ISSN 2962–5688
Website :
jurnal.umj.ac.id/index.php/TripleA
Email : triplea@umj.ac.id

TRIPLE A
Jurnal Pendidikan Teknologi Informasi

PUBLIC KEY INFRASTRUCTURE : KERANGKA VALIDASI YANG DISEMPURNAKAN

Syahreza Mitzardie Yacub [1*], Rikaro Ramadi[2*], Dani Ernawati [3*]
[1,2,3]Pendidikan Teknologi Informasi, Fakultas Ilmu Pendidikan, Universitas Muhammadiyah Jakarta, Jl. K.H. Ahmad Dahlan, Cireundeu, Kec. Ciputat Timur., Kota Tangerang Selatan, Banten 15419

[*] tarantula.brawl@gmail.com

ABSTRACT

Public Key Infrastructure (PKI) is a comprehensive information security framework for providing secure information and communication over the internet. This research work examines the current PKI framework validation process operated by vendors and customers to identify weaknesses and propose an improved approach to its validation mechanism. Using the approach of reviewing secondary data, critical weaknesses of integrity, trust proof and single point of failure are identified with the current PKI framework. Therefore, this research advances the proposed solution to address the identified weaknesses by specifically introducing multiple Certificate Authorities, storage, visibility and searchability of customer information in a public repository. Comprehensive details of its implementation are proposed to address the identified weaknesses of uncertain integrity, trust for certificate authorities and preventing single point of failure. Furthermore, the proposed enhancements are validated with protection motivation theory and a framework for empirically testing the enhancements is suggested.
Keywords*: Public Key Infrastructure, PKI Validation, Cyber Security*

ABSTRAK

Publik Key Infrastructure (PKI) adalah kerangka kerja keamanan informasi yang komprehensif untuk menyediakan informasi dan komunikasi yang aman melalui internet. Karya penelitian ini mengkaji proses validasi kerangka kerja PKI saat ini yang dioperasikan oleh vendor dan pelanggan untuk mengidentifikasi kelemahan dan mengusulkan pendekatan yang ditingkatkan untuk mekanisme validasinya. Menggunakan pendekatan meninjau data sekunder, kelemahan kritis integritas, bukti kepercayaan dan satu titik kegagalan diidentifikasi dengan kerangka kerja PKI saat ini. Oleh karena itu, penelitian ini memajukan solusi yang diusulkan untuk mengatasi kelemahan yang teridentifikasi dengan secara khusus memperkenalkan beberapa Otoritas Sertifikat, penyimpanan, visibilitas, dan kemudahan pencarian informasi pelanggan di repositori publik. Detail yang komprehensif dari implementasinya diusulkan untuk mengatasi kelemahan yang teridentifikasi dari integritas yang tidak pasti, kepercayaan untuk otoritas sertifikat dan mencegah satu titik kegagalan. Selanjutnya, perangkat tambahan yang diusulkan divalidasi dengan teori motivasi perlindungan dan kerangka kerja untuk menguji perangkat tambahan secara empiris disarankan.

Kata Kunci: *Infrastruktur Kunci Publik, Validasi PKI, Keamanan Siber*

DOI:https://

TRIPLE A: Jurnal Pendidikan Teknologi Informasi. Vol. 1 (2), pp: 77-80.

PENDAHULUAN

Public Key Infrastructure (PKI) adalah kerangka kerja yang digunakan dalam membuat dan mengelola sertifikat digital dan enkripsi kunci publik Esensinya adalah untuk mendukung transmisi data elektronik yang aman untuk berbagai fungsi jaringan seperti surat pribadi, e-commerce, dan perbankan berbasis internet. Kerangka kerja ini secara khusus memungkinkan untuk membuat, menggunakan, menyimpan, mengelola, mendistribusikan, dan membatalkan sertifikat digital serta mengelola enkripsi kunci publik. PKI adalah landasan untuk membangun komunikasi tepercaya di jaringan; lapangan telah berkembang sebagai pijakan untuk memberikan komunikasi data yang aman dan keamanan internet. “Identifikasi dan otentikasi, integritas data, kerahasiaan, dan non-repudiasi teknis digabungkan adalah elemen yang menyediakan lingkungan yang aman dan tidak dapat dipecahkan untuk semua jenis transaksi elektronik

PKI telah menjadi platform atau infrastruktur di mana layanan skema enkripsi simetris dan asimetris disediakan untuk semua orang yang berlangganan, oleh karena itu diperlukan dalam situasi di mana bukti yang lebih kuat sangat penting untuk memeriksa identitas pihak yang berkomunikasi dan mengotentikasi informasi. sedang ditransfer.

Penelitian ini bertujuan untuk memperluas pemahaman tentang infrastruktur PKI, metodenya, operasi dan teorinya, kemungkinan cara untuk meningkatkannya dan kelemahan yang melekat pada infrastruktur, kemungkinan peningkatan dan revisi di masa mendatang. Keluaran dan kontribusi penting dari penelitian ini menghasilkan proposal solusi untuk mengatasi kelemahan yang teridentifikasi dengan secara khusus memperkenalkan beberapa otoritas sertifikat, penyimpanan, visibilitas, dan kemudahan pencarian informasi pelanggan di repositori publik.

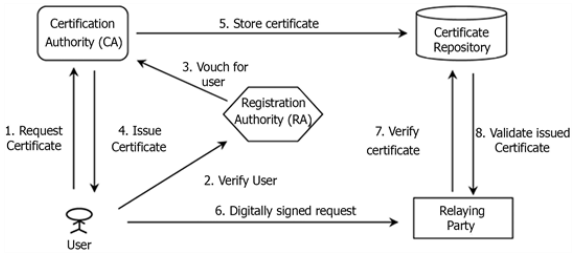
METODE PENELITIAN

Rastegari, Susilo, dan Dakhilalian mengusulkan kriptografi kunci publik tanpa sertifikat (CL-PKC) sebagai sarana untuk mengatasi masalah pengaturan berbasis PKI dan ID. “Dalam PKI konvensional, CA dianggap dipercaya sepenuhnya. Namun, dalam praktiknya, tanggung jawab mutlak CA untuk memberikan kepercayaan menyebabkan masalah keamanan dan privasi yang besar”. Oleh karena itu, arsitektur PKI baru diusulkan dengan "transparansi sertifikat berdasarkan blockchain yang disebut CertLedger, untuk menghilangkan serangan dunia terpisah dan untuk memberikan transparansi sertifikat/pencabutan". Ini belum digunakan secara luas untuk pengujian menyeluruh.

Implementasi Sistem

Metode dan Algoritma Enkripsi Kunci Publik berevolusi dari Rivest, Shamir, dan Adleman (RSA) dan didasarkan pada skema faktorisasi bilangan bulat, pertukaran Kunci Diffie-Hellman didasarkan pada skema logaritma diskrit, Digital Signature Algorithm (DSA) berdasarkan Elgamal enkripsi atau algoritme tanda tangan digital, Elliptic curve Diffie-Hellman key exchange (ECDH) berdasarkan skema kurva Elliptic dan algoritme tanda tangan digital kurva Elliptic yang didasarkan pada kurva eliptik yang dapat menawarkan tahapan keamanan dengan kunci panjang pendek. Skema kunci publik dapat digunakan untuk menyediakan layanan seperti kerahasiaan, sertifikat digital, non-repudiasi, tanda tangan digital, integritas data, dan pembuatan kunci.

Sejumlah kelemahan telah diidentifikasi untuk PKI, sebuah laporan penelitian akademis yang ditulis oleh tim dari sekolah informatika dan komputasi di Universitas Indiana Bloomington, Bug perangkat lunak dan kesalahan interpretasi standar industri menyumbang 42% dari sertifikat SSL yang diterbitkan secara tidak benar.



Gambar 1. Validasi Sistem

SIMPULAN

Penggunaan PKI terus tumbuh dengan cepat; dengan internet of things (IoT) menjadi pendorong utama pertumbuhan ini, perangkat komputasi masa depan akan terus dalam tren yang semakin cepat, lebih bertenaga, lebih andal, dan lebih portabel. Kecenderungan kecepatan koneksi Internet broadband yang terus meningkat di masa depan akan terus bertambah cepat. Kemajuan teknologi terutama kecepatan koneksi internet yang meningkat membuat kecepatan koneksi internet tidak lagi menjadi batasan sistem online seperti dulu. Perangkat seluler mampu melakukan tugas komputasi desktop penuh dan akses internet broadband kecepatan tinggi. Memproses validasi dan verifikasi PKI dalam kerangka yang diusulkan ini akan memberikan manfaat yang dibutuhkan tanpa mengorbankan kinerja dan efisiensi karena perangkat komputasi dan platform internet keduanya mampu melakukan tugas komputasi tersebut. Setelah memajukan solusi yang diusulkan untuk mengatasi kelemahan yang teridentifikasi dengan secara khusus memperkenalkan beberapa Otoritas Sertifikat, penyimpanan, visibilitas, dan kemampuan pencarian informasi pelanggan di repositori publik, disarankan agar penelitian lebih lanjut dilakukan dalam otentikasi multi-faktor tanpa mengorbankan kinerja PKI secara keseluruhan.

DAFTAR PUSTAKA

Lynch (2017) Hashed Out.

https://www.thesslstore.com/blog/wide-world-pki

Homeland Security, DISA Provides Public Key Infrastructure Security for the Mobile Environment.

https://www.hstoday.us/subject-matter-areas/infrastructure-security/disa-provides-public-key-infrastructure-security-for-the-mobile-environment

Ricks, M., Simakov, S. and Rabourn, S. (2014) Securing Public Key Infrastructure (PKI). Microsoft IT Information Security and Risk Management, 126.

Doowon, K., Kwon, B.J. and Dumitras, T. (2017) Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI.

Soltani, S.Z. (2013) Improving PKI Solution Analysis in Case of CA Compromisation.

Höglund, J., Lindemer, S., Furuhed, M. and Raza, S. (2020) PKI4IoT: Towards Public Key Infrastructure for the Internet of Things. Computers & Security, 89, Article ID: 101658. https://doi.org/10.1016/j.cose.2019.101658

Dudovskiy, J. (2018) The Ultimate Guide to Writing a Dissertation in Business

Studies: A Step-by-Step Assistance. Sage Publications, New York.

Adams, C. and Lloyd, S. (2003) Understanding Public-Key Infrastructure. Macmillan Technical Pub., Indianapolis.

Choudhury, S., Bhatnagar, K. and Haque, W. (2002) Public Key Infrastructure Implementation and Design. M&T Books, New York.

Rastegari, P., Susilo, W. and Dakhilalian, M. (2019) Certificateless Designated Verifier Signature Revisited: Achieving a Concrete Scheme in the Standard Model. International Journal of Information Security, 18, 619-635.

https://doi.org/10.1007/s10207-019-00430-5

Kubilay, M.Y., Kiraz, M.S. and Mantar, H.A. (2019) CertLedger: A New PKI Model with Certificate Transparency Based on Blockchain. Computers and Security, 85, 333-352. https://doi.org/10.1016/j.cose.2019.05.013

Karatsiolis, E., Wiesmaier, A. and Buchmann, J. (2013) Introduction to Public Key Infrastructures. Springer-Verlag, New York.

Sinnott, R. (2011) Public Key Infrastructure.

https://www.researchgate.net/figure/A-public-key-infrastructure_fig1_220566584

Sheets, D. (2019) Trusted Computing.

https://www.militaryaerospace.com/trusted-computing/article/14035441/trusted-computing-algorithms-asymmetric

Kessler, G.C. (2019) An Overview of Cryptography.

https://www.garykessler.net/library/crypto.html#skc