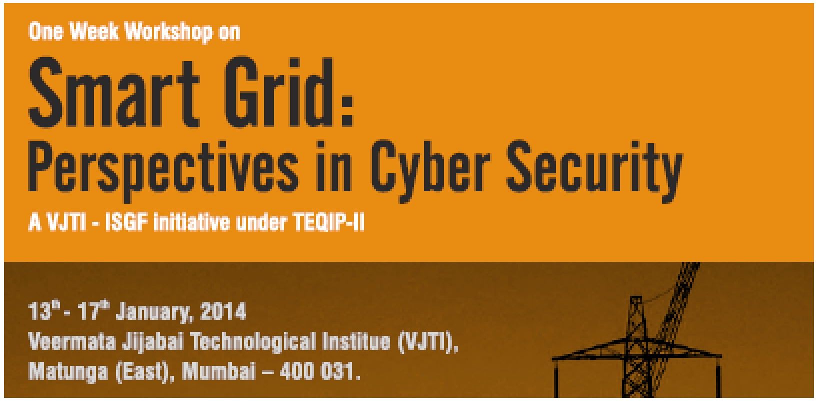
Demonstrate to “Ethically Hack”

As Part of Smart Grid : Perspectives in Cyber Security

Day : 4 , 1.5 hr. session

Download my presentations from http://hacking.suven.net



One Week Workshop on

Smart Grid:

Perspectives in Cyber Security

A VJTI - ISGF initiative under TEQIP-II

13th - 17th January, 2014
Veermata Jijabai Technological Institue (VJTI),
Matunga (East), Mumbai – 400 031.

Conducted by

Rocky Jagtiani - Technical Head

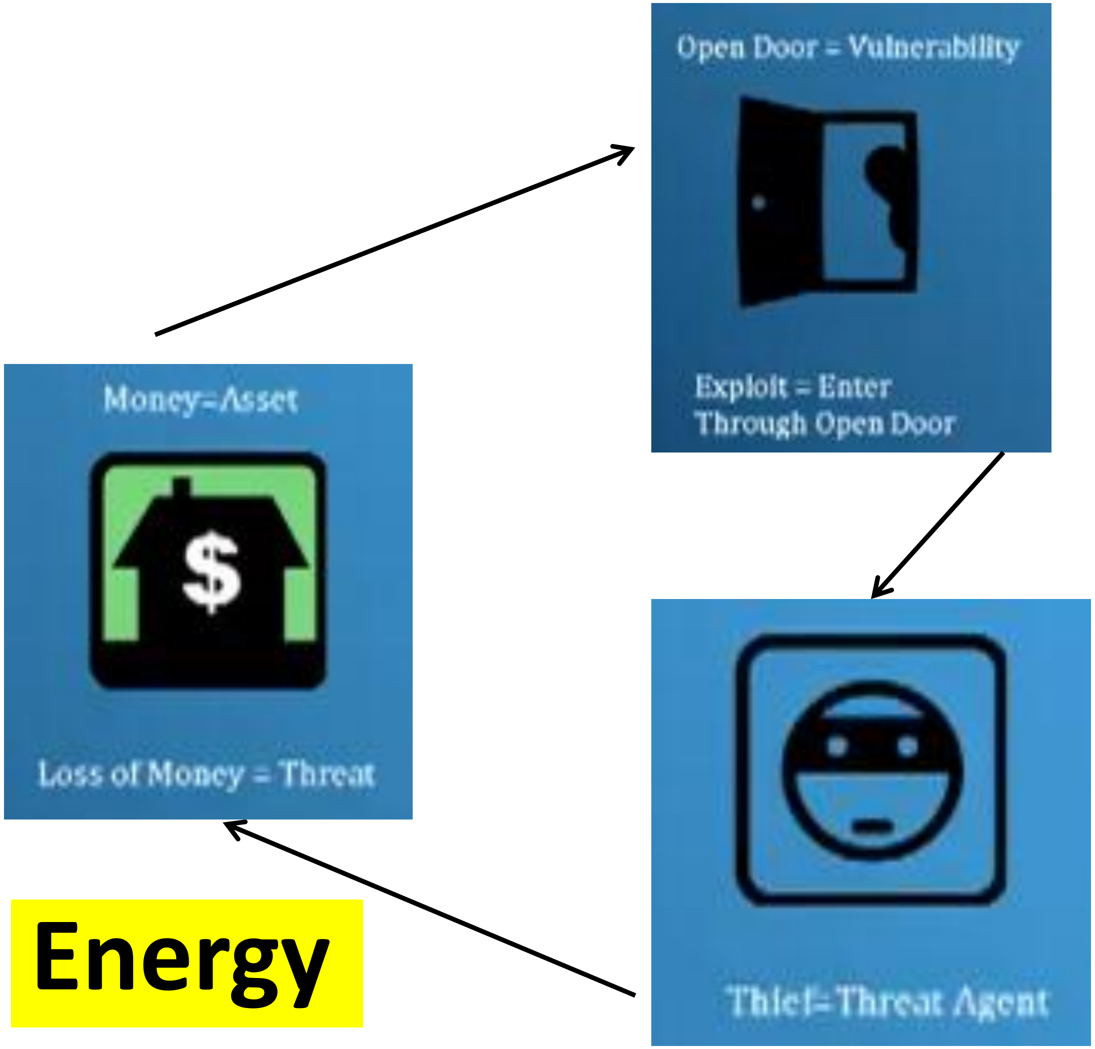
Suven Consultants & Technology Pvt Ltd.

Official Member to monster India

H.O : 4 / B , Ground floor, Trishul Apts, Sindhi Society, Chembur, Mumbai – 71
(O) 022-32634450 , 022-32268360

Training Centers : Thane , Dadar , Borivali , Ghatkopar , Nerul

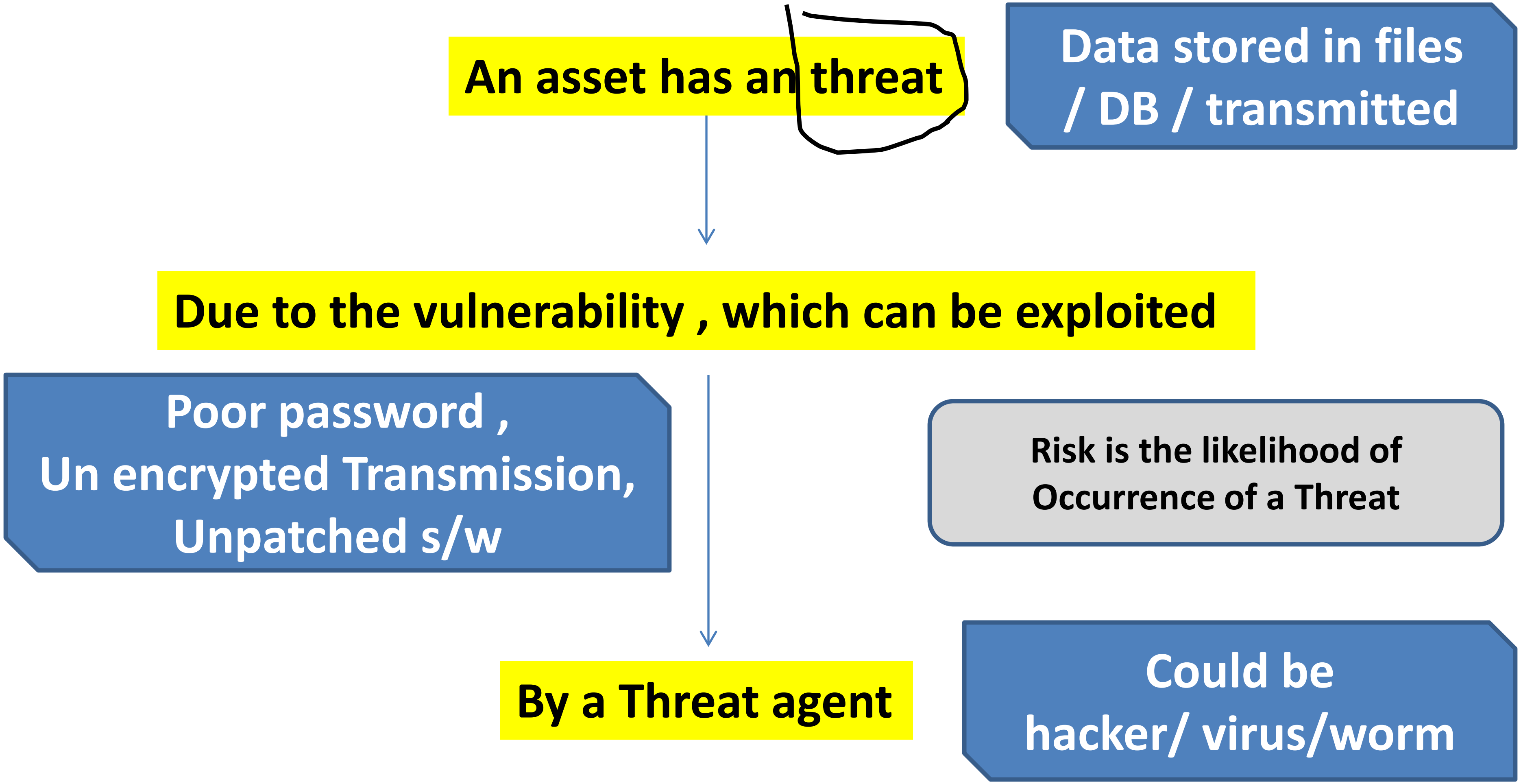
Section A: Basics



Energy

- Asset
- Risk
- Exploit
- Vulnerability
- Threat
- Threat Agent

Some Virus like Stuxnet



An asset has an threat

Data stored in files / DB / transmitted

Due to the vulnerability , which can be exploited

Poor password ,
Un encrypted Transmission,
Unpatched s/w

Risk is the likelihood of Occurrence of a Threat

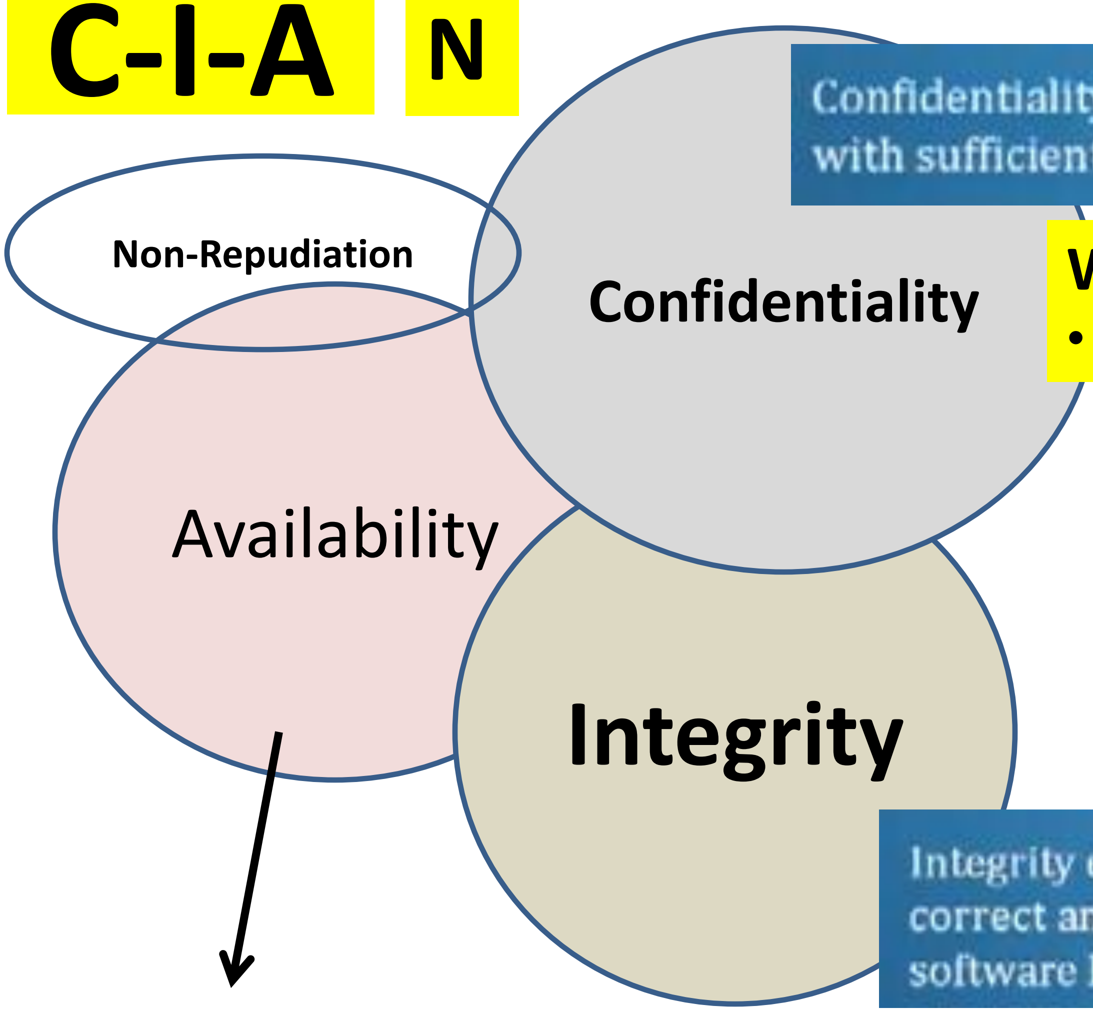
By a Threat agent

Could be hacker/ virus/worm

Threat is any action which en-dangers the C I A of data

C I A → loss or corruption of data OR Denial of Service

C-I-A N



Confidentiality ensures that only authorized parties with sufficient privileges may view the information.

We Achieve Confidentiality by

- **Encryption**

Applies to data storage, processing and Transmission

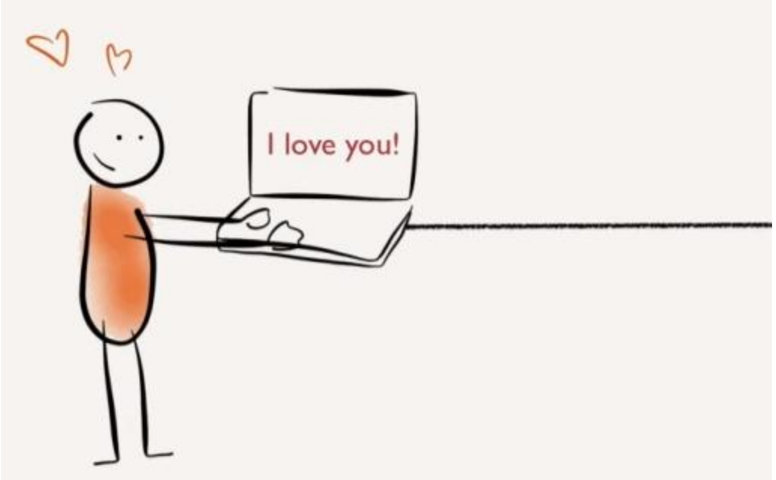
Integrity ensures that the data stored on devices is correct and no unauthorized persons or malicious software has altered data.

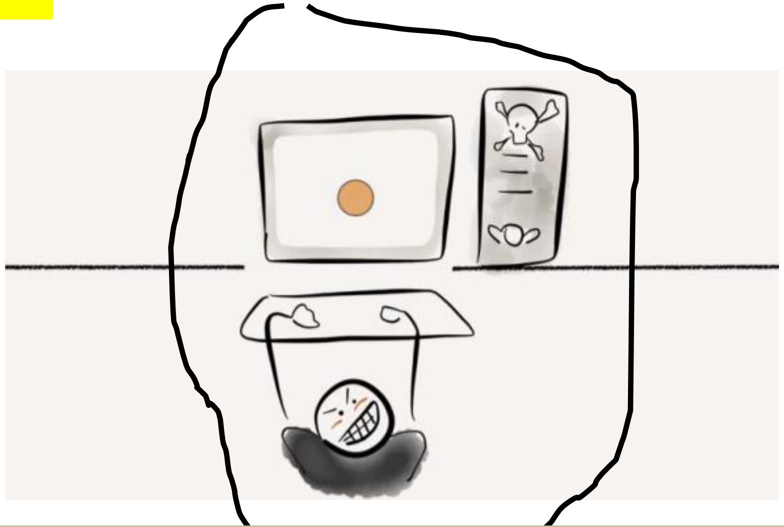
Availability ensures network resources are readily accessible to authorized users.

We Achieve Integrity by

- **Checksums**
- **File Hashing**

Example of Integrity

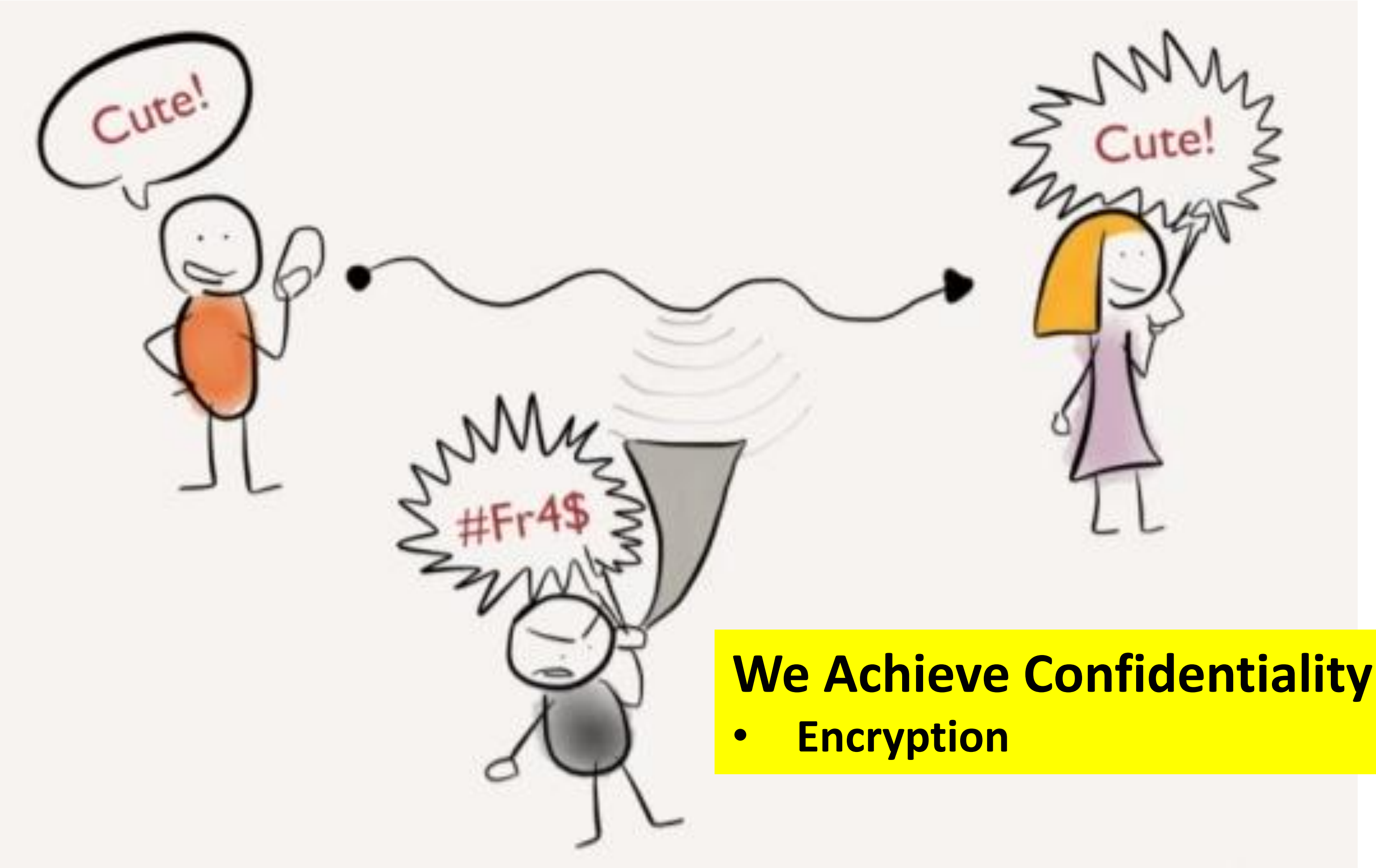




Confidentiality lost , data changed hence Integrity lost

Some one modifies the data w/o proper authorization, then INTEGRITY of data is lost

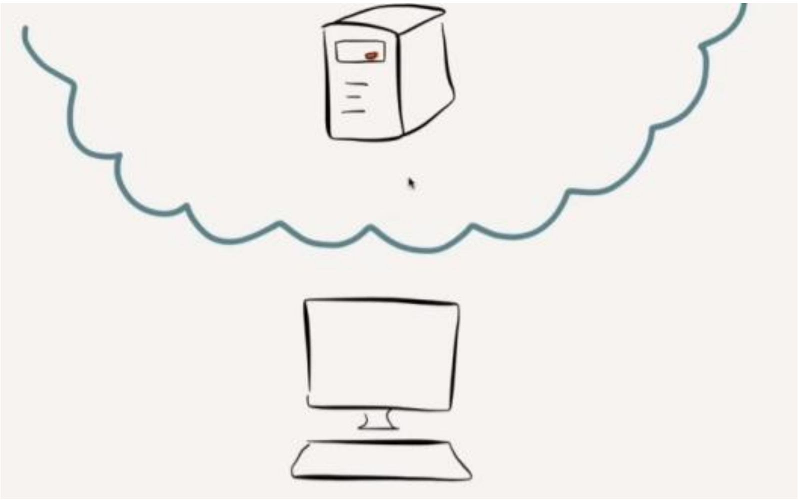
Hacker able to modify → as able to understand



We Achieve Confidentiality by

- **Encryption**

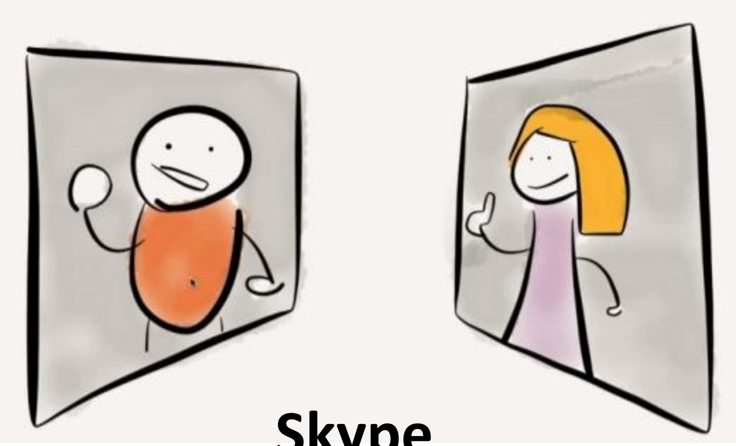
Availability → making the resources (h/w and s/w) always Available



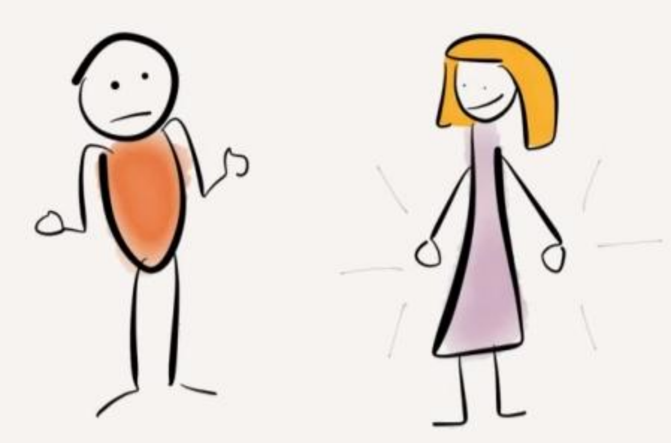
For HDD → use RAID

For s/w , files and data → do BACKUP

Non-Repudiation -> No participant in the transaction can deny of what he is send or received.

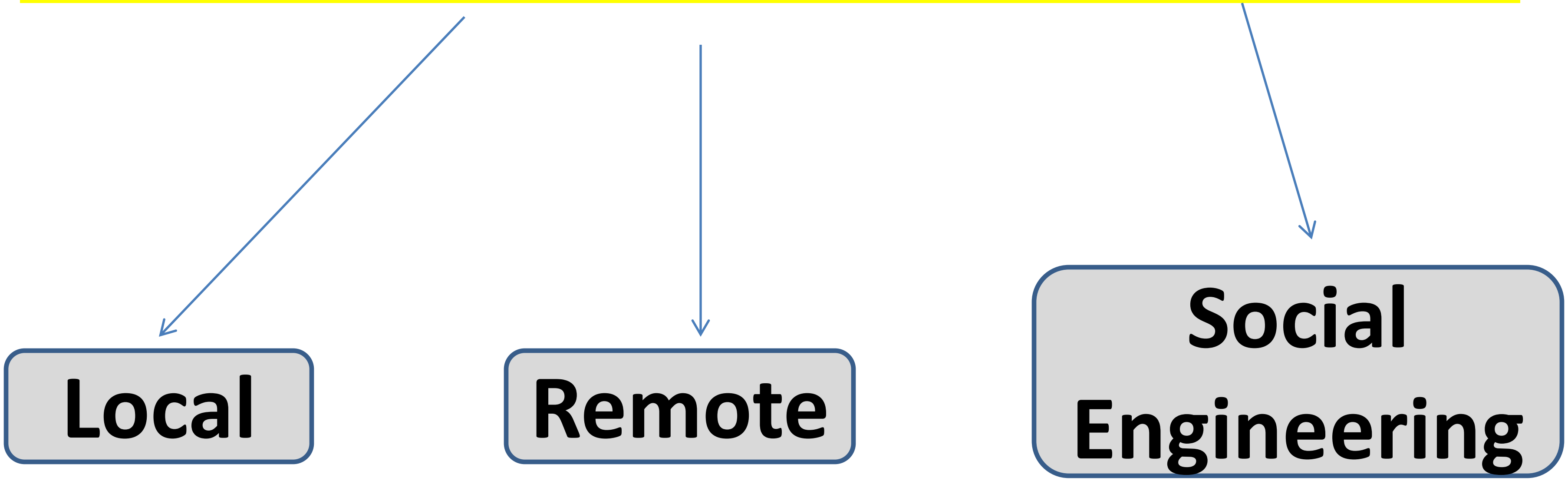


Skype



Use WhatsApp

Hacking : process to bypass security mechanism of an Information system



Local

Remote

Social Engineering

Local → done by physical Access

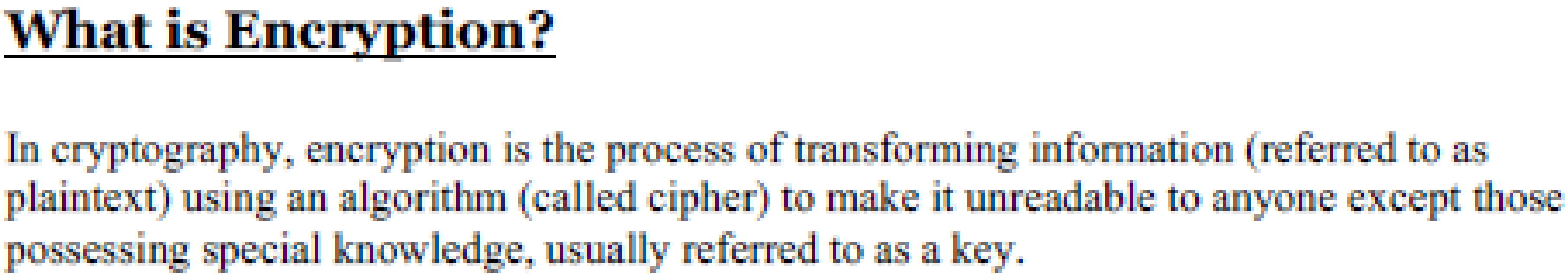
Remote → done Remotely over www

Social Engineering → manipulating people into performing actions or diverging confidential information.

Section B: Password Hacking

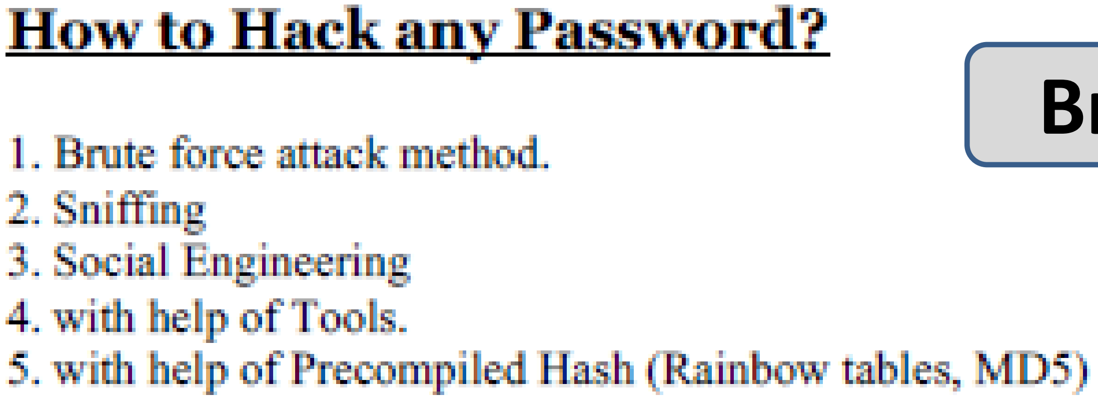
Password → secret word or string of characters used for authentication, to prove identity and get access to resource

Passwords are protected by Encryption



What is Encryption?

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.



How to Hack any Password?

1. Brute force attack method.
2. Sniffing
3. Social Engineering
4. with help of Tools.
5. with help of Precompiled Hash (Rainbow tables, MD5)

Brute Force Attack

Sniffing

Spoofing

Brute Force Attack

Is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN).

Generates a large number of probable passwords

It is a guessing technique.

Some basic know ledge / information is required to attack

Project 1 : Code brute force tool using HTML – Php

Sniffing

Capturing data over a n/w or on K/w

Scanning captured data

Replaying with or w/o alteration

Network Performance Series
Want to learn more about the history and internals of TCPDUMP, WinPcap, and Wireshark? Want to hear about the future of network performance management from the creators of these open source tools? Riverbed Technology is sponsoring The Pioneer Lecture Series: Network Performance Management in a city near you. Sign up today!

March 9, 2011 — Portland, OR

March 16, 2011 — Bellevue, WA

SHARKFEST '11 Early Registration
December 8, 2010
Save $100 by registering before March 10th! Details at the Sharkfest web site

More News »

How To Read IPv6 Addresses
Feb 8 | By Gerald Combs

Wireshark Has a New Home
Oct 21 | By Gerald Combs

Announcing ask.wireshark.org
Sep 13 | By Gerald Combs

Built free or die Blog »

Learn how to get up and running with Wireshark
Duration 5:51 (mm:sec)

Riverbed Cascade Shark: 10GbE Distributed Analysis
- Sustained multi gigabit traffic recording
- Retrospective analysis and drill-down in multi-TB network data recordings
- Extended-duration network Trending and Alerting
- Mix and match 1 & 10GbE NICs

Learn More

AirPcap: Wireless Packet Capture
Plug & play 802.11 packet capture for Wireshark
802.11 A/B/G/N
- Multi-channel capture
- Management, control and data frames

Most common is N/w packet Sniffing

Wire-Shark is one of the most popular n/w protocol analyzer tool

Sniffing is done with out touching the information / data

Like hiding and overseeing some one

More common / easier way to hack password is

Spoofing - means to mimic something and create an illusion of the presence of the original. Also called **Masquerading**

Steps :

1. Create a look-like page to yahoo / Gmail account login.
2. Code a php file which reads password.(typed in by user)
3. Store it in a hidden / secret txt file.

Project 2 : lets Code a look-alike Gmail page and **spoof** a friends account **LIVE** using HTML-Js-Php

Section C: Web App or Site hacking

Different ways to hack a Web App

- Injection Attacks
- PHP Remote File Includes
- Cross Site Scripting (XSS)
- Cross Site Request Forgeries (CSRF)
- Insecure Communications

First : Injection Attacks – 2 types – SQL & Browser

What is it ?

Injection is passing malicious user-supplied data to an interpreter.

Most common form : SQL Injection, where the hacker passes a SQL command to your database.

Project 3 : Code a login page using simple 3 – tier programming and perform SQL Injection.

Injection attack in the Browser Address Bar

Unchecked path

Injections can also be performed via the browser address bar.

Example : HTTP GET requests with URLs of the following form

http://somesite.com/index.php***?id=10***

Try changing the data passed to the URL string like this,

http://somesite.com/index. php***?id=11***

Project 4 : Code a product description page and perform Browser Injection by changing the product ID.

2 methods to fix Injection attack

1)

Always sanitize user-submitted data (if a username can’t contain a single quote character, don’t let users enter it),

E.g. :

```
$email= mysql_real_escape_string($_POST['email']);
$password= mysql_real_escape_string($_POST['password']);
```

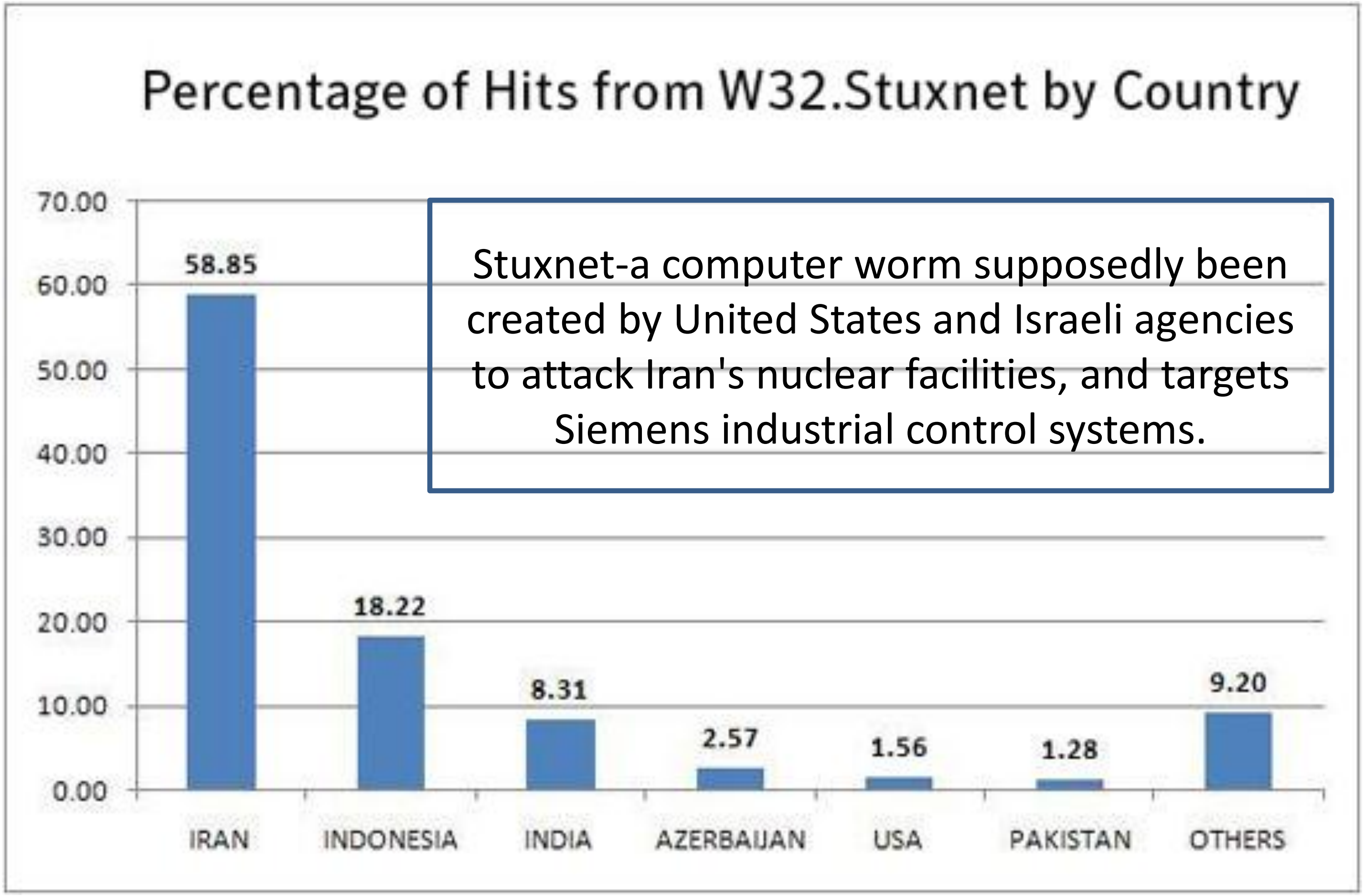
It adds backslash to the following characters: *\x00, \n, \r, \', \“.*

2)

Encode the data before appending to the URL.

Eg : Use base64_encode(‘some string’); and then append to the URL

Many such small tips of Ethical hacking (your own system)



Stuxnet-a computer worm supposedly been created by United States and Israeli agencies to attack Iran's nuclear facilities, and targets Siemens industrial control systems.

Thank you!

Download my presentations from http://hacking.suven.net