ISSN:0975-9646

Cyber Security Tools

Gunjan.Hardasmalani[#1], Rashmi.Bajaj[#2], Harsha.Sachdev[#3]

[1,2,3]*Department Of Computers*
Thadomal Shahani Engineering College,
Mumbai

Abstract **- Cyber crime has become one of the most serious economic and national security threats to our nation. There is need of cyber security to secure economic and confidential data. Cyber security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption of services they provide. Cyber security is critical in almost any industry which uses computers. The field is of growing importance due to the increasing reliance of computer systems in most industries as almost every industry has become part of 'Internet of Things'. In proposed system the effort is made to aware people and exposes the idea that it is not safe to navigate in cyber world without security.**

Keywords **- TrueCrypt, CryptoCat, John the Ripper(linux), CodeGuard, RSA web threat Detection**

I. INTRODUCTION

In this ever growing cyber world where millions and trillions of bytes of data is transferred everyday over the internet, the security of this data is a top priority and a major challenge. Cyber security has become a necessity for every individual who is connected to internet and uses the internet for any purpose.

While India is witnessing a steady increase in the number of cyber crimes, there is another worrying statistic that goes on to suggest that the nearly 13 per cent of the cases are targeted against outraging or blackmailing a woman.

One such case was reported from Kottayam in Kerala where a girl went to meet with a person she had become friends on Social networking site. However when she met him, she was abducted. The girl was however traced and later she told the police that when she met with the boy he had forcibly taken her to a hotel and assaulted her. The police say that despite being warned and told not to meet with strangers, these girls often bite the bait and end up in trouble. In Kerala, a statistic would reveal that 29 cases registered with the cyber crime wing have been against women. These are cases of revenge, fraud and blackmail the police found during their investigation.

Operations like online money transactions, transfer of sensitive information, web services, and numerous other operations need security of data. Along with these operations on the internet, data security is also essential and important in databases.

II. TOOLS FOR CYBER SECURITY

1. Password Security Tools

Password can be simplified defined as a secret word or phrase that must be used to gain admission to a place. As we all know how important password is for our day to day things, it is necessary to protect it. Every few months it seems another huge company reports a hacking resulting in millions of people's account information being compromised.

And with the recent Heart bleed bug, many popular websites were affected directly. Although data breaches are out of your control, it's still imperative to create passwords that can withstand brute-force attacks and relentless frenemies. Avoiding both types of attacks is dependent on the complexity of your password. One should never use same password for every site you login to.

The logic is simple: if you recycle the same password (or a variation of it), and a hacker cracks one account, he or she will be able to access the rest of your accounts.

A good password manager takes the strain off you by helping to generate, manage, and store all those long, complex, and unique passwords. Further, good password manager includes features like security assessments, random-character generation, and other tools. Some password managers offer two-factor authentication, requiring a smartcard as well as your password to log in.

With this type of two-factor authentication, even if your password is decrypted, hackers still can't access your account but neither can you, if you don't have your smartcard. That's why this type of authentication is usually offered as an option. As the most favourite password managers among users are Keepass, Dashlane, and Lastpass.

Here we discuss some other password security tools and why they are better.

We all use cloud computing services to store our important data. These services are invaluable for synchronizing data across different computers and mobile devices or sharing it with others. But are we aware of the fact that the administrators of those computing services can access our data.

1.1. *TrueCrypt:*

The free utility TrueCrypt lets you effortlessly encrypt entire folders, so your cloud-synced data remains truly yours. TrueCrypt works by creating virtual encrypted disks; this means that, as far as cloud can tell, a TrueCrypt-encrypted disk is just a blob of random binary data. However, when you mount that volume using TrueCrypt, you need only enter the correct password and a new drive shows up on your system. Every file you put into this drive is instantly encrypted, secure from prying eyes. As soon as you unmount the volume (eject the disk, so to speak), it becomes completely inaccessible. TrueCrypt is very serious about security, to the point of providing plausibly deniable encryption. Let's say that some person or legal entity finds

out you're keeping files inside a TrueCrypt volume, and has the power to compel you to give away your password. With a less serious security solution, this is game over: As soon as you give over your password, your data is forfeit.

TrueCrypt lets you get around this limitation by creating a hidden volume inside a TrueCrypt container. Enter one password to decrypt the volume, and you get one set of files (decoy files you put there in advance, which should seem believable enough to stand in for the contents of that volume).Enter a different password to decrypt that same volume, and suddenly you get an entirely different set of files, which are the real files you're trying to protect. In other words, whoever coerced you to give away your password now thinks they have whatever files you were hiding, when in fact they don't (but you can claim they do, and there's no way to detect that two-password trick).

1.2. *Cryptocat*

If secure traffic tunnelling and steganography sound too cloak-and-dagger for you, consider a friendly, real-world security hole: Chat. Chatting online is easier than ever; chatting securely, not so much. The chat clients built into Facebook and Gmail.

Emphasize ubiquity and ease of use far more than encryption. Free chat client Cryptocat claims that you can have both security and convenience, and it made quite a splash upon its arrival.

CryptoCat's simple aesthetic makes it easy to focus on the conversation. The least mature tool in this roundup, Cryptocat demonstrates an important lesson about security software: Newer rarely means better. Following a glowing profile piece that Wired published on Cryptocat and its developer, 21-year-old Nadim Kobeissi, security guru Bruce Schneier published a cautionary post in his blog letting readers know Cryptocat wasn't as safe as it seemed. At the time, the problem was that Cryptocat handled security host-side, rather than locally. This issue has since been addressed, and Cryptocat now runs as a browser extension and handles encryption locally. Still, this is an important example to keep in mind: Encryption software, even when it's open-source, can't be considered secure until it's been thoroughly audited and battle-tested (preferably for years).While I wouldn't use Cryptocat for mission-critical secret communications, it does add a modicum of security and privacy over the features built into Google and Facebook, and it's just as easy to use.

After installing a Chrome or Firefox extension, all you have to do is pick a nick (a handle) and a title for your chat room, and presto—you can chat with any other Cryptocat user who joins the room. The aesthetic is decidedly old-school 8-bit, but that only adds to Cryptocat's charm. It's a nice way to chat with friends, and can serve as a reminder that it's important to use other forms of security, too.

1.3. *John The Ripper: Only for Linux*

John the Ripper is a fast password cracker for UNIX/Linux and Mac OS X. Its primary purpose is to detect weak UNIX passwords,

Though it supports hashes for many other platforms as well. There is an official free version, a community-enhanced version (With many contributed patches but not as much quality assurance), and an inexpensive pro version.

It can be run against various encrypted password formats including several crypt password hash types most commonly found on various UNIX.

2. DATABASE SECURITY TOOLS

Data security has become a necessity for every individual who is connected to internet and uses the internet for any purpose. It is a requirement that is a must in every aspect of the operation performed on the internet. Operations like online money transactions, transfer of sensitive information, web services, and numerous other operations need security of data. Along with these operations on the internet, data security is also essential and important in databases. Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks. It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment. Database security covers and enforces security on all aspects and components of databases. This includes:

- Data stored in database
- Database server
- Database management system (DBMS)
- Other database workflow applications

Purpose of Database Security

The purpose of database security tools is to provide more complete protection of relational database management system offerings, beyond the security features that are integrated into those products. Some of these add-ons deliver high-end data, analysis and auditing tools as well. The appeal of database security tools is that they don't alter the database or application, and they result in only minimal performance impacts.

2.1. CodeGuard

CodeGuard is a service that provides an automatic website backup solution for HostGator customers with Shared hosting packages. CodeGuard monitors your site and keeps you informed of any changes while offering frequent backups and restore options so that downtime can be avoided.

CodeGuard’s service includes:

- BACKUP
  CodeGuard only creates backups of your site files and databases, and does not backup the email accounts associated with the domain of your website.

Initial Backup:

Once connected, CodeGuard will begin running an initial backup on the website. During this process, a complete data retrieval of all files that CodeGuard has access to will be compiled. It is during this process that you will also be able to view real-time updates on the backup process.

There are four main steps within the initial backup process:

1. Process Initiation - CodeGuard verifies the credentials provided.
2. File Pickup - The file structure of the website is analyzed before Codeguard creates a git repository into a cloud server.
3. File Transit - The file pickup process is finalized by confirming the list of files that will be copied over to the git repository created for the site. Once confirmed, the files are then transferred over the git repository onto the cloud server.
4. Final Delivery - Files are moved from the git repository onto the cloud server and encrypted as they are moved to a digital storage facility. Once moved and encrypted, the files are removed from the cloud server.

2.2. RSA Web Threat Detection

The RSA Web Threat Detection platform collects and analyzes massive amounts of live data from web traffic to provide web session intelligence, delivering complete visibility into all web and mobile-application activity. This intelligence also powers the software's behavioural analysis engine, which creates heuristics and rules to detect anomalies, IT security threats, navigation layer fraud, insider threats, business logic abuse, and other malicious activity in real time.

RSA Web Threat Detection is deployed at some of the world's largest ecommerce companies and banks, monitoring nearly half of all U.S. banking traffic. Designed to support how fraud and info-sec teams actually work, RSA Web Threat Detection can help your organization unlock the power of big data to deliver security intelligence and cyber-crime protection.

Features:

Real-time threat detection:

An innovative and functional user interface helps simplify threat detection and investigation by leveraging big data analytics in the form of web session intelligence and one-click incident investigation.

Enhanced visibility:

Receive greater insight into the online threat environment. Equipped to provide visibility into mobile traffic and third-party sites, RSA Web Threat Detection defends against attacks originating outside your web session.

Streaming analytics:

Support more intelligent, risk-based behavioural threat detection with a real-time, click-by-click threat-scoring platform. The self-learning statistical models and web session intelligence platform dynamically adjust to account for changes in usage patterns and the website.

III. SUMMARY

We summarize the above data in the given table:

Type	Tools	Description
Password	TrueCrypt	Security for files on cloud applications
Password	CryptoCat	Security for chatting privately
Password	John The Ripper	Only for Linux password security
Database	CodeGuard	Data Backup for a website
Database	RSA Web Threat Detection	Provides real time web detection and enhanced visibility

ACKNOWLEDGEMENT

We would like to show our gratitude to the ijcsit team for organizing such publications of technical paper.

REFERENCES

[1] Cyber Warfare: Techniques, Tactics and Tools for security practioners by Jason Andress.
[2] Cyber security and Cyber warfare by P.W Singer. http://www.huffingtonpost.com/entry/password-tools_n_3769501.html?section=india
[3] www.cnet.com/how-to/the-guide-to-password-security-and-why-you-should-care/
[3] www.darkreading.com/risk-management/10-top-password-managers/d/d-id/1109759?
[4] in.pcmag.com/password-managers/36444/feature/the-best-password-managers-for-2015
[5] searchsecurity.techtarget.com/feature/Comparing-the-top-database-security-tools