نشریه پژوهش‌های نوین در مدیریت کارآفرینی و توسعه کسب و کار
جلد۲، شماره۳، پاییز ۱۴۰۰، صفحه: از۲۵۸ تا ۲۸۶ ISSN 2717-2570
https://science-journals.ir https://pnmktk.science-journals.ir

بررسی تهدیدهای نوظهور در امنیت سایبری

رهبر زارعی[۱]

۱- دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش معماری کامپیوتر، دانشگاه غیر انتفاعی کارون

چکیده

حملات سایبری و اقدامات متقابل به عنوان یک نیاز فوری در جامعه امنیت سایبری در نظر گرفته شده است. برای کمک به دستیابی به این هدف، ابتدا نمای کلی از آسیب پذیرترین سوءاستفاده در لایه‌های سخت افزار در لایه های اطلاعاتی کشور، نرم افزار و شبکه موجود را ارائه می‌دهیم. این به دنبال انتقاد از تکنیک‌های مدرن موجود در زمینه تسکین در مورد چرایی کار یا عدم موفقیت آنها است.سپس الگوهای جدید حمله را در فناوری های نوظهور مانند رسانه‌های اجتماعی، رایانش ابری، فناوری الکترونیکی و زیرساخت‌های مهم مورد بحث قرار می‌دهیم.

واژگان کلیدی: تهدید، آسیب، اقدامات، پیشنهادات، امنیت سایبری

۱- مقدمه

جامعه، اقتصاد و زیرساخت‌های مهم ما تا حد زیادی به شبکه‌های رایانه‌ای و راه حل‌های فناوری اطلاعات وابسته شده است. با وابستگی ما به فناوری اطلاعات، حملات سایبری جذاب‌تر و به طور بالقوه فاجعه بارتر می‌شوند. مطابق گزارش سایبر سایبری که در آوریل ۲۰۱۲ منتشر شد [17] قربانیان حملات سایبری نیز به میزان قابل توجهی در حال رشد هستند. براساس نظرسنجی انجام شده توسط سیمانتیک که شامل مصاحبه با ۲۰،۰۰۰ نفر در ۲۴ کشور بوده است، ۶۹٪ گزارش داده‌اند که قربانی یک حمله سایبری در طول زندگی خود بوده‌اند [105].

چرا حملات سایبری شکوفا می‌شود؟ به این دلیل است که حملات سایبری ارزانتر، راحت و کم خطرتر از حملات جسمی است [1]

مجرمان سایبری فقط به یک کامپیوتر و اتصال به اینترنت نیاز به هزینه‌های کمی دارند. آن‌ها از نظر جغرافیایی و مسافت محدود نیستند. به دلیل ماهیت ناشناس بودن اینترنت، هویت و پیگرد قانونی آنها دشوار است. با توجه به اینکه حملات علیه سیستم‌های فن آوری اطلاعات بسیار جذاب است، انتظار می‌رود تعداد و پیشرفت‌های حملات سایبری همچنان رو به رشد باشد.

نگرانی امنیت سایبری با درک از اطراف مسائل مربوط به حملات سایبری متنوع و ابداع استراتژی دفاع (یعنی اقدامات متقابل) است که حفظ محرمانگی، یکپارچگی و در دسترس بودن هر ته دیجیتال و اطلاعات را درنظر می‌گیرد[18] .

- **محرمانه** اصطلاحی است که برای جلوگیری از افشای اطلاعات برای افراد یا سیستم‌های غیرمجاز به کار می‌رود.
- **صداقت** اصطلاحی است که برای جلوگیری از هرگونه اصلاح / حذف به روشی غیرمجاز به کار می‌رود.
- در **دسترس بودن** اصطلاحی است که برای اطمینان از سیستم‌های مسئول تهیه، ذخیره و پردازش اطلاعات در صورت نیاز و توسط افراد نیازمند در دسترس است.

بسیاری از کارشناسان امنیت سایبری معتقدند که بدافزار گزینه اصلی سلاح برای انجام بد دهنی است و قصد دارد در تلاش برای امنیت سایبری در فضای مجازی نقض کند [12]. بدافزارها به طبقه گسترده‌ای از حملات اشاره می‌کنند که به طور معمول بدون اطلاع صاحب قانونی از سیستم بارگیری می‌شود تا سیستم را به سود یک طرف مقابل سازش کند. بنابراین کلاسهای نمونه بدافزار شامل ویروس‌ها، کرم‌ها، اسب‌های تروجان، نرم افزارهای جاسوسی و ربات‌های اجرایی هستند[15]. بدافزارها سیستمها را به روشهای مختلفی برای انتشار نمونه از دستگاههای آلوده، فریب کاربر برای باز کردن فایلهای ضخیم، یا جذب کاربران به سایتهای تبلیغی بدافزار آلوده می‌کنند. در نمونه بارزتر آلودگی به بدافزار، ممکن است بدافزار خود را بر روی درایو[1] قرار داده شده در یک دستگاه

[1] USB

آلوده بارگذاری کرده و سپس هر سیستم دیگری را که متعاقباً در آن دستگاه قرار داده شده، آلوده کند. ممکن است بدافزارها از طریق دستگاهها و تجهیزاتی که حاوی سیستمهای جاسازی شده و منطق محاسباتی هستند، پخش کنند. به طور خلاصه، بدافزارها را می‌توان در هر نقطه از چرخه عمر سیستم وارد کرد. قربانیان بدافزار می‌توانند از سیستم‌های کاربر نهایی، سرورها، دستگاه‌های شبکه (به عنوان مثال ، روترها، سوئیچ‌ها و غیره) و سیستم‌های کنترل فرآیند مانند کنترل نظارت و دستیابی به اطلاعات[2] برخوردار باشند. گسترش و پیشرفته‌تر شدن سریع تعداد بدافزارها امروزه یکی از دغدغه‌های اصلی اینترنت است.

به طور سنتی، حمله بدافزارها در یک نقطه از سطح در بین تجهیزات سخت افزاری، قطعات نرم افزاری یا در سطح شبکه با بهره گیری از آسیب پذیری های موجود در طراحی و اجرای موجود در هر لایه اتفاق افتاده است. به جای محافظت از هر دارایی، از استراتژی دفاعی محیط استفاده می‌شود که عمدتاً برای قرار دادن دیوار در خارج از تمام منابع داخلی برای محافظت از همه چیز در داخل از هرگونه نفوذ ناخواسته از خارج استفاده می‌شود. اکثر سازوکارهای دفاعی محیطی از نرم افزارهای ضد آتش و ضد ویروس نصب شده در سیستم نفوذ استفاده می‌کنند. هرگونه ترافیکی که از خارج وارد شود، مورد ضبط و بررسی قرار می‌گیرد تا اطمینان حاصل شود که هیچ بدافزار به منابع داخل نفوذ نمی‌کند. استقبال عمومی از این مدل دفاعی محیطی اتفاق افتاده است زیرا تأمین امنیت یک محیط بسیار آسانتر و به ظاهر کم هزینه‌تر از آن است که بتواند حجم زیادی از برنامه‌ها یا تعداد زیادی شبکه داخلی را تأمین کند. برای دسترسی بیشتر تعریف شده به منابع داخلی خاص، از مکانیسم‌های کنترل دسترسی در رابطه با مکانیسم دفاعی محیط استفاده شده است. در بالای دفاع محیطی و کنترل دسترسی، مسئولیت پذیری برای شناسایی یا مجازات هرگونه سوء رفتار، با این حال، تلاش‌های ترکیبی از استراتژی دفاعی محیطی با پیشرفت و پیشرفت نرم افزارهای مخرب، ناکارآمد است. همیشه به نظر می‌رسد که بدافزارهای در حال تکامل، حفره‌هایی پیدا می‌کنند که در کل از دفاعی محیط پیرامون خود دور بزنند. ما با جزئیات بیشتر متداول‌ترین بهره برداری‌ها را در سه بخش مجزا از سیستم اطلاعات موجود در لایه‌های سخت افزاری، نرم افزاری و شبکه توصیف می‌کنیم. سپس درباره جوانب مثبت و منفی‌ترین مکانیسم‌های دفاعی که در این لایه‌ها استفاده شده است بحث می‌کنیم.

بدافزار با گذشت زمان از سرمایه گذاری بر رویکردهای جدید استفاده می‌کند و از نقص‌های موجود در فن آوری های نوظهور برای جلوگیری از تشخیص استفاده می‌کند. ما تعدادی از الگوهای جدید حملات بدافزار موجود در فن آوری های نوظهور را شرح می‌دهیم.

در انتخاب فن آوری های نوظهور برای تصویر، ما معدودی را مورد توجه قرار می‌دهیم که شیوه زندگی روزانه خود را تغییر داده‌اند. این موارد شامل رسانه‌های اجتماعی، رایانش ابری، فناوری تلفن‌های هوشمند و زیرساخت‌های مهم است. ما در مورد ویژگی‌های منحصر به فرد هر یک از این فن آوری های نوظهور و چگونگی استفاده بدافزار از ویژگی‌های منحصر به فرد برای افزایش حرفه‌ای خود بحث می‌کنیم. به عنوان مثال، رسانه‌های اجتماعی، مانند سایت‌های شبکه‌های اجتماعی و وبلاگ‌ها، اکنون جزئی جدایی ناپذیر از سبک زندگی ما هستند زیرا بسیاری از افراد

[2] SCADA

در مورد وقایع زندگی خود، روزنامه نگاری، و همچنین دوست داشتن، روزنامه نگاری می‌کنند. مخالفان با درک پتانسیل خود برای پیوند زدن میلیونها نفر به یکباره، از حسابهای رسانه‌های اجتماعی برای دوست داشتن کاربران مظنون استفاده می‌کنند تا از آنها به عنوان وسیله نقلیه برای ارسال اسپم به دوستان قربانی استفاده کنند در حالی که دستگاه قربانی در بخشی از بات نت قرار می‌گیرد.

استفاده از منابع رایانه‌ای مانند برنامه‌های کاربردی که در آن کاربران فقط هزینه‌ای را برای استفاده پرداخت می‌کنند بدون آنکه نیاز به هزینه اضافی داشته باشند یا نیاز به مهارت در مدیریت زیرساخت‌های محاسباتی پیچیده داشته باشند. وسعت روز افزون داده‌های متمرکز در سرویس‌های ذخیره سازی ابر اکنون مهاجمین را به خود جلب می‌کند. در ژوئن ۲۰۱۲، مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) با کاهش نقص در سرویس پست صوتی AT & Tبرای کاربران تلفن همراه خود سرویس کاهش تقاضای خدمات[3] را در به همین ترتیب، سرویس بازیابی حساب Google برای کاربران CloudFlare به خطر انداختند[19] . با رشدی که در سال ۲۰۱۵ توسط ۲ میلیارد کاربر گوشی‌های هوشمند انجام شده است، رشد مهمی در بدافزارهای موبایل در سالهای اخیر شاهد بوده است. به عنوان مثال، تعداد تشخیص‌های منحصر به فرد بدافزار برای اندروید در جهان در سال ۲۰۱۲ نسبت به سال قبل17برابر افزایش یافته است [107]. همچنین در مورد تهدیدهای سایبری به زیرساخت‌های حساس مانند شبکه‌های برق و سیستم‌های مراقبت‌های بهداشتی برای استفاده در تروریسم، خرابکاری و جنگ اطلاعات، نگرانی‌های رو به رشد وجود دارد. جدای از تحقیق در مورد بهره برداری از طریق ویژگی‌های منحصر به فرد در فن آوری های منتخب در حال ظهور، ما همچنین در مورد الگوهای حمله بدافزارها به طور کلی بحث می‌کنیم تا روش‌ها و روند حملات جدید را بفهمیم.

سرانجام، ما مشاهدات سوداگرانه خود را به عنوان مکانهای تحقیق در نظر گرفته شده است. این موارد عبارتند از: (۱) نگرانی‌های مربوط به حریم خصوصی برای محافظت از افزایش حجم اطلاعات شخصی وارد شده در اینترنت، (۲) الزام به داشتن نسل جدیدی از اینترنت ایمن از ابتدا با در نظر گرفتن الگوهای رشد و استفاده ذهنی که چنین نبوده است. با اینترنت که امروزه از آن استفاده می‌کنیم، (۳) سیستم معتبری که معماری بنیادی آن متفاوت از ابتدای آنها در برابر تحمل هرگونه بدافزار در حال تحول است، (۴) قادر به شناسایی و ردیابی منبع حملات به کمک توسعه سیستم مدیریت هویت در مقیاس جهانی است. و تکنیک‌های ردیابی، و (۵) تأکید جدی بر امنیت قابل استفاده برای دادن کنترل‌های امنیتی به افراد که می‌توانند درک و کنترل کنند.

در اوایل دسامبر، بدافزارها به سادگی به عنوان آزمایشاتی برای برجسته سازی آسیب پذیری های امنیتی یا در برخی موارد برای نشان دادن توانایی‌های فنی نوشته می‌شدند. امروزه از بدافزارها برای سرقت اطلاعات حساس شخصی، مالی یا شغلی به سود دیگران استفاده می‌شود [129, 131]. به عنوان مثال، بدافزارها اغلب برای هدف قرار دادن وب سایتهای دولتی یا شرکتها برای جمع آوری اطلاعات محافظت شده یا مختل کردن عملکرد آنها استفاده می‌شود. در موارد دیگر، از بدافزارها علیه افراد برای بدست آوردن اطلاعات شخصی مانند شماره‌های امنیتی اجتماعی یا

[3] DDoS

شماره کارتهای اعتباری نیز استفاده می‌شود. از زمان ظهور دسترسی گسترده به اینترنت پهن باند که ارزان‌تر و سریعتر است، بدافزارها بطور فزاینده‌ای نه تنها برای مخفی کاری اطلاعات بلکه صرفاً برای اهداف سودآور طراحی شده‌اند [130]. به عنوان مثال ، اکثر بدافزارهای گسترده برای کنترل رایانه‌های کاربر برای استفاده در بازار سیاه مانند ارسال اسپم ایمیل یا نظارت بر رفتارهای مرور کاربر کاربر و نمایش تبلیغات غیرمجاز طراحی شده‌اند. بر اساس گزارش گروه ضد بدافزار [101] ، در سال ۲۰۱۲ تعداد ۲۶ میلیون بدافزار جدید گزارش شده است.

نویسندگان بدافزار از تعدادی واسطه اجاره‌ای متفاوت برای پخش بدافزارها برای آلوده کردن سیستم قربانی استفاده می‌کنند. به طور سنتی، اسپم، فیشینگ و بارگیری وب متداولترین واسطه برای این منظور بوده‌اند.

-اسپم به ارسال پیام‌های نامربوط، نامناسب و ناخواسته به هزاران دیسی یا میلیون‌ها گیرنده اشاره دارد. از آنجایی که اسپم به صورت ناشناس و بدون هزینه‌ای که فراتر از مدیریت لیست‌های پستی باشد، ناخواسته ارسال شده است اما هرزنامه یک بازار بسیار سودآور است. به دلیل وجود چنین مانع کم برای ورود، اسپم‌ها بی شمار هستند و حجم نامه‌های دارای مجوز غیرقابل رشد بسیار زیاد شده است. در سال ۲۰۱۱، رقم تخمینی برای پیام‌های اسپم حدود هفت تریلیون است [2]. این رقم شامل هزینه‌های مربوط به بهره وری و کلاهبرداری از دست رفته و ظرفیت اضافی لازم برای مقابله با هرزنامه است. امروزه، بیشترین اشکال هرزنامه شناخته شده اسپم‌ها، نامه‌های ناخواسته ایمیل است. مطابق گزارش کارگروه ضد سوءاستفاده پیام [1]، بین ۸۸ تا ۹۲ درصد پیام‌های ایمیل ارسال شده در نیمه اول سال ۲۰۱۰ اسپم بوده است.

فیشینگ راهی برای تلاش برای به دست آوردن اطلاعات حساس از قبیل نام کاربری، رمز عبور یا جزئیات کارت اعتباری با نقاب به عنوان یک نهاد قابل اعتماد است. بیشتر کلاهبرداری های فیشینگ به فریب کاربر در مراجعه به وب سایت‌های مخرب ادعا می‌کنند که از مشاغل و آژانس‌های قانونی استوار است. سوء استفاده کاربر وارد وب سایت مخرب می‌شود که بعداً توسط مجرمان مخرب مورد استفاده قرار می‌گیرد. به نظر می‌رسد اکثر روش‌های فیشینگ از نوعی فریب فنی استفاده می‌کنند که برای ایجاد پیوند در یک ایمیل (و وب سایت ناسازگار) طراحی شده‌اند که متعلق به یک سازمان قانونی ، مانند بانک معروف است. URLهای نادرست یا استفاده از زیر دامنه‌ها ترفندهای متداولی است که توسط فیشرها استفاده می‌شود. گزارش فنی ضد فیشینگ [101]بیان داشت که، در سال ۲۰۱۱ روند قابل توجهی از فیشرها برای پنهان کردن اهداف خود با جلوگیری از استفاده از میزبان IP obv ious برای میزبانی صفحات ورود به سیستم جعلی وجود دارد. در عوض، فیشرها برای جلوگیری از شناسایی، ترجیح می‌دهند در یک دامنه به خطر بیافتند. گزارش شده است که ۱۶ درصد کاهش در تعداد URL های فیشینگ حاوی نام شرکت spoofedدر URL وجود دارد. روند SE ترکیب نشان دهد که چگونه از فیشینگ در حال سازگار به عنوان کاربران تبدیل شدن بیشتر مطلع و آگاه در مورد صفات از یک سرقت از معمولی است.

دانلود درایورها– مربوط به بارگیری‌های ناخواسته بدافزار از اینترنت است و به طور فزاینده‌ای توسط مهاجمین استفاده می‌شود تا سریع بدافزارها را گسترش دهند. بارگیری درایو در شرایط متنوعی اتفاق می افتد. به عنوان مثال، وقتی کاربر از یک وب سایت بازدید می‌کند، هنگام مشاهده پیام ایمیل توسط کاربر یا وقتی کاربران روی یک پنجره فریب

دهنده پاپ آپ کلیک می‌کنند. با این حال، محبوب‌ترین بارگیری‌های درایو هنگام بازدید از وب سایت‌ها اتفاق می افتد. تعداد فزاینده‌ای از صفحات وب به انواع مختلف بدافزارها آلوده شده‌اند. مطابق نظرسنجی تحقیقات [3] تا سال ۲۰۰۸، ۱۱ میلیون انواع بدافزار کشف شد و ۹۰٪ این بدافزارها از دانلودهای پنهان از وب سایتهای محبوب و غالباً قابل اعتماد ناشی می‌شوند. قبل از اینکه بارگیری انجام شود، ابتدا یک کاربر باید به سایت مخرب مراجعه کند. برای اینکه کاربران را به بازدید از وب سایت با محتوای مخرب سوق دهند، مهاجمین ایمیل‌های اسپم را ارسال می‌کنند که پیوندهایی به سایت دارند. در هنگام مراجعه به وب سایت مشکوک کاربر مشکوک، بدافزارها بدون اطلاع کاربر در دستگاه قربانی بارگیری و نصب می‌شوند. به عنوان مثال، کرم بدنام طوفان باعث می‌شود تا از شبکه شخصی خود، چندین رایانه آلوده، برای ارسال ایمیل‌های اسپم حاوی پیوند به چنین صفحات حمله استفاده کند [102]

۲. از بین بردن آسیب‌های موجود در مقابل بد افزارها (کاربردهای متصور از طرح)

پس از اجرای بدافزار به سیستم قربانی، مجرمان سایبری می‌توانند جنبه‌های مختلفی از آسیب پذیری های موجود در سیستم قربانی را به کار گیرند و از آنها در فعالیت‌های جنایی خود استفاده کنند. ما بیشترین توانایی‌های آسیب پذیر موجود را در سخت افزار، نرم افزار و سیستم‌های شبکه مورد سوء استفاده قرار می‌دهیم. این بعد از بحث در مورد تلاشهای موجود است که برای کاهش اثرات منفی از بهره برداری‌ها پیشنهاد شده است.

۱.۲ سخت افزار

سخت افزار ممتازترین موجودیت است و بیشترین توانایی را برای دستکاری در یک سیستم محاسباتی دارد. این سطح در حالی است که این امکان را دارد که در صورت به خطر انداختن سخت افزار، به مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) منعطف و قدرت انعطاف پذیری گسترده‌ای را انجام دهد تا در صورت به خطر انداختن حملات امنیتی مخرب [23]،[24]. با حملات سطح نرم افزار مقایسه کنید که بسیاری از تکه‌های امنیتی، ابزارهای تشخیص نفوذ و اسکنرهای ضد ویروس برای شناسایی دوره‌ای از حملات مخرب وجود دارد ، بسیاری از حملات مبتنی بر سخت افزار توانایی فرار از چنین تشخیصی را دارند. بهره گیری در فقدان ابزار پشتیبانی در شناسایی سخت افزار، حملات مبتنی بر سخت افزار گزارش شده است که در حال افزایش است [23].

در میان انواع مختلف سوء استفاده از سخت افزار، سخت افزار تروجان مخوف‌ترین و متداول‌ترین سوء استفاده از سخت افزار است [24]. سخت افزار تروجان اصلاح شده مخرب و عمداً مخفی است که در سخت افزار در دستگاه‌های الکترونیکی از قبیل Integrity Circuits (IC) در سخت افزار ایجاد شده است [25]. سخت افزارتروجان دارای درجه‌های مختلفی است که باعث ایجاد انواع مختلفی از اثرات نامطلوب می‌شود. یک تروجان سخت افزاری ممکن است باعث شود که ماژول تشخیص خطا ورودی‌هایی را که باید رد شوند، بپذیرد. یک تروجان ممکن است بافرهای بیشتری را در اتصالات تراشه وارد کرده و از این رو انرژی بیشتری مصرف کند، که به نوبه خود می‌تواند باتری را به سرعت تخلیه کند. در مورد جدی‌تر، تروجان های Denial-of-Service (DoS) مانع از عملکرد یک منبع یا منابع می‌شوند. تروجان می‌تواند باعث شود که ماژول هدف از منابع کمیاب مانند پهنای

باند، محاسبات و باتری استفاده شود. همچنین می‌تواند به صورت فیزیکی پیکربندی دستگاه را از بین ببرد، غیرفعال یا تغییر دهد، و باعث شود پردازنده نتواند وقفه را از یک محیط خاص نادیده بگیرد.

از آنجا که احتمال سخت افزار تقلبی غیرقانونی برای داشتن پشتیبان مخرب یا سخت افزار تروجان ها افزایش می‌یابد، کلون‌های غیرقانونی سخت افزار به منبع لک‌های سخت افزاری تبدیل می‌شوند. شانس تولید سخت افزار غیرمجاز با روند جدیدی در شرکت‌های ITدر تلاش برای کاهش هزینه IT خود از طریق و خرید سخت افزار غیر قابل اعتماد از سایت‌های آنلاین افزایش یافته است. کاری و همکاران [26]بحث می‌کند که چگونه مدل IT در خارج از تأمین منابع مالی در افزایش شانس تولید قطعات سخت افزاری سخت کارخانه‌های غیر قابل اعتماد در کشورهای خارجی کمک کرده است. به همین ترتیب، همچنین خاطرنشان می‌شود که شرکت‌های IT اغلب سخت افزارهای غیر قابل اعتماد مانند تراشه‌ها و روترها را از سایت‌های حراج آنلاین یا فروشندگان خریداری می‌کنند که به نوبه خود ممکن است دارای تروجان های سخت افزاری مضر باشد. این شیوه‌ها نه تنها برای شرکت‌های ITکه بر روی سخت افزار دستکاری شده و دارای ورودی درونی بالقوه کار می‌کنند مشکل ساز است ، بلکه این احتمال را می‌دهد که طرح اصلی و جزئیات حالات داخلی سیستم به افراد غیرمجاز فاش شود.

حملات کانال جانبی هنگامی اتفاق می افتد که مخالفان با بررسی اطلاعات فیزیکی دستگاه مانند مصرف برق، تابش الکترومغناطیسی و اطلاعات زمان بندی اطلاعات در داخل و خارج ازCPU ، اطلاعاتی در مورد حالات داخلی سیستم بدست آورند. داده‌های حساس را می‌توان از طریق نتایج چنین حملات کانال جانبی فاش کرد. رویکردی در [22]گزارش شده است که کلید رمز پنهان الگوریتم رمزنگاری شده در نتیجه تحلیل فرکانس رادیویی را نشان می‌دهد.

تعدادی از تکنیک‌ها برای خنثی کردن حملات به سخت افزار سخت افزار ارائه شده است. دستگاه‌های سخت افزاری مقاوم در برابر Tamper به دلیل اهمیت آن به عنوان نقطه ورود به امنیت کلی سیستم، مورد توجه مهمی قرار گرفته‌اند. ماژول بسترهای نرم افزاری مورد اعتماد (TPM) فراهم می‌کند اولیه اولیه رمزنگاری و ذخیره سازی محافظت شده همراه با عملکرد عملی برای تبادل شواهد مقاوم در برابر دستکاری با سرورهای از راه دور [29-31،28]. اصطلاح (TCB[۴]) برای اشاره به بخش‌هایی از یک سیستم، مجموعه کلیه قطعات سخت افزاری و نرم افزاری تعریف شده است که برای امنیت کلی سیستم بسیار مهم است. TCBباید دارای اشکالات یا آسیب پذیری هایی باشد که در داخل اتفاق می افتد زیرا این ممکن است امنیت کل سیستم را به خطر اندازد. بررسی کامل و دقیق مبنای کد آن از طریق نرم افزار آیودیت یا برنامه تأیید صحت برنامه برای اطمینان از امنیت TCB انجام می‌شود. در واترمارک سخت افزاری، اطلاعات مالکیت در توضیحات مدار تعبیه شده و پنهان می‌شود که از جعل غیرقانونی شیء میزبان جلوگیری می‌کند. سخت افزار سخت افزاری تکنیکی برای اصلاح توضیحات یا ساختار سخت افزار الکترونیکی برای پنهان کردن عمدی عملکرد آن است [22]. این تکنیک‌ها برای جلوگیری از بدست آوردن مخالفان از طراحی اصلی یا جعل/ کلون کردن قسمت‌های مهم سخت افزار مانند واحدهای ICاستفاده می‌شوند. برخی از

[۴] Trusted Computing Base

اقدامات متقابل برای شمارش در برابر حملات کانال جانبی شامل معرفی صداهایی است به طوری که نمی‌توان اطلاعات فیزیکی را مستقیماً نمایش داد، برخی از قسمت‌های اطلاعات فیزیکی را فیلتر می‌کند، و ایجاد / کور می‌کند که به دنبال از بین بردن هرگونه ارتباط بین داده‌های ورودی و انتشار کانال جانبی است [23, 24]

۲,۲. رفع نقص نرم افزار

یک اشکال نرم افزاری اصطلاح رایجی است که برای توصیف خطا، عیب، خطا یا خطا در یک برنامه رایانه‌ای مانند سیستم عامل داخلی، درایورهای خارجی I / O رابط و برنامه‌های کاربردی استفاده می‌شود [103]. حملات سایبری از خطاهای نرم افزاری در مزایای خود استفاده می‌کنند تا باعث شوند سیستم‌ها به شیوه‌های ناخواسته‌ای که با قصد اصلی آنها متفاوت است رفتار کنند. امروزه اکثر حملات سایبری همچنان در نتیجه آسیب پذیری های نرم افزارهای کاوشگر ناشی از اشکالات نرم افزاری و نقص در طراحی رخ می‌دهد [104].

سوء استفاده مبتنی بر نرم افزار هنگامی رخ می‌دهد که از ویژگی‌های خاصی از نرم افزارهای stack و رابط استفاده شود. بیشترین آسیب پذیری نرم افزار به عنوان یک پیامد بهره برداری از نرم افزار دانلود رخ اشکالات دوباره در حافظه، اعتبار سنجی ورودی کاربر، شرایط مسابقه و امتیازات دسترسی کاربر 40]،39،[42. نقض ایمنی حافظه توسط مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) انجام می‌شود تا محتوای یک مکان حافظه را تغییر دهند. بیشترین روش نمونه گیری، سرریز بافر است. گردش بافر ovarهنگامی رخ می‌دهد که یک برنامه سعی می‌کند داده‌های بیشتری را در یک بافر از آنچه که برای نگهداری در نظر گرفته شده است، ذخیره کند. از آنجا که بافرها برای حاوی مقدار محدودی از داده‌ها ایجاد می‌شوند، اطلاعات اضافی می‌توانند به درون بافرهای مجاور سرریز شوند و داده‌های معتبری که در آنها نگهداری می‌شود را خراب یا بازنویسی کنند. این اجازه می‌دهد تا مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) به کد فرآیند موجود مداخله کنند. اعتبار سنجی ورودی فرایندی است برای اطمینان از اینکه داده‌های ورودی از قوانین خاصی پیروی می‌کنند. اعتبارسنجی نادرست داده‌ها می‌تواند منجر به فساد داده‌ها شود، همانطور که در تزریق SQL مشاهده می‌شود. SQL inje ction یکی از شناخته شده ترین تکنیک‌هایی است که از یک خطای برنامه در نرم افزار وب سایت بهره برداری می‌کند. یک مهاجم دستورات SQL را از فرم وب تزریق می‌کند یا محتوای دیتابیس را تغییر می‌دهد یا اطلاعات دیتابیس مانند کارتهای اعتباری یا کلمه عبور را برای حمله به آن ریخته است. طرف مقابل از نقص در فرآیندی سوء استفاده می‌کند که خروجی فرایند به طور غیر منتظره و جدی وابسته به زمان وقایع دیگر باشد. زمان بررسی تا زمان استفاده، اشکالی است که در اثر تغییر در سیستم بین بررسی یک شرکت همکاری و استفاده از نتایج آن چک ایجاد می‌شود. همچنین به آن خطای شرط بهره برداری می گویند. سردرگمی Privilege عملی با سوءاستفاده از یک اشکال با دسترسی زیاد به منابعی است که بطور معمول از یک برنامه یا کاربر محافظت می‌شوند. نتیجه این است که مخالفان با امتیازات بیشتری اقدامات غیرمجاز مانند دسترسی به کلیدهای مخفی محافظت شده را انجام می‌دهند.

در جامعه برنامه نویسی، تعدادی پروژه آغاز شده است که به افزایش امنیت به عنوان یک هدف اصلی اختصاص داده شده است [36-38]. بدون تی تنها حضور به رفع مجموعه مشترک ذاتی نقص‌های امنیتی، نگرانی اصلی از این

پروژه‌ها است که به ارائه ایده‌های جدید در تلاش برای ایجاد یک محیط امن. در یک روش کدنویسی ایمن مبتنی بر بررسی کد، مهندسان نرم افزار خطاهای برنامه نویسی رایج را که منجر به آسیب پذیری نرم افزار می‌شود، تعیین استانداردهای رمزگذاری ایمن استاندارد، آموزش توسعه دهندگان نرم افزار و پیشبرد وضعیت این روش در رمزگذاری ایمن، شناسایی می‌کنند. در یک روش برنامه نویسی ایمن مبتنی بر زبان، تکنیک‌هایی برای اطمینان از اینکه به برنامه‌ها می‌توان به عدم نقض سیاست‌های مهم امنیتی اعتماد کرد، استفاده شده است. پرکاربردترین تکنیک‌ها شامل تجزیه و تحلیل و دگرگونی است. یک شکل شناخته شده از تجزیه و تحلیل عبارت است از "بررسی نوع" که در آن برنامه قبل از اجرای برنامه، انواع بی خطر بودن اجسام را شناسایی می‌کند. یکی دیگر از اشکال شناخته شده از تحول برنامه علاوه بر این از چک زمان اجرا که در آن برنامه را در راه آمادهسازی است که مانع از این برنامه را از هر گونه تغییر و تحول سیاست نقض [42]. کد فرآیندی برای تولید منبع یا کد دستگاه است که درک آن برای انسان دشوار بوده است [43]،[44]. برنامه نویسان غالباً برای پنهان کردن هدف یا منطق آن، از کد برای جلوگیری از هرگونه امکان در مهندسی معکوس، آگاهانه کد می‌کنند. چرخه طراحی و توسعه ایمن نیز در [41]، [27] ارائه شده است که مجموعه‌ای از تکنیک‌های طراحی را امکان پذیر می‌سازد تا تأیید کارآمد را انجام دهد که یک قطعه از اجزای سیستم عاری از هرگونه نقص احتمالی از طرح اصلی خود باشد. اگرچه آنها رویکردهای تند و تیز چندانی ندارند، اما روشهای رسمی امکان کاوش جامع در طراحی و شناسایی آسیب پذیری های امنیتی پیچیده را فراهم می‌آورد. ابزاره [34]، [35و تکنیکهای 32]، [33]برای تسهیل در تأیید ویژگیهای مهم ایمنی مأموریت تهیه شده‌اند. این ابزارها و تکنیک‌ها به ترجمه اهداف امنیتی سطح بالاتر در مجموعه‌ای از خصوصیات اتمی برای تأیید کمک می‌کنند.

۲،۳. زیرساخت‌های شبکه و آسیب پذیری های پروتکل

پروتکل اولیه شبکه برای پشتیبانی از محیطی کاملاً متفاوت که امروزه در مقیاس بسیار کوچکتر ایجاد شده ساخته شده است و اغلب در بسیاری از موقعیت‌هایی که امروزه مورد استفاده قرار می‌گیرد به درستی کار نمی‌کند. ضعف در پروتکل‌های شبکه وقتی پیچیده باشد که هم مدیران سیستم و هم کاربران از دانش محدودی در مورد زیرساخت‌های شبکه استفاده کنند [46]،[47] . به عنوان مثال، سرپرستان سیستم از طرح رمزگذاری کارآمد استفاده نمی‌کنند، تکه‌های توصیه شده را به موقع اعمال نمی‌کنند، یا استفاده از فیلترها یا خط مشی‌های امنیتی را فراموش می‌کنند.

یکی از رایج‌ترین حملات شبکه با سوء استفاده از محدودیت‌های پروتکل شبکه متداول پروتکل اینترنت(IP) ، پروتکل کنترل انتقال (TCP) یا سیستم نام دامنه (DNS) رخ می‌دهد [14]. پروتکل اصلی لایه شبکه است. اطلاعات مورد نیاز برای روت کردن بسته‌ها در بین روترها و رایانه‌های شبکه را فراهم می‌کند. پروتکل IP اصلی هیچ مکانیسمی برای بررسی صحت و حریم خصوصی داده‌های منتقل شده ندارد. این اجازه می‌دهد تا هنگام انتقال از طریق شبکه ناشناخته بین دو دستگاه ، داده‌ها رهگیری یا تغییر داده شوند. برای جلوگیری از بروز مشکل، IPSec برای رمزگذاری ترافیک IP ایجاد شد. در سالهای متمادی، IPSecبه عنوان یکی از اصلی‌ترین فناوری‌ها برای ایجاد یک شبکه خصوصی مجازی (VPN) مورد استفاده قرار گرفته است که یک کانال امن الکترونیکی را از طریق اینترنت بین یک کامپیوتر از راه دور و یک شبکه قابل اعتماد (یعنی اینترانت شرکت) ایجاد می‌کند. TCPدر

بالای IP قرار دارد تا بسته‌ها را به صورت قابل اعتماد (یعنی انتقال مجدد بسته‌های از دست رفته) منتقل کند و دستور تحویل بسته‌ها را صادر کرد. SSL در ابتدا برای تأمین امنیت پایان به پایان رسید، به عنوان مخالف تنها پروتکل مبتنی بر لایه، بین دو رایانه که در پروتکل کنترل انتقال قرار دارد (TCP) قرار دارد. SSL / TLS معمولاً از http استفاده می‌شود تا https را برای صفحات وب ایمن ایجاد کند. سرور نام دامنه (DNS)پروتکلی است که اسامی میزبان قابل خواندن انسان را به آدرسهای پروتکل ۳۲ بیتی اینترنت (IP) ترجمه می‌کند. در اصل به عنوان یک کتاب دایرکتوری برای روترهای اینترنتی گفته می‌شود که آدرس IP را برای راهنمایی بسته‌ها هنگام کاربر URL به کار می‌برد. از آنجا که پاسخ‌های DNS تأیید نشده است، ممکن است یک مهاجم بتواند پیام‌های DNSمخرب را برای جعل هویت یک سرور اینترنتی ارسال کند. یکی دیگر از نگرانی‌های عمده در موردDNS ، در دسترس بودن آن است. از آنجا که حمله موفقیت آمیز علیه سرویس DNS باعث ایجاد اختلال در ارتباطات مهمی در اینترنت می‌شود، DNSهدف حملات چند انکار سرویس (DoS) قرار گرفته است.

رمزنگاری یک ابزار ضروری برای محافظت از داده‌هایی است که از طریق رمزگذاری داده‌ها بین کاربران منتقل می‌شود به گونه‌ای که فقط کاربران در نظر گرفته شده با کلیدهای مناسب می‌توانند رمزگشایی داده‌ها را انجام دهند. رمزنگاری رایج‌ترین مکانیسم مورد استفاده در حفاظت از داده‌ها است. نظرسنجی انجام شده توسط موسسه امنیت رایانه در سال ۲۰۰۷ [132]نشان داد که ۷۱٪ از شرکتها از رمزگذاری برای داده‌های خود در ترانزیت استفاده می‌کنند. با استفاده از محدودیت‌های الگوریتم‌های رمزنگاری موجود، تعدادی از حرکات در حال افزایش هستند. انستیتوی ملی استاندارد و فناوری ایالات متحده (NIST) اخیراً از قطع SHA-1 و استفاده از استاندارد Advanced Hash (ASH)از سال ۲۰۱۲ خبر داد [15]. پتانسیل استفاده از رمزگذاری مبتنی بر هویت، یک برنامه تحقیقاتی فعال برای برنامه‌هایی است که نیاز به رمزگذاری سریع دارند برای جلوگیری از استفاده از طول کلید آهسته ۲۰۴۸ بیتی آهسته به همراه دخالت نادرست مقام صدور گواهینامه معتبر [15]. رمزنگاری کوانتومی یک فناوری نوظهور است که در آن دو طرف همزمان با استفاده از انتقال حالتهای کوانتومی از نور، کلید اصلی رمزنگاری مخفی مشترک، را تولید می‌کنند [48].

مخالفان ماهر امروز از یک تکنیک پیشرفته استفاده می‌کنند که مبلغ ترافیکی مخرب را مبدل می‌کند که بیشتر شبیه به بارهای ترافیکی قانونی است. علاوه بر این، حجم زیادی از جریان داده‌ها در شبکه‌های با ظرفیت بالا به تکنیک‌های تجزیه و تحلیل جدید نیاز دارد تا محاسبه یک dنیز عدم اطمینان به مجموعه داده‌ها را تجسم کند. این چالش زمینه تحقیق جدیدی را ایجاد کرده است که مجموعه مهارتهای ترکیبی از دست اندرکاران شبکه و جامعه تجسم لازم است تا ترافیک شبکه را با تکنیک‌های بهتر سازی بصری یونی جذب کند [53]. ارائه بصری از داده‌ها سپس توسط کارشناسان شبکه با دانش عمیق دامنه در سیستم شبکه تحلیل می‌شود.

3.4بحث

اگرچه بسیاری از تکنیک‌ها و پیشنهادات جداگانه برای اصلاح آسیب پذیری ها در سخت افزار، نرم افزارهای نرم افزاری و لایه‌های شبکه وجود دارد، به جای اینکه روی هر لایه متمرکز شوید، تکنیک‌های محافظت از امنیت که

همه چیز را از حملات خارجی محافظت می‌کند، در روش سنتی اتخاذ شده است. اکثریت قریب به اتفاق شرکتها از یک مدل امنیتی دفاعی پیرامونی برای محافظت از شبکه شرکت از هرگونه نفوذ احتمالی در خارج استفاده می‌کنند [47]. این رویکرد بر استراتژی‌های "دفاع لایه‌ای" یا "دفاع در عمق" متمرکز است که در آن داراییهای مهم فناوری اطلاعات داخلی، مانند سرورها یا ماموریتهای مهم حیاتی ، توسط دیوارها و استحکامات محافظت می‌شوند.

پدافندهای محیطی معمولی شامل فناوری‌هایی مانند فایروال‌ها و سیستم‌های تشخیص نفوذ (IDS) هستند. فایروال پرکاربردترین فناوری برای محافظت از دارایی‌های داخلی بوده است. هدف اصلی آن کنترل ترافیک شبکه ورودی و خروجی از طریق تجزیه و تحلیل بسته‌های داده و تعیین اینکه آیا از طریق مجوز تعیین شده از پیش تعیین شده باید اجازه عبور یا اجازه آن را داشته باشد. یک فایروال را می‌توان در لایه‌های مختلف در زیرساخت شبکه قرار داد. فایروال‌های لایه شبکه، که فیلترهای بسته نیز نامیده می‌شوند، در سطح نسبتاً کم لایه شبکه کار می‌کنند و مانع عبور بسته‌ها از طریق فایروال نمی‌شوند، مگر اینکه با مجموعه قانون تعیین شده (یعنی تنظیمات) تعریف شده توسط واسطه‌های شبکه شبکه مطابقت داشته باشند. گرچه بسیاری از فایروال‌های مدرن پیشرفته‌تر هستند، اما فایروال‌های لایه شبکه نمی‌توانند ترافیک ناخواسته مانند بار نرم افزار مخرب را فیلتر کنند که از آدرس‌ها و پورت‌های IP قانونی استفاده می‌کند. فایروال لایه برنامه با نظارت و مسدود کردن صدای ضعیف تماس، ورودی یا خروجی سرویس‌های سیستم که خط مشی تنظیم شده فایروال لایه شبکه را برآورده نمی‌کند، کار می‌کند. سرور پروکسی ممکن است با پاسخگویی به بسته‌های ورودی (به عنوان مثال، درخواست اتصال) به شیوه برنامه در هنگام مسدود کردن سایر بسته‌ها، به عنوان یک فایروال عمل کند. فایروال لایه‌ای هر دو برنامه و همچنین پراکسی‌ها مشکل در سیستم داخلی را مشکل‌تر می‌کنند. اما با افزایش توانایی و ظرافت، مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) امروز روشهای حمله پیشرفته‌تری برای انتقال بسته‌های مخرب به یک شبکه هدف طراحی کرده‌اند. به عنوان مثال، متجاوزان ممکن است یک سیستم با دسترسی عمومی را ربوده و از آن به عنوان یک پروکسی برای اهداف خود استفاده کنند. با استفاده از پروکسی رهگیری شده، متجاوز با هدف مخفی کردن هویت فرستنده یا جعل هویت سیستم محاسباتی دیگر ، بسته‌هایی را با یک آدرس IP جعلی ایجاد می‌کند.

سیستم‌های تشخیص نفوذ فیلتر هر گونه فعالیت مشکوک و یا غیر عادی بر روی شبکه [19]،[47. این سیستم‌های ردیابی به شکلی با ارزش هستند که به دنبال آن هستند که مراحل اولیه حمله را کشف کنند (به عنوان مثال، یک پروب حمله کننده از ماشین یا شبکه برای آسیب پذیری های خاص) و در نتیجه می‌توانند در مراحل بعدی حمله به محافظت از یک دستگاه کمک کنند. همچنین، این سیستم‌ها به دنبال کشف علائم گوینده از فعالیت‌های مشکوک یا الگوهای رفتاری هستند که توسط کاربر، برنامه یا یک قطعه کد مخرب که فایروال‌ها یا سایر ابزارهای محافظ ممکن است از دست ندهد یا نادیده گرفته شود. بسیاری از شناسه‌های مختلف سیستم برای شناسایی بارهای مخرب شبکه وجود دارند. چنین تشخیص‌هایی یا مبتنی بر امضا یا مبتنی بر ناهنجاری است. در امضای مبتنی بر، سیستم تشخیص بسته‌های حمله را به دلیل اثر انگشت یا امضاهای شناخته شده خود می‌شناسد زیرا این بسته‌ها از آستانه دروازه شبکه عبور می‌کنند. در مبتنی بر ناهنجاری، سیستم تشخیص هیچ آگاهی قبلی از بسته‌های بدی ندارد.

سیستم تشخیص با بررسی الگو، غالباً در زمان واقعی، تعیین میزان ترافیک عادی را تعیین می‌کند و رفتارهای ترافیکی غیر عادی را بر اساس آنالیز در این الگو گزارش می‌دهد. سیستم شناسایی مبتنی بر امضا به دلیل عدم گسترش و پیشرفت نویسنده بدافزار در سالهای اخیر بی اثر تلقی شده است [۱۶،۱۷]. در نظر گرفته می‌شود که تقریباً غیرممکن است تا بتوانید امضای بدافزار در حال تکامل را با روشهای تشخیص الگوی که در روش مبتنی بر امضا مورد استفاده قرار می‌گیرد، جابجا کنید. پیشنهاد تشخیصات مبتنی بر ناهنجاری پیشرفته، یک منطقه فعال در زمینه تحقیقات بوده است [133]. در این روش، سیستم به طور مثال (یادگیری خود (می‌آموزد که با مشاهده ترافیک برای مدت زمان طولانی و ساختن الگویی از فرآیند زمینه‌ای، چه چیز عادی را تشکیل می‌دهد. روند تکامل (خود سازگار) با تکامل امضای بدافزار است.

به جای تمرکز بر روی اصلاح خاص به عنوان حفره‌های فایروال وIDS ، به منظور ایجاد ابعاد مکانیزم بهتر برای خنثی کردن ترافیک ناخواسته از منابع خارجی، رویکردهای کلی‌تر برای درک الگوهای حمله به شبکه مورد نیاز است. حوزه پزشکی قانونی شامل مطالعه نظارت و تحلیل پایش از طریق شبکه با استراق سمع به اترنت، / TCP IPیا اینترنت از جمله مرورگر وب، ایمیل، گروه خبری، چت همزمان و ترافیک همتا به همسالان است [49-51]. شواهد برای اقدام قانونی یا برای درک الگوهای حمله شبکه‌ای استفاده می‌شود. از هرگونه اطلاعاتی که توسط لانه زنبوری گرفته می‌شود برای تحقیق در مورد تهدیدهای سازمان‌ها و یادگیری چگونگی محافظت بهتر در برابر این بیماری‌ها استفاده می‌شود. تکنیک‌های مجازی سازی اغلب برای میزبانی چندین لانه زنبوری در یک دستگاه فیزیکی واحد استفاده می‌شود. بنابراین، حتی اگر آب شیرین به خطر بیفتد، احتمال بهبودی سریعتر با هزینه کمتر وجود دارد. یک لانه زنبوری در مقیاس بزرگ، مانند honeyne t که دو یا چند عسل دریایی را به یک شبکه وصل می‌کند، برای نظارت بر شبکه بزرگتر و متنوع‌تر استفاده می‌شود. این عسل‌ها غالباً به عنوان قسمت‌هایی از سیستم‌های بزرگتر تشخیص نفوذ شبکه اجرا می‌شوند. HoneyFarmیک مجموعه متمرکز از ابزارهای آنالیز و لانه زنبوری است [54].

از آنجا که امکان دستیابی یکنواخت به منابع امکان پذیر نیست، از مکانیسم‌های کنترل دسترسی استفاده شده است که یک اختیار را برای کنترل دسترسی به برخی منابع خاص فراهم می‌کند. در کنترل دسترسی، به اشخاصی که می‌توانند در سیستم عملکردهایی انجام دهند ، "موضوعات" نامیده می‌شوند و به اشخاصی که منابعی را که باید به آنها دسترسی داشته باشند، نیاز دارند کنترل می‌کنند، "اشیاء" نامیده می‌شوند. در کنترل دسترسی مبتنی بر قابلیت، به یک موضوع اعطا می‌شود اگر سوژه دارای یک مرجع یا توانایی باشد ، به یکشی دسترسی پیدا کند. به عنوان مثال، اگر یک کاربر شناسه و رمز ورود صحیح ارائه دهد، کاربر به مشاهده صورت بانکی خود اجازه می‌دهد. با انتقال چنین توانایی از طریق کانال امن، دسترسی به طرف دیگر انتقال می‌یابد. به عنوان مثال، گواهی نامه ایجاد شده است تا کاربر آن را برای تأیید صحت ارائه دهد. در رویکرد مبتنی بر لیست کنترل دسترسی، دسترسی یک موضوع به یک موضوع به این بستگی دارد که آیا هویت آن در لیست مرتبط با شی وجود دارد یا خیر. به عنوان مثال، اگر آلیس در لیست پزشکان قرار داشته باشد، به وی داده می‌شود تا سوابق بیمار را مشاهده کند. دسترسی یا ویرایش لیست انتقال می‌یابد. به عنوان مثال، وقتی آلیس از بیمارستان خارج شود، دیگر در لیست پزشکان قرار ندارد و قادر

به مشاهده سوابق بیمار نخواهد بود. سه روش مختلف شناخته شده کنترل عبارتند از: کنترل دسترسی اختیاری (DAC)، کنترل دسترسی اجباری (MAC) و کنترل دسترسی مبتنی بر نقش(RBAC) . درDAC ، مالک تصمیم می گیرد چه کسی اجازه دسترسی به اشیاء خاص و چه امتیازاتی را دارد. در روشMAC ، این سیستم عامل توانایی دسترسی سوژه‌ها (به عنوان مثال پردازش یا موضوع) را برای دسترسی یا انجام عملیات روی اشیاء (به عنوان مثال پرونده‌ها، فهرست‌ها، پورت‌های TCP / UDP یا بخش‌های حافظه مشترک) محدود می‌کند، یا با یک قاعده که تعریف می‌کند. شرایط خاص یا توسط یک ساختار ریاضی که بزرگترین مقادیر کم تحرک و کمترین حد بالایی را تعریف می‌کند. RBACیک رویکرد جایگزین جدیدتر برای MAC و DAC است که دسترسی به سیستم را فقط برای کاربران مجاز محدود می‌کند. این توسط اکثر شرکت‌ها استفاده می‌شود و اکثر فروشندگان IT RBACرا در محصولات سنگ معدن یک یا یک متر عرضه می‌کنند.

سیستم‌های کنترل دسترسی سنتی خدمات اساسی مانند تأیید اعتبار، مجوز و پاسخگویی را ارائه می‌دهند. احراز هویت و مجوز، فرایند تأیید صحت اتصال یک موضوع به یک شیء است. احراز هویت سنتی و مکانیسم‌های کمکی از سه عامل مختلف برای هویت یابی یک موضوع استفاده می‌کنند تا تأیید کنند آیا سوژه دارای توانایی درستی برای دسترسی به جسم است. عامل اول چیزی است که شما می‌شناسید، برای مثال رمزعبور یا شماره شناسایی شخصی (PIN). فرض می‌شود که فقط صاحب حساب که رمز یا پین را می داند برای دسترسی به حساب نیاز دارد. عامل دوم چیزی است که شما دارید و شامل کارت هوشمند یا علائم امنیتی است. این فرض می‌کند که فقط صاحب حساب دارای کارت هوشمند مورد نیاز برای باز کردن حساب است. عامل سوم چیزی است که شما دارید، مانند اثر انگشت، صدا یا خصوصیات عنبیه. روند فعلی در تأیید هویت، رویکردی لایه بردار است، که اغلب به عنوان احراز هویت قوی گفته می‌شود و به ارائه دو یا چند عامل تأیید اعتبار پاسخ می‌دهد [55]. تعدادی از انواع مختلف علائم احراز هویت به اندازه جیب پیشنهاد شده است. این نشانه‌ها حاوی یک کلید رمزنگاری در ذخیره سازی مقاوم در برابر دستکاری هستند. با استفاده از ماهیت همه گیر درگاه رایانه‌های رایانه ای امروز ، نشانه‌های مبتنی بر USB نیز به سادگی به عنوان ذخیره گواهی X.509 یا پروتکل چالش / پاسخ پیشنهاد شده‌اند 56]،13،[86. برای بهره مندی از جمعیت روزافزون در حال رشد کاربران تلفن همراه، تعدادی از اسناد مکانیزم تأیید اعتبار کاربران موبایل را هدف قرار داده‌اند [58-56]. از فناوری بیومتریک در کاربردهای محدود استفاده شده است. برخی از رایانه‌های شخصی و ایستگاه‌های کاری با رابطهای بصری و تصویری پیچیده‌تر شده‌اند، علاقه جدیدی به کار می رود که از فناوری بی هویت بیومتریک در محیط شبکه استفاده می‌کند 59]،60،[62.

پاسخگویی یکی دیگر از جنبه‌های کنترل دسترسی است که شامل مطالعه می‌شود که اطمینان حاصل کند که هر کسی یا هر چیزی که به یک مؤلفه سیستم دسترسی داشته باشد، مانند دستگاه محاسبات، برنامه، شبکه ، می‌تواند پاسخگوی نتایج چنین دسترسی باشد. پاسخگویی تکنیک‌ها و ابزاری را ارائه می‌دهد که می‌توانند هرگونه سوء رفتار را شناسایی و مجازات کنند [20]. تکنیک‌های متنوعی وجود دارد که محققان در پاسخگویی از آن استفاده می کنند، که مهم‌ترین آن‌ها حل مسئله، حسابرسی و حل اختلاف است [21.94]. مطالعه پاسخگویی به طور معمول با ورود به سیستم آغاز می‌شود. تعدادی پرونده ورود خودکار برای ثبت هرگونه اطلاعات دسترسی ایجاد شده است،

به عنوان مثال، پرونده‌های ورود به سیستم برای ثبت logons و logoff کاربر، برنامه شروع شده یا پرونده‌های دسترسی. چنین سیاهه های مربوط به تاریخ باید به اندازه کافی باشند تا مدارکی در مورد اختلافات بعدی ارائه دهند. شناسایی اطلاعات مهم برای ورود به سیستم یکی از مناطق تمرکز است. تکنیک‌های ورود به سیستم مقاوم در برابر Tamper ارائه شده است. Audi ts برای مشخص کردن روایی و اعتبار اطلاعات به طور معمول با بررسی پرونده‌های ورود به سیستم هنگام شناسایی یک مورد سوء استفاده انجام می‌شود (همچنین برای تشخیص مشکلات نیز به کار می‌رود). از ابزارهای نظارتی معمولاً در فرایند حسابرسی برای تجزیه و تحلیل کارایی و عملکرد سیستم استفاده می‌شود. حل تعارض به عنوان راهی برای مقابله با علت اصلی ارائه شده است، به عنوان مثال منع سرویس‌های نقض کننده از تعامل بیشتر یا ورود افراد متخلف به لیست سیاه. حریم خصوصی یک نگرانی فزاینده در زمینه پاسخگویی است. چه مقدار داده را می‌توان اسیر برای به عنوان مدرک استفاده بدون نقض حریم خصوصی یک کاربر سؤال تعدادی از محققان به آدرس سعی شده است [93].

۳. رفع تهدیدهای نوظهور (برون رفت از مشکلات و مسایل متصور در سازمان)

حملات سایبری به فضای مجازی از طریق سرانه زمانی تحریک می‌شود که رویکردهای جدید را می‌طلبد. بیشتر اوقات، مجرمان سایبری می‌توانند امضاهای موجود در بدافزارها را تغییر دهند تا از نقص موجود در فن آوری های جدید استفاده کنند. در موارد دیگر، آن‌ها به سادگی ویژگی‌های منحصر به فرد فن آوری های جدید را برای یافتن نقاط ضعف برای شناسایی بدافزار کشف می‌کنند. با استفاده از فن آوری های جدید اینترنت با میلیون‌ها و میلیارد کاربر فعال، مجرمان سایبری از این فن آوری های جدید استفاده می‌کنند تا به تعداد بسیار زیاد قربانیان سریع و کارآمد دسترسی پیدا کنند. ما چهار پیشرفت پیشرفته در زمینه فنی و حرفه‌ای را انتخاب می‌کنیم که شامل: رسانه‌های اجتماعی، رایانش ابری، فناوری تلفن‌های هوشمند و زیرساخت های مهم هستند، به عنوان نمونه بارز برای کشف تهدیدات موجود در این فناوری‌ها. ما در مورد خصوصیات منحصر به فرد هر یک از این فناوری‌های نوظهور بحث می‌کنیم و تعدادی از الگوهای حمله مشترک ارائه شده در آنها را تجزیه و تحلیل می‌کنیم.

۳,۱. رسانه‌های اجتماعی

رسانه‌های اجتماعی مانند فیس بوک و توییتر رشد انفجاری را در سالهای اخیر نشان داده‌اند. در پایان سال ۲۰۱۲، بیش از ۴۵۰ میلیون حساب کاربری فعال در توییتر وجود دارد در حالی که این تعداد در فیس بوک به صورت نمایی رشد می کند. سایت‌های شبکه‌های اجتماعی بسیار پرطرفدار بوده و به اکثر روش‌های ارتباطی برای اکثر نسل‌های جوان تبدیل شده‌اند. هر یک از این وب سایت‌های رسانه‌های اجتماعی به طور معمول ابزاری را ارائه می‌دهند که در آن کاربران اطلاعات شخصی خود را به اشتراک می‌گذارند (به عنوان مثال نام، آدرس ، تاریخ تولد، تاریخ تولد، اولویت در موسیقی و فیلم)، عکس، داستان و لینک‌های منتشر شده.

مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) از شوق رسانه‌های اجتماعی به عنوان یک وسیله جدید برای شروع حملات موذیانه استفاده می‌کنند. در پایان سال ۲۰۰۸، مجموعه آزمایشگاه کسپرسکی حاوی سنگ معدن بیش از ۴۳۰۰۰ پرونده مخرب مربوط به سایت‌های رسانه‌های اجتماعی بود [109]. گزارشی

که توسط شرکت امنیت IT و حفاظت از داده‌های Sophos منتشر شده است، از افزایش نگران کننده حملات کاربران وب سایت‌های رسانه‌های اجتماعی خبر داد. براساس گزارش آنها [111]، حدود ۶۰ درصد از کاربران در شبکه‌های اجتماعی هرزنامه دریافت کرده‌اند. با توجه به دسترسی نامحدود به پروفایل کاربران، مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) می‌توانند اطلاعات مربوط به اسرار شرکت و اسرار تجاری را بیشتر به دست آورند. در نظرسنجی انجام شده توسط سوفوس [111] ، حدود ۶۰٪ شرکت ها نگران هستند که کارمندان آنها اطلاعات زیادی را در شبکه‌های اجتماعی ارائه دهند در حالی که حدود ۶۶٪ شرکت‌ها فکر می‌کنند استفاده از شبکه‌های اجتماعی تهدید بزرگی برای شرکت‌ها محسوب می‌کند.

کرم Koobface [110] که در سال ۲۰۰۹ از طریق سایت‌های رسانه‌های اجتماعی پخش می‌شود، به ویژه شناخته شده ترین مورد مخرب است که از گسترش سایت‌های رسانه‌های اجتماعی استفاده می‌کند.

سایت‌های شبکه‌های اجتماعی نیز مخاطرات برای حفاظت از حریم خصوصی به دلیل مرکزیت مطرح کرده‌اند تورم از حجم انبوهی از داده‌های کاربر، صمیمیت از اطلاعات شخصی جمع آوری و در دسترس بودن داده تا به تاریخ است که همواره برچسب گذاری شده و فرمت شده [109]. این امر باعث می‌شود که سایت‌های شبکه‌های اجتماعی به عنوان هدف جذاب برای انواع مختلفی از سازمان‌ها به دنبال جمع آوری مقادیر زیادی از داده‌های کاربر، برخی برای اهداف مشروع و برخی برای موارد مخرب باشند. در بیشتر موارد، استخراج داده‌ها انتظار کاربران از حریم شخصی را نقض می‌کند. محافظت از داده‌های شخصی کاربر که در سرویس دهنده‌های شبکه‌های اجتماعی نگهداری می‌شوند، مورد بررسی قرار گرفته است. لوکاس و همکاران [112] برای رمزگذاری و رمزگشایی داده‌های حساس با استفاده از JavaScript در سمت مشتری، یک برنامه فیسبوک ارائه دادند. این معماری تضمین می‌کند که داده‌ها هرگز در ارائه دهنده خدمات شبکه‌های اجتماعی به شکلی غیرقابل توصیف وارد نمی‌شوند و از مشاهده و جمع آوری اطلاعاتی که کاربران از طریق شبکه انتقال می‌دهند، جلوگیری می‌کند. موضوعات و ابزارهای مربوط به آگاهی از حریم خصوصی که به کاربران کمک می‌کند تنظیمات حریم خصوصی خود را بطور مستقیم تر تنظیم کنند نیز پیشنهاد شده است.

۳،۲. پردازش ابری

کارآیی انتقال داده‌ها و برنامه‌های کاربردی به cloud همچنان به جذب مشتریانی است که داده‌های خود را در DropBoxو iCloud ذخیره می‌کنند، از Gmail و نامه Live برای مدیریت ایمیل استفاده می‌کنند و زندگی خود را با استفاده از خدماتی مانند Evernote و Mint.com ردیابی می‌کنند. محاسبات ابری مسلماً یکی از مهمترین تغییر تکنولوژی در زمان‌های اخیر است [16]. ایده صرف اینکه بتوانیم از محاسبات به روشی مشابه با استفاده از یک ابزار استفاده کنیم، در دنیای سرویس‌های فناوری اطلاعات مجدداً تبلیغ می‌شود و از پتانسیل بسیار خوبی برخوردار است. مشتریان، اعم از بنگاه‌های بزرگ یا مشاغل کوچک، به سمت وعده‌های ابر از چابکی، کاهش هزینه‌های سرمایه و منابع فناوری اطلاعات پیشرفته ترسیم می‌شوند. شرکت‌های فناوری اطلاعات از محاصره

زیرساخت‌های فناوری اطلاعات خود به سمت استفاده از خدمات محاسباتی ارائه شده توسط ابر برای نیازهای فناوری اطلاعات خود در حال تغییر هستند [66].

ویژگی‌های منحصر به فردی را ارائه می‌دهد که با رویکردهای سنتی متفاوت است. پنج ویژگی اصلی کلیدواژه محاسبات ابری شامل سرویس سلف سرویس در صورت تقاضا، دسترسی به همه جا شبکه، جمع آوری منابع مستقل از محل، کشش سریع و خدمات اندازه گیری شده است که همه آنها به سمت استفاده از ابرها یکپارچه و شفاف در نظر گرفته شده‌اند [67]. و منابع رأی گیری CE به توانایی که در آن هیچ منابع به یک کاربر اختصاص داده شده اما به جای با هم مخلوط برای خدمت به مصرف کنندگان متعدد اشاره دارد. منابع، چه در سطح برنامه، میزبان و چه در شبکه، در صورت نیاز به این مصرف کنندگان اختصاص داده و مجدداً واگذار می‌شوند. خدمات سلف سرویس در صورت تقاضا به جایی اطلاق می‌شود که کاربران می‌توانند منابع اضافی مانند قدرت ذخیره سازی یا پردازش را بطور خودکار و بدون دخالت انسان اختصاص دهند. این قابل مقایسه با محاسبات خودمختار است که در آن سیستم رایانه‌ای قادر به مدیریت جن‌ها است. همراه با تأمین منابع خود، محاسبات ابری با قابلیت یافتن و آزاد کردن منابع به همان میزان که لازم باشد مشخص می‌شود، این اصطلاح اغلب به عنوان "خاصیت ارتجاعی" خوانده می‌شود. این امر به مصرف کنندگان این امکان را می‌دهد تا منابع مورد نیاز خود را در هر زمان مقابله کنند تا بارهای سنگین و سنبله‌های مصرفی را برطرف کنند، و با بازگشت منابع به استخر، پس از اتمام، آن‌ها را کاهش دهند. خدمات اندازه گیری شده، که اغلب به عنوان پرداخت به شما پرداخت می‌شود، امکان ایجاد ابر را به عنوان ابزاری فراهم می‌کند که در آن کاربران مبلغ مصرفی را پرداخت می‌کنند، به همان روشی که برای پرداخت هزینه‌های برق مانند برق، گاز و آب انجام می‌شود. [68].

4.5سایر مناطق مورد توجه نگرانی

امنیت سایبری در سیستم‌های تعبیه شده و سنسورها مباحثی هستند که به دلیل افزایش استفاده آنها در هر جنبه‌ای از زندگی ما، در سال‌های اخیر مورد توجه روزافزون صنعت و دانشگاه‌ها قرار گرفته‌اند. به عنوان مثال، وسایل کوچک جاسازی شده در اتومبیل، لوازم خانگی، تلفن همراه و تجهیزات صوتی / تصویری درج شده به طور فزاینده بخشی از زندگی ما می‌شوند. به طور مشابه، سنسورها شاهد تحقیقات گسترده‌تر و استقرار تجاری در برنامه‌های نظامی، علمی و تجاری از جمله نظارت بر زیستگاه‌های بیولوژیکی، کشاورزی و فرآیندهای صنعتی هستند. نگرانی‌های امنیتی در این مناطق از مشکلات امنیتی سنتی در رایانه‌های شخصی و رایانه‌ای ناشی از ماهیت متفاوت و محیط عملیاتی آنها نیست 72]،[73. سیستم‌ها و سنسورهای جاسازی شده معمولاً بسیار مقرون به صرفه هستند و از آنها نیاز به استفاده از پردازنده‌های کوچکتر دارند که فضای محدودی برای امنیت بالایی دارند، به عنوان مثال برای ذخیره یک کلید رمزنگاری بزرگ. بنابراین، اکثر راه حلهای امنیتی سازمانی در جهان سیستم تعبیه شده کار نمی‌کنند. سیستم‌ها و حسگرهای جاسازی شده به دلیل ماهیت اندازه کوچک، از نظر منابع، حافظه، سرعت محاسباتی و پهنای باند ارتباطی محدود هستند. آن‌ها مرز اعتماد جسمی بسیار ضعیفی دارند. به عنوان مثال، آن‌ها در ساکنین و دارایی‌های تجاری، در مزارع خارج نصب شده‌اند، یا توسط انسان در دستان خود قرار می‌گیرند و یا دستمال‌هایی از آنها گرفته می‌شود که حملات جسمی متفاوتی را ممکن می‌سازد. آن‌ها اغلب از اتصال صمیمی بین سخت افزار و

نرم افزار بدون محافظ سیستم عامل استفاده می‌کنند. ماهیت متفاوت سیستم‌های تعبیه شده و حسگرها مجموعه‌های مختلفی از آسیب پذیری های امنیتی ایجاد کرده‌اند [74]،[75]. به عنوان مثال، قدرت باتری محدود در سیستم‌های تعبیه شده، آن‌ها را در برابر حمله‌هایی که این منبع را تخلیه می‌کند، آسیب پذیر می‌کند [73]. نزدیکی سیستم‌های تعبیه شده به یک مهاجم بالقوه آسیب پذیری برای حمله‌هایی ایجاد می‌کند که دسترسی فیزیکی به سیستم ضروری باشد. این به مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) اجازه می‌دهد حملات مربوط به استفاده از سیستم بدنی را انجام دهند، به عنوان مثال، حملات تجزیه و تحلیل قدرت یا حملات خفه کننده به اتوبوس سیستم. سیستم‌های جاسازی شده NEاد به درون یک شرایط محیطی مناسب به کار گیرند. با توجه به محیط عملیاتی بسیار در معرض سیستم‌های تعبیه شده، آسیب پذیری بالقوه‌ای برای حمله‌هایی که سیستم را بیش از حد گرم می‌کند (یا باعث آسیب‌های محیطی دیگری می‌شود) وجود دارد. مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) یک سیستم جاسازی شده به سرقت رفته برای استفاده بیشتر از آنها برای سوء استفاده مجدد اقدام می‌کنند. اقدامات متداول امنیتی متداول برای جلوگیری از دسترسی غیرمجاز از طریق تأیید هویت کاربر، تکنیک‌های حفظ تمامیت داده‌ها از طریق رمزنگاری‌ها و مکانیسم‌های دفاعی شبکه، منطقه فعال و مورد علاقه در این زمینه است. با این حال، جلوگیری از حملات انجام شده با بررسی یا تغییر سیستم بدنی کاملاً بی نظیر است، برای مثال تکنیک‌هایی از قبیل ماسک زدن، روش‌های پنجره و قرار دادن دستورالعمل ساختگی در کد/ الگوریتم ارائه شده است [72].

جنگ سایبری به هک شدن با انگیزه سیاسی برای انجام خرابکاری و جاسوسی اشاره دارد. در کتاب سایبر [92]، جنگ سایبری به عنوان "اقدامات یک کشور–ملت برای نفوذ به رایانه‌ها یا شبکه‌های کشور دیگر به منظور ایجاد آسیب یا اختلال" تعریف شده است. بیشتر نگرانی‌های مربوط به جنگ سایبری بر نقض امنیت ملی و خرابکاری زیرساخت‌های مهم کشور متمرکز شده است [76]. مورد اول مربوط به جاسوسی کامل ملی است که در آن اطلاعات غیرمجاز طبقه بندی شده که ممکن است امنیت ملی را نقض کند، توسط افراد غیرمجاز به طور غیرقانونی دسترسی یا تغییر پیدا کند. مورد دوم مربوط به هرگونه اختلال احتمالی در زیرساخت‌های مهم کشور مانند ساقه شبکه برق و سیستم حمل و نقل است. در سال ۲۰۰۸، یک تمرین شبیه سازی شده با نام "طوفان سایبری" توسط وزارت امنیت میهن انجام شد. هدف از این تمرین آزمایش دفاع کشور در برابر جاسوسی دیجیتال بود. تمرین سایبر طوفان شکاف‌ها و کاستی‌های دفاع سایبری کشور را روشن کرد. از آن زمان، محققان تعدادی از اولویت‌های جدید را در رابطه با استراتژی دفاع سایبری کشور[77] ، [78]پیشنهاد داده‌اند. شناسایی سیستم‌های حیاتی کشور مطرح شده است [80]به تشخیص سیستم‌های اینترنت را فعال کنید که به دفاع سایبری کشور و هر وابستگی متقابل سیستم‌های حیاتی هستند. تعدادی راهکار برای محافظت از زیرساخت‌های مهم کشور با شناسایی و اصلاح آسیب پذیری، و کاهش تهدیدات و پاسخ به آنها پیشنهاد شده است [79]،[77].

۴. پیشنهادات اجرایی طرح

با رشد شگرف در دسترس بودن به اینترنت و پیشرفت دستگاههای فعال شده در اینترنت، تعداد فزاینده‌ای از جمعیت از اینترنت در همه بیداری‌های زندگی خود استفاده می‌کنند و غالباً بدون درک عواقب سوء استفاده از داده، اطلاعات

شخصی بسیار حساس را در معرض نمایش قرار می‌دهند. ما حدس می‌زنیم که موضوعات مربوط به حریم شخصی کاربر نهایی مطابق با حجم فزاینده اطلاعات شخصی از طریق اینترنت، به طور مداوم در آینده رشد خواهد کرد. علاوه بر این، مسائل قابلیت استفاده به عنوان راهی برای تأمین مکانیسم امنیتی متمرکز کاربر نهایی که در آن کاربران می‌توانند بطور شهودی و بدون پیچیدگی یا منحنی یادگیری عمیق، از آنها محافظت کنند و از داده‌های خود استفاده کنند، توجه بیشتری به دست می‌آورند.

به طور سنتی، فعالیت در جامعه امنیت سایبری مبتنی بر تکه‌های افزایشی است که مشکلات فعلی امنیت و حریم خصوصی را اصلاح می‌کند و سپس به مرحله بعد حرکت می‌کند. برخی بر این باورند که این رویکرد افزایشی به خوبی کار نکرده است و نمی‌تواند نیازهای آینده را تأمین کند، زیرا اینترنت اولیه برای محیطی بسیار متفاوت از آنچه امروزه مورد استفاده قرار گرفته اختراع شده است. رویکردی برای اندیشیدن به "خارج از جعبه" بدون تکیه بر سیستم محاسبات فعلی و اینترنت، اما با شروع چیزهای جدید، استفاده از تقاضاهای رو به رشد اینترنت سریع‌تر پیشنهاد شده است [126].

ماهیت ناشناس اینترنت به عنوان منبعی برای افزایش حمله سایبری تعریف شده است و ردیابی مجرم دشوار است. مدیریت هویت در مقیاس جهانی و تکنیک‌های ردیابی Ack به عنوان یک برنامه استراتژیک برای خنثی کردن تعداد مهاجمان در مبانی اطلاعاتی نیروهای کشوری (به طور مثال سحافا) سایبری در آینده، به ویژه هنگامی که زیرساخت‌های مهم درگیر باشد، به یک منطقه فعال تحقیقاتی تبدیل شده است. ما در بخش‌های بعدی به تفصیل بیشتر در مورد این جهت‌های تحقیقاتی آینده تحقیق خواهیم کرد.

۱. روی حریم شخصی تمرکز کنید

در سالهای اخیر، حریم خصوصی با گسترش گسترده سیستم‌های شبکه و اینترنت به یک موضوع مهم تبدیل شده است. در حال حاضر، اینترنت در همه بیداری‌های زندگی ما مورد استفاده قرار می‌گیرد که خواستار افزایش حجم اطلاعات شخصی است تا در فضای مجازی قرار گیرد. براساس گزارش سالانه JP Morgan [122] ، فروش جهانی تجارت الکترونیک با نرخ سالانه ۱۹٫۴٪ و به سال ۲۰۱۳ به ۹۶۳ میلیارد دلار فروش رسیده است. این افزایش در خرید آنلاین نشان می‌دهد که کاربران اینترنت با به اشتراک گذاری اطلاعات مالی حساس خود راحت‌تر می‌شوند. مانند شماره کارتهای اعتباری و آدرسهای حمل و نقل. به همین ترتیب، سایت‌های حرفه‌ای و شبکه‌های اجتماعی که افراد را با علایق مشابه به صورت آنلاین پیوند می‌دهند، در دهه گذشته شاهد رشد نمایی بوده‌اند. LinkedIn، یک سایت حرفه‌ای شبکه سازی که در ماه مه سال ۲۰۰۳ تأسیس شد، تا ژانویه ۲۰۱۳ ۲۰۰ میلیون کاربر دارد. فیس بوک، که در فوریه ۲۰۰۴ راه اندازی شد، تا سپتامبر ۲۰۱۲ به یک میلیارد کاربر فعال رسیده است. این تعداد نشان می‌دهد که مردم به طور فزاینده‌ای احساس راحتی می‌کنند تا اطلاعات شخصی را در مورد خودشان قرار دهند. برخط. افراد همچنین مایل هستند در هنگام انجام فعالیت‌های آنلاین، در مورد آنچه تصور می‌کنند حمله به حریم خصوصی می‌دانند، صحبت کنند.

با افزایش حجم اطلاعات در اینترنت، احتمال وقوع سازش حریم خصوصی نیز افزایش می‌یابد. به عنوان مثال، ویزیت‌های آنلاین فرد برای نفوذ در اطلاعات و ارسال تبلیغات بر اساس سابقه مرور شخص مشاهده می‌شود. روش‌های سازش می‌تواند از طریق جمع آوری آمار در مورد کاربران، تا اقدامات مخرب‌تر از قبیل گسترش جاسوسی را شامل شود. مجرمان سایبری از سایتهای شبکه‌های اجتماعی برای سرقت اطلاعات شخصی برای استفاده در کلاهبرداری و سرقت هویت استفاده می‌کنند [16]،[17]. برای جلوگیری از بروز چنین نشتی‌های حریم خصوصی، چندین سایت شبکه‌های ارتباطی بین المللی اقدامات حریم خصوصی را ارائه می‌دهند. به عنوان مثال، فیس بوک تنظیمات حریم خصوصی را برای همه کاربران ثبت نام شده فراهم می‌کند. تنظیمات موجود در فیس بوک شامل امکان مسدود شدن برخی افراد از دیدن پروفایل شخصی، امکان انتخاب "دوستان" شخص و امکان محدود کردن دسترسی به تصاویر و فیلم‌های شخصی است. تنظیمات حریم خصوصی در سایر سایت‌های شبکه‌های اجتماعی مانند Google Plus و Twitter نیز موجود است. کودکان و نوجوانان بسیار مستعد سوءاستفاده از Inte rnet و درنهایت خطر حفظ حریم خصوصی آنها هستند. نگرانی فزاینده‌ای بین والدینی وجود دارد که فرزندانشان اکنون به طور روزانه از فیس بوک و سایر سایت‌های رسانه‌های اجتماعی استفاده می‌کنند. شیوه‌های گردآوری اطلاعات وب سایت یکی دیگر از نگرانی‌های رو به رشد است زیرا افراد جوان آسیب پذیرتر و از این واقعیت آگاه نیستند که تمام اطلاعات و مرور آنها هنگام بازدید از یک سایت خاص می‌تواند و ممکن است ردیابی شود.

هدف امنیت آگاهی از حریم خصوصی این است که کاربران و سازمانها را قادر به بیان بهتر، محافظت و کنترل محرمانه بودن اطلاعات خصوصی خود، حتی در صورت به اشتراک گذاشتن (یا نیاز به) به اشتراک گذاشتن آن با دیگران بدانیم [65]. یک جریان از تحقیقات در این زمینه با نحوه دسترسی و افشای داده‌ها ضمن محافظت از حریم خصوصی سروکار دارد [65]. تعدادی تحقیق برای بررسی چگونگی افشای انتخابی داده‌ها، چگونگی محافظت از داده‌هایی که توسط افراد به اشتراک گذاشته می‌شود و همچنین روش‌های سالم سازی داده‌ها انجام می‌شود [141]. جریان دیگری از تحقیقات انجام شده در این زمینه مربوط به تدوین چارچوب مشخصات برای ایجاد و تقویت سیاست حفظ حریم خصوصی است [88]. توسعه ساختمان تعدادی از مشخصات برای ارائه ضمانت حریم خصوصی از قبیل زبانها برای تعیین سیاست‌های حفظ حریم خصوصی، مشخصات نقض حریم خصوصی، و تشخیص نقض حریم خصوصی، یک منطقه تحقیقاتی فعال است. ساختن تکنیک‌های خط مشی داده برای جمع آوری داده‌ها، به اشتراک گذاری داده‌ها و انتقال و مقابله با تخلفات حریم خصوصی از دیگر مناطق فعال تحقیق در این دسته است.

۲. امنیت بعدی نسل بعدی اینترنت

شکی نیست که اینترنت پدیده‌ای اجتماعی بوده است که تغییر کرده است، و همچنان به تغییر چگونگی برقراری ارتباط، مشاغل، نحوه کار با شرایط اضطراری و ارتش در میان بسیاری موارد دیگر ادامه می‌دهد. علیرغم اهمیت حیاتی شبکه اینترنت، برخی از بخش‌های اینترنت شکننده هستند و حملات مداوم در حال انجام است که از بهره برداری از نرم افزار گرفته تا تکذیب سرویس می‌باشد. یکی از دلایل اصلی این آسیب پذیری های امنیتی این است که معمار اینترنت و پروتکلهای پشتیبان آن در درجه اول برای یک محیط خوش خیم و قابل اعتماد طراحی شده‌اند،

اما در مورد مسائل امنیتی کم و بیش مورد توجه قرار نگرفته است 125]،[126. این فرض به وضوح دیگر برای اینترنت امروز معتبر نیست، که میلیون‌ها نفر از مردم ، رایانه‌ها و شرکت‌ها را در یک وب پیچیده و متشکل از سراسر جهان به هم متصل می‌کند.

۳. به سمت سیستمهای قابل اعتماد

اصطلاح سیستم‌های قابل اعتماد توسط وزارت امنیت داخلی (DHS) در ایالات متحده تعریف شده است [15]به عنوان هدف طولانی مدت برای نشان دادن یک سیستم محاسباتی که ذاتاً ایمن، در دسترس و قابل اعتماد است، با وجود اختلال در محیط زیست، خطاهای کاربر کاربر و اپراتور و حملات احزاب خصمانه در راستای این هدف، نویسنده [45] از الزامات سخت افزاری و نرم افزارهای ترکیبی نرم افزاری ایمن به عنوان بلوک ساختمان اساسی به سمت سیستم قابل اعتماد حمایت می‌کند. در این پیشنهاد، سیستم‌ها و دستگاه‌ها اطلاعات قابل اعتماد و استانداردی را تأیید می‌کنند که اعتماد به نفس آنها، راه حل‌های سخت افزاری کالا با اطمینان از امنیت عمومی در همه سطوح و سیستم‌هایی که قادر به تعیین اعتماد به یک دستگاه، بسته نرم افزاری یا شبکه بر اساس اطلاعات اعتماد به دست آمده پویا هستند، به اشتراک می‌گذارند. ریشه در سیاست‌های امنیتی و سخت افزاری تعریف شده توسط کاربر. در راستای این هدف، چندین موضوع کار تحقیقاتی در زمینه تکنیک انزوا قابل اعتماد[143]جداسازی و مجازی سازی در سخت افزار و نرم افزار انجام شده است [134]، [143]، تجزیه و تحلیل‌هایی که می‌توانند ارزیابی اعتبار را قبل از به کار انداختن بسیار ساده‌تر کنند [144]، معماری قدرتمندی که خودآزمایی و تشخیص خود را ارائه می‌دهد [145]،[147]

٤. تکنیک‌های مدیریت هویت و ردیابی در مقیاس جهانی

مدیریت هویت وظیفه کنترل اطلاعات در مورد کاربران در رایانه‌ها است. چنین اطلاعاتی شامل اطلاعاتی است که هویت کاربر را تأیید می‌کند، اطلاعاتی که اطلاعات و عملکردهایی را که اجازه دسترسی و یا انجام آنها را دارند، توصیف می‌کند. همچنین شامل مدیریت اطلاعات de scriptiveدر مورد کاربر و چگونگی دستیابی و اصلاح آنها به اطلاعات می‌باشد. اشخاص مدیریت شده معمولاً شامل کاربران، منابع سخت افزاری و شبکه و حتی برنامه‌های کاربردی می‌شوند [15].

رویکردهای فعلی بسیاری در مورد مدیریت هویت وجود دارد. به عنوان مثال، بسیاری از وب سایت‌ها از سیستم ورود به سیستم با نام کاربری و رمز عبور استفاده می‌کنند تا فقط کاربران واجد شرایط ورود به سرویس را نمایش دهند. با این حال، بسیاری از این موارد هنوز کاملاً با سایر سرویس‌ها در سازمانهای مختلف قابل تعامل نیستند و مقیاس پذیر هستند. آن‌ها فقط برای موارد یکبار مصرف یا محدود به روش‌های دیگر هستند. اشاره شده است که [15] به دلیل عدم مدیریت کافی هویت، اغلب ردیابی سرقت هویت بسیار دشوار است.

۵. رمزگذاری در قابل استفاده در همه جا

با گسترش دامنه تهدیدهای احتمالی از طریق اینترنت، کاربران نهایی به طور فزاینده‌ای خود را در موقعیتی پیدا می‌کنند که بخواهند تصمیمات امنیتی را اتخاذ کنند، به عنوان مثال از طریق پیکربندی تنظیمات مربوط به امنیت، پاسخ دادن به پیام‌های مربوط به رویدادهای مربوط به امنیت ، یا مجبور به تعیین امنیت سیاست و حقوق دسترسی [128]. متأسفانه، تجربه نشان می‌دهد که اگرچه ویژگی‌های امنیتی غالباً ارائه می‌شوند، اما به شکلی منتقل می‌شوند که قابل فهم یا قابل استفاده برای بسیاری از اعضای مخاطب نیست. از آنجا که بیشتر کاربران قادر به درک ویژگیهای امنیتی ارائه شده نیستند، بسیاری از پیشرفتهای امنیتی بدون استفاده باقی می‌مانند و کاربران نهایی را در موقعیت آسیب پذیر از حملات مخرب قرار می‌دهند. نیاز به امنیت قابل استفاده و مشکلات ذاتی در تحقق راه حل‌های کافی در حال افزایش است. [99,100].

بسیاری از فناوری‌های امنیتی سعی در بهبود جنبه‌های قابلیت استفاده دارند. بیشتر آنها از نظر قابلیت استفاده کوتاه است. اعتقاد بر این است که نقشه‌های رمزعبور یکی از بخش‌های مهم امنیت قابل استفاده است. بنابراین، چندین روش پیچیده مانند فرکانس تغییر، درج کاراکترهای غیر الفبایی یا رمزهای عبور مبتنی بر دیداری و بیومتریک پیشرفت کرده است که کاربران مجبور نیستند آنها را به خاطر بسپارند. علیرغم این تلاش‌ها، مشکلات امنیتی در طرح‌های رمز عبور ضعیف اجرا شده در طول سالها گسترده است. کاربران متوسل می‌شوند که آنها را روی برگه‌های کاغذ بنویسند یا آنها را بدون رمزگذاری در دستگاه‌های دستی ذخیره کنند [15].

۵. پیشنهاداتی جهت رفع مسایل و مشکلات سازمانی در سطح کلان و راهبردی

ما همچنین مسیرهای تحقیق بالقوه آینده را نشان داده‌ایم. هرچه افراد بیشتر و بیشتر به اینترنت وصل می‌شوند، درک همه سطوح کاربران اعم از کارشناسان و افراد غیر متخصص در سیستم محاسبات و ایجاد ابزارهای امنیتی متناسب با سطح اطمینان آنها پیشنهاد شده است. به عنوان یک تحقیق مهم در آینده، بررسی حفظ حریم خصوصی کاربران توسط بسیاری از کارشناسان امنیتی مورد تأکید قرار گرفته است، زیرا میزان اطلاعات شخصی از طریق اینترنت در سالهای اخیر به سرعت گسترش یافته است. به جای تلاش برای حل مشکل خاص در اینترنت و سیستم‌های محاسباتی، به تدریج، رویکردهای خلاقانه‌تر برای دیدن "تصویر بزرگتر" یا فکر کردن "خارج از جعبه" پیشنهاد شده است، زیرا برخی شواهد نشان می‌دهد که ظرفیت فن آوری مدرن امروز اشباع می‌شود و با استفاده از رویکردهای افزایشی سنتی، دیگر مقیاس خوبی ندارد. تحولات اینترنت بعدی و سیستم‌های قابل اعتماد نسل بعدی به عنوان مهمترین تحقیق برای بررسی آینده پیشنهاد شده است. توسعه روشهای مدیریت هویت در مقیاس جهانی و تکنیک‌های ردیابی برای فعال کردن ردیابی دشمنان نیز به عنوان یک مسئله مهم مورد توجه در آینده مورد توجه قرار گرفته است.

نتیجه گیری

این بررسی بر دو جنبه سیستم اطلاعاتی متمرکز شده است: درک آسیب پذیری در خروج فناوری‌ها و تهدیدهای ظهور در آینده و پیشرفت در فن آوری های ارتباط از راه دور و اطلاعات. تهدیدهای رو به رشد در فن آوری های نوظهور، مانند رسانه‌های اجتماعی، رایانش ابری، فناوری تلفن‌های هوشمند و زیرساخت‌های مهم یافت شده است،

که اغلب از ویژگی‌های منحصر به فرد آنها بهره می‌گیرند. ما ویژگی‌های هر یک از فن آوری های نوظهور و شیوه‌های مختلف انتشار بدافزار در این فناوری‌های جدید را شرح دادیم. سپس، ما در مورد مجموعه متداول الگوهای حمله عمومی که در فناوری نوظهور یافت می‌شود، بحث می‌کنیم. به عنوان مثال، از آنجا که بسیاری از این فن آوری های نوظهور از طریق آنلاین خدمات ارائه می‌دهند، برخی از حملات مربوط به حملات به طور فزاینده‌ای از امنیت مرورگر از طریق بدافزار پنهان شده در پسوند یا آسیب پذیری پنهان شده در اسکریپت زبانها برای دسترسی به داده‌های محرمانه استفاده می‌کنند. مخالفان همچنین برای جلوگیری از تشخیص، زمینه نبرد خود را از روی دسکتاپ به سیستم عامل‌های دیگر در تلفیق تلفن‌های همراه، رایانه‌های لوحی و VoIP تغییر می‌دهند. به خصوص بدافزارهای موبایل با افزایش تعداد کاربران موبایل و پیشرفت نرم افزارهای موبایل در چند سال اخیر به شدت افزایش یافته است. کلاهبرداری با استفاده از مهندسی اجتماعی در حال افزایش است. سایت‌های محبوب شبکه‌های اجتماعی مانند فیس بوک، توییتر و دیگران به طور فزاینده‌ای به عنوان مکانیسم‌های تحویل مورد استفاده قرار می‌گیرند تا کاربران مظنون به نصب یا گسترش بدافزارها شوند. حملات سازمان یافته بیشتری از طریق استفاده از باتنت گزارش شده است. از آنجا که تأثیر چنین صدماتی بسیار بیشتر از حملات فردی است، نگرانی فزاینده‌ای برای خنثی کردن بات نت وجود دارد. همچنین آمارهای اخیر نشان می‌دهد که تعداد حملات سایبری متناسب با یک سیستم خاص، به عنوان مثال سیستم فرمان و کنترل، با استفاده از دانش و پرسنل داخلی ، در حال افزایش است.

منابع

1. **http://www.maawg.org/, last accessed: June 2013.**
2. **http://www.antiphishing.org/, last accessed: June 2013.**
3. **http://www.ostermanresearch.com/downloads.htm, last accessed: June 2013.**
4. **http://en.wikipedia.org/wiki/Mebroot, last accessed: June 2013.**
5. **http://www.emailtrackerpro.com, last accessed: June 2013.**
6. **http://www.tamos.com, last accessed: June 2013.**
7. **https://www.mandiant.com/resources/download/web-historian, last accessed: June 2013.**
8. **http://www.majorgeeks.com/index.dat_analyzer_d5259.html, last accessed: June 2013. [9] http://www.winpcap.org/, last accessed: June 2013.**
9. **http://www.riverbed.com/products-solutions/products/performance-management/wireshark-enhancement-products/Wireless-Traffic-PacketCapture.html, last accessed: June 2013.**
10. **http://shibboleth.internet2.edu/, last accessed: June 2013.**
11. **Australian Parliament the report of the inquiry into Cyber Crime, http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf. [13] www.it2trust.com/pdf/Aladdin.SafeWord_PO_SafeWord.pdf, last accessed: June 2013.**
12. **A. Cardenas, T. Roosta, G. Taban, S. Sastry, Cyber security basic defenses and attack trends, Fujitsu Lab., http://www.flacp.fujitsulabs.com/~cardenas/Papers/Chap4v2.pdf, last accessed: June 2013.**
13. **DHS S&T, Roadmap for cybersecurity research, Jan. 2009, http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf, last accessed: June 2013.**

14. Annual Emerging Cyber Threats Report, Georgia Tech Information Security Center, http://www.gtisc.gatech.edu/, last accessed: June 2013.
15. Internet Security Threats Report. سیمانتیک, http://www.سیمانتیک.com/threatreport/, last accessed: June 2013.
16. S.E. Goodman, H.S. Lin (Eds.), Toward a Safer and More Secure Cyberspace, The Nat'l Academics Press, 2007.
17. R.C. Newman, Computer Security: Protecting Digital Resources, first edition, Jones & Bartlett Publishers, February 20, 2009.
18. B.W. Lampon, Privacy and security – Usable security: how to get it, Commun. ACM 52 (11) (2009) 25–27.
19. A. Haeberlen, P. Kouznetsov, P. Druschel, Practical accountability for distributed systems, in: SOSP 2007, pp. 175–188.
20. M. Tehranipoor, C. Wang, Introduction to Hardware Security and Trust, Springer, 2011.
21. N. Potlapally, Hardware security in practice: Challenges and opportunities, in: HOST 2011, pp. 93–98.
22. Q. Li, H. Gao, B. Xu, Z. Jiao, Hardware threat: The challenge of information security, in: ISCSCT 2008, pp. 517–520.
23. R.S. Chakraborty, S. Narasimhan, S. Bhunia, Hardware Trojan: Threats and emerging solutions, in: HLDVT 2009, pp. 166–171.
24. R. Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, Trustworthy hardware: Identifying and classifying hardware trojans, IEEE Comput. 43 (10) (2010) 39–46.
25. H. Mouratidis, Secure by design: Developing secure software systems from the group up, Intern. J. Secure Software Eng. 2 (3) (2011) 23–41.
26. A. Sadeghi, Trusted computing — special aspects and challenges, in: V. Geffert, et al. (Eds.), SOFSEM, in: Lect. Notes Comput. Sci., vol. 4910, Springer, Berlin, 2008, pp. 98–117.
27. Trusted Computing Group, TPM Main, Part 1, Design Principles, Specification version 1.2. Revision 94, 2006. [30] Trusted Computing Group, TPM Main, Part 2, TPM Structures, Specification version 1.2. Revision 94, 2006.
28. Trusted Computing Group, TPM Main, Part 3, Design Principles, Specification version 1.2. Revision 94, 2006.
29. B. Beckert, R. Hähnle, P.H. Schmitt (Eds.), Verification of Object-Oriented Software: The KeY Approach, Lect. Notes Comput. Sci., vol. 4334, Springer, Heidelberg, 2007.
30. C. Hoare, J. Misra, G.T. Leavens, N. Shankar, The verified software initiative: A manifesto, ACM Comput. Surv. 41 (2009) 1–22.
31. K.R.M. Lein, An automatic program verifier for functional correctness, in: E.M. Clarke, A. Voronkov (Eds.), LPAR-16 2010, in: Lect. Notes Comput. Sci., vol. 6355, Springer, Heidelberg, 2010, pp. 348–370.
32. M. Sitaraman, B. Adcock, J. Avigad, Building a push-button RESOLVE verifier: Progress and challenges, in: Formal Aspects of Computing, 2010, pp. 1–20. [36] J. MaManus, The CERT Sun Microsystems Secure Coding Standard for Java, CERT, 2009.
33. R. Seacord, Top 10 Secure Coding Practice, CERT, 2010.

34. R. Gennaro, J. Katz, H. Krawczyk, T. Rabin, Secure network coding over the integers, in: P.Q. Nguyen, D. Pointcheval (Eds.), PKC 2010, in: Lect. Notes Comput. Sci., vol. 6056, Springer, Heidelberg, 2010, pp. 142–160.
35. M. Howard, D. LeBlanc, J. Viega, 19 Deadly Sins of Software Security, McGraw–Hill, 2005.
36. K. Tsipenyuk, B. Chess, G. McGraw, Seven pernicious kingdoms: A taxonomy of software security errors, IEEE Secur. Priv. 3 (6) (2005) 81–84.
37. C.B. Haley, R. Laney, J.D. Moffett, B. Nuseibeh, Security requirements engineering: A framework for representation and analysis, IEEE Trans. Softw. Eng. 34 (1) (2008) 133–153.
38. G. McGraw, Software Security: Building Security In, Addison–Wesley, 2006.
39. M.I. Sharif, A. Lanzi, J.T. Giffin, W. Lee, Impeding malware analysis using conditional code obfuscation, in: Network and Distributed System Security Symposium (NDSS), 2008.
40. J.-M. Borello, L. Mé, Code obfuscation techniques for metamorphic viruses, J. Comput. Virol. 4 (3) (2008) 211–220.
41. F.T. Sheldon, V. Vishik, Moving toward trustworthy systems: R&D essentials, IEEE Comput. Mag. (2010) 31–40.
42. W. Stallings, Cryptography and Network Security Principles and Practices, third edition, Pearson Educations, 2010.
43. E. Cole, R. Krutz, J. Conley, Network Security Bible, second edition, Wiley Publishing, 2011.
44. T. Rubya, N. Prema Latha, B. Sangeetha, A survey on recent security trends using quantum cryptography, IJCSE 2 (9) (2010) 3038–3042.
45. E.S. Pilli, R.C. Joshi, R. Niyogi, Network forensic frameworks: Survey and research challenges, Dig. Investigation (Int'l. J. Dig. Investigation) (2010), in press.
46. A. Almulhem, I. Traore, Experience with engineering a network forensics system, in: C. Kim (Ed.), ICOIN 2005, in: Lect. Notes Comput. Sci., vol. 3391, Springer, Heidelberg, 2005, pp. 62–71.
47. B.J. Nikkel, A portable network forensic evidence collector, Dig. Investigation (Int'l. J. Dig. Investigation) 3 (3) (2006) 127–135.
48. A. Mairh, D. Barik, K. Verma, D. Jena, Honeypot in network security: a survey, in: ICCCS, 2011, pp. 600–605.
49. F. Fischer, F. Mansmann, D.A. Keim, S. Pietzko, M. Waldvogel, Large-scale network monitoring for visual analysis of attacks, in: J.R. Goodall, G.J. Conti, K.-L. Ma (Eds.), VizSEC, in: Lect. Notes Comput. Sci., vol. 5210, Springer, 2008, pp. 111–118.
50. M. Vrable, J. Ma, J. Chen, D. Moore, E. Vandekieft, A. Snoeren, G. Voelker, S. Savage, Scalability, fidelity and containment in the Potemkin virtual honeyfarm, in: Proceedings of the 2005 Symposium on Operating Systems Principles, October 2005.
51. H.K. Lu, A. Ali, Communication security between a computer and hardware token, in: ICONS 2008, pp. 220–225.
52. F. Aloul, S. Zahidi, W. El-Hajj, Two factor authentication using mobile phones, in: IEEE International Conference on Computer Systems and Applications (AICCSA), Rabat, Morocco, May 2009.

53. D. Ilett, US bank gives two-factor authentication to millions of customers, available at http://www.silicon.com/financialservices/0,3800010322,39153981,
54. 00.htm, 2005.
55. D. de Borde, Two-factor authentication, Siemens Enterprise Communications UK-Security Solutions, available at http://www.insight.co.uk/files/ whitepapers/Twofactor authentication (White paper).pdf, 2008.
56. J. Bringer, H. Chabanne, An authentication protocol with encrypted biometric data, in: AFRICACRYPT, in: Lect. Notes Comput. Sci., 2008, pp. 109–124.
57. M.K. Khan, J.S. Zhang, X.M. Wang, Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices, Chaos Solutions & Fractals 35 (2008) 519–524.
58. G. Coker, J. Guttman, P. Loscocco, J. Sheehy, B. Sniffen, Attestation: Evidence and trust, in: ICICS '08, 2008, pp. 1–18.
59. J. Jang, H. Hwang, S. Nepal, Biometric enabled portable trusted computing platform, in: TurstCom 2011, pp. 436–442.
60. The CERT guide to insider threats: How to prevent, detect, and respond to theft of critical information, sabotage, and fraud, www.cert.org/ archive/pdf/insidercross051105.pdf.
61. J. Hunker, C.W. Probst, Insiders and insider threats—An overview of definitions and mitigation techniques, J. Wireless Mobile Netw. Ubiquitous Comput. Dependable Appl. 2 (1) (2011) 4–27.
62. P. Guarda, N. Zannone, Towards the Development of Privacy-Aware Systems, Information and Software Technology, 2008.
63. K. Dahbur, B. Mohammad, A.B. Tarakji, A survey of risks, threats and vulnerabilities in cloud computing, 2011, pp. 12–18.
64. H. Takabi, J. Joshi, G. Ahn, Security and privacy challenges in cloud computing environments, IEEE Secur. Priv. (2010) 24–31.
65. Q. Zhang, L. Cheng, R. Boutaba, Cloud computing: state-of-the-art and research challenges, J. Internet Serv. Appl. 1 (2010) 7–18.
66. M.T. Louw, J.S. Lim, V.N. Venkatakrishnan, Extensible web browser security, in: B.M. Hammerli, R. Sommer (Eds.), DIMVA, in: Lect. Notes Comput. Sci., vol. 4579, Springer, 2007, pp. 1–19.
67. C. Soghoian, A remote vulnerability in Firefox extensions, http://paranoia.dubfire.net/2007/05/remote-vulnerability-in-firefox.html, last accessed: June 2013.
68. C. Reis, A. Barth, C. Pizano, Browser security: lessons from google chrome, Commun. ACM 52 (2009) 45–49.
69. P. Koopman, Embedded system security, IEEE Comput. 37 (7) (2004) 95–97.
70. S. Parameswaran, T. Wolf, Embedded systems security – an overview: DAES 2008, vol. 12, pp. 173–183, http://dx.doi.org/10.1007/s10617-008-9027-x.
71. J.P. Walters, Z. Liang, Wireless sensor network security: A survey, in: Y. Xiao (Ed.), Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press, 2006.
72. Y. Zhou, Y. Fang, Y. Zhang, Securing wireless sensor networks: a survey, IEEE Commun. Surv. Tutor. 10 (3) (2008) 6–28.

73. S.J. Collier, A. Lakoff, The vulnerability of vital systems: How “critical infrastructure” became a security problem, in: Critical Infrastructure, Risk and (In)security, 2008, pp. 17–39.
74. C.W. Ten, Cybersecurity for critical infrastructures: Attack and defense modeling, IEEE Trans. Syst. Man Cybern. 40 (4) (2010) 853–865.
75. Critical infrastructure protection report, Government Accountability Office, Washington, DC, May 2005. [Online]. Available: http://www.gao.gov/new. items/d05434.pdf, last accessed: June 2013.
76. J.M. Weiss, Control systems cybersecurity–maintaining the reliability of the critical infrastructure, in: Testimony of Joseph M. Weiss Control Systems Cybersecurity Expert before the House Government Reform Committee’s Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census U.S. House of Representatives, Mar. 30, 2004.
77. W.L. McGill, B.M. Ayyub, The meaning of vulnerability in the context of critical infrastructure protection, in: Critical Infrastructure Protection: Elements of Risk, School of Laws, George Mason Univ., Arlington, VA, Dec. 2007.
78. S. Abraham, I.S. Chengalur-Smith, An overview of social engineering malware: Trends, tactics, and implications, Technol. Soc. 32 (2010) 183–196.
79. M. Feily, A. Shaherestani, S. Ramadass, A survey of botnet and botnet detection, in: SECURWARE 2009, pp. 268–273.
80. M. Bailey, E. Cooke, F. Jahanian, et al., A survey of botnet technology and defense, in: CATCH 2009, pp. 299–304.
81. Z. Zhu, G. Lu, Y. Chen, et al., Botnet research survey, in: COMPSAC 2008, pp. 967–972.
82. C. LI, W. Jiang, X. Zou, Botnet: survey and case study, in: ICICIC 2009, pp. 1184–1187.
83. S. Nepal, J. Zic, D. Liu, J. Jang, Trusted computing platform in your pocket, in: ECU 2010, pp. 812–817,.
84. R. Sailer, X. Zhang, T. Jaeger, L. van Doorn, Design and implementation of a TCG-based integrity measurement architecture, SSYM 2004,.
85. M. Johnson, S. Egelman, S. Bellovin, Facebook and privacy: it’s complicated, in: Proc. SOUPS 2012, ACM, 2012.
86. C. Dwyer, S. Hiltz, K. Passerini, Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace, in: Americas Conference on Information Systems (AMCIS), Keystone, Colorado, USA, 2007.
87. R. Gross, A. Acquisti, Information revelation and privacy in online social networks (the Facebook case), in: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 2005, pp. 71–80.
88. G. Hogben, Security issues and recommendations for online social networks, in: Position Paper. ENISA, European Network and Information Security Agency, 2007.
89. R.C. Clark, Cyber War, Ecco, 2010.
90. D. Weitzner, et al., Information accountability, Commun. ACM 51 (6) (2008) 82–87.
91. J. Yao, S. Chen, C. Wang, Accountability as a service for the cloud, in: SCC 2010, pp. 81–88.

92. S. Egelman, J. King, R.C. Miller, N. Ragouzis, E. Shehan, Security user studies: methodologies and best practices, in: CHI 2007, http://dx.doi.org/10.1145/1240866.1241089.
93. J. Wang, J.N. Whitley, R.C.W. Phan, Unified parametrizable attack tree, J. Inform. Security Res. (IJISR) 1 (1) (2011) 20–26.
94. A. John, T. Sivakumar, Ddos: Survey of traceback methods, in: IJRTE, 2009.
95. B. Kordy, M. Pouly, P. Shweitzer, Computational aspects of attack-defense trees, in: SIIS 2011, in: Lect. Notes Comput. Sci., vol. 7053, 2012, pp. 103–116.
96. L.F. Cranor, S. Garfinkel (Eds.), Security and Usability: Designing Secure Systems that People Can Use, O'Reilly Media, 2005.
97. L.F. Cranor, S. Garfinkel, Secure or usable?, IEEE Secur. Priv. 2 (2004) 16–18.
98. Anti-phishing group tech reports: http://www.antiphishing.org/phishReportsArchive.html, last accessed: June 2013.
99. C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G.M. Voelker, V. Paxson, S. Savage, Spamalytics: an empirical analysis of spam marketing conversion, in: CCS, 2008, pp. 3–14.
100. H. Shahriar, M. Zulkernine, Mitigating program security vulnerabilities: Approaches and challenges, ACM Comput. Surv. 44 (3) (2012), Article No. 11.
101. S. Liu, B. Cheng, Cyberattacks: "Why, what, who and how", in: IT Pro., IEEE Computer Society, May/June 2009.
102. http://www.pcmag.com/article2/0,2817,2392570,00.asp, last accessed: June 2013.
103. http://www.cert.org/cybersecurity-engineering/, last accessed: June 2013.
104. http://www.welivesecurity.com/2012/12/11/trends-for-2013-astounding-growth-of-mobile-malware/, last accessed: June 2013.
105. http://www.huffingtonpost.com/brian-honigman/100-fascinating-social-me_b_2185281.html, last accessed: June 2013.
106. W. Luo, J. Liu, J. Liu, C. Fan, An analysis of security in social networks, in: Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp. 648–651.
107. K. Thomas, D.M. Nicol, The Koobface botnet and the rise of social malware, in: Proceedings of the 5th International Conference on Malicious and Unwanted Software (Malware 2010), 2010, pp. 63–70.
108. Sophos security threat reports: http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx.
109. M. Lucas, N. Borisov, Flybynight: Mitigating the privacy risks of social networking, in: WPES, 2008.
110. L. Fang, K. LeFevre, Privacy wizards for social networking sites, in: Proc. WWW '10, pp. 351–360.
111. Nicolas Carr, The Big Switch: Our New Digital Destiny, W.W. Norton & Co., 2008.
112. Y. Zhang, J. Joshi, Access control and trust management for emerging multidomain environments, in: S. Upadhyaya, R.O. Rao (Eds.), Annals of Emerging Research in Information Assurance, Security and Privacy Services, Emerald Group Publishing, 2009, pp. 421–452.

113. D. Shin, G.-J. Ahn, Role-based privilege and trust management, Comput. Syst. Sci. Eng. 20 (6) (2005) 401–410.
114. Q. Zhang, L. Cheng, R. Boutaba, Cloud computing: state-of-the-art and research challenges, J. Internet Serv. Appl. 1 (2010) 7–18.
115. Timo Gendrullis, A real-world attack breaking A5/1 within hours, in: Proceedings of CHES '08, Springer, November 2008, pp. 266–282.
116. C.R. Mulliner, Security of smart phones, Master's thesis submitted to University of California, Santa Barbara, June 2006.
117. Sampo Töyssy, Marko Helenius, About malicious software in smartphones, J. Comput. Virology (Springer Paris) 2 (2) (2006) 109–119, http://dx.
118. doi.org/10.1007/s11416-006-0022-0, retrieved 2010-11-30.
119. Ken Dunham, Saeed Abu Nimeh, Michael Becher, Mobile Malware Attack and Defense, Syngress Media, ISBN 978-1-59749-298-0, 2008.
120. http://resources.pbecomm.com/global-ecommerce-blog/understanding-the-global-ecommerce-market-blog/goldman-sachs-forecasts-growth-rate-ofglobal-e-commerce-sales-asia-factors-big/, last accessed: June 2013.
121. S.M. Bellovin, D.D. Clark, A. Perrig, D. Song, A clean-slate design for the next-generation secure internet, National Science Foundation, Tech. Rep., Mar. 2005.
122. A. Feldmann, Internet clean-slate design: What and why?, Comput. Commun. Rev. 37 (3) (2007) 59–64.
123. M. Conti, S. Chong, S. Fdida, W. Jia, H. Karl, Y.-D. Lin, P. Mahonen, M. Maier, R. Molva, S. Uhlig, M. Zukerman, Research challenges towards the Future Internet, Comput. Commun. 34 (18) (2011) 2115–2134.
124. S. Paul, J. Pan, R. Jain, Architectures for the future networks and the next generation Internet: A survey, Comput. Commun. 34 (1) (2011) 2–42.
125. S. Furnell, Making security usable: Are things improving?, Comput. Secur. 26 (6) (2007) 434–443.
126. B.D. Payne, W.K. Edwards, A brief introduction to usable security, IEEE Internet Comput. 12 (2008) 13–21.
127. E.E. Schultz, Where have the worms and viruses gone? New trends in malware, Comput. Fraud Secur. 2006 (7) (2006) 4–8.
128. U. Bayer, I. Habibi, D. Balzarotti, E. Kirda, C. Kruegel, A view on current malware behaviours, in: USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), April 2009.
129. G. Cluley, Sizing up the malware threat-key malware trends for 2010, Netw. Secur. (2010), http://dx.doi.org/10.1016/S1353-4858(10)70045-3.
130. http://gocsi.com/sites/default/files/uploads/2007_CSI_Survey_full-color_no marks.indd_.pdf, last accessed: June 2013.
131. P. García-Teodoroa, J. Díaz-Verdejoa, G. Maciá-Fernándeza, E. Vázquez, Anomaly-based network intrusion detection: Techniques, systems and challenges, Comput. Secur. 28 (1–2) (2009) 18–28.
132. W. Hasselbring, R. Reussner, Toward trustworthy software systems, Computer 39 (4) (2006) 91–92, http://dx.doi.org/10.1109/MC.2006.142.
133. L.M.R. Gadelha Jr., B. Clifford, M. Mattoso, M. Wilde, Provenance management in Swift, Future Gener. Comput. Syst. 27 (6) (2011) 775–780.

134. L. Moreau, J. Freire, J. Futrelle, R.E. McGrath, J. Myers, P. Poulson, The open provenance model, http://openprovenance.org/, last accessed: June 2013.
135. K.-K. Muniswamy-Reddy, D.A. Holland, U.B.M.I. Seltzer, Provenance-aware storage systems, in: Proc. USENIX Conf., Usenix, 2006, pp. 43–56.
136. N.R. Mathiasen, S. Bodker, Experiencing security in interaction design, in: Proc. CHI 2011, 2011, pp. 2325–2334.
137. L. Barkhuus, The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI, in: Proc. CHI 2012, 2012, pp. 367–376.
138. M.Y. Ivory, M.A. Hearst, The state of the art in automating usability evaluation of user interfaces, ACM Comput. Surv. 33 (2001) 470–516.
139. M. Madden, Privacy management on social media sites, http://pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx, February 2012.
140. J. Pan, S. Paul, R. Jain, A survey of the research on future Internet architectures, IEEE Commun. Mag. 49 (7) (2011) 26–36.
141. H.P. Bui, J. Cox, S. Theobald, S. Wiegand, Trustworthy IT systems, trustworthy.googlecode.com/svn-history/r27/trunk/tex/doc.pdf, 2012.
142. S. Ding, X.J. Ma, S.L. Yang, A software trustworthiness evaluation model using objective weight based evidential reasoning approach, Knowl. Inf. Syst. 33 (2012) 171–189.
143. T. Eze, R. Anthony, C. Walshaw, A. Soper, A new architecture for trustworthy autonomic systems, in: EMERGING 2012, 2012, pp. 62–68.
144. A. Casimiro, P. Verissimo, D. Kreutz, TRONE: Trustworthy and resilient operations in a network environment, in: Proc. Dependable Sys. and Networks Workshops, 2012, pp. 1–6.
145. R. Maas, E. Maehle, Applying the organic robot control architecture ORCA to cyber-physical systems, in: Proc. SEAA, 2012, pp. 250–257.
146. H.S. Lim, G. Ghinita, E. Bertino, A game theoretic approach for high-assurance of data trustworthiness in sensor networks, in: Proc. ICDE, 2012, pp. 1192–1203.
147. M.A.P. Leandro, T.J. Nascimento, Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth, in: Proc. ICN, 2012, pp. 88–93.
148. J. Jensen, Federated identity management challenges, in: Proc. ARES, 2012, pp. 230–235.
149. D.W. Chadwick, M. Hibbert, Towards automated trust establishment in federated identity management, in: C. Fernandez-Gago, et al. (Eds.), IFIPTM 2013, in: IFIP AICT, vol. 401, 2013, pp. 33–48.
150. S. Mathew, M. Petropoulos, H.Q. Ngo, A data-centric approach to insider attack detection in database systems, in: RAID 2010, in: Lect. Notes Comput. Sci., vol. 6307, 2010, pp. 382–401.