علوم و مهندسی کامپیوتر
نشریه علمی پژوهشی انجمن کامپیوتر ایران
مجلد ۷، شماره ۱ و ۳ (الف)، ۱۳۸۸
صفحات ۹-۱۵
مقاله کوتاه

ارائه پیشنهاداتی جهت ارتقای کارآمدی پروتکل SSL

مهدی برنجکوب امینه صالحی نجف‌آبادی

دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

چکیده

سرعت، قابلیت اطمینان و دسترسی آسان به اینترنت باعث گسترش چشمگیر آن در دو دهه‌ی اخیر شده و قابلیت‌های موجود در آن هر روز بیش از پیش مورد توجه مردم قرار می‌گیرد. اینترنت یک سیستم همگانی است و اغلب مسیرهای ارتباطی آن به طور اجتناب‌ناپذیری ناامن هستند و بنابراین لازم است تدابیری برای برقراری امنیت در آن اندیشیده شود. برای پاسخگویی به این نیاز، پروتکل SSL به صورت یک لایه‌ی مجزا به معماری اینترنت اضافه شده و بین لایه‌های کاربرد و انتقال قرار می‌گیرد. نظر به گستردگی استفاده از پروتکل SSL، تا کنون نسخه‌های متعددی از SSL منتشر شده و پیاده‌سازی‌های مختلفی از آن صورت گرفته است و تلاش برای ارتقای کارایی آن ادامه دارد. یکی از پارامترهای مهم سنجش کارایی یک پروتکل، سرعت برقراری ارتباط امن در آن است. کاهش ترافیک شبکه و همچنین تعداد مراحل تبادل پیام، به ویژه در محیط‌هایی همچون شبکه‌های بی‌سیم که تأخیر بالا دارند، اهمیت زیادی دارد. در این مقاله موضوع تسریع پروتکل دستداد SSL مورد بررسی قرار گرفته و در این راستا پیشنهاداتی ارائه شده است. اولین پیشنهاد، یک دستداد سه مرحله‌ای است که سرعت انجام مذاکره برای یک جلسه جدید را افزایش می‌دهد. پیشنهاد بعدی روشی است برای تسریع تغییر حالت جاری اتصال که تنها نیاز به دو مرحله تبادل پیام دارد. سرانجام یک راه حل برای یکپارچه‌سازی این راهکارها در قالب یک پروتکل جامع ارائه شده که امکان افزایش انعطاف‌پذیری SSL را فراهم می‌آورد.

کلمات کلیدی: رمزنگاری، احراز اصالت، پروتکل برقراری کلید، گواهینامه، دستداد[1]، SSL[2].

۱- مقدمه

سرعت، قابلیت اطمینان و دسترسی آسان به اینترنت باعث گسترش چشمگیر آن در سال‌های اخیر شده و پتانسیل‌های موجود در آن هر روز بیش از پیش مورد توجه مردم قرار می‌گیرد. در هر حال، اینترنت یک سیستم همگانی است و طبیعی است که نمی‌توان کنترلی روی افراد و آزادی‌های آنان داشت. راه‌های بسیاری برای عملکرد مخرب در اینترنت وجود دارد و به همین علت تدابیر مختلفی برای برقراری امنیت در اینترنت اندیشیده شده‌اند. یکی از پروتکل‌های امنیتی متداول در اینترنت، پروتکل SSL است. نسخه‌های متعددی از این پروتکل منتشر شده که هر یک نسبت به نسخه قبلی خود دارای برتری هستند [۱، ۲، ۳، ۴].

هدف از طراحی پروتکل SSL، برقراری اتصال امن بین کارفرما و کارگزاری است که در یک محیط ناامن ارتباط برقرار کرده‌اند. محیط‌هایی که از SSL برای ایجاد امنیت بهره می‌گیرند، شرایط یکسانی ندارند و بدیهی است که تنها اشتراک آنها در ناامن بودن نهفته است. این عدم امنیت ناشی از تهدیدات مختلفی می‌تواند باشد و تفاوت بین محیط‌ها در همین تفاوت بین تهدیدها است. پیکربندی اصلی SSL با دقت بالایی طراحی شده است و ضعف‌های باقیمانده‌ای که از آن گزارش شده‌اند، هیچ یک موجب شکستن SSL نیستند.

تلاش زیادی صورت گرفته تا پروتکل SSL در محیط‌های متنوع، انعطاف‌پذیری و کارآمدی لازم را داشته باشد [۵]. مقاله حاضر نیز در همین چارچوب به دنبال آن است که با ایجاد تسریع بیشتر در مرحله آغازین مذاکره SSL (پروتکل دستداد) بر کارآمدی SSL بیفزاید. بدیهی است که در صورت مقبولیت پیشنهادات ارائه‌شده در جامعه علمی و حرفه‌ای امنیت اطلاعات، زمینه لازم برای پذیرش آنها به عنوان گسترش SSL به وجود خواهد آمد.

در این مقاله پس از اتمام مقدمه، ابتدا مروری بر پروتکل دستداد استاندارد SSL می‌شود. سپس، یک دستداد سه مرحله‌ای پیشنهاد می‌شود که به طرفین ارتباط امکان می‌دهد جلسه امن را با سرعت بیشتری برقرار کنند. در ادامه برای

تغییر حالت جاری اتصال[۳]، روشی پیشنهاد شده که موجب تسریع عملکرد پروتکل می‌گردد. در انتهای مقاله، پروتکل جامعی ارائه شده که بدون تغییر چارچوب استاندارد SSL، امکان استفاده از قابلیت‌های مختلف را برای طرفین ارتباط فراهم می‌کند.

۲- مروری بر دستداد استاندارد SSL

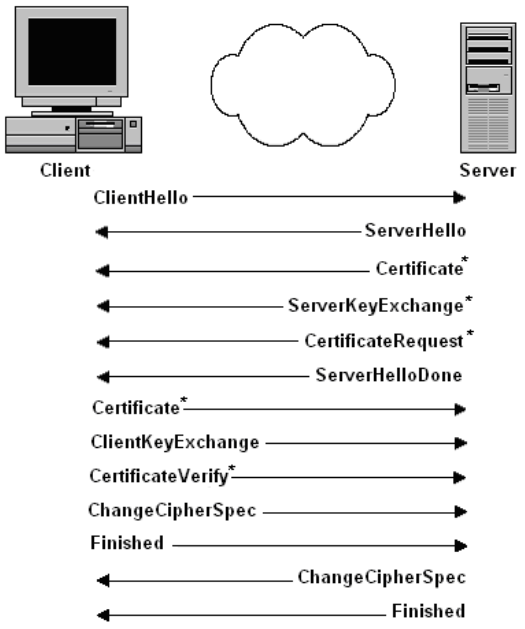
پروتکل دستداد به طرفین ارتباط اجازه می‌دهد که یکدیگر را احراز اصالت کنند و قبل از ارسال یا دریافت اطلاعات کاربردی، در مورد الگوریتم‌ها و کلیدها مذاکره کنند. بطور خلاصه می‌توان گفت که یک دستداد کامل مراحل زیر را شامل می‌شود:

- مبادله پیام‌های Hello به منظور توافق روی الگوریتم‌ها و مبادله اعداد تصادفی و همچنین تعیین نوع جلسه (مذاکره جلسه جدید یا ازسرگیری جلسه قبلی).
- تبادل پارامترهای رمزنگاری لازم برای توافق طرفین روی یک pre-master-secret .
- مبادله گواهینامه ها و اطلاعات رمزنگاری به منظور احراز اصالت کارگزار و کارفرما.
- تولید master-secret به کمک pre-master-secret و اعداد تصادفی مبادله شده.
- فراهم کردن پارامترهای امنیتی حالت اتصال برای لایه ثبت[۴].
- مبادله پیام‌های finished که به کارگزار و کارفرما امکان می‌دهد که از یکسان بودن پارامترها و محاسبات یکدیگر و همچنین عدم دخالت دشمن در دستداد مطمئن شوند.

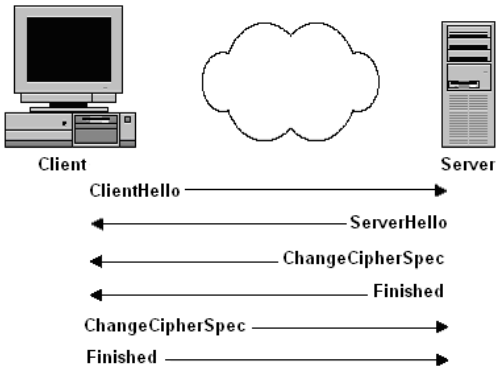
روند تبادل پیام‌ها در یک دستداد کامل مطابق شکل (۱) است. در این شکل پیام‌های ستاره‌دار پیام‌هایی هستند که ارسال آنها به خواست طرفین بستگی دارد و اجباری نیستند. برای آشنایی با جزئیات بیشتر پروتکل دستداد به [۳] رجوع شود. پروتکل SSL قابلیت از سرگیری جلسه را دارد. یعنی کارفرما و کارگزار می‌توانند جلسه‌ای را که قبلاً مذاکره کرده‌اند، در اتصالات دیگری هم استفاده کنند یا حتی در اتصال جاری نسبت به تازه کردن پارامترهای رمز اقدام کنند. این کار برای کاهش محاسبات و همچنین صرفه جویی در زمان است و چون پارامترهای امنیتی تازه‌ای تولید می‌شوند، به امنیت لطمه‌ای نمی‌خورد. روند تبادل پیام‌ها هنگام از سرگیری جلسه در شکل (۲) نشان داده شده است. شناسه جلسه[۵] موجود در پیام ClientHello به کارگزار می‌گوید که کدام جلسه را باید از سر بگیرد. هنگام ازسرگیری جلسه نیازی به تبادل گواهینامه و pre-master-secret نیست و طرفین باید بوسیله master-secret ذخیره شده و اعداد تصادفی جدید، پارامترهای امنیتی را از نو محاسبه و آنها را فعال کنند. مشابه قبل، پیام Finished برای اطمینان از امنیت جلسه و درستی پارامترها مبادله می‌شود و دستداد به اتمام می‌رسد.

۳- سرعت بخشیدن به آغاز مذاکره SSL

یکی از مباحث مورد توجه در پروتکل‌های امنیتی، سرعت برقراری ارتباط امن در آنها می‌باشد. SSL به منظور سرعت بخشیدن به روند مذاکره یک اتصال امن، امکان ازسرگیری جلسه‌ای را که قبلاً مذاکره شده فراهم کرده است. چنین امکانی موجب کاهش پیام‌های مورد مبادله و همچنین حذف عملیات رمز کلید عمومی می‌گردد که تأثیر بسزایی بر روی سرعت مذاکره دارد. اما مسئله در اینجاست که در همه این اتصالات از یک master-secret استفاده می‌شود. به همین دلیل، امنیت این اتصالات بستگی به امنیت کلید master-secret دارد. اگر مقدار این کلید به طریقی کشف شود، تمامی اتصالاتی که با استفاده از آن امن می‌شوند، مورد تهدید قرار خواهند گرفت. مثلاً اگر دشمن بتواند به حافظه نگهداری جلسات در طرف کارفرما، دست پیدا کند، مقدار master-secret را یافته و در اتصالات بعدی دخالت می‌کند. بنابراین اگر بتوان سرعت برقراری یک جلسه تازه را افزایش داد، از لحاظ امنیتی ارزش بیشتری دارد.



شکل ۱- روند تبادل پیام‌ها در یک دستدادکامل



شکل ۲- روند تبادل پیام‌ها هنگام از سرگیری نشست

در ابتدا باید عوامل کند شدن سرعت مذاکره را شناسایی کرد. اولین و مهمترین عامل، چهار مرحله‌ای بودن پروتکل دستداد است. دو دلیل اساسی برای چهار مرحله‌ای شدن پروتکل دستداد می‌توان ذکر کرد. علت اول این است که کارفرما پس از ارسال پیام ClientHello قادر به ارسال پیام دیگری نیست. کارفرما باید منتظر پاسخ کارگزار بماند، چون نمی‌داند کدام یک از موارد پیشنهادی‌اش برای استفاده در مذاکره، انتخاب می‌شوند. علت دیگر چهار مرحله‌ای شدن دستداد، فرآیند تبادل کلید است. برای توافق روی یک کلید محرمانه مشترک، طرفین باید چند پیام تبادل کرده و همچنین عملیات سنگین نمارسانی را انجام دهند. زمانی که صرف عملیات کلید عمومی می‌شود، دومین عامل کاهش سرعت مذاکره است؛ اما در بسیاری از موارد، این زمان قابل قیاس با زمانی که به خاطر چهار مرحله‌ای بودن دستداد از دست می‌رود، نیست. از طرف دیگر امکانات و شرایط محیط‌ها مختلف است و به همین علت، محیط‌های متنوع راهکارهای متنوعی را می‌طلبند.

اگر کارفرما و کارگزار قبل از انجام مذاکره برای برقراری جلسه امن، کلید مشترکی را به طور محرمانه باهم توافق کرده باشند می‌توانند مذاکره را سریعتر انجام دهند. در این راستا، IETF[۶] نسخه استاندارد استفاده از PSK[۷] [۶] را منتشر کرده است. در الگوریتم‌های تبادل کلیدی که این نسخه ارائه کرده است نیاز به تبادل گواهینامه نیست. بعد از توافق طرفین بر روی استفاده از اینگونه تبادل کلید (با تبادل پیام‌های Hello)، کارفرما شناسه PSK را برای کارگزار ارسال می‌کند. برای سرعت بخشیدن به مذاکره، کارفرما می‌تواند بلافاصله پس از پیام ClientHello (که در آن الگوریتم تبادل کلید PSK را پیشنهاد کرده است)، شناسه PSK مربوطه را در پیام ClientKeyExchange ارسال کند. حتی می‌توان پیام ClientHello را بسط داد و عبارتی به آن اضافه کرد که بیانگر شناسه PSK باشد و کارفرما مجبور به ارسال پیام دیگری نباشد. کارگزار پس از دریافت پیشنهاد کارفرما تصمیم خواهد گرفت که چنین جلسه‌ای برقرار بشود یا مسیر آن به سمت یک دستداد معمولی تغییر یابد. در هرحال کارفرما محاسبه‌ای انجام نداده که وقتش را تلف کرده باشد.

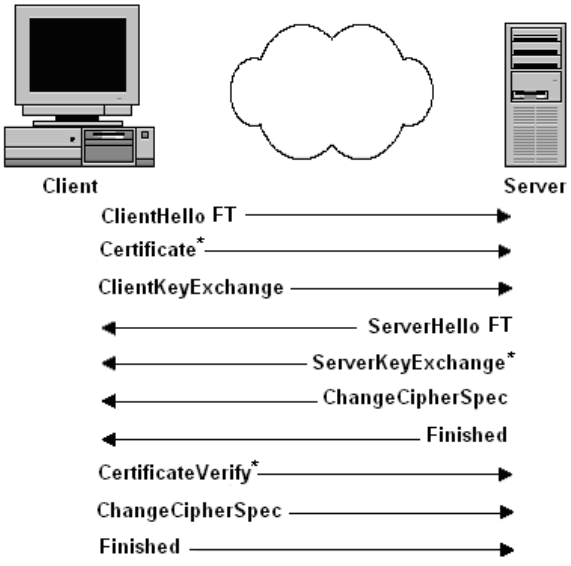
در این مقاله، تلاش بر این است که بدون تغییر چارچوب اصلی SSL استاندارد، راهکاری برای تسریع مذاکره ارائه شود. به همین جهت فرض شده که فرآیند تبادل کلید باید انجام شود و احراز اصالت باید مبتنی بر گواهینامه باشد، (به این ترتیب استفاده از PSK برای حذف عملیات کلید عمومی راهکار اساسی به شمار نمی‌آید). در ادامه ابتدا روشی که توسط IETF ارائه شده، شرح داده می‌شود و پس از آن، روش جایگزینی برای سرعت بخشیدن به مذاکره پیشنهاد می‌شود.

۳-۱- مذاکره به روش سریع

اگرفرض شود که کارفرما بخواهد همان ابتدا پس از پیام ClientHello، پیام ClientKeyExchange را ارسال کند؛ او در درجه اول باید روش تبادل کلید را بداند و همچنین باید گواهینامه کارگزار و در صورت لزوم گروه دیفی‌هلمن او را داشته باشد. کارفرما باید بداند که آیا نیاز به احراز اصالت او هست یانه و اگر هست، چگونه گواهینامه‌ای باید ارسال کند. اگر کارفرما این اطلاعات را داشته باشد می‌تواند مذاکره را با سه مرحله تبادل پیام به انجام برساند. در همین راستا IETF نسخه پیش‌نویس سریع[۸] [۷] را در اواخر سال ۲۰۰۱ میلادی منتشر نموده است که به طرفین امکان می‌دهد در صورت تمایل، جلسه امن را سریع‌تر برقرار کنند.

در ابتدای امر، کارفرما باید در یک دستداد معمولی SSL (چهار مرحله‌ای)، درخواست خود را به کارگزار اعلام کند. بنابراین در پیام ClientHello، ضمیمه fasttrack-capable را ارسال می‌کند؛ مبنی بر اینکه وی تمایل و توانایی برای انجام مذاکره به روش سریع را دارد (لازم به ذکر است که IETF برای افزایش قابلیت پروتکل SSL، امکان گسترش پیام‌ها را فراهم کرده است و شرایط استاندارد تعریف بسطهای جدید را در [۸] منتشر نموده است). کارگزار هم در صورتی که موافق باشد، عبارت مشابه را در پیام ServerHello برای کارفرما ارسال می‌کند. بدین ترتیب هر دو طرف از توانایی و تمایل یکدیگر برای انجام مذاکره سریع در جلسات بعدی مطمئن می‌شوند؛ دستداد انجام شده را دستداد تعیین‌کننده[۹] می‌نامند. در نهایت، کارفرما باید پارامترهای مورد نیاز را نگهداری کند تا در دستداد آینده مورد استفاده قرار دهد. این پارامترها را اصطلاحاً پارامترهای تعیین‌کننده[۱۰] مذاکره سریع می‌نامند.

شکل (۳) روند تبادل پیام‌ها را در یک مذاکره سریع برای برقراری یک جلسه امن تازه نشان می‌دهد. کارفرما دستداد به روش سریع را با ارسال پیام ClientHelloFT برای کارگزار آغاز می‌کند. این پیام بسط‌یافته پیام ClientHello است و تفاوت زیادی با آن ندارد. این پیام علاوه بر مجموعه پارامترهای رمز و همچنین روش‌های فشرده‌سازی شامل دو ضمیمه fasttrack-capable و fasttrack-hash نیز می‌باشد. ضمیمه اول مشابه قبل، تمایل کارفرما را برای انجام مذاکره سریع نشان می‌دهد و ضمیمه دوم مربوط به حاصل درهم پارامترهایی است که کارفرما از جلسه قبل نگهداری کرده تا در این مذاکره سریع از آنها استفاده کند. بدین ترتیب دو طرف می‌توانند مطمئن باشند که پارامترهای مشابهی را به کار می‌برند. پیام ClientCertificate مشابه پیامی است که در یک دستداد معمولی SSL برای گواهینامه کارفرما استفاده می‌شود. این پیام فقط و فقط به این شرط ارسال می‌شود که در دستداد تعیین‌کننده، کارگزار تقاضای احراز اصالت کارفرما را کرده باشد. به این ترتیب کارفرما دو مؤلفه انواع گواهینامه و مراکز صدور مورد قبول کارگزار را در لیست پارامترهای تعیین‌کننده دارد و گواهینامه‌ای متناسب با این شرایط برای کارگزار ارسال می‌نماید. پیام ClientKeyExchange همان ساختار استاندارد را دارد و با توجه به پارامترهای تعیین‌کننده، ایجاد و ارسال می‌شود.



شکل ۳- روند تبادل پیام‌ها در مذاکره به روش سریع

اگر کارگزار با مذاکره سریع موافق باشد، باید با استفاده از محتوای پیام ClientHelloFt و همچنین پیکربندی خود، پارامترهای تعیین‌کننده اتصال را پیدا کند و تابع درهم SHA-1 را روی این مقادیر، اعمال نماید. اگر حاصل درهم بدست آمده، مشابه حاصل درهم ارسالی کارفرما بود، کارگزار با ارسال پیام ServerHelloFT (که شامل عبارت fasttrack-capable می‌باشد) به کارفرما اعلام می‌کند که مذاکره سریع را پذیرفته است. مشابه حالت استاندارد مذاکره ، ارسال پیام ServerKeyExchange با توجه به الگوریتم تبادل کلید انجام می‌شود. چون هر دو طرف پارامترهای لازم برای انجام محاسبات را دارند، کارگزار می‌تواند پیام ChangeCipherSpec و به دنبال آن پیام Finished را برای کارفرما ارسال کند. اگر کارفرما گواهینامه خود را فرستاده باشد، در این مرحله باید پیام CertificateVerify را ارسال کند. علت ارسال این پیام در مرحله سوم تبادل پیام، جلوگیری از حمله تکرار است؛ چون تازه بودن این پیام، بستگی به تازه بودن مقادیر تصادفی کارفرما و کارگزار دارد. سرانجام کارفرما پیام ChangeCipherSpec و به دنبال آن پیام Finished را برای کارگزار ارسال کرده و سپس مبادله اطلاعات کاربردی را آغاز می‌کند.

تحلیل کامل امنیت و کارایی این مذاکره در [۹] انجام شده است. با توجه به این تحلیل می‌توان نتیجه گرفت که امنیت مذاکره سریع کمتر از یک مذاکره معمولی نیست و با انجام آن تعداد بایت‌های مبادله شده در دستداد تا حد زیادی کاهش می‌یابد. اگرچه این روش ساده‌ترین راهکاری است که برای تسریع مذاکره

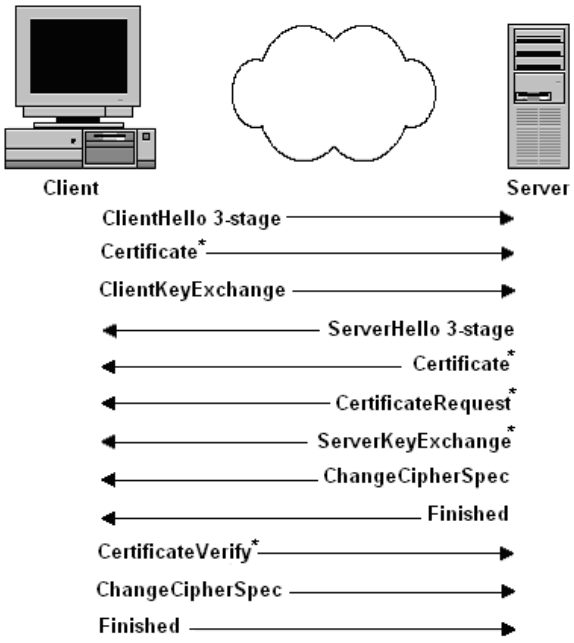
SSL به ذهن می‌رسد، اما اشکالاتی به آن وارد است: اول اینکه کارفرما باید پارامترهای تعیین‌کننده را نگهداری کند و حجم این اطلاعات مقدار مشخصی ندارد. از طرفی کارگزار هم باید قادر به محاسبه حاصل درهم پارامترهای تعیین‌کننده باشد. به همین منظور یا باید برخی از این پارامترها را به همراه شناسه جلسه و همینطور کلید master-secret نگهداری کند و یا در بازه‌های زمانی نه چندان کوتاهی باید پارامترهای تعیین‌کننده را ثابت نگه دارد. اشکال دوم این روش، ثابت ماندن مجموعه پارامترهای رمز در جلسات متوالی است. مجموعه پارامترهای رمز یکی از پارامترهای تعیین‌کننده است که کارفرما در جلسات سریعی که مذاکره می‌کند، قادر به تغییر آن نیست و هرگاه که تمایل به تغییر پارامترها داشت، باید مجدداً یک دستداد تعیین‌کننده با کارگزار مورد نظرش مذاکره کند و پارامترهای تعیین‌کننده جدیدی را نگهداری کند. آخرین نکته‌ای که باید ذکر شود، این است که مذاکره سریع خطر حمله DoS[11] را هم افزایش می‌دهد. قابل توجه اینکه، IETF نسخه پیش‌نویس مربوط به این روش را تجدید انتشار نکرده است.

۳-۲- ارائه یک دستداد سه مرحله‌ای برای برقراری جلسه

همانطور که گفته شد، یکی از عوامل کندسازی مذاکره SSL، تعداد پیام‌هایی است که طرفین برای رسیدن به مقدار pre-master-secret مبادله می‌کنند. به طوریکه همیشه کارگزار، نیمه اول فرآیند تبادل کلید را انجام می‌دهد و کارفرما تکمیل‌کننده این فرآیند است. حال اگر این روند برعکس شود؛ یعنی کارگزار تکمیل‌کننده فرآیند تبادل کلید باشد، سرعت مذاکره افزایش می‌یابد. در این حالت، روند تبادل پیام‌ها مطابق شکل (۴) تغییر خواهد کرد.

کارفرما طبق معمول، پیشنهادات خود را به همراه عبارت 3-stage مبنی بر تمایل به مذاکره به روش سه مرحله‌ای در پیام ClientHello ارسال می‌کند. اگر کارفرما گواهینامه معتبر داشته باشد، آن را پس از پیام ClientHello می‌فرستد و در هر حال، پس از آن باید پیام ClientKeyExchange را که شامل پارامترهای دیفی‌هلمن موقت کارفرما می‌باشد، ارسال کند. اگر کارگزار با مذاکره به روش سه مرحله‌ای موافق باشد، با توجه به قابلیت‌های کارفرما تصمیم‌گیری نموده و نتیجه را به همراه عبارت 3-stage در پیام ServerHello ارسال می‌کند وگرنه پیام‌های ارسالی کارفرما را نادیده گرفته و مذاکره را به حالت عادی انجام می‌دهد. اگر کارفرما گواهینامه با کلید عمومی RSA داشته و ارسال کرده باشد، کارگزار می‌تواند الگوریتم تبادل کلید RSA را انتخاب کند. در غیر اینصورت، تبادل کلید باید با الگوریتم دیفی‌هلمن (موقت یا ثابت) انجام شود. نکته دیگر این است که اگر برای کارگزار، احراز اصالت کارفرما مهم باشد ولی کارفرما گواهینامه قابل قبولی ارسال نکرده باشد یا اصلاً گواهینامه نفرستاده باشد، کارگزار باید پیام خطا ارسال کند.

کارگزار پس از پیام ServerHello، باید گواهینامه‌اش را ارسال کند، مگر اینکه تبادل کلید گمنام[12] توافق شده باشد. اگر کارگزار گواهینامه قابل قبولی از کارفرما دریافت کرده باشد ولی آن را در فرآیند تبادل کلید استفاده نکرده باشد، می‌تواند از کارفرما بخواهد که با محاسبه پیام CertificateVerify فرآیند احراز اصالتش را کامل کند. به همین منظور، باید پیام CertificateRequest را خالی از محتوا ارسال کند. سپس باید پیام ServerKeyExchange را بفرستد که تکمیل‌کننده فرآیند تبادل کلید است. اگر تبادل کلید RSA توافق شده باشد، کارگزار باید مقدار تصادفی pre-master-secret را با کلید عمومی RSA کارفرما رمز کرده و سپس آن را با کلید گواهینامه خود امضاء کرده و ارسال کند. اگر تبادل کلید دیفی‌هلمن توافق شده باشد، کارگزار باید پارامترهای دیفی‌هلمن موقت خود را امضاء کرده و در پیام ServerKeyExchange ارسال کند. تنها حالتی که نیاز به ارسال این پیام ندارد، زمانی است که تبادل کلید دیفی‌هلمن توافق شده باشد و کارگزار کلید عمومی دیفی‌هلمن ثابت مطابق با گروه دیفی‌هلمن پیشنهادی کارفرما داشته باشد.



شکل ۴- روند تبادل پیام‌ها در دستداد کامل به روش سه مرحله‌ای

بدین ترتیب در مرحله دوم ارسال پیام، فرآیند تبادل کلید تکمیل شده و هر دو طرف می‌توانند کلید master-secret و به دنبال آن پارامترها و کلیدهای جلسه را محاسبه کنند. کارگزار پس از انجام محاسبات، پیام ChangeCipherSpec و به دنبال آن پیام Finished را برای کارفرما می‌فرستد. کارفرما نیز پس از بررسی صحت پیام Finished دریافت شده از سوی کارگزار، پیام‌های CertificateVerify (در صورت لزوم) و ChangeCipherSpec و Finished را برای تکمیل دستداد می‌فرستد. برای جلوگیری از حمله تکرار، ارسال پیام CertificateVerify در این مرحله قرار داده شده است.

اگرچه این مذاکره مانند مذاکره به روش سریع سه مرحله‌ای است، اما در روش پیشنهادی، لازم نیست کارفرما و کارگزار پارامتری را نگهداری کنند و هر بار می‌توانند از مجموعه پارامترهای رمز جدیدی استفاده کنند. میزان محاسبات حاصل از این مذاکره سه مرحله‌ای، بستگی به الگوریتم تبادل کلید توافق شده دارد. اگر تبادل کلید RSA توافق شده باشد، کارگزار باید اعمال رمزگذاری و امضاء را انجام دهد که نسبت به مذاکره استاندارد، عمل رمزگذاری اضافه شده است. از آنجا که مقدار نمای کلید عمومی RSA غالباً برابر با ۳ انتخاب می‌شود، این محاسبه هزینه زیادی نخواهد داشت. اگر تبادل کلید دیفی‌هلمن موقت توافق شده باشد، محاسبات این روش نسبت به مذاکره استاندارد تفاوتی نخواهد کرد. در جدول (۱) مقایسه‌ای بین سه دستداد استاندارد، سریع و دستداد پیشنهادی انجام شده است.

چنانچه در این جدول مشاهده می‌شود، دستداد سه مرحله‌ای پیشنهادی نسبت به دستداد سریع دو مزیت اساسی دارد که انعطاف‌پذیری بیشتر و حافظه مورد نیاز کمتر می‌باشند. توضیحات آمده در معرفی این دو پروتکل، شواهد روشن و کافی برای اثبات صحت این مدعا در اختیار می‌گذارند.دستداد پیشنهادی در برخی قابلیت‌ها مشابه دستداد استاندارد است که در جدول مشخص شده‌اند. کاهش مراحل تبادل پیام در دستداد پیشنهادی، موجب افزایش سرعت در روند

برقراری ارتباط می‌گردد. توجه شود که دستدادهای سریع و پیشنهادی دقیقاً به اندازه زمان یک تبادل کامل[۱۳] (زمان رفت و برگشت یک پیام بین طرفین) نسبت به دستداد استاندارد سریع‌تر می‌باشند. این قابلیت در محیط‌هایی همچون شبکه‌های بی‌سیم که تأخیر بالایی دارند (مانند شبکه‌های ماهواره‌ای)، اهمیت شایانی دارد.

در مورد خطر حمله DoS، این روش و روش سریع ارائه شده در بخش قبل به طور یکسان آسیب‌پذیر هستند. از طرف دیگر، یک دستداد معمولی SSL هم مورد تهدید حمله DoS هست و در استانداردهای منتشر شده، راهکاری برای مقابله با این حمله اتخاذ نشده است. در هر حال اگر کارگزار نگران حمله DoS نباشد، استفاده از مذاکره سه مرحله‌ای ارجحیت دارد. در حالت کلی باید گفت که محیط همیشه هم پر مخاطره نیست و در موارد زیادی، محیط برقراری اتصال برای چنین مذاکراتی مناسب است.

۴- سرعت بخشیدن به تغییر حالت جاری اتصال در قالب یک جلسه یکپارچه

در ارتباط کارفرما و کارگزار، مواقعی هست که احراز اصالت پیام‌ها کافی است و یا حتی نیاز به هیچ امنیتی احساس نمی‌شود. اگر در طول یک ارتباط امن برقرار شده با SSL ، طرفین بتوانند پارامترهای امنیتی حالت اتصال را به سرعت تغییر دهند، سرعت تبادل اطلاعات افزایش می‌یابد. استفاده از طرح از سرگیری جلسه تنها در حالتی مناسب است که طرفین قصد تغییر الگوریتم‌ها را نداشته باشند. ولی اگر طرفین، تصمیم بگیرند که به شکل دیگری تبادل پیام‌ها را ادامه دهند باید جلسه را به پایان رسانده و جلسه جدیدی را با پارامترهای دلخواهشان ایجاد کنند. مسلم است که انجام یک مذاکره تازه، نیاز به زمان زیادی دارد و باید به دنبال راهکار بهتری بود.

این مسئله از دو جنبه قابل بررسی است. جنبه اول مربوط به حالاتی است که نیاز به محاسبات جدید ولی با سرعت بالا دارند. این حالت کاملاً مانند طرح از سرگیری جلسه است، تنها باید به طرفین امکان داده شود که مجموعه پارامترهای رمز را تغییر دهند و با همان master-secret قبلی، پارامترهای جدید را تولید کنند.

جنبه دیگر مسئله، مربوط به حالاتی است که طرفین قصد محاسبه پارامترهای جدید را ندارند. مثلاً ممکن است یکی از طرفین بخواهد که از کلیدهای MAC محاسبه شده، برای احراز اصالت پیام‌ها استفاده کند ولی رمزگذاری را انجام ندهد. در این حالت، کارفرما باید پیام ClientHello را ارسال کند. چون کارفرما تمایل داردکه از همان پارامترها استفاده شود، پیشنهاد می‌شود که عبارت pending را همراه با بقیه گزینه‌ها ارسال کند. سپس باید قسمتی از حالت جاری اتصال را که مربوط به MAC است به حالت معطل ببرد و بعد از ارسال پیام ChangeCipherSpec حالت معطل نوشتن خود را جاری کند. اکنون می‌تواند پیام Finished را محاسبه نموده و بفرستد. اگر کارگزار موافقت کند، مجموعه پارامترهای رمز پیشنهادی وی را انتخاب کرده و همراه با عبارت pending در پیام ServerHello می‌فرستد. سپس حالات معطل را مقداردهی نموده و حالت معطل خواندن را جاری می‌کند. پس از ارسال پیام ChangeCipherSpec، حالت معطل نوشتن را نیز جاری کرده و پیام Finished را ارسال می‌کند.

مثال دیگر این است که طرفین تصمیم بگیرند جلسه به حالت معطل برود و تبادل اطلاعات را تا مدتی به صورت کاملاً آشکار ادامه دهند. کارفرما باید این تقاضا را با ارسال پیام pending اعلام کند و سپس اتصال را خاتمه دهد و پیام مشابهی از کارگزار دریافت نماید. پس از آن، طرفین باید همه پارامترهای حالت اتصال و همچنین مقدار شماره سریال را نگه دارند تا در اتصال بعدی مورد استفاده قرار دهند. در اتصال بعدی کافیست که کارفرما همراه با پیام ClientHello ضمیمه pending و شناسه جلسه مربوطه را ارسال کند. پس از آن می‌تواند حالت معطل اتصال را با پارامترهای قبلی مقداردهی کرده و پیام ChangeCipherSpec را ارسال نماید. پس از آن، حالت نوشتن خود را فعال کرده و پیام Finished را می‌فرستد. اگر کارگزار موافق باشد، پیام ServerHello را همراه ضمیمه pending و شناسه جلسه مشابه ارسال می‌کند. به دنبال آن، وی حالات معطل خود را مقداردهی نموده و مشابه مثال قبل، پیام‌های ChangeCipherSpec و Finished را می‌فرستد. هر دو طرف باید اطلاعات خود را بر اساس شماره سریالی که از قبل نگه داشته‌اند مبادله کنند تا احتمال انجام موفق حمله تکرار منتفی شود.

نکته‌ای که توجه به آن ضروری است، عمر یک جلسه امن است. مدت زمان اعتباری که برای شناسه جلسه در نظر گرفته می‌شود محدود است و به انتخاب کارگزار بستگی دارد. در نسخه استاندارد TLS1.0 مدت ۲۴ ساعت پیشنهاد شده است [۳]. اما برخی کارگزارها مدت زمان بسیار کوتاهتری (مثلاً ۵ دقیقه) را برای نگهداری یک جلسه انتخاب می‌کنند. بدیهی است که در این شرایط، ممکن است استفاده از این روش برای تغییر حالت جاری اتصال مفید نباشد.

۵- ارائه یک پروتکل جامع برای استفاده از روش‌های مختلف

هدف از طراحی پروتکل SSL، برقراری اتصال امن بین کارفرما و کارگزاری است که در یک محیط ناامن ارتباط برقرار کرده‌اند. محیط‌هایی که برای برقراری امنیت از SSL استفاده می‌کنند، شرایط یکسانی ندارند و بدیهی است که تنها اشتراک آنها در ناامن بودن است. پیکربندی اصلی SSL با دقت بالایی طراحی شده است و نکات امنیتی اساسی در آن لحاظ شده‌اند. اما پروتکل SSL در محیط‌های متنوع انعطاف‌پذیری لازم را ندارد.

جدول ۱- مقایسه دستداد سریع و دستداد پیشنهادی با دستداد استاندارد

	تعداد مراحل تبادل پیام	انعطاف‌پذیری	حافظه نگهداری جلسات	محاسبات فرآیند تبادل کلید		قابلیت استفاده از راهکارهای مقابله با حمله DoS
				دیفی‌هلمن موقت	تبادل کلید RSA	
دستداد سریع	بهتر (سه مرحله)	بدتر	بدتر	یکسان	یکسان	بدتر
دستداد پیشنهادی	بهتر (سه مرحله)	یکسان	یکسان	یکسان	تقریباً یکسان	بدتر

به طور مثال با وجود راهکارهایی که برای مقابله با حمله DoS ارائه شده [۱۰]، اما طراحان SSL لزومی ندانسته‌اند که قابلیت مقابله با این حمله در پروتکل SSL گنجانده شود. در ادامه یک پروتکل جامع و یکپارچه شرح داده خواهد شد که با حفظ چارچوب اصلی SSL به کاربردها امکان بکارگیری هریک از مذاکرات مطرح‌شده در قسمت‌های پیشین مقاله و همچنین امکان استفاده از معمای کارفرما[۱۴] [۱۱] برای مقابله با حمله DoS را می‌دهد.

قبل از شرح پروتکل جامع، لازم است توجه شود که روند تبادل پیام‌ها بستگی به نوع مذاکره‌ای دارد که طرفین توافق می‌کنند. بنابراین اگر مذاکره استاندارد توافق شده باشد، روند تبادل پیام‌ها از شکل (۱) یا (۲) تبعیت می‌کند و اگر مذاکره سه مرحله‌ای توافق شده باشد، این روند مطابق شکل (۴) خواهد بود. در ادامه، هریک از پیام‌های اصلاح‌شده دستداد شرح داده خواهند شد.

HelloRequest: این پیام به کارگزار امکان می‌دهد که در صورت طولانی شدن جلسه، از کارفرما تقاضای تجدید دستداد و شروع یک جلسه جدید را نماید. این پیام، فاقد محتواست.

ClientHello: کارفرما هر زمان که تصمیم گرفت اتصال جدیدی را آغاز کند، این پیام را برای کارگزار ارسال می‌کند. محتوای پیام، مانند حالت استاندارد است و تنها مؤلفه‌ای به عنوان ضمیمه به انتهای آن اضافه می‌شود. این مؤلفه یک بایت طول دارد و هر بیت آن، مشخص‌کننده قابلیتی از کارفرما است. استفاده از این مکانیسم، روش ساده‌تری را برای بسط SSL فراهم می‌کند و به طرفین امکان می‌دهد که تنها با یک بایت قابلیت‌های خود را اعلام کنند.

اگر کم ارزشترین بیت ضمیمه برابر ۱ باشد، نشان‌دهنده این است که کارفرما تمایل و توانایی برای مذاکره سه مرحله‌ای را دارد. دومین بیت کم ارزش به قابلیت کارفرما برای حل معما اختصاص داده شده که اگر ۱ باشد، نشان‌دهنده این است که کارفرما توانایی حل معما را دارد. سومین بیت کم ارزش مربوط به حالت معطل است و تنها در طول یک جلسه قابل استفاده است. اگر کارفرما تمایل به معطل نگه داشتن برخی پارامترهای حالت اتصال داشت، این بیت را برابر ۱ قرار می‌دهد. بیت‌های دیگر ضمیمه برای کاربردهای آینده قابل استفاده خواهند بود.

ServerHello: این پیام همیشه اولین پاسخی است که کارگزار برای کارفرما ارسال می‌کند و تصمیمات نهایی را به کارفرما اعلام می‌کند. محتوای این پیام علاوه بر مؤلفه‌های حالت استاندارد، شامل مؤلفه یک بایتی ضمیمه نیز هست. کارگزار یکی از بیت‌های ضمیمه را می‌تواند ۱ ارسال کند؛ چون اگر مذاکره سه مرحله‌ای باشد، معمای کارفرما قابل استفاده نیست و حالت معطل هم در ایجاد یک جلسه جدید به کار نمی‌آید. اگر کارگزار همه بیت‌های ضمیمه را برابر صفر قرار دهد، به این معنا است که باید مذاکره را به شکل استاندارد انجام دهند. کارگزار با هر یک از دیگر روش‌ها که موافق باشد، روند مذاکره را مطابق همان روش باید ادامه دهد. اگر کارگزار گزینه‌های پیشنهادی کارفرما را کافی نداند (مثلاً کارفرما قابلیت حل معما را نداشته باشد ولی کارگزار نگران حمله DoS باشد) خطای insufficient_security را فرستاده و جلسه را خاتمه می‌دهد. اگر کارگزار بخواهد برای کارفرما معما ارسال کند، پس از مؤلفه ضمیمه باید مقادیر لازم برای معما را نیز ارسال کند که شامل حاصل درهم یک عدد تصادفی و تعدادی از بیت‌های آن عدد تصادفی می‌باشند [۱۱].

ServerCertificate: این پیام فقط زمانی ارسال نمی‌شود که تبادل کلید گمنام توافق شده باشد. در مذاکره به شیوه استاندارد، کلید عمومی درون گواهینامه باید متناظر با الگوریتم تبادل کلید باشد و در دستداد سه مرحله‌ای، گواهینامه باید کلیدی برای وارسی امضاء داشته باشد؛ مگر اینکه کارگزار گواهینامه دیفی‌هلمن با پارامترهای پیشنهادی کارفرما داشته باشد.

CertificateRequest: این پیام در مذاکراتی که برای ایجاد جلسه جدید انجام می‌شوند قابل استفاده است. در مذاکره چهار مرحله‌ای همان ساختار استاندارد را دارد و در مذاکره سه مرحله‌ای فاقد محتوا ارسال می‌شود تا کارفرما فرآیند احراز اصالت خود را با ارسال CertificateVerify کامل کند.

ServerKeyExchange: در مذاکره استاندارد، این پیام شامل پارامترهای موقت کارگزار است که توسط وی امضاء شده و برای کارفرما ارسال می‌گردد. در دستداد سه مرحله‌ای، این پیام تکمیل‌کننده فرآیند تبادل کلید است و کارگزار باید پارامتر تکمیل‌کننده (حاصل رمز شده pre-master-secret یا کلید عمومی دیفی‌هلمن) را امضاء کرده و برای کارفرما بفرستد. بدیهی است که در تبادل کلید گمنام، نیازی به امضاء نیست.

ServerHelloDone: این پیام فقط در مذاکره چهار مرحله‌ای و به همان شکل استاندارد قابل استفاده است.

ClientCertificate: اگر کارفرما در پیام ClientHello برای انجام مذاکره سه مرحله‌ای اعلام تمایل کرد، پس از آن باید گواهینامه‌اش را ارسال نماید. ممکن است کارفرما اصلاً گواهینامه‌ای نداشته باشد و یا گواهینامه معتبری ارسال نکند؛ در هر صورت، کارگزار حق تصمیم‌گیری دارد و می‌تواند مذاکره با شرایط کارفرما را نپذیرد.

ClientKeyExchange: اگر کارفرما در پیام ClientHello برای انجام مذاکره سه مرحله‌ای اعلام تمایل کرد، باید پارامترهای دیفی‌هلمن موقت پیشنهادی خود را در پیام ClientKeyExchange برای کارگزار بفرستد. اگر وی گواهینامه ارسال کرده باشد، این پیام را پس از گواهینامه می‌فرستد و در غیر اینصورت آن را پس از پیام ClientHello ارسال می‌کند. اگر مذاکره چهار مرحله‌ای توافق شود، این پیام به شکل استاندارد خواهد بود و اگر معمایی برای کارفرما ارسال شده باشد، وی باید پاسخ معما را یافته و در پیام ClientKeyExchange ارسال کند.

CertificateVerify: این پیام همیشه در مرحله سوم و برای تکمیل احراز اصالت کارفرما ارسال می‌شود. اگر کارگزار از کارفرما تقاضای احراز اصالت کرده باشد، کارفرما باید پیام CertificateVerify را طبق حالت استاندارد تولید کرده و ارسال کند.

Finished: این پیام همیشه پس از ChangeCipherSpec ارسال می‌شود و محاسبه آن مطابق استاندارد انجام می‌شود.

چنانچه مشاهده می‌شود، این پروتکل انعطاف‌پذیری کافی برای قابلیت استفاده از دستداد استاندارد، دستداد سه مرحله‌ای، تغییر حالت جاری اتصال و همچنین معمای کارفرما را دارد. بیتهای دیگر ضمیمه نیز برای بسط‌های دیگر قابل استفاده هستند. از لحاظ امنیتی و همچنین ساختار و پیکربندی، خدشه‌ای به SSL وارد نشده و نکاتی که برای هریک از روش‌ها به طور جداگانه بیان شدند، برای این پروتکل نیز صادق هستند.

۶- نتیجه‌گیری

یکی از مباحث مورد توجه در پروتکل‌های امنیتی، سرعت برقراری ارتباط امن در آنها می‌باشد. پروتکل SSL یکی از شایع‌ترین پروتکل‌های امنیتی مورد استفاده در انتقالات وب می‌باشد و متخصصین رمزنگاری همواره به دنبال راهکارهایی برای بهبود کارایی آن هستند. به همین جهت است که مسئله تسریع مذاکره در این پروتکل، اهمیت دارد و باید مورد بررسی قرار گیرد. در این مقاله به برخی تلاش‌ها که قبلاً برای این کار صورت گرفته اشاره شد و راهکارهای تازه‌ای نیز پیشنهاد شدند. برای سرعت بخشیدن به مذاکره یک جلسه جدید، دستداد سه مرحله‌ای پیشنهادی شرح داده شد و مقایسه‌ای بین ویژگی‌های آن و دستداد سریع منتشر شده [۷] نسبت به دستداد استاندارد صورت گرفت. این مقایسه نشان داد، دستداد پیشنهادی مزایای اساسی نسبت به دستداد سریع دارد و مانند آن، قابلیت استفاده از راهکارهای مقابله با حمله DoS را ندارد. اما از آنجا که مقابله با حمله DoS، در

همه کارگزارهای وب مطرح نیست و اهمیت این مسئله در استاندارد SSL نیز تا حدودی نادیده گرفته شده است، پرداختن چنین بهایی در قبال افزایش سرعت مذاکره، ناچیز به نظر می‌رسد.

یکی دیگر از پیشنهاداتی که در این مقاله شرح داده شد، روشی برای سرعت بخشیدن به تغییر حالت اتصال است. با استفاده از روش پیشنهادی، طرفین در طول یک جلسه می‌توانند پارامترهای حالت اتصال را با دو مرحله تبادل پیام تغییر دهند.

به منظور رسیدن به یک چارچوب یکپارچه که همه روش‌های مذاکره را در بر داشته باشد، در انتها به توضیح یک پروتکل جامع پرداخته شد. در این پروتکل ساختار اصلی SSL حفظ شده و با تغییرات اندکی این امکان فراهم شده است که طرفین به راحتی درباره مذاکره دلخواهشان به توافق برسند. گنجانیدن روش‌های مختلف مذاکره در یک پروتکل موجب افزایش انعطاف‌پذیری SSL می‌گردد و به همین جهت سودمند می‌باشد.

مراجع

[1] K. Hickman, *The SSL Protocol*, Ver. 2, Netscape Communications Corp., February 1995.

[2] A. Frier, P. Karlton, and P. Kocher, *The SSL3.0 Protocol*, Netscape Communications Corp., November 1996.

[3] T. Dierks, and C. Allen, *The TLS Protocol, version 1.0*, IETF, RFC 2246, January 1999.

[4] T. Dierks, and E. Rescorla, *The TLS Protocol, version 1.1*, IETF, May 2005.

[۵] ا. صالحی، *بررسی امنیت پروتکل SSL*، پایان‌نامه کارشناسی‌ارشد مهندسی مخابرات، دانشگاه صنعتی اصفهان، اصفهان، ایران، ۱۳۸۵.

[6] P. Eronen, and H. Tschofenig, *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*, IETF, RFC 4279, December 2005.

[7] H. Shacham, and D. Boneh, *TLS Fast-Track Session establishment*, IETF, August 2001.

[8] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, and T. Wright, *Transport layer security (TLS) extensions*, IETF, RFC 3546, June 2003.

[9] H. Shacham, D. Boneh, and E. Rescorla, "Fast-Track Session Establishment for TLS," *Proc. Internet Society's Symposium on Network and Distributed System Security*, pp. 195-202, 2002.

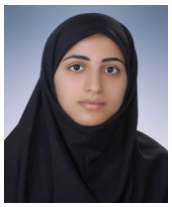
[10] C. Castelluccia, E. Mykletun, and G. Tsudik, "Improving Secure Server Performance by Re-Balancing SSL/TLS Handshakes," *Proc. ACM Symposium on Information, computer and communications security*, pp. 26-34, 2006.

[11] D. Dean, and A. Stubble_eld, "Using Client Puzzles to Protect TLS," *Proc. The Conference on USENIX Security Symposium*, pp. 1-1, 2001.

مهدی برنجکوب دکترای مهندسی برق خود را در سال ۱۳۷۸ از دانشگاه صنعتی اصفهان اخذ نمود و بلافاصله در دانشکده برق و کامپیوتر همین دانشگاه به عنوان استادیار فعالیت آموزشی و پژوهشی خود را آغاز کرد که کماکان این همکاری ادامه دارد. دروس تحصیلات تکمیلی ارائه شده توسط وی عبارتند از: اصول رمزنگاری، پروتکل‌های رمزنگاری، امنیت شبکه و پردازش گفتار. وی متجاوز از بیست پروژه تحصیلات تکمیلی را در زمینه‌های رمزنگاری و امنیت شبکه هدایت کرده است. او همچنین یکی از اعضای هیئت مؤسس انجمن رمز ایران در سال ۱۳۷۹ بوده است. از دیگر مسئولیت‌های وی مدیریت گروه پژوهشی امنیت شبکه و سیستم دانشکده برق و کامپیوتر و مدیریت مرکز تخصصی آپا دانشگاه صنعتی اصفهان است و پروژه‌های متعددی را اجرا و هدایت کرده است. عناوین پژوهشی مورد علاقه وی در حال حاضر امنیت در شبکه‌های بی‌سیم و پروتکل‌های احراز اصالت می‌باشد.

آدرس پست‌الکترونیکی ایشان عبارت است از:

brnjkb@cc.iut.ac.ir



امینه صالحی نجف‌آبادی فارغ التحصیل رشته مخابرات-سیستم در مقطع کارشناسی‌ارشد از دانشگاه صنعتی اصفهان است و در حال حاضر به عنوان مدرس با دانشگاه آزاد اسلامی واحد نجف‌آباد همکاری می‌کند. وی در پایان‌نامه خود که زیر نظر دکتر مهدی برنجکوب انجام شده، به بررسی کامل پروتکل SSL و نقاط ضعف آن پرداخته و برخی راهکارها را برای ارتقای آن ارائه نموده است که بخشی از آن در مقاله آورده شد.

اطلاعات بررسی مقاله:

تاریخ ارسال: ۸۵/۷/۱۶

تاریخ اصلاح: ۸۹/۵/۲۶

تاریخ قبول شدن: ۸۹/۶/۹

نویسنده مرتبط: دکتر مهدی برنجکوب، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران.

[1] Handshake
[2] Secure Socket Layer
[3] Connection
[4] Record Layer
[5] Session ID
[6] Internet Engineering Task Force
[7] Pre Shared Key
[8] Fast-Track
[9] Determining Handshake
[10] Determining Parameters
[11] Denial of Service
[12] Anonymous
[13] Round Trip Time
[14] Client puzzle