Prototipe Teknik Mutual Authentication untuk Digital Rights Management

Yoso Adi Setyoko[1], Anggi Zafia[2], Aulia Desy Nur Utomo[3]
[1]Fakultas Informatika Institut Teknologi Telkom Purwokerto
e-mail: [1]yoso@ittelkom-pwt.ac.id, [2]zafia@ittelkom-pwt.ac.id, [3]auliautomo@ittelkom-pwt.ac.id

Abstrak

Penelitian kami adalah adopsi teknik mutual authentication pada smart card untuk Digital Rights Management (DRM) yang diterapkan menggunakan rekayasa protokol jaringan. Rekayasa protokol tersebut kami adopsi dari teknik mutual authentication yang dimiliki oleh smart card Mifare Desfire. Pengujian yang dilakukan di penelitian kami adalah pengujian aspek keamanan autentikasi dan kerahasiaan data. Pengujian autentikasi kami lakukan dengan mengubah master key client dan server yang menentukan keberhasilan autentikasi. Sedangkan pengujian kerahasiaan data dilakukan dengan menyadap data yang dikirim dari client ke server DRM. Ketika autentikasi oleh client dan server gagal dilakukan maka perangkat lunak dinyatakan sebagai software tidak valid begitu juga sebaliknya. Hasil penelitian kami adalah keberhasilan implementasi adopsi teknik mutual authentication milik smart card untuk proteksi aplikasi dalam DRM mencakup fungsi autentikasi, enkripsi.

Kata kunci*— *Prototipe, mutual authentication, DRM, kerahasiaan, rekayasa protokol

Abstract

Our research is the adoption of mutual authentication techniques on smart cards for Digital Rights Management (DRM) which is applied using network protocol engineering. We adopted the protocol engineering from the mutual authentication technique owned by the Mifare Desfire smart card. The tests carried out in our research are testing the security aspects of authentication and data confidentiality. Our authentication test is done by changing the client and server master keys that determine the success of authentication. Meanwhile, data confidentiality testing is carried out by tapping data sent from the client to the DRM server. When authentication by the client and server fails, the software is declared invalid and vice versa. The result of our research is the successful implementation of the adoption of the smart card's mutual authentication technique for application protection in DRM including authentication and encryption functions.

Keywords— *Prototype, mutual authentication, DRM, encryption, protocol engineering*

1. PENDAHULUAN

Penelitian yang kami lakukan saat ini merupakan implementasi dari rancangan protokol keamanan yang kami buat pada penelitian sebelumnya. Penelitian ini dilakukan dengan mengadopsi protokol keamanan yang ada sebelumnya pada *smart card* [1]. Perlu diketahui bahwa kelebihan *smart card* dalam melakukan komunikasi dengan alat pembaca *smart card* menerapkan protokol keamanan secara *offline*. Kemudian kelebihan kedua *smart card* membangun komunikasi aman dengan pembaca tidak menggunakan *Public Key Infrastructure* (PKI) [2]. Oleh sebab itu kami mengadopsi teknik komunikasi aman tersebut untuk keperluan lain di luar penggunaan *smart card* yaitu *Digital Rights Management* (DRM). Ada perbedaan implementasi *mutual authentication* pada *smart card* dengan implementasi pada penelitian ini yaitu pada penelitian ini kami tidak menggunakan perangkat keras *Secure Access Module* (SAM) untuk penyimpanan kunci privat.

Adapun metode penelitian yang kami terapkan adalah *Design Science Research Methodology* (DSRM). Tahapan pada DSRM terdiri dari identifikasi masalah, menentukan tujuan penelitian, rancangan, demonstrasi, evaluasi, dan komunikasi. Analisis hasil penelitian yang kami lakukan yaitu bahwa protokol pada *smart card* berhasil diadopsi untuk DRM. Implementasi penelitian kami mencakup beberapa aspek keamanan antara lain aspek autentikasi, aspek kerahasiaan, dan aspek user identitas. Evaluasi hasil penelitian kami adalah penelitian yang kami lakukan terdapat keterbatasan bahwa kunci privat tidak disimpan dalam SAM. Kelanjutan dari penelitian ini adalah penggunaan SAM pada *device* komunikasi.

2. METODE PENELITIAN

Bagian dua akan menjelaskan tentang metode penelitian yang dilakukan oleh penulis. Adapun literature riview kami meliputi *mutual authentication*, DRM, Philips *mutual authentication*, key diversification, AES, Triple DES, SAM, dan *smart card*. Keterangan lebih detail tentang literatur kami jelaskan sebagai berikut.

2.1 Mutual Authentication

Mutual Authentication adalah proses autentikasi yang dilakukan oleh dua buah *device* sebelum melakukan pertukaran data. Studi kasus pada penelitian kami melibatkan dua buah *device* yaitu *client* dan *server*. Mekanisme *mutual authentication* pada penelitian kami adalah *challenge* dan *response*. *Server* melakukan *challenge* kepada *client* dan begitu pula *client* memberikan *challenge* kepada *server*. Jika *challenge* berhasil dijawab maka proses authentikasi berhasil dan jika sebaliknya maka proses autentikasi gagal. Jika proses autentikasi gagal maka komunikasi antar *client* dan *server* tidak bisa dilanjutkan.

2.2 Digital Rights Management (DRM)

Digital Rights Management secara luas mengacu pada seperangkat kebijakan, teknik dan alat-alat yang memandu penggunaan yang tepat dari konten digital [3]. Fungsi utama DRM sangat beragam. Fungsi-fungsi DRM termasuk memfasilitasi pengemasan konten mentah ke dalam bentuk yang sesuai untuk distribusi dan pelacakan yang mudah, melindungi konten untuk transmisi anti rusak, melindungi konten dari penggunaan yang tidak sah, dan memungkinkan spesifikasi hak yang sesuai, yang menentukan mode konsumsi konten. Penelitian kami menggunakan DRM untuk melindungi keaslian perangkat lunak.

2.3 Philips Mutual Authentication

Philips Semiconductors mengeluarkan skema *mutual authentication* yang digunakan pada *smart card*. Skema tersebut sesuai dengan dokumen yang diterbitkan oleh Philips [1]. Skema *mutual authentication* yang dibuat oleh Philips menggunakan kunci privat. Skema tersebut digunakan untuk autentikasi yang bersifat offline antara reader dan *smart card*. Skema tersebut memiliki tiga step untuk *mutual authentication*. Kami mengadopsi mekanisme tersebut untuk implementasi DRM. Hipotesa kami mekanisme ini cocok untuk diterapkan pada DRM karena mampu melindungi perangkat lunak. Selain itu mekanisme *mutual authentication* milik Philips ini merupakan mekanisme protokol yang ringan karena tidak memerlukan algoritma kunci public.

2.4 Key Diversification

Proses pembuatan kunci-kunci baru yang bersifat sementara dari kunci master menggunakan beberapa metode disebut sebagai *key diversification* [4]. Salah satu implementasi *key diversification* yaitu ada pada *smart card*. Dengan adanya *key diversification* maka kunci yang ada pada *smart card* beragam [4]. Kunci pada *smart card* satu dengan *smart card* yang lain akan berbeda-beda. Teknik *key diversification* merupakan langkah pertama yang akan diadopsi pada penelitian kami untuk DRM. Kunci yang akan terbentuk akan beragam untuk masing-masing *client*. Proses *key diversification* menggunakan algoritma AES 128 bit [3][5].

2.5 Advance Encyption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma yang digunakan untuk melindungi data elektronik [6]. Algoritma AES merupakan symmetric block cipher yang dapat mengenkripsi dan mendekripsi informasi. Enkripsi adalah proses mengubah data ke dalam bentuk yang tidak dapat dibaca manusia yang disebut sebagai *ciphertext*. Sedangkan dekripsi adalah proses mengkonversi ciphertext ke bentuk semula yang dapat dibaca manusia yang disebut sebagai *plaintext*. Algoritma AES dapat diimplementasikan dengan kunci kriptografi berukuran 128, 192, dan 256 bit untuk mengenkripsi dan mendekripsi data dalam blok-blok berukuran 128 bit.

2.6 *Triple Data Encryption Standard* (Triple DES)

DES merupakan algoritma yang digunakan untuk mengenkripsi data. Triple DES merupakan pengembangan dari Data Encryption Standard (DES) [7]. Menurut skema triple DES merupakan algoritma yang di dalamnya terdiri dari algoritma DES yang digunakan sebanyak tiga kali. Triple DES memiliki skema enkripsi tiga kali menggunakan algoritma DES yang mana masing-masing operasi DES menggunakan kunci yang berbeda-beda. Sehingga triple DES menggunakan tiga kunci.

2.7 *Secure Access Module* (SAM)

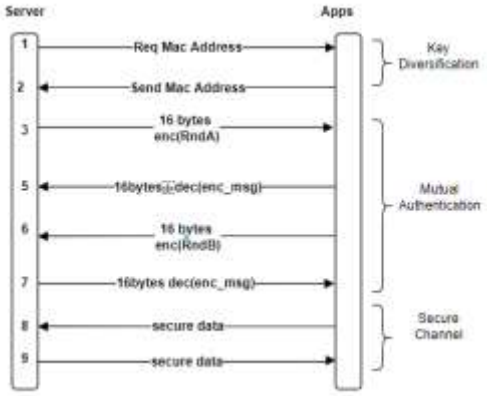
SAM adalah *smart card* yang digunakan untuk meningkatkan keamanan dan perfomansi kriptografi pada suatu *devices*. Umumnya digunakan pada *device* yang membutuhkan transaksi aman seperti system pembayaran [8]. Contoh system pembayaran yang menggunakan SAM di Indonesia adalah pembayaran dengan transaksi Uang Elektronik (U-nik) untuk bank Mandiri, BRI, BNI, BCA, dan Bank DKI [9]. Namun prototipe peneltian kami saat ini tidak menggunakan perangkat SAM.

2.8 *Smart Card*

Smart Card merupakan sebuah kartu yang memiliki kemampuan komputasi [10]. *Smart card* juga dikatakan memiliki kemampuan kriptografi di dalamnya. *Smart card* digunakan diberbagai keperluan sehari-hari antara lain untuk *Subscriber Identity Module (SIM) Cards*, *financial transactions, urban transportation system, dan ID cards* [10].

3. HASIL DAN PEMBAHASAN

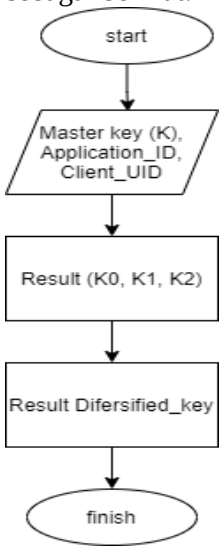
Rancangan protokol yang kami buat terdapat tiga tahap yaitu *key diversification, mutual authentication, secure message exchange*. Kami mengadopsi juga teknik *key diversification* pada jurnal sebelumnya [1]. Selanjutnya kami mengadopsi Teknik *mutual authentication* yang sebelumnya ada pada *smart card* Philips Mifare Desfire [1]. Kemudian *secure communication* dibangun menggunakan kunci sesi yang dihasilkan pada tahapan sebelumnya. Implementasi protokol keseluruhan dari awal hingga akhir penelitian kami adalah sebagai berikut.



Gambar 1 Skema Protokol Keseluruhan

3.1 Key Diversification

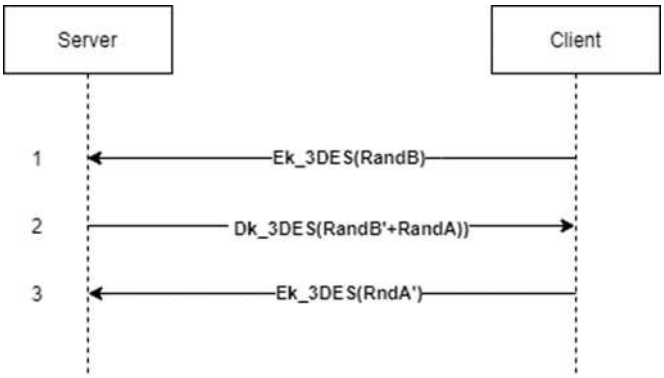
Key diversification merupakan tahap awal dari rekayasa protokol yang kami bangun. Penelitian kami menggunakan teknik *key diversification* yang digunakan pada *smart card* [4][5]. Key diversification yang coba terapkan adalah sebagai berikut.



Gambar 2 Tahap *Key Diversification*

Tahap *key diversification* di atas menghasilkan sebuah kunci dengan nama diversified_key yang selanjutnya digunakan untuk enkripsi dan dekripsi pada proses *mutual authentication*. Algoritma yang digunakan pada proses key diversification adalah AES 128 bit. Proses key diversification melibatkan application ID dan UID pada *smart card*. Pada penelitian kami application ID dan UID diganti dengan kode unik perangkat keras. Proses *key diversification* ini berdampak pada kunci masing-masing *device* yang menggunakan protokol rancangan kami akan bersifat unik. Perlu diketahui bahwa proses key diversification dilakukan oleh kedua belah pihak *client* dan *server*.

3.2 *Mutual Authentication*

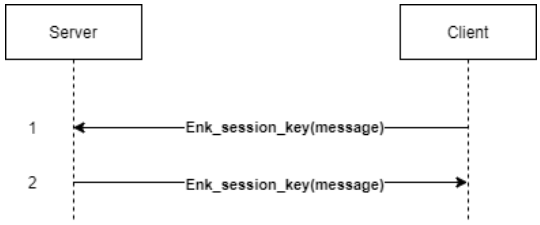


Gambar 3 Tahap 2 Mutual Authentication

Sequence diagram di atas adalah proses *mutual authentication*. Ada tiga langkah untuk melakukan *mutual authentication*. Pada langkah nomor 1 *client* memberikan *challenge* kepada *server* dengan mengenkripsi random byte dengan ukuran 8 byte. Kemudian langkah nomor 2 *server* melakukan dekripsi message yang dikirimkan oleh *client* dan mengirimkan ulang pesan RandB yang ditorasi kiri dan digabung dengan RandA milik *server*. Selanjutnya *client* mengenkripsi pesan dan mendapatkan hasil RandB' kemudian RandB' dirotasi kanan. Jika hasil rotasi kanan RandB' sama dengan RandB milik *client* maka autentikasi *server* berhasil dan jika sebaliknya maka *client* menolak komunikasi. Selanjutnya langkah nomor 3 *client* melakukan rotasi kiri RandA menjadi RandA' kemudian dienkripsi oleh *client*. Hasil enkripsi RandA' dikirim ke *server*. Kemudian *server* merotasi kanan RandA' dan mencocokkan RandA dari *client* dan RandA yang dimiliki oleh *server*. Jika RandA valid maka *mutual authentication* berhasil. Namun jika RandA tidak valid maka proses *mutual authentication* gagal dan *server* menolak komunikasi. Proses *mutual authentication* akan menghasilkan *session key* yang dapat digunakan untuk proses selanjutnya misalnya untuk komunikasi antar *client* dan *server* secara aman. Kunci sesi yang dibuat adalah kombinasi dari RandA, RandB, RandA', dan RandB'. Kunci sesi yang dihasilkan akan selalu berbeda-beda dan acak ketika *client* dan *server* memulai komunikasi.

Proses *mutual authentication* inilah yang fungsinya diadopsi pada penelitian kami untuk melakukan DRM. Pada DRM pihak *client* maupun *server* dapa melakukan verifikasi dengan proses ini. Perangkat lunak dapat berlaku sebagai *client* DRM yang melakukan *mutual authentication* dengan *server*. Teknik ini dapat menjadi terobosan baru untuk melindungi perangkat lunak dari pembajakan yang sebelumnya hanya menggunakan *serial number*.

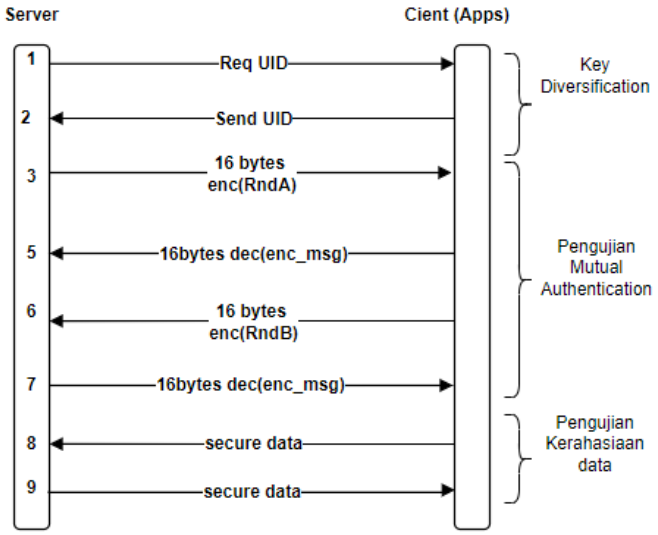
3.3 *Secure Communication*



Gambar 4 Tahap 3 *Secure Message*

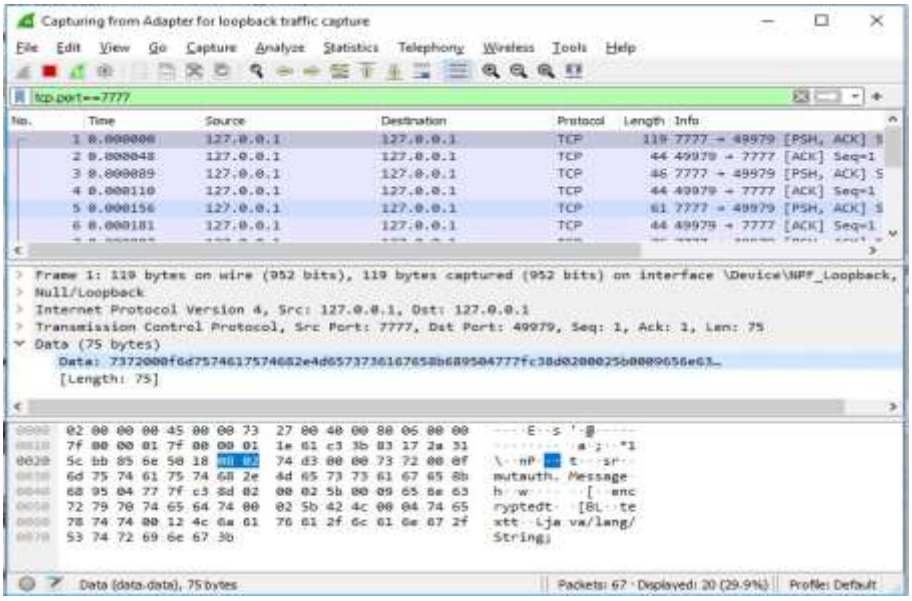
Fungsi ketiga *secure message* merupakan fungsi lanjutan setelah proses *mutual authentication* berhasil. Fungsi DRM ada pada *mutual authenticataion*. Dengan memanfaatkan kunci sesi yang terbentuk maka *client* dan *server* dapat memanfaatkan kunci sesi untuk bertukar pesan secara aman atau terenkripsi. Pembahasan dan implementasi tentang komunikasi aman melalui adopsi protokol ini akan menjadi bahan penelitian selanjutnya.

3.4 Pengujian Autentikasi



Gambar 5 Pengujian *Key Diversification*, *Mutual Authentication* dan *Secure Message*

Tahap ini merupakan pengujian proses *mutual authentication* (di dalam bingkai warna hijau). Proses pengujian ini dilakukan dengan memasang UID yang berbeda antara *client* dan *server* maka proses *mutual authentication* gagal dilakukan. Hal ini disebabkan karena *key diversification* yang dihasilkan oleh *client* berbeda dengan *server*. Dengan kunci yang berbeda antara *client* dan *server* maka *server* gagal menjawab *challenge* dari *client*. Dengan gagalnya proses *mutual authentication* tersebut maka client dan *server* tidak dapat membentuk kunci sesi.



Gambar 6 Pengujian Kerahasiaan Data dengan Wireshark

Tahap pengujian selanjutnya adalah pengujian *secure message* atau *encrypted message*. Pada figure 3 terdapat pada bingkai warna oranye. Kemudian untuk figure 4 di atas merupakan pengujian sadap data menggunakan tool wireshark. Pada figure 4 data terenkripsi ditandai dengan bingkai warna oranye. Dengan tool wireshark kami mencoba menyadap komunikasi antar *client* dan *server*. Kami mendapatkan capture data melalui wireshak dan mendapatkan data yang terenkripsi antara *client* dan *server*. Ini membuktikan bahwa pesan komunikasi antara *client* dan *server* terlindungi oleh enkripsi dan aman.

4. KESIMPULAN

Penelitian berhasil dilakukan sesuai dengan tujuan penelitian yaitu mengadopsi protokol komunikasi *smart card* untuk diterapkan pada DRM. Seluruh tahap protokol key diversification, *mutual authentication*, dan secure communication telah diimplementasikan dengan baik. Adapun aspek-aspek yang dapat kami capai dalam rekayasa protokol ini yaitu aspek autentikasi, aspek user

identity, dan aspek confidentiality. Pengujian kerahasiaan data kami lakukan dengan bantuan tool *wireshark* untuk menyadap komunikasi. Hasil penyadapan komunikasi membuktikan bahwa komunikasi antar *client* dan *server* sudah terenkripsi dan mencapai aspek *confidentiality*. Dengan ini maka rancangan *mutual authentication* untuk DRM pada penelitian kami sebelumnya berhasil diimplementasikan dan diuji. Penelitian kami selanjutnya dari penelitian ini adalah rancangan dan implementasi *secure messaging*. Kemudian kami juga akan mempertimbangkan bagaimana rancangan dan implementasi protokol untuk mengganti fungsi SAM.

DAFTAR PUSTAKA

[1] M. D. E. S. Fire and C. Stanford, "Mifare ® DES Fire," no. April, 2009.

[2] S. Goswami, S. Misra, and M. Mukesh, "A Replay Attack Resilient System for PKI Based Authentication in Challenge-Response Mode for Online Application," *Proc. - 2014 3rd Int. Conf. Eco-Friendly Comput. Commun. Syst. ICECCS 2014*, pp. 144–148, 2015, doi: 10.1109/Eco-friendly.2014.104.

[3] R. Engelberger, M. Fetscherin, and D. Günnewig, "Digital rights management," *Wirtschaftsinformatik*, vol. 47, no. 2, pp. 141–147, 2005, doi: 10.1007/BF03250987.

[4] Ç. Polat, K. Yildiz, U. C. Çabuk, and G. Dalkiliç, "Providing key diversity for symmetric encryption in Ad-Hoc wireless networks," *2nd Int. Conf. Comput. Sci. Eng. UBMK 2017*, pp. 298–303, 2017, doi: 10.1109/UBMK.2017.8093393.

[5] NXP, "Symmetric key diversifications," no. March, pp. 1–23, 2010, [Online]. Available: http://www.nxp.com/documents/application_note/AN10922.pdf.

[6] B. Rothke, "A look at the Advanced Encryption Standard (AES)," *Inf. Secur. Manag. Handbook, Sixth Ed.*, pp. 1151–1158, 2007, doi: 10.1201/9781439833032.ch89.

[7] A. Biryukov and C. Cannière, "Data encryption standard (DES)," *Encycl. Cryptogr. Secur.*, vol. 3, pp. 129–135, 2006, doi: 10.1007/0-387-23483-7_94.

[8] Dr. Peter Klein, "Secure Access Module (SAM)," *CardLogic.com*, 2011. https://www.cardlogix.com/glossary/sam-card-secure-access-module-secure-application-module/.

[9] F. Sibarani, "Kartu SAM, Master App yang Dilakukan dengan Sarana & Keadaan Apa Adanya," 2022, [Online]. Available: https://www.aktualdetik.com/berita/7117/kartu-sam-master-app-yang-dilakukan-dengan-sarana--keadaan-apa-adanya.html.

[10] R. Chandramouli and P. Lee, "Infrastructure standards for smart ID card deployment," *IEEE Secur. Priv.*, vol. 5, no. 2, pp. 92–96, 2007, doi: 10.1109/MSP.2007.34.