The Information Society

How Safe Is It?

Alexander NTOKO
Chief, E-Strategies Unit
ITU Telecommunication Development Bureau (BDT)
Information and Network Security was identified as one of the key challenges in ITU-D Survey.

Results of recent ITU/BDT Survey on Key Challenges for e-transactions – ITU-D Study Group 2 Question 17

Bar chart showing the percentage of replies for different categories:
- Information and network security: 38
- Infrastructure: 35
- Banking system: 22
- Others: 22

©1998-2005 ITU Telecommunication Development Bureau (BDT) – E-Strategy Unit..
Security Threats

• The Information Society is not safe.
• There’s a wide range of threats aimed at destroying critical infrastructure and data, stealing identity, intercepting communications and destroying trust and confidence in the use of Internet for critical transactions.
MALWARE
Some of the threats: Viruses

What is a virus?

- **Virus (n.)** Code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or information.

- Just as human viruses range in severity from Ebola to the 24-hour flu, computer viruses range from the mildly annoying to the downright destructive. The good news is that a true virus does not spread without human action to move it along, such as sharing a file or sending an e-mail.
Some of the threats: **Viruses**

**Are Viruses new? The Brain Virus.**

- The first computer virus for Microsoft DOS was apparently written in 1986 and contains unencrypted text with the name, address, and telephone number of Brain Computer Services, a store in Lahore, Pakistan. This virus infected the boot sector of 5¼ inch floppy diskettes with a 360 kbyte capacity. Robert Slade, an expert on computer viruses, believes the Brain virus was written as a form of advertising for the store in Pakistan.

A variant of the Brain virus was discovered at the University of Delaware in the USA during Oct 1987 where the virus destroyed the ability to read the draft of at least one graduate student's thesis.
What is a worm?

- Worm (n.) A subclass of virus. A worm generally spreads without user action and distributes complete copies (possibly modified) of itself across networks. A worm can consume memory or network bandwidth, thus causing a computer to stop responding.

- Because worms don't need to travel via a "host" program or file, they can also tunnel into your system and allow somebody else to take control of your computer remotely. Recent examples of worms included the Sasser worm and the Blaster worm.
Some of the threats: Trojan

What is a Trojan?

- Remember the Trojan horse appeared to be a gift, but turned out to contain Greek soldiers who overtook the city of Troy.

- Trojan (n): A computer programs that appear to be useful software, but instead compromises your security and cause a lot of damage.

- A recent Trojan came in the form of an e-mail message that included attachments claiming to be Microsoft security updates, but turned out to be viruses that attempted to disable antivirus and firewall software.
Are Viruses new? The Brain Virus.

- The first computer virus for Microsoft DOS was apparently written in 1986 and contains unencrypted text with the name, address, and telephone number of Brain Computer Services, a store in Lahore, Pakistan. This virus infected the boot sector of 5¼ inch floppy diskettes with a 360 kbyte capacity. Robert Slade, an expert on computer viruses, believes the Brain virus was written as a form of advertising for the store in Pakistan.

A variant of the Brain virus was discovered at the University of Delaware in the USA during Oct 1987 where the virus destroyed the ability to read the draft of at least one graduate student's thesis.
By Executing the Code.

- Virtually all viruses and many worms cannot spread unless you open or run an infected program.
- Many of the most dangerous viruses were primarily spread through e-mail attachments—the files that are sent along with an e-mail message.
- The virus is launched when you open the file attachment (usually by double-clicking the attachment icon).
Just how costly are some of the known viruses?

The estimated costs in the following table are from Computer Economics in January 2002.

<table>
<thead>
<tr>
<th>Name of Virus program</th>
<th>Estimated US$ cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Melissa</td>
<td>$1.10 \times 10^9</td>
</tr>
<tr>
<td>ILOVEYOU</td>
<td>$8.75 \times 10^9</td>
</tr>
<tr>
<td>CodeRed</td>
<td>$2.62 \times 10^9</td>
</tr>
<tr>
<td>SirCam</td>
<td>$1.15 \times 10^9</td>
</tr>
<tr>
<td>Nimda</td>
<td>$0.635 \times 10^9</td>
</tr>
</tbody>
</table>
Just how fast can these viruses spread?

Geometric Series: $A + AR + AR^2 + AR^3 \ldots AR^{n-1}$

1. In the hypothetical scenario below, each victim’s computer provides email addresses of four (4) new victims.

2. Assume that it takes one hour for the warm to be received by the next four victims. In 24 hours, it could theoretically would have reached $10^{14}$ victims. *More than the population of the earth!*

<table>
<thead>
<tr>
<th>time in hours</th>
<th>number of new victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>64</td>
</tr>
<tr>
<td>4</td>
<td>256</td>
</tr>
<tr>
<td>5</td>
<td>1024</td>
</tr>
<tr>
<td>6</td>
<td>4096</td>
</tr>
<tr>
<td>7</td>
<td>16384</td>
</tr>
<tr>
<td>8</td>
<td>65536</td>
</tr>
<tr>
<td>9</td>
<td>262144</td>
</tr>
<tr>
<td>10</td>
<td>1048576</td>
</tr>
</tbody>
</table>
SPAM
What is SPAM?

- Unsolicited e-mail.
- Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.
- To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. Noun: electronic "junk mail".
The battle for combating spam is an ongoing one with an increasingly sophisticated level of finding ways to send unsolicited messages to recipients worldwide. Some of the common spammer tactics include:

- Dictionary attacks
- Email and DNS Spoofing
- Social Engineering and Urban legends/Hoaxes
- Message Board and Chat Room Mining
- Open Proxies and Mail Relaying
- Chain Letters
- *Always-On* Broadband connections
One of the core problems with spam is we don't know, Yahoo doesn't know, the user doesn't know ... if it really came from the party who it says it came from," Brad Garlinghouse, vice president for communication products at Yahoo, said. "What we're proposing here is to re-engineer the way the Internet works with regard to the authentication of e-mail."
Spam does not only cause loss of revenue and time for email recipients and companies but also reduces trust and confidence in email transactions.
SPAM – Constantly Evolving

Spam is not only growing, but is evolving to become broader threat to Internet security.
Some Cyber Security Threats…

1. **Identity Interception**: The observation of identities of communicating parties for misuse.
2. **Data Interception**: The observation of user data during a communication by an unauthorized user.
3. **Manipulation**: The interception and modification of information in a private communication.
4. **Masquerade**: Pretending to be another user to access information or to acquire additional privileges.
5. **Replay**: The recording and subsequent replay of a communication at some later date.
6. **Repudiation**: The denial by a user of having participated in part or all of a communication.
7. **Denial of Service**: The prevention or interruption of a communication or the delay of time-critical operations.
8. **Traffic Analysis**: The unauthorized analysis and observation of information (e.g. frequency, sequence, type, amount, etc.).
Significant incidents recently reported to HackerWatch.org

24 Hours: 78,541,667
7 Days: 547,791,660
30 Days: 2,356,379,550

Note: Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, as of 2004, we will no longer publish the number of incidents reported. Instead, we will be working with others in the community to develop and report on more meaningful metrics, such as the 2004 E-Crime Watch Survey. Source - CERT/CC
Thank You for your attention

For further information
Web:  http://www.itu.int/ITU-D/e-strategy
Email: e-strategy@itu.int