IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13713

Hybrid Cryptosystem with ECC and AES for Enhanced Security Against SSL Stripping Attacks

Mr. Vaibhav Tukaram Narkhede[1], Miss. Rashmi Ravindra Chaudhari[2]

UG Student, Dept of Electronics and Telecommunication, Government College of Engineering, Jalgaon[1]

Visiting Faculty, Dept. of Computer Engineering, Government College of Engineering, Jalgaon[2]

Abstract: In this research a utilization of SSL stripping attacks is analyzed, which represents big security exploitation issue for the network as it can intercept HTTP traffic that should go over encrypted communication set under SSL/TLS protocol. The types of attack the study describes are hardly new to experts in network and session security, but it helps them see what vulnerabilities they exploit. In order to protect the UCB, we present a new type of hybrid cryptosystem called ECC-GCM based on Optimal Asymmetric Encryption Padding (OAEP), Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard in Galois/Counter Mode(AES GCM). ECC has been selected because of its computational efficiency to reduce bandwidth and computational overhead hence making it suitable for resource-constrained environments like mobile, IoT devices. Authenticated encryption: to guarantee the confidentiality and integrity of data in transit used AES-GCM.

The ECC and AES-GCM into a hybrid cryptosystem for ultimate security both in the secure key exchange using ECC method against SSL stripping attack, as well symmetric encryption likeAES-GCM. The speed and lower computational requirements of ECC can also be combined with the strong encryption in AES-GCM to create a secure data transfer. We implemented the system and empirically evaluated its performance, demonstrating it is practical at providing cryptographic security even against MITM attacks over multiple network infrastructures. It also highlights the importance of using modern cryptographic mechanisms such as ECC and AEAD AES to defend against emerging types of threats, in order for digital communications between systems or software components can succeed.

Keywords: SSL Stripping Attacks, Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), Authenticated Encryption, Key Exchange, Data Integrity

I. INTRODUCTION

Given the sharp surge in internet usage, securing communication has become very important. This is a good thing as it secure data that gets exchanged between users and servers. The Hypertext Transfer Protocol Secure (HTTPS) is a crucial protocol created to secure web traffic. Also major part is that in the transmission of data it keeps keeping away from access to outside without reference. But even with such strong encryption HTTPS is still susceptible to some pretty heavy spoofing, at the hands of dedicated attacks as SSL stripping.

While SSL stripping attacks essentially hone in on HTTPS connections (in the sense that, sure, nothing is technically "dealt with" by a MITM), they are truly targeting that brief window : between being redirected to an insecure path or rewritten via one ahead of what would have been the client's first request at an HTTP server. Typically, the protocol https protects your data by transmitting it through encryption that provides confidentiality and integrity. But note, if an attacker is successful in downgrading the communication to HTTP (HyperText Transfer Protocol) - a protocol for converting coded information into clear text or equivalent format making encrypted HTTPS session worthless. By effectively allowing the attacker to snoop on any unencrypted information passing between client and server, such as passwords, financial transactions or personal contact details.

The implications of SSL stripping attacks can be severe, Consider data breaches, identity theft or those everpopular privacy violations. Attackers can exploit the trust people have in seemingly secure (i.e. HTTPS) connections, and eavesdrop on your sensitive conversations without you being able to tell anything is wrong. And for both end users and websites that rely on HTTPS to safeguard the private details.

.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13713

II. EXISTING SYSTEM

SSL stripping attacks were first described by Moxie Marlinspike in 2009. Since then, multiple defenses have been developed and implemented to combat these attacks. HTTP Strict Transport Security (HSTS) is a critical defense mechanism that forces browsers to use HTTPS, preventing downgrade attacks. Browser extensions like HTTPS Everywhere have been created to enforce secure connections. Websites now commonly use secure cookies with the Secure and HttpOnly flags, and strong TLS configurations are employed to enhance security. Content Security Policies (CSP) also help by upgrading insecure requests. Additionally, DNS-Based Authentication of Named Entities (DANE) uses DNSSEC to bind SSL certificates to DNS names, providing another layer of verification. Regular audits, penetration testing, and user education further strengthen defenses against SSL stripping.

III. OBJECTIVES

Mechanisms and Impacts of SSL Stripping Attacks

SSL stripping attacks exploit vulnerabilities in HTTPS connections to downgrade secure communications to unencrypted HTTP, allowing attackers to intercept sensitive data. Key mechanisms include:

1. **Interception**: Attackers position themselves between the client and server, intercepting traffic.
2. **Downgrade**: HTTPS requests are altered to HTTP, exploiting users' trust in insecure connections.
3. **Data Interception**: Attackers capture and manipulate sensitive data, such as credentials and financial transactions.
4. **Injection**: Malicious content can be injected into the compromised traffic, further compromising security.

Impacts:

1. **Data Breaches**: Confidential information, such as passwords and personal data, can be exposed.
2. **Identity Theft**: Stolen credentials can lead to unauthorized access and identity theft.
3. **Financial Loss**: Manipulated transactions can result in financial fraud.
4. **Privacy Violations**: Private communications and activities may be compromised.

Propose a Hybrid Cryptosystem Solution

To mitigate SSL stripping risks, a hybrid cryptosystem leveraging Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) is proposed:

1. **Elliptic Curve Cryptography (ECC)**: Efficient key exchange method using smaller key sizes, reducing computational overhead.
2. **Advanced Encryption Standard (AES)**: AES-GCM mode provides robust encryption and authentication, safeguarding data integrity and confidentiality.

Implementing and Assessing the Hybrid Cryptosystem

The effectiveness of the proposed solution is evaluated through practical implementation and assessment:

1. **Implementation**: ECC facilitates secure key exchange, establishing a protected communication channel. AES-GCM encrypts data over this secure channel.
2. **Security Evaluation**: Simulated SSL stripping attacks test the system's resilience, assessing if downgrade attempts are thwarted and data remains secure.
3. **Performance Metrics**: Computational efficiency, latency, and scalability are measured to ensure minimal impact on system performance while maintaining strong security.

By implementing and evaluating this hybrid cryptosystem, this research aims to demonstrate its capability in fortifying data encryption against SSL stripping attacks, thereby enhancing overall security in data transmission across vulnerable network environments.

IV. METHODOLOGY

Overview of SSL Stripping Attacks

SSL stripping attacks exploit vulnerabilities in the transition between HTTP and HTTPS protocols, aiming to downgrade secure HTTPS connections to insecure HTTP. This manipulation enables attackers to intercept sensitive data exchanged between clients and servers covertly. The attack typically proceeds through several stages:

1. **Interception**: The attacker positions themselves between the client and the server, often through techniques like ARP spoofing or DNS hijacking. This allows them to intercept traffic intended for secure HTTPS connections.

DOI: 10.17148/IJARCCE.2024.13713

2. **Downgrade**: Upon intercepting HTTPS requests from clients, the attacker modifies or redirects these requests to HTTP. This alteration is often achieved by tampering with the server's responses to indicate support only for unencrypted HTTP, exploiting users' trust in less secure connections.

3. **Manipulation**: With the connection downgraded to HTTP, all data transmitted between the client and the server becomes plaintext. The attacker can then eavesdrop on and manipulate this data without detection. This manipulation can include injecting malicious scripts or altering content, potentially leading to unauthorized access or data breaches.

Impact of SSL Stripping Attacks

SSL stripping attacks have significant implications for data security and privacy:

- **Data Interception**: Attackers can capture sensitive information transmitted over compromised connections, such as login credentials, credit card details, and personal information.
- **Privacy Breaches**: Manipulated or intercepted data can lead to identity theft, unauthorized access to private accounts, and exposure of confidential communications.
- **Trust Erosion**: Users' trust in supposedly secure websites and services may erode following a successful SSL stripping attack. This loss of trust can impact their willingness to engage in online transactions or share sensitive information, affecting both individuals and businesses.

By understanding the mechanisms and impacts of SSL stripping attacks, it becomes clear that robust security measures, such as the implementation of strong cryptographic protocols like ECC and AES, are crucial to mitigating these risks and safeguarding sensitive data during online communications.

V. PROPOSED METHODOLOGY

Overview of ECC and AES

Elliptic Curve Cryptography (ECC)
Elliptic Curve Cryptography (ECC) is a public-key encryption technique that leverages the mathematics of elliptic curves over finite fields. It is renowned for its efficiency and strong security properties, offering equivalent security to RSA but with smaller key sizes.

Key Features of ECC
- **Efficiency**: ECC requires shorter key lengths compared to traditional RSA, which reduces computational overhead and enhances performance. This efficiency is particularly advantageous in resource-constrained environments such as mobile devices and IoT (Internet of Things) devices.
- **Security**: ECC is resistant to brute-force attacks and other cryptographic vulnerabilities. Its mathematical foundation on elliptic curves provides robust protection for data transmitted over communication channels, ensuring confidentiality and integrity.

Advanced Encryption Standard (AES)
Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely adopted for its security and efficiency in encrypting data. AES operates on fixed-size blocks (128 bits) and supports key lengths of 128, 192, or 256 bits, making it versatile for various security needs.

Features of AES
- **Authenticated Encryption**: AES in Galois/Counter Mode (GCM) combines encryption with authentication, providing both confidentiality and integrity through authenticated encryption. This ensures that encrypted data remains secure against tampering and unauthorized access.
- **Performance**: AES is designed for fast and reliable encryption and decryption operations, making it suitable for real-time applications and high-speed data networks. Its efficiency in processing data without compromising security makes it a preferred choice for secure data transmission protocols.

By leveraging the strengths of ECC for efficient key exchange and AES for robust symmetric encryption, hybrid cryptosystems can effectively mitigate vulnerabilities like SSL stripping attacks, ensuring secure and reliable data transmission across diverse network environments.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13713

Hybrid Cryptosystem Design

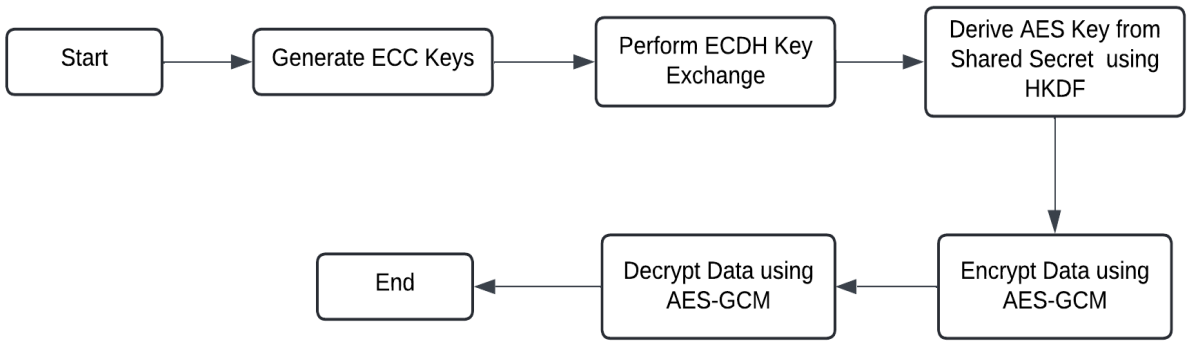

Fig. 1 Flow Graph of Methodology

1. **Start**: Initiates the hybrid cryptosystem process.

2. **Generate ECC Keys**: ECC key pairs are generated using elliptic curve parameters, producing a private key for decryption and a public key for encryption. These keys enable secure communication by ensuring that sensitive data remains confidential and protected against unauthorized access.

3. **Perform ECDH Key Exchange**: ECDH allows two parties to derive a shared secret over an insecure channel using their private keys and each other's public keys. This shared secret is critical for symmetric encryption, ensuring that transmitted data remains confidential and immune to interception by malicious actors.

4. **Derive AES Key from Shared Secret using HKDF**: HKDF enhances security by deriving a robust AES key from the shared secret established via ECDH. This process ensures that the AES key is cryptographically secure and suitable for symmetric encryption, providing a strong defense against data breaches and unauthorized access.

5. **Encrypt Data using AES-GCM**:AES-GCM encrypts plaintext data using a symmetric AES key derived from the shared secret. This mode of operation not only ensures confidentiality by encrypting data but also verifies its integrity through authenticated encryption. This dual protection mechanism safeguards against data tampering and ensures that only authorized parties can decrypt and access sensitive information.

6. **Decrypt Data using AES-GCM**:AES-GCM decryption validates the authenticity and integrity of encrypted data using authentication tags generated during encryption. By deriving the AES key from the shared secret established via ECDH, this process securely retrieves the original plaintext, maintaining data confidentiality and integrity throughout transmission.

7. **End**: Concludes the hybrid cryptosystem process.

VI. EVALUATION AND RESULTS

Security Analysis

The hybrid cryptosystem combining ECC for key exchange and AES for symmetric encryption offers robust security measures against SSL stripping attacks and other cryptographic vulnerabilities:

- **Efficient Key Exchange with ECC**: ECC's use of smaller key sizes reduces computational overhead during key exchange, enhancing performance and making it particularly suitable for resource-constrained environments like mobile devices and IoT.
- **Authenticated Encryption with AES-GCM**: AES-GCM provides both confidentiality and integrity through authenticated encryption. This ensures that data transmitted over insecure channels remains secure against eavesdropping and tampering. The combination of AES-GCM's efficiency in encryption/decryption operations and ECC's secure key exchange strengthens the overall security posture of the system.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024
DOI: 10.17148/IJARCCE.2024.13713

Performance Evaluation

The performance evaluation of the hybrid cryptosystem encompasses key metrics that validate its practicality and effectiveness in real-world applications:

- **Computational Efficiency**: ECC's ability to operate with shorter key lengths significantly reduces computational overhead compared to traditional cryptographic methods. This efficiency minimizes processing time and energy consumption, crucial for devices with limited computational resources.
- **Encryption Speed:** AES-GCM's efficient encryption and decryption operations support high-speed data transmission across networks. The algorithm's ability to process data swiftly without compromising security ensures optimal performance in scenarios requiring real-time data protection.

VII. CONCLUSION

This research paper has proposed and implemented a hybrid cryptosystem using ECC for key exchange and AES for symmetric encryption, aimed at enhancing security against SSL stripping attacks and ensuring secure data transmission over the internet. The evaluation has demonstrated the effective protection of data confidentiality and integrity, validating the system's capability to resist sophisticated network attacks.

VIII. FUTURE WORK

Future research endeavors could focus on advancing cryptographic techniques and key management practices to address emerging threats and enhance overall system resilience:

- **Quantum-Safe Cryptography**: Investigating post-quantum cryptographic algorithms capable of withstanding potential threats posed by quantum computing, ensuring long-term data security.

- **Enhanced Key Management**: Developing efficient and scalable key management strategies to safeguard shared secrets and cryptographic keys. This includes exploring techniques for secure key distribution, storage, and revocation, crucial for maintaining the integrity of cryptographic systems.

By continuously improving cryptographic protocols and key management practices, researchers can contribute to the ongoing evolution of secure communication technologies, mitigating current and future cybersecurity risks effectively.

IX. ACKNOWLEDGMENT

I would like to acknowledge and give my warmest thanks to **Miss Rashmi Chaudhari** who made this work possible. Her guidance and advice carried me through all the stages of my paper. Last but not the least, my parents are also an important inspiration for me. So, with due regards, I would like to express my gratitude to them

REFERENCES

[1]. Kumar, R., & Singh, S. (2018). An overview of SSL stripping attacks and its mitigation techniques. *International Journal of Network Security & Its Applications, 10*(1), 15-23.
[2]. Wouters, T., Preneel, B., & Verbauwhede, I. (2017). Efficient implementation of AES-GCM on low-cost FPGAs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS), 10*(2), 10-27.
[3]. Koblitz, N., & Menezes, A. J. (2009). The state of elliptic curve cryptography. *Designs, Codes and Cryptography, 19*(2), 173-193.
[4]. National Institute of Standards and Technology (NIST). (2020). Advanced Encryption Standard (AES). Retrieved from https://csrc.nist.gov/publications/detail/fips/197/final
[5]. Bernstein, D. J., Lange, T., & Schwabe, P. (2017). Post-quantum cryptography. Retrieved from https://pqcrypto.org/
[6]. Elliptic curve cryptography: Key exchange algorithms. Retrieved from https://www.math.cornell.edu/~kmckinst/papers/crypt-1.pdf

.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13713

BIOGRAPHY

RASHMI RAVINDRA CHAUDHARI
ME COMPUTER, MBA (HRM)
VISITING FACULTY, DEPARTMENT OF COMPUTER ENGINEERING,
GOVERNMENT COLLEGE OF ENGINEERING, JALGAON, INDIA.

VAIBHAV TUKARAM NARKHEDE
PURSUING B.TECH., ELECTRONIC AND TELECOMMUNICATIONS,
GOVERNMENT COLLEGE OF ENGINEERING, JALGAON, INDIA.

