UN-ESCWA

Practical Application of Cyber Crime Issues

Nibal Idlebi and Matthew Perkins

United Nations Economic and Social Commission of Western Asia (UN-ESCWA)

Information and Communication Technology Division

Practical Applications

- This presentation highlights the techniques and tools used in three realms of cyber crime:
  - Commission
  - Detection
  - Prevention

Background

Understand the Fundamentals

- In order to draft effective legislation, it is necessary to understand the technological background of cyber crime.

Legal Principles

- There can be no crime without a law for it.
- In order for an action to be illegal, there must be a specific law forbidding it.
- Most laws applied to cyber crime are based on efforts to make old law modern. This does not tend to work very well.

How to Commit Cyber Crime

- Cyber crime is a broad and complex field, with many different facets. This presentation highlights ways criminals use to break security systems, such as:

Compromising passwords

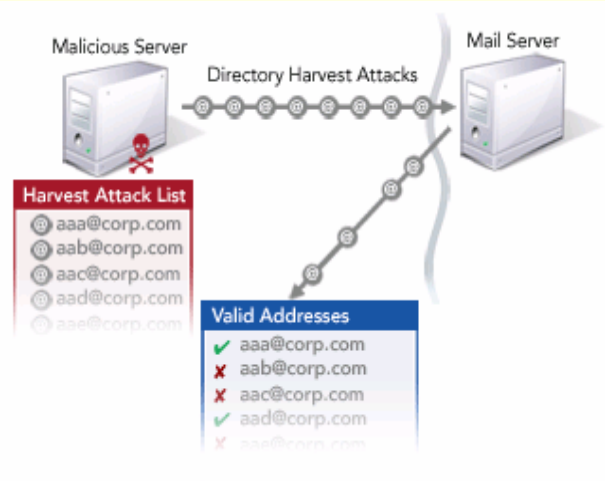
How to Commit Cyber Crime

- Most people choose passwords that are relatively easy for a computer to guess using a technique called "**Brute force**".

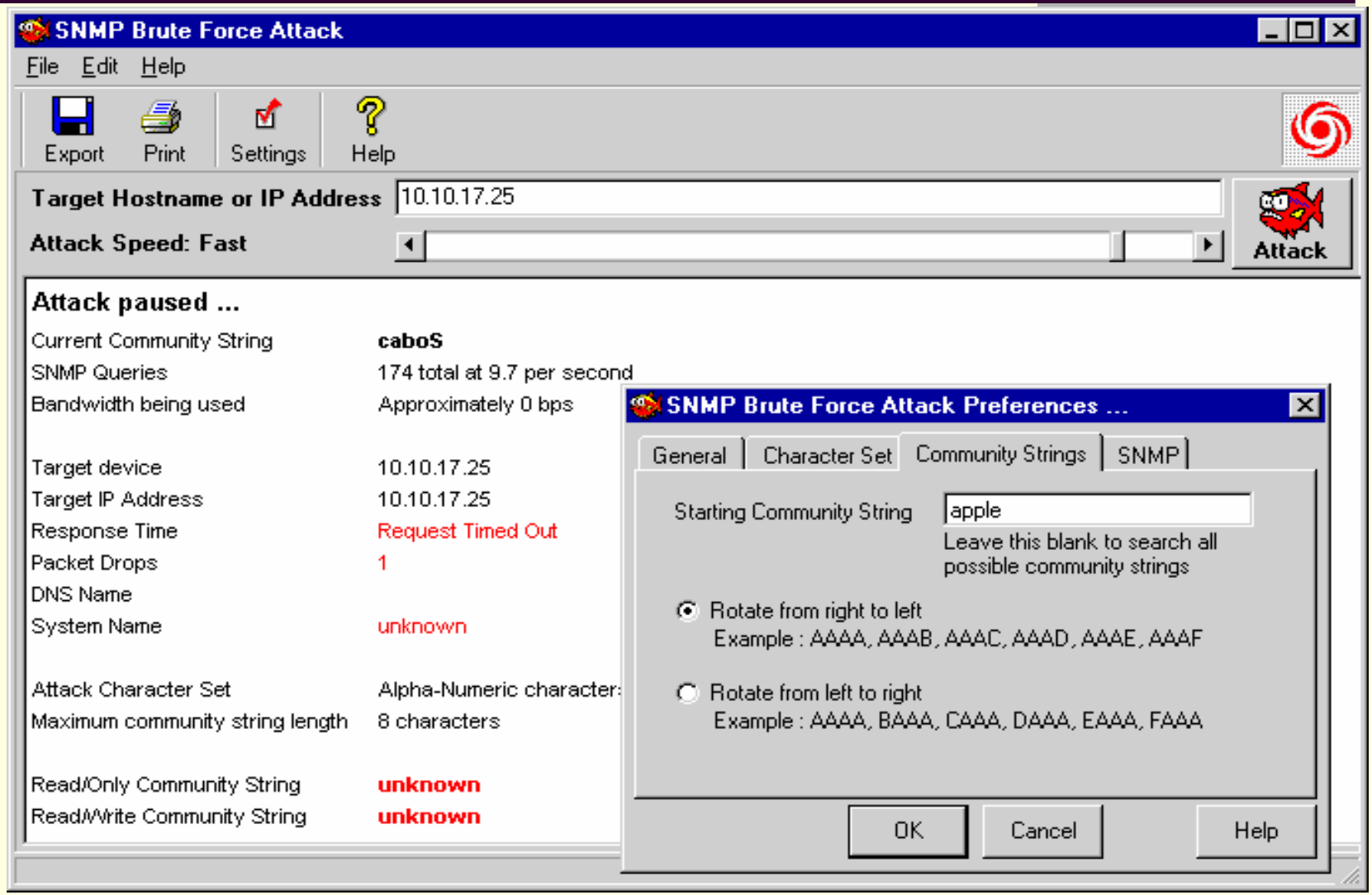
- In a brute force attack, the computer attempts to determine the password by using a large number of possibilities.

How to Commit Cyber Crime

- **Brute force** attack is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys in order to decrypt a message.



How to Commit Cyber Crime Solar Winds



How to Commit Cyber Crime

- Advantages:
  - Can be extremely effective at obtaining unsecure passwords.
- Disadvantages:
  - Can take an extensive amount of time.
  - Easily detectable for properly configured systems.

How to Commit Cyber Crime

- Other applications:

  Nessus vulernability scaner

  - Designed to automate the testing and discovery of known security problems before a hacker takes advantage of them.
  - Reveals problems in a network, and can be used by both administrators and hackers
  - Could be used by a hacker group, a security company, or a researcher to violate the security of a software product.

How to Commit Cyber Crime

- **Nessus vulernability scaner**
  - Lots of capabilities.
  - Fairly complex
  - Detection of remote flaws
  - Scalable

How to Commit Cyber Crime

- Other applications:

  Cain & Abel

  - is a password recovery tool for Microsoft Operating Systems.

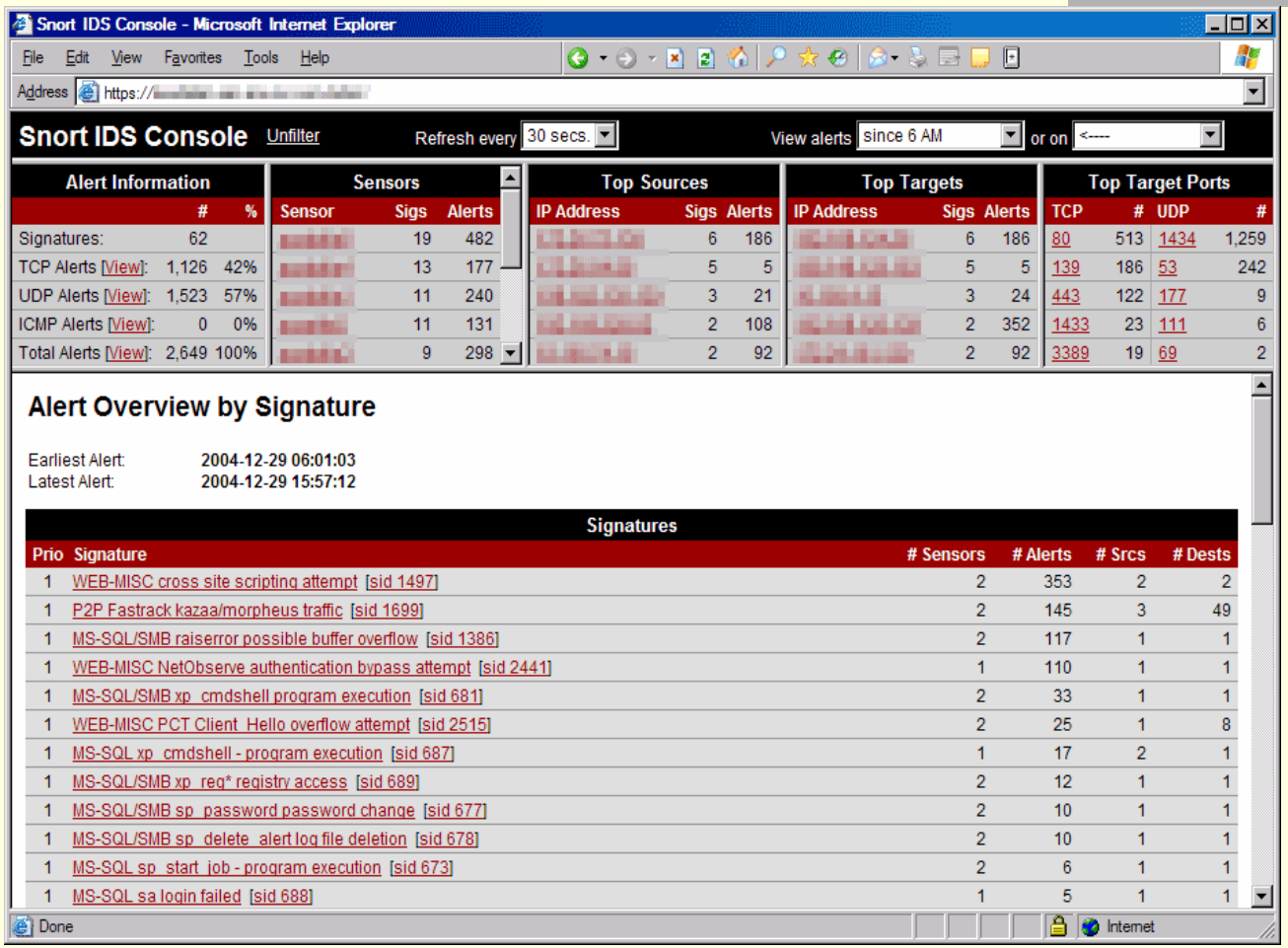
How to Detect Cyber Crime

- Use of Intrusion Detection System (IDS)
- Anti Virus does not detect such crimes
- One of the most known system is **Snort**:
  - Robust open source tool which exist for monitoring network attacks.
  - Its development started in 1998, and through years, it has evolved into a mature software (de facto standard) and even better than many commercial IDS.

How to Detect Cyber Crime

- It monitors network traffic to detect unusual behavior based on rules established by the administrator:
  - Unauthorized applications
  - Viruses
  - Intrusions
  - Brute force attacks
- There is a large Snort community interacting through Snort web site.

How to Detect Cyber Crime



UN-ESCWA

How to Detect Cyber Crime

Alert Overview by Signature

Earliest Alert: 2004-12-29 06:01:03
Latest Alert: 2004-12-29 15:57:12

Prio	Signature
1	WEB-MISC cross site scripting attempt [sid 1497]
1	P2P Fastrack kazaa/morpheus traffic [sid 1699]
1	MS-SQL/SMB raiserror possible buffer overflow [sid 1386]
1	WEB-MISC NetObserve authentication bypass attempt [sid 2441]
1	MS-SQL/SMB xp_cmdshell program execution [sid 681]
1	WEB-MISC PCT Client Hello overflow attempt [sid 2515]

How to Detect Cyber Crime

- Advantages
  - Allows monitoring of network traffic
  - Flexible rules set by administrator
  - Open source
- Disadvantages
  - Can create extensive logs
  - Effectiveness depends on configuration

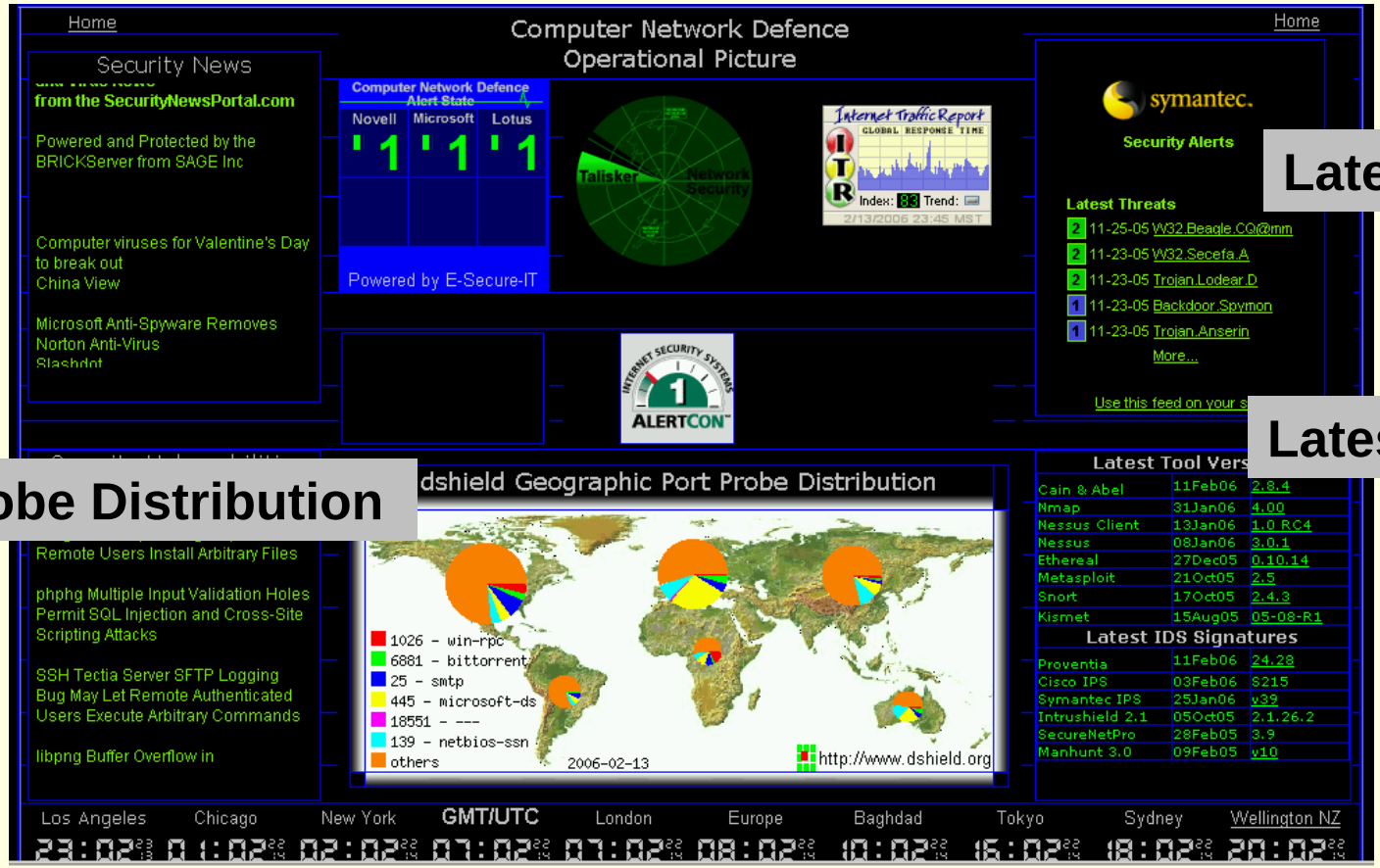
How to Prevent Cyber Crime

Vitally important to have current information on emerging issues.

How to Monitor Cyber Crime

www.dshield.com

How to Monitor Cyber Crime



Latest Threats

Latest Tools

Port Probe Distribution

http://securitywizardry.com/radar.htm

UN-ESCWA

How to Monitor Cyber Crime

- **Advantages:**
  - Provides information on threats, tools and responses.
- **Disadvantages:**
  - Information very technical
  - Little Response time

How to Prevent Cyber Crime

- Detailed acceptable use policies for the organization
- Firewall strategy
- Threat specific protection
- Use of Spyware Prevention Programs
- Some of Intrusion Detection System (IDS) are also preventing cyber crime

How to Prevent Cyber Crime

- Basic features:
  - Detect and protects system and network from external attacks: Spywares, Adwares and other Malwares.
  - Provide real-time protection
  - Consume PC power and network bandwidth
  - Complements existing antivirus and firewall installation.
  - Example : eTrust Pest Patrol

How to Prevent Cyber Crime

- **eTrust Pest Patrol features:**
  - Scan files and directories
  - Cleaning Spyware
  - Removes cookies
  - Report all activities to a central log
- **Characteristics:**
  - Centralized management with transparent deployment and operation
  - Efficient resource usage
  - Customized protection for different levels of vulnerability

Conclusion

- Many technological tools are dual use, can serve both commission and prevention of cyber crime.

- Example:

Encryption

Conclusion

- Encryption
  - Provides privacy and freedom of speech
  - Can also facilitate criminal activity.

Conclusion

- Comprehensive approach would have several layers:
  - Adoption of strong legislation against cybercrime
  - Development of technical measures
  - The establishment of industry partnership
  - Education of consumer and industry players about anti-crime measures
  - International cooperation to allow global coordination approach to the problem

Conclusion

- Cyber legislation must be responsive and adapt to emerging technological developments.