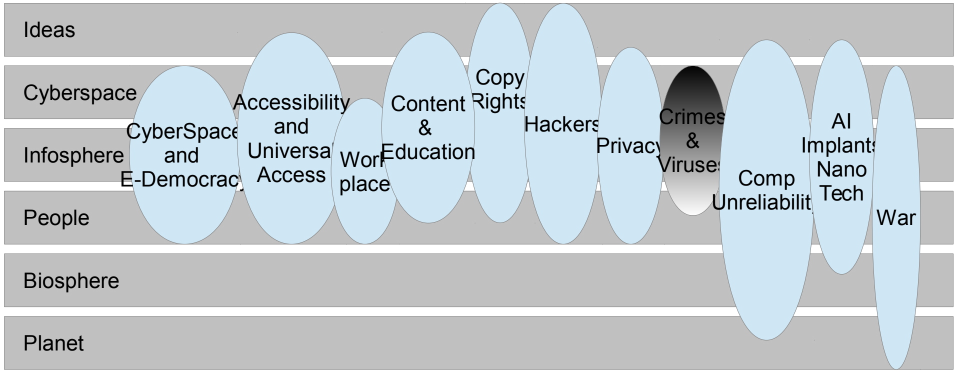
Professional Issues in IT

Omar Usman Khan, PostDoc., PhD.
omar.khan@nu.edu.pk

Assistant Professor
Department of Computer Sciences

National University of Computer & Emerging Sciences
Peshawar, Pakistan



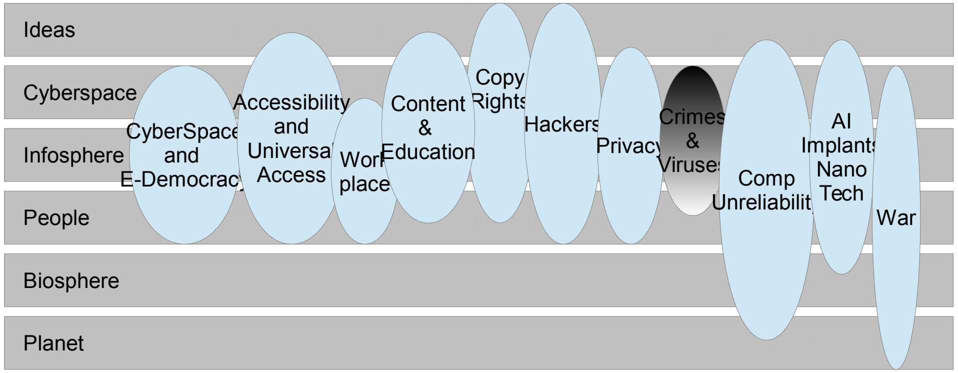
Computer Crime & Security

- Security of ICT's is very important for all stake-holders

Protect **Confidential Data** (Banks, Governments, Your employee details, Your Customer details, Your Operating System)

Means of Protection against Malicious attacks, Theft of Data, Disruption of operations

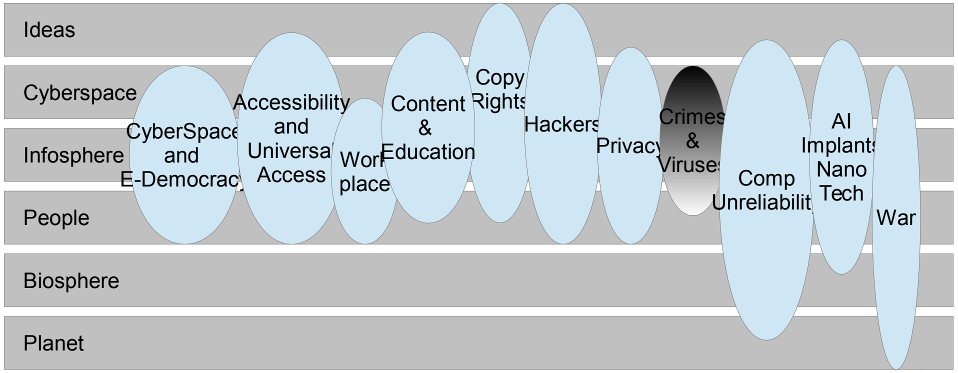
How to **balance between security issues** and **normal business operations**



Computer Crime

- Ethical Issues with this thought?
  - My customer information has been hacked and sold by the hacker to a 3rd party. I have found the hacker. If I prosecute the criminal, the affair will go public. People will find out about the hack and will loose trust in my business.
  - Security is important to my company. Therefore, I have set-aside 10% of my profits in maintaining data security. If my company is facing a financial crisis, should I reduce this percentage?

How to **balance between security issues** and **normal business operations**

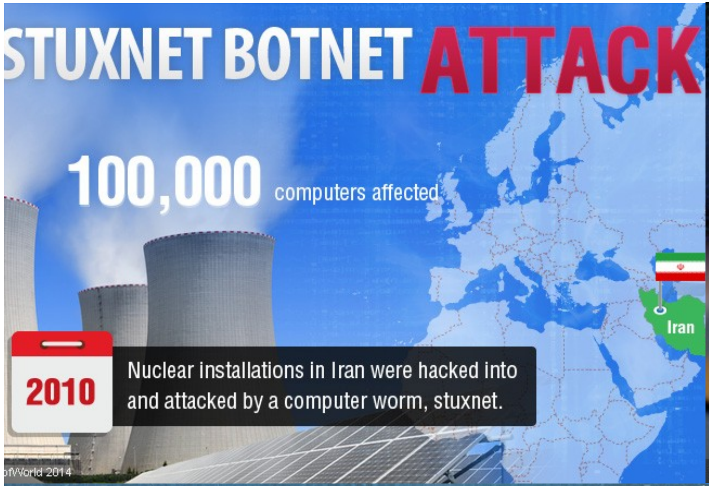


Computer Crime

- Ethical Issues with this thought?
  - To make sure there are no spy-bots visiting my site, I have programmed numerous CAPTCHA's in my code.
    As a result, the spy-bots are kept out.
    On the other hand, my genuine and regular visitors have stopped visiting due to this added security. Should I remove the CAPTCHA ??
  - Many Many other examples …

How to **balance between security issues** and **normal business operations**

Number of IT-related security incidents is **increasing around** the world ..



STUXNET BOTNET ATTACK

100,000 computers affected

2010 Nuclear installations in Iran were hacked into and attacked by a computer worm, stuxnet.

SAUDI ARABIA Hackers Breach 400k ISRAELI Credit Cards

JAN 2012 Bank of Israel later said that about 15,000 cards' information was stolen.

Israel
Saudi Arabia
© MapsofWorld 2014

CREDIT CARDS & CUSTOMER INFO HACKED

TARGET 40 million customer accounts hacked

27 NOV 2013 – 15 DEC 2013

USA
psofWorld 2014

Fake Tweet on 'Obama, Explosions' CAUSES MARKET CRASH

The Associated Press @AP
Breaking: Two Explosions in the White House and Barack Obama is injured
Expand

Loss: $136 million

DOW JONES April 23 2013

AP
psofWorld 2014

SPAMHAUS ATTACK SLOWS GLOBAL INTERNET SPEED

APR 2013

- Largest cyber attack in Europe.
- Anti-spamming organization 'Spamhaus' struck.
- Servers hit by data requests at 300 Gbps.

Europe
© MapsofWorld 2014

NSA'S SECRET DIVISION Hacks Computers Globally

Top secret division of National Security Agency called 'Tailored Access operations' (TAO) alleged to be stealing data by inserting *"invisible back door spying devices into computer systems"*

DEC 2013

USA
Germany
Report by
DER SPIEGEL
© MapsofWorld 2014

2 MILLION ONLINE ACCOUNTS HACKED

NOV 2013

57% of these were Facebook accounts.

Report by
Trustwave
Security begins with Trust
USA
Germany
Singapore
© MapsofWorld 2014

SYRIAN ELECTRONIC ARMY HACKS skype's TWITTER ACCOUNT

JAN 2014 SEA hacked Skype's social media platforms, its Twitter account and official blog.

Syr
ofWorld 2014

Types/Reasons !!

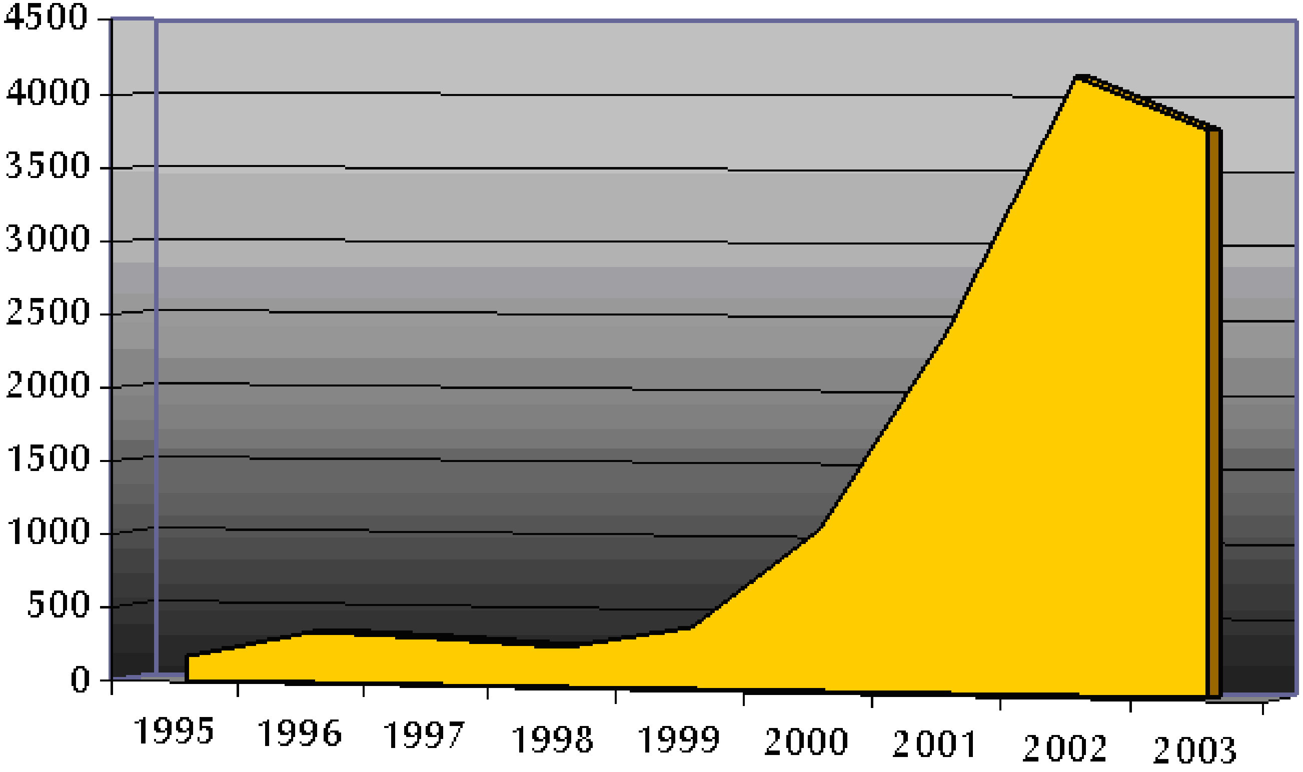
Breaches,
Stealing,
Hyping,
Denial of Service,
Espionage

IMG Credits: Maps of World

Why/How are these happening?

- Bad Quality Software is Being Written (vulnerabilities)
- Sharing of Hardware/Data
- Users do not care (strong passwords, lax rules, etc.)
- Increased reliance on commercial software with known vulnerabilities.

Increased Complexity =
Increased Vulnerability

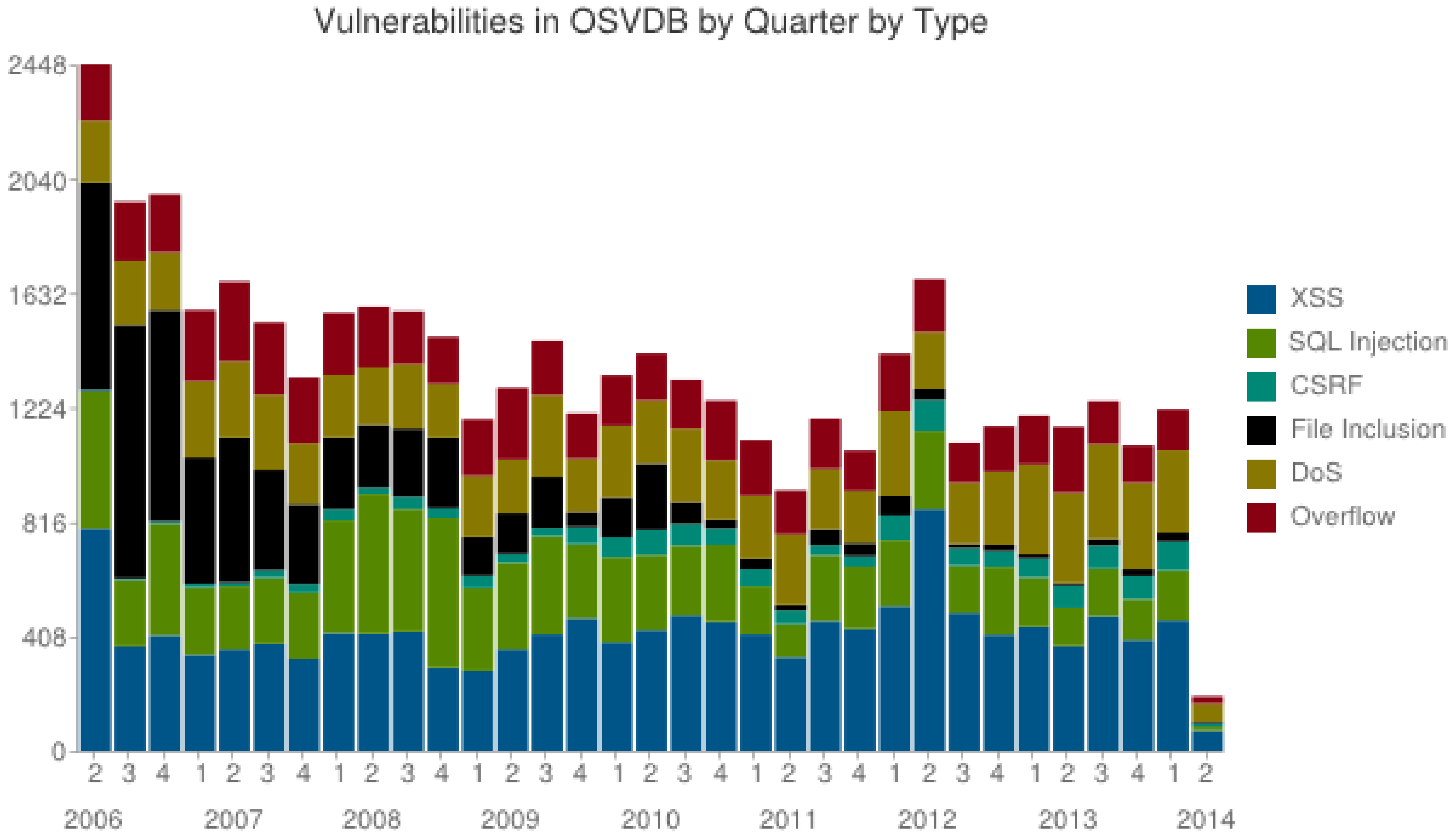


	1995	1996	1997	1998	1999	2000	2001	2002	2003
Vuln's	171	345	311	262	417	1090	2437	4129	3784

Img: Open Source Vulnerability Database (http://osvdb.org)

Why/How are these happening?

- But there is some small decline also … ?? why ??



Img: Open Source Vulnerability Database (http://osvdb.org)

National Security Council Bill, 2014

- Some points from the bill:
  - Access **an information system without authorization** and face 6 months in jail and/or Rs 100,000 fine. Change data on the information system and get 9 months jail and/or Rs 200,000 fine.
  - If **electronic fraud** is found and proved then guilty can face an imprisonment of up to five years or a fine of up to Rs. 10 million or both.
  - If someone is found guilty of posing **another person's identity** then he/she may face imprisonment of three months of a fine of Rs. 50,000 or both
  - Unauthorized interception of private data **(for example hacking emails)** can result into imprisonment of two years or a fine up to Rs. 500,000 or both
  - **Special protection for women:** If someone is found publicly spreading any content (video/pictures/audio) that may harm the reputation of women then he/she may face imprisonment for one year or a fine up to Rs. 1 million or both

Drafting policy guidelines: Cyber security bill presented in Senate

By Our Correspondent Published: April 15, 2014

THE EXPRESS TRIBUNE

PAKISTAN LATEST STORIES

Emergency room: Magazine awards doctors for saving lives

Hifza Jillani | 8 minutes ago

Some Terminologies

- Exploit != Vulnerability
  - Exploit = Attack that takes advantage of a particular system vulnerability
- Zero-day attack
  - Takes place before a vulnerability is discovered or fixed
- Patch
  - A "Fix" to eliminate a problem
  - Problem: Users responsible to install patches

Types of Attacks

Viruses	Worm	Trojan Horse	Denial of Service	...

- A program that disguises itself as something else and which causes undesirable events.
- Usually attached to a file/folder. When infected file is opened, virus delivers payload .. includes following:
  - Transmitting strategy
    - Not automatically transmitted. Human negligence big source of transmission
    - Re-transmitted in forms of infected emails, document attachments, infected USB's.
  - Damaging strategy:
    - Damage files/folders and other programs
    - Other programs may be Targeted User Software, Operating Systems, Boot Loader, or BIOS.

Types of Attacks

Viruses | Worm | Trojan Horse | Denial of Service | ...

- A text file is a file that cannot be executed. A virus is a computer program and it can be executed. How can a virus be "bound" to a text file, or even folder for that matter?
  - Macro-Virus: Many files support macro-languages, e.g. VBScript, JavaScript.
- Resident Viruses: Resident in memory. Serves as an OS service. Overwrites interrupt-handling + signal handling functions of OS. Present from Computer start to shutdown.
- Non-Resident Viruses: Scans disk for files and corrupts all of them. When done, exits from memory.
- Boot Sector Virus: Targets the BIOS and/or MBR/GPT

Types of Attacks

Viruses	Worm	Trojan Horse	Denial of Service	...

- Counter-Measures
  - Anti-Virus software
    - Search for virus signatures in files that they are known to infect.
    - Heuristic based scanning: Identify behavior of programs. Leads to false positives. E.g., a software supporting online ads may be flagged as a virus/un-trusty software.
  - Patch current software (Security Updates)
- Removal Methods
  - System Restore (some resident viruses disable this + task manager + command prompt to avoid removal)
  - Anti-Virus Scan and Quarantine
  - Re-install the operating system (be careful !! If not formatted, the virus is still on the file-system)

Types of Attacks

Viruses

Worm

Trojan Horse

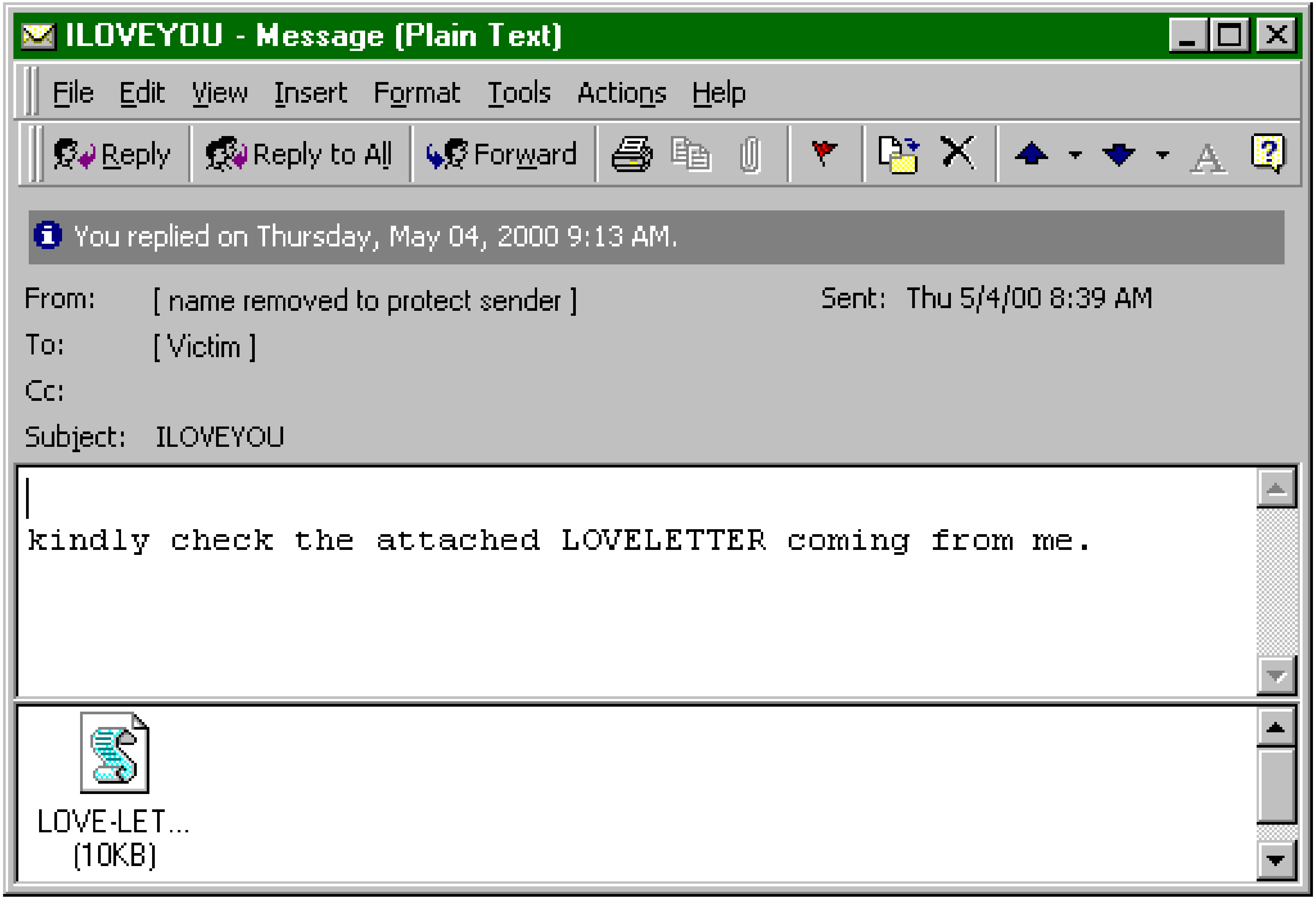
Denial of Service

...

- Same as viruses but with the possibility to transmit without human intervention.
- ILOVEYOU
  – 2000: Sent to all contacts on address book (as attachment LOVE-LETTER-FOR-YOU.TXT.vbs)
  – Patch written in 2 days. Within this time, infected 10 million computers. Repair cost estimated at 8.75 Billion $
  – Virus written by a student in Philippines after his project was rejected by his teacher.

Types of Attacks

Viruses | Worm | Trojan Horse | Denial of Service | ...


ILOVEYOU - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

You replied on Thursday, May 04, 2000 9:13 AM.

From: [name removed to protect sender]
Sent: Thu 5/4/00 8:39 AM
To: [Victim]
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

LOVE-LET...
(10KB)

Types of Attacks

Viruses

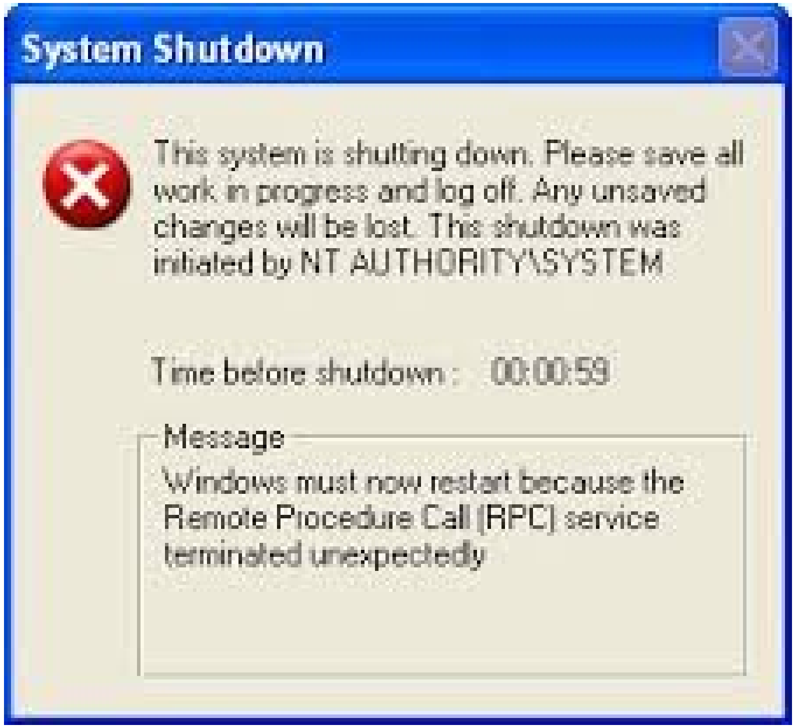
Worm

Trojan Horse

Denial of Service

...

- 1999: Melissa
  20% of computers world-wide affected through email retransmission
- 2000: Blaster
  “Billy Gates, why do you make this possible? Stop making money, and fix your software!”. Exploited RPC.
- 2004: SASSER
  Exploited RPC in Windows 2000/XP
- 2004: W32.MyDoom@mm
  10% reduction in global internet access. Transmission through email attachments.



System Shutdown

This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM

Time before shutdown : 00:00:59

Message

Windows must now restart because the Remote Procedure Call (RPC) service terminated unexpectedly

Types of Attacks

Viruses	Worm	Trojan Horse	Denial of Service	...

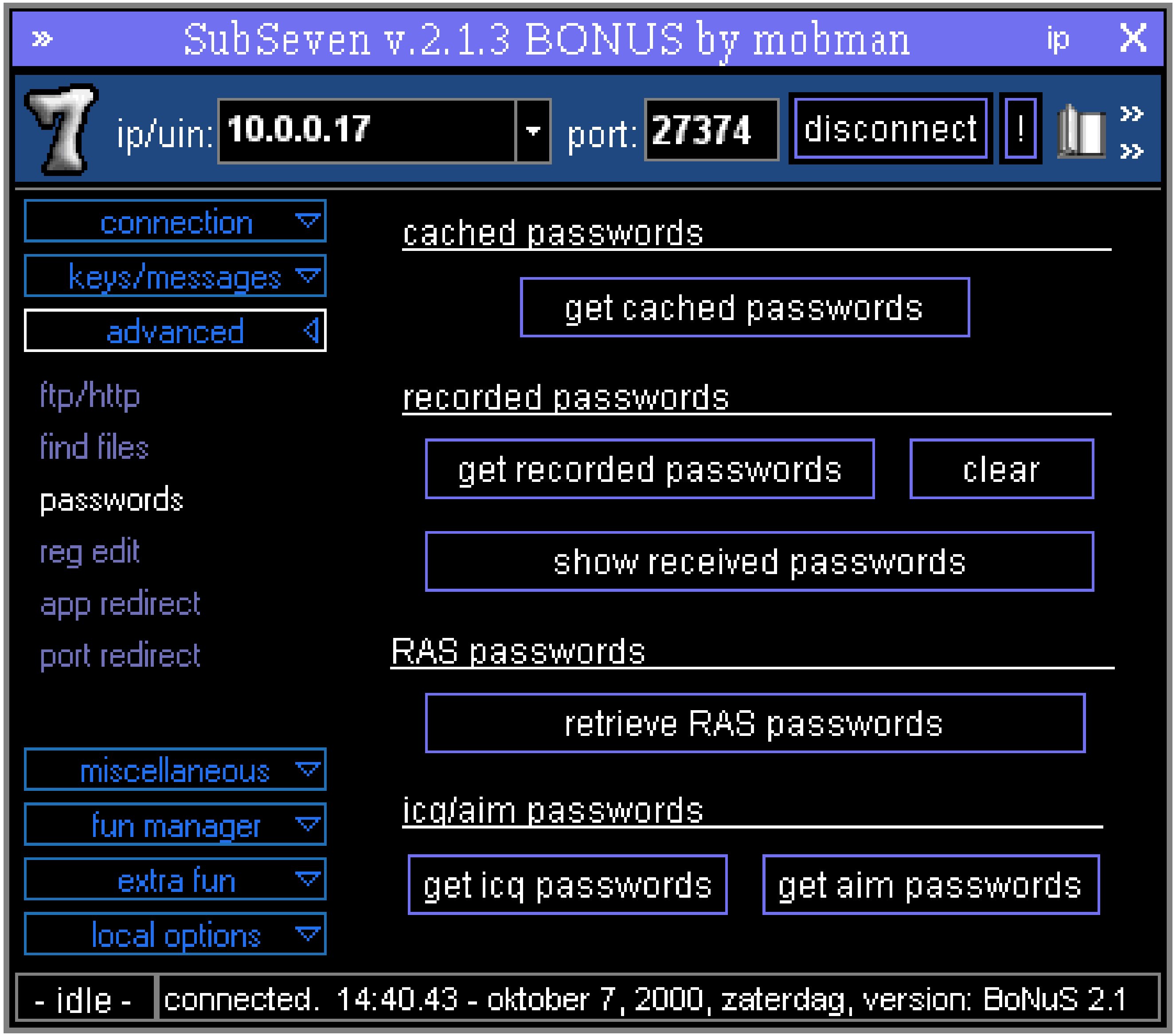
- Gets secretly installed on a computer, planting a minimum payload.
- Steal passwords, listen for key-strokes and transmitting to 3rd party.
- Transmission methods can be through email (worm-like behavior), or installed by physically/remotely breaching system.
- Different from **Logic Bomb**. Logic Bomb triggered when specific condition occurs. E.g., a specific time/date.

Types of Attacks

Viruses	Worm	Trojan Horse	Denial of Service	...

Sub7

Owner claimed his software
is simply a remote administration tool with added support
e.g., recover lost passwords, etc.



SubSeven v.2.1.3 BONUS by mobman

ip/uin: 10.0.0.17

port: 27374

- idle -

connected. 14:40.43 - oktober 7, 2000, zaterdag, version: BoNuS 2.1

Types of Attacks

Viruses | Worm | Trojan Horse | Denial of Service | ...

Back Orifice http://sourceforge.net/projects/boxp/

Remote administration tool … also controversial

Sir Dystic
Cult of Dead Cow
Regular speaker at DefCON Conferences

DefCON Documentary !!!!!

Types of Attacks

Viruses | Worm | Trojan Horse | Denial of Service | ...

- ... Distributed Denial of Service
- Break-in to source computers (thousands of them), ideally through worm. Flood a target site with data packets from compromised computers. Idea is not to breach the target, but keep it busy so legitimate traffic can not go through.
- Avoid self-denial attack by **spoofing** return addresses on packets sent out.

Types of Attacks

Viruses	Worm	Trojan Horse	Denial of Service	...

- ISP's can identify false IP addresses. Incoming false addresses are processed through ingress filtering, while outgoing false addresses are processed to egress filtering.
- Filtering is expensive (w.r.t processing time)
- Solution: Invest in more powerful router with built-in filtering.

Cost of Attacks

Viruses

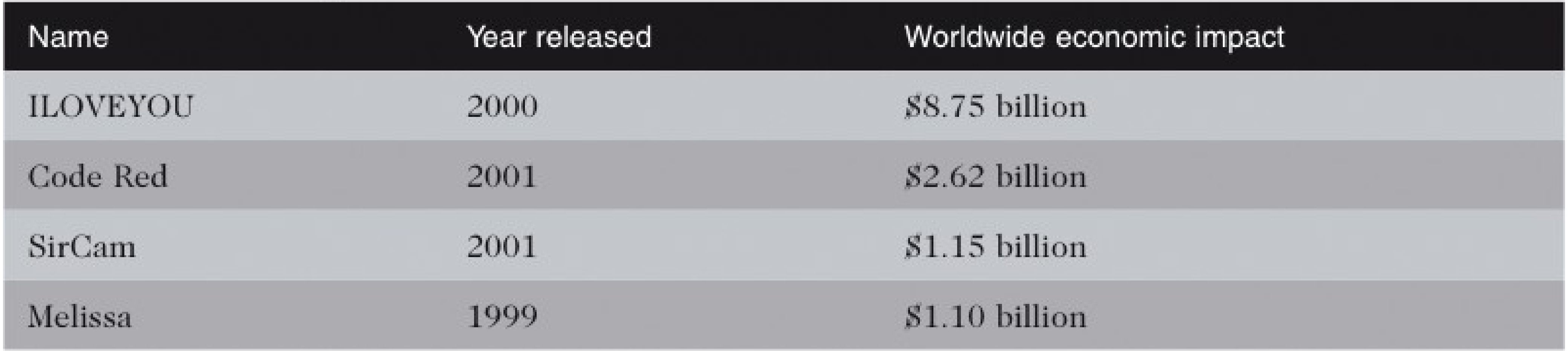
Worm

Trojan Horse

Denial of Service

...

- Lost Data and Software
- Lost productivity
  - (employees can't work on damaged systems)
  - (employees work on fixing their computers instead of doing company work)



Name	Year released	Worldwide economic impact
ILOVEYOU	2000	\$8.75 billion
Code Red	2001	\$2.62 billion
SirCam	2001	\$1.15 billion
Melissa	1999	\$1.10 billion

Who are the Perpetrators ?

Hacker	Cracker	Insider	Industrial Spy	Cyber-Criminal	Cyber-Terrorist

- Test Limits of Computer System out of "intellectual curiosity" ... to see how far they can go.
- Desire to learn more about the system internals.
- Common profile is a male, 20-25, avid gamers, plenty of spare time, little/no money
- Lamers/Script Kiddies ⟵ Hackers whose knowledge only limited to available tools
- Prefer to be part of community instead of working alone. Get a lot of information from chat-groups (mIRC). Have a Pseudonym.

Who are the Perpetrators ?

Hacker Cracker Insider Industrial Spy Cyber-Criminal Cyber-Terrorist

- Hackers argue that they break-in to check the vulnerabilities of a computer/computer network.
- Crackers engage in clear criminal activity.
  - Deface websites, crash computers, spread harmful programs, spread offensive messages, forge program software installation keys, and write scripts/programs that allow other crackers to do the same type of activities.

Who are the Perpetrators ?

Hacker | Cracker | Insider | Industrial Spy | Cyber-Criminal | Cyber-Terrorist

- The biggest threat to companies. More than 70% of network intruders are found to be company insiders.
- Who is an insider: Employee, contractor, consultant.
- Not necessary to be hired as an IT professional. Numerous Non-IT Professionals are equally good at hacking/cracking.
- Difficult to catch. So companies introduce access control levels. Each employee only allowed, designed to access information that is relevant to his level.
- Collusion: Cooperation between an insider and outsider

Who are the Perpetrators ?

Hacker | Cracker | Insider | Industrial Spy | Cyber-Criminal | Cyber-Terrorist

- Professionally hired to get inside secrets (e.g., trade secret or new product information) of an organization or spy on another government

NSA'S SECRET DIVISION
Hacks Computers Globally
USA
Germany
Report by
DER SPIEGEL
DEC
2013

Top secret division of National Security Agency called 'Tailored Access operations' (TAO) alleged to be stealing data by inserting "invisible back door spying devices into computer systems"

© MapsofWorld 2014

IMG: Maps of the World

Who are the Perpetrators ?

Hacker | Cracker | Insider | Industrial Spy | Cyber-Criminal | Cyber-Terrorist

- Hack into computer networks to steal money related assets.
  - Steal credit card numbers (for fraud)
  - Steal personal identity (for fraud)
  - Steal cell-phone information (for fraud)
- Checks & measures
  - Keep strong passwords and change them often.
  - Credit Cards: Website encryption, Match card-holder name, card expiry, CCV code, address of card, added password check, added finger-print verification.

Who are the Perpetrators ?

Hacker

Cracker

Insider

Industrial Spy

Cyber-Criminal

Cyber-Terrorist

- Intimidates governments/organizations to advance political/social objectives. For this purpose, attempt to
  - Breach computer systems and steal sensitive information
  - Perform Denial of Service Attacks
- Engage in propaganda through online forums, social groups, video sharing sites.
- Interact/pass messages discretely to other cyber-terrorists.
  - Encrypted Messages
  - Code words/symbols
  - Correspond through Email without sending Emails

Perpetrator Summary

Type	Objective	Resources Available	Level of Risk acceptable to perpetrator	Frequency of Attack
Hacker	Test limits of system Gain Publicity	Limited	Minimal	High
Cracker	Cause problems Steal data Corrupt systems	Limited	Moderate	Medium
Insider	Make money Disrupt company information sys	Knowledge of systems & passwords	Moderate	Low
Industrial Spy	Capture trade secretes Gain advantage	Well funded Well trained	Minimal	Low
Cyber-Criminal	Make money	Well funded Well trained	Moderate	Low
Cyber-Terrorist	Destroy key infrastructures	Not necessarily funded or trained	Very high	Low

What can be done to prevent this ?

- Should USB's be allowed in the office?
- Should IM/P2P/Social networking sites be allowed in the office?
- Encryption methods and their enforcement
- VPN Systems
- Educate employees about good measures (for e.g., how to choose a good password)
- Installation of firewalls, anti-virus software
- Defining role of employees (e.g., access levels)
- Keep track of well known vulnerabilities (install patches)
- Regular system backups
- … many many more examples