Jurnal Sistem Informasi dan Ilmu Komputer
Volume. 2 No. 4 November 2024
e-ISSN: 2986-4976; dan p-ISSN: 2986-5158, Hal. 01-08
DOI: https://doi.org/10.59581/jusiik-widyakarya.v2i2.3995
Available online: https://journal.widyakarya.ac.id/index.php/jusiik-widyakarya

Peningkatan Keamanan Data dengan Kriptografi Modern pada Sistem Operasi

Rakhmadi Rahman[1*)], Khumaedi[2)], Nugrah Surya Pratama[3)]
[1,2,3)]Jurusan Sains, Program Studi Sistem Informaso, Institut Teknologi Bacharuddin Jusuf Habibie, Indonesia
**meliodas00012@gmail.com*

Alamat: Jl. Balaikota No.1, Bumi Harapan, Kec. Bacukiki Bar., Kota Parepare, Sulawesi Selatan 91122
Korespondesi penulis: meliodas00012@gmail.com

Abstract: *In the current digital era, data security is a top priority for individuals, organizations, and businesses. Data is considered a valuable asset that needs to be protected from various security threats, especially in operating systems where data is stored (data at rest) and transmitted (data in motion) through networks. This research aims to enhance data security by implementing modern cryptographic methods. The cryptographic methods used include RC4, AES, and WPA3. Penetration testing is conducted to evaluate the effectiveness and efficiency of each cryptographic method. The research results show that the implementation of modern cryptography provides an additional layer of security against security threats to data in motion and data at rest within the operating system.*

Keywords: *Data Security, Modern Cryptography, RC4, AES, WPA3, Penetration Testing*

Abstrak: Di era digital saat ini, keamanan data merupakan prioritas utama bagi individu, organisasi, dan bisnis. Data dianggap sebagai aset berharga yang perlu dilindungi dari berbagai ancaman keamanan, terutama dalam sistem operasi di mana data disimpan (data at rest) dan dikirimkan (data in motion) melalui jaringan. Penelitian ini bertujuan untuk meningkatkan keamanan data dengan menerapkan metode kriptografi modern. Metode kriptografi yang digunakan meliputi RC4, AES, dan WPA3. Penetration testing dilakukan untuk menguji efektivitas dan efisiensi dari masing-masing metode kriptografi. Hasil penelitian menunjukkan bahwa penerapan kriptografi modern mampu memberikan lapisan keamanan tambahan terhadap ancaman keamanan data in motion dan data at rest di dalam sistem operasi.

Kata Kunci: Keamanan Data, Kriptografi Modern, RC4, AES, WPA3, Pengujian Penetrasi

1. PENDAHULUAN

Di era digital saat ini, data menjadi aset yang sangat berharga, baik bagi individu, organisasi, maupun bisnis. Data dapat dianalogikan sebagai "tambang emas" yang menyimpan informasi kritis, mulai dari data pribadi, finansial, hingga rahasia bisnis yang sangat penting. Pada sistem operasi, data ini tidak hanya disimpan (data at rest) tetapi juga dikirimkan (data in motion) melalui jaringan yang rentan terhadap ancaman keamanan seperti pencurian data, akses tidak sah, dan serangan siber (Hidayat & Sari, 2022). Oleh karena itu, menjaga keamanan data pada sistem operasi menjadi prioritas utama untuk melindungi integritas dan kerahasiaan informasi.

Kriptografi modern digunakan karena, efisiensi dan kinerja optimal pada perangkat modern, serta fleksibilitas dalam berbagai skema enkripsi. Kriptografi modern juga lebih tahan

Received: Juni 25, 2024; Revised: Juli 05, 2024 Accepted: Juli 21, 2024, 2024; Online available: Juli 22, 2024
* Rakhmadi Rahman, *meliodas00012@gmail.com*

terhadap serangan mutakhir, termasuk serangan kuantum dan serangan sampingan, serta didukung oleh komunitas penelitian aktif yang terus memperbarui dan meningkatkan algoritma untuk menghadapi ancaman baru (Kumar, P., Sahoo, G., & Routray, 2020).

Kriptografi modern hadir sebagai solusi untuk menjawab tantangan tersebut. Dengan menggunakan algoritma yang lebih canggih dan metode yang lebih kompleks, kriptografi modern mampu memberikan tingkat keamanan yang lebih tinggi. Implementasi kriptografi modern pada sistem operasi menjadi salah satu pendekatan strategis dalam menjaga keamanan data. Sistem operasi sebagai platform yang mengelola sumber daya dan operasi komputer memiliki peran krusial dalam memastikan bahwa data yang disimpan, diproses, dan ditransfer tetap aman dari ancaman.

Dalam konteks ini, peningkatan keamanan data melalui penerapan kriptografi modern pada sistem operasi bukan hanya relevan, tetapi juga mendesak. Dengan semakin banyaknya serangan yang menargetkan kelemahan sistem operasi, penting bagi para pengembang dan peneliti untuk terus mengembangkan dan mengimplementasikan solusi keamanan yang inovatif dan efektif (Munir, R, 2023). Dengan demikian, pengguna dapat memiliki kepercayaan lebih tinggi terhadap keamanan data mereka, yang pada akhirnya mendukung terciptanya lingkungan digital yang lebih aman dan terpercaya (Rahman, A. F., & Nugroho, 2021).

Metode kriptografi modern menawarkan solusi yang efektif untuk mengamankan data di kedua kondisi tersebut. Kriptografi tidak hanya memastikan bahwa data yang disimpan terlindungi dari akses tidak sah, tetapi juga menjamin bahwa data yang dikirimkan melalui jaringan tetap rahasia dan tidak dapat diubah oleh pihak yang tidak berwenang. Dengan menggunakan algoritma kriptografi yang canggih dan teknik enkripsi yang kuat, sistem operasi dapat meningkatkan lapisan keamanan data in motion dan data at rest secara signifikan, memberikan perlindungan yang lebih baik terhadap ancaman yang semakin kompleks di dunia maya.

2. METODE PENELITIAN

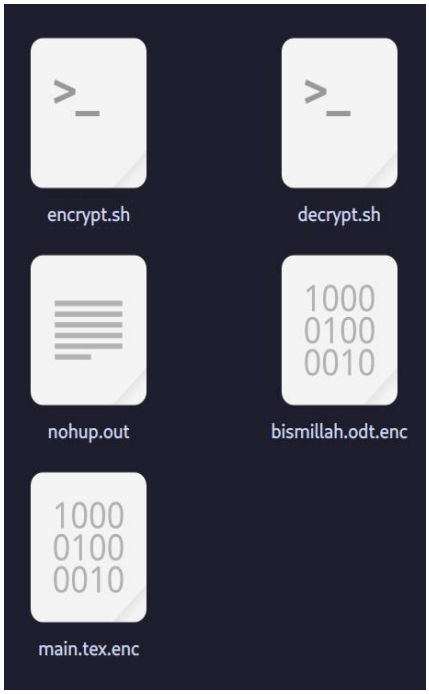
Metode yang digunakan dalam penelitian ini melibatkan tinjauan literatur, analisis komparatif terhadap berbagai metode kriptografi modern yang digunakan untuk mengamankan data pada sistem operasi. Dalam penelitian ini, keefektifan, kelebihan, dan kelemahan dari masing-masing metode dibandingkan dalam berbagai skenario penggunaan data in motion dan data at rest. Berdasarkan penelitian oleh Zaid dan Hashem (2021), diketahui bahwa AES sangat efisien dalam mengenkripsi data at rest, dilihat dari kecepatan enkripsinya, ukuran kunci, dan

strukturnya, sedangkan RC4 sangat efisien untuk enkripsi data secara realtime (Zaid & Hashem, 2021). Selain itu, dalam penelitian ini kami juga menggunakan metode terapan dengan harapan untuk memecahkan masalah sehingga hasil penelitian ini dapat dipergunakan secara luas baik oleh individu, hingga organisasi atau pelaku bisnis

3. HASIL DAN PEMBAHASAN

Pengujian sistem enkripsi AES

Dalam penggunaan ini, kami menggunakan script bash yang telah kami buat untuk mensimulasikan cara suatu perusahaan atau organisasi dapat menggunakan server SSH untuk meningkatkan keamanan data mereka.



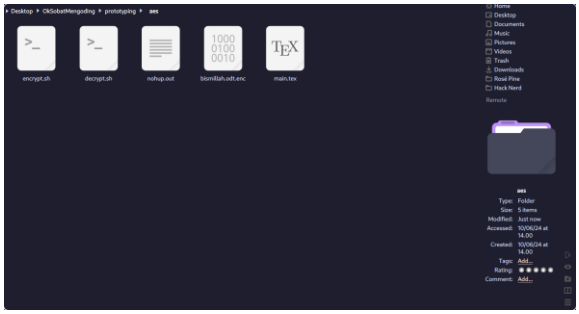
Gambar 1 Main.tex dimasukkan ke direktori yang akan mengenkripsi file

Pada tahap ini, script encrypt.sh akan dijalankan kemudian pengguna akan memasukkan file yang telah di desain khusus untuk mengenkripsi file yang masuk kedalamnya. File tersebut tidak akan bisa diakses oleh pihak yang tidak bertanggung jawab karena filenya telah terenkripsi.

```
~/Desktop/OkSobatMengoding/prototyping/aes ❯ john --format=raw-md5 --wordlist=wordlist.txt main.tex.enc          1m 4s 18:36:38

[mesinTempurAmek:1291170] shmem: mmap: an error occurred while determining whether or not /tmp/ompi.mesinTempurAmek.1000/jf.0/2
502230016/shared_mem_cuda_pool.mesinTempurAmek could be created.
[mesinTempurAmek:1291170] create_and_attach: unable to create shared memory BTL coordinating structure :: size 134217728
Warning: invalid UTF-8 seen reading main.tex.enc
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
```

Gambar 2 Melakukan uji coba penetrasi file yang terenkripsi menggunakan *JohnTheRipper*



Gambar 3 File main.tex kembali ke bentuk semula

Saat menjalankan skrip decrypt.sh, file main.tex akan kembali seperti semula, memberikan akses kepada pengguna untuk mengakses file tersebut.

Pengujian sistem enkripsi dengan RC4

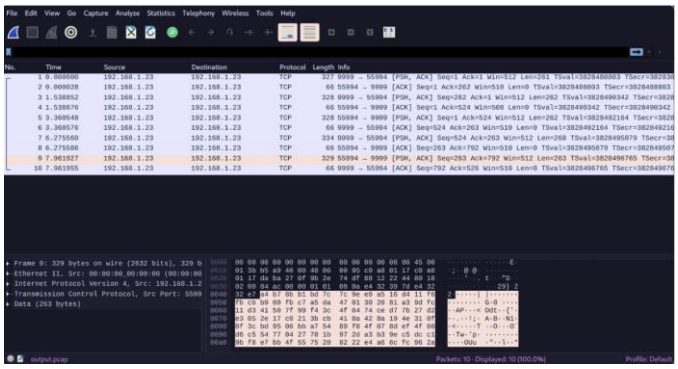
Dalam implementasi ini, kami mensimulasikan cara suatu perusahaan atau organisasi menggunakan *chat room* yang terhubung ke jaringan mereka sendiri untuk meningkatkan keamanan. Untuk melakukan ini, kami menambahkan enkripsi RC4 dan *signature* untuk meningkatkan keamanan.

```
~/Desktop/OkSobatMengoding/prototyping/RC4 > python3 enc
ryptchatprot1.py                                        09
:49:52
Apakah kamu ingin membuat sebuah room (1) atau masuk ke
room (2): 1
hi angga!
You: hi angga!
Partner: halo!
terkait pengembangan software yang sedang dilakukan, har
ap untuk menggunakan API KEY berikut : 0dd4$klja()#
You: terkait pengembangan software yang sedang dilakukan
, harap untuk menggunakan API KEY berikut : 0dd4$klja()#
harap untuk tidak menyebarkan API KEY tersebut ya!
You: harap untuk tidak menyebarkan API KEY tersebut ya!
Partner: siap pak!
```

Gambar 4 *Chat room* (1)

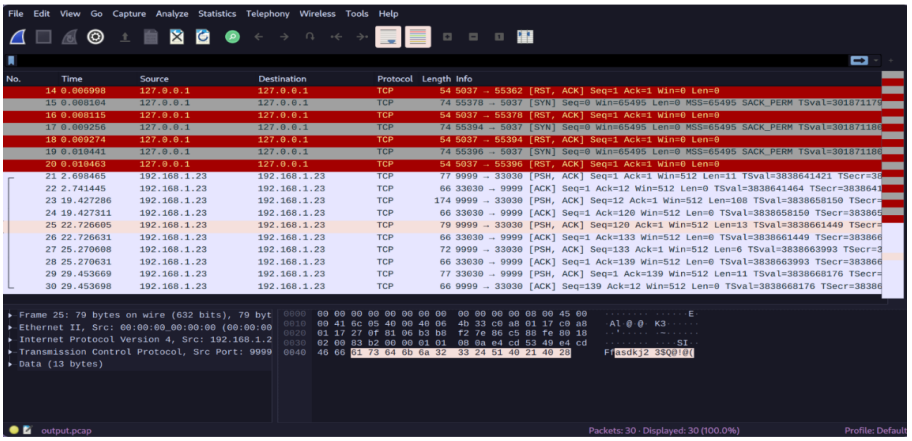
```
~/Desktop/OkSobatMengoding/prototyping/RC4 ❯ python3 encryptchatprot1.py
09:50:04
Apakah kamu ingin membuat sebuah room (1) atau masuk ke room (2): 2
Partner: hi angga!
halo!
You: halo!
Partner: terkait pengembangan software yang sedang dilakukan, harap untuk menggunakan API KEY berikut : 0dd4$kljaQ)#
Partner: harap untuk tidak menyebarkan API KEY tersebut ya!
siap pak!
You: siap pak!
```

Gambar 5 *Chat room* (2)



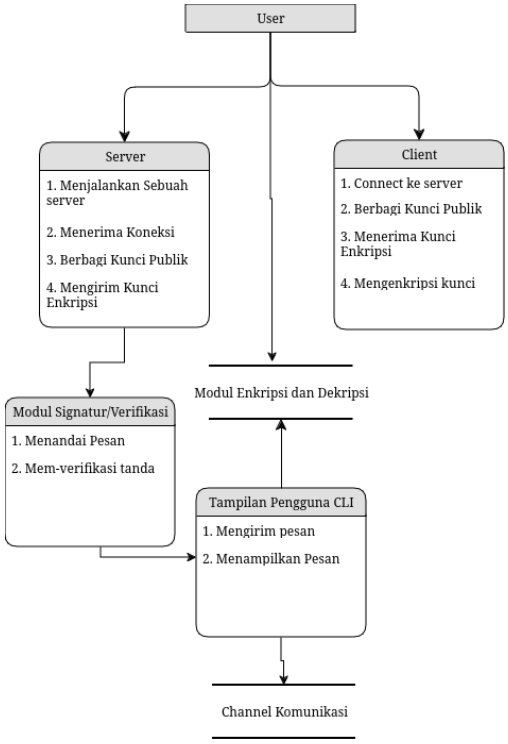
Gambar 6 serangan sniffing pada jaringan yang digunakan oleh chatroom

Dapat dilihat bahwa pada gambar 6 paket yang berlalu lintas pada jaringan tidak dapat dibaca oleh pihak yang tidak bertanggung jawab karena pesannya telah terenkripsi oleh RC4 dan tidak dapat juga di dekripsi karena tidak dapat melakukan verifikasi *signature* dan tidak adanya kunci dekripsi yang dimiliki oleh pihak ketiga



Gambar 7 Serangan *sniffing* pada jaringan yang digunakan oleh chatroom tanpa enkripsi dan *signature*

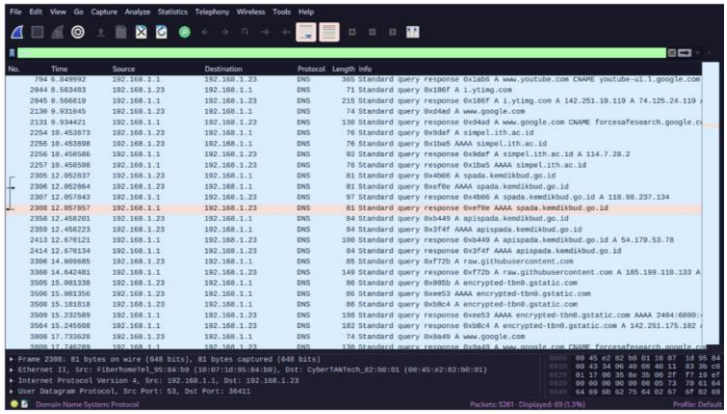
Sementara itu di gambar 7 paket yang berlalu lintas pada jaringan pada chatroom dapat dibaca dengan mudah, karena tidak di enkripsi oleh RC4 dan tidak ada verifikasi *signature*



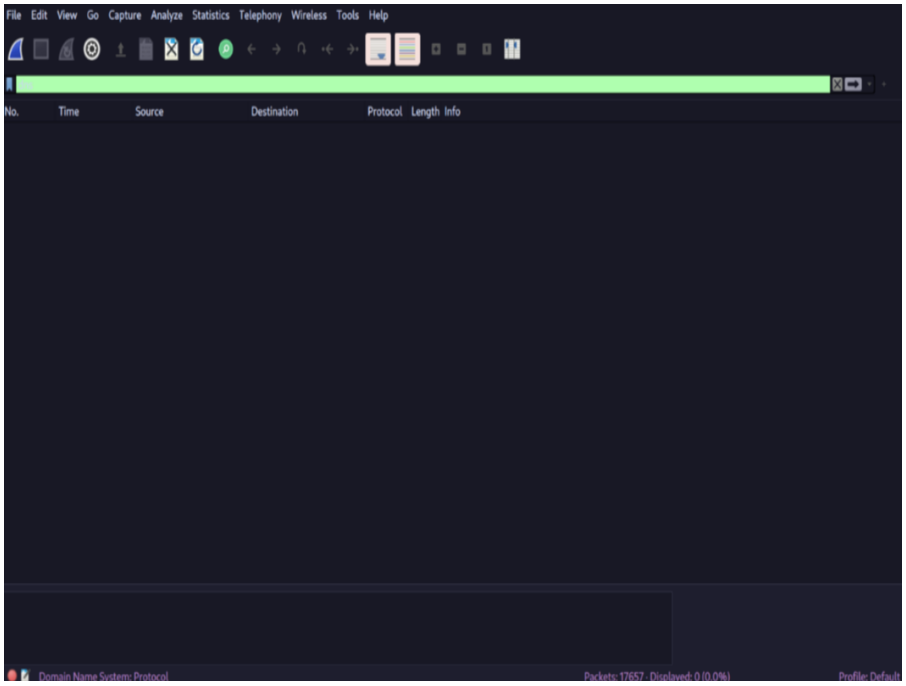
Gambar 8 Data Flow Diagram Level 1 Chatroom

Pengujian Sistem Enkripsi WPA3

Dengan menggunakan keamanan WPA3, suatu organisasi atau bisnis dapat melindungi keamanan jaringan mereka. Implementasi saat ini hanya tersedia apabila organisasi atau bisnis terkena serangan sniffing.



Gambar 9 Paket dari Jaringan Tanpa Keamanan WPA3



Gambar 10 Paket dari Jaringan dengan Keamanan WPA3

Perbandingannya sangat jelas, bahkan tidak terlihat dari trafik DNSnya. Ini menunjukkan bahwa dengan keamanan WPA3, lalu lintas DNS organisasi atau perusahaan masih aman bahkan dalam situasi terburuk jika jaringan dibobol.

4. SIMPULAN

Tiga teknik kriptografi modern yang digunakan dan diuji dalam penelitian ini untuk meningkatkan keamanan data baik dalam keadaan diam maupun dalam pergerakan, serta untuk melindungi jaringan nirkabel. Kami menyarankan untuk pengembangan tambahan. Pertama, gunakan teknik kriptografi ini di jaringan yang lebih luas, misalnya di lingkungan bisnis. Pengujian ini akan memberikan pemahaman yang lebih baik tentang kinerja dan efektivitas teknik kriptografi dalam lingkungan kehidupan nyata. Kedua, untuk memastikan keamanan yang optimal, tetap perbarui dan tingkatkan skrip dan aplikasi yang digunakan. Terakhir, lakukan pengujian lebih mendalam terhadap kinerja dan keamanan metode kriptografi, termasuk uji penetrasi, untuk menemukan kerentanan potensial. Pertimbangkan rekomendasi literatur dan penelitian terbaru tentang cara meningkatkan keamanan implementasi kriptografi. Metode kriptografi modern yang digunakan dalam penelitian ini akan efektif dalam memperkuat keamanan data di lingkungan yang lebih luas dengan menerapkan rekomendasi ini. Ini akan menjadi landasan yang kuat untuk langkah-langkah selanjutnya yang bertujuan untuk meningkatkan keamanan sistem informasi.

DAFTAR PUSTAKA

Hidayat, R., & Sari, D. P. (2022). Studi Komparatif Algoritma Kriptografi pada Sistem Operasi Mobile. Jurnal *Riset Informatika dan Sistem Informasi*, 14(3), 89-97.

Kumar, P., Sahoo, G., & Routray, S. K. (2020). Peningkatan Keamanan Data menggunakan Kriptografi pada Sistem Operasi. Jurnal Teknologi Informasi dan Komputer, 12(1), 15-22.

Munir, R. (2023) 'Kriptografi modern', PowerPoint slides, Institut Teknologi Bandung. Available at: http://www.itb.ac.id/presentations/kriptografi (Accessed: 17 June 2024).

Rahman, A. F., & Nugroho, A. D. (2021). Implementasi Algoritma Kriptografi Modern untuk Keamanan Data pada Sistem Operasi Berbasis Cloud. Jurnal Keamanan Siber dan Informatika, 5(2), 45-52.

Zaid, Mustafa & Hashem, Soukaena. (2021). Survey on Modern Cryptography. 10.31642/JoKMC/2018/070101.