Computer Network Security

Project Proposal COMP_3260

Submitted to: Dr. Anthony Aighobahi

Yassh Singh, Deyao Cao

T00690838, T00569950

Due Date: 11th October 2024

Hybrid IBE/PKI Integration with Risk-Based Automation for Enhanced Automated Certificate Management

Introduction:

The security of digital communication is crucial in today's interconnected world, where Public Key Infrastructure (PKI) systems play a central role in enabling encrypted data transmission. Automated certificate authorities like Let's Encrypt have made secure communication more accessible by simplifying certificate management. However, traditional PKI systems' reliance on centralized Certificate Authorities (CAs) creates vulnerabilities, as a compromised CA can jeopardize the security of all its issued certificates. Additionally, static revocation mechanisms such as Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP) struggle to address real-time threats effectively.

This project aims to enhance automated certificate management by integrating Identity-Based Encryption (IBE) into an existing PKI framework. Unlike traditional PKI, which relies on CAs to issue certificates tied to public keys, IBE uses a user's identity (e.g., email address) directly as the public key. This decentralizes key management and reduces the need for a trusted CA, as private keys are generated based on identity information. By combining IBE with traditional PKI, the proposed solution leverages the strengths of both approaches: the familiarity and compatibility of PKI, and the flexibility and reduced centralization of IBE. This hybrid system provides a more adaptable way to manage certificates, addressing limitations in traditional certificate issuance and distribution.

In addition, the project introduces a risk-based automation system for dynamic certificate revocation. This mechanism evaluates real-time threat indicators, such as multiple failed authentication attempts or unusual access patterns, and automatically revokes certificates when suspicious activity is detected. Unlike static revocation lists, this risk-based approach offers a proactive response to emerging security threats, enhancing the resilience of the hybrid IBE/PKI system. Together, these innovations aim to improve both the issuance and management of certificates, providing a comprehensive and resilient solution for secure digital communications.

Objectives:

The project focuses on improving automated certificate management through a hybrid approach that integrates Identity-Based Encryption (IBE) with traditional Public Key Infrastructure (PKI). The main objectives are:

1. **Integrate Identity-Based Encryption (IBE) into the PKI Framework**:
    - Implement a system where IBE is used alongside PKI to reduce dependence on centralized Certificate Authorities (CAs). In this hybrid model, IBE allows identity information (such as an email address) to function as the public key, making key management more decentralized and flexible.
    - The goal is to use IBE for internal encryption tasks, such as securing communication within an organization, while still employing PKI for issuing traditional certificates needed for external services. This combination aims to leverage the strengths of both IBE and PKI, enhancing the security and adaptability of the overall certificate management process.
2. **Develop a Risk-Based Automation System for Certificate Revocation**:

- Create a system that continuously monitors user activity and certificate usage to assess the risk level in real-time. If risky behaviors are detected—such as multiple failed login attempts, unusual access locations, or signs of key compromise—the system will automatically revoke the affected certificates.
- This risk-based automation aims to provide a proactive security measure that responds dynamically to potential threats, addressing the limitations of static revocation methods like Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP). The approach will enable faster and more effective mitigation of security risks.

Literature Review:

The paper "Reducing Trust in Automated Certificate Authorities via Proofs-of-Authentication" discusses the limitations of relying on centralized Certificate Authorities (CAs) for automated Public Key Infrastructure (PKI) systems, such as Let's Encrypt. The paper points out that while automated CAs simplify certificate issuance, they also introduce risks, as certificates can be issued without proper verification of the user's identity, leading to potential misuse or fraudulent certificates. To address this, the paper proposes embedding **proofs-of-authentication** in the certificates, ensuring that a certificate is only issued after successful user authentication has been verified. This solution aims to improve the integrity and trustworthiness of the certificate issuance process by making the authentication event a verifiable part of the certificate.

However, while embedding proofs of authentication enhances the **pre-issuance security** by ensuring that certificates are issued to legitimate entities, it does not fully address other vulnerabilities in PKI systems. Risks can still arise **after** a certificate is issued, such as if the certificate is compromised or if there is improper management of revocation. Traditional revocation mechanisms like **Certificate Revocation Lists (CRLs)** and **Online Certificate Status Protocol (OCSP)** are often slow and not effective in responding to real-time security threats, leaving a gap in post-issuance security.

To tackle these limitations, this project takes an alternative approach that extends beyond the **pre-issuance** focus of the paper. Instead of embedding proofs in the certificates, we propose **integrating Identity-Based Encryption (IBE)** within the PKI framework to improve the flexibility and security of certificate management. IBE allows for a decentralized approach where **identity information** (such as an email address) is used as the public key, reducing the dependency on traditional certificates issued by centralized CAs. By combining IBE with traditional PKI, we aim to create a hybrid system that benefits from both approaches: IBE for **internal encryption tasks** and PKI for **external communications**, thus reducing reliance on centralized authorities while retaining compatibility with existing infrastructure.
In addition to integrating IBE, the project introduces a **risk-based automation system for dynamic certificate revocation** to enhance **post-issuance security**. Unlike the paper's approach, which primarily focuses on ensuring authentication before certificate issuance, our solution involves **continuous monitoring** of user activity and certificate usage to dynamically assess risk. If potentially risky behaviors are detected—such as multiple failed login attempts, suspicious access patterns, or signs of key compromise—the system can **automatically revoke the affected certificates**. This risk-based automation provides a proactive security measure that responds to

threats in real-time, addressing the limitations of traditional static revocation methods like CRLs and OCSP.

By taking an alternative approach with a hybrid **IBE/PKI model** and adding a **risk-based automation system**, the project aims to provide a more comprehensive solution to improve both **pre-issuance** and **post-issuance security** in automated PKI systems. This approach not only seeks to reduce trust in centralized CAs but also introduces a dynamic mechanism to handle emerging threats, enhancing the overall resilience and adaptability of certificate management.

Methodology:

1. **Implement of Identity-Based Encryption (IBE) System**:
    - Set up a system using the **Charm-Crypto** library to generate private keys based on user identities (e.g., email addresses) for internal encryption. This reduces reliance on traditional certificates for internal purposes.
    - Use IBE for securing internal communications and data transfers.

    Tools: Charm-Crypto (for IBE), Python (for scripting encryption tasks).
2. **Integration with Public Key Infrastructure (PKI) for Certificate Management**:
    - Use **Certbot** with **Let's Encrypt** to automate the issuance and renewal of SSL/TLS certificates for external services. This ensures compliance with PKI standards while managing certificates automatically.
    - Build a hybrid system where IBE handles internal encryption and PKI manages external certificates.

    Tools: Certbot (for Let's Encrypt), OpenSSL (for certificate handling), Python (for scripting automation).
3. **Implemention Risk-Based Automation for Certificate Revocation**:
    - Set up the **ELK Stack** (Elasticsearch, Logstash, Kibana) to monitor user activity (e.g., failed logins, suspicious access patterns) and detect potential risks.
    - Automate certificate revocation using scripts that respond to risk assessments from the ELK Stack.

    Tools: ELK Stack (for monitoring), Python(for automating certificate revocation), Certbot and OpenSSL (for handling certificate management).
4. **Testing and Validation**:
    - Simulate risk scenarios like unauthorized access or key compromise to validate the system's risk-based revocation capabilities.
    - Assess how accurately the system detects risks and revokes certificates in real-time.

    Tools: Python testing frameworks (e.g., pytest) for automated tests, Kibana (for visualizing test results).

In Scope:

1. **Integration of IBE with PKI**:
    - Implement a hybrid system where IBE is used for internal encryption tasks, while PKI is used for external certificate management.

    - Configure the IBE system using a cryptographic library (e.g., Charm-Crypto), including the setup of the Private Key Generator (PKG) to issue private keys based on user identities.
2. **Automated Certificate Management with Let's Encrypt**:
    - Automate the issuance and renewal of SSL/TLS certificates for external services using Let's Encrypt and Certbot.
    - Develop a mechanism that allows the system to seamlessly switch between IBE for internal communications and PKI for external services.
3. **Risk-Based Automation for Certificate Revocation**:
    - Implement a risk assessment system using the ELK Stack to monitor user activity, assess login patterns, and identify risk indicators.
    - Create automation scripts that trigger the revocation of certificates or keys based on predefined risk thresholds, such as abnormal access patterns or multiple failed login attempts.
4. **Testing and Evaluation**:
    - Simulate risk scenarios (e.g., unauthorized access, key compromise) to validate the effectiveness of the risk-based revocation mechanism.
    - Assess system performance, including response time for automated revocation and the accuracy of risk detection.

Out of Scope:

1. **Physical Deployment on Hardware Devices**:
    - The project will be conducted in a virtual environment; physical implementation on hardware firewalls or dedicated devices is not included.
2. **Integration with Third-Party Cloud Security Services**:
    - The focus will be on local and automated certificate management without incorporating external cloud-based security services.
3. **Advanced Machine Learning for Risk Detection**:
    - While basic risk assessment will be performed using predefined criteria, sophisticated machine learning techniques for anomaly detection are beyond the project's scope.

Deliverables:

The project will produce the following key deliverables:

1. **Hybrid IBE/PKI System Prototype**:
    - A functional prototype integrating Identity-Based Encryption (IBE) with Public Key Infrastructure (PKI), demonstrating the use of IBE for internal encryption tasks and PKI for external certificate management.
2. **Automated Certificate Management Solution**:
    - An automated system for issuing, renewing, and managing SSL/TLS certificates using Let's Encrypt. The solution will include scripts and configurations for seamless integration between IBE and PKI.
3. **Risk-Based Automation for Certificate Revocation**:
    - A risk assessment system that dynamically monitors user activity and certificate usage using the ELK Stack. The system will automatically revoke certificates or keys based on predefined risk criteria.
4. **Documentation and Test Results**:

- Complete documentation covering system design, setup instructions, code explanations, and configuration details.
- A report summarizing the results of testing scenarios (e.g., failed logins, suspicious access) to evaluate the system's performance, including the effectiveness of the risk-based revocation mechanism.

5. **Final Presentation**:
   - A presentation summarizing the project's objectives, methodology, implementation, and key findings. The presentation will highlight the benefits and challenges of the hybrid IBE/PKI approach and the risk-based automation system.

Timeline:

The project is expected to be completed over a period of 8 weeks, with the following milestones:

Week 1-2: Research and Design

- Conduct research on IBE and PKI integration.
- Finalize system architecture for the hybrid IBE/PKI system and design the risk-based automation system for revocation.

Week 3-4: IBE and PKI Implementation

- Implement the IBE system using Charm-Crypto.
- Set up Let's Encrypt with Certbot for automated certificate issuance and renewal.
- Begin integrating IBE with PKI to handle both internal encryption and external certificates.

Week 5-6: Risk-Based Automation Implementation

- Implement the monitoring system using the ELK Stack to collect and analyze logs.
- Develop scripts for automating certificate revocation based on detected risk factors.
- Test initial functionality and begin refining based on feedback.

Week 7: Testing and Evaluation

- Simulate various risk scenarios (e.g., failed logins, abnormal access patterns).
- Measure system performance and assess the accuracy of the automated revocation mechanism.
- Make adjustments based on testing results.

Week 8: Final Documentation and Presentation

- Finalize documentation covering the system design, implementation steps, testing results, and recommendations.
- Prepare and deliver the final presentation summarizing the project outcomes and key findings.

Division of Responsibilities

Deyou's Role:

1. **Implement IBE System**:
   - Continue developing the **Identity-Based Encryption (IBE)** system and integrate it with the PKI infrastructure for hybrid key management, using IBE for internal encryption and PKI for external certificates.
2. **Manage Let's Encrypt**:
   - Set up and automate **Let's Encrypt** for SSL/TLS certificate issuance and renewal using **Certbot**, ensuring smooth integration with the hybrid system.

3. **System Design**:
    - Collaborate on the overall system architecture, ensuring effective interaction between the IBE and PKI components.

Yassh's Role:

1. **Develop Risk-Based Automation**:
    - Design and implement a **risk-based automation system** to monitor user activity, assess risks, and trigger certificate revocation based on real-time threats, using the **ELK Stack**.
2. **Integrate Automated Revocation**:
    - Build and integrate automated revocation scripts that dynamically revoke certificates and keys based on risk assessments, ensuring seamless operation with both IBE and PKI components.
3. **Testing and Validation**:
    - Perform system testing by simulating risk scenarios to validate the effectiveness of the revocation system, and refine as necessary based on results.

References

Newman, Z. (2023). *Reducing trust in automated certificate authorities via proofs-of-authentication*. arXiv. https://doi.org/10.48550/arXiv.2307.08201