Jurnal Informatika Universitas Pamulang **ISSN: 2541-1004**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2622-4615**
Vol. 5, No. 2, Juni 2020 (203-207) **10.32493/informatika.v5i2.5675**

Arsitektur Keamanan Siber Dengan Protokol Denning-Sacco

Rama Dian Syah

Fakultas Teknologi Informasi, Universitas Gunadarma, Jl. Margonda Raya 100, Depok, Jawa Barat, Indonesia, 16424
e-mail: rama_ds@staff.gunadarma.ac.id

Submitted Date: June 25th, 2020 Reviewed Date: June 26th, 2020
Revised Date: June 27th, 2020 Accepted Date: June 30th, 2020

Abstract

Currently messages can be transmitted using information and communication technology. The message that is transmitted can contain data and information that is privacy or confidential. Messages that are confidential and privacy are only intended for parties that have been determined. Attacks by unauthorized parties may occur during the process of sending the message. Security in a private or confidential message exchange system is very much needed. The message exchange system is regulated by protocol to avoid certain party attacks. The method used in this research is the Denning-Sacco Protocol which is implemented in the exchange of messages from the sender to the recipient. This protocol uses a security key generated by the Key Distribution Center (KDC). The Denning-Sacco Protocol was developed from the Needham-Schroeder Protocol. This study produces an overview of the architecture of the Denning-Sacco Protocol to overcome the weaknesses of the Needham-Schroeder Protocol called the relpy attack. The steps of exchanging messages using the Denning-Sacco Protocol are explained in detail.

Keywords: Cyber Security; Denning-Sacco Protocol

Abstrak

Saat ini pesan dapat ditransmisikan menggunakan teknologi informasi dan komunikasi. Pesan yang ditransmisikan dapat berisi data dan informasi yang bersifat privasi atau rahasia. Pesan yang bersifat rahasia dan privasi hanya ditujukan untuk pihak yang sudah ditentukan. Serangan oleh pihak yang tidak berwenang mungkin terjadi pada saat proses pengiriman pesan tersebut. Keamanan pada sistem pertukaran pesan yang bersifat privasi atau rahasia sangat dibutuhkan. Sistem pertukaran pesan diatur oleh protokol untuk terhindar dari serangan pihak tertentu. Metode yang digunakan dalam penelitian ini yaitu Protokol Denning-Sacco yang diimplementasikan pada pertukaran pertukaran pesan dari pihak pengirim ke penerima. Protokol ini menggunakan kunci keamanan yang dibangkitkan oleh Key Distribution Center (KDC). Protokol Denning-Sacco dikembangan dari Protokol Needham-Schroeder. Penelitian ini menghasilkan gambaran arsitektur Protokol Denning-Sacco untuk mengatasi kelemahan dari Protokol Needham-Schroeder yang disebut dengan *reply attack*. Langkah-langkah pertukaran pesan menggunakan Protokol Denning-Sacco dijelaskan secara terperinci.

Kata Kunci: Keamanan, Siber; Protokol Denning-Sacco

1. Pendahuluan

Kemajuan teknologi informasi dapat membantu manusia dalam proses pertukaran pesan. Pesan dapat bersifat privasi dan rahasia yang hanya ditujukan untuk pihak yang sudah ditentukan. Pesan yang ditransmisikan melalui media teknologi mungkin diakses oleh pihak yang tidak berwenang.

Isu kemananan data dan informasi saat ini merupakan hal yang sangat penting dalam melindungi data dan informasi. Kejahatan yang dilakukan pada data dan informasi yang ditransmisikan pada media internet merupakan bagian dari kejahatan siber. Kejahatan siber adalah perilaku ilegal yang ditujukan kepada keamanan informasi pada sistem komputer menggunakan teknologi informasi sebagai alat kejahatan (Chintia, et al., 2019).

Kejahatan siber terkini dilansir oleh Liputa6 pada Mei 2019. Kejahatan ditargetkan

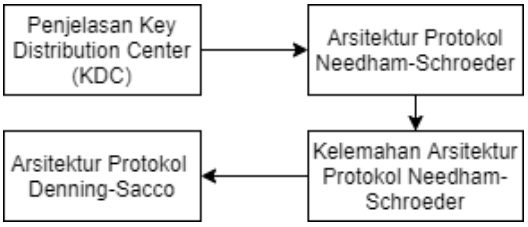
pada aplikasi media sosial untuk mengambil pesan dan data pribadi pengguna. Penyerang dapat memberikan *spyware* dan *malware* kepada pengguna media sosial untuk mengambil pesan dan data pribadi. Kasus ini membuktikan bahwa diperlukan suatu keamanan dalam pertukaran pesan atau menjaga data pribadi agar tidak diakses oleh pihak yang tidak bertanggung jawab.

Teknik pengamanan pesan dapat dilakukan dengan protokol kriptografi dan enkripsi. Enkripsi merupakan teknik untuk meningkatkan keamanan data dan informasi pada sebuah pesan, dimana pesan akan diacak sehingga sulit untuk disimpulkan tanpa mengetahui kode atau sandi khusus (Syah & Suhatril, 2019). Peningkatan keamanan pesan dapat dilakukan dengan pendekatan protokol Denning-Sacco.

Pada penelitian ini akan disajikan arsitektur keamanan pertukaran pesan dengan menggunakan Protokol denning-sacco. Protokol Denning-Sacco dikembangkan berdasarkan Protokol Needham-Schroeder. Tujuan dari pengembangan protokol yaitu untuk mengatasi masalah *reply attack* yang mungkin terjadi pada protokol Needham-Schoroeder. Arsitektur dari Protokol Denning-Sacco digambarkan dan dijelaskan secara terperinci.

2. Metode Penelitian

Penelitian dilakukan dengan 4 tahapan yaitu: (1) penjelasan Key Distribution Center (KDC); (2) arsitektur protokol Needham-Schroeder; (3) Kelemahan arsitektur protokol Needham-Schroeder; (4) arsitektur protokol Denning-Sacco. Diagram alur tahapan penelitian dapat dilihat pada Gambar 1.

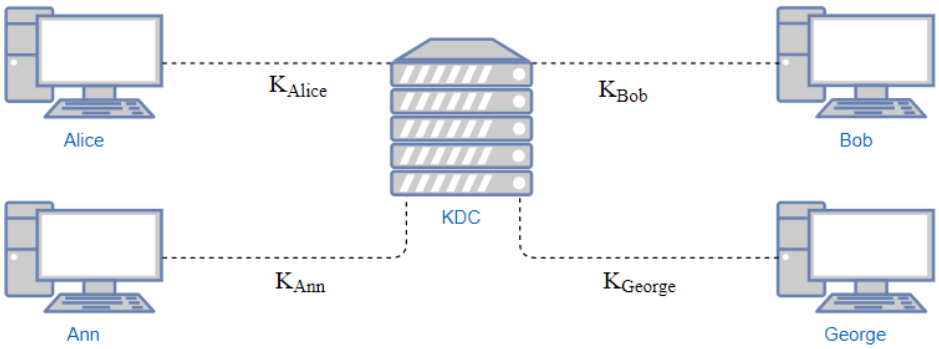


Gambar 1. Tahapan Penelitian

Protokol kriptografi merupakan suatu aturan yang berisi rangkaian langkah-langkah yang melibatkan dua atau lebih orang yang dibuat untuk menyelesaikan suatu kegiatan menggunakan kriptografi. Protokol kriptografi diperlukan mengatur peredaran informasi yang ditransmisikan (Sanjaya, 2017). Protokol kriptografi yang menjadi dasar dari banyak protokol manajemen adalah protokol yang diusulkan oleh Needham Schoreder pada tahun 1978. Protokol ini berbasiskan protokol kriptografi simetris dimana server keotentikan (KDC) akan membuat sesi rahasia untuk membuktikan keaslian dalam interaksi oleh pengirim dan penerima.

2.1 Key Disribution Center (KDC)

KDC merupakan sebuah server untuk transmisi informasi yang aman antara para pengguna (Sultana, Jabiullah, & Rahman, 2019). Setiap pengguna akan membuat kunci rahasia bersama dengan KDC. Berikut merupakan arsitektur KDC terdapat pada gambar 1.

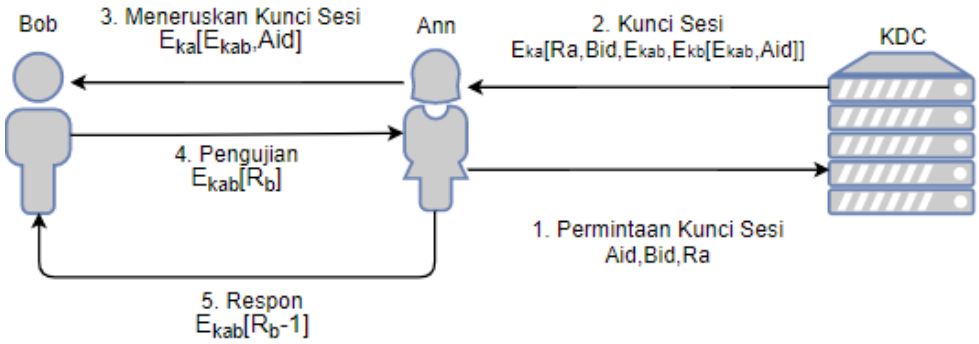


Gambar 1. Key-Distribution Center (KDC)

Setiap pengguna mempunyai kunci rahasia yang hanya diketahui oleh client itu sendiri dan KDC. Jika Ann ingin berkomunikasi dengan Bob maka sebuah kunci sesi akan dibuat antara Ann dan Bob. Kunci sesi tidak lagi dapat digunakan ketika komunikasi selesai atau diakhiri.

2.2 Protokol Needham-Schroeder

Protokol Needham-Schroeder menggunakan otentikasi diantara dua pihak yang berkomunikasi. Berikut merupakan arsitektur protokol Needham-Schroeder pada gambar 2.



Gambar 2. Arsitektur Protokol Needham-Schroeder

Keterangan gambar 2:

- E_{Ka} = Kunci rahasia milik Ann
- E_{Kb} = Kunci rahasia milik Bob
- R_a = Nonce milik ann
- R_b = Nonce milik Bob
- Aid = Identifier milik Ann
- Bid = Identifier milik Bob
- R_b-1 = Nonce Bob dikurangi 1

Tahapan pada protokol Needham-Schroeder:

1. Ann mengirim permintaan kunci sesi [Aid,Bid,Ra] ke KDC dimana Ra adalah nonce yang dibuat oleh Ann. Nonce adalah angka acak yang hanya dapat digunakan sekali saja.
2. KDC akan membalas dengan pesan yang diacak dengan kunci rahasia milik A [E_{Ka}]. Pesan berisi Nonce milik Ann [Ra], identifier Bob [Bid], kunci sesi [E_{kab}] dan sub pesan E_{kb}[E_{kab},Aid] yang diacak menggunakan kunci rahasia Bob [K_b].
3. Jika nonce [Ra] dan identifier Bob [Bid] sesuai dengan permintaan sebelumnya, menerima kunci sesi baru dan meneruskan pesan ke Bob.
4. Bob akan menerima pesan yang berisi kunci sesi [E_{kab}] dan identifier ann [Aid]. Kemudian Bob akan melakukan pengujian pesan dengan membuat Nonce milik Bob [Rb] dan mengirimkannya ke Ann.
5. Ann membaca Nonce milik Bob dengan kunci sesi. Kemudian mengurangi satu dan mengacak pesannya kembali menggunakan kunci sesi [E_{kab}] dan mengirimkan kembali pesan ke Bob.
6. Jika Bob menerima pesan yang berisi Nonce [Rb-1], maka Bob menerima kunci sesi yang otentik.

Pada protokol Needham-Schroeder terdapat suatu kelamahan yang disebut dengan *reply attack*. Serangan *reply attack* adalah serangan dengan merekam sesi komunikasi dan mereply seluruh atau sebagian sesi, pada suatu saat nanti. Kelemahan pada protokol ini harus diatasi dengan memodifikasi prosedur pada tahapan pengiriman pesan.

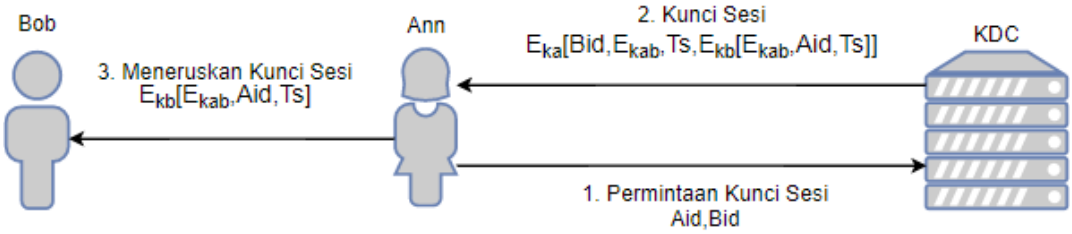
3 Hasil dan Pembahasan

Protokol Denning-Sacco dikembangkan dengan tujuan untuk memperbaiki kelemahan pada Protokol Needham-Schroeder. Serangan *reply attack* mungkin terjadi pada saat perukaran pesan pada protokol Needham-Schroeder. Berikut merupakan gambaran dari serangan *reply attack* yang terjadi pada protokol Needham-Schroeder terdapat pada Gambar 3.

Gambar 3. Reply Attack pada Protokol Needham-Schroeder

Apabila penyerang mampu mengambil pesan pada langkah 3 dan menggunakan kunci sesi lama, maka penyerang dapat melihat pesan dan merekamnya. Penyerang dapat menipu Bob agar menggunakan kunci sesi lama hanya dengan mengirim ulang langkah 3. Jika penyerang dapat mencegat pesan pengujian (handsahake message) pada langkah 4, maka penyerang dapat meniru respons Ann di langkah 5.

Untuk memperbaiki kelemahan protokol Needham-Schroeder maka Denning-Sacco memodifikasi protokol Needham-Schroeder dengan mengganti Nonce menjadi Timestamp untuk membuktikan bahwa kunci yang diterima merupakan kunci yang fresh (Nesi & Rucci, 2005). Berikut merupakan arsitektur protokol Denning-Sacco terdapat pada gambar 4.



Gambar 4. Arsitektur Protokol Denning-Sacco

Keterangan gambar 4 sama dengan keterangan gambar 2, Hanya saja R (Nonce) diganti dengan Ts (Timestamp).
Tahapan pada protokol Denning-Sacco:

1. Ann mengirim permintaan kunci sesi [Aid,Bid] ke KDC
2. KDC akan membalas dengan pesan yang diacak dengan kunci rahasia milik A [E_{Ka}]. Pesan berisi Timestamp [Ts], identifier Bob [Bid], kunci sesi [E_{kab}] dan sub pesan $E_{kb}[E_{kab},Aid,Ts]$ yang diacak menggunakan kunci rahasia Bob [K_b].
3. Jika Timestamp [Ts] dan identifier Bob [Bid] sesuai, menerima kunci sesi baru dan meneruskan pesan ke Bob.
4. Bob menerima pesan kunci yang otentik

4 Kesimpulan

Pada penelitian ini disajikan arsitektur protokol Denning-Sacco untuk keamanan pesan yang ditransmisikan dari pengirim ke penerima pesan. Kelemahan dari protokol Needham-Schroeder yaitu *reply attack* dapat diatasi dengan mengganti *nonce* menjadi *timestamp* yang ada pada protokol Denning-Sacco. Penelitian ini dapat dikembangkan lagi dengan menggunakan protokol kriptografi

asimetris dengan kunci yang digunakan yaitu kunci publik dan kunci privat.

Daftar Pustaka

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & S.kom., M. N. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal of Information Engineering and Educational Technology, 2*(2), 65-69. doi:10.26740/jieet.v2n2.p65-69.

Syah, R. D., & Suhatril, R. J. (2019). *Digital Image Cryptography Using Combination of Arnold's Cat Map and Bernoulli Map Based on Chaos Theory*, *4*(2), 258-262. doi:10.5281/zenodo.3153338.

Sanjaya, M. B. (2017). Inisialisasi Key Generating Kriptografi AES Pada Pendekatan Protokol SMSSEC. *Jurnal Infotel*, *9*(1), 18-23. doi:10.20895/infotel.v9i1.142.

Sultana, S., Jabiullah, M. I., & Rahman, M. L. (2009). Improved Needham-Schroeder protocol for secured and efficient key distributions. *2009 12th International Conference on Computers and Information Technology*. doi:10.1109/iccit.2009.5407301.

Nesi, M., & Rucci, G. (2005). Formalizing and Analyzing the Needham-Schroeder Symmetric-Key Protocol by Rewriting. *Electronic Notes in Theoretical Computer Science, 135*(1), 95-114. doi:10.1016/j.entcs.2005.06.002.