Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 8; April-June, 2015 pp. 98-100
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Cybercrime Network Security and Cryptograph

Parardha Kumar

Indian School of Mines, Dhanbad
E-mail: parardhakumar@gmail.com

Abstract— *The rising danger of crimes committed against computers and other information systems has begun to claim attention worldwide. There are new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists. We can win only through partnership and collaboration of both government and individuals. This paper will focus on cybercrime, network security and cryptography.*

1. INTRODUCTION

"The art of war teaches us not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

—The art of War, Sun Tzu

Cybercrime is an increasing concern in the www World. Cybercrime is something that could affect us all, although still undefined in any constitutional act. Cybercrime is any type of crime that occurs over the computer or by electronica means.All efforts to protect systems and networks attempt to achieve three outcomes: data availability, integrity, and confidentiality. And as we have also seen, no infrastructure security controls are 100% effective. In a layered security model, it is often necessary to implement one final prevention control wrapped around sensitive information: encryption

2. ATTACKS, SERVICES AND MECHANISMS

Any transferred information is vulnerable to three possible attacks: Interruption, Interception, Modification and Fabrication. The names used for these attacks are descriptive of their nature. Any action that compromises the information security is known as a Service Attack.

Security Services enhance the security of data processing and transferring while a Security Mechanism helps a system to detect, prevent and recover from a security attack.

3. CRYPTOGRAPHY

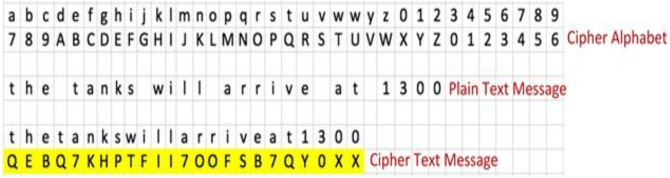
Encryption is not a security panacea. It will not solve all your data-centric security issues. Rather, it is simply one control among many.

Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. Achieving strong encryption, the hiding of data's meaning, also requires intuitive leaps that allow creative application of known or new methods.

So cryptography is also an art.

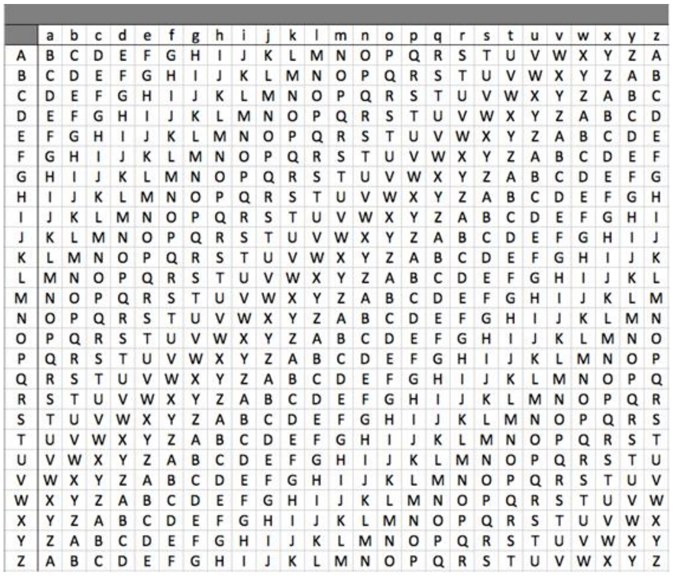
4. CIPHERS

A cipher is an algorithm for performing encryption or decryption. There are different types of ciphers. The most common ones are Vigenere Cipher, Monoalphabetic Substitution Ciphers, Transposition Ciphers etc.



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	w	y	z	0	1	2	3	4	5	6	7	8	9	
7	8	9	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	Cipher Alphabet
t	h	e		t	a	n	k	s		w	i	l	l		a	r	r	i	v	e		a	t		1	3	0	0	Plain Text Message							
t	h	e	t	a	n	k	s	w	i	l	l	a	r	r	i	v	e	a	t	1	3	0	0													
Q	E	B	Q	7	K	H	P	T	F	I	I	7	O	O	F	S	B	7	Q	Y	0	X	X	Cipher Text Message												

Monoalphabetic Substitution Shift Cipher



	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Vigenère Table

5. HOW CRYPTOGRAPHY HELPS IN REDUCING CYBERCRIME?

Cybercrime can be reduced by encrypting your data, proper key management, reducing attack surface etc. All these can be done using cryptography.

Cryptography provides the main principles of Key Management, i.e. Key Storage, Key protection and Key Strength.

6. WHEN TO ENCRYPT DATA?

Sensitive information must be protected at all times. Also, data moving from one zone to the other must be protected. When a data is important and is liable to be stolen, it must be encrypted. This helps in reducing attacks such as fabrication.

7. PREVENTION OF CYBERCRIMES

The processes underlying all widely accepted ciphers are and should be known, allowing extensive testing by all interested parties: not just the originating Cryptographer. The security of the encryption scheme must depend only on the secrecy of the key and not on the secrecy of the algorithm .

7.1 Principles of Key Management

Managing keys requires three considerations:

1. Where will you store them?

2. How will you ensure they are protected but available when needed?

3. What key strength is adequate for the data protected?

7.2 Key Storage

Many organizations store key files on the same system, and often the same drive, as the encrypted database or files. While this might seem like a good idea if your key is encrypted, it is bad security. What happens if the system fails and the key is not recoverable? Having usable backups helps, but backup restores do not always work as planned.

Regardless of where you keep your key, encrypt it. Escrow storage can be a safe deposit box, a trusted third party, etc. Under no circumstances allow any one employee to privately encrypt your keys.

7.3 Key Protection

Encrypted keys protecting encrypted production data cannot be locked away and only brought out by trusted employees as needed. Rather, keep the keys available but safe. Key access security is, at its most basic level, a function of the strength of your authentication methods. Regardless of how well protected your keys are when not used, authenticated users (including applications) must gain access.

7.3 Key Strength

Most, if not all, attacks against your encryption will try to acquire one or more of your keys. Use of weak keys or untested/questionable ciphers might achieve compliance, but it provides your organization, its customers, and its investors with a false sense of security. So what is considered a strong key for a cipher like AES? AES can use 128-, 192-, or 256-bit keys. 128-bit keys are strong enough for most business data, if you make them as random as possible. Key strength is measured by key size and an attacker's ability to step through possible combinations until the right key is found. However you choose your keys, ensure you get as close as possible to a key selection process in which all bit combinations are equally likely to appear in the key space.

8. AUTHENTICATION SYSTEMS

Authentication is about making sure that one can verify the identity of the person or entity he is dealing with. This isn't really a subversion of encryption itself, it just goes to show that encryption in itself is not a total solution. Digital certificates are used for authentication because the identity of the person or the business has been verified by the company that issued the Digital Certificate.

The main components of a good component system are

1. A security key (One has)

2. The password (One knows)

3. The fingerprint (One is)

8.1 Kerberos : A Common Authentication System

Kerberos is a free program and it is also included in many commercial products, including the newer versions of MS Windows. Kerberos works by providing users with "tickets" that are used to identify themselves to other users or computers. It also provides cryptographic keys for secure communication with other users.

9. ACKNOWLEDGEMENTS

This paper, entitled "Cybercrime, Network Security and Cryptography", would have been utterly impossible to be materialized if I could not have received the extraordinary support of my father and mother, who served as editors, and mentors.

Also, I am amazingly fortunate to have such knowledgeable grandparents and my professors at Indian School of Mines, Dhanbad. They gave important lectures which served as the soul of this project.

I dedicate this project to my brother Prajneya who has been by guide throughout the research.

REFERENCES

[1] http://www.cs.iit.edu/~cs549/lectures.

[2] https://technet.microsoft.com/en-us/library/cc962027.aspx

[3] http://resources.infosecinstitute.com/role-of-cryptography/

[4] McMillan, Robert. “Three Years Undercover With Cybercriminals.” 2009. 5 May 2009

[5] Ferguson, Schneier, &Kohno, 2010, p. 24.