چهارمین کنفرانس ملی کامپیوتر ، فناوری اطلاعات و کاربردهای هوش مصنوعی
۱۵ بهمن ۱۳۹۹

مروری بر مخاطرات سایبری در سیستم‌های نظارت تصویری تحت شبکه و ارائه راهکار جهت توسعه امن سازی آن

سید علی صموتی [۱]، حسام حسن‌پور [۲]، علی خلیلی [۳]

[۱] مدرس دانشکده شهید شمسی‌پور ، دانشجوی دکتری مهندسی فناوری اطلاعات دانشگاه آزاد اسلامی
Ali.samouti@gmail.com
[۲] استادیار ، فناوری اطلاعات و کامپیوتر ، دانشگاه آزاد اسلامی ، سبزوار hesam_78@yahoo.com
[۳] پژوهشگر فناوری اطلاعات ، شرکت توسعه تجارت وب ، تهران Ali.khalili2@gmail.com

چکیده

سیستم‌های نظارتی مبتنی بر IP از تأسیسات صنعتی ، راه‌آهن ، پمپ‌بنزین‌ها و حتی خانه‌های شخصی محافظت می‌کنند.سیستم‌های نظارت تصویری به‌عنوان یک بخش بسیار مهم در اینترنت اشیا محسوب می‌شوند، اما این پیشرفت سبب شده است که حملات و تهدیدهای متنوعی در کمین این سیستم‌ها قرار بگیرند. بنابراین ، دسترسی غیرمجاز به این سیستم‌ها پیامدهای جدی امنیتی را به همراه خواهد داشت. در این تحقیق، در بدو امر و در نخستین گام عوامل تهدید بررسی‌شده‌اند و در گام بعد به تشریح و تحقیق و لیست بندی اهداف حمله پرداختیم، در گام سوم حملات عملی حملات مطرح‌شده در مقالات دیگر، اشاره و نمونه‌ای از حملات توسط نویسندگان که به مرحله ظهور رسیده است، تشریح گردیده است. در گام چهارم ضمن بررسی نتایج احتمالی حمله به روش‌های پایداری سیستم در بحران اشاره می‌گردد. در بخش انتهایی بردارهای حمله را برای یک سیستم نظارتی بر اساس برخی از مستندات اشاره خواهد شد و یک بردار حمله بر اساس حمله عملی به یک سیستم توسط نویسندگان تشریح می‌گردد. معرفی برخی از امکانات سیستم‌های نظارت تصویری برای مقابله با این حملات و رفع حملات و ارائه سناریو بخش آخر این مقاله است. اقداماتی نظیر استفاده از کانال امن SSH و امن سازی از طریق سناریوهای HA (High Availability) و امن سازی دسترسی 802.1x و بررسی روش‌های دسترسی دهی AAA برای معماری سیستم‌های نظارت تصویری ازجمله مواردی است که برای امنت سازی یک سیستم نظارت تصویری امن به آن اشاره می‌شود.

واژه‌های کلیدی : حملات دوربین مداربسته، تهدیدهای دوربین تحت شبکه ، حمله منع سرویس دوربین مداربسته،

۱- مقدمه

این روزها سیستم‌های نظارت تصویری را می‌توان در همه‌جا، ازجمله در خیابان‌ها ، ایستگاه‌های قطار ، محل کار ، کارخانه‌ها و حتی در خانه‌ها یافت. برنامه‌های هوشمند ، شبکه‌های نظارتی بزرگ را برای مدیریت کاربردهای عملی ایجاد کرده‌اند. به‌عنوان‌مثال ، فناوری شناسایی چهره ، شناسایی تهدیدها ، تشخیص رویداد ، ردیابی اشیا، و بررسی سریع حوادث ، می‌تواند در هزاران دوربین در مناطق وسیع جغرافیایی گسترش یابد. طی چند دهه گذشته ، فن‌آوری‌های نظارتی از سیستم‌های آنالوگ به سیستم‌های تحت شبکه تبدیل‌شده‌اند. علاوه بر این ، سیستم‌های نظارت تصویری به دلیل محبوبیت و گسترده بودن اینترنت اشیا (IoT) مقرون‌به‌صرفه می‌باشند.

متأسفانه در سال‌های اخیر ، این سیستم‌ها و اجزای آن‌ها هدف حملات سایبری قرارگرفته‌اند. به‌عنوان‌مثال ، آن‌ها هدف حملات منع سرویس توزیع‌شده (DDoS) قرارگرفته، و برای حمله به حریم خصوصی کاربران و حتی استخراج ارزهای رمز پایه مورد سو استفاده قرارگرفته‌اند. این سیستم‌ها همچنین برای انجام اقدامات مخرب در بات نت‌ها استخدام‌شده‌اند. [۱]

بسیاری از سازندگان و رهبران صنعت امنیت نظارت تصویری برای راهکارهای امن سازی سایبری سیستم‌های نظارت تصویری گزارش‌های جالب را عرضه کرده‌اند، شرکت جنتک خسارت‌های سایبری را بر اساس مؤسسات مالی کانادا ۳۷۵ تا ۵۷۵ میلیارد دلار تخمین زده‌اند و معتقد است ۲۰۵ روز طول می‌کشد تا نشت اطلاعات شناخته شود و ۳۲٪ شرکت‌های مبتنی بر فناوری اطلاعات معتقد هستند که به امنیت بهایی نمی‌دادند و معتقد بودند حمله برای شرکت‌های دیگر است. در همین گزارش آمده است ۱,۵ بیلیون دوربین تحت حمله DDoS در سال ۲۰۱۶ قرارگرفته است و ۶۶۵ گیگابایت ترافیک برای حملات منع سرویس تخمین زده‌شده است. [۲] از سویی دیگر شرکت IPVM که به‌عنوان منبع و مرجع سیستم‌های نظارت تصویری محسوب می‌شود، گزارش‌های دیگری را درزمینهٔ اهمیت نگرش به امن سازی سیستم‌های نظارت تصویری ارائه کرده است. [۳] از سویی دیگر شرکت‌های اکسیس و بوش به‌صورت جداگانه، روش‌های امن سازی سیستم‌های نظارت تصویری را منحصراً به پیاده‌سازی روش‌های چندگانه سوق می‌دهند. [۴, ۵]

برای حفظ امنیت اطلاعات در سامانه‌های نظارت تصویری باید از سه منظر به این موضوع نگریست : [۱, ۴, ۵]

۱. دسترسی به شبکه ۲. امنیت انتقال ۳. امنیت سرور و پایگاه ذخیره‌ساز . درمجموع، اطلاعات ذخیره‌شده شامل تصاویر ، اطلاعات کاربران (نام کاربری و رمز عبور) ، کلمه عبور دوربین‌ها و لاگ‌های سیستم و .. است ، باید این اطلاعات از در دسترسی غیرمجاز مخفی نگه‌داشته شده و از تغییر حفظ گردند. این اطلاعات باید در زمان موردنیاز در دسترس قرار گیرند. در این سیستم‌ها با توجه به اصول CIA و AAA باید داده‌های دیگر ما که رشته تصاویر هستند به‌طور دقیق با نگرش مناسب امن سازی شوند و دسترسی به این داده‌ها بر اساس مکانیسم خاصی مدیریت شود. [۶-۸]

جایگاه‌ها ، داده‌ها و تصاویر حکم اصلی دارایی را دارند. در سیستم‌های گذشته با محدودسازی دسترسی و محدودسازی شبکه دارایی‌ها در دسترس افراد محدودی بود و فقط با کنترل دسترسی گامی برای امنیت برداشته می‌شد، اما اینک با گسترش شبکه‌های سلسله مراتبی و پدر فرزندی federation نمی‌توان انتظار محدودسازی شبکه را داشت و باید به اصول امنیت شبکه پناه برد. [۵, ۹]

در این مقاله ، امنیت سایبری سیستم‌های نظارتی مدرن را مرور خواهیم کرد. در ابتدا معماری و توپولوژی سیستم‌های مدرن نظارت تصویری کار را تشریح می‌گردد. در مرحله بعدی اهداف یک مهاجم را با توجه به تأثیر آن‌ها بر محرمانه بودن ، صحت داده و در دسترس بودن سیستم، بررسی می‌گردد. پس‌ازآن ، خواهیم فهمید که چگونه یک مهاجم می‌تواند از طریق چندین مرحله حمله شامل شناسایی آسیب‌پذیری و عوامل تهدید مختلف و سو استفاده از اقدامات مخرب ، به هدف خود می‌رسد. در بخش آخر شیوه‌ها و راهکارهای امنیتی شناخته‌شده را بررسی خواهیم کرد که می‌تواند برای کاهش تهدیدات سایبری استفاده شود.

۲- طبقه‌بندی و بررسی معماری امنیت سیستم‌های نظارت تصویری

امنیت سیستم‌های نظارت تصویری در مرحله با امنیت اینترنت اشیا یکسان به نظر می‌آید، اما وقتی با مفاهیم CPS همسو می‌گردد، اهمیت آن بسیار بیشتر می‌گردد. دلیل این امر آن است که سیستم‌های نظارت تصویری، سیستم‌های فیزیکی سایبری هستند. [۱۰] آن‌ها

عملاً امنیت فیزیکی ما را پشتیبانی و اجرا می‌کنند. هنگام بررسی و مقایسه ، امنیت فیزیکی و امنیت از جوانب دیگر، به دلیل حس امنیت و آرامش برای انسان، این نوع امنیت اهمیت بالایی دارد. [۱۱-۱۴] در این نوع سیستم‌ها فلسفه امنیت متفاوت است و عوامل تهدید، دارایی ، توپولوژی و انگیزه متفاوت به نظر می‌رسد. [۱]

عاملان تهدید (چه کسی): هدف مهاجمان برای بهره‌برداری از کاربری یا اطلاعات این سیستم‌ها است و یا هدف آن‌ها می‌تواند بهره‌کشی از منابع پردازنده باشد. نمونه از هدف مهاجمان سو استفاده از تصاویر ضبط‌شده و شناسایی محل برای اهداف بعدی است. (نظیر اهداف تروریستی است) [۳, ۱۵]

دارایی‌ها (چه چیزهایی): در صورت به خطر افتادن این سیستم‌ها می‌توانند تصاویر خصوصی شخصی را در اختیار مهاجم قرار دهند که منجر به نقض مستقیم حریم خصوصی می‌شود در بسیاری از استانداردها حریم شخصی و دوربین مداربسته الزاماتی را برای بهره‌برداری تدوین نموده است. [۷] هرچند این مسئله نیز از دید الزامات استاندارد ایزو۲۷۰۰۰ نیز زیر ذره‌بین رفته است. [۱۶, ۱۷]

این سیستم‌ها همچنین دارایی‌های پردازشگرانه سودآوری برای دارندگان بات نت (بلاک چین) دارند، زیرا معمولاً دارای منابع پردازنده قوی و پهنای باند بالا (برای حملات DDoS) و قابلیت بالای محاسبات مناسب (برای استخراج بیت کوین) هستند. [۱, ۱۸, ۱۹]

توپولوژی (کجا مورد هدف قرار گیرد): برخلاف سایر توپولوژی و معماری‌های اینترنت اشیا، سیستم‌های نظارتی اغلب سیستم‌های متمرکز متصل به یک سرور هستند. آن‌ها همچنین فقط به یک شبکه مجزا معمولاً به اینترنت (اینترانت) و یا یک شبکه خصوصی داخلی (LAN/CAN) متصل می‌شوند - درنتیجه یک بردار نفوذ بالقوه را نشان می‌دهد. [۱, ۱۰]

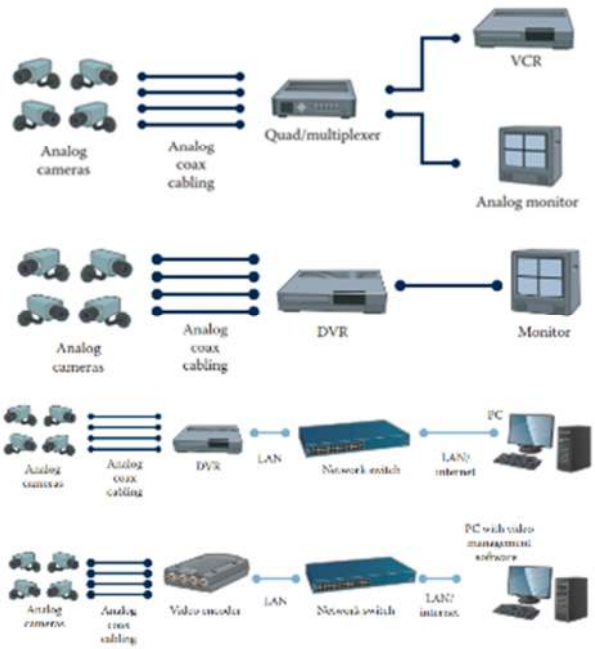
انگیزه (چرا): سیستم‌های نظارت تصویری علاوه بر تداخل با شبکه‌های دیگر نظیر شبکه‌های داده و یا اسکادا [۲۰] ، می‌تواند اهداف باج افزاری، جاسوس‌افزاری، ترس‌افزاری نیز داشته باشد. [۳] به‌جز موارد فوق، یک مهاجم از سیستم قربانی برای حملات منع سرویس به‌عنوان زامبی استفاده می‌نماید و یا برای نفوذ فیزیکی به منطقه با استفاده از تصادم و یا اختلال و یا دوباره ارسال کردن تصاویر دوربین همان منطقه ، سبب مختل شدن استریم در یک منطقه می‌شود و به هدف تروریستی و یا دزدی دست می‌یابد. [۳, ۱۵, ۲۱]

بردارهای حمله (چگونگی): سیستم‌های نظارت تصویری به دلیل ضعف در آسیب‌پذیری روز صفرم همیشه نقصان‌هایی دارند. [۲۲] به‌عنوان‌مثال ، ویدیو سرورها (انکدرها) معمولاً سعی می‌کنند از نوع پلتفرم باز و سازگار با مدل‌های مختلف دوربین باشند تا دوربین آنالوگ را به دوربین تحت شبکه تبدیل و استریم تصاویر را به استریم شبکه تبدیل کنند. [۱, ۹, ۱۵] درنتیجه ، این سرورها اغلب از مجموعه رمزنگاری/کدگذاری منسوخ‌شده استفاده می‌کنند که با توجه به کارکرد مبتنی بر خود معرف (خود تائید کننده گواهی‌نامه) می‌تواند سبب حمله مردمیانی شود.

در این مقاله ضمن تشریح معماری سیستم‌های نظارت تصویری، آسیب‌پذیری و ریسک‌ها تشریح و لیست می‌شود و بر اساس تجارت نویسندگان حملات آزمایشگاهی تشریح خواهد شد. امید است با شناسایی معماری و فلسفه حملات سایبری در این حوزه بتوان، اقدامات اساسی را به‌صورت بنیادین نهادینه کرد.

۳- بررسی اجمالی سیستم

سیستم‌های نظارت تصویری سابقه طولانی داشته‌اند و از Watchmanها شروع و با گذر از آنالوگ به سیستم‌های شبکه رسیده‌اند. در شکل ۱ معماری کلی سیستم‌های نظارت تصویری را از گذشته تاکنون نمایش داده‌شده است. [۹, ۲۱]



شکل ۱- معماری سیستم‌های نظارت تصویری و مکان‌های آسیب‌پذیر

بررسی اجمالی : هنگامی‌که صحبت از سیستم‌های نظارت تصویری می‌شود، برای بحث امنیت و پیاده‌سازی آن باید از چهار منظر به آن نگریست. این چهار منظر عبارت‌اند از : نوع نیاز و یا هدف ، روش پیاده‌سازی سیستم و مخاطرات آن، توپولوژی و حفاظت. [۱] البته برخی مراجع امنیت را فقط به بستر و پروتکل معطوف کرده‌اند و ابعاد نیاز را نادیده گرفته‌اند. [۳-۵, ۲۳]

۳-۱- هدف:

هدف سیستم نظارت تصویری به نیاز کاربر بستگی دارد. گاهی نیاز احراز هویت است و در برخی مواقع تشخیص و در گام آخر نیاز کنترلی است. [۹, ۲۳] در برخی مراجع هدف و آسیب‌پذیری‌ها را به‌صورت لیست زیر گرداوری کرده‌اند : [۱, ۹, ۲۴]

اجرای قانونی: قوانین اصناف برای برخی از مشاغل الزام این سیستم‌ها را سبب می‌شود، پس قوانینی وجود دارد تا برای شناسایی در سرقت از تصاویر بهره بگیرند. [۲۵]

مانیتورینگ (نظارت): کاربران سیستم نظارتی را برای نظارت کودکان و یا کهن‌سالان و یا امنیت منزل نصب می‌کنند.

قابلیت شناسایی (ردیابی): مدیر یک کارخانه برای رصد کردن خط تولید.

عملیات: مدیر پروژه برای نظارت پیشرفت کار از دوربین بهره می‌گیرد.

بازدارندگی : نصب دوربین یا نمونَک دوربین برای پیشگیری و ترساندن مجرم یا سارق یا نفوذ گر.

۳-۲- پیاده‌سازی :

مدیریت سیستم و جمع‌آوری تصاویر دوربین‌ها و ارسال آن بر ویدیو وال و یا کاربر دیگر بر نوع امن سازی تأثیر بالایی دارد. در برخی از سناریوها به سراغ nvr/dvr می‌روند و در برخی دیگر از سرور استفاده می‌کنند و نرم‌افزارهای VMS و CMS را روی آن بهره‌برداری می‌کنند. [۹, ۲۱] درروش سرور برای امن سازی از روش‌های متفاوت می‌توان استفاده کرد و بر اساس استانداردهای موجود چهار راهکار می‌تواند پیاده‌سازی شود: امن سازی مبتنی بر سرور، امن سازی مبتنی بر کلاینت، امن سازی انتها به انتها و امن سازی نقطه‌به‌نقطه [۲۶] . اما از سویی

دیگر در [۲۱] پیاده‌سازی بر اساس هوشمند سازی نیز اشاره‌شده است و در آن اشاره‌ای بر یادگیری عمیق گردیده است و در [۱] پیاده‌سازی سیستم را به دودسته زیر تقسیم‌شده است.

مانیتورینگ: این مانیتورینگ و نظارت بر استریم ویدیو دارد. نظارت می‌تواند به‌صورت مستقیم از دوربین به نمایشگر و یا از دستگاه مدیریت NVR/DVR/CMS/VMS به نمایشگر و یا از طریق اینترنت (انتقال تصویر) و یا از بستر کلود و یا از طریق P2P باشد . تجزیه‌وتحلیل تصاویر به دو فرم انسانی و هوشمند صورت می‌گیرد. هوشمند ساری‌های متنوعی عرضه‌شده‌اند که می‌توان به موارد زیر اشاره کرد: تشخیص حرکت ، یا برنامه‌های پیشرفته مانند ردیابی اشیا ، تشخیص تصویر ، تشخیص چهره و تشخیص رویداد انجام می‌شود. در بسیاری از مستندات امنیت کلود و p2p بررسی‌شده‌اند و مزایا و معایب آن اشاره‌شده است. [۱, ۸, ۲۷]

ارتباطات: با توجه به بسترهای آنالوگ و تحت شبکه بستر می‌تواند به‌صورت مسی، رادیو ، فیبر و یا اینترنت باشد. با استفاده از روش‌های آنالوگ ، فیلم به‌صورت سیگنال آنالوگ به DVR ارسال می‌شود (که می‌تواند به اینترنت متصل می‌شود). در سیستم‌های تحت شبکه پس از فشرده‌سازی این ارتباط از tcp/ip تبعیت می‌کند که آسیب‌پذیری متفاوتی را در هر لایه به دنبال خواهد داشت. یک روش معمول ، فشرده‌سازی جریان با کدک H.264 و H.265 سپس ارسال آن از طریق شبکه با پروتکل زمان واقعی مانند RTP از طریق UDP است و یا از پروتکل اتصال گرا TCP استفاده می‌کند. [۱, ۱۵]

۳-۳- توپولوژی:

توپولوژی یک سیستم نظارت مبتنی بر IP را می‌توان با توزیع ، و معماری آن بیان نمود. در این مرحله گستردگی جغرافیایی موردبحث قرار می‌گیرد، در یک موقعیت جغرافیایی و یا چند موقعیت؟ در صورت استفاده از اینترنت آیا روش‌های امن سازی رعایت شده است؟ [۱, ۳, ۵] در گامی دیگر این معماری و توپولوژی را بر اساس هدایت‌شده (بستر کابلی و نوری) و هدایت نشده (بی‌سیم نظیر ماکروویو، 802.1 و یا UHF و یا HF طبقه‌بندی می‌کنند. بر اساس تجارب و پروژه نویسندگان شبکه‌های بی‌سیم به دلیل مسدودکننده در بسیاری از پروژه‌ها مردود و طردشده‌اند.

۳-۴- حفاظت:

در زمان پیاده‌سازی سیستم‌های نظارت تصویری نیاز است که امنیت فیزیکی سیستم‌های نظارت تصویری و امنیت سایبری آن سنجیده و در صورت نیاز مکانیزه‌های مناسب سایبری را همچون امنیت سایبر شبکه برقرار نمود. با توجه به روش‌های امن سازی مبتنی بر سرور، مبتنی بر کلاینت و امنیت انتها به انتها راهکارهای سایبری به شرح پیشنهاد می‌شود: [۱, ۶, ۷, ۲۲]

میزبان: با استفاده از مکانیسم‌های کنترل دسترسی مناسب می‌توان از دوربین‌ها ، DVRها و سایر دستگاه‌ها محافظت کرد. و با بررسی جایگاه‌ها از آسیب‌پذیری و تهدیدهای بعدی جلوگیری نمود. محافظت از میزبان در برابر حملات ممکن است شامل نرم‌افزار ضدویروس یا سایر روش‌ها باشد.

شبکه : در این حالت از روش‌های امنیتی نقطه‌به‌نقطه بهره می‌گیرند و یا به‌جای امنیت اطلاعات از امنیت شبکه استفاده می‌کنند. بسته به توپولوژی ، دسترسی به دستگاه‌های سیستم ممکن است از طریق DVR ، دروازه اینترنت یا مستقیماً از طریق اینترنت حاصل شود. یک کاربر ممکن است با ایمن‌سازی شبکه از طریق رمزگذاری، دیوارهای آتش و اتصالات شبکه خصوصی مجازی (VPN) از دستگاه‌ها و سیستم به‌طورکلی محافظت کند.

۴- دارایی‌ها :

دارایی امری ارزشمند است که ممکن است توسط یک مهاجم هدف قرار گیرد. در مورد ما ، دارایی‌ها داده‌ها ، دستگاه‌ها ، نرم‌افزار و زیرساخت‌ها هستند: [۳, ۷-۹, ۲۲]

DVR – سرور رسانه: ضبط کننده فیلم دیجیتال یا سرور رسانه دیگر ، که وظیفه دریافت ، ذخیره ، مدیریت و مشاهده تصاویر ویدئویی ضبط‌شده / بایگانی‌شده را بر عهده دارد.

دوربین‌ها: دستگاه‌هایی که فیلم‌های ضبط‌شده را ضبط می‌کنند. انواع دوربین‌ها ، مارس‌ها و مدل‌های مختلفی از دوربین‌های IP وجود دارد که هرکدام قابلیت‌ها ، ویژگی‌ها و آسیب‌پذیری‌های خاص خود رادارند. برای پیکربندی ، برخی از دوربین‌های IP رابط‌های مبتنی بر وب (HTTP، Telnet و غیره) را ارائه می‌دهند اما برخی دیگر به یک سرور در ابر متصل می‌شوند. اکثر دوربین‌ها به‌عنوان یک سرور وب عمل می‌کنند که محتوای ویدئویی را به مشتریان مجاز ارائه می‌دهند (به‌عنوان‌مثال DVR به‌عنوان مشتری به دوربین متصل می‌شود).

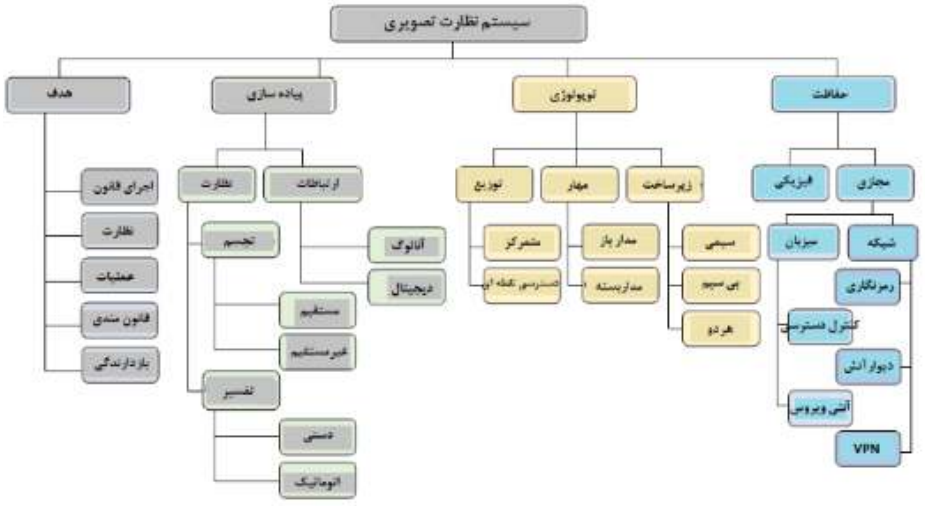
پایانه‌های مشاهده: دستگاه / برنامه‌ای که برای مشاهده و مدیریت محتوای ویدئو به DVR یا دوربین متصل می‌شود. به‌عنوان‌مثال ، یک برنامه اندرویدی که روی تلفن هوشمند یا خود DVR اجرا می‌شود.

زیرساخت شبکه: عناصری که دوربین‌ها را به DVR و DVR را به پایانه مشاهده کاربر متصل می‌کنند. به‌عنوان‌مثال ، روترها ، سوئیچ‌ها ، کابل‌ها و ... این زیرساخت همچنین شامل تجهیزات و پیونده‌ای شبکه خصوصی مجازی (VPN) است. VPNها LANهایی هستند که با استفاده از رمزگذاری ، ترافیک لایه (اترنت) را از طریق اینترنت ، بین پورت‌ها و دستگاه‌های کاربر انجام می‌دهند. VPNهای سایت به سایت می‌توانند دو بخش از شبکه نظارت را از طریق اینترنت متصل کنند. اتصال سایت از راه دور مستقیماً از پایانه کاربر به شبکه نظارت تونل می‌زند.

محتوای ویدئو: استریم ویدئویی که ضبط می‌شوند یا برای بازپخش در ذخیره‌سازی/ شبکه ذخیره‌سازی شده‌اند.

مجوزهای کاربری : نام‌های کاربری ، رمزهای عبور ، کوکی‌ها و نشانه‌های احراز هویت برای دسترسی به DVR ، دوربین‌ها و روترها استفاده می‌شود. از اعتبارنامه برای تأیید اعتبار کاربران و تعیین مجوزهای دسترسی به محتوای ویدئویی ، تنظیمات دستگاه و سایر دارایی‌ها استفاده می‌شود.

ترافیک شبکه - داده‌ها از طریق زیرساخت شبکه منتقل می‌شوند. این می‌تواند اطلاعات کاربری ، محتوای ویدئویی ، داده‌های کنترل سیستم (به‌عنوان‌مثال pan، tilt یا zoom) و سایر پروتکل‌های شبکه (ARP، DNS، HTTP، SSL، TCP، UDP و غیره) باشد.



شکل ۲-مروری بر سیستم‌های نظارت تصویری

۴-۱- بستر ارتباطی و چیدمان المان‌ها

روش‌های مختلفی برای استقرار سیستم نظارت مبتنی بر IP وجود دارد. توپولوژی‌های شبکه را می‌توان متمرکز کرد (همه دوربین‌ها به NVR/DVR متصل می‌شوند) یا توزیع می‌شوند (کاربر به هر دوربین جداگانه متصل می‌شود). ازنظر قابلیت دسترسی ، سیستم می‌تواند از طریق اینترنت مستقیماً قابل‌دسترسی باشد یا به‌هیچ‌وجه از بسترهایی نظیر اینترنت قابلیت دسترسی ندارد. در این راستا ، ما سه دسته از قابلیت دسترسی را شناسایی می‌کنیم:

مدارباز فیزیکی (POC Physically open circuit) وقتی میزبان شبکه در سیستم (دوربین ، DVR و غیره) آدرس IP عمومی دارند. این بدان معنی است که هرکسی از اینترنت می‌تواند بسته درخواست را به دستگاه‌ها بفرستد.

مداربسته فیزیکی (PCC Physically close circuit): وقتی میزبان شبکه در سیستم آدرس IP خصوصی دارد و هیچ زیرساختی شبکه را به اینترنت متصل نمی‌کند. این بدان معنی است که هیچ‌کس از اینترنت نمی‌تواند بسته‌ها را مستقیماً به دستگاه‌ها بفرستد. به این سیستم‌ها شبکه‌های هوای بسته نیز گفته می‌شود [۹].

مداربسته مجازی (VCC : Virtually close circuit) وقتی میزبان شبکه در سیستم آدرس IP خصوصی دارد و شبکه از طریق اینترنت با استفاده از VPN متصل می‌شود. این بدان معنی است که هیچ‌کس از اینترنت نمی‌تواند بسته‌ها را مستقیماً به دستگاه‌ها بفرستد ، مگر اینکه آن‌ها بسته‌ها را از طریق VPN ارسال کنند.

۵- نقض‌های امنیتی

نقض امنیت را می‌توان حمله به محرمانگی ، یکپارچگی و در دسترس بودن سیستم توصیف کرد (معروف به سه‌گانه CIA). نقض رازداری یا عدم تمامیت ، به دسترسی غیرمجاز به اطلاعات اشاره دارد. نقض یکپارچگی به دست‌کاری عمدی و تغییر اطلاعات اشاره دارد. درنهایت ، نقض دسترس‌پذیری به عمل جلوگیری از دسترسی کاربران مجاز به خدمات یا منابع در صورت لزوم اشاره دارد. اهدافی که ممکن است یک مهاجم در حمله به سیستم داشته باشد را می‌توان با توجه به سه‌گانه CIA توصیف کرد: [۲, ۳, ۵, ۲۸]

۵-۱- نقض محرمانه بودن

دسترسی غیرمجاز به محتوای ویدئویی ، اعتبار کاربر ، ترافیک شبکه. در این حالت ، مهاجم قصد دارد فیلم‌های ویدئویی را برای اهداف پلید خود مشاهده کند. درنتیجه ، این هدف حریم خصوصی و امنیت جسمانی محل را به خطر می‌اندازد.

۵-۲- نقض یکپارچگی

دست‌کاری محتوای ویدئویی یا تداخل فعال یک کانال امن در سیستم (به‌عنوان‌مثال ، حمله تنزل رتبه POODLE SSL). در این حالت ، مهاجم قصد دارد محتوای ویدئو (در حالت استراحت یا در حال حرکت) را تغییر دهد. تغییر می‌تواند شامل انجماد قاب ، حلقه زدن یک کلیپ بایگانی‌شده یا درج برخی از مطالب دیگر باشد. این اطلاعات اشتباه می‌تواند منجر به آسیب فیزیکی یا سرقت شود.

یک مهاجم ممکن است برای هدفی که ارتباط مستقیمی با محتوای ویدئو ندارد ، یکپارچگی سیستم را نقض کند. به‌عنوان‌مثال ، ممکن است مهاجم بخواهد از آسیب‌پذیری‌های سیستم سو to استفاده کند و حرکت جانبی به سمت خارج را به‌عنوان مجموعه به دست آورد. برای دستیابی به دارایی‌های خارجی زیر ممکن است از این سیستم به‌عنوان سیستم پایه استفاده شود:

شبکه داخلی : سیستم‌های نظارتی (خصوصاً سیستم‌های مداربسته) برای اهداف مدیریتی ممکن است به شبکه داخلی سازمان متصل شوند. یک مهاجم برای دستیابی به دارایی‌های اطلاعاتی داخلی سازمان ممکن است از این پیوند استفاده کند.

کاربران: ممکن است کاربران سیستم توسط مهاجم هدف قرار گیرند. به‌عنوان‌مثال ، ممکن است مهاجم بخواهد باج افزار را در پایانه مانیتورینگ نصب کند یا حساب‌های شخصی کاربر را به سرقت ببرد.

به‌کارگیری یک بات نت: بات نت یک فرآیند خودکار است و رایانه‌ای را به خطر می‌اندازد که از طریق سرور دستور و کنترل (C&C) دستوراتی را از هکر دریافت می‌کند. به مجموعه ربات‌ها بات نت گفته می‌شود و معمولاً برای راه‌اندازی حملات DDoS ، استخراج ارزهای رمز پایه ، دست‌کاری سرویس‌های آنلاین و سایر فعالیت‌های مخرب استفاده می‌شود.

۵-۳- نقض دسترسی

عدم دسترسی به تصاویر ویدئویی ذخیره‌شده یا زنده. در این حالت ، هدف مهاجم این است (۱) غیرفعال کردن یک یا چند استریم تصویر دوربین (پنهان کردن فعالیت) ، (۲) حذف محتوای ذخیره‌شده فیلم (حذف شواهد) ، یا (۳) حمله به باج افزار (کسب درآمد).

۶- حملات

انواع مختلفی از حملات وجود دارد. برخی از سناریوها شامل یک مرحله هستند (به‌عنوان‌مثال ، DDoS و ایجاد یک پیوند VPN) ، درحالی‌که برخی دیگر مراحل زیادی دارند (به‌عنوان‌مثال ، سرقت مجوز نامه‌ها و لایسنس ها با ارسال یک ایمیل فیشینگ ، نصب یک بدافزار و غیره). از توالی مراحل حمله غالباً به‌عنوان بردار حمله یاد می‌شود. هر مرحله در بردار به مهاجم امکان دسترسی به برخی از دارایی‌ها را می‌دهد و مرحله آخر در بردار هدف مهاجم را برآورده می‌کند. به‌عنوان‌مثال ، شکل ۳ دو بردار حمله را نشان می‌دهد که به یک هدف می‌رسند: حمله ۱ نتیجه‌ای را به دست می‌آورد که یک دارایی را به خطر بیندازد. درنتیجه ، مهاجم می‌تواند حمله ۲ یا ۳ را انجام دهد تا به هدف برسد. متناوباً ، مهاجم ممکن است حمله ۲ را انجام دهد و مستقیماً در یک مرحله به هدف برسد ، اما ممکن است انجام آن دشوارتر باشد. برای درک بردار حمله ، باید جنبه‌های زیر را بررسی کنیم:

- **عامل تهدید**: شخص ، دستگاه یا کدی که یک مرحله حمله را از طرف مهاجم انجام می‌دهد.
- **اقدام تهدید**: فعالیت مخربی که یک نماینده می‌تواند در هر مرحله انجام دهد (دسترسی ، سو استفاده ، اصلاح و غیره)
- **نتیجه / بازخورد تهدید:** آنچه مهاجم با اتمام موفقیت‌آمیز مرحله حمله به دست می‌آورد.
- **هدف حمله:** نتیجه نهایی که مهاجم سعی دررسیدن به آن دارد (در انتهای بردار حمله). اکنون هر یک از این جنبه‌ها را با توجه به سیستم نظارت بررسی خواهیم کرد.

۶-۱- عوامل تهدید

عوامل تهدید / عاملان حمله برای سیستم‌های نظارت تصویری مربوطه زیر در بسیاری از منابع شناسایی‌شده‌اند [۱, ۱۵, ۲۸]

۱) **هکر** - فردی که درزمینهٔ سو استفاده از آسیب‌پذیری‌های رایانه باتجربه است ، فعالیت‌های غیرمجاز وی سیاست‌های امنیتی سیستم را نقض می‌کند. یک هکر می‌تواند در یک مکان از راه دور (به‌عنوان‌مثال اینترنت) یا در مجاورت یک شبکه فیزیکی باشد.

۲) شبکه میزبان - رایانه‌ای متصل به شبکه سیستم که کد مخربی را اجرا می‌کند. رایانه می‌تواند یک دوربین IP، DVR یا هر دستگاه قابل‌برنامه‌ریزی در شبکه باشد. به کمک مهندسی اجتماعی در یک مرکز برای شناخت منافذ توسط نویسندگان یک بدافزار به سیستم تحت نظر مدیر سیستم وارد شد و آموزش به کارکنان ارائه شد.

۳) عامل خودی - کاربر مجاز سیستم که مهاجم است یا با مهاجم تبانی دارد. ممکن است عامل خودی یک کاربر عادی باشد (به‌عنوان‌مثال افسر امنیتی) ، یک عضو پشتیبانی فناوری اطلاعات یا حتی سرپرست سیستم. در یک پروژه کارشناس اتاق مانیتورینگ به دلیل خواب بودن سیستم و بیدار شدن ناگهانی، کلیه تصاویر ذخیره‌شده را از ترس اخراج پاک کرد و یا در پروژه دیگر پیمانکار به دلیل دسترسی از راه دور، برای عقد قرارداد نگهداری از مهندسی اجتماعی معکوس استفاده نمود.

۶-۲- اقدامات تهدیدآمیز

تهدیدهای مختلفی برای سیستم‌های نظارت تصویری شناخته‌شده است و نویسندگان در مقاله جداگانه طبقه‌بندی این تهدیدها را ازنظر لایه‌های شبکه نیز در حال بررسی هستند. حملات ذکرشده در بخش زیر برای سنجش امنیت در یک آزمایشگاه توسط نویسندگان صورت گرفت.

۶-۲-۱- انجام تزریق کد

تزریق کد آلوده به پایگاه داده VMS یا SQL می‌تواند سرآغاز حملات بعدی باشد. [۱, ۳]. برخی از دوربین‌ها سرورهای محلی HTTP را اجرا می‌کنند تا کنسول پیکربندی مناسب در اختیار کاربران قرار دهند. بسیاری از این کنسول‌ها از ضعف‌های امنیتی بهره می‌گیرند. [۱۵]

۶-۲-۲- دست‌کاری / مشاهده ترافیک

یک عامل تهدید ممکن است ترافیک شبکه را دست‌کاری ، تغییر مسیر یا مشاهده کند. به‌عنوان‌مثال ، یک عامل ممکن است یک حمله مردمیانی (MitM) را در شبکه محلی انجام دهد ، و سپس یک تصویر ویدیویی را مسدود کند یا به یک استریم تصاویر ضبط‌شده مشابه که قبلاً دریافت کرده است، مستقیم به شبکه وارد کند. [۸] برای حمله MitM ، مهاجم می‌تواند از طریق دستگاه قربانی آلودگی ARP ، جعل DHCP / DNS را از طریق او تغییر مسیر دهد.

برای تزریق ، از ابزار VideoJak می‌توان برای بهره‌برداری از جریان‌های ویدئویی رمزگذاری نشده با استفاده از پروتکل‌های RTSP یا RTP استفاده کرد. این پروتکل‌ها معمولاً در سیستم‌های نظارت تصویری مورداستفاده قرار می‌گیرند و در صورت یافتن در استقرار PCC ، ممکن است بدون رمزگذاری باقی بمانند. [۱]

۶-۲-۳- نفوذ اطلاعات

از دوربین‌ها می‌توان برای نفوذ اطلاعات به یک مهاجم بهره برد [۷]. به‌عنوان‌مثال در حمله به دوربین اکسیس ۱۳۵۶P توسط نویسندگان، یک بدافزار موجود سبب شد وضعیت دوربین را تغییر داده و چراغ آن چشمک بزند (با حمله به دوربین و ریست آن به دلیل منع سرویس) . با تبدیل وضعیت دوربین و مشاهده وضعیت نشانگر، توانستیم در زمان راه‌اندازی مجدد دوربین و ورود اطلاعات توسط کاربر، رمز عبور را بخوانیم. در حمله که توسط نویسندگان انجام شد با قطع برق رک، دوربین چشمک‌زن شد و با شنود بسته‌های دوربین، رمز عبور ورودی تشخیص و به دوربین حمله شد. در حمله مشابه دیگر توسط نویسندگان، رمز عبور از توابع فشرده‌ساز استفاده کرده بود که با استفاده از پایگاه کالی و مدهای گیت‌هاب رمز عبور دست‌یافتنی شد.

۶-۲-۴- تزریق سیلابی و اخلال در کار

درتهدید دیگر با استفاده از ابزار golden eye و ddos attack و ابزار psyn به دوربین حمله منع سرویس صورت گرفت. و اخلال در کار دوربین را فراهم گردید. دوربین‌های IP معمولاً مستعد ابتلا به این حملات هستند زیرا معمولاً ازنظر منابع محدود دستگاه‌هایی هستند. [۱]

به‌عنوان‌مثال ، بعضی از دوربین‌ها فقط می‌توانند تا ۸۰ اتصال هم‌زمان HTTP را پشتیبانی کنند که به‌راحتی قابل‌مصرف هستند. مثال دیگر حمله بازسازی SSL که عامل به‌طور مکرر درخواست مذاکره مجدد کلیدی می‌کند که پردازنده دستگاه را بیش‌ازحد بارگذاری می‌کند. سایر حملات DoS با بهره‌گیری از اشکالات و آسیب‌پذیری‌ها قابل انجام است. به‌عنوان‌مثال ، یک دوربین می‌تواند با ارسال درخواست‌های بزرگ HTTP POST از شبکه خارج شود و یا یک مسیریاب VPN به دلیل بسته‌های ساخته‌شده مجبور به قطع تمام اتصالات می‌شود. [۲۶]

در آزمایشی که توسط نویسندگان به کمک کالی انجام شد با ابزارهای DDoS attack و Golden Eye دوربین‌ها و دستگاه ذخیره‌ساز قوی نظیر اکسیس و بوش ظرف ۹۰ ثانیه از کار افتادند. البته دوربین‌های ضعیف‌تر نظیر هایک‌ویژن در ۱۵ ثانیه از شبکه خارج شدند

۶-۲-۵- اسکن و شناسایی

یکی از روش‌های تهدید در محیط نظارت تصویری و در بخش سایبر آن، اسکن شبکه است تا به کمک آن از توپولوژی ، دارایی‌ها ، پورت‌های شبکه باز و خدمات موجود آگاهی پیدا کرد و در گام بعدی بهره‌برداری بالقوه انجام پذیرد. ابزارهای مختلف توسط سازندگان دوربین و یا نرم‌افزارهای شبکه وجود دارد. مثلاً NMAP می‌تواند برای لیست کردن موجودیت‌ها و آدرس پورت به کار رود. از سویی دیگر به کمک نرم‌افزار پویشگر کارخانه‌ای هکر به اطلاعات ارزنده دست پیدا می‌کند تا حملات محرمانه‌ای به رابط‌های وب در معرض آن انجام دهد. بسیاری از سازندگان نرم‌افزار شناسایی دوربین و یا پورت را نظیر ip utility ، IP config , و ... را عرضه می‌کنند. در یک حمله که توسط نویسندگان صورت گرفت، این حمله و تغییرپذیری معمولاً خارج از سایت انجام می‌شود زیرا تشخیص آن آسان است. به کمک این روش با شناسایی فرم‌ویر و پورت باز، از آسیب‌پذیری‌های شناخته‌شده استفاده می‌شود و هکر می‌تواند حمله را انجام دهد.

۶-۲-۶- استفاده از یک پیکربندی اشتباه

یک عامل تهدید ممکن است از تنظیمات اشتباه برای نصب بدافزار یا دسترسی به داده‌های حساس استفاده کند. پیکربندی اشتباه به‌عنوان‌مثال شامل اعتبار پیش‌فرض ، سرویس‌های در معرض (به‌عنوان‌مثال ، Telnet) و قوانین کنترل دسترسی نامناسب است. یک پیکربندی اشتباه می‌تواند توسط کاربر سیستم یا سازنده ایجاد شود. در یک حمله در یک شبکه با استفاده از پورت‌های باز شبکه بی‌سیم و عدم بسته بودن WPS به شبکه حمله گردید و حمله منع سرویس و شنود رمز عبور صورت گرفت و کلیه رمزها تغییر یافت و کل ذخیره‌سازی منهدم شد.

۶-۲-۷- انجام یک حمله Brute-Force

حمله Brute-Force تلاشی است برای حدس زدن یک ورودی صحیح با آزمایش گزینه‌های ممکن. از حملات Brute-Force می‌توان برای آشکار کردن اطلاعات خصوصی کاربر مانند نام کاربری و گذرواژه استفاده کرد. این حملات را می‌توان با محدود کردن تعداد ورود ناموفق مجاز در هر دقیقه کاهش داد. بااین‌حال ، در برخی موارد ، تولیدکنندگان دوربین این ویژگی امنیتی را اجرا نمی‌کنند. برای دستیابی سریع به یک‌راه حل ، ممکن است از فرهنگ لغت رمزهای عبور رایج به‌عنوان یک حدس استفاده شود. مهندسی اجتماعی کارکنان فناوری اطلاعات ، حراست و اتاق مانیتورینگ از روش‌های دیگری بود که توسط مهندسین اجرا شد. نمونه این نرم‌افزارها هیدرا hydra، جانی johnyو rainbrrowcrack بود که برای دوربین‌های آزمایشگاهی مورداستفاده قرار گرفت و بعد از ۴۷ ساعت رمز آن شکسته شد.

۶-۲-۸- مهندسی اجتماعی (SE)

در مهندسی اجتماعی با شناخت ضعف‌های روانی و به نحوی مناسب بدافزار را وارد سیستم نمایند، بیشتر بدافزارها در این حوزه یا جاسوس‌افزار یا پردازش افزار هستند. حملات مشترک SE شامل ایمیل‌های فیشینگ و طعمه‌گذاری است.

در یک حمله ساده توسط مهندسین نگاه از پشت و کول بری کارکنان اتاق مانیتورینگ صورت گرفت و به رمز عبور دست‌یافتیم. در حمله دیگر که فقط به‌صورت تئوری در نظر گرفته شد، ارائه فلش مموری هدیه به کارکنان اتاق مانیتورینگ بود، این افراد می‌توانستند بدافزار را یا به رایانه‌های محل کار و یا به موبایل خویش وارد نمایند. در این سناریو دسترسی به وب کم موبایل مدنظر قرار گرفت. در فیشینگ ، عامل تهدید پیامی (ایمیل ، پیام کوتاه و غیره) را که به‌عنوان منبع قابل‌اعتماد مبدل شده است ، می‌فرستد تا سعی کند گیرنده را به نصب برخی از بدافزارها و یا درنهایت اطلاعات شخصی کاربر نشان دهد.

۶-۲-۹- دسترسی فیزیکی

دسترسی فیزیکی جایی است که یک عامل تهدید حمله‌ای را انجام می‌دهد که نیاز به تماس فیزیکی مستقیم با سیستم دارد. به‌عنوان‌مثال ، نصب یک شنود گوشی، دستگاه دارای درب مخفی ، دسترسی به پایانه در اتاق سرور ، نفوذ به سفت افزار دوربین (فرم‌ویر) ، انسداد دید دوربین با بریدن کابل شبکه یا کابل کواکسیال.

۶-۲-۱۰- مهندسی معکوس

یک عامل تهدید ممکن است با استفاده از مهندسی معکوس (RE) ، در پی سنجش میزان آسیب‌پذیری دوربین باشد. مهندسی معکوس معمولاً خارج از سایت و با استفاده از همان سخت‌افزار / نرم‌افزار/ سفت افزار جهت سو استفاده از قربانی مورداستفاده قرار می‌گیرد. مهندسی معکوس که آن را با RE می‌شناسند، یک فرآیند تجزیه‌وتحلیل کد یا سخت‌افزار مخفی‌شده برای شناسایی اجزای سیستم و روابط متقابل آن‌ها است. در طی این فرآیند ، آسیب‌پذیری‌ها و حتی اطلاعات کاربری به‌سختی قابل‌مشاهده است.

یک روش دیگر، تجزیه‌وتحلیل میان‌افزار از قبل کامپایل شده و ارائه‌شده توسط سازنده است. در ارائه‌های [۲۹] نویسندگان بر روی دوربین‌های IP متمرکزشده‌اند که مبتنی بر اینترنت هستند و آن‌ها را از طریق تصاویر میان‌افزار تهیه‌شده توسط فروشندگان دوربین تجزیه‌وتحلیل می‌کنند. نویسندگان آسیب‌پذیری‌های روز صفر را در تجهیزات نظارت دیجیتال از شرکت‌های مختلف ازجمله D-Link Corp، Cisco Systems، Linksys، TRENDnet و غیره با استفاده از ابزارهای موجود مشاهده کردند.

۶-۳- پیامد تهدید

موفقیت یک حمله در طی یک مرحله ، توانایی‌های جدیدی را برای مهاجم فراهم می‌کند. به‌عنوان‌مثال دسترسی به دارایی‌های اطلاعاتی جدید ، توانایی اجرای کد و توانایی انجام حملات جدید مواردی است که می‌توان به آن اشاره کرد. موارد زیر به‌عنوان عواقب اصلی تهدید شناسایی است:

۶-۳-۱- توسعه مجوزهای دسترسی

یک مهاجم ممکن است اعتبارنامه‌های جدید را دریافت کرده یا یک کد را به‌گونه‌ای اجرا کند که دسترسی به مجموعه‌هایی را که قبلاً محدودشده است ، فراهم نماید. از این تشدید می‌توان برای جمع‌آوری اطلاعات ، لغو / نصب نرم‌افزار ، غیرفعال کردن مکانیسم محافظتی و غیره استفاده کرد. به‌عنوان‌مثال ، یک وب‌سایت محافظت نشده با روش CGI می‌تواند به کاربر غیرمجاز امکان دور زدن صفحه ورود به سیستم و دسترسی به محتوای وب کم را ارائه دهد؛

۶-۳-۲- دسترسی به محتواهای ویدیویی

مهاجم ممکن است بتواند تصاویر ویدئویی را به‌صورت زنده یا از پیش ضبط‌شده مشاهده یا بارگیری نماید.

۶-۳-۳- اجرای خودسرانه کد (ACE)

یک تهدید امنیتی قابل‌توجه که یک مهاجم را قادر می‌سازد هر دستوری را روی یک ماشین هدف یا در یک فرایند هدف اجرا کند. درنتیجه ، مهاجم می‌تواند افزایش امتیاز ، نصب بدافزار ، سرقت اطلاعات و سایر اقدامات مخرب را انجام دهد. نقاط ضعف ACE بسیاری در دوربین‌های IP، DVRها و روترهای VPN کشف‌شده است

۶-۳-۴- نصب بدافزار

مهاجم ممکن است بتواند فرایند موردنظر خود را روی دستگاه هدف نصب و اجرا کند. از این نرم‌افزار به‌عنوان بدافزار یاد می‌شود؛ یعنی کد مخربی که برای آسیب رساندن به رایانه باهدف مخرب طراحی‌شده باشد. انواع بدافزارها شامل کرم‌ها ، اسب‌های تروا ، ویروس‌ها ، جاسوس‌افزارها ، لوازم زرهی ، اسکیمرها ، باج افزارها ، نرم‌افزارهای تبلیغاتی و روت کیت‌ها است. از بدافزار می‌توان برای سرقت داده‌های حساس ، رمزگذاری یا حذف داده‌های کاربر ، آسیب‌رسانی به دستگاه ، استخراج ارزهای رمز پایه ، افزودن دستگاه به بات نت یا نقش محوری برای حرکت جانبی از طریق شبکه موردحمله استفاده کرد.

۶-۳-۵- حرکت جانبی

یک مهاجم با این کار می‌تواند جایگاه محکم‌تری در سیستم نظارت داشته باشد و به دارایی‌های اطلاعاتی غیرقابل دسترسی قبلی دست یابد. همچنین ممکن است مهاجم بتواند به سیستم‌های دیگر دسترسی پیدا کند و دستگاه‌های کاربر متصل به سیستم را آلوده نماید.

۶-۳-۶- حمله مردمیانی (MitM)

با مشاهده رابطه ورودی و خروجی، حملات سایبری در فناوری‌ها بدان معناست که یک مهاجم می‌تواند با جلب اعتماد از گیرنده حمله را انجام دهد. برای مقابله نیاز است که از شناسایی ، جعل شناسایی یک شیء یا حتی ایجاد حمله DoS جلوگیری شود . [۶, ۱۵]

۶-۳-۷- منع سرویس (DoS)

یک مهاجم ممکن است بتواند بر روی در دسترس بودن سرویس ، داده یا منبع تأثیر بگذارد. اگر مهاجم به دوربین‌ها یا DVR آسیب رسانده باشد ، در این صورت می‌تواند باعث توقف انتقال دوربین توسط محتوای فیلم ، حذف محتوای تاریخچه ، جلوگیری از دسترسی به DVR یا ازکارافتادن اتصال VPN شود. درنتیجه ، جرمی ممکن است بدون داشتن شواهد دیجیتالی در محل انجام شود. یک مهاجم همچنین ممکن است بدون ایجاد هشدار در DVR ، از شناسایی فرار کند. این می‌تواند از طریق حمله تزریق فیلم یا حمله یادگیری ماشین متخاصم ایجاد شود. البته در آزمایش توسط نویسندگان حمله منع سرویس به یک دوربین و به‌واسطه آن ازکارافتادن سوئیچ و مسیریاب میسر شد.

۶-۳-۸- دسترسی به یک شبکه‌ی ایزوله

در برخی موارد ، DVR به اینترنت (POC یا VCC) و همچنین به شبکه‌ای متصل است که گفته می‌شود از اینترنت جداشده است (به‌عنوان‌مثال ، فرودگاه‌ها ، بیمارستان‌ها ، کارخانه‌ها و غیره). با به خطر انداختن DVR یا یکی از موارد دیگر در دوربین‌ها ، مهاجم می‌تواند حرکت جانبی را به شبکه‌ی جداشده انجام دهد. در یک آزمایش به کمک ورود به سیستم دوربین و قربانی کردن کلاینت‌های سرور مداربسته، حمله به دوربین میسر شد. [۱]

۶-۴- اقدامات مقابله‌ای و بهترین روش‌ها

در بخش زیر اقدامات متقابل موجود و بهترین روش‌هایی را که می‌تواند برای محافظت از سیستم‌های نظارتی مدرن استفاده شود ، مرور می‌کنیم.

۶-۴-۱- سیستم‌های تشخیص و پیشگیری از نفوذ

دفاع سایبری اساسی را باید در هر شبکه رایانه‌ای در اولویت قرارداد. به‌عنوان‌مثال ، برای شناسایی و جلوگیری از آلودگی به بدافزارها ، نرم‌افزار ضدویروس باید روی پایانه‌های کاربر و DVRها نصب شود. در توپولوژی‌های توزیع نشده POC ، باید یک دیوار آتش مقاوم برای عبور حداقل ترافیک شبکه موردنیاز به‌منظور استفاده از سیستم (مانند ، شبکه راه دور بلوکی ، بسته‌های "پینگ" ICMP و غیره) استفاده شود. با حفاظت توسط دیوار آتش، می‌توان از یک سیستم شناسایی نفوذ شبکه (NIDS) برای شناسایی الگوهای ترافیکی مخرب بهره‌گیری کرد. در این حالت می‌توان از NIDS رایگان مانند Snort و Suricata یا نرم‌افزار تجاری استفاده نمود.

۶-۴-۲- پیکربندی و رمزگذاری

باید تنظیمات دوربین‌ها ، روترها ، پایانه‌ها و DVR را با دقت مرور کرد. به‌عنوان‌مثال ، گذرواژه‌های ضعیف یا پیش‌فرض باید تغییر کنند و در صورت امکان باید از رمزهای عبور مختلف در میان دستگاه‌های مختلف استفاده شود. علاوه بر این ، APIها و سایر ویژگی‌های مشابه در صورت عدم نیاز باید غیرفعال باشند. همچنین در صورت امکان، باید ارتباطات ایمن فعال‌شده باشد و اطمینان حاصل گردد که دستگاه‌ها از گواهینامه‌های SSL (به‌عنوان یک تنظیم پیش‌فرض مشترک) استفاده نمی‌کنند. درنهایت ، باید به‌صورت دوره‌ای CVEهای جدید را بررسی کرد و دید که آیا نرم‌افزار / سیستم‌عامل همه دستگاه‌ها به‌روز هستند یا خیر.

۶-۴-۳- محدود کردن دسترسی فیزیکی

اساسی‌ترین دفاع محیطی، محدود کردن دسترسی فیزیکی به دارایی‌های اطلاعاتی سیستم است. در صورت امکان ، سیم‌کشی نباید از مکان‌های عمومی عبور کند ، کلیه تجهیزات شبکه (سوئیچها ، روترها و غیره) باید از طریق قفل محافظت شوند و دسترسی به سیستم باید تحت مدیریت ، ثبت و نظارت دقیق باشد.

را دیگر پیاده سازی سرویس های 802.1x است که میتواند محدود سازی دسترسی به پورت های شبکه را فراهم سازد این کار در کنار vlan سبب می شود از نظر دسترسی به شبکه ها و اقدامات مخرب فوق الذکر امنیت بیشتری را فراهم نمود.

۶-۴-۴- دفاع در برابر حملات DoS

پروتکل‌های متنوعی برای بهره‌گیری از آسیب‌پذیری آن‌ها به‌منظور انجام حمله DDoS وجود دارد. متعاقب آن ، سازوکارهای دفاعی مختلفی نیز به وجود آمده است که می‌تواند به این منظور به کار گرفته شود. حفاظت مطلوب شامل مراحل زیر است: (۱) تشخیص حمله ، (۲) انتخاب بسته‌های مخرب / مضر و (۳) ثبت یا فیلتر نمودن بسته‌های شناسایی‌شده. برای تشخیص حمله ، از یادگیری ماشین و روش‌های آماری - مانند تشخیص ناهنجاری سبک می‌توان استفاده کرد.

۶-۴-۵- دفاع در برابر حملات MitM

برای جلوگیری از شنود و دست‌کاری بسته (به‌عنوان‌مثال ، تزریق فیلم) درنتیجه حمله MitM ، باید از رمزگذاری مناسبی استفاده شود. بااین‌حال ، گاهی اوقات برخی آسیب‌پذیری‌ها در پروتکل‌های رمزگذاری کشف می‌شوند، و سیستم‌ها نیز ممکن است پیکربندی نادرستی داشته باشند. برای تشخیص دست‌کاری (تزریق فیلم) ، می‌توان زمان را با توجه به موقعیت‌های پنهان ارجاع داد.

۶-۴-۶- آموزش

در بسیاری از تهدیدات مداوم پیشرفته (APT) ، نفوذ اولیه به‌صورت یک حمله مهندسی اجتماعی است. مؤثرترین راه برای کاهش این تهاجمات اولیه ، عبارت است از: (۱) آموزش استفاده از سیستم در برابر ناقلین احتمالی حمله ، و (۲) هشدار به کاربران به‌منظور مراقبت از پیام‌ها و درخواست‌های ناخواسته‌ای که به بهانه‌های دروغین انجام می‌شود.

۷- نتیجه‌گیری

در این مقاله به بررسی امنیت سیستم‌های نظارت تصویری مدرن پرداخته‌ایم. همچنین با مروری بر این سیستم‌ها ، قرارگیری‌های متداول را ارائه داده و دارایی‌های اطلاعاتی سیستم را فهرست بندی کرده‌ایم. با استفاده از این اطلاعات، و با استفاده از کاوش در سطح حمله سیستم ، قابلیت‌های مهاجم را برشمرده و با ارائه برخی از بردارهای حمله ، امنیت این سیستم‌ها را بررسی نموده‌ایم. درنهایت نیز، خلاصه‌ای از بهترین شیوه‌ها و راه‌حل‌های امنیتی را که می‌تواند برای تقویت امنیت استفاده شود ، ارائه دادیم. امید است این مقاله به امنیت سیستم‌های نظارت تصویری موجود و آینده کمک شایانی بنماید. یکی از محورهای مهم در پایداری سیستم بحث افزونگی است، که برای برق و شبکه باید در نظر گرفته شود و از اهداف آتی نویسندگان به شمار می‌آید

۸- پژوهش‌های آتی

در این مقاله، تهدیدهای مختلفی که می‌تواند سیستم‌های نظارت تصویری را دچار مشکل نماید معرفی گردید، از یک‌سو با پیشرفت یادگیری ماشین و هوش مصنوعی خودکار سازی حملات در حال رشد است و این امر سبب اختلال و چالش در شناسایی آن‌ها شده است. این سری از تهدیدها بیشتر در حیطه نظارت تصویری خلاصه می‌شوند که نویسندگان هدف بعدی مقاله خود قرار داده‌اند. از سویی دیگر سیستم‌های نظارت تصویری تحت شبکه ، از تهدیدهای متداول شبکه نیز در امان نیستند. تهدید در حال

ظهور این است که چگونه این سیستم‌ها در بات نت آلوده‌شده و منجر به حمله به شبکه داخلی می‌شوند (به‌عنوان‌مثال ، انفجار داده‌ها ، جاسوسی یا استفاده از سیستم نظارت بر حرکت جانبی) یا سایر شبکه‌های خارجی (به‌عنوان‌مثال ، DDoS، SPAM).
برای رفع این تهدیدات ، اقدامات آتی باید بر حفاظت از الگوریتم‌های یادگیری ماشین و مقاوم‌سازی آن‌ها در برابر حملات یادگیری ماشین خصمانه و توسعه راهکارهای امنیتی هدفمند برای سیستم‌های نظارت تصویری برای بهبود حفاظت آن‌ها در برابر حملات سایبری متمرکز باشد.
بنابراین ، اعتقاد [۱] بر این است که تحقیقات آتی باید بر روی ایجاد یک محافظت مداوم خارجی متمرکز باشد که بتواند با اطلاعات مربوط به حملات تازه کشف‌شده به‌راحتی به‌روزرسانی شود. یکی از راه‌های جمع‌آوری اطلاعات در مورد تهدیدهای در حال ظهور سیستم‌های نظارتی ، استفاده از سیستم پیشرفته هانی پات است. علاوه بر این ، با شناسایی این سو استفاده‌ها ، مدیران می‌توانند از سیستم‌های خود قبل از آلوده شدن محافظت نمایند. درنهایت، اگرچه در بیشتر موارد ارتباط سیستم‌های پیشرفته نظارت تصویری رمزگذاری شده‌اند، اما می‌توان با استفاده از حملات کانال‌های جانبی به‌طور محرمانه، اشخاص نیز پنهان شوند. بنابراین، تحقیقات آینده باید بر روی شناسایی و حذف کانال‌های جانبی نیز متمرکز باشد. {Kalbo, 2020 #17}
از سویی دیگر نویسندگان روشهای مختلف منع سرویس و ابزارهای آن را نیز به صورت جداگانه تجزیه و تحلیل کرده و در مقاله نوینی ارائه خواهند داد.

۹- سپاسگزاری

سپاس فراوان از مدیریت شرکت ایمن تصویر امرتات جناب آقای مهندس زارعی و مدیریت شرکت افراد دید آسیا جناب آقای مهندس اعلمی به دلیل فراهم کردن محیط آزمایشگاهی و امانت دادن محصولات نظارت تصویری برای آزمودن و بررسی و تکمیل این مقاله.

۱۰- مراجع

[1]. Kalbo N, Mirsky Y, Shabtai A, Elovici Y. The Security of IP-Based Video Surveillance Systems. Sensors (Basel). 2020;20.(۱۷)
[2]. Omnicast G. Who’s keeping your things secure? 2020 [Available from: https://info.genetec.com/securityofsecurity#%20.
[3]. IPVM .Cybersecurity for IP Video Surveillance Guide: IPVM; [Available from: https://ipvm.com/reports/network-security-for-ip-video-surveillance.
[4]. Bosch. Video security and the Internet of Things. Bosch website; 2020.
[5]. communication A. Cybersecurity Partners in protection. Axis Communication; 2019.
[6]. Stallings W. Effective cybersecurity : understanding and using standards and best practices. Upper Saddle River, NJ: Addison-Wesley; 2019. xxxi, 768 pages p.
[7]. Stallings W. Information privacy engineering and privacy by design : understanding privacy threats, technology, and regulations based on standards and best practices. 1. ed. Hoboken: Pearson Education, Inc.; 2019. pages cm p.
[۸]. صموتی س, فتحی م. ارزیابی تهدیدها، آسیب پذیری و ریسک در زیر ساخت سامانه های نظارت تصویری تحت شبکه سامانه های حمل و نقل هوشمند. دومین همایش سیستم های حمل و نقل هوشمند جاده ای: 1395 ;undefined.
[9]. Fredrik Nilsson CA. Intelligent Network Video. Understanding Modern Video Surveillance Systems SE, editor: CRC Press; 2016.
[۱۰]. فتحی م, ملکیان ا. اینترنت اشیاء: مفاهیم، معماری، کاربردها: کانون نشر علوم ۱۳۹۷.
[11]. Bondavalli A, Bouchenak S, Kopetz H. Cyber-Physical Systems of Systems : Foundations - A Conceptual Model and Some Derivations: The AMADEOS Legacy. Cham: Springer International Publishing : Imprint: Springer,; 2016.

[12]. Guo S, Zeng D. Cyber-Physical Systems: Architecture, Security and Application. Cham: Springer International Publishing : Imprint: Springer,; 2019.

[13]. Hu L, Xie N, Kuang Z, Zhao K, editors. Review of Cyber-Physical System Architecture. 2012 IEEE 15th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops; 2012 11-11 April 2012.

[14]. Suh SC, Tanik UJ, Carbone JN, Eroglu A. Applied cyber-physical systems. New York, NY: Springer; 2014. xii, 253 pages p.

[15]. Zhaoyu L, Dichao P, Yuliang Z, Liu J, editors. Communication protection in IP-based video surveillance systems. Seventh IEEE International Symposium on Multimedia (ISM'05); 2005 14-14 Dec. 2005.

[16]. Calder A, Watkins S. IT governance : an international guide to data security and ISO 27001/ISO 27002. Seventh edition. ed. London: KoganPage; 2020. x, 395 pages p.

[17]. Garrett GA. Cybersecurity in the digital age : tools, techniques, and best practices. Riverwoods, IL: Wolters Kluwer; 2019. xiii, 540 pages p.

[۱۸]. آنتونوپولوس آ. کتاب همه چیز درباره ی بیت کوین نص; ۱۳۹۷.

[19]. DDoSPedia. DDoS Attack Definitions - DDoSPedia 2018 [Available from: https://security.radware.com/ddos-knowledge-center/ddospedia/pyloris/.

[۲۰]. صموتی سع, مرادنوری م, مرادی ر. بررسی تهدید موجود در کنترل شریان‌های حیاتی کشور در مناطق ویژه و حساس بر مبنای سنسورهای تحت شبکه با رویکرد پدافند غیر عامل سایبر. اولین همایش شهر هوشمند و اینترنت اشیا; دانشگاه فردوسی مشهد: SCIOT 2017; 1396.

[21]. Harwood E. Digital CCTV - A Security Professional's Guide: Elsevier; 2008.

[22]. Forouzan BA. Introduction to cryptography and network security. Boston: McGraw-Hill Higher Education; 2008. xxvi, 721 p. p.

[23]. IPVM. 2020 IP Networking Book: IPVM; 2020.

[۲۴]. صموتی س, فتحی م, تفنگچی ت. مطالعه میدانی سامانه های نظارت تصویری در صنعت ریلی و ارایه راهکار های هوشمندسازی برای افزایش امنیت از دیدگاه پدافند غیر عامل. دومین کنفرانس ملی پدافند غیرعامل و پیشرفت پایدار: undefined; 1396.

[۲۵]. صموتی س, یارمحمدی ع. مطالعه میدانی پارامترهای اصلی اتاق کنترل برای مانیتورینگ دقیق و صحیح وقایع و حوادث در شبکه های بصری سازمان ها. دومین کنفرانس ملی پدافند غیرعامل و پیشرفت پایدار: undefined; 1396.

[26]. Nestler VJ. Principles of computer security, CompTIA security+ and beyond : lab manual. 2nd ed. New York: McGraw-Hill Osborne Media; 2011. xx, 332 p. p.

[۲۷]. IPVM. مروری بر دوربین های مداربسته شرکت ایمن تصویر امرتات; ۱۳۹۹.

[28]. Davis JPV, Tim. Forensic facial identification : theory and practice of identification from eyewitnesses, composites and CCTV: John Wiley & Sons Inc; 2015. 376\38

[29]. p.

[30]. Heffner C. Exploiting surveillance cameras. Technical report. Black Hat conference; 2013.