Analisis perbandingan algoritma RSA dan ECDSA pada autentikasi DTLS dalam implementasi video conference berbasis WEBRTC = Comparative analysis of RSA and ECDSA algorithms in implementation of WEBRTC based video conference

Mas Eka Setiawan, author

Abstrak

Komunikasi real-time merupakan komunikasi yang dilakukan tanpa adanya waktu transmisi yang signifikan. VoIP dan video telephony merupakan beberapa teknologi komunikasi real-time dimana aliran media dilewatkan dalam jaringan IP. webRTC sebagai teknologi baru, membawa teknologi seperti VoIP dan Video Telephony ke dalam web. Untuk menjamin keamanan data yang dikirimkan, webRTC mengharuskan implementasi dengan menggunakan enkripsi. Namun, RTP yang merupakan protokol komunikasi real-time, tidak menggunakan enkripsi dalam implementasinya sehingga perlu penggunaan protokol yang lebih aman yaitu SRTP. SRTP menggunakan kunci simetris untuk melakukan enkripsi data dalam komunikasi real-time. SRTP menggunakan DTLS untuk melakukan manajemen kunci, pertukaran kunci dan autentikasi. DTLS menggunakan sertifikat digital dan mekanisme tanda tangan digital dalam skema autentikasinya. Kriptografi dengan kunci asimetris diimplementasikan pada skema autentikasi DTLS. Dua algoritma yang pada umumnya digunakan untuk melakukan autentikasi tersebut adalah RSA dan ECDSA. Pendekatan perhitungan antara kedua algoritma tersebut berbeda. RSA menggunakan faktorisasi bilangan prima yang besar sedangkan ECDSA menggunakan perhitugnan pada kurva eliptis. Perbedaan tersebut menghasilkan parameter komputasi yang berbeda. Dalam tulisan ini dilakukan perbandingan algoritma RSA dan ECDSA dalam hal penggunaan sumber daya dan implikasinya dalam webRTC. Tulisan ini menggunakan dua pendekatan dalam percobaan perbandingan. Pendekatan pertama melakukan komputasi langsung dalam sebuah perangkat untuk melihat penggunaan sumber daya yang diperlukan. Perdekatan kedua dilakukan dalam sistem panggilan video sehingga perbedaan terlihat dalam implementasi webRTC. Dari hasil pengujian pada dua pendekatan tersebut, didapatkan bahwa RSA memiliki peningkatan kebutuhan sumber daya dan waktu penyelesaian autentikasi yang lebih tinggi dibandingkan dengan ECDSA. Rasio waktu CPU ECDSA terhadap RSA terus berkurang seiring peningkatan tingkat keamanan. Rasio menurun dari 0.2 menjadi 0,0002 pada pembuatan kunci, 2,6 menjadi 0,01 pada pembuatan signature, dan 62,0 menjadi 0,02 pada verifikasi signature untuk tingkat keamanan 80 dan 256. Alokasi memori RSA mendekati sepuluh kali lipat dibandingkan ECDSA pada tingkat keamanan 256 dan diprediksi meningkat seiring meningkatnya tingkat keamanan. Besar kunci yang digunakan mempengaruhi besar sertifikat dan verifikasi yang kirimkan. DTLS dengan maximum transmission unit sebesar 1500 byte memerlukan mekanisme fragmentasi untuk mengirimkan keseluruhan informasi. RSA dengan panjang kunci 15360 bit mengirimkan tiga puluh fragmen untuk sertifikat dan lima belas fragmen untuk verifikasi yang mempengaruhi waktu penyelesaian DTLS.Komunikasi real-time merupakan komunikasi yang dilakukan tanpa adanya waktu transmisi yang signifikan. VoIP dan video telephony merupakan beberapa teknologi komunikasi real-time dimana aliran media dilewatkan dalam jaringan IP. webRTC sebagai teknologi baru, membawa teknologi seperti VoIP dan Video Telephony ke dalam web. Untuk menjamin keamanan data yang dikirimkan, webRTC mengharuskan implementasi dengan menggunakan enkripsi. Namun, RTP yang merupakan protokol komunikasi real-time,

tidak menggunakan enkripsi dalam implementasinya sehingga perlu penggunaan protokol yang lebih aman yaitu SRTP. SRTP menggunakan kunci simetris untuk melakukan enkripsi data dalam komunikasi real-time. SRTP menggunakan DTLS untuk melakukan manajemen kunci, pertukaran kunci dan autentikasi. DTLS menggunakan sertifikat digital dan mekanisme tanda tangan digital dalam skema autentikasinya. Kriptografi dengan kunci asimetris diimplementasikan pada skema autentikasi DTLS. Dua algoritma yang pada umumnya digunakan untuk melakukan autentikasi tersebut adalah RSA dan ECDSA. Pendekatan perhitungan antara kedua algoritma tersebut berbeda. RSA menggunakan faktorisasi bilangan prima yang besar sedangkan ECDSA menggunakan perhitugnan pada kurva eliptis. Perbedaan tersebut menghasilkan parameter komputasi yang berbeda. Dalam tulisan ini dilakukan perbandingan algoritma RSA dan ECDSA dalam hal penggunaan sumber daya dan implikasinya dalam webRTC. Tulisan ini menggunakan dua pendekatan dalam percobaan perbandingan. Pendekatan pertama melakukan komputasi langsung dalam sebuah perangkat untuk melihat penggunaan sumber daya yang diperlukan. Perdekatan kedua dilakukan dalam sistem panggilan video sehingga perbedaan terlihat dalam implementasi webRTC. Dari hasil pengujian pada dua pendekatan tersebut, didapatkan bahwa RSA memiliki peningkatan kebutuhan sumber daya dan waktu penyelesaian autentikasi yang lebih tinggi dibandingkan dengan ECDSA. Rasio waktu CPU ECDSA terhadap RSA terus berkurang seiring peningkatan tingkat keamanan. Rasio menurun dari 0.2 menjadi 0,0002 pada pembuatan kunci, 2,6 menjadi 0,01 pada pembuatan signature, dan 62,0 menjadi 0,02 pada verifikasi signature untuk tingkat keamanan 80 dan 256. Alokasi memori RSA mendekati sepuluh kali lipat dibandingkan ECDSA pada tingkat keamanan 256 dan diprediksi meningkat seiring meningkatnya tingkat keamanan. Besar kunci yang digunakan mempengaruhi besar sertifikat dan verifikasi yang kirimkan. DTLS dengan maximum transmission unit sebesar 1500 byte memerlukan mekanisme fragmentasi untuk mengirimkan keseluruhan informasi. RSA dengan panjang kunci 15360 bit mengirimkan tiga puluh fragmen untuk sertifikat dan lima belas fragmen untuk verifikasi yang mempengaruhi waktu penyelesaian DTLS.
<hr>
Real time communication RTC is a communication type without any significant transmission delay. VoIP and Video Telephony is an example of RTC technology where media streams are passed on IP networks. webRTC as a new technology brings VoIP and Video Telephony technologies into the web. To ensure the security data, webRTC requires implementation with encryption. RTP which is an RTC protocol does not implement encryption, so it needs to use a more secure protocol which is SRTP. SRTP uses symmetric keys to perform data encryption in the RTC. SRTP uses DTLS to perform key management, key exchanges and authentication. DTLS uses digital certificates and digital signature mechanisms to authenticate. Cryptography with asymmetric keys is implemented in the DTLS authentication mechanism. Two commonly used algorithms for authentication are RSA and ECDSA. The calculation approach between those two algorithms is different. RSA uses prime factorization while ECDSA uses elliptical curve computation. These differences produce different computational parameters. In this paper we compare the RSA and ECDSA algorithm in terms of resources and its implication in webRTC. This paper uses two approaches for comparative experiments. The first approach is do direct computing in a device to see the use resources. The second approach is done in a video call system so that differences are seen in webRTC implementation. From the test results in both approaches, it was found that RSA has higher resource requirements and process completion times compared to ECDSA. The ratio for CPU time of ECDSA to RSA continues to decrease as security levels increase. The ratios decreases from 0.2 to 0.0002 in key generation, 2.6 to 0.01 in key generation, and 62.0 to 0.02 in key generation for security levels of 80 and

256. RSA memory allocation approximately ten times higher than ECDSA at 256 security level and predicted to increases with increasing of security level. Size of key affect the size of the certificate and the verification in DTLS. DTLS with a maximum transmission unit of 1500 bytes requires a fragmentation mechanism to send whole information. RSA with a key length of 15360 bits sends thirty fragments for certificates and fifteen fragments for verification which affect DTLS completion time.