بسم تعالی

ارتقای امنیت پروتکل SSL در وب سایت با استفاده از کنترلر فازی

محدثه میاندار

استاد:

سرکار خانم خادم القرآنی

دانشگاه شیخ بهایی

خرداد 1402

چکیده

یکی از خواسته های کاربران اینترنت امنیت صفحات وب می باشد. صفحات وب روزانه مورد حمله تعداد بسیار زیادی از هکرها قرار می گیرند. در این مقاله به بررسی آسیب پذیری های ssl و حملات روی این پروتکل می پردازیم و روش جدیدی برای بالا بردن امنیت آن معرفی میکنیم. این روش از منطق فازی استفاده می کند. داده های رمز نگاری شده در پروتکل SSL با استفاده از کنترلر فازی به داده های فازی یا کیفی تبدیل می شوند. این روش پروتکل SSL را در برابر حملاتی مانند POODLE امن می سازد و از بهترین روش های بالا بردن امنیت وب سایت ها با استفاده از پروتکل HTTPS است.

واژه های کلیدی: SSL، منطق فازی، امنیت وب سایت

فصل اول

1. مقدمه

با توجه به افزایش کاربرد فناوری اطلاعات در جوامع بشری، سازمان‌ها تمایل دارند سیستم‌های اطلاعاتی را پیاده‌سازی کنند و از فرصت‌هایی که این فناوری‌ها به آن‌ها می‌دهد استفاده کنند. بنابراین، هر ساله سازمان‌ها سرمایه‌گذاری‌هایی در زمینه فناوری و سیستم‌های اطلاعاتی انجام می‌دهند، اما با این حال، برخی از سازمان‌ها به دلیل عدم توانایی در استفاده از سیستم‌های اطلاعاتی به شکست می‌خورند. بر این اساس، تحقیقات زیادی درباره عوامل مؤثر در موفقیت یا شکست پروژه‌های امنیت وب سایت انجام شده است و عوامل مؤثر در شکست یا موفقیت سیستم‌های امنیتی وب سایت، به عنوان یکی از موضوعات محبوب در بین محققان محسوب می‌شود. با پیشرفت سریع فناوری برتر، به ویژه در زمینه ارتباطات، رایانه و وب سایت‌ها، الگوی رشد اقتصادی جهان تغییر کرده و به دنبال آن، امنیت در شبکه به عنوان مهمترین سرمایه جایگزین سرمایه‌های پولی و فیزیکی محسوب می‌شود.

2. بیان مسئله

پروتکل لایه سوکت های امن (SSL) یک پروتکل امنیتی پرکاربرد برای ارتباط آنلاین بین مشتری و سرور است. پروتکل SSL با رمزگذاری ارتباط بین مشتری و سرور، محرمانه بودن و یکپارچگی داده های منتقل شده از طریق اینترنت را تضمین می کند. با وجود اثربخشی پروتکل SSL، هنوز چندین آسیب پذیری وجود دارد که می تواند توسط مهاجمان برای به خطر انداختن امنیت وب سایت مورد سوء استفاده قرار گیرد. یکی از راه حل های ممکن برای افزایش امنیت پروتکل SSL استفاده از کنترل کننده فازی است. کنترل کننده فازی نوعی کنترل کننده هوش مصنوعی (AI) است که از منطق فازی برای تصمیم گیری استفاده می کند. منطق فازی نوعی منطق ریاضی است که با اطلاعات غیر دقیق و نامطمئن سروکار دارد. کنترل کننده های فازی می توانند بر اساس مجموعه ای از قوانین که رفتار سیستم را تعریف می کنند، تصمیم گیری کنند.
در مورد امنیت پروتکل SSL، یک کنترل کننده فازی می تواند به صورت پویا پارامترهای SSL را بر اساس شرایط شبکه و ترافیک فعلی تنظیم کند تا از امنیت مطلوب اطمینان حاصل کند. با این حال، تحقیقات کافی در مورد اثربخشی کنترل‌کننده های فازی در افزایش امنیت پروتکل SSL وجود ندارد. بنابراین، بیان مشکل بررسی امکان‌سنجی و اثربخشی استفاده از یک کنترل‌کننده فازی برای افزایش امنیت پروتکل SSL در وبسایت است. در نتیجه، افزایش امنیت پروتکل SSL در وب سایت با استفاده از یک کنترل کننده فازی می تواند یک راه حل امیدوارکننده برای اطمینان از امنیت مطلوب باشد. با این حال، امکان سنجی و اثربخشی استفاده از یک کنترل کننده فازی باید به طور کامل بررسی شود تا بقای آن به عنوان یک مکانیسم افزایش امنیت مشخص شود.

3. اهمیت و ضرورت موضوع تحقیق

اهمیت و ضرورت موضوع تحقیق افزایش امنیت پروتکل SSL با استفاده از کنترل کننده فازی در نیاز به تضمین امنیت ارتباطات آنلاین و حفاظت از داده های حساسی است که از طریق اینترنت منتقل می شود. همانطور که ارتباطات آنلاین در زندگی روزمره ما رایج تر می شود، ایمن سازی انتقال داده ها به طور فزاینده ای حیاتی شده است. هر گونه مصالحه در امنیت ارتباطات آنلاین می تواند منجر به عواقب جدی مانند ضرر مالی، سرقت هویت یا سایر موارد نقض امنیتی شود.

پروتکل SSL به طور گسترده ای برای ایمن سازی ارتباط آنلاین بین مشتری و سرور استفاده می شود. با این حال، آسیب پذیری های موجود در پروتکل SSL همچنان می تواند توسط مهاجمان برای به خطر انداختن امنیت وب سایت مورد سوء استفاده قرار گیرد. برای افزایش امنیت پروتکل SSL، یک راه حل ممکن استفاده از یک کنترل کننده فازی برای تنظیم پویا پارامترهای SSL بر اساس شرایط شبکه و ترافیک فعلی است. این می تواند به تضمین امنیت مطلوب و جلوگیری از حملات احتمالی کمک کند.

موضوع تحقیق افزایش امنیت پروتکل SSL با استفاده از یک کنترل کننده فازی مهم و ضروری است زیرا می تواند بینش های ارزشمندی در مورد اثربخشی استفاده از کنترل کننده فازی به عنوان مکانیزم افزایش امنیت ارائه دهد. از طریق این تحقیق، ما می توانیم درک بهتری از نحوه استفاده از یک کنترل کننده فازی برای بهبود امنیت ارتباطات آنلاین و محافظت از داده های حساس به دست آوریم. علاوه بر این، این تحقیق می تواند به توسعه راه حل های امنیتی قوی تر و قابل اعتمادتر برای وب سایت ها کمک کند، که در عصر دیجیتال امروز ضروری است.

در نتیجه، موضوع تحقیق افزایش امنیت پروتکل SSL با استفاده از یک کنترل کننده فازی در تضمین امنیت ارتباطات آنلاین و محافظت از داده های حساس منتقل شده

از طریق اینترنت بسیار مهم است. از طریق این تحقیق، می‌توانیم اقدامات امنیتی مؤثر را شناسایی کرده و راه‌حل‌های امنیتی قوی‌تر و قابل اعتمادتری برای جلوگیری از حملات احتمالی و حفظ امنیت آنلاین ایجاد کنیم.

4. اهداف تحقیق

هدف کلی:

هدف کلی این تحقیق بررسی امکان سنجی و اثربخشی استفاده از کنترل کننده فازی برای افزایش امنیت پروتکل SSL در وب سایت می باشد.

اهداف ویژه:

1. بررسی ادبیات امنیت پروتکل SSL و کنترل‌کننده های فازی برای شناسایی نظریه‌ها و مفاهیم مرتبط.

2. طراحی و پیاده سازی یک کنترل کننده فازی برای تنظیم پویا پارامترهای SSL بر اساس شرایط شبکه و ترافیک فعلی.

3. ارزیابی اثربخشی کنترل‌کننده فازی در افزایش امنیت پروتکل SSL با انجام تست‌های نفوذ برای شبیه‌سازی حملات احتمالی.

4. برای مقایسه سطح امنیتی به دست آمده با استفاده از یک کنترل کننده فازی با پروتکل سنتی SSL بدون کنترل کننده فازی.

5. برای ارزیابی تاثیر استفاده از یک کنترل کننده فازی بر عملکرد وب سایت و تجربه کاربری.

اهداف عملی:

1. راه اندازی یک محیط آزمایشی برای اجرای پروتکل SSL و تست نفوذ.

2. توسعه نرم افزار برای پیاده سازی کنترل کننده فازی.

3. ع آوری و تجزیه و تحلیل داده ها در مورد شرایط شبکه و ترافیک.

4. انجام تست های نفوذ برای شبیه سازی حملات احتمالی و ارزیابی امنیت وب سایت.

5. سنجش عملکرد وب سایت و تجربه کاربر با استفاده از معیارهای مربوطه.

6. تفسیر و گزارش یافته های تحقیق به صورت واضح و مختصر.

5. سوالات پژوهشی

1. تئوری ها و مفاهیم کلیدی مرتبط با امنیت پروتکل SSL و کنترل کننده های فازی چیست؟

2. وضعیت فعلی تحقیقات در مورد استفاده از کنترل کننده های فازی در افزایش امنیت پروتکل SSL چگونه است؟

3. محدودیت ها و چالش های استفاده از کنترل کننده های فازی برای امنیت پروتکل SSL چیست؟

4. چگونه می توان یک کنترل کننده فازی برای تنظیم پارامترهای SSL بر اساس شرایط شبکه و ترافیک طراحی کرد؟

5. ورودی و خروجی های لازم کنترل کننده فازی چیست؟

6. چگونه می توان کنترل کننده فازی را با اجرای پروتکل SSL ادغام کرد؟

7. چه نوع حملاتی در تست های نفوذ شبیه سازی خواهند شد؟

8. شاخص های کلیدی عملکرد برای ارزیابی اثربخشی کنترل کننده فازی چیست؟

9. چگونه اثربخشی کنترل کننده فازی با پروتکل SSL سنتی بدون کنترل کننده فازی مقایسه می شود؟

10. تفاوت های کلیدی در سطح امنیتی که با استفاده از یک کنترل کننده فازی در مقابل پروتکل SSL سنتی به دست می آید چیست؟

11. عملکرد کنترل کننده فازی از نظر سطح امنیتی چگونه با پروتکل سنتی SSL مقایسه می شود؟

12. معاوضه بین استفاده از یک کنترل کننده فازی با پروتکل سنتی SSL از نظر امنیت و عملکرد چیست؟

13. معیارهای کلیدی عملکرد برای ارزیابی تأثیر استفاده از کنترل کننده فازی بر عملکرد وب سایت چیست؟

14. عملکرد وب سایت با استفاده از یک کنترل کننده فازی در مقایسه با پروتکل SSL سنتی چگونه است؟

15. تصورات و تجربیات کاربر از استفاده از یک وب سایت با کنترل کننده فازی برای امنیت پروتکل SSL چیست؟

6. شرح واژه ها و اصطلاحات به کار رفته در پژوهش

پروتکل SSL:

پروتکل لایه سوکت های امن (SSL) یک پروتکل استاندارد است که ارتباط امن بین یک وب سرور و یک مرورگر وب را امکان پذیر می کند. این رمزگذاری داده های منتقل شده بین سرور و مرورگر را فراهم می کند و اطمینان می دهد که داده های مبادله شده بین این دو خصوصی و ایمن نگه داشته می شوند. پروتکل SSL به طور گسترده ای برای ارتباط امن در برنامه های کاربردی وب مانند بانکداری آنلاین، تجارت الکترونیک و خدمات ایمیل استفاده می شود (Freier et al., 2011).

کنترل کننده فازی:

کنترل کننده فازی یک سیستم کنترلی است که از منطق فازی برای تنظیم پارامترهای سیستم بر اساس داده های ورودی استفاده می کند. برخلاف سیستم های کنترل سنتی که از مدل های دقیق ریاضی استفاده می‌کنند، کنترل‌کننده های فازی از اطلاعات نادقیق، نامطمئن یا ناقص برای تصمیم‌گیری استفاده می‌کنند. کنترل‌کننده های فازی معمولاً در سیستم هایی استفاده می‌شوند که مدل‌سازی ریاضی آنها دشوار است، مانند فرآیندهای صنعتی، روباتیک و سیستم های کنترل ترافیک (Passino et al., 1998).

امنیت وب سایت:

امنیت وب سایت به اقداماتی اطلاق می شود که برای محافظت از یک وب سایت در برابر دسترسی غیرمجاز، سرقت داده ها و سایر موارد نقض امنیتی انجام می شود. امنیت وب سایت برای حفظ محرمانه بودن، یکپارچگی و در دسترس بودن داده های حساس مانند اطلاعات کاربر، تراکنش های مالی و داده های تجاری بسیار مهم است. اقدامات رایج امنیتی وب سایت شامل رمزگذاری، فایروال

ها، سیستم های تشخیص نفوذ و پیشگیری، و شیوه های کدگذاری ایمن است (Stein, 1998).

شرایط شبکه:

شرایط شبکه به وضعیت شبکه از جمله حجم ترافیک، تاخیر و پهنای باند اشاره دارد. شرایط شبکه می تواند تأثیر قابل توجهی بر عملکرد و امنیت سیستم داشته باشد، به ویژه در مورد برنامه های کاربردی وب که بر ارتباطات شبکه متکی هستند. شرایط بد شبکه می تواند باعث تاخیر در انتقال داده ها، از دست دادن داده ها و ازدحام شبکه شود که منجر به کاهش عملکرد سیستم و افزایش خطرات امنیتی می شود (McGrath & Krackhardt, 2003).

تست نفوذ:

تست نفوذ که به عنوان تست قلم نیز شناخته می شود، یک حمله سایبری شبیه سازی شده به یک سیستم کامپیوتری برای ارزیابی سطح امنیتی آن است. تست نفوذ توسط هکرهای اخلاقی انجام می شود که سعی می کنند از آسیب پذیری های سیستم برای دسترسی غیرمجاز به داده های حساس سوء استفاده کنند. نتایج تست نفوذ برای شناسایی نقاط ضعف در سیستم و توسعه و اجرای اقدامات امنیتی برای محافظت در برابر نقض‌های امنیتی احتمالی استفاده می‌شود (Bacudio et al., 2011).

معیارهای عملکرد:

معیارهای عملکرد معیارهای کمی هستند که برای ارزیابی عملکرد یک سیستم یا فرآیند استفاده می شوند. معیارهای عملکرد می تواند شامل معیارهایی مانند زمان پاسخ، توان عملیاتی، نرخ خطا و استفاده از منابع باشد. معیارهای عملکرد برای ارزیابی اثربخشی یک سیستم یا فرآیند و شناسایی زمینه های بهبود استفاده می شود (Palmer, 2002).

تجربه ی کاربر:

تجربه کاربری به تجربه کلی و رضایت کاربر از یک محصول یا خدمات اشاره دارد. در مورد برنامه های کاربردی وب، تجربه کاربر می تواند تحت تأثیر عواملی مانند طراحی وب سایت، سهولت استفاده و عملکرد سیستم باشد. تجربه مثبت کاربر می تواند منجر به افزایش تعامل کاربر و وفاداری مشتری شود، در حالی که تجربه منفی کاربر می تواند منجر به کاهش رضایت کاربر و کاهش حفظ مشتری شود (Allam & Dahlan, 2013).

افزایش امنیت:

ارتقای امنیت به فرآیند بهبود امنیت یک سیستم یا فرآیند از طریق اجرای اقدامات امنیتی جدید اشاره دارد. افزایش امنیت اغلب با تغییرات در چشم انداز تهدید، آسیب پذیری ها یا ضعف های جدید کشف شده در سیستم یا الزامات نظارتی انجام می شود. ارتقای امنیت می تواند شامل اجرای کنترل های امنیتی جدید، به روز رسانی اقدامات امنیتی موجود، یا تغییر در سیاست ها و رویه های امنیتی باشد (Jalal & Zeb, 2008).

فصل دوم

1. مقدمه

در این مقاله ما می‌خواهیم تکنیک جدیدی را معرفی کنیم تا امنیت بلاک رمزنگاری یا plaintext را بالا برده و در نتیجه امنیت پروتکل SSL 2، افزایش یابد. برای رسیدن به این هدف منطق فازی را معرفی می‌کنیم.

2. مروری بر مفاهیم و ادبیات تحقیق

HTTPS پروتکلی است که در بستر آن امکان رمزنگاری (encrypt) اطلاعات فراهم می‌شود، به لحاظ تخصصی درHTTP پورت ۸۰ مورد استفاده قرار می‌گیرد، در حالی که در HTTPS پورت ۴۴۳ مورد استفاده است. در HTTP داده‌ها به صورت متن ساده (plain text)

هستند اما در HTTPS رمزنگاری داده‌ها به وسیله SSL انجام می‌شود. SSL مخفف Secure Sockets Layer است و در اصطلاح به سیستم امن و رمزی انتقال داده اطلاق می‌شود، SSL را ابتدا به منظور نقل و انتقال امن و رمزی اطلاعات بوجود آمد و اکنون تقریباً تمام مرورگرهای استاندارد آن را پشتیبانی می‌نمایند (Georgiev et al., 2012).

به بیانی ساده، در SSL پس از برقراری اتصال امن، اطلاعات به وسیله دو کلید رمزنگاری می‌شوند، کلید عمومی برای اشخاص سوم شخص قابل خواندن است اما کلید دوم تنها توسط ارسال کننده و دریافت کننده داده قابل استفاده می‌باشد. چند فاکتور در تعیین معتبر بودن گواهی یک سایت نقش دارند، اول از همه کلید کوچکی است که در مرورگرها نشان داده می‌شود. در بعضی مرورگرها هنگام اتصال امن، نوار آدرس را به رنگ سبز نیز نشان داده می‌شود؛ فاکتوردیگر وجود عبارت https در ابتدای آدرس آن سایت است (Clark & Van Oorschot, 2013).

تاکنون چندین آسیب‌پذیری مهم در پروتکل SSL/TLS با حملات شناخته شده از جمله Poodle شناسایی شده‌اند. وظیفه پروتکل های امنیتی لایه حمل و نقل (SSL/TLS) حفظ محرمانگی اطلاعات منتقل شده است. از مهم‌ترین مشکلات این حملات عدم آگاهی قربانی از آن‌ها می‌باشد. به راحتی و با اتصال به وب سایت‌های جعلی بانک و وارد کردن اطلاعات خود، مهاجم به اطلاعات محرمانه رمزنگاری نشده دسترسی پیدا کرده و می‌تواند از آن استفاده کند. شرکتTrustworthy Internet Movement پیرو طرحی جدید با نام PulseSSL، کیفیت و ایمنی سایت‌های برتر در سراسر اینترنت را بررسی کرده که طی آن 75 درصد این سایت‌ها در مقابل حمله BEAST SSL آسیب‌پذیر شناخته شده و تنها 10 درصد از سایت‌های بررسی شده، امن برآورد شدند.

این طرح بررسی می‌کند که هر سایت از کدام پروتکل‌های TLS و SSL پشتیبانی می‌کند و آیا در مقابل حمله BEAST و دیگر حملات آسیب‌پذیر هست یا خیر. اطلاعاتی که به وسیله این طرح جمع‌آوری شد نشانگر این است که از نزدیک به ۲۸۸ هزار سایت بررسی شده در این طرح، اکثر آن‌ها نیاز به‌کمک جدی برای رفع مشکلات مربوط به پیاده‌سازی SSL داشتند (Möller et al., 2014). این حمله از chosen-plaintext استفاده می‌کند که علیه پیاده‌سازی AES در پروتکل TLS 1.0 انجام می‌شود و برای حمله کننده امکان استفاده از ابزاری خاص برای سرقت و رمزگشایی کوکی‌های HTTPS را فراهم می‌کند. سپس حمله کننده می‌تواند درخواست‌های SSL توسط قربانی به سایت‌های تجارت الکترونیکی و یا اینترنت بانک را برباید.حمله BEAST بسیار پیچیده است، اما نگرانی جدی و واقعیت این است که سه چهارم از سایت‌هایی که در این‌طرح مورد بررسی قرار گرفتند، هنوز هم در معرض انواع حملات دردسرساز هستند. این سایت‌ها می‌توانستند تنها با کاهش انتشار TLS 1.0 میزان حملات را کاهش دهند و برای این کار لازم بود که تنظیمات سرورهایشان‌طوری باشد که در طی ارسال درخواست‌های TLS 1.0 و SSL 3.0 تنها از حروف رمزی RC4 استفاده کنند. نگرانی بزرگ دیگر درباره اطلاعات به دست آمده از گزارش SSL این است که یک سوم از سایت‌هایی که از پروتکل SSL 2.0 پشتیبانی می‌کنند ناامن تلقی می‌شوند. متخصصان توصیه می‌کنند که به دلیل ضعف موجود در SSL 2.0 از این ورژن استفاده نشود. بیشتر الگوریتم‌های رمز نگاری مورد استفاده در SSL روی بلاک‌های 8 یا 16 بایتی از داده کار می‌کنند. در اینجا برای راحتی فرض می‌کنیم که از یک الگوریتم 16 بایتی استفاده می‌شود؛ بنابراین مثلاً داده باید به تکه‌های 16بایتی تقسیم شده و عملیات رمز نگاری

روی این بسته‌های 16 بایتی انجام شود. چون ممکن است طول داده مضربی از 16 نباشد، ابتدا باید با اضافه کردن چند کاراکتر اضافی به انتهای داده (padding) می‌گویند طول آن را به مضربی از 16 تغییر داد. روش مورد استفاده در SSL 3 این‌طور است که آخرین کاراکتر نشان می‌دهد که چند کاراکتر padding وجود دارد.

در مورد نحوه استفاده از آسیب‌پذیری، ابتدا حمله کننده باید طول درخواست را به گونه ای تغییر دهد که یک‌کاراکتر (مثلا آخرین کاراکتر کوکی در آخر یک بلاک قرار بگیرد (طبق فرضها او طول و جای کوکی را می‌داند) و ضمناً طول درخواست هم به گونه ای باشد که یک بلاک کامل به padding اختصاص داده شود. هر بلاک رمزنگاری نشده یا plaintext از P1 تا P5 نام گذاری شده است. حمله کننده با استفاده از جاواسکریپت می‌تواند urlو body درخواست را تغییر دهد چون به بلاک رمزنگاری شده دسترسی دارد (Clark & Van Oorschot, 2013; Georgiev et al., 2012).

3. خلاصه فصل

در این فصل، به معرفی یک تکنیک جدید به نام منطق فازی می‌پردازیم که به افزایش امنیت بلاک رمزنگاری یا plaintext و در نتیجه افزایش امنیت پروتکل SSL 2 کمک می‌کند. تکنیک منطق فازی باعث ایجاد بردارهای ورودی تصادفی و متغیر می‌شود که در بررسی و آزمایش پروتکل SSL 2 استفاده می‌شوند.

این روش، موجب افزایش پوشش تست و شناسایی مشکلات امنیتی مختلف می‌شود. با استفاده از منطق فازی، امنیت پروتکل SSL2 قابل بهبود است و می‌تواند راهکارهای جدیدی را برای مقابله با تهدیدات امنیتی فراهم کند.

فصل سوم

1. مقدمه

در این فصل، به بررسی روش تحقیق مورد استفاده در این گزارش کتبی خواهیم پرداخت. روش تحقیق ابزاری است که ما را در جمع‌آوری و تحلیل داده‌ها، درک و بررسی سوالات تحقیقاتی و در نهایت به دست آوردن نتایج و استنباط‌های قابل اعتماد کمک می‌کند.

ابتدا، در این فصل، به شرح و توصیف روش تحقیق مورد استفاده خواهیم پرداخت. این شامل توصیف جامعه‌ی آماری، انتخاب نمونه و تعیین اندازه نمونه، جمع‌آوری داده‌ها و فرایند انجام آن، و همچنین ابزارها و روش‌های استفاده شده در جمع‌آوری و سنجش داده‌ها می‌شود. سپس، خواهیم پرداخت به توصیف و بررسی روش‌های تحلیل داده که در این تحقیق به کار گرفته شده‌اند. این شامل توضیح روش‌های آماری و تحلیلی است که برای تجزیه و تحلیل داده‌ها به کار گرفته شده‌اند و نحوه‌ی استخراج نتایج و استنباط‌های مربوطه می‌باشد.

در نهایت، به بررسی روایی و اعتبارپذیری روش تحقیق مورد استفاده خواهیم پرداخت. ما به بررسی قوت‌ها و ضعف‌ها، محدودیت‌ها و معایب، و همچنین رویکردهایی که برای افزایش قابلیت اطمینان و صحت نتایج مورد استفاده قرار گرفته‌اند، خواهیم پرداخت. با بررسی دقیق روش تحقیق مورد استفاده در این گزارش کتبی، ما قادر خواهیم بود تا به طور دقیق‌تر نتایج و استنباط‌های حاصل از تحقیق را در فصل‌های بعدی ارائه کنیم.

2. روش تحقیق

مکانیزم های تشکیل دهنده SSL با استفاده از داده های فازی

تأیید هویت سرویس دهنده:

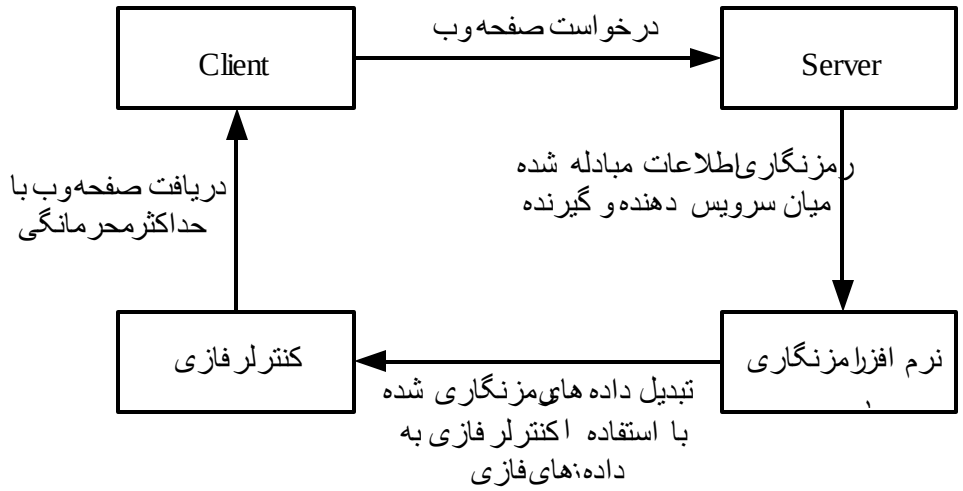
با استفاده از این ویژگی درSSL یک کاربر از صحت هویت یک سرویس دهنده مطمئن می شود. نرم افزارهای مبتنی بر SSL سمت سرویس گیرنده (مثلاً یک مرورگر وب نظیر Internet Explorer) با استفاده از تکنیک های استاندارد رمزنگاری مبتنی بر کلید عمومی و مقایسه با کلیدهای عمومی یک سرویس دهنده)مثلاً یک برنامه سرویس دهنده وب نظیر IIS) می تواند از هویت او مطلع شود و پس از اطمینان کامل، کاربر می تواند نسبت به وارد نمودن اطلا عات خود مانند شماره کارت های اعتباری و یا گذرواژه ها اقدام نماید.

تأیید هویت سرویس گیرنده:

برعکس حالت قبلی در اینجا سرویس دهنده است که می بایست از صحت هویت سرویس گیرنده اطمینان یابد .طی این مکانیزم، نرم افزار مبتنی بر SSL سمت سرویس دهنده پس از مقایسه نام سرویس گیرنده با نام های مجاز موجود در لیست سرویس گیرنده های مجاز که در داخل سرویس دهنده تعریف می شود ، در صورت وجود، اجازه استفاده از سرویس های مجاز را به او می دهد.

ارتباطات رمز شده:

کلیه اطلاعات مبادله شده میان سرویس دهنده و گیرنده می بایست توسط نرم افزارهای موجود در سمت سرویس دهنده و سرویس گیرنده ، رمزنگاری (Encrypt) شده و با استفاده از کنترلر فازی این داده های رمزگذاری شده به داده های فازی تبدیل شوند و در طرف مقابل رمزگشایی (Decrypt) و بعد داده های رمزگشایی که فازی هستند دوباره به داده های نرمال تبدیل شوند (با استفاده از کنترلر فازی) تا حداکثر محرمانگی (Confidentiality) در این گونه سیستم ها لحاظ شود. شکل 1 این مکانیزم ها را نشان می دهد:



شکل 1 - مکانیزم های تشکیل دهنده SSL با استفاده از منطق فازی

طراحی کنترلر فازی

اصولا برای طراحی کنترل کننده منطق فازی دو روش وجود دارد:

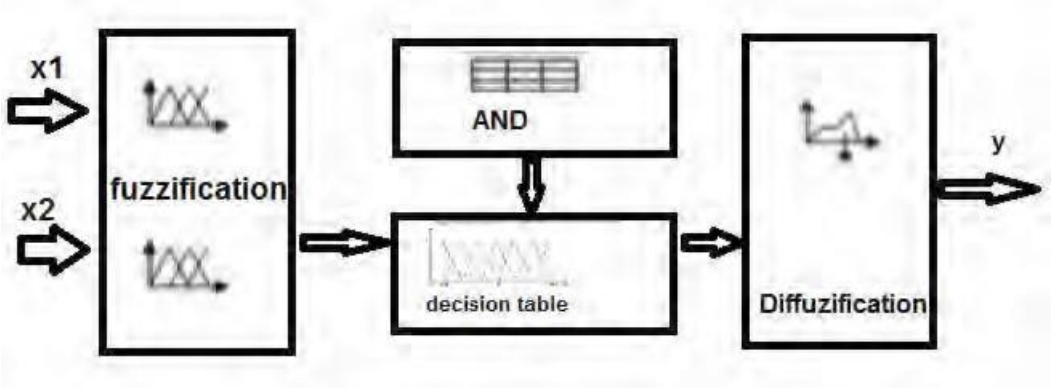
1- روش مهندسی کنترل

2- روش تخصصی

در ابتدا، ساختار کنترل کننده فازی و انتخاب پارامترها لازم است. طراحی و اجرای کنترل کننده منطق فازی اغلب به دانش و تجربه متخصصان و یا بینش و حرفه کارشناسان بستگی دارد. این رویکرد می تواند به ساخت یک مدل فازی یا مدل اولیه یک کنترل کننده فازی کمک کند. رویکرد بعدی کاربرد مهندسی کنترل و طراحی کنترل کننده فازی در بعضی جنبه ها شبیه طراحی های معمولی با انتخاب پارامترها بستگی به کارایی کنترل کننده دارد. در کنترل فازی از قوانین منطق فازی برای به دست آوردن کاربردهای کنترلی استفاده می شود. قوانین فازی بر پایه قوانین کنترلی استوار است .طراحی سیستم منطق فازی بر پایه مدل ریاضی نمی باشد . کنترل کننده های فازی با استفاده از منطق فازی، منطق بشری را پیاده کرده است که با توابع عضویت ،قوانین فازی و قوانین عضویت برنامه ریزی شده است. کنترل کنندههای فازی، خطا و تغییرات خطا را به عنوان تغییرات ورودی در نظر می گیرند.

در اینجا کنترل کننده فازی را در یک سیستم کنترل حلقه بسته در نظر می گیریم .خروجی با ورودی مقایسه می شود. کنترل کننده منطق فازی شامل چهار اصل می باشد که در شکل 2 نشان داده می شود. اصول فازی و دفازی برای تبدیل سیگنال های موج دار به فازی و برعکس استفاده شده و یک تطابق بین جریان فازی

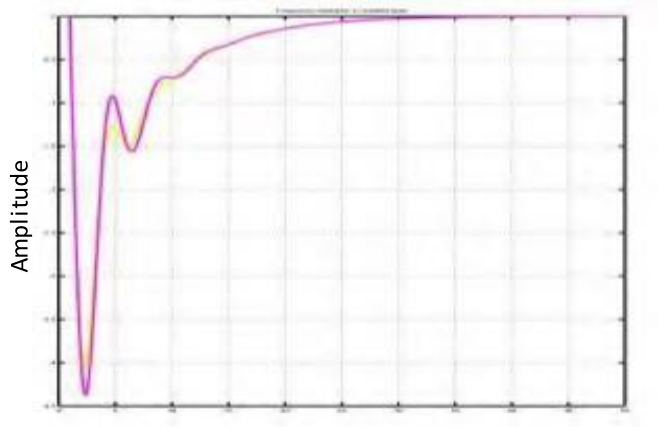
inference مکانیسم استنتاج ورودی با میدان ورودی به وجود می آورد. سپس قواعد برانگیختگی ترکیب می شوند تا قوانین کنترلی را شکل دهند.



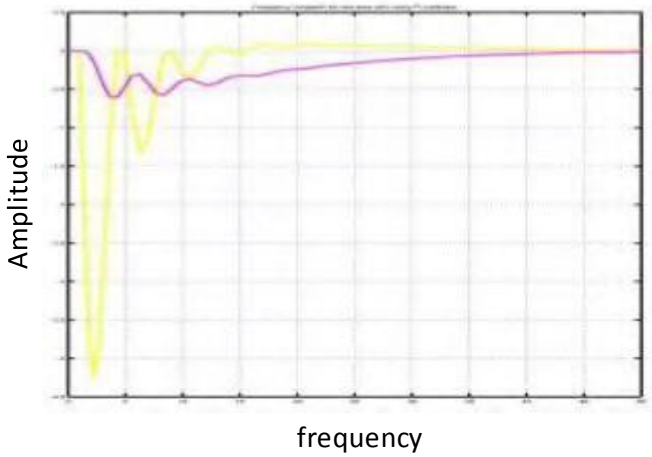
شکل 2 - کنترل کننده منطق فازی

نتایج و شبیه سازی

کنترل کننده فازی طراحی شده به دو ناحیه سیستم قدرت اعمال شده است. پاسخ سیستم با کنترل کننده های معمولی PI و نوع تکمیل شده کنترل کننده ، مقایسه شده است. شبیه سازی سیستم با استفاده از سیمولینک و ویژوال++C و جعبه ابزار fuzzy logic toolbox بوده و شکل موج ها بصورت شکل های 4 و4 نشان داده شده است



شکل 3 - انحراف frequencyفرکانس در کنترلر PI

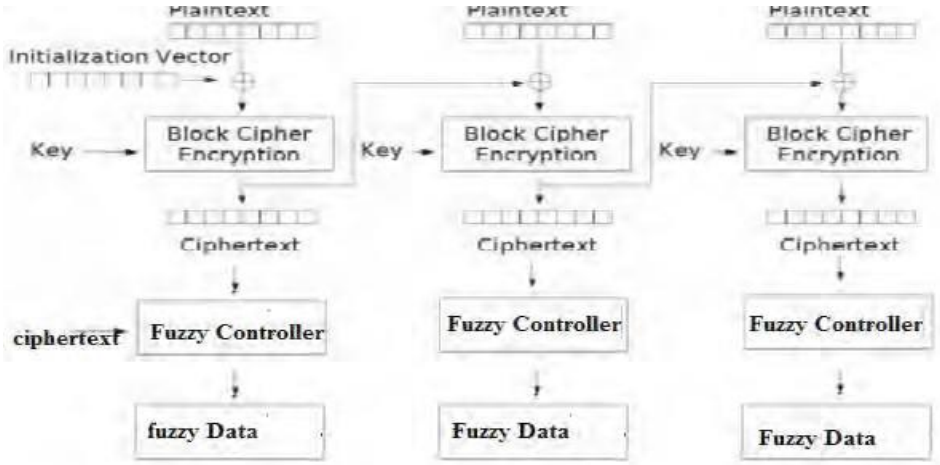


شکل 4 - انحراف فرکانس در کنترلر فازی

نحوه استفاده از آسیب پذیری و رفع آن با استفاده از روش پیشنهادی

ابتدا حمله کننده باید طول درخواست را به گونه ای تغییر دهد که یک کاراکتر (مثلا آخرین کاراکتر کوکی) در آخر یک بلاک قرار بگیرد (طبق فرضها او طول و جای کوکی را می داند) و ضمنا طول درخواست هم به گونه ای باشد که یک بلاک کامل به padding اختصاص داده شود.

هر بلاک رمزنگاری نشده (یا plaintext) از P1 تا P5 نام گذاری شده است. دقت شود که حمله کننده با استفاده از جاواسکریپت می تواند url و body درخواست را تغییر دهد اما دسترسی ای به محتوای cookie ندارد. متن درخواستی برای ارسال به سرور در سمت کاربر (کلاینت) رمز می شود و محتوای رمز شده توسط فازی کنترلر به فازی تبدیل می شود و به سمت سرور ارسال می شود. حمله کننده در بین راه محتوای رمز شده فازی را چیزی مانند شکل5 می بیند :



شکل5

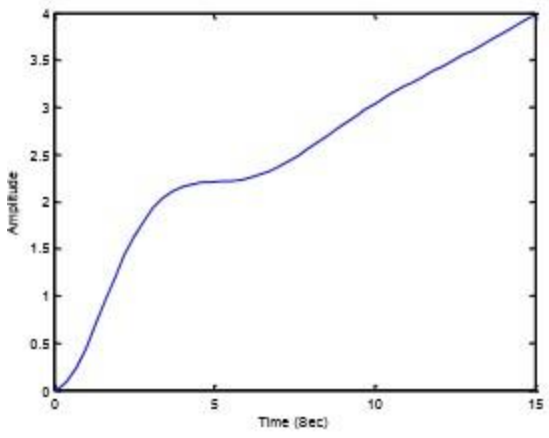
هر بلاک رمزنگاری شده (یا ciphertext) از C1 تا C5 نام گذاری شده است. البته او می داند که بلاک آخر متناظر padding و بلاک C2 هم متناظر با P2 است. به صورت پیش فرض SSL از روشCBC برای chain کردنِ بلاک ها استفاده می کند.

بنابراین حمله کننده می داند که این جملات صادق هستند:

Encrypt (C1⊕ P2) = C2

Encrypt (C4⊕ P5) = C5

و می داند که P5 = 0x0F است، چون padding یک سطر کامل است. در این حال حمله کننده که بین کلاینت و سرور حائل شده است نمی تواند بلاک C5 را (که متناظر با padding است) دستکاری کند و آنرا مساوی C2 قرار دهد. در روش پیشنهادی از دستکاری بلاک ها جلوگیری می شود چرا که بلاک ها توسط فازی کنترلر ، فازی شده اند .ولی در SSLV3 بدون فازی ، هکر می تواند بلاک C5 را دستکاری کرده و آنرا مساوی C2 قرار دهد. شکل ۱ کارایی بالای SSL فازی را نشان می دهد.



شکل 6 – نمودار عملکرد فازی SSL

8. کاربرد نتایج تحقیق

اینترنت، اینترانت، اکسترانت و شبکه های بی سیم همگی فناوری های مهمی هستند که ارتباطات و عملیات تجاری را تسهیل می کنند. اینترنت یک شبکه جهانی از رایانه ها و دستگاه هایی است که به افراد اجازه می دهد به اطلاعات دسترسی داشته باشند و با دیگران در سراسر جهان ارتباط برقرار کنند. اینترانت ها شبکه های خصوصی درون یک سازمان هستند که به کارکنان اجازه دسترسی به اطلاعات و ارتباط با یکدیگر را می دهند. اکسترانت ها شبیه شبکه های داخلی هستند اما به طرف های خارجی مانند تامین کنندگان یا مشتریان اجازه دسترسی به بخش های خاص شبکه را می دهند. شبکه های بی سیم از امواج رادیویی برای اتصال دستگاه ها بدون نیاز به کابل استفاده می کنند.

شرکت ها برای برقراری ارتباط با یکدیگر، به اشتراک گذاری اطلاعات و انجام معاملات به این فناوری ها متکی هستند. با رشد تجارت الکترونیک، که شامل خرید و فروش کالاها و خدمات آنلاین است، اطمینان از ایمن بودن صفحات وب و پرداخت های آنلاین اهمیت فزاینده ای پیدا کرده است. یکی از راه های رسیدن به این هدف استفاده از امنیت SSL(لایه سوکت های امن) است.
SSL پروتکلی است که ارتباط امنی را از طریق اینترنت فراهم می کند. این تضمین می کند که داده های منتقل شده بین مرورگر کاربر و سرور وب رمزگذاری شده است و بنابراین رهگیری برای هکرها دشوار است. SSL خدمات محرمانه بودن، یکپارچگی داده ها و احراز هویت سرور را در اختیار کاربران قرار می دهد. با

افزایش امنیت SSL، صفحات وب نیز ایمن شده و هکرها نمی توانند به اهداف خود دست یابند.
با این حال، SSL یک پروتکل با امنیت بالا است که هکرها اغلب آن را هدف قرار می دهند. یک نمونه از حمله به SSL، POODLE (Padding Oracle On Downgraded Legacy Encryption) است که SSL نسخه 3 (SSLV3) را هدف قرار می دهد. این آسیب پذیری نیاز به افزایش امنیت SSL برای جلوگیری از این نوع حملات را برجسته می کند.
برای رفع این آسیب‌پذیری‌ها، یک پروژه تحقیقاتی برای افزایش امنیت پروتکل SSL با استفاده از منطق فازی انجام شده است. منطق فازی نوعی منطق است که امکان ورودی های غیر دقیق یا نامطمئن را فراهم می کند. هدف این پروژه طراحی یک کنترل کننده فازی است که می تواند داده های رمزگذاری شده را به صورت مرحله ای استخراج کند و به خطر انداختن پروتکل SSL برای مهاجمان دشوارتر شود. نتیجه این پروژه یک پروتکل SSL فازی است که در برابر حملاتی مانند POODLE مقاوم است.

9. خلاصه فصل

ارتباطات و تراکنش های امن در عملیات تجاری مدرن ضروری است. فناوری هایی مانند اینترنت، اینترانت، اکسترانت و شبکه های بی سیم برای این عملیات حیاتی هستند و امنیت SSL برای اطمینان از یکپارچگی و محرمانه بودن تراکنش های آنلاین ضروری است. پروتکل فازی SSL توسعه یافته از طریق این پروژه تحقیقاتی، گام مهمی در جهت ارتقای امنیت ارتباطات و تراکنش های آنلاین است.

منابع

Allam, A., & Dahlan, H. M. (2013). User experience: challenges and opportunities. *Journal of Information Systems Research and Innovation*, *3*(1), 28-36.

Bacudio, A. G., Yuan, X., Chu, B.-T. B., & Jones, M. (2011). An overview of penetration testing. *International Journal of Network Security & Its Applications*, *3*(6), 19.

Clark, J., & Van Oorschot, P. C. (2013). SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. 2013 IEEE Symposium on Security and Privacy,

Freier, A., Karlton, P., & Kocher, P. (2011). *The secure sockets layer (SSL) protocol version 3.0* (2070-1721).

Georgiev, M., Iyengar, S., Jana, S., Anubhai, R., Boneh, D., & Shmatikov, V. (2012). The most dangerous code in the world: validating SSL certificates in non-browser software. Proceedings of the 2012 ACM conference on Computer and communications security,

Jalal, A., & Zeb, M. A. (2008). Security enhancement for e-learning portal. *IJCSNS International Journal of Computer Science and Network Security*, *8*(3).

Kickert, W., & Mamdani, E. (1993). Analysis of a fuzzy logic controller. In *Readings in Fuzzy Sets for Intelligent Systems* (pp. 290-297). Elsevier.

Ma, X.-J., Sun, Z.-Q., & He, Y.-Y. (1998). Analysis and design of fuzzy controller and fuzzy observer. *IEEE Transactions on fuzzy systems*, *6*(1), 41-51.

McGrath, C., & Krackhardt, D. (2003). Network conditions for organizational change. *The Journal of Applied Behavioral Science*, *39*(3), 324-336.

Meyer, C., & Schwenk, J. (2013). Lessons learned from previous SSL/TLS attacks-a brief chronology of attacks and weaknesses. *Cryptology ePrint Archive*.

Möller, B., Duong, T., & Kotowicz, K. (2014). This POODLE bites: exploiting the SSL 3.0 fallback. *Security Advisory*, *21*, 34-58.

Mortazavi, S. H., Yazdani ,M., Jalilzadeh, F., & Avadhani, P. (2014). A novel secure protocol called FSSL using fuzzy controller for Web security. 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC),

Palmer, J. W. (2002). Web site usability, design, and performance metrics. *Information systems research*, *13*(2), 151-167.

Passino, K. M., Yurkovich, S., & Reinfrank, M. (1998). *Fuzzy control* (Vol. 42). Addison-wesley Reading, MA.

Stein, L. D. (1998). Web security. *Addison-Wesley, Massachusetts*, *26*, 1-4.

Ying, H. (2000). *Fuzzy control and modeling: analytical foundations and applications*. Wiley-IEEE Press.

Zadeh, L. A. (1965). Fuzzy sets. *Information and control, 8*(3), 338-353.

Zadeh, L. A. (2023). Fuzzy logic. In *Granular, Fuzzy, and Soft Computing* (pp. 19- .(49Springer.

Zakaria, A., Zamiri, R., Vaziri, P., Saion, E., & Husin, M. S. (2011). World Academy of Science, Engineering and Technology. *International Journal of Physical and Mathematical Sciences, 5*, 928.