BAB 6

KESIMPULAN DAN SARAN

Bab ini akan membahas kesimpulan yang dihasilkan lewat penelitian ini serta saran yang yang dapat dilakukan untuk mengembangkan penelitian ini lebih lanjut.

6.1 Kesimpulan

Kesimpulan yang dihasilkan dari penelitian ini adalah:

- Protokol Megrelishvili dapat diimplementasikan dengan berpegang pada teori-teori yang sudah ada dan dengan memanfaatkan *thread* untuk melakukan komputasi pembangunan kunci secara paralel.
- Pengujian eksperimental dilakukan dengan cara menguji signifikansi fitur *handshake*, mencoba melakukan penyerangan untuk menguji fitur pertahanan terhadap *man in the middle attack* baik dengan menggunakan vektor verifikasi maupun yang menggunakan tanda tangan digital, serta mengetes dampak nilai orde dan bilangan *integer* unik yang dipilih terhadap waktu eksekusi pembangunan kunci.
- Pertahanan terhadap *man in the middle attack* dapat dilakukan dengan memanfaatkan vektor verifikasi untuk melakukan verifikasi pesan. Tanda tangan digital yang dibangun dengan memanfaatkan AES *cipher* masih belum dapat digunakan untuk melakukan pertahanan terhadap *man in the middle attack* karena masih membutuhkan penelitian lebih lanjut.
- Pengembangan terhadap protokol Megrelishvili dapat dilakukan dengan menambahkan pertahanan terhadap *man in the middle attack*, khususnya dengan menggunakan tanda tangan digital yang lebih sederhana ketimbang vektor verifikasi. Selain itu pengembangan juga dapat dilakukan dengan menambahkan inisiasi komunikasi atau *handshake* sebelum komunikasi dan pembangunan kunci dilakukan.
- Fitur *handshake* yang dimiliki oleh perangkat lunak yang telah dibangun merupakan fitur yang cukup signifikan. Fitur ini dibutuhkan agar komunikasi dalam perangkat lunak dapat berlangsung dengan baik dan benar.
- Pertahanan terhadap *man in the middle attack* dengan menggunakan vektor verifikasi sudah dapat bekerja dengan cukup baik. Pertahanan ini hanya dapat ditembus oleh segelintir kecil kasus penyerangan, yaitu kasus penggantian pesan dengan pesan yang memiliki anggota blok yang tetap sama dengan pesan aslinya.
- Pertahanan terhadap *man in the middle attack* dengan menggunakan tanda tangan digital AES belum dapat bekerja dengan cukup baik. Hal ini disebabkan karena kunci sesi yang digunakan bisa saja berasal dari *attacker* sehingga tanda tangan digital yang dibuat bisa saja telah dipalsukan oleh *attacker* yang mengetahui kunci sesi yang digunakan.

- Sebelum berkomunikasi, *communicating entity* sebaiknya melakukan autentikasi entitas terhadap server yang memperantarai komunikasi agar *attacker* tidak dapat berpura-pura menjadi server. Hal ini perlu dilakukan agar kunci sesi yang nantinya akan digunakan untuk berkomunikasi terjamin berasal dari server sehingga tanda tangan digital dapat dibuat tanpa bisa dipalsukan oleh *attacker*.
- Nilai orde yang telah ditentukan berbanding lurus dengan waktu eksekusi yang dibutuhkan untuk melakukan pembangunan kunci. Semakin besar nilai orde yang ditentukan, semakin lama pula waktu yang dibutuhkan untuk melakukan pembangunan kunci.
- Nilai bilangan *integer* unik yang dipilih oleh *communicating entity* memiliki pengaruh yang kurang signifikan terhadap waktu eksekusi yang dibutuhkan untuk melakukan pembangunan kunci. Hal ini disebabkan karena bilangan tersebut hanya akan digunakan untuk melakukan pemangkatan matriks sedangkan algoritma pemangkatan matriks memiliki kompleksitas yang cukup rendah sehingga cenderung akan selesai dalam waktu yang cukup cepat.
- Waktu eksekusi pembangunan kunci pada tipe pertahanan vektor verifikasi cenderung lebih tinggi dari pembangunan kunci pada tipe pertahanan tanda tangan digital AES. Hal ini disebabkan karena pembangunan vektor verifikasi dilakukan bersamaan dengan pembangunan kunci, sedangkan pembangunan tanda tangan digital tidak dilakukan bersamaan dengan pembangunan kunci. Maka dari itulah pembangunan kunci pada tipe pertahanan tanda tangan digital cenderung akan selesai dalam waktu yang lebih cepat dibanding pembangunan kunci pada tipe pertahanan vektor verifikasi.
- Waktu eksekusi pembangunan kunci pada skenario *man in the middle attack* cenderung lebih tinggi dari Waktu eksekusi pembangunan kunci pada skenario normal. Hal ini disebabkan karena pada skenario *man in the middle attack* terdapat aktor tambahan yaitu *attacker* yang harus melakukan pembangunan kunci bersama dengan kedua *communicating entity*.

6.2 Saran

Saran yang yang dapat dilakukan untuk memperbaiki dan mengembangkan penelitian ini lebih lanjut adalah:

- Lakukan penelitian lebih lanjut mengenai penentuan matriks publik agar matriks publik yang digunakan tidak harus memenuhi syarat yang telah dibahas pada Subbab 3.2.1. Hal ini dilakukan untuk memenuhi teori dasar protokol Megrelishvili yang tidak terikat dengan batasan syarat-syarat tersebut.
- Lakukan penelitian lebih lanjut mengenai kasus-kasus *man in the middle attack* selain kasus ketika *attacker* berpura-pura menjadi server. Hal ini dilakukan untuk membuktikan bahwa protokol Megrelishvili benar-benar memiliki tingkat keamanan yang baik dalam melawan *man in the middle attack*.
- Lakukan penelitian lebih lanjut untuk melakukan implementasi protokol Megrelishvili dengan memanfaatkan lebih dari satu *device* sehingga tiap aktor dapat berada pada *device* yang berbeda-beda.

DAFTAR REFERENSI

[1] Arzaki, M. (2016) Elementary algorithms analysis of megrelishvili protocol. *Indonesian Journal of Computing*, **1**, 11–24.

[2] Arzaki, M. (2018) Strengthening megrelishvili protocol against man-in-the-middle attack. *2018 6th International Conference on Information and Communication Technology (ICoICT)*, Bandung, Indonesia, 3-5 Mei, pp. 274–280. IEEE, New York.

[3] Forouzan, B. A. (2008) *Cryptography and Network Security*. Tata Mc-Graw Hill, Delhi.

[4] Herhily, M. dan Shavit, N. (2011) *The art of multiprocessor programming*. Morgan Kaufmann, Waltham.