معرفی پروژه‌های مرکز کامپیوتر و شبکهٔ پژوهشگاه

مقدمه

مرکز کامپیوتر و شبکهٔ پژوهشگاه دانش‌های بنیادی در زمستان سال ۱۳۸۲ با ایجاد هستهٔ تحقیق و توسعه اقدام به تعریف، طراحی و پیاده‌سازی سه پروژهٔ کاربردی کرد که عبارت‌اند از: پروژهٔ ویدئو کنفرانس، پروژهٔ بررسی ترافیک شبکه، و پروژهٔ جلوگیری از حملات احتمالی در شبکه.

دلایل اصلی اجرای این پروژه‌ها در مرکز شبکه عبارت‌اند از:

۱. ایجاد نرم‌افزارهایی با کد آزاد (Open Source)ـ به‌منظور به‌کارگیری در سایر مراکز آکادمیک دنیا،

۲. فراهم کردن ابزارهای مورد نیاز مدیران شبکه،

۳. تولید نرم‌افزارهای غیر قابل ابتیاع به‌دلیل وجود تحریم‌های اقتصادی،

۴. ایجاد توان و روح تحقیق و توسعه در کنار ارائهٔ خدمات مرسوم در مرکز کامپیوتر و شبکهٔ پژوهشگاه.

در زیر به‌اختصار به تشریح این پروژه‌ها می‌پردازیم.

پروژه جلوگیری حملات در شبکه

ایجاد امنیت و جلوگیری از حملات احتمالی (Intrusion-Prevention System) از مهم‌ترین مسائل در نگهداری ساختار شبکه است.

به این منظور عموماً در نقاط تماس شبکه با خارج، سیستم‌های firewall (بارو یا حفاظ) نصب می‌گردد تا از هر گونه حملهٔ احتمالی جلوگیری شود. اما استفاده از سیستم firewall به‌تنهایی کافی نیست و سیستم‌های مکملی در شبکه نصب می‌شوند که وظیفهٔ تشخیص حمله (Intrusion Detection System, IDS) را به‌عهده دارند. پس از شناسایی اختلال و منبع ایجاد آن توسط IDS وظیفهٔ جلوگیری از حمله با firewall است و پیکربندی و تنظیمات لازم از سوی مدیریت شبکه در firewall اعمال می‌گردد. IPS مجموعه‌ای از IDSها و firewallهاست.

به‌منظور تولید IPS از برخی نرم‌افزارهای رایگان استفاده شده‌است (از نرم‌افزارهای ACID و Snort به‌عنوان IDS و از نرم‌افزار Iptables سیستم‌عامل لینوکس به‌عنوان firewall). در زیر به توضیح اجزاء تشکیل دهندهٔ IPS می‌پردازیم.

۱. سیستم تشخیص حمله (IDS)

به‌منظور پیاده‌سازی این قسمت از پروژه از نرم‌افزار Snort استفاده می‌شود. این نرم‌افزار بر روی چند کامپیوتر که حسگر (Sensor) نامیده می‌شوند نصب و پیکربندی و در گسترهٔ شبکه قرار داده می‌شوند. حسگرها کلیهٔ بسته (Packet)های در حال انتقال در شبکه را بررسی و در صورت مشاهدهٔ بسته‌های غیر عادی مراتب را تحت عنوان «اعلام حمله» به سیستمی که به‌منظور اخذ گزارش از حسگرها در نظر گرفته شده است منعکس و همزمان سیستم firewall را برای جلوگیری از ادامهٔ حمله پیکربندی می‌کنند. این امر مستلزم اعمال پاره‌ای تغییرات در نرم‌افزار Snort و تعریف قاعده (rule)های جدید در آن است.

۲. ثبت و ارسال گزارش حمله

به‌منظور پیاده‌سازی این قسمت، از نرم‌افزار ACID استفاده شد. نرم‌افزار فوق در صورت دریافت گزارش حمله از سوی حسگرها، اطلاعات ارسالی را به‌همراه بسته‌های مظنون از حسگر اخذ و ثبت می‌کند و همزمان مدیر شبکه را از حمله مطلع می‌سازد (با ارسال ای‌میل و یا سایر امکانات هشداردهنده که به نرم‌افزار الحاق خواهد شد).

با توجه به مشکلات نرم‌افزار فوق برخی از جنبه‌های آن نیازمند تغییر اساسی است زیرا به‌علت محدودیت‌های ACID، در صورت زیاد شدن حجم و تعداد بسته‌های ارسالی توسط حسگرها، سیستم فوق ازکار خواهد افتاد و نیز امکان ذخیره‌سازی و تحلیل بسته‌ها را دارا نیست و این امکان باید به نرم‌افزار اضافه شود.

۳. پیکربندی خودکار سیستم Firewall

در این مرحله از نرم‌افزار Iptables موجود در سیستم‌عامل لینوکس استفاده شده است. با پیکربندی مناسب نرم‌افزار فوق می‌توان از امکانات کامل آن به‌عنوان firewall جهت تأمین امنیت شبکه و دفع حملات به شبکه بهره جست.

در این نرم‌افزار کلیهٔ قواعد مربوط به انتقال بسته‌ها با پیکربندی فایل config مربوطه قابل تعریف است. با به‌کارگیری قوانین صحیح می‌توان ترافیک ورودی و خروجی شبکه را در سطح بسته کنترل نمود. بنابراین پس از تشخیص حمله در حسگرها تحت Snort تنظیمات مناسب و از پیش طراحی شده جهت جلوگیری از ادامهٔ حمله در config فایل مربوطه به‌طور خودکار به Iptables اضافه خواهد شد.

- این پروژه در مرحلهٔ پایانی مطالعه و بررسی است که پس از اتمام این مرحله، طراحی سیستم آغاز خواهد شد.

پروژهٔ ویدئو کنفرانس

این پروژه به‌منظور ایجاد سیستم ویدئو کنفرانس تحت شبکه طراحی و پیاده‌سازی شده است. این ابزار امکان برگزاری کنفرانسی را که شرکت‌کنندگان

آن در مکان‌های مختلف شبکه قرار گرفته‌اند فراهم می‌کند. شرکت‌کنندگان کنفرانس در دو گروه قرار می‌گیرند: کسانی‌که ارسال‌کنندهٔ تصویر و صدا هستند و کسانی که دریافت‌کننده‌اند. نیاز سخت‌افزاری اولیهٔ «ارسال‌کننده» علاوه بر کامپیوتر متصل به شبکه، ابزار وب‌بین (webcam) و نیاز «دریافت‌کننده» کامپیوتر متصل به شبکه است. همچنین در این طرح چند کاربر می‌توانند به‌طور همزمان «ارسال‌کننده» و «دریافت‌کننده» باشند.

سیستم ویدئوکنفرانس شامل یک کارگزار (server) مرکزی و یک کارگزار وب بوده و استفاده‌کنندگان اعم از ارسال‌کننده و یا دریافت‌کننده در ابتدا به کارگزار وب متصل می‌شوند و پس از اعتبارسنجی (Authentication) خود مبنی بر ارسال‌کننده و یا دریافت‌کننده، امکان آغاز کنفرانس را خواهند داشت. ایجاد ارتباط و انتقال اطلاعات صوتی و تصویری از سوی ارسال‌کننده به دریافت‌کننده به‌عهدهٔ کارگزار اصلی است. در کارگزار اصلی امکان مدیریت لایه‌ای جهت تعریف مدیر اصلی کنفرانس، تعریف اعضاء کنفرانس توسط مدیرکنفرانس، زمان برپایی و پایان کنفرانس، تعداد اعضاء ارسال و دریافت‌کننده و تعدد کنفرانس‌های همزمان و ... فراهم شده است.

محیط عملکرد سیستم کنفرانس و مدیریت کنفرانس محیط وب است تا دسترسی به آن از طریق شبکهٔ اینترنت امکان پذیر باشد. اجرای این طرح بر اساس زبان Java و Activex صورت پذیرفته است.

در زیر به تشریح اجزاء تشکیل دهندهٔ این سیستم می‌پردازیم.

۱. کارگزار اصلی

این کارگزار وظیفهٔ تبادل اطلاعات صوتی و تصویری بین کاربران را به‌عهده دارد. اعتبارسنجی ارسال‌کننده و دریافت‌کننده، تعاریف مربوط به هرکنفرانس و اعضاء آن در این کارگزار صورت می‌پذیرد.

۲. کارگزار وب

این کارگزار واسط بین کاربر و کارگزار اصلی است و کاربر در ابتدا به این کارگزار متصل و از طریق آن اعتبارسنجی می‌شود. کلیهٔ صفحات مربوط به‌تعریف کنفرانس، مدیرکنفرانس و ... و صفحات مربوط به‌ارسال‌کنندگان و دریافت‌کنندگان کنفرانس‌ها در این کارگزار قرار دارد و هیچ اتصال مستقیم بین مدیر، کاربر، و کارگزار اصلی وجود ندارد.

۳. ارسال کنندهٔ اطلاعات

ارسال‌کنندهٔ اطلاعات شامل کامپیوتر و وب‌بین است که کاربر آن توسط کارگزار اصلی به‌عنوان «ارسال‌کننده» مجاز شناخته می‌شود.

۴. دریافت‌کنندهٔ اطلاعات

کاربرانی که توسط مدیرکنفرانس به‌عنوان دریافت‌کننده معرفی شده‌اند با استفاده از یک دستگاه کامپیوتر متصل به شبکه پس از اعتبارسنجی، امکان دریافت اطلاعات صوتی و تصویری کنفرانس را (از طریق صفحهٔ وب که کارگزار وب در اختیار آنها قرار می‌دهد)، خواهند داشت.

۵. سیستم پایگاه داده‌ای

در این سیستم اطلاعات مربوط به کنفرانس‌ها و دریافت‌کنندگان و ارسال‌کنندگان نگهداری می‌شود. اطلاعات موجود در این پایگاه توسط مدیر اصلی سیستم و مدیرکنفرانس‌ها فراهم می‌شود و برای تأیید مجوز مورد استفادهٔ کاربران قرار می‌گیرد.

- نسخهٔ اول این پروژه تهیه شده و در حال استفادهٔ آزمایشی است تا ایرادهای احتمالی آن شناسایی و رفع شود.

پروژهٔ بررسی ترافیک واسط‌های شبکه

از اساسی‌ترین مسائل در نگهداری شبکه اعم از شبکهٔ محلی و شبکهٔ گسترده، بررسی ترافیک ایجاد شده و در حال انتقال از واسط‌های مختلف شبکه از قبیل مسیریاب‌ها (Routers)، سویچ‌ها، و کارگزارهاست که این بررسی تا سطح پایانهٔ کاربر قابل تعمیم است. برخی از نتایج حاصل از این کنترل عبارت است از تعیین حجم ترافیک طبیعی شبکه، میزان ترافیک مورد نیاز، وجود اشکال و اختلال، پیش‌بینی ترافیک مورد نیاز و اخذ بسیاری از داده‌های آماری تحلیلی که در طراحی و توسعهٔ شبکه و واسط‌های آن کاربرد دارد. پروتکل SNMP امکان اخذ بسیاری از اطلاعات مورد نیاز از واسط‌ها را فراهم می‌سازد. بررسی توسط نرم‌افزار MRTG صورت می‌گیرد که امکان تحلیل برخی از اطلاعات فراهم شده توسط SNMP را داراست و حاصل این تحلیل، رسم نمودارهایی برحسب زمان/ترافیک است. از آنجایی‌که نرم‌افزار MRTG فرم عمومی اطلاعات SNMP را تحلیل می‌کند بسیاری از امکانات مورد نیاز مدیر شبکه را ندارد. لذا در این پروژه طراحی و تولید نرم‌افزاری مد نظر است که نیازهای مدیر و کاربر شبکه را برآورده سازد.

در این پروژه علاوه بر ایجاد امکان تحلیل ترافیک واسط‌ها، امکان تعریف کاربران با سطوح دسترسی مختلف، و اضافه نمودن مکان‌های مجزا، و واسط‌های مختلف فراهم شده است.

به‌طور خلاصه امکانات حاصل از این پروژه عبارت‌اند از:

- تعریف کاربر سیستم در سطوح مختلف فیزیکی
- تعریف مسیریاب‌ها و سوئیچ‌ها
- تعریف مکان فیزیکی واسط‌ها
- ایجاد و ثبت اطلاعات مربوط به واسط‌ها
- امکان تولید و نمایش اطلاعات مورد خواست کاربر

این نرم‌افزار تحت محیط وب و مستقل از نوع سیستم‌عامل با استفاده از زبان برنامه‌نویسی Java پیاده‌سازی شده است. در زیر به تشریح بخش‌های مختلف این نرم افزار می‌پردازیم.

۱. کارگزار MRTG

این کارگزار وظیفهٔ اخذ اطلاعات ترافیکی از واسط‌های شبکه را عهده‌دار است.

اطلاعات فوق از طریق پروتکل SNMP از هر واسط اخذ و کارگزار اطلاعات دریافتی را به‌صورت لحظه‌ای، روزانه، هفتگی و ماهانه درپایگاه داده‌ای به‌صورت چرخشی (Round Robin) ذخیره می‌کند.

این روش در مؤسسهٔ فناوری فدرال سوئیس (SFIT) با همکاری و مشارکت بسیاری از محققان در سطح دنیا طراحی و اجرا شده است.

از دیگر امکانات این کارگزار، تهیه نمودارهای مورد درخواست کاربر از اطلاعات ذخیره شده و نمایش آن از طریق واسط است. این کارگزار تحت زبان برنامه‌نویسی Java پیاده‌سازی شده و فارغ از نوع سیستم‌عامل قابل نصب است.

۲. کارگزار وب

کارگزار وب واسط بین کاربر و کارگزار MRTG و نیز واسط بین کاربر و کارگزار SQL است.

کنترل کلیهٔ عملیات در این کارگزار و توسط زنجیره‌ای از Servletها صورت می‌پذیرد. با توجه به‌نوع درخواست کاربر، کارگزار وب عمل درخواستی را به کارگزار SQL و یا MRTG ارجاع و نتیجه را به کاربر ارسال می‌دارد.

۳. پایگاه داده‌ای

پیاده‌سازی این بخش با نرم‌افزار My SQL صورت گرفته است و در واقع کلیهٔ اطلاعات مربوط به لایهٔ کاربری، لایهٔ واسط‌ها و گره‌ها در آن نگهداری می‌شود.

- نسخهٔ اولیهٔ این نرم‌افزار تهیه شده و در حال حاضر نصب و مراحل آزمون را می‌گذراند.

عباس نوذری، پژوهشگاه و دانشگاه تهران.
کامران شکوفنده، پژوهشگاه.

از راست: عباس نوذری، سعید خادمی، اکبر بهزادی، مقصود عباسپور، و کامران شکوفنده

جمعی از همکاران مرکز کامپیوتر و شبکهٔ پژوهشگاه