Computer Forensics

RCMP
ROYAL CANADIAN MOUNTED POLICE

Cpl. Jacques Boucher

Royal Canadian Mounted Police

Atlantic Region Integrated Technological Crime Unit

RCMP
ROYAL CANADIAN MOUNTED POLICE

Objective

Provide you with an introduction to computer forensics and incident handling. This includes proper handling of computer evidence, disaster recovery, and when to involve police.

RCMP
ROYAL CANADIAN MOUNTED POLICE

Table Of Content

RCMP
ROYAL CANADIAN MOUNTED POLICE

Mandate of ARITCU

Assist officers in the field with investigations where a computer is involved

Computer Forensics

Investigate pure computer crimes

RCMP
ROYAL CANADIAN MOUNTED POLICE

Computer Forensics

RCMP
ROYAL CANADIAN MOUNTED POLICE

What Is Computer Forensics?

Computer forensics is the identification, extraction, preservation, and interpretation of computer evidence.

The proper application of computer forensic ensures data integrity.

RCMP ROYAL CANADIAN MOUNTED POLICE

Reduce/Eliminate Contamination

The collection of the computer evidence must be done in such a manner that you can demonstrate that the original data was not altered in the process. To achieve this you must acquire the data (hard drive, floppy, USB flash, etc.) in read-only mode.

RCMP
ROYAL CANADIAN MOUNTED POLICE

Reduce/Eliminate Contamination

If it's off, leave it off

If it's on,

- Photograph the screen
- Note applications running
- If it's printing, let it finish printing
- Save any open files
- Proper shutdown

RCMP
ROYAL CANADIAN MOUNTED POLICE

Just Looking Around…

I'm just looking around. What harm am I doing?

The act of turning on a computer accesses well over 1,000 files in a Windows 2000 Professional environment. This number increases depending on what services are loaded at bootup. This action also overwrites parts of the swap file, and unallocated space. Valuable evidence can be lost as a result of this act.

Real world example…

RCMP
ROYAL CANADIAN MOUNTED POLICE

Just Looking Around (cont…)

So what gets contaminated?

RECENT folder

Registry Entries

Date & time stamps

System logs

Application logs

And no doubt other things…

RCMP ROYAL CANADIAN MOUNTED POLICE

Less Is Better

Your chances of being successful decreases according to the amount of activity on that computer or storage media after the point in time that the incident took place (either accidental deletion, re-partitioning, or something of criminal or civil interest).

Secure the computer/storage media at the earliest possible opportunity. This reduces possible contamination and increases the chances of a successful analysis.

RCMP
ROYAL CANADIAN MOUNTED POLICE

Places To Go

RCMP
ROYAL CANADIAN MOUNTED POLICE

Where To Look

User-Created Files

User-Protected Files

Computer-Created Files

Other Data Areas

RCMP
ROYAL CANADIAN MOUNTED POLICE

User-Created Files

Documents or text files

Address books

Image, audio or video files

Calendars

Database and spreadsheet files

E-mail files

Internet bookmarks/favourites.

RCMP
ROYAL CANADIAN MOUNTED POLICE

User-Protected Files

Compressed files

Encrypted files

Hidden files

Misnamed files

Password-protected files

Steganography

Computer-Created Files

Temporary files

System files

Printer spool files

History files

Cookies

Swap files

Log files

RCMP
ROYAL CANADIAN MOUNTED POLICE

Other Data Areas

Deleted files

Computer date, time and password

Free space

Bad clusters

Hidden partitions

Lost clusters

Metadata

Other Data Areas

Other partitions.

Slack space.

Software registration information.

System areas.

Unallocated space.

RCMP ROYAL CANADIAN MOUNTED POLICE

Date, Time & Time Zone

The time zone of the computer that generated the computer evidence (whether it's an entire hard drive, a floppy, or an individual file), as well as the current date & time set on that computer is critical in a number of situations. The file system (i.e. NTFS, fat32, ext2fs) is also important as it impacts how the date/time meta information in relation to each file is stored.

The time zone information can be forensically retrieved from the system registry files.

System time of the system that created the data can be forensically retrieved by doing a controlled boot of the computer in question and going into the BIOS to compare the date/time settings with the actual date/time settings (use atomic clock to compare).

RCMP
ROYAL CANADIAN MOUNTED POLICE

Forensic Tools & Suppliers

Access Data (Password Recovery & FTK – Forensic Tool kit)

Coroner's Took Kit – Linux tool

DBX & MBX – freeware to extract .eml files

QuickViewPlus

Foundstone tools

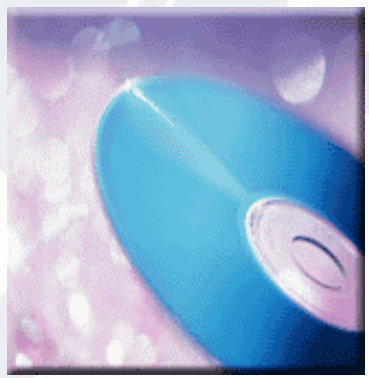
iLook (exclusive to law enforcement)

EnCase

SMART – Linux tool

Mailbag Assistant

Norton Utilities



RCMP
ROYAL CANADIAN MOUNTED POLICE

Forensic Tools & Suppliers

NTI

OnTrack

SnapBack

ByteBack

Snagit – screen capture utility

Winternals

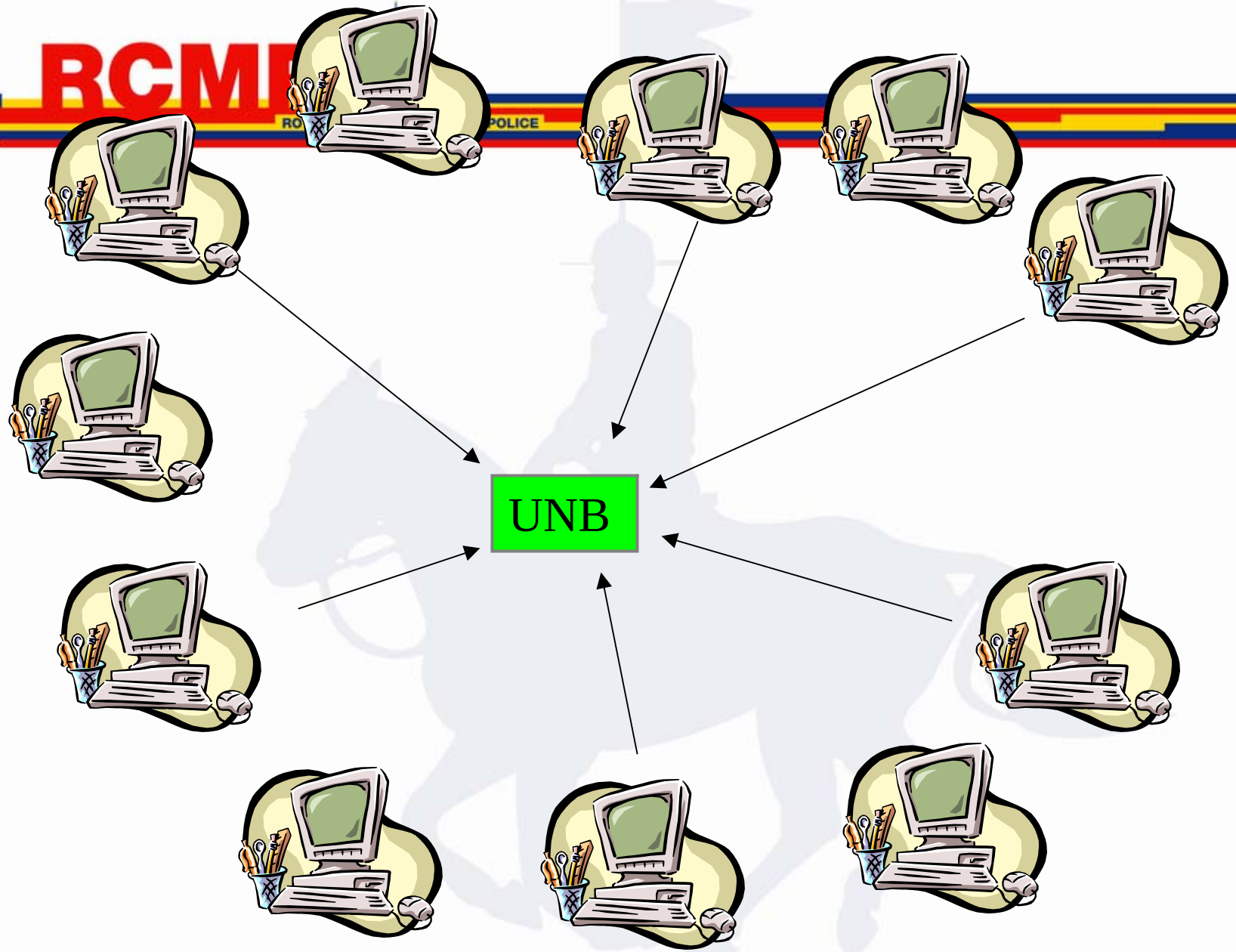
List of tools & suppliers compliments of:

http://www.dmares.com/maresware/linksto_forensic_tools.htm

RCMP
ROYAL CANADIAN MOUNTED POLICE

Distributed DOS Attack

A Coordinated Attack


UNB

RCMP ROYAL CANADIAN MOUNTED POLICE

Why Is This Possible?

The weakness in the IP protocol is that it is based on trust. The protocol trusts that the systems contacting it has legitimate reason to do so, and therefore replies. It does not test the trustworthiness of the connection.

Therefore it becomes an innocent victim of the malicious traffic.

RCMP
ROYAL CANADIAN MOUNTED POLICE

Tools Of The Trade

Compromised slave/zombie machines with high speed connections

Masters to control the zombies

A puppet master to control the masters

A target to attack

RCMP
ROYAL CANADIAN MOUNTED POLICE

Who Are The Zombies (& the masters)?

Unsuspecting individuals with high speed connection

Unpatched vulnerabilities

No anti-virus or not up to date

No firewall (or poorly configured through lack of knowledge – authorizing all requests for access).

RCMP
ROYAL CANADIAN MOUNTED POLICE

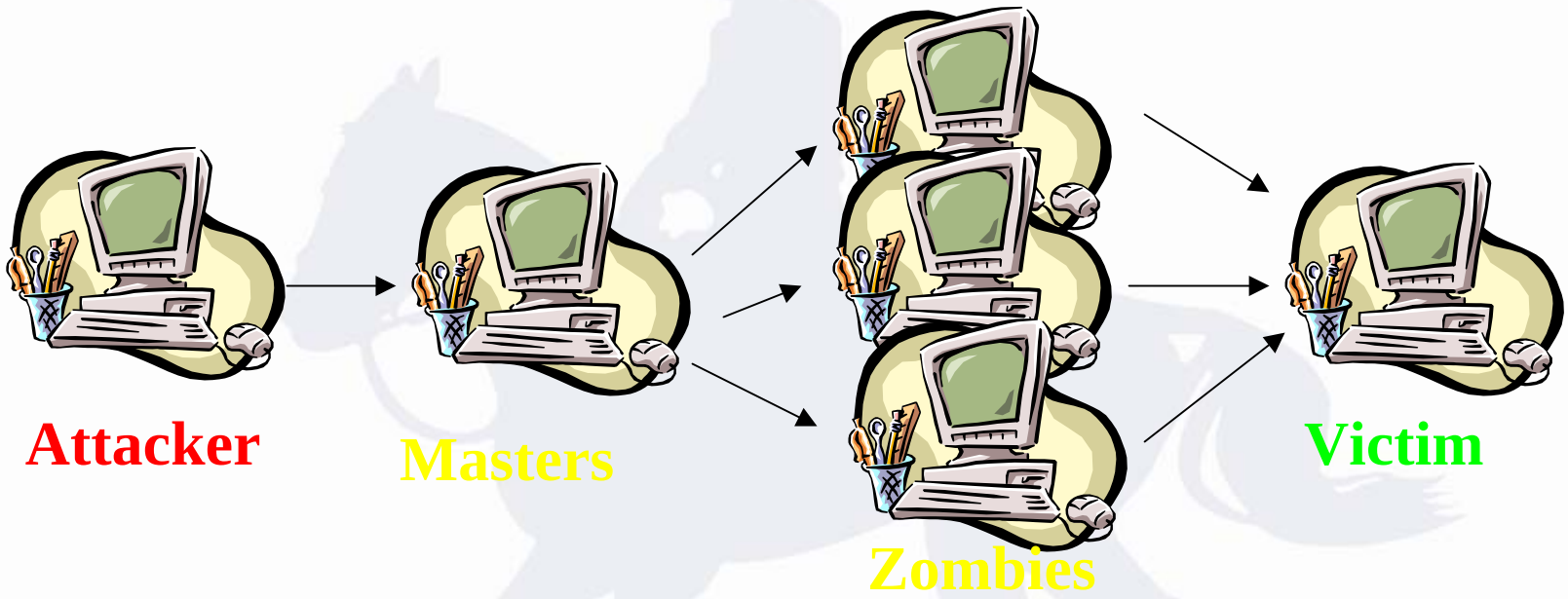
How Do We Track The Source of a DDOS?

RCMP
ROYAL CANADIAN MOUNTED POLICE

Layers Of Protection

Unfortunately, we are talking about 3 layers of protection between the victim and the true attacker.

An attacker initiates a command to master computers that he's taken over. These masters in turn initiate commands to the zombies to launch the attack.



An attacker will have multiple Masters which in turn control multiple Zombies.

RCMP
ROYAL CANADIAN MOUNTED POLICE

The Challenge
Lack Of Logs

The zombie PCs or the master PCs are usually home computers. The vast majority of home computers have limited if any traffic logging.

So what can be done?

RCMP
ROYAL CANADIAN MOUNTED POLICE

Not Only Your Battle…

Companies must prepare in advance (Disaster Recovery Plan).

Companies must have a patch management system in place.

ISPs must strengthen their filtering mechanisms.

End users must be educated about safe-computing practices.

RCMP
ROYAL CANADIAN MOUNTED POLICE

I'm A Victim… Now What?

As normal course of business, keep logs to ensure admissibility.

System being attacked not mission critical? Keep it running to gather further logs

System mission critical? Implement Disaster Recovery Plan.

RCMP
ROYAL CANADIAN MOUNTED POLICE

Secure Evidence

Secure logs

Secure compromised system if possible

RCMP
ROYAL CANADIAN MOUNTED POLICE

The Role Of Police

Police have the responsibility to investigate such incidents and lay criminal charges where applicable.

A DDOS constitute mischief, which is the interfering with the lawful enjoyment/use of property.

The act of compromising the systems is yet another offence, being unauthorized access of computers.

The police is not in a position to be able to provide you with Disaster Recovery Planning, or to clean up the mess afterwards. We are experienced investigators, not experienced Information Security Officers or such.

RCMP
ROYAL CANADIAN MOUNTED POLICE

So When Do I Call The Police?

The police should be contacted at the earliest possible opportunity once it has been determined that you are dealing with a criminal incident that you are prepared to pursue criminally.

Computer log evidence is volatile. How quickly we can get to the next set of logs (system logs, firewall logs, router logs) will dictate our chances of success.

RCMP ROYAL CANADIAN MOUNTED POLICE

Sources Of Information On DDOS Attacks

www.sans.org

http://www.cert.org/csirts/

http://www.csoonline.com/read/050103/bad.html

Distributed Denial of Service Attacks: Threats, Motivations & Management – GSEC Practical Assignment (www.sans.org) by Tom Simcock dated November 5, 2002.

RCMP
ROYAL CANADIAN MOUNTED POLICE

EVIDENCE HANDLING

RCMP
ROYAL CANADIAN MOUNTED POLICE

Evidence Handling

Evidence handling is critical to the successful administration of a forensic service (either private or law enforcement). Anybody handling evidence (computer or otherwise) where you may be required to testify in criminal or civil court, or in front of some other formal hearing board should adopt an evidence handling policy/practice that can demonstrate continuity in the handling of the item. This is better known as chain of custody.

RCMP ROYAL CANADIAN MOUNTED POLICE

Storage Of Evidence

If it's a matter that may be pursued in the courts or through some other judicial process (i.e. internal discipline hearing), chain of custody becomes critical. Exhibits should be stored by the individuals who seized them pending them being turned over to police or to the private forensic examiner. Alternatively it could be stored by a person within the company designated to maintain secure continuity of such material.

RCMP
ROYAL CANADIAN MOUNTED POLICE

Chain Of Custody

Chain of Custody: A means of accountability that shows who obtained the evidence, where and when the evidence was obtained, who secured the evidence, and who had control or possession of the evidence from the time it was collected to the time it is presented in court.

Use a movement control sheet to document chain of custody.

A defence lawyer can attack the continuity of the evidence. If it is not properly documented, it could result in the evidence being inadmissible.

RCMP ROYAL CANADIAN MOUNTED POLICE

Collection Of Evidence

Preserving a chain of custody for electronic evidence as well as the integrity of the evidence itself, at a minimum, requires proving:

- **No information has been added, changed, or removed,**
- **A complete copy was made (never work on the original)**
  - **Validate it using MD5 hash**
- **A reliable copying process was used, and**
- **All media was properly secured**

MD5 Hash

The process of taking a file (or a string) of arbitrary length and outputs a 128-bit unique "fingerprint" of the input. If even one bit is different, the checksum will indicate this.

Sample hash of a file created in Linux Red Hat using vi, with the content being "This is a test."

Hash result: 02bcabffffd16fe0fc250f08cad95e0c

I created a second file with the exact same content, and received the exact same MD5 hash.

Date/time stamps, or file name will not affect the hash value.

How Unique Is MD5 Hash?

The likelyhood of winning the 6/49 is approximately 1 in 14 Million (1.4 X 10^7).

The likelyhood of two people having the same DNA structure is 1 in 100 Billion (1 X 10^11).

A 128 bit value has 2^128 possible values for output.

The likelyhood of two different files having the same MD5 hash is approx. 3.4 X 10^38.

RCMP ROYAL CANADIAN MOUNTED POLICE

Collection/Storage of Evidence

Use CD-Rs ensure that the media is sterile, and data cannot be modified later.

Keep detailed notes (all involved in the chain of custody.)

Include an accurate description of the items handled/collected.

Date/time and initial items that you seize.

Photograph the scene (including hardware, s/n). It can further assist in establishing identity of the item later on (for court or otherwise).

RCMP ROYAL CANADIAN MOUNTED POLICE

Summary

Sound policies on computer incident response handling and a disaster recovery plan are necessary in today's environment. It can make the difference between being down for a short while, or a long time. It can also make the difference between gathering the necessary evidence to maximize the chances of tracking down the person(s) responsible and holding them accountable in civil and/or criminal proceedings.

RCMP ROYAL CANADIAN MOUNTED POLICE

Thank You

Cpl. Jacques Boucher

jacques.boucher@rcmp-grc.gc.ca

(e-mail me for PDF of this presentation)

Royal Canadian Mounted Police
Atlantic Region Integrated
Technological Crime Unit
(506) 452-4245