Project Report

“Securing message through Cryptography using python”

By

Ravi teja

Final Year Undergraduate Student

CBIT,Hyd.

Under the Supervision of
Vishnu Vardhan
(Exposys Data labs)

Executed During
Internship Programme
At
Exposys Data Labs

EXPOSYS DATA LABS

CERTIFICATE

Certified that this is a bonafide record of the summer internship project work entitled

Securing message through Cryptography using python

Done by

M.Ravi teja

Of Department of Electrical and Electronics Engineering, CBIT during Aug-Sept 2022.

Vishnu Vardhan
(Project Guide)

Acknowledgement

I am very grateful to my project guide Vishnu Vardhan for giving his valuable time and constructive guidance in doing the Project. It would have not been possible to complete this project in this short period of time without his encouragement and valuable guidance.

Date: **Signature**

Name of the Student

(M.Ravi teja)

Index:

Note: Code library used in the project are all from Python 3.9

Introduction

The Cryptoanalysis is that the process of attempting to get the plain text and/ or the key.

Applications of varied Cryptographic Technologies. Why & the way to Provide Network Security within the Certificates issuing, The Validity & Trust for Certificate Services, Certificate Revocation within the Internet, Intranet and other Network Communications, the Applications of Network Security to the varied Data Transfer techniques and protocols.

From the dawn of civilization, to the highly networked societies that we sleep in Today communication has always been an integral part of our existence.

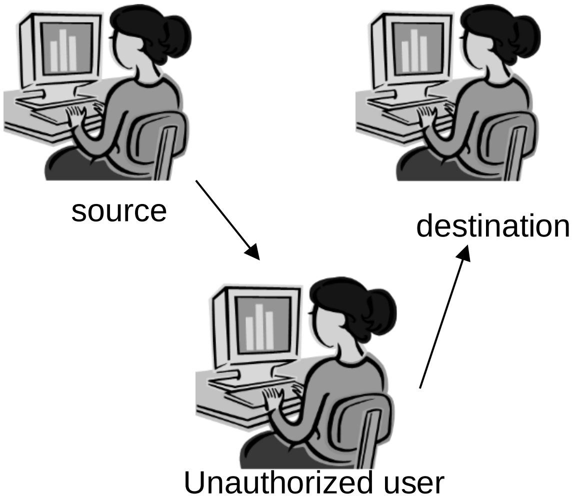
* Radio communication
* Network communication
* Mobile communication
* Telephonic communication

All these methods and means of communication have played a crucial role in our lives, but within the past few years, network communication, especially over the Internet, has emerged together of the foremost powerful.

Methods of communication with an awesome Impact on our lives. Such rapid advances in Communications technology have also given rise to Security threats to individuals and organizations.

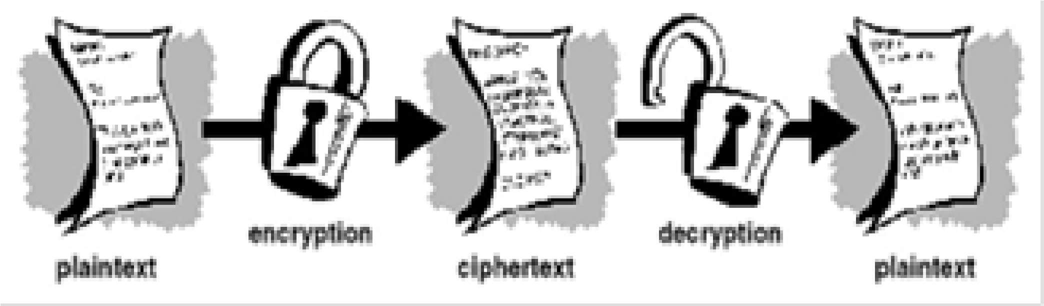
Fundamental Requirements

- Confidential: is that the process of keeping information private and Secret in order that only the intended recipient is able to know the knowledge.
- Authentication: is that the process of providing proof of identity of the sender to the recipient, in order that the recipient is often assured that the person sending the information is who and what he or she claims to be.
- Integrity: is that the method to make sure that information is not tampered with during its transit or its storage on the network. Any unauthorized person shouldn't be able to tamper with the knowledge or change the Information during transit.
- Non-repudiation: is that the method to make sure that information can't be disowned. Once the non-repudiation process is in situ, the sender cannot deny being the originator of the info, source, destination, Unauthorized user.



Security Attacks

- Interruption: In an attack where one or more of the systems of the organization become unusable thanks to attacks by unauthorized users. This results in systems being unavailable to be used.
- Interception: An unauthorized individual intercepts the message content and changes it or uses it for malicious purposes. After this sort of attack, the message doesn't remain confidential.
- Modification: The content of the message is modified by a 3rd party. This attack affects the integrity of the message. So, for maintaining the info secretly while communicating data between two persons or two organizations data is to be converted to other format and the data is to be transmitted. So now we affect the Cryptography which is process of transmitting data securely with none interruption. Network security is that the security of knowledge transmission within the communication.



What is Cryptography?

The term cryptology has its origin in Greek Krypto’s logos, which suggests “hidden word.” Cryptography is that the science of protecting data, which provides means and methods of converting data into unreadable form, in order that Valid User can access Information at the Destination. Cryptography is that the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) in order that it can't be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is that the science of analysing and breaking secure communication. Cryptanalysts also are called attackers. Cryptology embraces both cryptography and cryptanalysis. Cryptography Terminology are:

- Plaintext: the first intelligible message.
- Cipher text: The transformed message.
- Cipher: An algorithm for transforming an intelligible message to unintelligible by transposition.
- Key: Some critical information employed by the cipher, known only to the sender & receiver.
- Encipher :(Encode) the method of converting plaintext to cipher text employing a cipher and a key.
- Decipher :(Decode) the method of converting cipher text back to plaintext employing a cipher & key.
- Cryptanalysis: The study of principles and methods of remodelling an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking
- Cryptology: Both cryptography and cryptanalysis

- Code: an algorithm for transforming an intelligible message into an unintelligible one using codes.
- Hash algorithm: Is an algorithm that converts text string into a string of fixed length.
- Secret Key Cryptography (SKC): Uses one key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Pretty Good Privacy (PGP): PGP may be a hybrid cryptosystem.
- Public Key Infrastructure (PKI): PKI feature is Certificate authority.

Why do you have to Do a Third-Party Risk Assessment?

Creating and maintaining third-party relationships are related to multiple risks.

What sorts of risks?

Reputation, strategy, management, information security, and economic burdens. Other risks include data compromise, illegal use of data by third parties, the detrimental and damaging effects of non-compliance, and irregularities in supply chain management.

Particularly, the globalization of commercial operations has led third parties to emerge throughout the planet. In turn, the graph of operation- and distribution-related risks has seen an upward trend.

Any natural, artificial, or deliberate disruption in any a part of the fashionable world adversely affects the assembly and services offered by enterprises.

If a multinational enterprise lacks a robust risk management program to tackle such third-party risks, it's going to suffer economic also as reputational losses. This creates the necessity for efficient risk assessment and risk management and entails the look for effective associated assessment services.

How to Perform a Third-Party Risk Assessment

1. Establish Vendor Risk Criteria

Create an inventory of vendor risk criteria. It should include the foremost destructive third-party risks that your organization could possibly face.

For instance, enterprises managing or outsourcing confidential data should have various information security risks as a part of their vendor risk criteria.

This, in turn, informs your organization’s risk assessment scope. Additionally, it impacts your actions and methods and therefore the techniques you'll use for a third-party or vendor risk assessment. supported such risk criteria, you'll also narrow down your third-party or vendor choices.

This brings you to subsequent step for your risk management program: classifying vendors. Basically, you create an actionable list of high-risk third-parties with whom you'll perform risk assessments.

2. Conduct Third-Party Onboarding and Screening

To predict and protect against any possible risk, you want to create an in-depth picture of third-party or vendor relations. the primary step is to mandate standard processes of risk management throughout your company.

Experts suggest that you simply construct a third-party risk management program with a framework which will standardize all third-party onboarding and screening. If possible, you'll also use a radical approach of real-time risk checking and containment measures.

Well-designed frameworks for your risk management program offer a win-win situation:

You can keep up of any probable third-party risks (and risky vendors) before risk assessments. Furthermore, a framework for your risk management program will assist you optimize time and undertake insightful risk assessments.

3. Make Risk Assessments Easier to Manage

As the quality of your assessment will directly impact your risk management program, you want to make sure the quality of your assessments, simple check-box assessments don't suffice. For this purpose, you want to comprehensively analyse if any vendor is risky, why they're, and the way you (or they) can address those risks.

Thereafter, an agreement with a risky third-party will warrant meticulous and consistent monitoring.

Next, you'll require specialized experts who will aid within the analysis of the info you've got gathered. for instance, professionals from policy, tech, cybersecurity, or account backgrounds can conduct holistic analyses and issue detailed reports. Today, powerful organizations deploy entire teams for such risk analysis programs.

4. Assess Performance Results, Not Only Risks

Results are symptoms of whether and to what degree your third-party relations are risky. as an example, information security ratings will enable you to consistently supervise your vendors' compliance and unpredictable risks.

In case you've got contracts with multiple third parties, keeping tabs on their information security and compliance scores will:

Enhance and ease third-party risk assessment,

Note any faults with security posture; and

Demand solutions to risky problems of the involved third parties.

5. Leverage the facility of Technology

Capital and resource availability are essential prerequisites for undertaking vendor risk assessments. to save lots of on expenditures, you ought to consider purchasing and deploying software that eases the whole process of third-party risk assessment and management.

As a technology that gives assessment services, it'll also standardize a cross-departmental framework for risk assessment in your organization.

Technology utilization is crucial to conducting holistic and thorough risk assessments and management.

Why?

For variety of reasons, including:

- It gives you control over a platform through which you'll regularly supervise any number of third parties and therefore the related risks.
- It increases your ability to predict and analyse internal and external third-party risks while influencing your assessment scope.
- It helps you collect and macro-analyse solid data on third-party risks over multiple assessments, which can enhance your organization’s future decisions about any vendor.
- It enables you to measure the efficacy of risk assessment metrics, which marks the standard and reliability of your data.

Conclusion:

Today, companies and enterprises tend to prioritize third-party risk management in the wake of several global trends. Namely, accelerated outsourcing in a milieu of increased prices, dependence on digital technology, and the awareness that many organizational breaches originate from trusted vendors who have themselves been compromised.

Hence, the reason third-party risk assessments and risk management programs have become imperative.

Thank you..

Reference:

- Cryptography and Network Security –By William Stallings.
- Introduction to Cryptography –By Aysel Ozgur
- https://towardsdatascience.com/what-is-third-party-risk-assessment-and-how-can-you-do-it-ef3c69a6e0ce
- www.en.wikipedia.org