Risk management

- Defense
  - Applying safeguards to to eliminate or reduce residual risks
- Transferal
  - Shifting risk to other areas or outside agencies
- Mitigation
  - Reducing the impact in the event of an attack (CP)
- Acceptance
  - Understanding the consequences of choosing to leave a risk uncontrolled
- Termination
  - Removing or disconnecting

Related terminologies

Risk control strategy	Categories used by NIST SP 800-30, Rev. 1	Categories used by ISACA and ISO/IEC 27001	Others
Defense	Research and Acknowledgement	Treat	Self-protection
Transfer	Risk Transference	Transfer	Risk transfer
Mitigation	Risk Limitation and Risk Planning	Tolerate (partial)	Self-insurance (partial)
Acceptance	Risk Assumption	Tolerate (partial)	Self-insurance (partial)
Termination	Risk Avoidance	Terminate	Avoidance

Justifying controls

- Before implementing one of the control strategies for a specific vulnerability, the organization must explore all consequences of vulnerability to information asset.
- Several ways to determine the advantages/disadvantages of a specific control
- Items that affect cost of a control or safeguard include cost of development or acquisition, training fees, implementation cost, service costs, and cost of maintenance.

Justifying controls (cont'd)

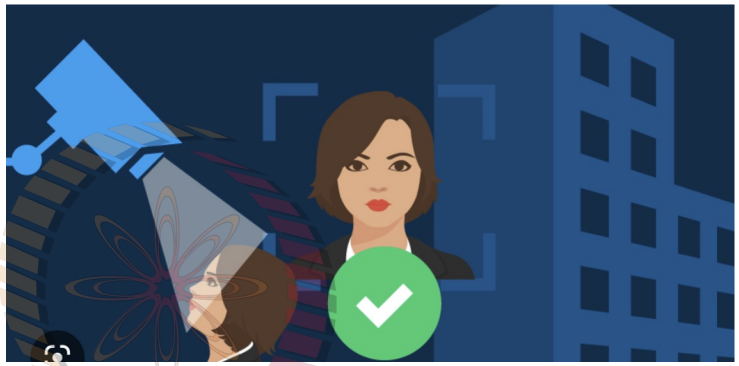
- Asset valuation involves estimating real/perceived costs associated with design, development, installation, maintenance, protection, recovery, and defense against loss/litigation.
- Process result is the estimate of potential loss per risk.
- Expected loss per risk stated in the following equation:
  - Annualized loss expectancy (ALE) = single loss expectancy (SLE) × annualized rate of occurrence (ARO)
- SLE [Loss magnitude] = asset value × exposure factor (EF)

The cost-benefit analysis (CBA)

- CBA determines if an alternative being evaluated is worth the cost incurred to control vulnerability.
  - The CBA is most easily calculated using the ALE from earlier assessments, before implementation of the proposed control:
    - CBA = ALE(prior) – (ALE(post) + ACS)
  - ALE(prior) is the annualized loss expectancy of risk before implementation of control.
  - ALE(post) is the estimated ALE based on control being in place for a period of time.
  - ACS is the annualized cost of the safeguard.

Implementation, monitoring, and assessment of risk controls

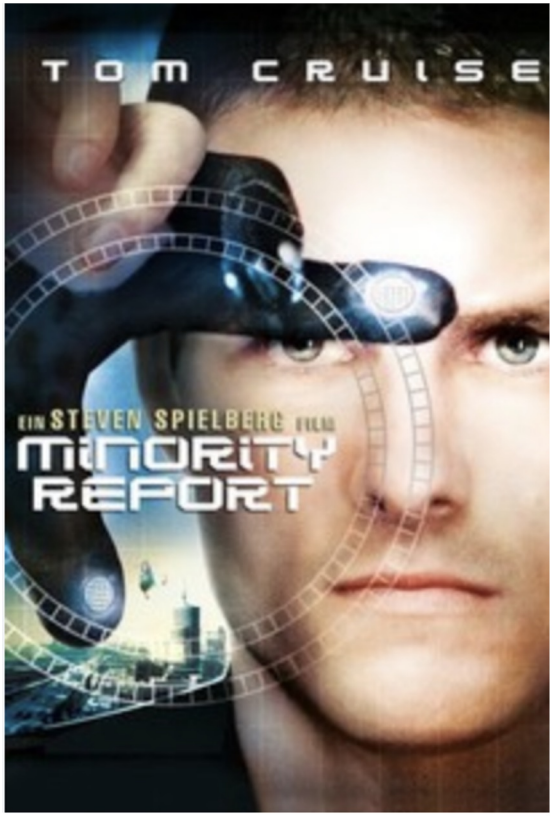
- The selection of the control strategy is not the end of a process.
- Strategy and accompanying controls must be implemented and monitored on ongoing basis to determine effectiveness and accurately calculate the estimated residual risk.
- Process continues as long as the organization continues to function.

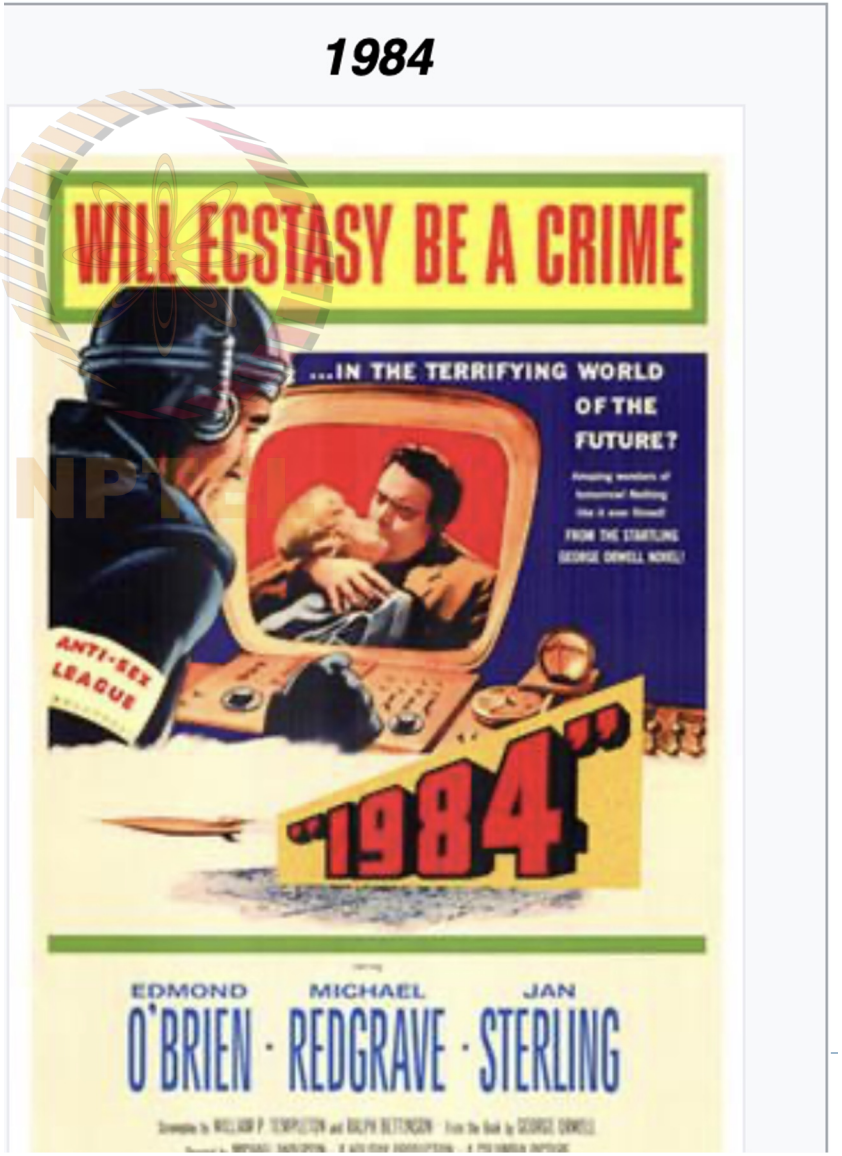


Cyber security technologies

Saji K Mathew, PhD
Professor, Management Studies
INDIAN INSTITUTE OF TECHNOLOGY MADRAS

Technology: Boon or a curse?





Access control

- Access control, key to Confidentiality and Integrity
- Enabled through policies, and technologies
- IAAA for access control
  - **I**dentification
  - **A**uthentication
  - **A**uthorization
  - **A**ccountability

IAAA for access control

- Identification
  - Get your ID
- Authentication
  - Something you know (password, passphrase, OTP)
  - Something you have (smart card)
  - Something you are (fingerprints, retina and iris scans)
  - Something you produce (voice, signature)

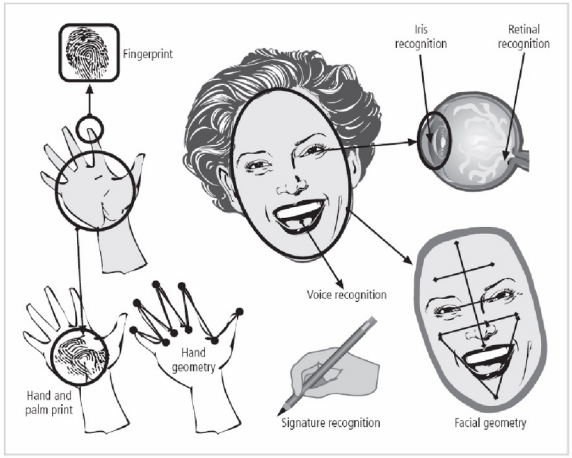


FIGURE 9-4 Recognition Characteristics

Evaluating biometrics

Cross Over Error Rate (CER)

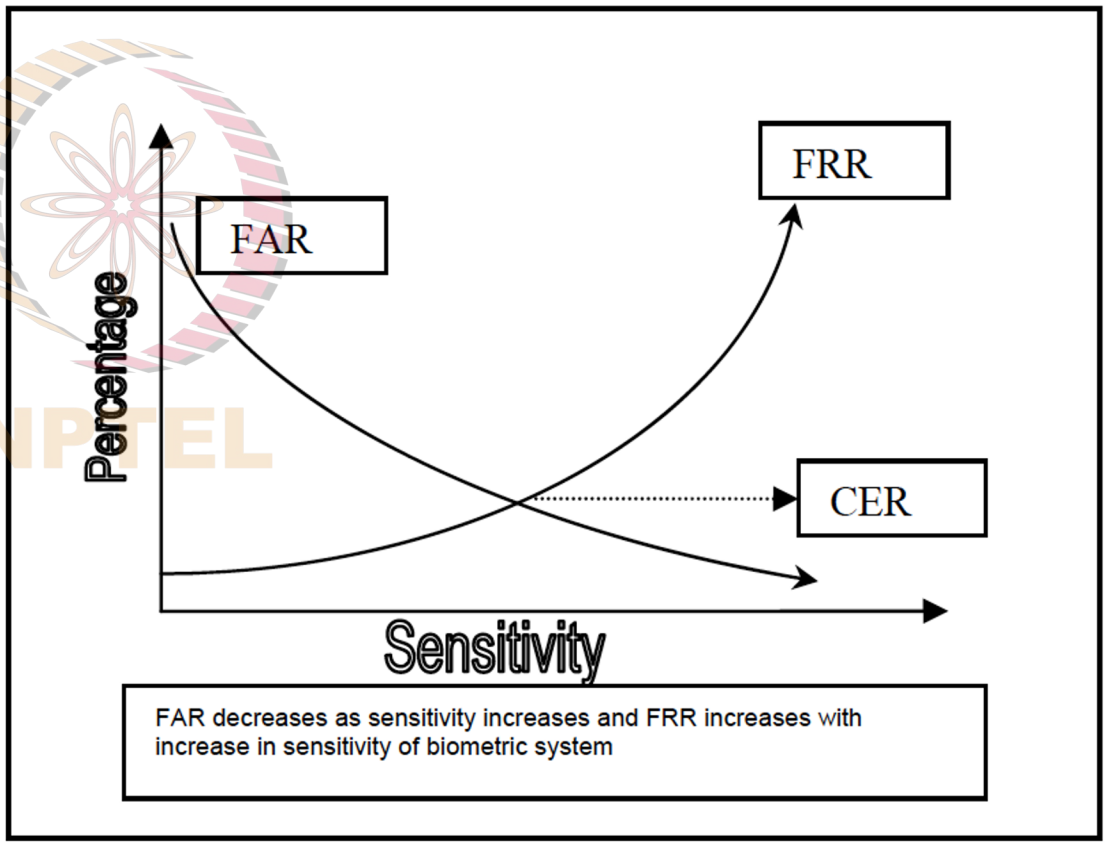
- FAR: False Acceptance Rate
  - FAR high: FP, TP high, FN low
- FRR: False Rejection Rate
  - FRR high: FP, TP low, FN high
- @CER: FAR=FRR

Widely used in comparison of biometric devices

What is a desirable CER for user authentication?

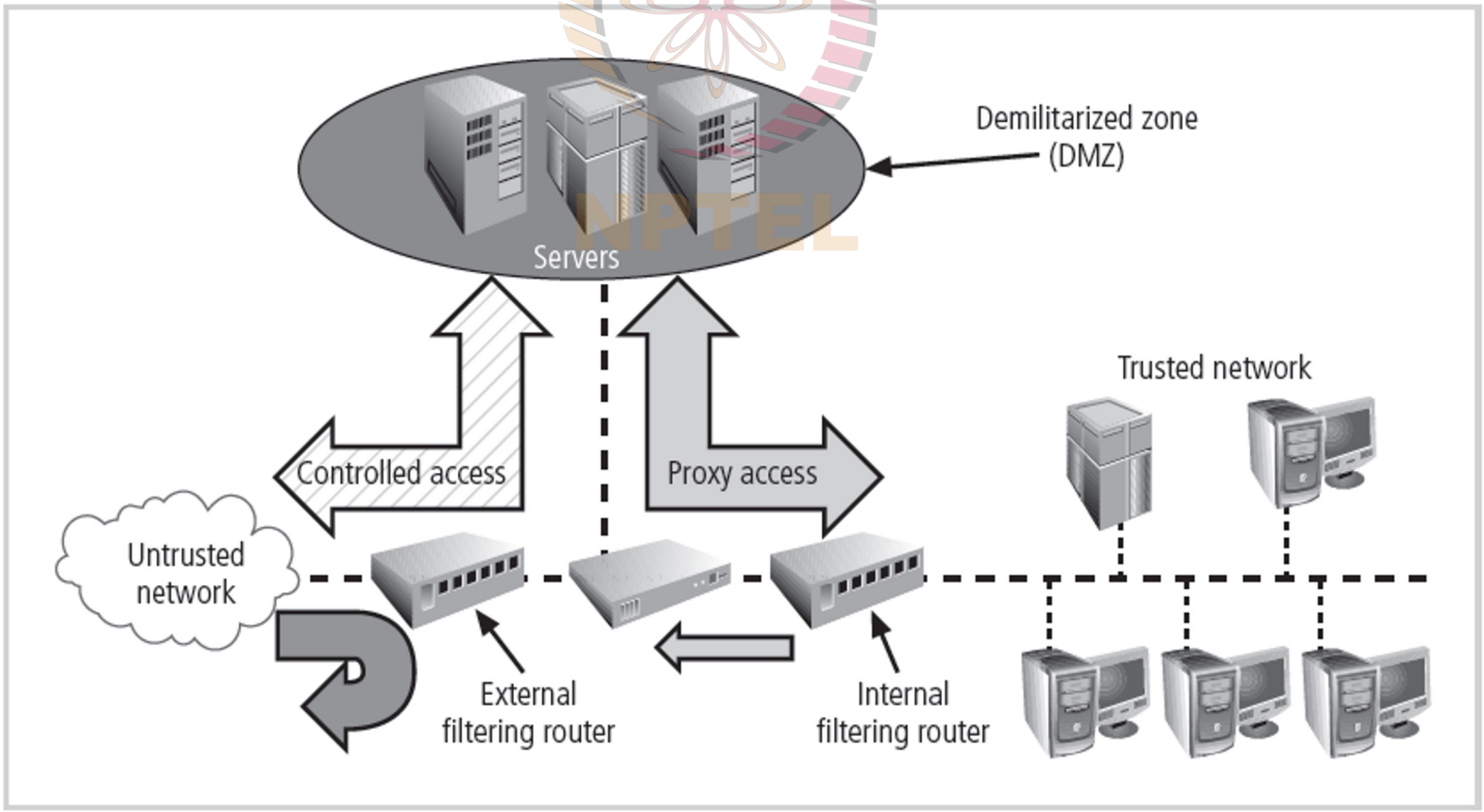
Mostly used biometrics:

- Fingerprints,
- Retina (blood vessel pattern) and
- Iris (random patterns of freckles, pits, striations, vasculature and coronas)



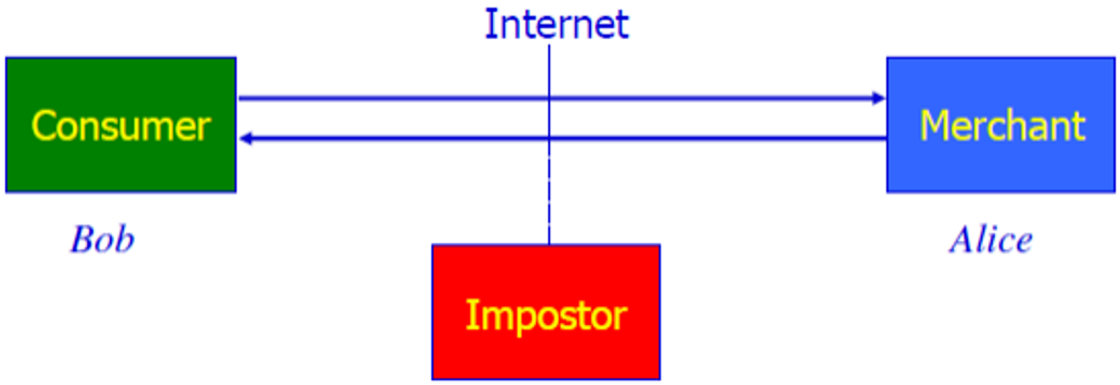
Firewalls

- Prevent specific types of information from moving between the outside world (untrusted network) and the inside world (trusted network);



Cryptography

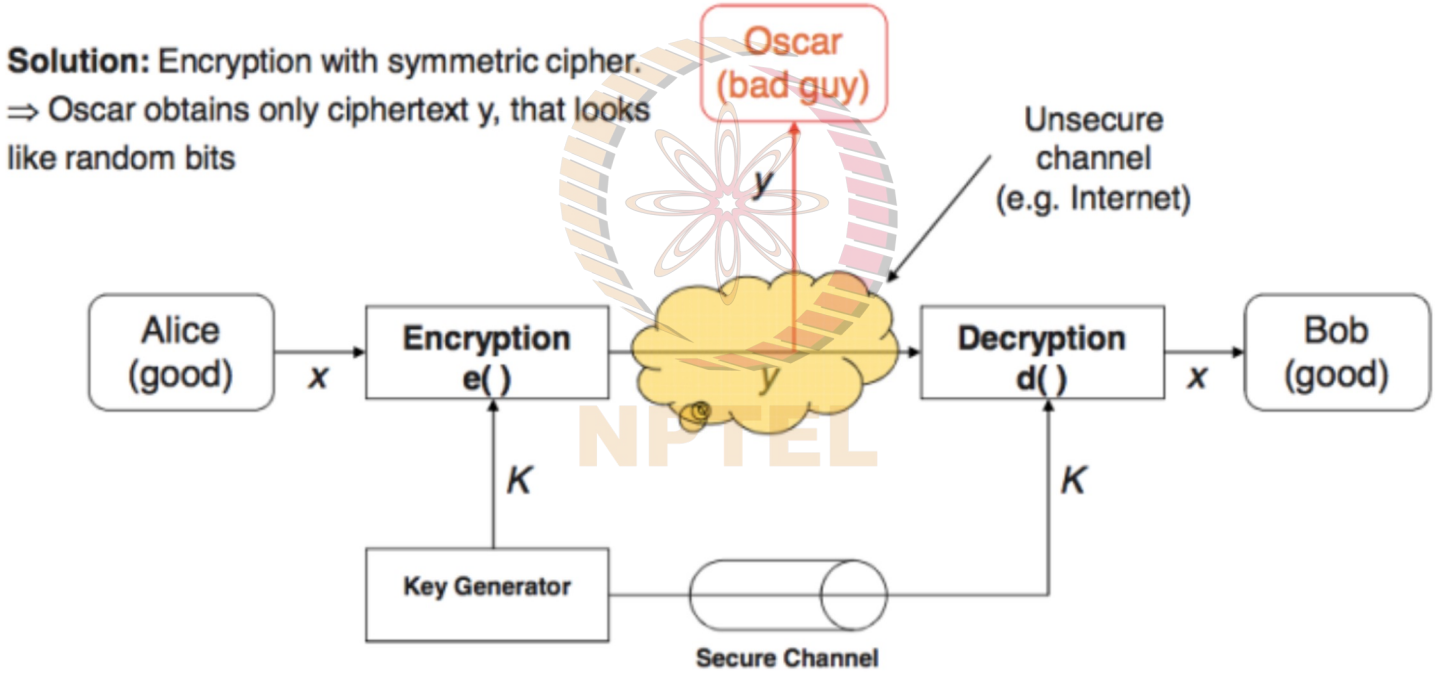
- Encryption is the process of converting an original message into a form that cannot be understood by unauthorized individuals
- Ensures confidentiality, integrity and non-repudiation
- Cryptology: the science of encryption
  - Cryptography [kryptos-graphein (hidden writing)] processes involved in encoding and decoding messages so that others cannot understand them



Related terms

- Plaintext can be encrypted using an algorithm
  - Bit stream: plaintext bit transformed into cipher bit one bit at a time
  - Block cipher: message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block of cipher bits
- Cipher: the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components
- Ciphertext or cryptogram: the unintelligible encrypted or encoded message resulting from an encryption
- Decipher: to decrypt or convert ciphertext to plaintext
- Key: the information used in conjunction with the algorithm to create the ciphertext from the plaintext

Symmetric key encryption

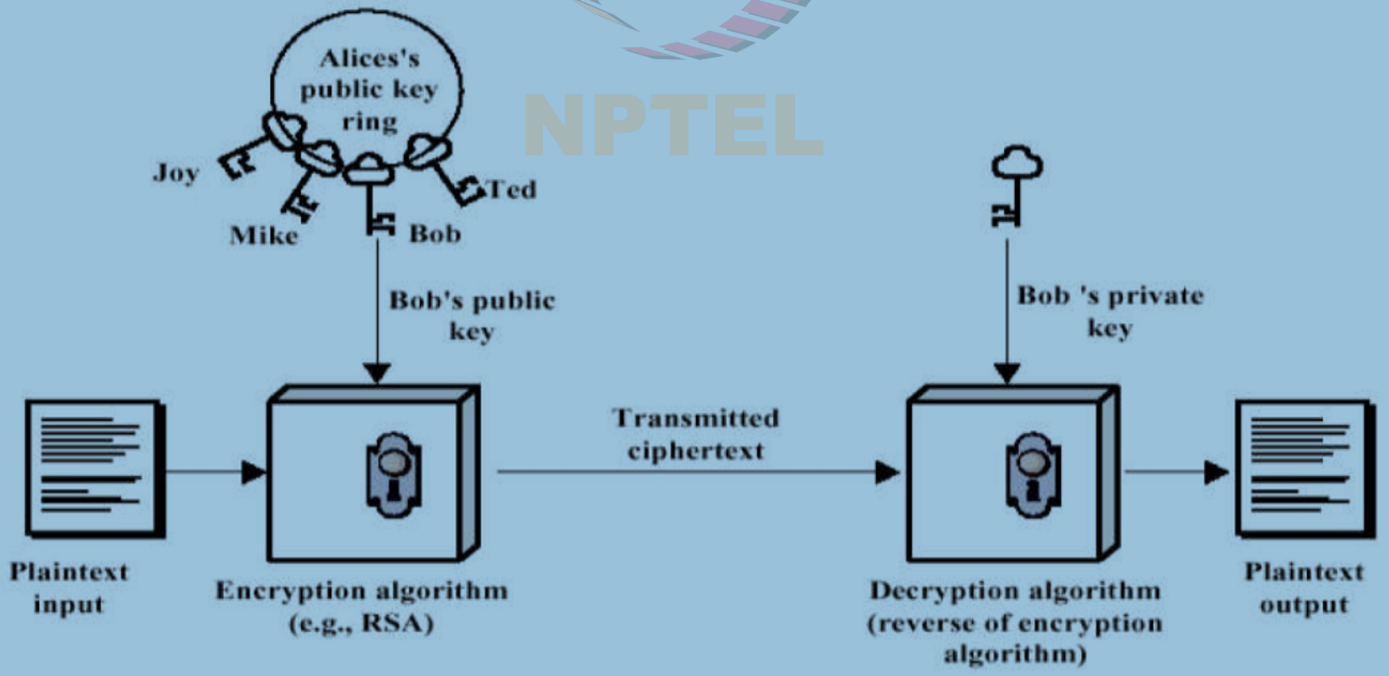


- x is the. **plaintext**
- y is the **ciphertext**
- *K* is the **key**
- Set of all keys {*K*1, *K*2, ...,*Kn*} is the **key space**

A cryptography system in which both parties have the same encryption key, as in secret key cryptography.

Asymmetric key encryption

Cryptography in which the key used in decryption is different from that used for encryption



Digital Signature, and certificates

- When the asymmetric process is reversed—the private key encrypts a (usually short) message, and the public key decrypts it—the fact that the message was sent by the organization that owns the private key cannot be refuted
  - This nonrepudiation is the foundation of digital signatures
- Digital signatures are encrypted messages that are independently verified by a central facility as authentic
- A digital certificate is an electronic document, similar to a digital signature, attached to a file certifying that the file is from the organization it claims to be from and has not been modified from the original format
- A certificate authority (CA) is an agency that manages the issuance of certificates and serves as the electronic notary public to verify their origin and integrity

SSL Digital Certificate

Common(basic) ciphers

- In encryption, the most commonly used algorithms include three functions: substitution, transposition, and XOR
- In a substitution cipher, you substitute one value for another
  - A monoalphabetic substitution uses only one alphabet
  - A polyalphabetic substitution uses two or more alphabets

PHHW PH DIWHU WKH WRJD SDUWB

What did Caesar tell his Commander?

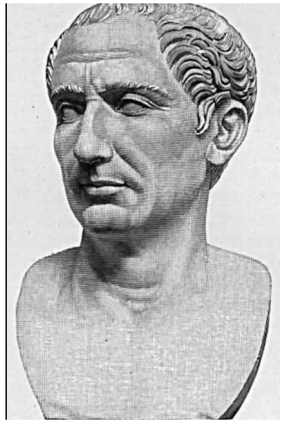
Substitution cipher

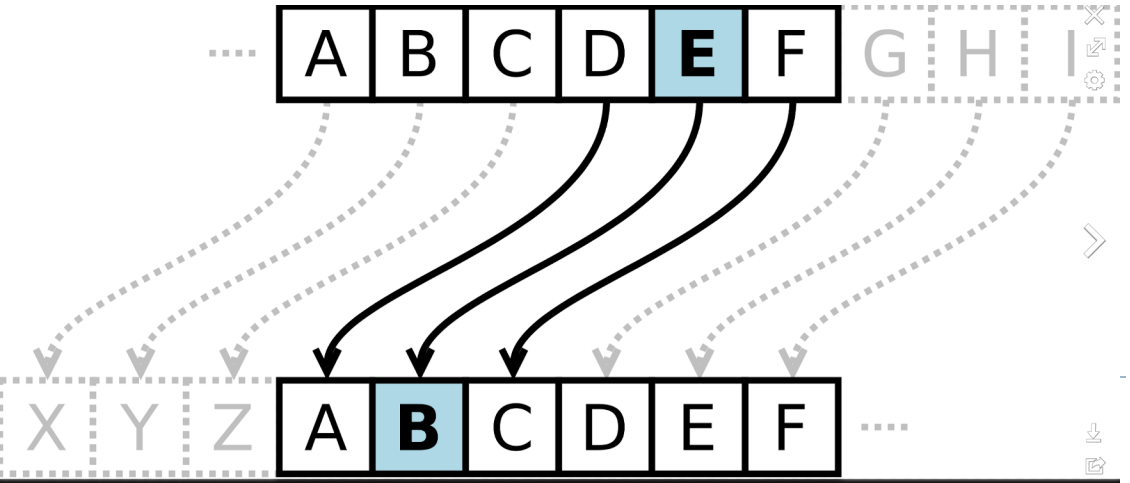
- Substitute one value for another
  - Monoalphabetic substitution uses only one alphabet
  - Polyalphabetic substitution uses two or more alphabets
- Example (Caesar cypher):

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

$c = E(p) = (p + k) \bmod (26)$

$p = D(c) = (c - k) \bmod (26)$





Vigenere cipher (Tabula recta)

	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	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Find the cipher text for DOMS using poly alphabetic substitution
Use IITM as the key and encode DOMS

Tabula recta

	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	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

D O M S
I I T M

Transposition cipher

Keys: 8-3, 7-6, 6-2, 5-7, 4-5, 3-1, 2-8, 1-4

Letter locations:	87654321|87654321|87654321
Plaintext:	__ENO_ON|_ERAPS_L|UAG_KCAS
Key:	Same key as above, but characters transposed
Ciphertext:	ON_ON_E_|_AEPL_RS|A_AKSUGC

Exclusive OR

- Truth table

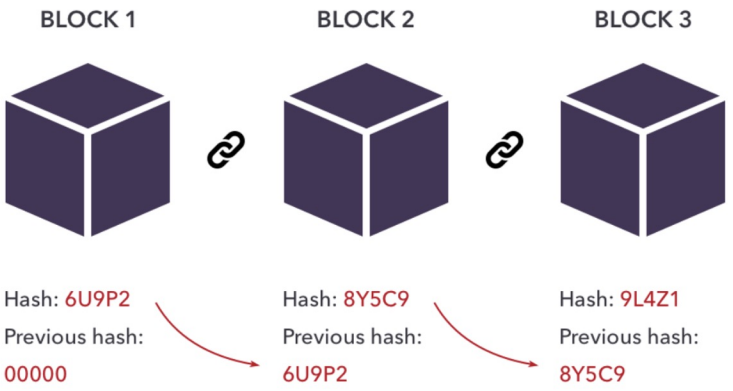
First Bit	Second Bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

- Message (binary): 00110101 01000101
- Key: 01010101 01010101
- Cipher text: 01100000 00010000

- Easy to break, used along with other methods

Block chains

- Ensures confidentiality through encryption and integrity through hashing
- Hash functions are mathematical algorithms that generate message summary/digest (hash value) to confirm message identity and confirm no content has changed
- Properties such as hiding, collision resistance helps block chains make transactions permanent
- Implemented as linked lists



Active Defense and 'Hacking Back'

GROUP 5

- MANO PATRIC
- BHUVAN DUBEY

Security against defeat implies defensive tactics; ability to defeat the enemy means taking the offensive

Sun Tzu

The only real defence is active defence

Mao Zedong

Why‘active defense’?

- To protect the most valuable information, something more than deployment of security software and network-monitoring process is required
- Even high amount of spending on technology defenses can secure the critical systems and help keep pace with the hackers

What is 'active defense'?

Active Defense ≠ Hacking Back

Direct defensive action taken to destroy, nullify or reduce the effectiveness of cyber threats against assets - Dorothy Denning

Example

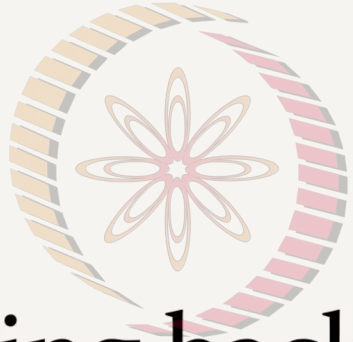
- Monitor for intrusion, and if detected, respond by blocking further network connections from the source
- Identify and shutdown a botnet used to conduct a DDoS attack

What is ‘active defense’?

Former CEO of National Cyber Security Center in UK:

https://m.facebook.com/cyberseceu/videos/2174647859531323/

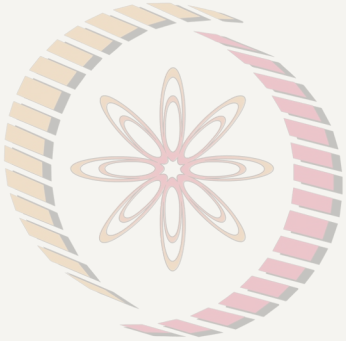
Should hacking back be attempted?



Expert opinion divided whether its part of active defence

Why do it?

- Gather intelligence about the source of intrusion
- Determine what data is stolen
- Identify the attacker for law enforcement to bring charges



Why not do it?

- Could be illegal
- No evidence that attacking the attacker works
- Could compromise government operations

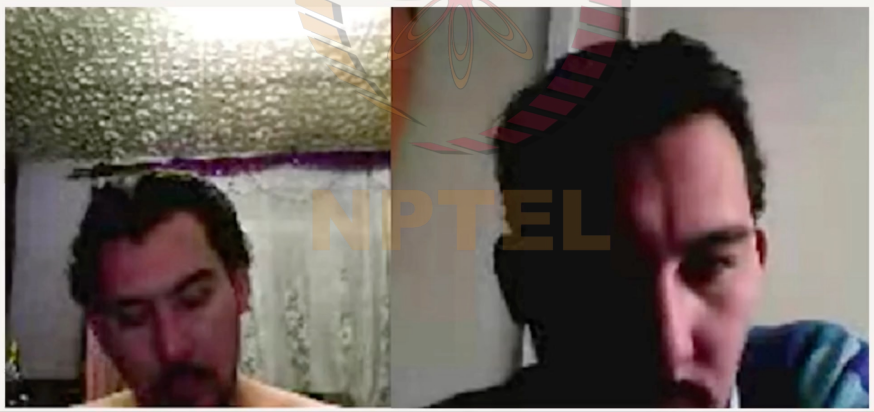
Expert advice

- Hacking back without legal authorization is unethical; targets are too evasive and networks are too complex, traversing innocent systems

Aggressive active defence or hacking back?

Case of Russian hacker who got malicious code onto Georgian govt. computers

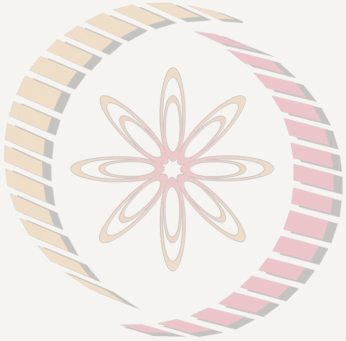
- Georgian authorities planted a spyware in a file named ‘Georgian-NATO agreement’
- Hacker’s malware detected the file and uploaded it to the drop server, which was downloaded by the hacker
- The spyware switched hacker’s webcam on and took a snapshot



Was it ethical?

It was ethical

- Georgian government took actions within its borders
- It didn't traverse a network to hit another system
- Hacker's own code led to spyware on his computer



It wasn't ethical

- Assumption that recipient was an attacker – may not have been correct
- Attacker could have been on a networked computer (e.g. a university computer)

Ethical active defense strategy

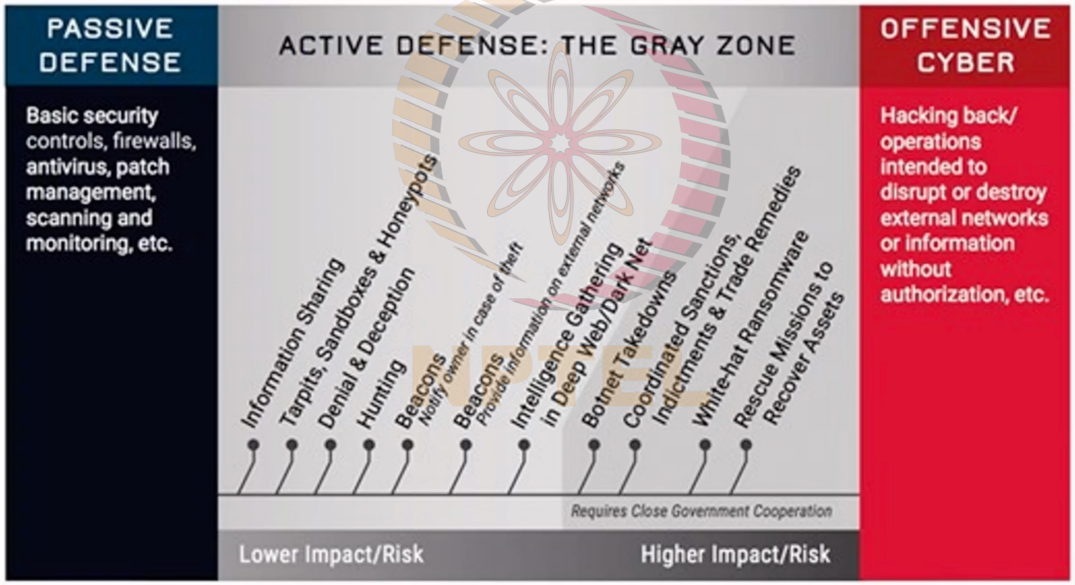
Active defense happens when someone crosses into your space –

- monitoring for missiles is passive defense,
- shooting them down when they are into your airspace is active defense

Examples

- Subscription to a service that can thwart DDoS attack and create a log
- Cooperating with law enforcement and international network of organizations combating hacking

Active Defense – the Gray Zone



Source: Center for Cyber and Homeland Security

Ethical considerations for active defense

Ethical and legal principles for active cyberdefense[1]

1. **Authority** – conducted with authorities granted by laws, contracts and policies
   - shutting down a botnet's C2 server, authority from the government may be needed
2. **Third-party immunity** – no intentional harm to third-parties
   - operation to shutdown a botnet should not harm victim machines on the botnet
3. **Necessity** – deployed only if necessary to mitigate the threat
   - disabling computers running the bots would be unnecessary to neutralize the botnet
4. **Proportionality** – not be deployed unless harm incurred is proportionate to the benefits gained
   - blocking all traffic from a DoS attack server may prevent it from sending legitimate traffic as well
5. **Human involvement** – even automated defenses should have human involvement
   - user access controls, firewalls, anti-malware controls require human to confirm their settings
6. **Civil liberties** – respect civil liberties of everyone, including rights to privacy and free-speech
   - active defenses that trigger additional collection or sharing of information that contain personal information

[1] Framework and Principles for Active Cyberdefence – Dorothy E. Denning