	متد GSMem – استفاده از فرکانس های سلولی	لینک[6]
	متد USBee – استفاده از USB	لینک[7]
	متد Funthenna – استفاده از GPIO	لینک[8]

[1] Optical Signals
[2] Sound Signals
[3] Electromagnetical Signals
[4] Broadcasting
[5] http://bit.ly/2kK00sA
[6] http://bit.ly/2kTq840
[7] http://bit.ly/2krg7Lf
[8] http://bit.ly/2lZ2u6u

مغناطیس	متد Magneto– ایجاد میدان مغناطیسی توسط CPU	لینک[1]
	متد ODINI – گریز از محافظ فارادی	لینک[2]
برق	متد PowerHammer – استفاده از خطوط برق فشار قوی	لینک[3]
صوت	متد Fansmitter – نویز فن کامپیوتر	لینک[4]
	متد DiskFiltration – نویز دیسک سخت	لینک[5]
	متد MOSQUITO – ارتباط اسپیکر به اسپیکر	لینک[6]
حرارت	متد BitWhisper – انتشار حرارت	لینک[7]
نور	متد LED-it-GO – استفاده از LED	لینک[8]
	متد VisiSploit – استفاده از LEDهای پنهان	لینک[9]
	متد aIR-Jumper – استفاده از دوربین‌ها	لینک[10]

جدول ۱: انواع حملات ایرگپ

در ادامه یکی از این حملات را مورد بررسی قرار خواهیم داد که متوجه شویم در این حملات چه اتفاقی رخ می‌دهد و اینکه چطور می‌توان جلوی این نوع حملات را گرفت تا یک بدافزار نتواند در شبکه‌های ایزوله با یک ایجنت مخرب ارتباط برقرار کند و برای آن اطلاعات محرمانه را ارسال کند.

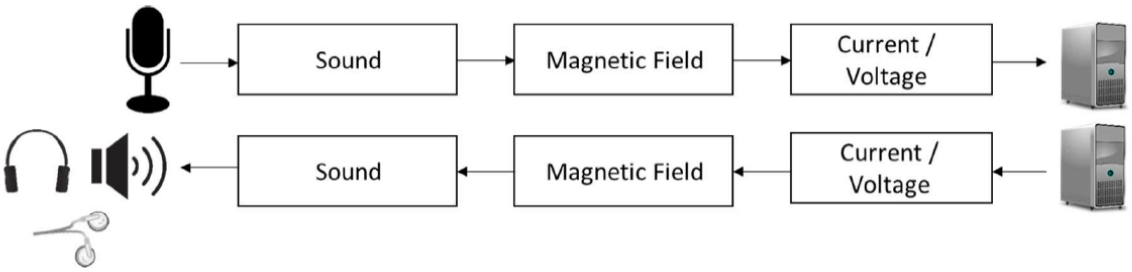
اصول بنیادی در حملات ایرگپ

در این قسمت حمله ایرگپ به واسطه کانال صوتی را مورد بررسی قرار خواهیم داد که به ما درک کلی از ماهیت این نوع حملات ارائه خواهد کرد. همانطور که در جدول ۱ نمایش داده شد، انواع حملات بر علیه شبکه‌های ایرگپ ارائه شده است. در هر یک از این حملات، شخص مهاجم می‌تواند از یک رسانای منحصربفردی برای ارسال و دریافت اطلاعات استفاده کند، اگرچه پیش نیاز تمامی این حملات آلودگی ماشین قربانی به بدافزار است تا در نهایت بدافزار بتواند اطلاعات محرمانه را به وسیله یک رسانای ارتباطی غیرمتعارف

[1] http://bit.ly/2kWYPpF
[2] http://bit.ly/2kK4a3G
[3] http://bit.ly/2kTtTGE
[4] http://bit.ly/2lWmAhH
[5] http://bit.ly/2mqmmzF
[6] http://bit.ly/2kvTVjg
[7] http://bit.ly/2mqvuEu
[8] http://bit.ly/2kWlDWp
[9] http://bit.ly/2kTu5pm
[10] http://bit.ly/2m0BDXE

به شکل پخش همگانی انتشار دهد. علاوه بر بدافزار، مهاجم نیازمند طراحی یک پشته شبکه به منظور ارسال، کدگذاری، و دریافت اطلاعات در سمت گیرنده و فرستنده است.

در هر صورت، مهاجمین برای اینکه بتوانند حملات ایرگپ را با موفقیت انجام بدهند، باید ابتدا بدافزاری را طراحی کنند که این بدافزار توانایی جمع‌آوری اطلاعات کاربردی از قبیل اعتبارنامه‌ها و ... را از سطح سیستم و همچنین انتقال اطلاعات جمع‌آوری شده از طریق یک کانال ارتباطی دیگر را داشته باشد. بدافزار برای اینکه بتواند اطلاعات جمع‌آوری شده خود را به واسطه کانال جانبی دیگر ارسال کند، نیازمند یک پشته شبکه جدید هم است که در آن قواعد ارسال و دریافت پاکت‌های شبکه به واسطه کانال جانبی مورد نظر به شکل صحیحی تعریف شده باشد.



تصویر ۲۶: کاربرد میکروفون و اسپیکر

به عنوان مثال، در حملات ایرگپ که از سیگنال‌های صوتی برای انتقال اطلاعات استفاده می‌شود، بدافزار طراحی شده با بهره‌برداری از آسیب‌پذیری تراشه صدا بر روی کامپیوتر سیگنالی‌های اطلاعاتی را در باند فرکانسی نزدیک به باند فراصوت[1] با استفاده از اسپیکرها به صورت پخش همگانی انتشار خواهد داد که گوش انسان قابلیت شنیدن صدا در این بازه فرکانسی را ندارد چون معمولاً بالاترین فرکانس شنوایی انسان حدود ۲۰ یا ۲۵ کیلوهرتز در نظر گرفته می‌شود و عملا انسان توانایی شنیدن صوت در باند فراصوت را ندارد. نقطه مقابل این امواج، امواج فروصوت یا هستند که دارای بسامد زیر حد پایین فرکانس شنوایی انسان (حدود ۲۰ هرتز) هستند.

در گام بعد کافی است یک موبایل دارای میکروفون یا هر وسیله‌ای که توانایی دریافت سیگنال‌های صوتی در باند فرکانسی فراصوت را دارد، سیگنال‌های صوتی ارسال شده در این باند فرکانسی را دریافت و در نهایت سیگنال‌های ارسال شده را آشکاری‌سازی کند. در نهایت اطلاعات نهفته شده در استریم ارسال شده توسط

[1] Ultrasound

بدافزار استخراج گردد. شایان ذکر است، وسیله ارسال سیگنال‌های صوتی در کانال فرکانسی فراصوت فقط توسط اسپیکرها نیست، بلکه در پژوهش‌های اخیر روش‌های دیگر برای ارسال این نوع سیگنال‌ها ارائه شده است که حتی با حذف اسپیکرها هم نمی‌شود جلوی این حمله را گرفت.

این اصول در تمامی حملات ایرگپ وجود دارد. ابتدا یک ماشین آلوده به بدافزار ایرگپ می‌شود، سپس آن بدافزار تلاش به ارسال پیام‌های سرقت شده از روی سیستم به واسطه سیگنال‌های صوتی، نوری و الکترومغناطیس و ... به صورت پخش همگانی خواهد کرد. در ادامه هر وسیله‌ای بتواند آن سیگنال را در کانال ارتباطی مورد نظر مهاجم رصد و دریافت کند، در نهایت خواهد توانست پیام ارسال شده توسط بدافزار را دریافت کند.

برای اینکه این ارسال پیام به شکل درستی صورت بگیرد، الگوریتم‌های زیادی به منظور همگام‌سازی گیرنده و فرستنده وجود دارد که در این مقاله قصد بررسی آن‌ها را نداریم. در هر صورت، بعد از ارسال و دریافت سیگنال‌ها مهاجمین می‌توانند بدون اینکه بین ماشین‌های دو کانال فیزیکی یا حتی وایرلس وجود داشته باشد، انتقال اطلاعات را به سبک یک ایستگاه فرستنده و گیرنده سیگنال‌های رادیویی انجام بدهند.

سخن آخر مقاله اول

با اینکه بدافزار استاکس‌نت به واسطه انجام حملات ایرگپ به درون ساختار هسته‌ای نطنز استقرار داده نشد، اما هنوز این حملات و تهدیدات نوظهور محیط سایبر مبتنی بر این حملات به عنوان یک مسئله امنیتی جدید مورد بحث هستند زیرا مهاجمین می‌توانند اکنون با انجام حملات ترکیبی و استفاده از روش‌های گوناگون یک بدافزار را وارد یک ساختار صنعتی ایزوله کنند و در نهایت به واسطه حملات ایرگپ در کانال‌های جانبی متنوعی به تعامل با بدافزار بپردازنند. اگرچه این حملات بسیار جدی هستند و تعداد بدافزارهای توسعه داده شده با محوریت حملات ایرگپ به صورت روزانه در حال رشد و توسعه هستند اما به هر صورت تمامی حملات ایرگپ را می‌توان با استفاده از رویکردهای امنیتی که توسط شرکت کی‌پاد مستندسازی شده است، جلوگیری کرد.