

# Risk Key

ISACA—Chennai, Issue # 3, July 1, 2009

## President's column

Dear Readers

*In our journey of securing information, in the initial stages, lot of attention, time and money might have been spent on Technology to safeguard our information and infrastructure. While on the journey, we realize time and again that in spite such investments, majority of failures happen mainly due to lax security policies and non adherence to preventive steps, non-monitoring etc.*

*In this issue, some of the articles provide a good reminder about the need for robust people process to get the maximum benefit out of technology.*

*As a part of our mission to enable members to constantly upgrade themselves to cope up with ever increasing challenges, we have arranged a three day seminar on "Core Banking solutions" with the help of external agency, having lot of experience in conducting the program on the subject.*

*By the time you read this newsletter, the seminar might have been successfully conducted. Based on the feedback and experience of participants, we would endeavor to arrange similar program in future as well, on select and cotemporary subjects for the benefit of members.*

*I take this opportunity to thank all our member fraternity for the overwhelming support for all the initiatives of our chapter*



*With Best Wishes*  
**NSN PILLAI**  
Chapter President

## Conficker Worm

Early computer viruses were mostly executable programs like .exe, .bat etc that typically spread via shared infected computer disks. The first computer virus to appear in the "wild" was the "Elk Cloner" virus that appeared in 1981 and spread via floppy disks affecting Apple II OS. Much has changed since then.

Malicious code that once used a floppy disk to proliferate now rides the internet to the final destination. This became evident on March 26, 1999, when a first new breed of virus dubbed "Melissa" made its debut as the first in-the-wild virus that used the information super highway to accelerate its spread. It affected about 1 lakh computers in the first 24 hours. Arrival of "I Love You" virus on May 4, 2000 signaled yet another major change in the computing industry where viruses are concerned. Over a five-hour period, this virus spread across Asia, Europe and the United States via e-mail messages. The menace clogged Web servers, overwrote personal files and caused corporate IT managers to shut down e-mail systems. While the earlier forms of viruses were relatively benign and more of a prank, newer worms and viruses have grown more sophisticated, virulent and malicious and can now cause world wide damage in a relatively short time.

A virus/worm currently causing serious concern is the Conficker worm, a.k.a.

Downadup/Kido worm. According to experts it is the worst infection since the SQL Slammer. Estimates of the number of computers infected range from almost 9 million to 15 million computers, however a conservative minimum estimate is more like 3 million which is more than enough to

cause great harm. The Cyber Security Institute claims that depending on the number of infections world wide, cost of Conficker worm to governments, businesses and individuals could reach as much as \$9.1 billion in terms of wasted time, resources, energy as well as direct cost of countermeasures.

### What is Conficker Worm?

The Conficker Worm is a computer worm which consist self replicating mechanisms and specifically designed to infect Microsoft Windows Systems. The Conficker Worm can spread itself and infect Microsoft Windows System from a removable drive, a network share or across network automatically, without human intervention. It spreads by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability. If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled. The worm instructs the target computer to download a copy of the worm from the host computer via HTTP protocol using the random port opened by the worm. It disables a number of system services such as Windows Automatic Update, Windows Security Center, Windows Defender and Windows Error Reporting and Internet connection sharing service. Conficker is known to block access to over 100 anti-virus and security websites. Some of the variants can also spread through corporate networks by infecting USB sticks and accessing weak passwords. It propagates by creating an autorun.inf file on all mapped drives so that it automatically executed as soon as the drive becomes accessible.

*(Continued on the next page)*

#15, Ground Floor, Luz Golden Enclave  
(TNHB Complex Next to Kamadhenu Theatre)  
180/4 Luz Church Road,  
Mylapore, Chennai 600004

Telephone # +91-44- 2498 4331

# Coficker Worm (contd...)

The first version of Conficker worm, called Conficker.A was discovered in November 2008. Since then the following variants of Conficker worm are discovered:

Win32/Conficker.A , Win32/Conficker.B  
Win32/Conficker.C, Win32/Conficker.D,  
Win32/Conficker.E

The computer systems which are up-to-date with the latest security updates issued by Microsoft and anti-virus software up-to-date with the latest virus definitions are protected from Conficker worm.

## Countermeasures

The following are the suggested counter measures when infected with Conficker Worm:

- Delete file created by the worm
- Delete the registry entries made by the Worm
- Apply appropriate patches as mentioned in [CERT-In \(CIVN-2008-170\)](#)
- Disable autoplay/autorun features on all drives and devices.
- Block ports 139 and 445 at the pe-

## Conficker Eye Chart



## Determine Infection

It is quite simple to determine whether a computer system is infected with the Conficker worm or not. Users are advised to apply a simple test for checking the presence of Conficker/Downadup/Kido worm on their systems. The presence of a Conficker worm infection could be determined if the users are unable to access websites of information security agencies, such as: <http://www.cert-in.org.in>, <http://www.avg.com>, <http://www.f-secure.com>, <http://www.mcafee.com>, <http://www.symantec.com>, <http://www.trendmicro.com>.

Conficker Eye Chart at [http://www.confickerworkinggroup.org/infection\\_test/cfeyechart.html](http://www.confickerworkinggroup.org/infection_test/cfeyechart.html)

can also indicate if infected or not.

Users may also try Windows Live Safety Scanner (online scanning tool) for determining infection or install/execute any of the tools suggested in the solution section by CERT-IN in their virus alert [http://www.cert-in.org.in/virus/win32\\_conficker.htm](http://www.cert-in.org.in/virus/win32_conficker.htm).

rimeter.

- Install and maintain updated anti-virus software at gateway and desktop level
- Install and maintain Desktop Firewall and block the ports which are not required
- Use caution when opening attachments and accepting file transfers
- Use caution when clicking on links to web pages
- Refer the following Guidance articles for protection against Conficker worm.

(References : [http://www.cert-in.org.in/virus/win32\\_conficker.htm](http://www.cert-in.org.in/virus/win32_conficker.htm), <http://www.confickerworkinggroup.org/wiki/>)

For circulation among members of ISACA only. Not for sale.

Please provide your feedback on the newsletter. It will help us to serve you better.

*This issue is edited & Published by K.B.Sankaran on behalf of EDITORIAL COMMITTEE OF ISACA, CHENNAI. Emani BSP Sarathy is the advisor to the Editorial Committee.*

## Looking Back



A section of the participants



K.B.Sankaran proposing vote of thanks



## Speakers and panelist

**ISACA Chennai Chapter conducted a one day seminar on 'Business Continuity management system- an overview' on April 25, 2009 at Industrial Consultancy & Sponsored Research Centre ( IC & RC) IIT Madras**

## Practical Cryptography

Cryptography a word with Greek origin, means "Secret Writing". However the current usage of the term refers to the art and science of transforming messages to make them secure and immune to attacks. Early forms of Cryptography dealt with mainly Confidentiality through encryption/decryption mechanisms where as modern Cryptography deals with other goals such as authentication, integrity and non-repudiation as well. These requirements have in fact become mandatory in the current scenario of on-line transactions and e-commerce business needs Privacy and Confidentiality guarantees the sender that only the authorized user can access/read the communication. Authentication and Integrity guarantees to the receiver, the identity of the sender, message is not modified and that no undue delay has occurred. Non-Repudiation service protects against repudiation by either the sender or the receiver. Components of basic cryptography are:

- Secret key or Symmetric key encryption.
- Public key or Asymmetric key encryption
- One way Hash functions

While the symmetric key encryption as the name suggests both the sender and receiver use identical keys to encrypt and decrypt. In asymmetric key encryption, a pair of keys, inversely related to each other are used. This means that what is encrypted with one key can be decrypted only with the other corresponding key in the pair. Hash functions convert a string of data of any size into a fixed length hash. The key properties of these hash functions are that even a slight modification like a comma or a full stop will change the hash, no two strings will result in the same hash and it is not possible to recover the original data from the hash. Some of security problems solved by cryptography are:

- Privacy and Confidentiality of stored data, messages and conversations.
- Transaction Integrity and Non-Repudiation
- User and Data Authentication
- Secure Audit Logs

Some of the typical applications are:

- Secure e-mail
- Confidentiality of files and directories
- Virtual Private Networks
- Web Security
- E-Commerce

### 1. Secure e-mail

Unlike IPSec and SSL where two parties create a session for secure exchange of

data, e-mail is a one-time activity and if so the issue is how can the sender and receiver agree on a cryptographic algorithm?. The sender has to therefore include in the message name or identifier of the algorithms. Most e-mail security protocols today require encryption/decryption to be done using a symmetric key algorithm and one-time secret key sent along with the message. The secret key is encrypted with the public key of the receiver. Two common protocols that deal with secure e-mail are PGP (Pretty Good Privacy) – Open PGP Standard, RFC 2440 and S/MIME (Secure Multipurpose Internet

Mail Extensions) – Message Specification, RFC 3851.

### 2. Confidentiality of Files and Directories

Concerns and Solutions are similar to e-mail. The software solutions establish and maintain encrypted files, folders and storage volume and the encryption is often on-the-fly meaning that data is automatically encrypted and decrypted right before it is loaded or saved with out user intervention. No data on the encrypted volume can be read with out using the right password or encryption key.

### 3. Virtual Private Networks

Most modern enterprises cross international boundaries and so are the partnerships. Privacy of business transactions is critical to success. Network connections privacy means deploying cryptography. VPN goals are confidentiality of communication, access for remote entities/employees and controlled access for clients. A study reveals that using encrypted tunnels over the internet to connect LANs and WANs can reduce the cost up to 50%. Secure VPNs use the tunneling mechanism to carry data on public Internet lines. In tunneling data is transmitted through a public network in such a way that routing nodes in the public network are unaware that the transmission is a part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network protocol data so that the tunneled data is not available to anyone to examine the transmitted data frames. IPSec and SSL are commonly used to secure VPNs. Recent technological trend is to harnesses IP Infrastructure based on MPLS Technology for IP VPN services. MPLS is an acronym for "Multi Protocol Label Switching". MPLS VPN service providers claim to offer reduced customer networking complexity and costs and totally do away with the requirement of in-house technical work force.

### 4. Web Security.

Enterprise today deploy web sites for both internal and external use. Protection of

these sites from unauthorized modifications and controlling access is vital. Message hash of all the files on the web site are kept in a database and periodic checking of the stored hashes is done with the hashes of the web pages is done. This is known as Integrity Checking. In addition the web pages can also be digitally signed.

### 5. E-Commerce.

Growth and development that E-Commerce has witnessed, is unthinkable without application of modern cryptography. In fact the IT Act 2000 was enacted to promote e-commerce and e-governance as the preamble to the act clearly states "An act to provide legal recognition for transactions carried out by means electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involves the use alternative to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies ....."

PKI (Public Key Infrastructure) has been established with the setting up of a Controller of Certifying Authorities who in turn will control Certifying Authorities for issue of Digital Certificates and related matters. CAs' issue three classes of digital certificates – Class 1, Class 2 and Class 3 for various purposes and varying levels of assurance. Class 1 certificates generally serve e-mail applications for encryption and digitally signing. As they do not provide strong authentication of user identity, they are not applicable for commercial use. Class 2 certificates are applicable to personal and commercial use in environments requiring obligatory identity proof, typically like participating in e-tenders etc. Class 3 certificates represent the highest degree of digital security available to individuals, devices, servers and organizations. Typically, they are used for Electronic Data Exchange (EDI), internet banking/broking, e-commerce and other web-based transactions.

---

ISACA Chennai Chapter will be holding its Annual General Meeting

---

## From the Print Media

The Economic Times –July 8, 2009

Worldwide IT spending likely to fall 6% to \$3.2 trillion: Gartner as against \$3.6 trillion recorded in 2008

- IT budgets are still being cut
- Spending on hardware to decline by 16.3%, software by 1.6%, IT services by 5.6% in 2009