

Pakistan Honeyynet Project

Fighting Spam with Honeyypots

Kamran Muzaffer

Speaker

- Kamran Muzaffer
 - System Security Engineer for Pakistan's largest ISP, Cyber Internet Services
 - Co-Founder, Pakistan Honeynet Project
 - BSI Certified BS 7799 Security Auditor
 - 3 years experience of managing email servers

Objective

- Knowledge Sharing
- Experience Sharing
- Raising awareness towards the intensity of the problem

Independence through Knowledge:

Bad people have joined hands and working together to make use of the innocent and ignorant users across the world.

Let's share and work together in the fight against Cyber evils.

Agenda

- Part 1 – Introduction to Spam
- Part 2 – Spam Protection
- Part 3 – Honeytraps / Honeytraps
- Part 4 – Spam and Honeytraps

Introduction to Spam

- What is Spam
- History
- The motives
- The damage
- Methods – How spam works?
- Myths about spamming

Spam Protection

- Different Methods of Spam Protection
- Spam Pattern designing
- Common Spam patterns
- Considerations for Spam protection

Honeypots

- **Introduction to Honeypots**
 - Goals
 - Research Alliance
 - Alliance members
- **How honeypots work**
 - What is honeypot
 - Advantages
 - Disadvantages
 - Types
 - Examples of honeypots
- **Honeynets**
 - How it works
 - HoneyNet Gen-II
 - Issues

Fighting Spam with Honeypots

- Purpose
- Spamming Life Cycle
- Honeypots versus Spammers
- Honeypots and Harvesting
- Honeypots and Open Relays
- Honeypots and Open Proxies
- Integrating results with mail servers

Part 1

Introduction to Spam

1.1 What is Spam?

The term "spam" is refers to unsolicited commercial e-mail or unsolicited bulk e-mail, i.e. e-mail that you did not request. Most often spam contains advertisements for dubious services or products.

1.2 History of Spam

The age of Spam

- March 31st, 2003 marks the 10th anniversary of the term Spam being applied to a USENET post
- May 3rd, 2003 marks the 25th anniversary of the earliest documented E-mail spam.

1.2 History of Spam

Where the term came from?

from the spam skit by Monty Python's Flying Circus. In the sketch, a restaurant serves all its food with lots of 'spam', and the waitress repeats the word several times in describing how much spam is in the items. When she does this, a group of Vikings in the corner start a song:

"Spam, spam, spam, spam, spam, spam, spam, spam, lovely spam! Wonderful spam!"

Until told to shut up.

Thus the *meaning* of the term at least: **something that keeps repeating and repeating to great annoyance.**

1.2 History of Spam

The first internet E-mail spam, sent by DEC

DEC announced a new DEC-20 machine in 1978 by sending an invite to all ARPANET addresses on the west coast, using the ARPANET directory, inviting people to receptions in California.

Compaq now owns DEC, so perhaps Bill Hewlett and Dave Packard's heirs are simply among those who vowed never to do business with spammers? Of course in 1978 nobody called this a spam.

1.2 History of Spam

First Giant Spam – ‘Jesus is coming soon’

The first major USENET spam came on January 18 of 1994 by The Andrews University sysadmin – Clarence Thomas . Every single newsgroup found in it a religious screed declaring:

Global Alert for All: Jesus is Coming Soon.

1.2 History of Spam

The birth of the term 'SPAM'

- In April of 1994, two lawyers from Phoenix named Canter and Siegel posted a message advertising their fairly useless services in an upcoming U.S. "green card" lottery.
- wasn't the first such abusive posting
- the first deliberate mass posting to commonly get that name.
- Hired a mercenary programmer, on April 12, to write a simple script to post their ad to every single newsgroup (message board) on USENET, the world's largest online conferencing system.

1.3 The Motives behind Spamming

- It costs zero to send spam, so if they get one sale, they've made a profit.
- they make money based on how many millions they can send the message to.

1.4 Damages caused by Spamming

- Wastage of network resources
- Wastage of Time
- Annoyance
- Decreasing the efficiency
- Possible DoS on mail servers
- Possible trouble for ignorant users

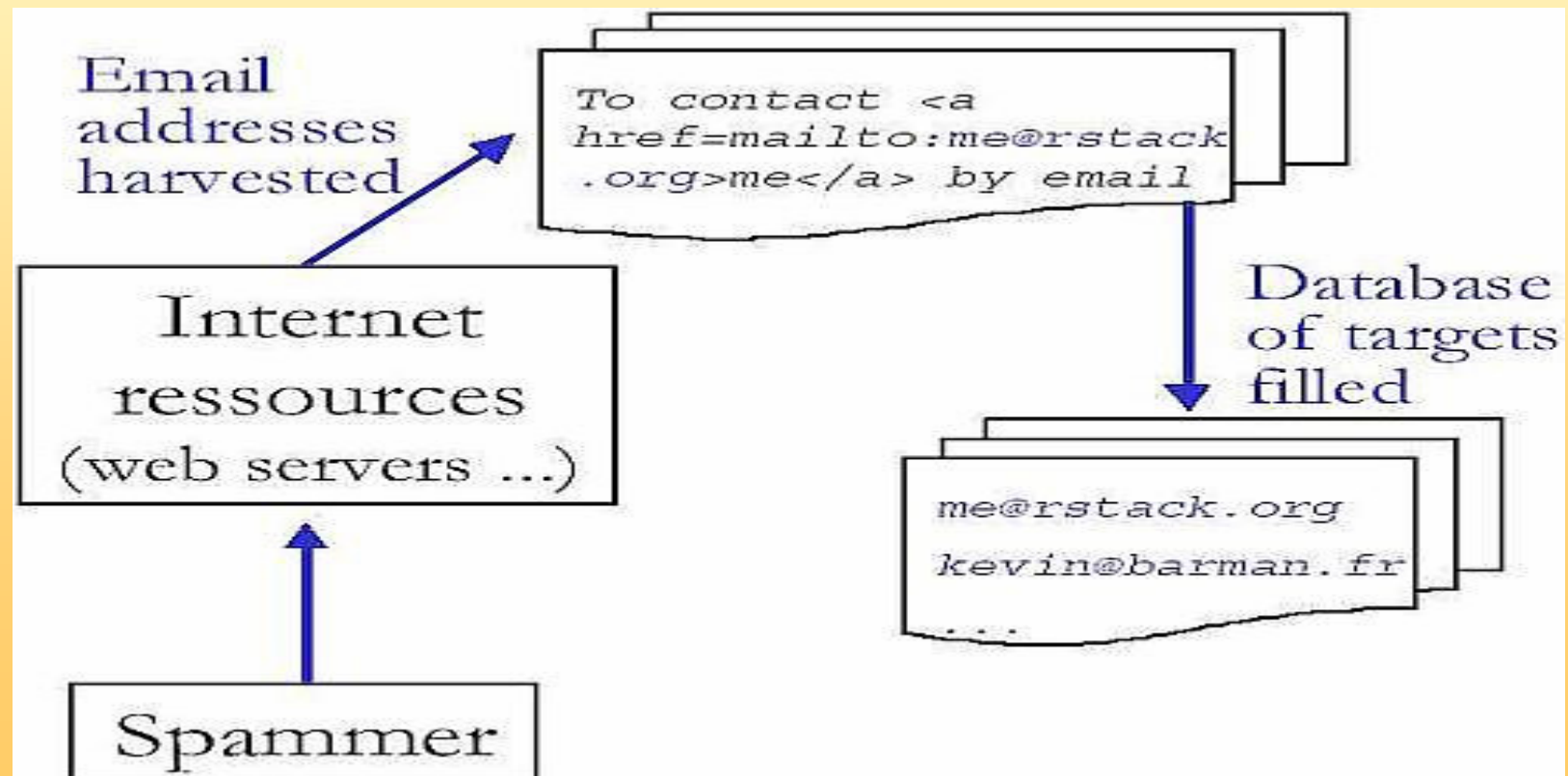
1.5 How spammers work

The spam is sent by spammers because it has become a paid activity of cyber mass advertisement. Spammers' work can be cut into different categories:

- **Harvest:** build a database of targets by finding valid email addresses
- **Stealth and open proxies:** work anonymously while sending ugly emails to their targets
- **Spam and open relays:** find and use servers that accept to relay emails anywhere

1.5 How spammers work

Harvesting the database:



1.5 How spammers work

Different methods for email address harvesting:

- Collection of addresses through automatic programs that are looking at the headers of every message posted. By saving specific fields (From:, Reply-To:), spammers may easily build huge lists of potential targets.
- Poorly configured mailing lists that give out the list of its subscribers.
- automatic programs crawling Web pages on Internet. For each HTML Web page found, such a program will check for a mailto: link ("send me an email by clicking here") and will follow the Web links proposed to continue this sort of evil seeking.

1.5 How spammers work

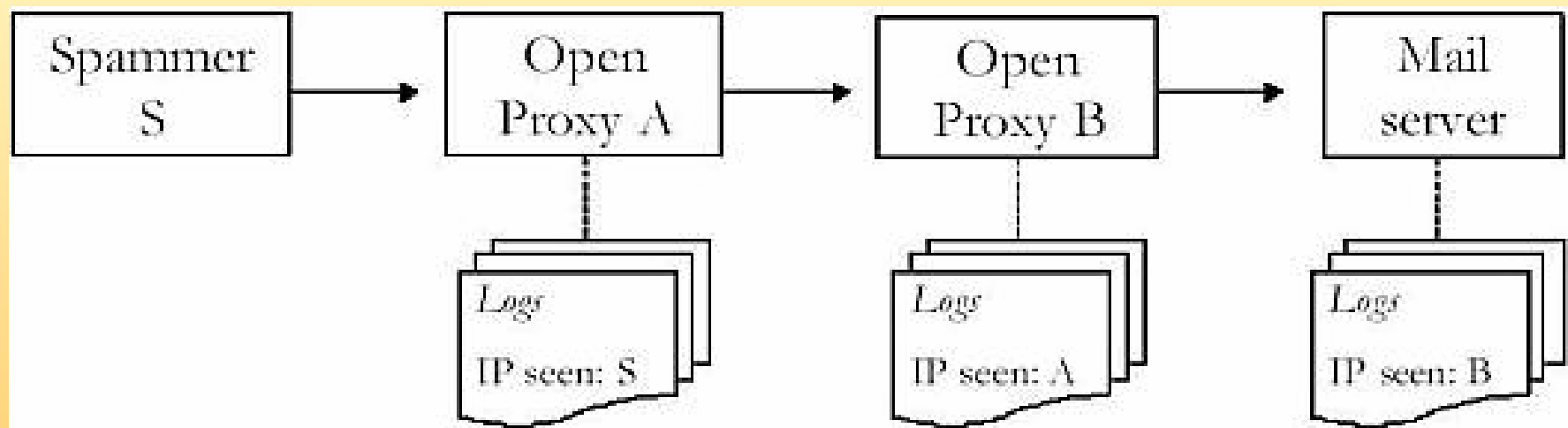
Open proxies:

- Relaying messages through the e-mail server of an innocent third party.
- Doubles the damages: both the receiving system and the innocent relay system are flooded with spam.
- The flood of complaints goes back to the innocent site because it was made to look like the origin of the spam.

Many spammers send their spam from a free account from a large ISP such as AOL, Yahoo!, or Hotmail, then abandon the account and open a new one to use for the next assault.

1.5 How spammers work

Proxy Chaining:



The longer the chain, the stealthier they become, but they will lose time as multiple bounces will result in multiple delays added

1.5 How spammers work

Open Relays:

Mail Transfer Agent (MTA) that accepts third-party relays of e-mail messages even though they are not destined for its domain and they forward emails that are neither to nor from a local user

1.6 Types of Spam

The most commonly seen spam includes the following:

- Chain letters
- Pyramid schemes
- Multilevel marketing
- "Make Money Fast" schemes
- Foreign bank scams
- Offers of phone sex lines and ads for pornographic Web sites
- Illegally pirated software

1.7 Spam Annoyance

- Messages selling pornography (91%)
- mortgages and loans(79%)
- investments (68%)
- real estate (61%)

Courtesy: <http://www.harrisinteractive.com/>

1.8 Myths about Spamming

- It's a kiddie's or amateur's little piece of fun.
- Its not worth fighting; simply ignore it
- It can not be stopped
- No difference in the following
 - Spammed mail (UCE)
 - Junk mail (UJE)
 - Virus infected mails
 - Returned Postmaster mails

Part 2

Spam Protection

2.1 Methods of Spam Protection

- Contacting ISPs
- Mail Server Blacklists
- Signature-Based Filtering
- Bayesian – Statistical Filtering
- Rule-based – Heuristic Filtering
- Challenge Response Filtering
- Laws Against Spamming

2.1 Methods of Spam Protection

- FFBs – Filters that Fights Back
- Slow Senders
- Penny per mail
- Secret Address
- Junk Address

Contacting ISPs

- **Good:** Raises cost of spamming.
- **Bad:** Laborious.
- **Role:** Partial solution, for experts.

Mail Server Blacklists

- **Good:** Block spam right at the server.
- **Bad:** Incomplete, sometimes irresponsible.
- **Role:** A first pass to eliminate up to 50% of spam early on.

Signature-Based Filtering

- **Good:** Rarely blocks legitimate mail.
- **Bad:** Catches only 50-70% of spam.
- **Role:** A first-pass filter on big email services.

Bayesian – Statistical Filtering

- **Good:** Catch 99% to 99.9% of spam, low false positives.
- **Bad:** Have to be trained.
- **Role:** Best current solution for individual users.

Rule-based – Heuristic Filtering

- **Good:** The best catch 90-95% of spam, easy to install.
- **Bad:** Static rules, relatively high false positives.
- **Role:** Easy server-level solution.

Challenge Response Filtering

- **Good:** Stops 99.9% of spam.
- **Bad:** Rude, delays or drops legitimate email.
- **Role:** Grandmothers, cranks.

Laws against Spamming

- **Good:** Truly threaten spammers.
- **Bad:** Aren't enforced, or are full of loopholes.
- **Role:** Could eliminate 80% of spam, if done right.

FFBs – Filters that Fight Back

- **Good:** Raise cost of spamming.
- **Bad:** Involve blacklists.
- **Role:** Speculative idea.

Slow Senders

- **Good:** Raises cost of spamming.
- **Bad:** Requires new email protocol.
- **Role:** Speculative idea.

Penny per mail

- **Good:** Raises cost of spamming.
- **Bad:** Requires new email protocol, bureaucracy.
- **Role:** Speculative idea.

Secret Address

- **Good:** Easy.
- **Bad:** Doesn't work.
- **Role:** Facile recommendation for brief news articles.

Junk Address

- **Good:** Cuts some spam.
- **Bad:** Can't always use them.
- **Role:** Use on web sites that make you register.






2.2 Spam Pattern Designing

- Valuable Stats from Mail Servers
- Analysis of Mail Server Stats
- Suspected Spam list detection
- Evaluation of suspected Spam list







Valuable Stats from Mail Servers

- Top mail sending hosts – Remote SMTP servers
- Top 'From' addresses
- Top sending domains (if possible)
- Top recipient addresses








Valuable Stats from Mail Servers

Top SMTP Connections from Hosts/IPs		
<u>IP Addresses</u>	<u>Count</u>	<u>%</u>
vic-dial-196-30-233-116.mweb.co.za	50738	
69.158.244.136	6154	
203.133.252.124	4269	
69.158.206.72	3677	
12.104.232.18	3210	

Valuable Stats from Mail Servers

Top 'From' Addresses		
<u>Email Address</u>	Count	<u>%</u>
reply@daily-serving.com	3106	
fr8eedmanbill@hotmail.com	2700	
editor@samonitor.com	2535	
email@Amh-pakistan.cjb.net	2214	
islam@Amh-pakistan.cjb.net	2020	
mx2@wisenet.com.sg	2002	

Valuable Stats from Mail Servers

Top Recipient Addresses		
<u>ID</u>	<u>Count</u>	<u>%</u>
<u>kirshan</u>	7044	
<u>Tahir Barry</u>	6830	
<u>Asiatic Chemicals</u>	6793	
<u>rqaf</u>	6753	
<u>tabindanoor</u>	4432	
<u>texplorer</u>	1062	
<u>risk</u>	1005	

Analysis of Mail Server Stats

- Why are these hosts sending so many mails to my domain?
- Are these hosts sending 'legitimate' messages to my server?
- Are these hosts legitimate SMTP servers or just a host without FQDN?
- Does the nature of client verify the reception of so many emails in a day?
- Why this specific address or domain sending so many mails to different users on my domain?
- Are the mails send to a specific address, legitimate mails or contains some sort of promotional or publicity contents?
- Are these mails genuine or just bounced back messages from post masters of different mail servers?

Suspected spam list detection

- The list of suspected spamming hosts
- The list of suspected 'From' addresses
- The list of suspected 'To' addresses that are under attack by spammers

Evaluation of suspected spam list

- No genuine mail will be lost if specific host, domain, From address or To address is blocked on my mail server.
- The client has not subscribed to any mass mailing, spamming or junk mail sending mailing list.

Recent Patterns

Senders (From Addresses):

- <> [empty from address]
- re-mail_system*
- error_mail*
- auto-mailer*
- info@*
- New_account*

Recent Patterns

Subject Line contents:

- Your mail password
- Your password
- Oh God it's
- *<Key:*>*
- *<ESMTP:*>*
- *<SMTP:*>*
- Details
- Invalid mail
- Confirmation
- Registration confirmation
- Mail delivery system

Recent Patterns

Envelope To Addresses

- Mail_List*@<host domain>
- contact@<host domain>
- All_Users*@<host domain>
- private@<host domain>
- Free_Mail*@<host domain>
- Mail-boxes*@<host domain>
- SMTP-Mail*@<host domain>
- mailer*@<host domain>
- Electronic_Mail*@<host domain>
- sender_gmail@<host domain>
- Mail-User*@<host domain>
- Your_Account*@<host domain>

Considerations for Spam Protection

- Understanding of mail server logs
- Understanding of email headers
- Verification of different scenarios that no legitimate mails is being dropped as a result of new spam pattern application
- Constant monitoring of mail server logs for

Part 3

Honeypots/
Honeynets

HoneyNet Project

- Volunteer organization of security professionals.
- Open Source, share all of our research and findings.
- Deploy networks around the world to be hacked.
- Everything we capture is happening in the wild.
- We have no agenda, no employees, nor anything to sell.

Goals

- Awareness: To raise awareness of the threats that exist.
- Information: For those already aware, to teach and inform about the threats.
- Research: To give organizations the capabilities to learn more on their own.

HoneyNet Research Alliance

Starting in 2002, the Alliance is a forum of organizations around the world actively researching, sharing and deploying HoneyNet technologies.

<http://www.honeynet.org/alliance/>

Alliance Members

- South Florida HoneyNet Project
- Georgia Technical Institute
- Azusa Pacific University
- Pakistan HoneyNet Project
- Paladion Networks HoneyNet Project (India)
- Internet Systematics Lab HoneyNet Project (Greece)
- Mexico HoneyNet (Mexico)
- HoneyNet.BR (Brazil)
- Irish HoneyNet
- Norwegian HoneyNet
- UK HoneyNet
- French HoneyNet Project
- Italian HoneyNet Project

How Honeynets Work

Honeypots

- A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.
- Has no production value, anything going to or from a honeypot is likely a probe, attack or compromise.
- Primary value to most organizations is information.
- Eliminates 'False Positives'
- Keep real resource farther from the intruder
- Increases the delay between and an actual resource.

Advantages

- Collect small data sets of high value.
- Reduce false positives
- Catch new attacks, false negatives
- Work in encrypted or IPv6 environments
- Simple concept requiring minimal resources.

Disadvantages

- Limited field of view (microscope)
- Risk (mainly high-interaction Honeypots)

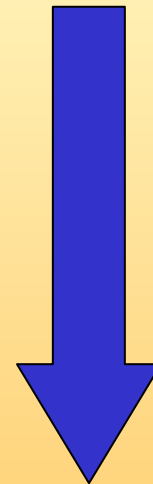
Types

- Low-interaction
 - Emulates services, applications, and OS's.
 - Low risk and easy to deploy/maintain, but capture limited information.
- High-interaction
 - Real services, applications, and OS's
 - Capture extensive information, but high risk and time intensive to maintain.

Examples of Honeypots

- BackOfficer Friendly
- KFSensor
- Honeyd
- Symantec Decoy Server
- Honeynets

Low Interaction



High Interaction

Honeynets

- High-interaction honeypot designed to capture in-depth *information*.
- Information has different value to different organizations.
- Its an architecture you populate with live systems, not a product or software.
- Any traffic entering or leaving is suspect.

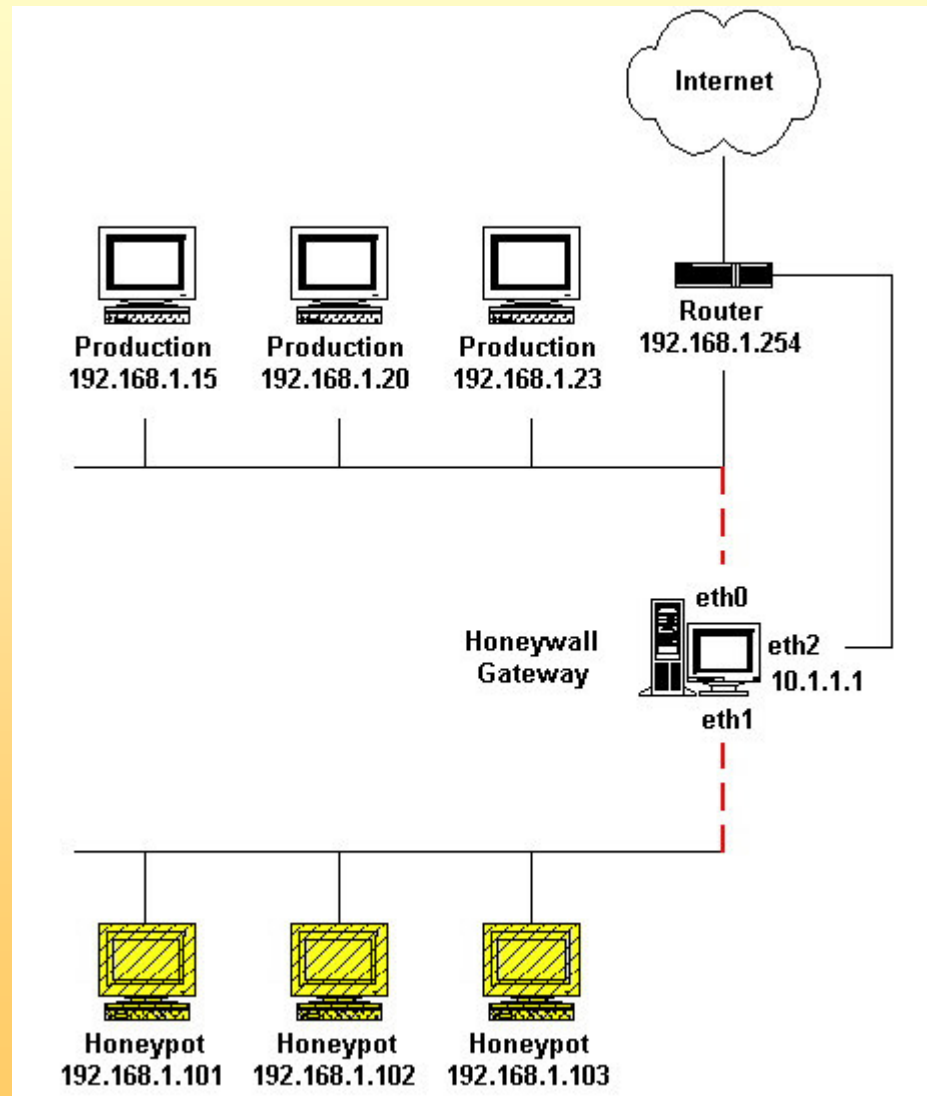
How it works

A highly controlled network where every packet entering or leaving is monitored, captured, and analyzed.

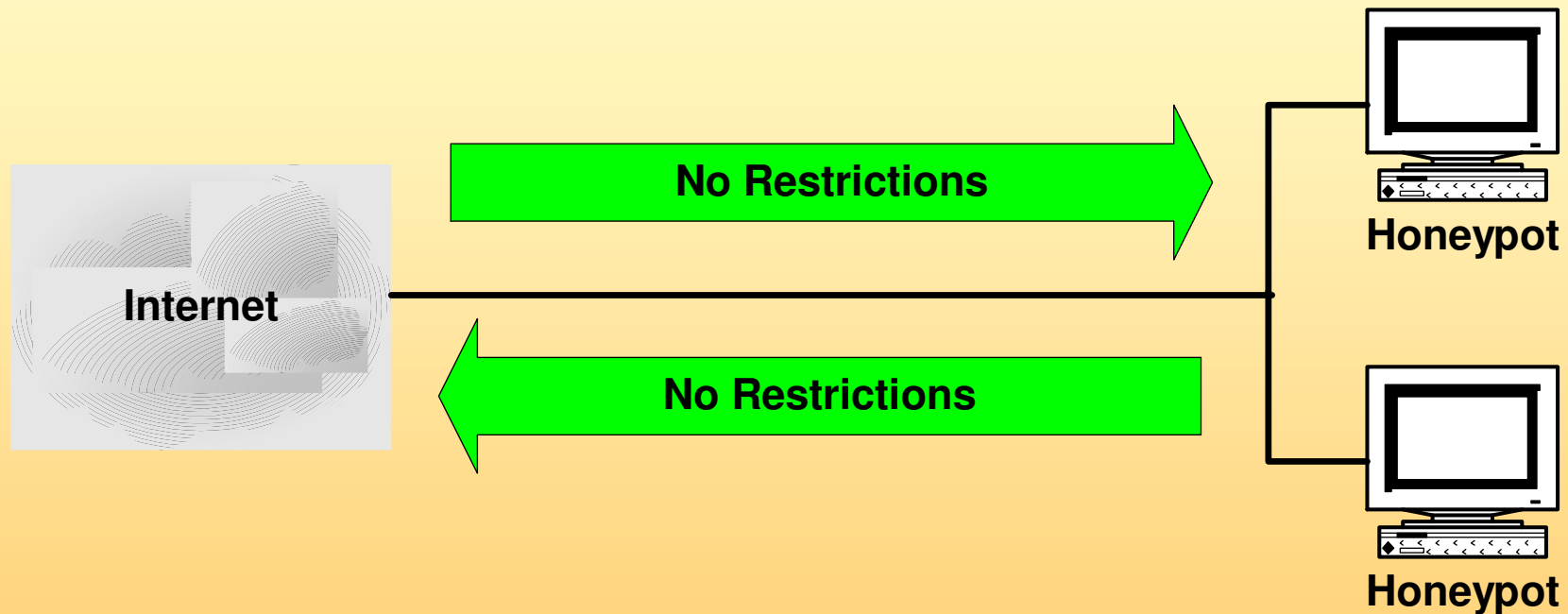
- Data Control
- Data Capture

<http://www.honeynet.org/papers/honeynet/>

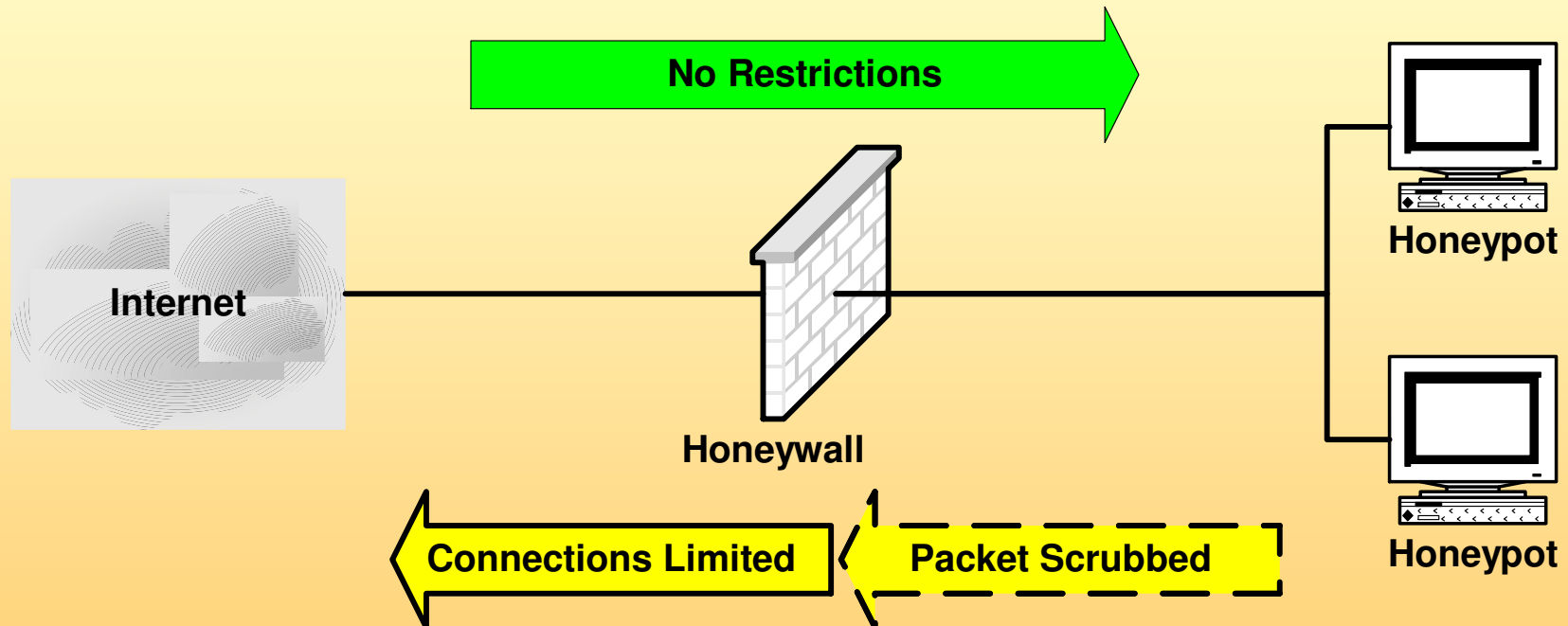
Honeynet - GenII



No Data Control



Data Control



Issues

- Require extensive resources to properly maintain.
- Detection and anti-honeynet technologies have been introduced.
- Can be used to attack or harm other non-Honeynet systems.
- Privacy can be a potential issue.

Part 4

Fighting Spam
with
Honeypots

Purpose

The sole purpose of using Honey pots against Spam is:

- Eliminate False Positives
- More freedom of work
- Protection of actual mail servers

Honey pots are servers which pretend to be a real server but actually it isn't. Hence, logically no traffic should enter the Honey pots except the probes and malicious attempts.

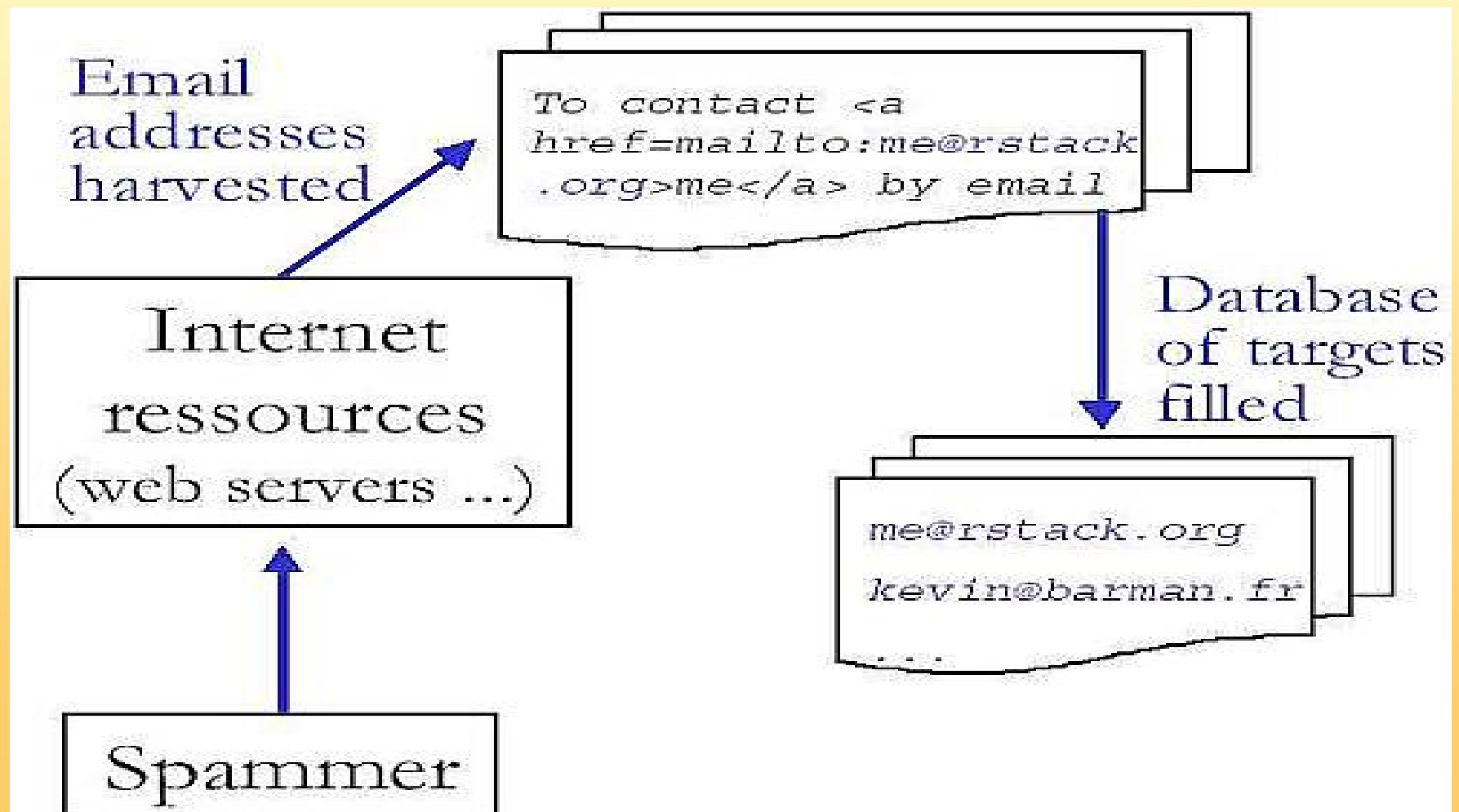
Spamming Life cycle

- **Harvest:** build a database of targets by finding valid email addresses
- **Stealth and open proxies:** work anonymously while sending ugly emails to their targets
- **Spam and open relays:** find and use servers that accept to relay emails anywhere

Harvesting techniques

- Automated scripts that scan posts on mailing list for 'Mail From:' and 'Reply-To:' addresses
- Misconfigured, badly managed mailing lists disclosing the complete subscribers' list
- Automated script for the detection of 'Mail To' parameter in HTML codes of the websites

Harvesting techniques



Open Proxies

- A proxy server opened to the world for almost any kind of request
- **Flow:** Attacker:any → Proxy:8080 → Target:25
- **Looks:** Proxy → Target
- **Result:** Attacker → Target
- **Possibility:** Attacker:any → Proxy1:8080 → Proxy2:8080 → Proxy3:8080 → Proxy[n]:8080 → Target:25

Example of Open Proxy Abuse

```
$ cat /var/log/snort/192.168.1.66/SESSION\.:8080-407
CONNECT 207.69.200.120:25 HTTP/1.0
HELO [217.128.a.b]
MAIL FROM:<openrelay@abuse.earthlink.net>
RCPT TO:<spaminator@abuse.earthlink.net>
DATA Message-ID: <36af800461754252ab1107386a9cd8eb@openrelay@abuse.earthlink.net>
To: <spaminator@abuse.earthlink.net>
Subject: Open HTTP CONNECT Proxy
X-Mailer: Proxycheck v0.45
This is a test of third-party relay by open proxy.
These tests are conducted by the EarthLink Abuse Department.
EarthLink, by policy, blocks such systems as they are discovered.
Proxycheck-Type: http
Proxycheck-Address: 217.128.a.b
Proxycheck-Port: 8080
Proxycheck-Protocol: HTTP CONNECT
This test was performed with the proxycheck program. For further information see
<http://www.corpit.ru/mjt/proxycheck.html>
.
QUIT
```

Open Relays

- Similar to open proxy
- MTA that accepts third-party relays
- Bypasses the direct IP/subnet blockage by the target MX server

Honeypots versus Spammers

Possible use of honeypots :

1. when spammers come to your Web site to steal email addresses and transform them into future targets;
2. when spammers try to connect to your proxy servers and try to bounce elsewhere by abusing your services;
3. when spammers inject SMTP traffic to your email servers in order to send unsolicited emails through you.

Mitigating Email Harvesting

- Secure and well managed mailing lists
- Use of images displaying email addresses on a web page instead of using 'Mail To:' tags
- Use of 'smart conventions' e.g
kamran@honeynet.org.pk =
kamran_at_honeynet.org.pk or
kamran@honeynet.....

Honeypots and Harvesting

PHP Code:

```
<?
echo '<a href=mailto:'. $REMOTE_ADDR. '_'. date('y-m-j'). '-
spamming@honeynet.org.pk
title="There is no spoon">For stupid spambots';
?>
```

Effect:

```
<a href=mailto:80.13.aa.bb_03-11-17-
spamming@frenchhoneynet.org>...
```

Result:

The day this email address is used as a target of spam, the owner will be able to determine the IP used by the spammer.

Honeypots and Harvesting

Publishing dummy pages

- Fake or testing email addresses displayed in the same font color as the background color.
- Only web scanners will be able to read it but no human.

Honeypots and Harvesting

Corrupting Spammers' database:

- Publish fake randomly generated email addresses on your website.
- Spamming mail server will not be able to resolve fake domains
- Increase in spamming servers' load – decrease in efficiency
- Increase in mail queue at spamming server

The more you publish the slower the spamming will get

Example: <http://www.hostedscripts.com/scripts/antispam.html>

Honeypots and Open Proxies

Honeyd configuration:

```
create relay
set relay personality "OpenBSD 2.9-stable"
add relay tcp port 25 "sh /usr/local/share/honeyd/scripts/sendmail.sh
    $ipsrc $sport $ipdst $dport"
add relay tcp port 3128 "sh /usr/local/share/honeyd/scripts/squid.sh
    $ipsrc $sport $ipdst $dport"
add relay tcp port 8080 "sh /usr/local/share/honeyd/scripts/proxy.sh
    $ipsrc $sport $ipdst $dport"
set relay default tcp action block
set relay default udp action block
bind 192.168.1.66 relay
```

Honeypots and Open Proxies

Use of 'Proxypot':

smtp1: the whole SMTP connection is faked.

Pros : no SMTP outbound traffic is needed, so it will save your network bandwidth.

Cons : only fool novices

smtp2: connect to the real SMTP server, read its 220 banner and maybe issue a HELP command to find out what kind of server it is, then hang up and use that information to fake a more convincing SMTP session.

Pros : if the spammer knows the version of the targeted email server, he will believe this is the real one and you won't have much of a fingerprinting problem.

Cons : generate outbound traffic.

smtp3: connect to the real SMTP server and pass through all recognized commands except DATA and EXPN. RCPT and VRFY are rate-limited.

Pros : this is the extreme simulation and it's almost impossible to do better, because using DATA properly would deliver the email and this is something you want to avoid.

Cons : like every simulator, a spammer may discover that this not a real one, and fingerprinting possibilities will still exist.

Honeypots and Open Relay

Reconfigure sendmail.mc file:

```
FEATURE(`promiscuous_relay')dnl  
define(`confDELIVERY_MODE', `queue')
```

- Verify the status by free Open Relay Check Service.
- Mails received should be available in the queued folder

Integrating Results with Mail Servers

- Creation of master mail box
- Forward all mails from the master mail box to a specific address on your main mail server
- From the main mailbox, extract the list of spamming IPs by the contents of subject line.
- Little bit of scripting, results can be integrated with mail server's or even firewall's blacklist

Questions?

Contact

<http://www.honeynet.org.pk>

kamran_at_honeynet.org.pk