JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-1 E-ISSN: 2347-2693

Ransomware: Evolution, Target and Safety Measures

A. K. Maurya[1*], N. Kumar[2], A. Agrawal[3], R. A. Khan[4]

[1*]Department of Information Technology, IET, Dr. Ram Manohar Lohia Avadh University, Faizabad, India
[2] Department of Information Technology, SIST, BBAU Lucknow, India
[3] Department of Information Technology, SIST, BBAU Lucknow, India
[4] Department of Information Technology, SIST, BBAU Lucknow, India

[*]Corresponding Author: aumaurya@gmail.com, Tel.: +91-9721246388

Available online at: www.ijcseonline.org

Received: 10/Dec/2017, Revised: 20/Dec/2017, Accepted: 11/Jan/2018, Published: 31/Jan/2018

Abstract— Security was a big deal for a long time. With the viruses, malware and ransomware are another problems seen by the practitioner. This paper shows working of ransomware with its evolution and general characteristics of few popular ransomware. In evolution part, the paper provides s study from first ransomware to current days. The study shows the light on various kind of infection performed by a ransomware including data infection and infected machine. Different attackers made choices to the target various attack; the paper provides a sight on various target types of the ransomware. This paper trying to demonstrate few ransomware attacks case studies to show the problem created by various ransomware as an example. After an attack, what a victim should do after infection is also discussed at the end of the paper. How people can save their system and what are the safety measures to save the system from ransomware, are also discussed by the researcher. At the end of the paper, the researcher points out few steps to save systems and data.

Keywords— Ransomware, Security, attack, Cryptowall, Cryptolock, Wannacry.

I. INTRODUCTION

Cybersecurity was always a challenging issue since arising from computers. It has been increased with the internet improvement of internet facilities. Many kinds of cyber-attacks are currently performed by cybercriminals. Apart from the other threat issues, spreading of a ransomware is an illegal business. It is in flow for the network since 2005 but for personal computer started from the year 2015[1]. Crypto ransomware is the category of malware that is able to encrypt data of victim machine whereas locker ransomware locks the machine, thus in the second kind user not able to use their own machine. Both ransomware can be understand just as first one is like a lock that applies on the home of victims goods by which he can enter the home but cannot use the items of their own whereas the second case is that someone locks gate of home of victim by their unknown lock in this case victim is not able to enter in their own house. Paper represents threats of ransomware in terms of IoT infrastructure. Few famous cases are enlisted here as:

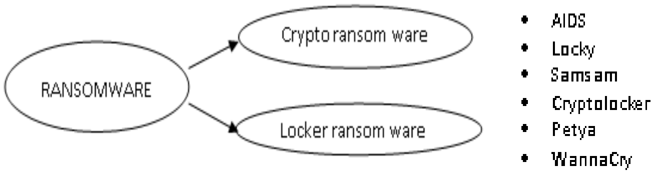


Figure 1: Classification and few examples

Attackers have developed a way to monetize files already on a victim's computer. They accomplish this through encrypting select files and then charging for access to the key. This type of malware has spawned a new classification, crypto-ransomware, but is more commonly known by the name of most prevalent version, CryptoLocker, or its variants TeslaCrypt and CryptoWall.

Famous Cases:

- In August 2016, Bournemouth University was successfully attacked and corrupted files by ransomware 21 times during previous 12 months.
- In April 2016, A Network Hospital of MedStar Health in Maryland, was attacked and blocked working by the SamSam ransomware.
- In February 2016, Hollywood Presbyterian Medical Center was attacked by Locky ransomware and disrupted working for two weeks until they paid 40 Bitcoin (about $17,000) to recover its files [2].

Study of the famous cases shows that ransomware attacker makes target to a system of professional bodies. After seeing the importance of the awareness about ransomware the study on ransomware was started. Evolution of ransomware has shown in section II with its division before ransomware as a service and after ransomware as a service. This section indicating basic characteristics of ransomware and indicates a light on new ransomware introduced in 2017. Section III, showing various kind of infections performed by a ransomware after an attack. After this, section IV classifies various targets for a ransomware attack it also shows a situation of a machine after an attack. At the end of the paper section V explain the safety measures for a ransomware while paper concluded in section IV.

II. EVOLUTION OF RANSOMWARE:

From 1989 attack of ransomware were started and got typical to crack with the expansion of type. Ransomware's attack got very common after included it as a service in form of ransomware-as-a-service. As per Ronny and Max [1], we have classified evolution in two parts as given in table 1 and 2:

A. Before Ransom as a service:

A ransomware with name AIDS Trozen had come into the existence in 1989 that was also famous as a PC cyborg. This virus was created by Joseph L. Popp and distributed through a floppy disk.

Table 1: Evolution of ransomware before Ransomware-as- a-service

Year, Name	Description
1989, AIDS Trozen (PC cyborg) [7]	▪ Symmetric cryptography based ▪ Distributed at WHO international AIDS conference by floppy drive
2005, Trozen.Gpcoder[7]	▪ Custom symmetric cryptography ▪ Via spam email to claiming a job application.
2006, Trojan.Cryzip[7]	▪ Deleted files; ▪ Create password protected achieved file after duplicacy;
2006, Trojan.Archiveus [7]	▪ like Trojan.Cryzip; ▪ Demanded order id of purchase medication of specific pharmacy for password.
Starting of Locker ransomware, 2007 [1] :	
2008, GPcode.AK [1]	▪ 1024-bit RSA key ▪ asked for payment of $100 to $200
2012, Citadel [1]	▪ released for cost $3000, to produce and distribute ransomware.
2012, Lyposit [1]	▪ Opened as pop-up to say machine involved in illegal activity ▪ Shows locked by the FBI/ Judiciary
Trojan.Randso.C [1]	▪ Displayed self as a Windows Security Centre message ▪ Asked to reactivate their Windows license
2013 CyptoLocker[1]	▪ encrypted about 67 file types, including MS Office data files; ▪ provide thee day to pay; ▪ if not paid within time limit than demands higher to retrieve files;
December,2013 CryptoLocker 2.0 [1]	▪ written in a different language than CryptoLocker; ▪ As per Symantec number of attacks grew from 100,000 in January to 600,000 in December; ▪ They estimated that 3% percent of infected users paid ransom.
2014 [1]	▪ Two vendors, FireEye and Fox-IT, found the database of decryption keys and released CryptoDefense.
2015, CryptoWall [1]	▪ CryptoWall passed Cryptolocker as the leading version of ransomware.

The year 2011 was very tough for internet user because of the attacked by bulk ransomware. In this year more than 30,000 sample was found in two starting quarter while 60000 ransomware sample attacked in third. the again year 2015 was found as a golden year for ransomware criminals. In this year a new kind of cryptolocker was introduced while a TOR website started ransomware as a service. This website provided ransomware on the commission of 20%.

A. After Ransom-as- a-Service:

After providing a ransomware on rent or commission, a frequency of ransomware attack has been increased, that is why researcher classifies the evolution into two parts as before and as after ransomware.

Table 2: Evolution of ransomware after Ransom-as-a-service

Year, Name	**Description**
May 2015, ransomware-as-a-service [1]	▪ Using a TOR website, attackers could create ransomware for free. ▪ The site handles payment and takes a 20 percent cut of the ransom.
2015, Tor sites [1]	▪ As the name implies, it targets Linux systems. It encrypts both data files and files associated with web applications.
September, 2015,LockerPin [1]	▪ It infects Android systems and changes the PIN.
Nov,2015 Linus.Encoder.1 [1]	▪ In was discovered by Dr.Web, a Russian computer security firm.
November, fourth iteration of CryptoWall [1]	▪ It includes a modified protocol to help avoid detection. ▪ Additionally, it alters the file names when it encrypts files, making it harder to determine what files were actually encrypted.
January, 2016. JavaScript-only[1]	▪ It is a ransomware-as-a-service; ▪ multi-platform attack, including Linus and MacOS X.
April, Petya[1]	▪ Makes the whole hard disk inaccessible until the ransom is paid . ▪ It does this by overwriting the master boot record (MBR) of the infected computer. ▪ Without the MBR, the operating system cannot reconstruct the unencrypted files .
KeRanger, Jan, 2016[1]	▪ KeRanger is first ransomware attack targeting Apple system; ▪ It takes three days to activate and is designed to encrypt more than 300 file types.
Xbot, feb 2016[1]	▪ To target Android devices in Australia and Russia. ▪ Tries to steal online banking details.
Jigsaw, 2016 [8,]	▪ Embeds an image of the clown from the Saw movies into a spam email. ransom payment of $150, according to Webroot.
Locky, July 2016[1]	▪ added a failsfe mechanism that begins encrypting files even if the ransomware cannot request a unique encryption key from the criminals' servers due to the target computer either being offline or blocking the communications (Constantin, 2016c).
NotPetya, 2017 [8]	▪ It comes with a fake software update, harms systems of more than 100 countries.
Jeff, 2017 [8]	▪ It attacked in May 2017 with spam mail and collected money in form of bitcoin.

Few ransomware with initial characteristics [3]:

Name	**Characteristics**
Samsam.exe	MD5 : a14ea969014b1145382ffcd508d10156 SHA1: ff6aa732320d21697024994944cf66f7c553c9cd Type :PE32 executable size: 218.624 bytes
Del.exe	MD5 : e189b5ce11618bb7880e9b09b09d53a588f SHA1: 964f7144780aff59d48da184daa56b1704a86968 Type : PE32 executable Size : 155,736 bytes
Selfdel.exe	MD5 : e189b5ce11618bb7880e9b09b09d53a588f SHA1: 964f7144780aff59d48da184daa56b1704a86968 Type : PE32 executable Size : 155,736 bytes

Other Ransomware are also tried to follow same structure with MD5 And SHA1 while every criminal tried to make it tough to toughest. Rest of the paper organizes as section 2, gives a light on evolution of ransomware yearly, whereas section three show the stages of attack by ransomware.

B. Recent Ransomware:

WannaCry [5,6]*:* It is just a ransomware with a computer worm, On May 12, 2017, it is a first attack the machines of across the globe through a malicious link or by opening an infected mail. As per various newspapers, this ransomware, within a day was reported to have infected more than 200,000 computers in over 150 countries. It affected some old unpatched MS windows systems of those people, who did not performed security updation of Operating system with exact patch, as per advisory of Microsoft that was released before 2 month by Microsoft on 14 March 2017 to remove few vulnerability noticed by them.

III. INFECTION BY RANSOMWARE

Once infected, a user has four options:

- Ø Pay the ransom
- Ø Restore from backup
- Ø Lose the files
- Ø Brute force the key

To brute force, the key would require factoring 617-digit numbers, which would take about 6.4 quadrillion years on a standard desktop computer [1].

3(a). Data on Infection

Symantec uses telemetry data to track ransomware infections by country. The rankings are shown in table 1 below. For the most part, criminals are targeting large or affluent countries [1].

In initial days ransomware was attacked on Windows platform but in these days it is able to infect Apple and Android systems, even few are also in the air to infect Smart watches that come into the category of IoT devices. Now ransomware moving to IoT, as services moving from Internet to world. From year 2016, SVG (scalable vector graphics) is a new method of a cyberattack. SVG files are a file that allows system code, such as JavaScript, to be embedded in the graphic. This code can be run through a browser [1]. Few codes and techniques also in the air to decrypt the files of the victim such as Popcorn Time allows a free decryption to files of victims if infected [1].

3 (b). An Infected Machine

Dealing with ransomware is a costly job even if has backed up and not going to pay; because correction of a system can take days to weeks. So after infection, a machine has limited options to operate. Ransomware does not destroy data. Rather, it locks up the data until a ransom is paid.

Antivirus company AVG recommends the following steps:

Step 1: Run a full scan to find out the ransomware used.

Step 2: Copy the encrypted files to a USB drive so they can be decrypted on an uninfected computer.

Step 3: Use a tool to decrypt the files on the USB drive. AVG provides free tools for decrypting six Ransomware strains: Apocalypse, BadBlcok, Crypt888, Legion, SZFLocker, and TeslaCrypt.

When files recovered ok in any way ransomware must be removed.

IV. TARGETS FOR RANSOMWARE

4(a). User wise:

The Average User: All age group considered as a target to get ransom, but it people who are not a technical personal pressurize easily. Attackers sometimes increase pressure by including a timer with the increment ransom amount. A solution of ransomware like Teslacrypt is coming in form of TeslaDecoder but if people do not use through with the decoding of the encrypted file then ransomware can do their job even it is easily decodable. Individual users are targeted because they pay ransom due to the fear of corrupted files and not having a backup for valuable data. On the other hand organizational members due to business secrecy sometimes they pay due to not having cybersecurity personnel.

As per Symantec 25% home users not having a backup, 55 % backup some files and only 25 % has regular backed up in a week. The rest only made backups sometimes.

Businesses: Businesses are on priority for a ransomware because their systems are the house of valuable database with sensitive data, important documents, and other information; in the meantime, they have general system updated and tried to secure. Crypto ransomware focuses to target the corporate network or individual systems to be spread in the whole network.

Emergency Services: Ransomware targets these organizations also due to Multi-State Information Sharing and its importance by which it can pay the cost of delay in terms of lives. Most vulnerable emergency services are law enforcement, fire departments, and hospital chains. On the other hand healthcare sector is not a traditional target for few years these also targeted including the example of Hollywood Presbyterian Hospital Medical Center which was infected with the Locky.

ransomware.

Financial Institutions: The banking and finance sector is the frequent target of ransomware schemes including botnet like problems. Dyre, Dridex, and Ramnit are botnets included especially for the banking sectors.

Educational Institutions, religious organization are also the favorite target of ransomware criminals due to these having all the costly data with least security mechanism.

4(b). System wise:

All kind of system is valuable to the user and also might be a target for ransomware due to the profitability target system including:

Personal computers (PC): PCs are the current primary target of ransomware due to easily compromise. These systems are generally used un-updated OS and software. Ransomware variants are designed to target various OS but windows systems are soft target generally.

Mobile devices: Ransomware currently active in the air for smartphone also.

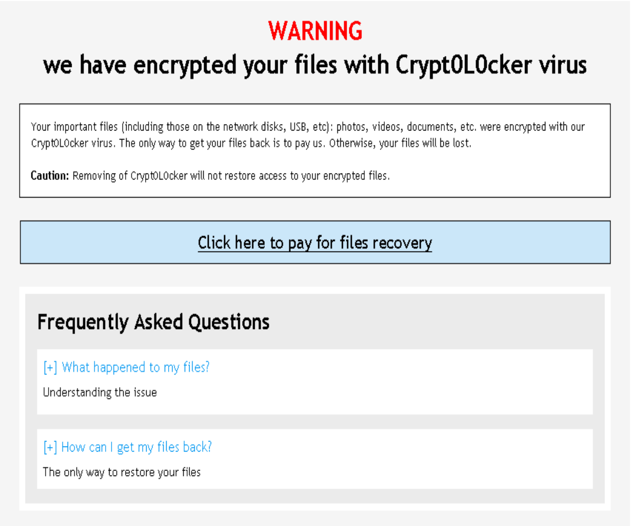
Servers: An organization's servers and databases store all of their critical information. Within a server are an organization's documents, databases, intellectual property, personnel files, client list, and other intangible resources. The compromise of one essential server can hobble an organization. Despite their value, organizations regularly fail to secure, update, and patch the systems. This makes servers susceptible to lateral movement and attack. When a server is compromised, the organization goes into a panic. Even if the attack is a ransomware attack, there is a concern for reputational harm due to the perception of lost customer data. Even if the organization has a business continuity plan or disaster recovery plan, the amount of time necessary to revert to a redundancy system may be unacceptable.

PAYMENT METHODS [4]:

Bitcoins is the first choice for criminals but in general we can say digital payment mechanism is the choice of criminals.

Bitcoins: Bitcoins is a kind of cryptocurrency that can be assumed as an electronic coin. It allow people to transfer digital payment from one end to another. It is an easy system of payment due to not involving any financial institution in the process for any kind of activity as a mediator.

To find out a payment a ransomware instructs to victims as:



WARNING

we have encrypted your files with Crypt0L0cker virus

Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our Crypt0L0cker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.

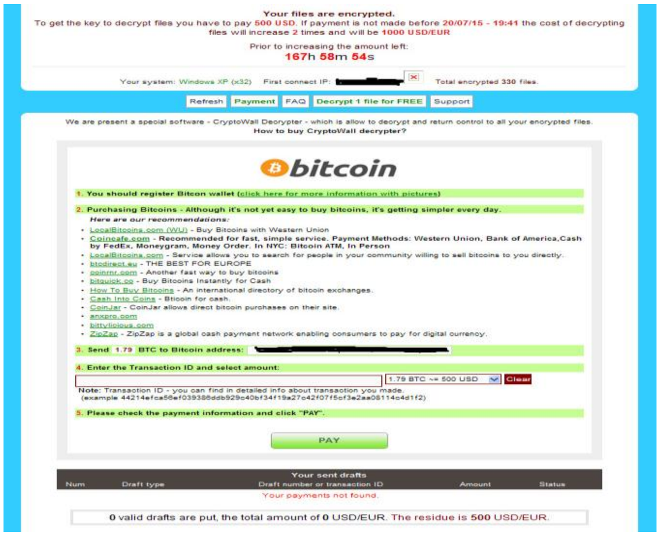
Caution: Removing of Crypt0L0cker will not restore access to your encrypted files.

Frequently Asked Questions

Understanding the issue

The only way to restore your files

Figure 4(A): Cryptolocker's message[4]



Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD. If payment is not made before 20/07/15 - 19:41 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:

167h 58m 54s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted 330 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- btcdirect.eu - THE BEST FOR EUROPE
- coinrnr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bticoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 1.79 BTC to Bitcoin address: [redacted]
4. Enter the Transaction ID and select amount:

1.79 BTC ~= 500 USD

Note: Transaction ID - you can find in detailed info about transaction you made. (example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. Please check the payment information and click "PAY".

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status
		Your payments not found.		

0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 500 USD/EUR.

Figure 4(B): Ransom message to pay[4]

V. SAFETY METHOD

Mobile phone also found attacked by ransomware as other machines, while data recovery from a ransomware affected system can be done by a forensic tool as per described by PH Rughani [9], who tested the practical over android phone and found better success rate on SD card than phone.

To deal with ransomware experts given few suggestions to use before and after infection as:

Step 1: Back Up

Step 2: Avoid all spam links if unknown.
Use Ad blockers can protect against malvertising.
Turning off Java and JavaScript.

Step 3: Patch and Block
All the OS, browsers, and security system should always be kept patched and up-to-date including third-party plug-ins, like Java and Flash.

Step 4: Drop-and-Roll
If a machine found the sign of infection, then to minimize the infection infected machine should immediately turn off, the network also should be turned off if this machine is on the network [1].

On the basis of case studies, to deal with ransomware, few suggestions are as:

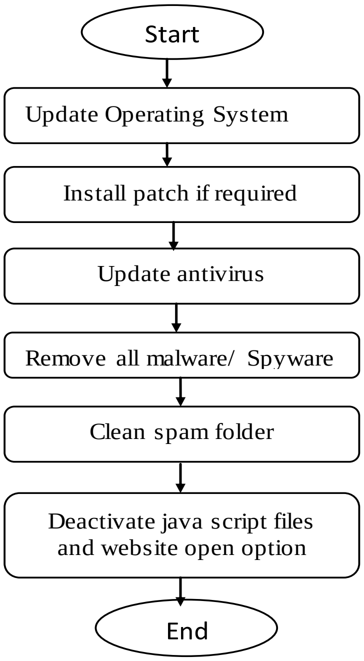

Start
Update Operating System
Install patch if required
Update antivirus
Remove all malware/ Spyware
Clean spam folder
Deactivate java script files and website open option
End

Figure 5: Flowchart to deal with ransomware

1. To save a system from ransomware attack first step to update the operating system, sometimes it requires the patches thus installation of patches is next step.
2. Do not use Operating System that is not supporting.
3. Tasks of step 1 are meaningless if the system does not have any updated antivirus, so it is a suggestion that system must have a good quality antivirus.
4. Cleaning of spam folder must be the next step after a removal of all malware/spyware.
5. Javascript files and website open option is risky so deactivate it at the end of all precautions.

VI. CONCLUSION FUTURE WORK

This work presents few facts about ransomware with its working and suggestion to save computers from attack. It shows safety guidelines from ransomware that will be helpful to researchers as well as society to save data in near future. The review discusses a picture of the evolution of ransomware with its effects on the system, way of working and tricks to save our data during the attack.

REFERENCES

[1]. R. Richardson and M. Nort, Ransomware: Evolution, Mitigation and Prevention", International Management Review, Vol. 13, No. 1 2017.

[2]. An Osterman Research, "Best Practices for Dealing With Phishing and Ransomware SPON", White Paper Published September 2016.

[3]. C.Beek and A. Furtak, "Targeted ransomware No Longer a Future Threat: Analysis of a targeted and manual ransomware campaign", Advanced Threat Research, Intel security, feb2016.

[4]. J. Wyke and A. Ajjan, "The Current State of Ransomware", A SophosLabs technical paper December 2015.

[5]. WannaCry Response, Metasys, Johnson Control, June 2017.

[6]. WannaCry Rensomware Analysis, White paper, May 2017, Stream scan.

[7]. B. N. Giri, N. Jyoti, Mc. A. AVERT, AVAR 2006, Auckland. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.5881&rep=rep1&type=pdf

[8]. P. Bihola, R. Sheth, "Emerging Threats of 2017: Ransomware, IOC's", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2 | Issue 6, pp.-996-1003.

[9]. P.H. Rughani, Data recovery from ransomware affectedandroid phone using forensic tools, vo.-5, issue-8, International Journal of Computer science and Engineering, pp. 67-70.

Authors Profile

Mr. A. K. Maurya completed his B.tech(CSE), from UPTU, Lucknow 2006 and M.Tech(IT) in 2010 from IIIT Allahabad(India). He is currently workig in Dr. RML Awadh Universities, Faizabad as a Assistant Professor in IT department since last 5 years. His main research work focuses on Computer Networks, Wireless communication and Network Security.

Mr N. Kumar completed his B.Tech(CSE) and M. Tech(IT) from UPTU, Lucknow and IIIT Allahabad in year 2005 and 2010, respectively. He is currently pursuing Ph.D. in IT from BBAU, Lucknow. He has published saveral pepers in reputed journals and conferences. His research work focuses on Applications of Network, Network Security, WSN and IoT. He has more than 5 years of teaching and research experience.

Dr. Alka is an Assistant Professor in the Department of Information Technology, BBAUniversity (A Central University), Lucknow (India). Dr. Alka has done her Ph.D. from Department of Information Technology, from BBAUniversity Lucknow. She has published four patents and authored two books on Software Engineering and Software Vulnerability. She has published several research papers in National, International Journals and conference proceedings. Her areas of expertise are Software Security and Software Usability.

Prof. R. A. Khan, Professor & Dean, School for Information Science and Technology, BBA University, Lucknow (INDIA) Dr. R A. Khan done MCA from Punjab Technical University & Ph.D. (Computer Science) from Jamia Millia Islamia (Central University), New Delhi. He has published six patents and written Eight books in Software Engineering, published more than hundered articles in the National and International journals and conference proceedings. The area of expertise are Software Quality Assurance, Software Security. He has done many projects on Software Security and also member of various professional bodies.