Cyber Security Concepts & Threats

Prof. P. S. Avadhani,
M. Tech., PhD., F.I.E.
Professor
AU College of Engineering(A)
ANDHRA UNIVERSITY
Visakhapatnam
Preamble
What is Cyber Security?

- Cyber security is about to protect the cyber world in terms of Confidentiality, Integrity, and Availability.
- Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.
What is Cyber(E)- crime?

- Any Unlawful act wherein the computer is either a tool or a target or both or Crime committed over Internet.

The Department of Justice categorizes computer crime in three ways:

- Computer as a target - attacking the others’ computers
  (Ex: spreading viruses).
- Computer as a weapon - using a computer to commit "traditional crime" that we see in the physical world (such as fraud or illegal gambling).
- The computer as an accessory - using a computer as a cabinet to store illegal or stolen information.
Various types of cyber crimes

- Financial Crimes
- Online gambling
- Intellectual Property Crimes
- Email Spoofing
- Forgery
- Cyber Pornography
- Cyber stalking
- Web defacement
- Trolling
Various types of cyber crimes (contd..)

- Time Bombing
- Data Diddling
- Denial of Service Attack
- Virus/WORM attack
- Trojans and Key loggers
- Internet Time Theft
- Web Jacking
- Email Frauds
- Cyber Terrorism
Security Vulnerabilities

• Customer Ignorance
• Disgruntled Employees
• Lack of proper security policy
• Misplaced confidence in among peers
  – Giving information informally
• Improper shutting down/ closing of the system
Issues

• Loss of Individual Privacy
• Authentication
• Loss of Confidentiality
• Loss of Credibility
• Data manipulation (Denmark Example)
• Data Protection (Not possible to tamper with)
• Data Maintenance (update/Modify when needed, like change of address in AADHAR card etc)
Problems that can lead to...

- Blackmailing
- Trolling
- DOS and DDOS Attacks
- Replay attack (Creating Delay)
- Interruption
- Interception
- Modification
- Fabrication
Concepts
Basic Concepts of Security

• **Confidentiality**: limiting information access and disclosure to authorized users -- "the right people" -- and preventing access by or disclosure to unauthorized ones -- "the wrong people".

• **Authentication**: process by which a system/person verifies the identity of a User who wants access to some resource. Access Control is normally based on the identity of the User who requests access to a resource.
Methods

• Symmetric Key Encryption

• Asymmetric / Public Key Encryption
Symmetric Key Encryption

• It is a form of computerized cryptography using a single encryption key to guise an electronic message.

• Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message.

• Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.
Symmetric Key Encryption Cont’d…

Original data → Symmetric key → Scrambled data → Symmetric key → Original data

Dear Ali: I have reviewed the new...

$\beta_f \neq 4h19 / r \beta x 8a + t (...) x 1_-$
Asymmetric/ Public Key Encryption

• Public-key encryption involves a pair of keys—a **public key** and a **private key**—associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data.

• Each public key is published, and the corresponding private key is kept secret.

• Data encrypted with your public key can be decrypted only with your private key.
Asymmetric/ Public Key Encryption

Cont’d…

- Original data
- Public key
- Scrambled data
- Private key
- Original data
Some Definitions

• **Hashing:** Extracting the sensitive part of a message of fixed size such that any change in the message reflects in hashing of that message.

• **Message Digest:** Hashed Message

• **Digital Signature:** is an encrypted message digest.

• It is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is **authentic**.
Authentication Using Digital Signature
Some Definitions

• **Digital Envelope**: A digital envelope is a secure electronic data container that is used to protect a message through encryption for data authentication.

• A digital envelope allows users to encrypt data with the secret and public key encryption.

• A digital envelope is also known as a **digital wrapper**.
Some Definitions  Cont’d…

• **Session Key**: is a single-use symmetric key used for encrypting all messages in one communication session.

• The key is invalid once the stipulated session time expires.
Authentication Methods

• Passwords
• Biometrics
  – Finger
  – Hand
  – Face
  – Iris
  – CAPTCHAs (Limited Applicability)
Digital Certification

• The Digital Certificate is a common credential that provides a means to verify identity of an entity.

• A trusted organization assigns a certificate to an individual or an entity that associates a public key with the individual.

• The individual or entity to whom a certificate is issued is called the subject of that certificate.
Digital Certification

• The trusted organization that issues the certificate is a **Certification Authority (CA)** and is known as the certificate's issuer.

• A trustworthy CA will only issue a certificate after verifying the identity of the certificate's subject.
Digital Certificate – X.509

• An X.509 certificate binds a name to a public key value.

• The role of the certificate is to associate a public key with the identity contained in the X.509 certificate.

• An X.509 certificate contains information about the certificate subject and the certificate issuer.
## Structure of X.509

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A subject name (DN)</td>
<td>A subject name (DN) that identifies the certificate owner.</td>
</tr>
<tr>
<td>The public key</td>
<td>The public key associated with the subject.</td>
</tr>
<tr>
<td>X.509 version information</td>
<td>X.509 version information.</td>
</tr>
<tr>
<td>A serial number</td>
<td>A serial number that uniquely identifies the certificate.</td>
</tr>
<tr>
<td>An issuer DN</td>
<td>An issuer DN that identifies the CA that issued the certificate.</td>
</tr>
<tr>
<td>Validity (Start and end Time)</td>
<td>Validity (Start and end Time).</td>
</tr>
<tr>
<td>The digital signature of the issuer.</td>
<td>The digital signature of the issuer.</td>
</tr>
<tr>
<td>Information about the algorithm used to sign</td>
<td>Information about the algorithm used to sign the certificate.</td>
</tr>
<tr>
<td>the certificate.</td>
<td></td>
</tr>
<tr>
<td>Some optional X.509 v.3 extensions; for example, an extension exists that distinguishes</td>
<td>Some optional X.509 v.3 extensions; for example, an extension exists that distinguishes between CA certificates and end-entity certificates.</td>
</tr>
</tbody>
</table>
SSL

• Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network.
• It creates a secure link between a Web server and browser to ensure private and integral data transmission.
• SSL uses Transport Control Protocol (TCP) for communication.
Objectives of SSL

Data integrity: Data is protected from tampering.

- Data privacy: Data privacy is ensured through a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change Cipher Spec Protocol and SSL Alert Protocol.

- Client-server authentication: The SSL protocol uses standard cryptographic techniques to authenticate the client and server.
SET

- A Secure Electronic Transaction (SET) is an open-source and cryptography-based protocol for secure payment processing via non-secure networks.

- SET was replaced by more advanced systems, such VISA’s 3-D Secure.

- In 1996, SET was launched and backed by VISA, MasterCard and other payment processing industry leaders.

- SET’s blinding algorithm ensures data confidentiality, data integrity and cardholder/merchant authentication.
The SET system includes the following components:

- Merchant
- Cardholder/acquirer
- Card issuer
- Payment gateway
- Certification authority (CA)
- **Dual signature**: A guaranteed SET data integrity innovation that links two different recipient messages
Turing Test

• Devised by Alan Turing to identify whether a machine is intelligent or not.

• A Human being and Machine are kept in two closed rooms connected to a questioner. If the machine can fool the questioner that it is a human being then the machine is intelligent.
CAPTCHAs

- CAPTCHAs establishes Humanness

- Completely Automated Public Turing test to tell Computers and Humans Apart, better known as CAPTCHA, is a test to ensure responses through a human versus a computer program.

- CAPTCHA was developed at Carnegie Mellon University by Nicholas J. Hopper, John Langford, Luis von Ahn and Manuel Blum.
Printed CAPTCHAs
Easy?

(Google)  (Yahoo!)
CAPTCHAs

The test was really hard. They showed me several unknown paintings and I had to fill in artist, historical episode and year of painting.

Wow! That sounds difficult! Did you pass the exam and get your master degree?

Exam? Master degree? It was a captcha.

In the future sophisticated captchas will lock out any bot.
Non-Text CAPTCHAs

• Secret Database
• Relies on Binary Classification
Re CAPTCHA
Cyber Forensics

- Cyber forensics is an electronic discovery technique used to determine and reveal technical criminal evidence.
- It often involves electronic data storage extraction for legal purposes.
- It is gaining importance as a viable way of interpreting evidence.
- Cyber forensics is also known as computer forensics.
Cyber Forensics

• Cybercrimes cover a broad spectrum, from email scams to downloading copyrighted works for distribution, and are fueled by a desire to profit from another person's intellectual property or private information.

• Cyber forensics can readily display a digital audit trail for analysis by experts or law enforcement.

• Developers often build program applications to combat and capture online criminals; these applications are the crux of cyber forensics.
Cyber Forensics

• Cyber forensic techniques include:
  
  – Printed-text CAPTCHAs that are prone segmentation attack
  – Cross-driven analysis that correlates data from multiple hard drives
  – Live analysis, which obtains data acquisitions before a PC is shut down
  – Deleted file recovery

• Each of the above techniques is applied to cyber forensic investigations.
System forensics can be done on standalone machines

- Data forensics major focuses on analysis of volatile and non-volatile data
- Memory forensics is similar to data forensics but deals data in raw form and carving the data from the raw dump
- Disk forensics deals with extracting evidence from storage media by searching active, deleted files and also from unallocated, slack spaces
- Database forensics is the study of databases and their related metadata
Types of Cyber Forensics

Other cyber forensics areas are proactive, enterprise and anti-forensics

• Proactive forensics is an ongoing forensics and there is an opportunity to actively, and regularly collect potential evidence in an ongoing basis

• Enterprise forensics is named in the context of enterprise; it is primarily concerned with incident response and recovery with little concern about evidence

• Anti-forensics emerged as one area, due to increase in the awareness of cyber criminals in the field of computer forensics, these criminal are following counter measures to forensics analysis
Types of Cyber Forensics

Network forensics involves the collection and analysis of network events in order to discover the sources of security attacks

• Wireless forensics provides the methodology and tools required to collect and analyze wireless network traffic data

• Router Forensics comes into picture when hacker has full control of the networks, then router forensics focuses on collecting evidence from configuration errors or known vulnerabilities
Types of Cyber Forensics

• Email forensics deals with one or more e-mails as evidence in forensic investigation
• Malware forensics investigates about analyzing malicious code for identification of malware, studies about payload and damage happened due to presence of malware
• Examining and analyzing mobile devices comes under mobile device forensics
Cyber Forensics Principles

Data Integrity

Free from Contamination

Full Documentation

Scientific Methodology

Cyber Forensics Examination
Goal of Cyber Forensic Investigation

- Determine how they broke in?
- Determine what damage was done?
- Determine who did it (attribution)?
- Where else did they go?
- Meet legal requirements, reduce liability
- Support prosecution
- Find the truth
  - Forensic examiner is a finder of fact
  - He or she seeks the truth
The Cyber Forensic Process

• Six stages

1) Identification
2) Acquiring (Mirroring/cloning/imaging)
3) Authenticating (Hashing)
4) Analysis (In readable form)
5) Documentation
6) Testimony
Acquire

- **System**
  - Live system
    - Collect
      - Volatile data
      - RAM dump
    - Shut down
- **Physical backup & not logical backup**
  - Disk cloning/imaging/mirroring
Forensic Duplication (Imaging) Approaches

• Three Approaches
  – Blocker acquisition
    • Remove the storage media from the suspect computer and attaching it to the forensic workstation via blocker device.

  – Disk- Disk acquisition
    • Image storage media by attaching a hard drive to the suspect computer.

  – Network acquisition
    • Client – Server
Authenticate (Image Validation)

- Hash Value
- Encase
  - MD5, CRC (every 32K)
- FTK
  - MD5, SHA-1
- ProDiscover
  - MD5 or SHA1 hash
- Winhex/X-Ways Forensic
  - Mass hash calculation for files
    (CRC32, MD5, SHA-1, SHA-256, PSCHF, ...)

[Image of a woman looking frustrated at a computer]
Analysis (Onion Model)

- Physical Media
- Operating System
- File System
- File
- Content Analysis
Analysis

• Extract, process, interpret
  – Extract - may produce binary 'junk' that isn't human readable
  – Process - make it humanly readable
  – Interpret - requires a deeper understanding of how things fit together

• Tools available to view files outside of native application
  – Quick view plus and conversions plus
Files to be Examined

• **Mostly three types**
  – User created files
    • .doc, .xls, database, image files etc.,
  – User protected files
    • Encryption, password protection, steganography, file extension
  – Computer created files
    • Temp. files, printer spool files, metadata, index files, cookies, temp, Internet files etc.,
    • Recycle bin
    • Registry information

• **Fourth category**
  – Unallocated space
Where Incrementing Data is Stored?

- Four areas
  - Active space
  - Slack space
  - Unallocated space
  - Swap files
Finding data the User doesn’t Intentionally Create

- Temporary Files
- Spooler Files
- Virtual Memory and Swap Files
- Internet Browser and History Files
- Temporary Internet Files
- Link files
- Log files
- Metadata
- Info Files
- Web based emails
Tools of Trade

• Unix/Linux systems
  – SMART Linux (Incident Response tool from ASR Data)
  – ForensiX (Fred Cohen associates)
  – Maresware
  – TCT – The Coroner's Toolkit, a comprehensive package of UNIX forensic tools
  – Lazarus – a file/inode un-deletion parser utility
Challenges

• Analysis of terabytes of data
• Standardization of tools, techniques
• Data from broken disks
• Defining the best practices in cyber forensics
• Increase in anti-forensic trends
• Developments in OS & Applications
Network Forensic Tools

— Web Forensics Tools
  • MyLastSearch
  • Pasco
  • CookiesView
  • CacheView
  • BrowsingHistory

— Wireless Forensics Tools
  • Mobile Devices analysis Tools
Network Forensic Tools

— Email Forensics Tools
  • WhoIS
  • FinaleMAIL
  • Google_Rapid_Response
  • Network_EMailEx

— Some other Network Forensics Tools
  • Malware Forensics Tools
  • Mobile Forensics Tools
  • Router Forensics Tools
System Forensics Tools

– Data_Forensics
  • Acquire Tools
  • Analysis Tools
  • ProDiscover_IR
  • FTKImager

– Database Forensics Tools
  • Analysis Tools
    – Windows_File_Analyzer
    – XnView
    – Ultra Search
    – My Event Viewer
Other system forensics Tools are

- Disk Forensics Tools
- Memory Forensics Tools
Other Forensics Tools

— Proactive Forensics Tools
  • Paraben’s_PL
  • ProDiscover

— Enterprise Forensics Tools
  • CyFIR
  • Encase
  • Windows_Forensics_ToolChest

— Some other Forensics Tools
  • Anti Forensics Tools
Fallacy 1 : Formatted the Drive

• Formatting a drive does not prevent recovery of digital evidence
  – In fact, format typically overwrites less than 1% of drive contents

• Format wipes out directories, so names of files are lost
  – A lot of the data can still be recovered by sifting through data that remains after the format operation
Fallacy 1: Used Web based Email

- Fallacy: use of web-based email rather than storing email messages directly on a computer is safer (in terms of thwarting recovery attempts)
  - It’s not. Even if you never download the email and immediately delete all messages on the server!

- Recently viewed web pages are stored in web browser’s cache which is often in a hard-to-find place...

- Internet Explorer ➔ Tools ➔ Internet Options ➔ Delete Files
  - Clears the cache in Internet Explorer
  - Files stored in browser cache are not securely deleted when the cache is cleared
  - Browser cache mining tools bring recently viewed web pages, including web-based email messages, back to life in a flash
Fallacy 2: Formatted the Drive

- Formatting a drive does not prevent recovery of digital evidence
  - In fact, format typically overwrites less than 1% of drive contents

- Format wipes out directories, so names of files are lost
  - A lot of the data can still be recovered by sifting through data that remains after the format operation
Trolling

• Trolls are anonymous online sadists.
• They attack computer users with threatening mails/phone calls.
• Australian celebrity Charl Otte Dawson committed suicide for being targeted by Trolls.
Problems

• Can Trolls be Actually be Punished?
  – The internet transcends boundaries in a way that most national laws do not.

• When to determine relevant jurisdiction of a particular crime by a criminal the following questions to be considered.
  – The law of the country where the victim resides?
  – The law of the country where the host server is located?
  – The law of the country where the criminal resides?
Ambiguity

• The answers could point to three different jurisdictions, it may be that a victim of a India, troll using a Australian server is located in England.

• Whether or not a troll could find him or herself being extradited will depend on which two countries are involved, the applicable Treaty or Convention governing extradition proceedings between the two countries and the specific facts of the case. In India, if trolls write offensive or having menacing character comments or comments with sexually colored remarks, they can be arrested without warrant and prosecuted.
SPAM-Advance-Fee Fraud

- Lottery or “419” scam
  - “You won 10 million € in this e-mail lottery”
  - “I inherited 65 million $. I need your help – you will get 20%”
  - but you need to advance some money first, “to cover expenses”
  - there was a 2 million victims in 2008
Law to punish Trolls

• Section 66A of IT Act 2000
  – Any information that is grossly offensive or has menacing character; or
  – Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device.
  – Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine. It is cognizable offence but bail able offence.
Case of Zeran v. America Online Inc

- It resulted primarily from trolling.
- Six days after the Oklahoma City bombing, anonymous users posted advertisements for shirts celebrating the bombing on AOL message boards, claiming that the shirts could be obtained by contacting Mr. Kenneth Zeran.
- The posts listed Zeran’s address and home phone number.
- Zeran was subsequently harassed.
Case of Tamiz v Google Inc

- The court held that an internet platform (Google) is a ‘publisher’ of defamatory material if it does not act promptly upon such notification.
Case of Delfi AS v Estonia

- European Court of Human Rights found the website liable for comments posted by anonymous users, despite the website having removed the comments complained of on the same day that the complaints were made.
Case of Daniel Hegglin Vs Google

• It was settled outside the court.
• For over three years the UK businessman has been the victim of a relentless campaign of internet abuse by an unknown troll.
• Nearly 4000 websites contain this slanderous material about him and any Google search for his name will bring them up.
• When he complained to Google they removed some links when alerted to them.
• But in his claim filed to the High Court in UK, Hegglin said the company didn’t do enough to stop the torrent of ‘vile and abusive’ material in its search results.
Cyber Crime
Cognizable Offenses
Work on Email Forensics
Conclusions

• 100% Secure System is a myth.
  – Proactive approach but not reactive

• A new approach to security planning is required to gain senior management support
  – Creation of is audit, network security, incident response, cyber forensic teams, bct, drt.

• Network security continuous process
  – Not a single day solution

• Collaboration between government, industry and academe is required to focus the limited resources.
Questions?
Thank You