

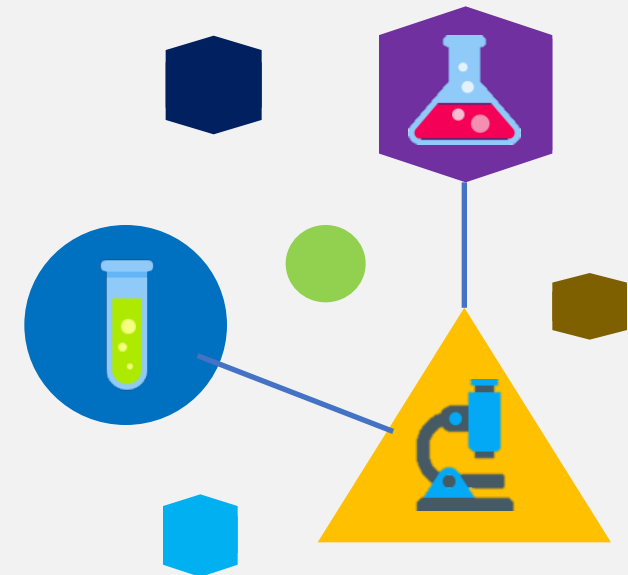
Using Test Ranges for Cyber Security Research

By Abigail Koay

Supervised by: Aaron Chen & Ian Welch

Victoria University of Wellington

eResearch 2016



Overview

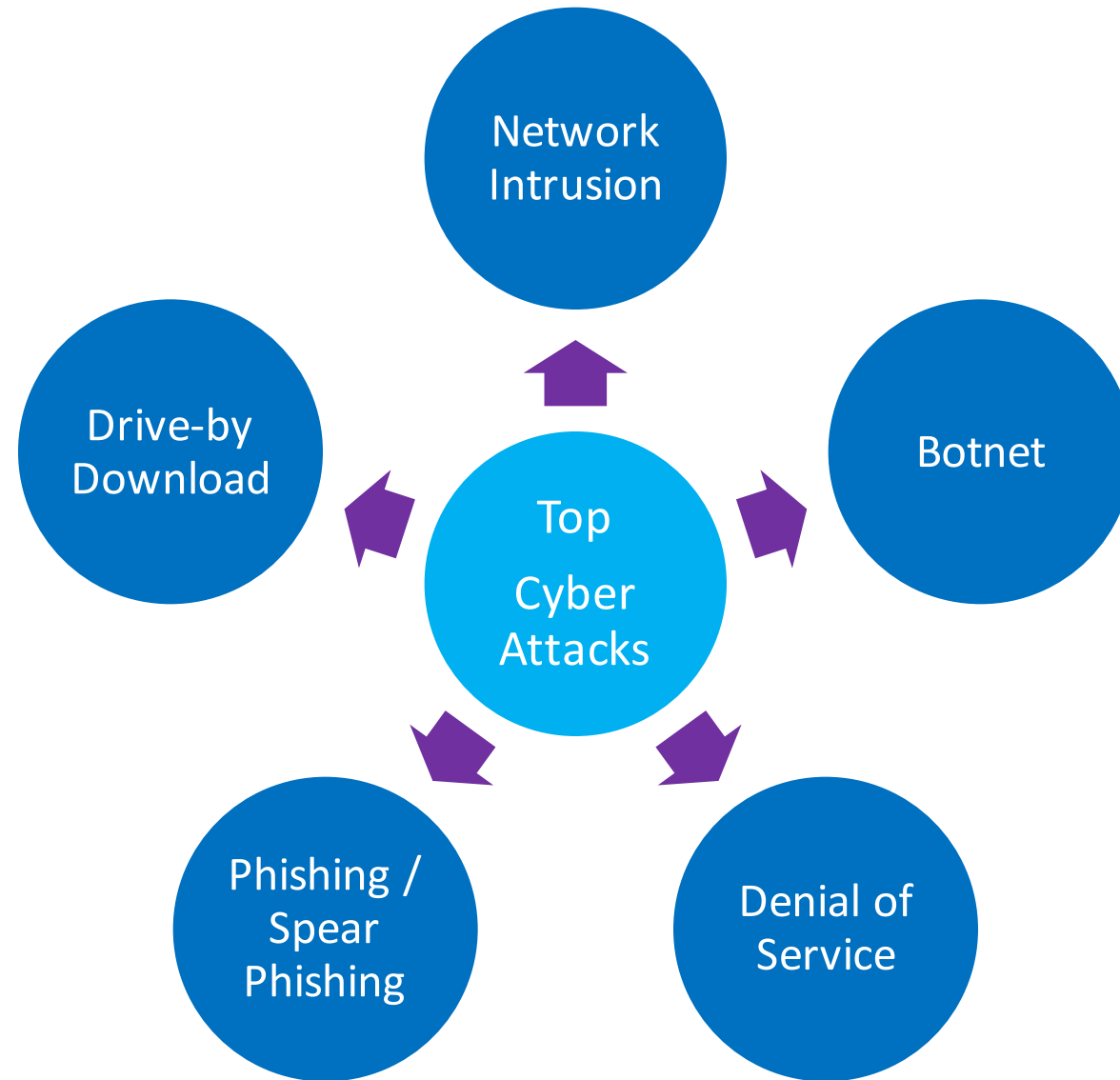
- > Cyber Security
- What we do?
- What we encounter?
- What we can improve

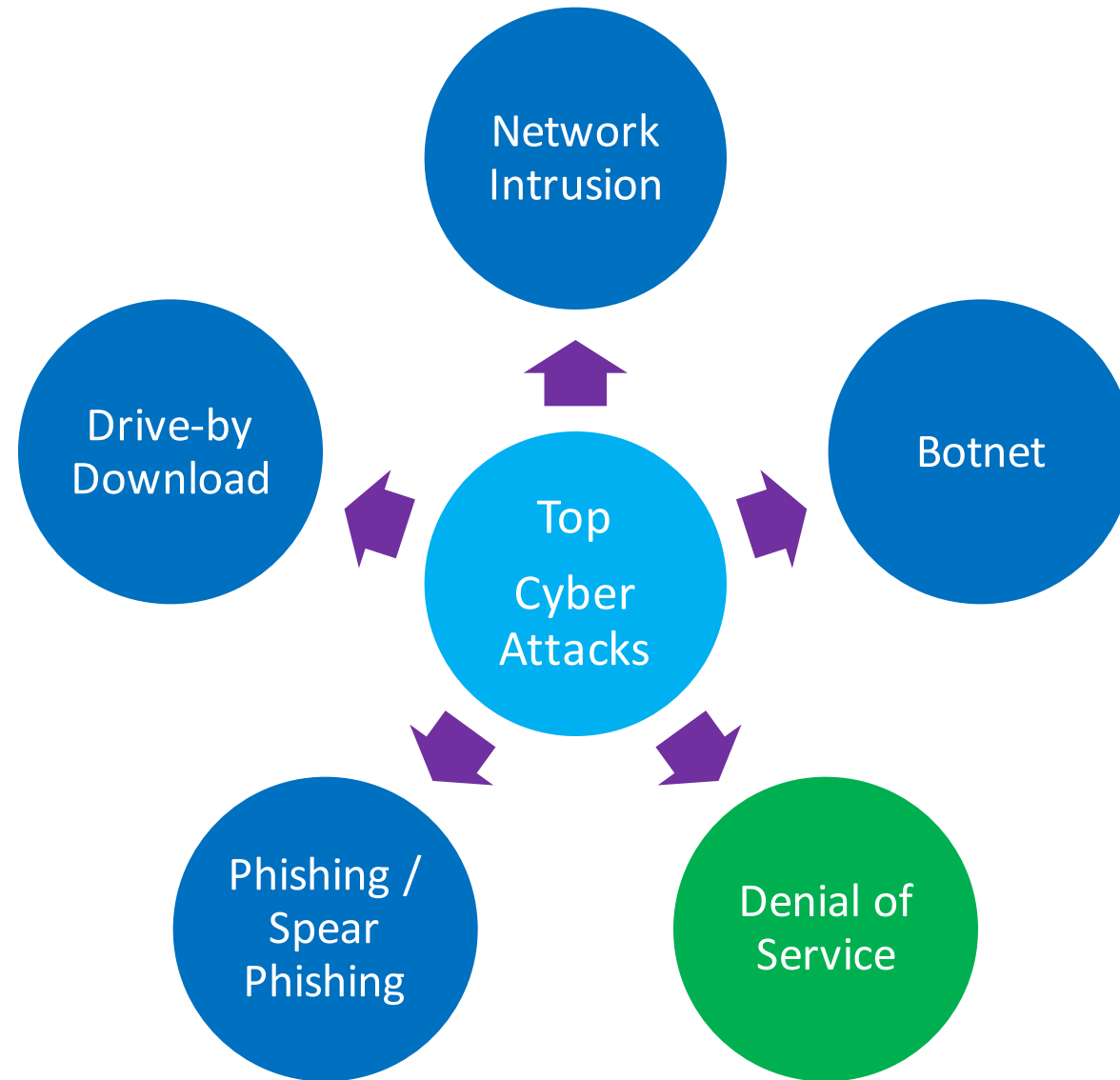
Cyber Attacks, in real time

[Live Cyber Attacks Digital Map](#)

ATTACK ORIGINS		ATTACK TYPES		ATTACK TARGETS		LIVE ATTACKS						
COUNTRY	#	PORT	SERVICE TYPE	#	COUNTRY	TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
United States	100	5060	o sip	219	United States	14-00-36.248	Sunnyvision Limited	124.248.211.19	Tsuen Wan, HK	Tsuen Wan, HK	sentinelstrm	1947
Canada	100	80	o http	15	United Arab Emir...	14-00-36.759	China Unicom Shanxi Province Network	124.163.208.1...	Taiyuan, CN	Dubai, AE	unknown	19320
China	7	138	o unknown	7	Romania	14-00-37.118	Akamai Technologies Inc.	104.117.180.64	Cambridge, US	Lynnwood, US	unknown	49623
Russia	6	22	o ssh	6	Russia	14-00-37.433	Syptec Las Vegas	70.96.87.201	Las Vegas, US	Las Vegas, US	unknown	138








DDoS on the Rise - Worldwide

Microsoft Xbox Live suffers DDoS attack from Phantom Squad, Sony PSN also threatened

By Peter Gothard

18 Dec 2015

 Print  Send

Massive DDoS Attack Leaves UK Universities Without Internet

By *Ryan De Souza* on December 10, 2015  Email  @hackread  **CYBER ATTACKS** **CYBER CRIME**

BBC Websites Taken Offline by DDoS Attack

BY *ANGELA MOSCARITOLO* JAN. 1, 2016, 2:17 A.M.

Thai government websites hit by denial-of-service attack

GitHub



GitHub's Largest DDoS Attack Is Still Going, 4 Days Later

March 30, 2015 // 10:38 AM EST

DDoS Attack on the Rise



Vodafone New Zealand adds Arbor Cloud to combat DDoS extortion

"We've seen a significant rise in the size of DDoS attacks in this country in recent months."

Kaspersky: Financial institutions in ANZ DDoS attack targets in Q3

Russian-based security firm, Kaspersky Lab, has found Australia and New Zealand financial institutions were amongst the first in the world to be hit with DDoS attacks in the third quarter of this year.



By Asha Barbaschow | November 4, 2015 -- 05:00 GMT (16:00 AEDT) | Topic: Security



Spark users experience internet meltdown

8:54 PM Saturday Sep 6, 2014

DDoS Attacks, in real time

[Live DDoS Attacks Digital Map](#)

CO
EC

Brazil

CL

MA

CB

IL

DE

CZ

IT

CU

VA

FI

UA

ES

VA

SV

SE

IN

China

KR

JP

Australia

+

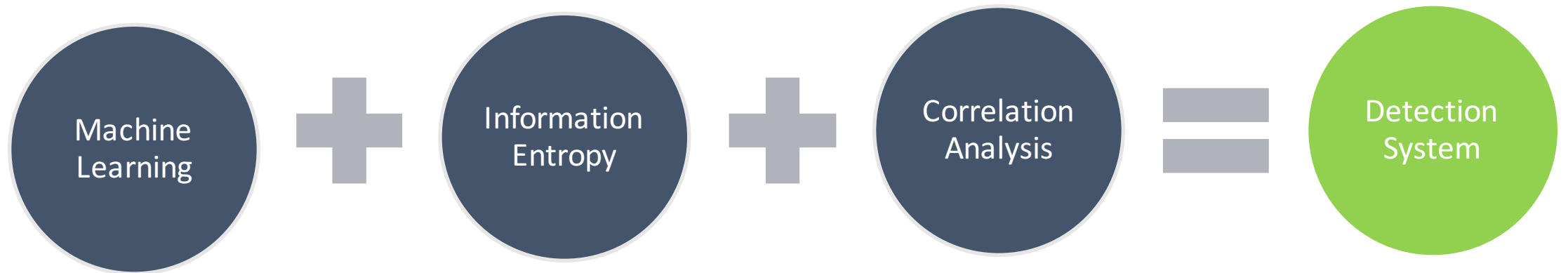
-

Overview

- Cyber Security
- > What we do?
- What we encounter?
- What we can improve

What's my research about?

Developing a better DDoS detection system for large scale network



How do I evaluate my system?

- Existing datasets
 - MIT Lincoln Lab DARPA Intrusion Detection Data Sets (1998-2000)
 - University of New Brunswick ISCX Intrusion Detection Evaluation DataSet (2012)
- Simulation / Emulations
 - Simulation software
 - Test ranges

What are Cyber Security Test Ranges?



A secure network environment for experimenters to launch attacks safely.

Publically Available Test Ranges





Cyber-Defense Technology
Experimental Research
Laboratory

- >600 researchers worldwide
- ~ 200 scientific papers
- >3800 students received training
- > 540 high-capacity multicore server nodes
(Berkeley, Los Angeles, Arlington)



New Project Application Form

All fields except those with a gray background are required.													
Project Leader Information: <i>All fields are required</i>													
Full Name: <i>Your full name including title</i>	<input type="text"/>												
Email Address: <i>The e-mail address that is most appropriate for communication with the DeterLab team, including notification of approval of your project, and of the project leader account at DeterLab</i>	<input type="text"/>												
Phone Number: <i>The phone number that the DeterLab team can use to contact you</i>	<input type="text"/>												
Position, Title, or Job Description: <i>Your position at your employer, e.g. Associate Professor, Research Director, or Director of Engineering</i>	<input type="text"/>												
Full Name of Employer or Affiliated Institution: <i>A corporation, academic institution, government organization, or NGO that you are employed by or affiliated with</i>	<input type="text"/>												
Institution Abbreviation: <i>The short name or abbreviation of your institution, for example: "CalTech" or "NIST"</i>	<input type="text"/>												
Institution's Web Site: <i>The main page of the web site of your corporation, academic institution, government organization, or NGO</i>	<input type="text" value="http://"/>												
Postal Address: <i>Your postal address at your affiliated institution.</i>	<table border="1"> <tr> <td>Address 1</td> <td><input type="text"/></td> </tr> <tr> <td>Address 2</td> <td><input type="text"/></td> </tr> <tr> <td>City</td> <td><input type="text"/></td> </tr> <tr> <td>State/Province</td> <td><input type="text"/></td> </tr> <tr> <td>ZIP/Postal Code</td> <td><input type="text"/></td> </tr> <tr> <td>Country</td> <td><input type="text" value="New Zealand"/></td> </tr> </table>	Address 1	<input type="text"/>	Address 2	<input type="text"/>	City	<input type="text"/>	State/Province	<input type="text"/>	ZIP/Postal Code	<input type="text"/>	Country	<input type="text" value="New Zealand"/>
Address 1	<input type="text"/>												
Address 2	<input type="text"/>												
City	<input type="text"/>												
State/Province	<input type="text"/>												
ZIP/Postal Code	<input type="text"/>												
Country	<input type="text" value="New Zealand"/>												
Username: <i>A 6-to-8-character username-- numbers and letters only-- that will be used a user-id for your login to DeterLab</i>	<input type="text"/>												
Password:	<input type="password"/>												
Retype Password:	<input type="password"/>												

All fields are required.

Project Information:

Project Name:

Your project's name or brief description

Project Plan:

Briefly describe your project's goals, and how you plan to use DeterLab

Project ID:

A 6-to-12-character identifier– numbers and letters only– that will be used a group-id name for members of your project

Project Web Site:

A page in a web site about your project, or your sponsoring organization

Project Organization Type:

Select one broad category that best fits your project

Project Research Focus:

Select one reaserch area that best fits your project

Project Funding or Support:

Select one type of funding or support that best fits your project

Project Listing:

Include your project on the public list of DeterLab projects

Submit

Begin an Experiment

Select Project:	vuwddos2015 ▾
Group:	Default Group ▾ (Must be default or correspond to selected project)
Name: (No blanks)	HTTP DDOS ATTACK
Description: (A concise sentence)	Generate dataset consisting HHTP DDoS Traffic
Your NS file:	Upload (500k max) <input type="button" value="Choose File"/> no file selected or On Server (/proj, /users, /groups, /share) <input type="text"/>
Swapping:	<input checked="" type="checkbox"/> Idle-Swap: Swap out this experiment after <input type="text" value="4"/> hours idle. If not, why not? <input type="text"/> <input checked="" type="checkbox"/> Max. Duration: Swap out after <input type="text" value="24"/> hours, even if not idle.
Linktest Option:	Skip Linktest ▾ (What is this?)
<input type="checkbox"/> Batch Mode Experiment (See Tutorial for more information)	
<input type="checkbox"/> Swap In Immediately	
<input type="button" value="Submit"/>	

```
#Create the topology nodes
foreach node { Attacker Client S1 S2 S3 S4 S5 R0 R1 R2 control } {
#Create new node
set $node [$ns node]
#Define the OS image
tb-set-node-os [set $node] Ubuntu1404-64-STD
}

#Create LAN/AS
set AS1 [$ns make-lan "$Attacker Client $R1" 90Mb 0ms]
set AS2 [$ns make-lan "$S1 S2 $R2 " 90Mb 0ms]
set AS3 [$ns make-lan "$S3 S4 $R1 " 90Mb 0ms]

tb-set-ip-lan $Attacker $Lan1 10.1.1.100
tb-set-ip-lan $Client $Lan1 10.1.1.50
tb-set-ip-lan $R1 $Net1 10.1.1.2
tb-set-ip-lan $S1 $Net2 10.1.2.20
tb-set-ip-lan $S2 $Net2 10.1.2.21
tb-set-ip-lan $R2 $Net2 10.1.2.2
tb-set-ip-lan $S3 $Net3 10.1.3.30
tb-set-ip-lan $S4 $Net3 10.1.3.31
tb-set-ip-lan $R1 $Net3 10.1.3.2
tb-set-ip-lan $R1 $Net3 10.1.3.2

#Create the links
set S5-R0 [$ns duplex-link $S5 $R0 90Mb 3ms DropTail]
set R0-R1 [$ns duplex-link $R0 $R1 90Mb 3ms DropTail]
set R1-R2 [$ns duplex-link $R1 $R2 90Mb 3ms DropTail]

tb-set-ip-link $R0 $S5-R0 10.1.4.2
tb-set-ip-link $S5 $S5-R0 10.1.4.40
tb-set-ip-link $R0 $R0-R1 10.1.8.10
tb-set-ip-link $R1 $R0-R1 10.1.8.11
tb-set-ip-link $R1 $R1-R2 10.1.9.10
tb-set-ip-link $R2 $R1-R2 10.1.9.11

#set node interface
tb-fix-interface $R1 $Net1 "eth1"
tb-fix-interface $R1 $Net3 "eth2"
tb-fix-interface $R1 $R0-R1 "eth3"
```

Example of .ns file

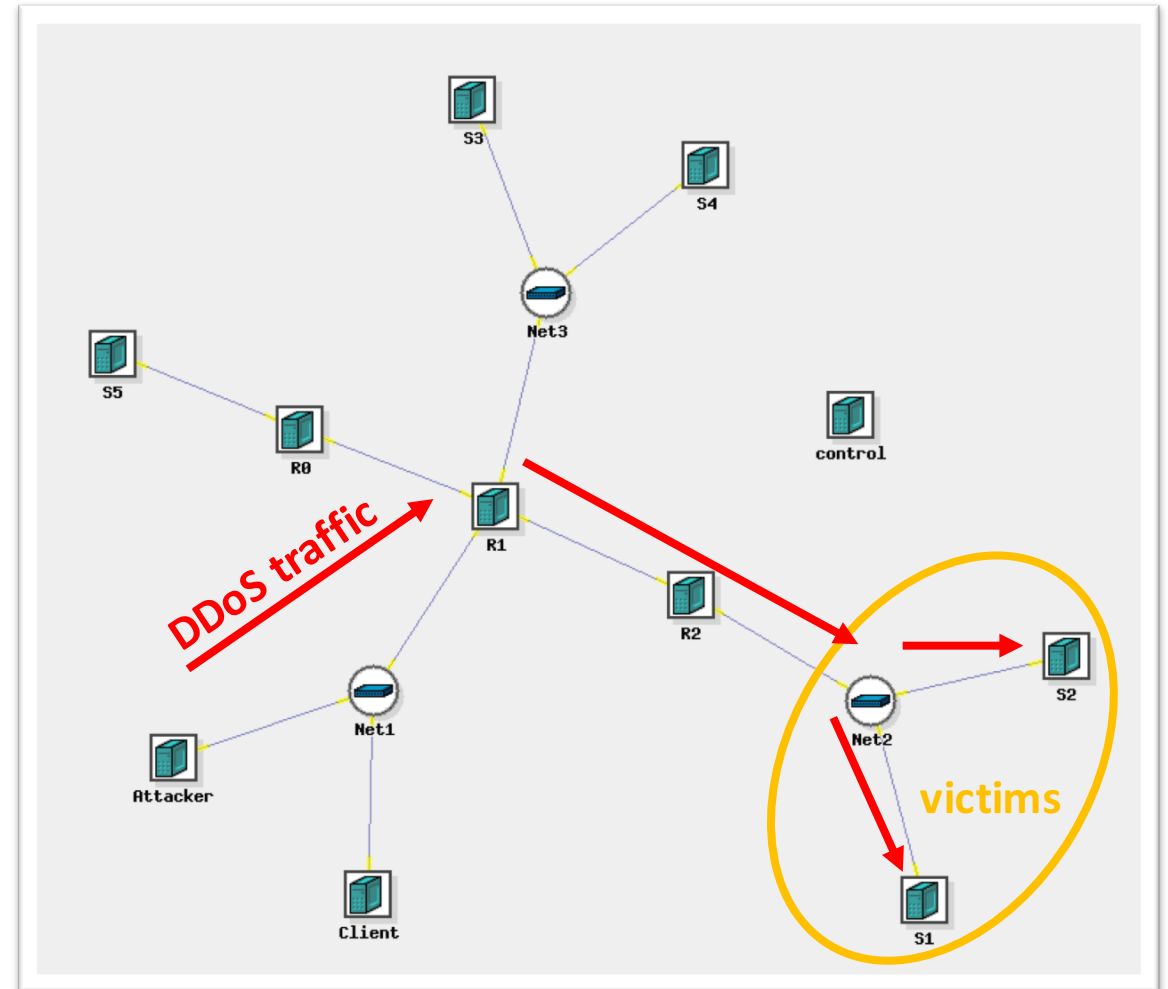
Example of Experiment

Objective : Generate network traffic environment with DDoS attack

Topology : Small network environment with 3 LAN.

Tools: HTTP Slowloris
Botnet generator (BoNeSi)
D-ITG

Packet capture : Wireshark

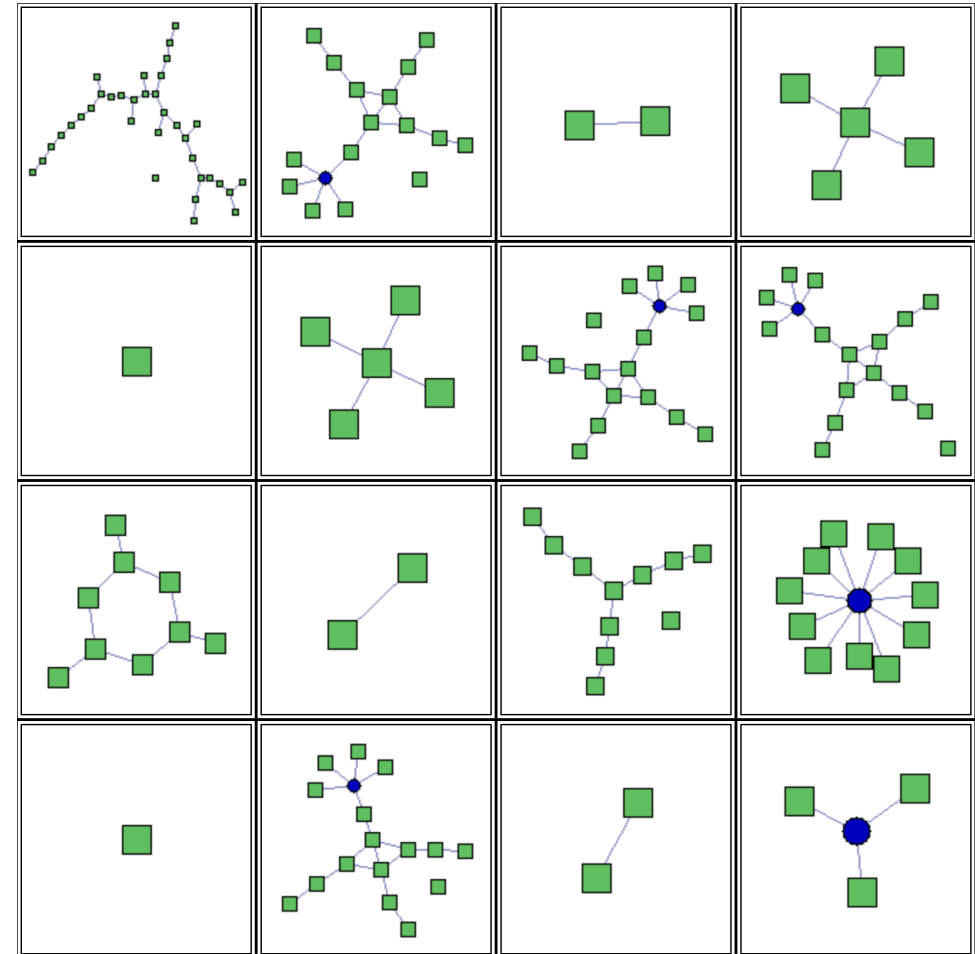


Topology created with Deterlab



What is good

- Scalable topologies
- Configurable bandwidth and delays for each network links
- Configurable routings
- Dedicated physical host for each node
- OS image selection
- Able to install tools



Overview

- Cyber Security
- What we do?
- > What we encounter?
- What we can improve



Challenges

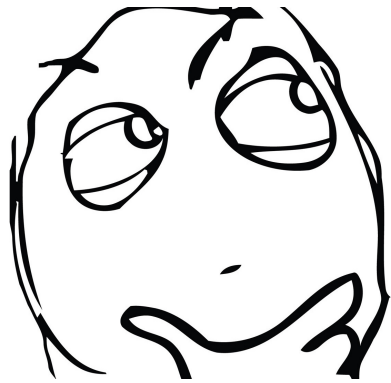
- Resources limitation
- Location / Time Difference
- Testbed architecture unfamiliarity
- Federated maintenance

Current Experiments	
42	<u>Active</u>
3	Idle
4780	<u>Swapped</u>
88	Free PCs

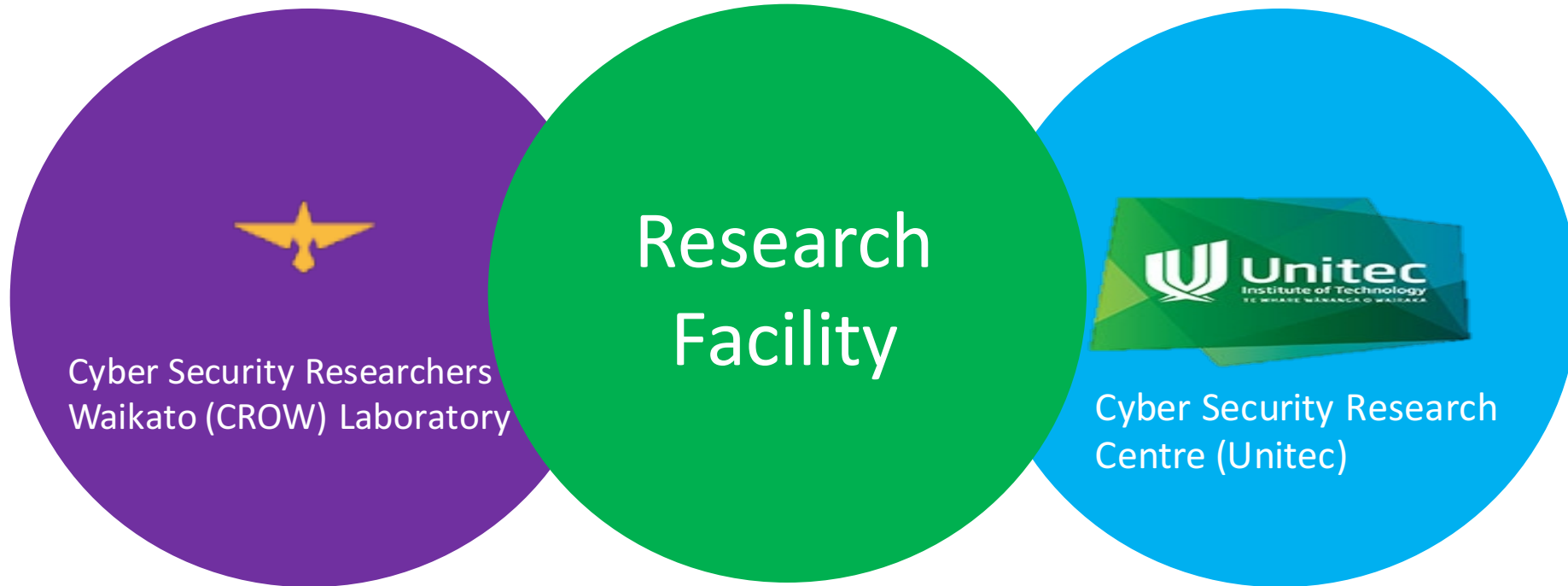
Overview

- Cyber Security
- What we do?
- What we encounter?
- > What we can improve

Would it be better if
we can have a similar
facility in NZ?



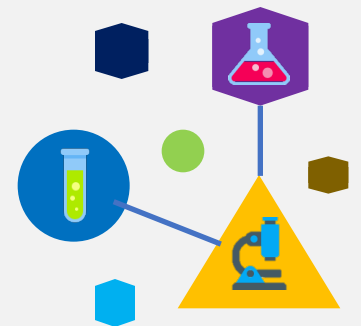
Current cyber security labs in NZ





Would it be better to have..

Questions?



Thank you.

--End--

