The Institute of Electronics, Communications and Information Technology

Metric Efficacy in WLAN Security

Jonny Milliken
PhD Student
2010

Presenter

Jonny Milliken

- PhD candidate at Queens University Belfast
- Supervised by Prof. Alan Marshall
- Digital Communications group (WLAN Security)
- Working on Cross Layer Intrusion Tolerant Networks

Key Points

Metric Efficacy in WLAN Security

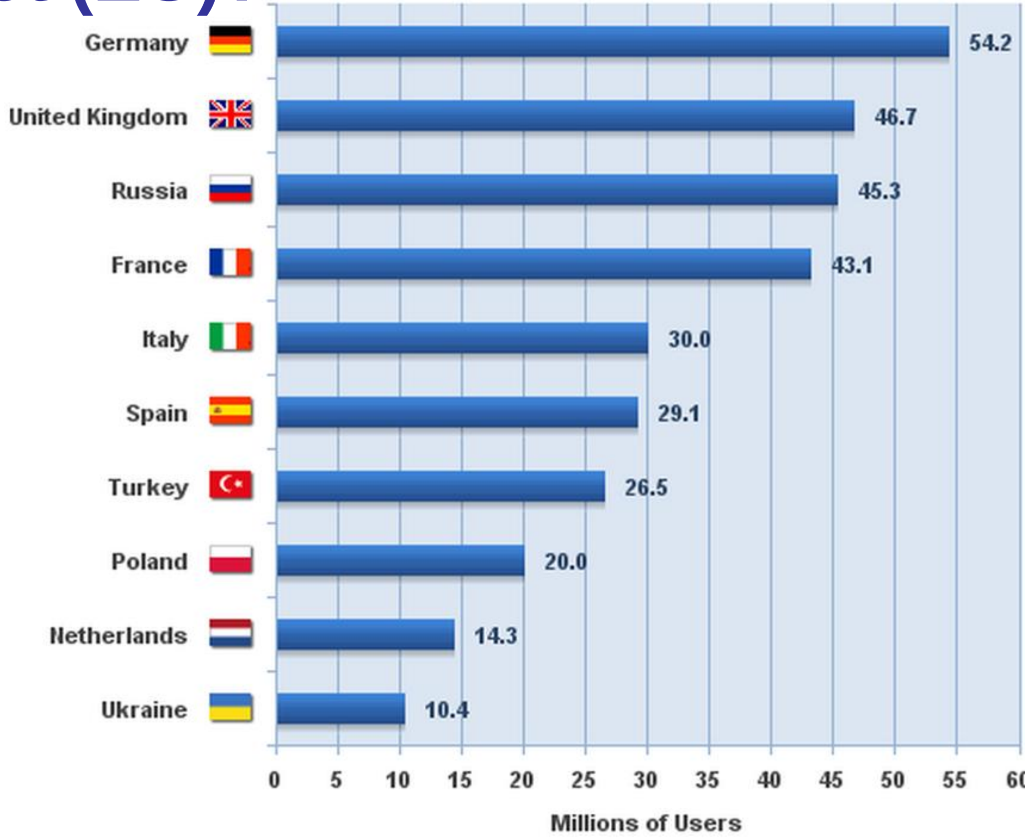
Key Points

Metric Efficacy in WLAN Security

- Metric selection is a key building block of WLAN security
- Current approaches to selecting attack metrics are sub-optimal
- A new approach which considers regenerative networks under threat from a knowledgeable attacker

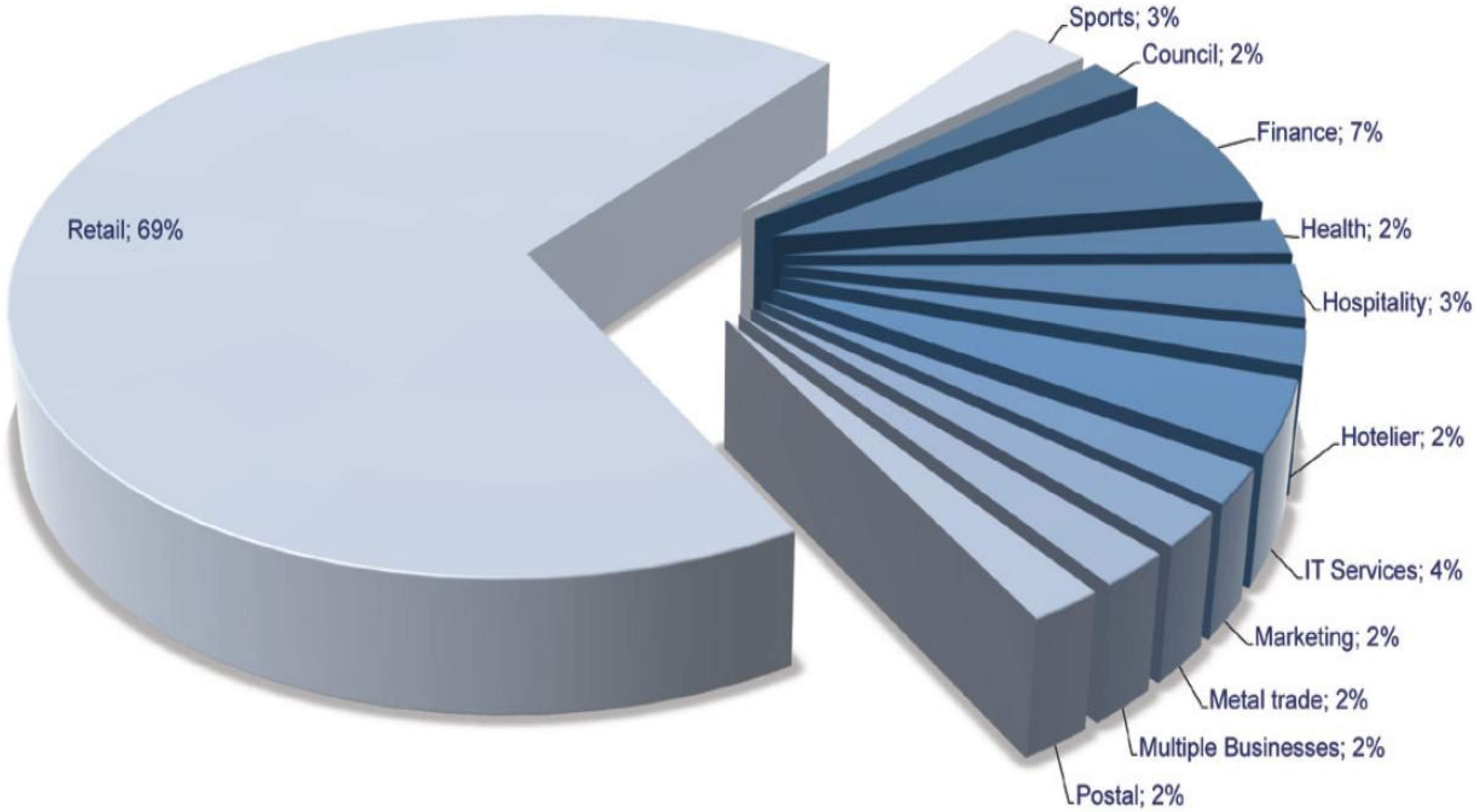
Internet Usage

In daily Life : How many people use the internet (EU)?



http://www.internetworldstats.com/stats.htm (Sept 2009)

Who is at threat?



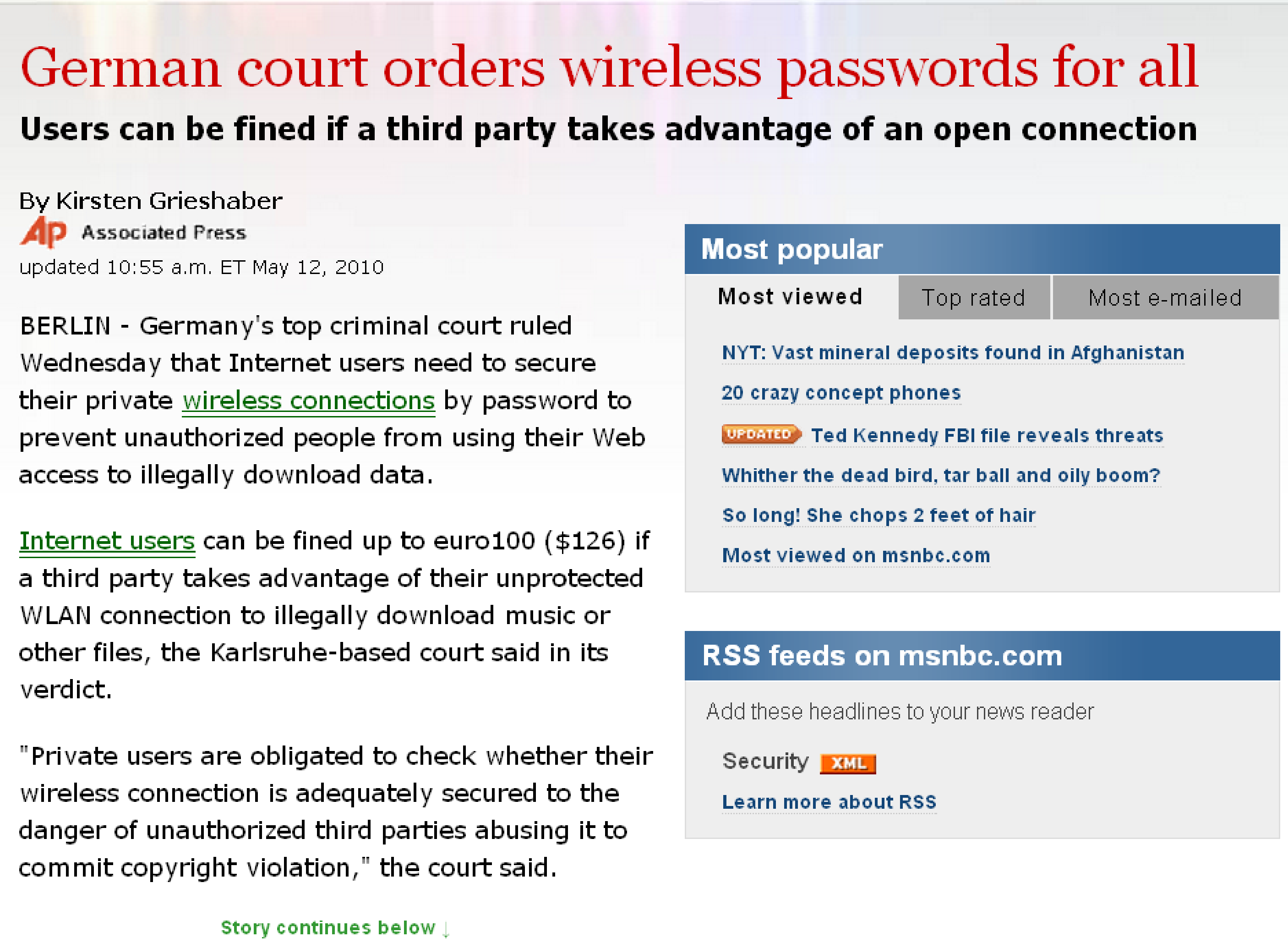
http://7safe.com/breach_report/Breach_report_2010.pdf (2010)

WLAN Security

Shown to be insecure in a number of ways

- **Poor encryption/password systems**
- **Unprotected management frames (DoS)**
- **MITM Attacks**

The Problem



German court orders wireless passwords for all

Users can be fined if a third party takes advantage of an open connection

By Kirsten Grieshaber
Associated Press
updated 10:55 a.m. ET May 12, 2010

BERLIN - Germany's top criminal court ruled Wednesday that Internet users need to secure their private wireless connections by password to prevent unauthorized people from using their Web access to illegally download data.

Internet users can be fined up to euro100 ($126) if a third party takes advantage of their unprotected WLAN connection to illegally download music or other files, the Karlsruhe-based court said in its verdict.

"Private users are obligated to check whether their wireless connection is adequately secured to the danger of unauthorized third parties abusing it to commit copyright violation," the court said.

Story continues below ↓

Most popular

Most viewed | Top rated | Most e-mailed

- NYT: Vast mineral deposits found in Afghanistan
- 20 crazy concept phones
- UPDATED Ted Kennedy FBI file reveals threats
- Whither the dead bird, tar ball and oily boom?
- So long! She chops 2 feet of hair
- Most viewed on msnbc.com

RSS feeds on msnbc.com

Add these headlines to your news reader

Security XML

Learn more about RSS

http://www.msnbc.msn.com/id/37107291/ns/technology_and_science-security (May 2010)

Protecting IT Systems

- Various imperfect methods of protection: Firewalls, Anti-Virus, Filters, Human vigilance...
- None of them help once an attacker gains access to the system.
- Intrusion Detection Systems (**IDS**) designed to mitigate this threat.

Commercial IDS

ARUBA® networks

AIRMAGNET®

MERU NETWORKS®
Powering the All-Wireless Enterprise™

MOTOROLA AIRDEFENSE

Open Source IDS

WLAN Metrics

Wait, what’s a metric?

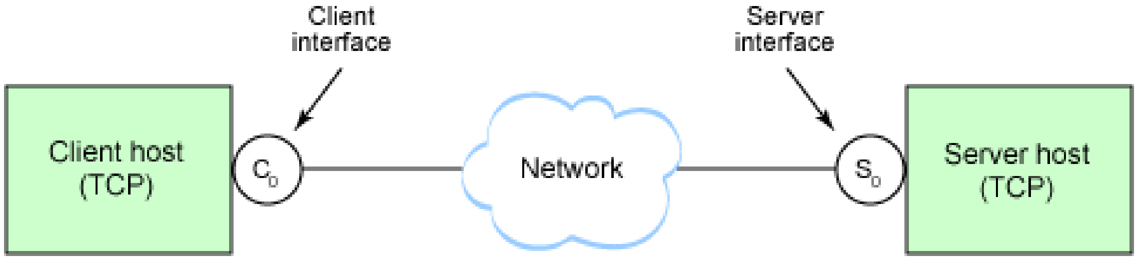
WLAN Metrics

Wait, what’s a metric?

- Unique and trackable
- Linked to a service within the network
- Changes with different network activity

Some examples

- TCP Connection attempts and drops



WLAN Metrics

Some examples

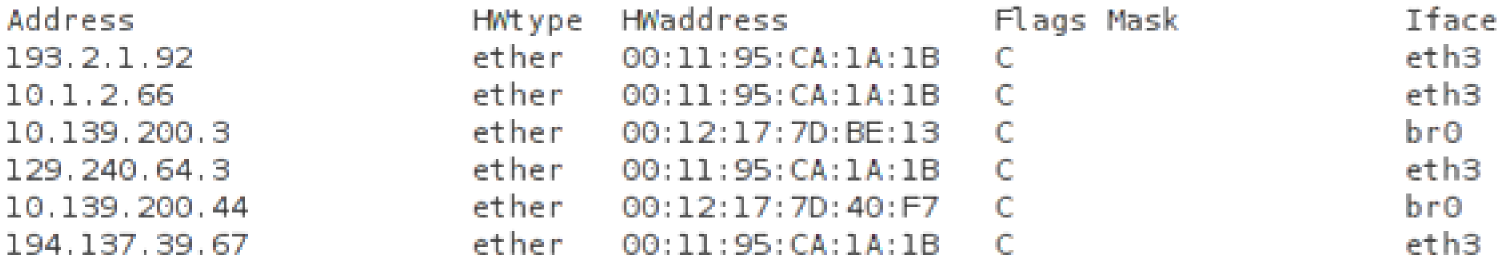
- TCP Connection attempts and drops
- Signal strength of beacons

ECIT

WLAN Metrics

Some examples

- TCP Connection attempts and drops
- Signal strength of beacons
- ARP Table updates



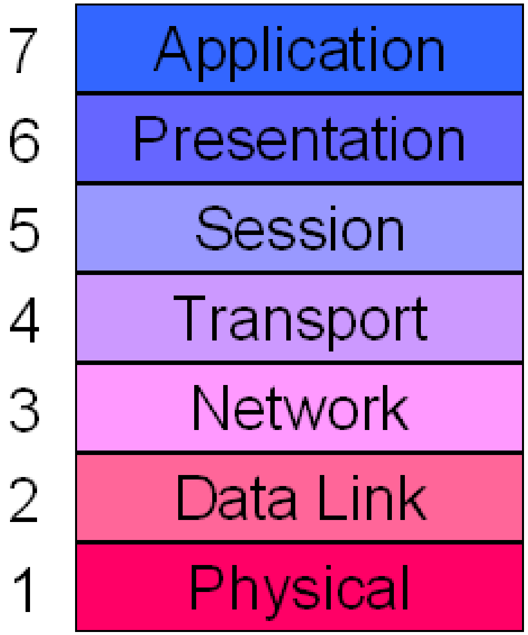
```
Address                  HWtype  HWaddress           Flags Mask            Iface
193.2.1.92               ether   00:11:95:CA:1A:1B   C                     eth3
10.1.2.66                ether   00:11:95:CA:1A:1B   C                     eth3
10.139.200.3             ether   00:12:17:7D:BE:13   C                     br0
129.240.64.3             ether   00:11:95:CA:1A:1B   C                     eth3
10.139.200.44            ether   00:12:17:7D:40:F7   C                     br0
194.137.39.67            ether   00:11:95:CA:1A:1B   C                     eth3
```

WLAN Metrics

Some examples

- TCP Connection attempts and drops
- Signal strength of beacons
- ARP Table updates

Cross Layer!



7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

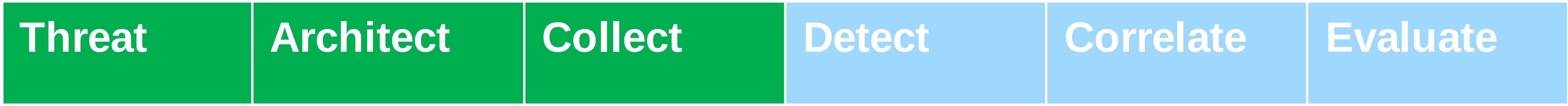
OSI Reference Model

ECIT

WLAN Metrics

Relevance for IDS

- Metric selection is an early foundation
- Supports detection performance very heavily


Threat
Architect
Collect
Detect
Correlate
Evaluate

Metric Selection

Metric Selection

- Choose metrics based on:

  1) Most effective metrics for each attack

  2) How good they are at reliably detecting attacks

ECIT

Metric Selection

Most effective metrics (DoS):

(Hussein et al, 03)*	# Connections to destination
(Lu & Traore, 05)*	Traffic in / Traffic out
(Qu, 04)*	Deviation in SYN rate
(Kabiri, 09)*	Various TCP Flags

*See references slide at end of presentation for paper details

Metric Selection

Success Rate (DoS):

(Hussein et al, 03)	35% FPR
(Lu & Traore, 05)	Unknown
(Qu, 04)	Detected attack
(Kabiri, 09)	98%

Metric Selection

Success Rate (DoS):

(Hussein et al, 03)	35% FPR (Observation – no rate)
(Lu & Traore, 05)	Unknown
(Qu, 04)	Detected attack
(Kabiri, 09)	98%

Metric Selection

Success Rate (DoS):

(Hussein et al, 03)	35% FPR (Observation – no rate)
(Lu & Traore, 05)	Unknown (Observation – no rate)
(Qu, 04)	Detected attack
(Kabiri, 09)	98%

Metric Selection

Success Rate (DoS):

(Hussein et al, 03)	35% FPR (Observation – no rate)
(Lu & Traore, 05)	Unknown (Observation – no rate)
(Qu, 04)	Detected attack (Lab – delta normal)
(Kabiri, 09)	98%

Metric Selection

Success Rate (DoS):

(Hussein et al, 03)	35% FPR (Observation – no rate)
(Lu & Traore, 05)	Unknown (Observation – no rate)
(Qu, 04)	Detected attack (Lab – delta normal)
(Kabiri, 09)	98% (Feature Extraction – no rate)

Metric Selection

Success Rate (DoS):

(Hussein et al, 03)	35% FPR (Observation – no rate)
(Lu & Traore, 05)	Unknown (Observation – no rate)
(Qu, 04)	Detected attack (Lab – delta normal)
(Kabiri, 09)	98% (Feature Extraction – no rate)

Metric Selection

Selection issues

- **Exact metrics are ill defined** (# connections, traffic in / out, etc.)
- **Success rate not identified** (On DARPA dataset, for single attack or on single network)
- **Different approaches** (Observation, lab testing and feature extraction)

PhD Approach

Addressing these issues

- **Exact metrics are ill defined**
- Assess for specific attacks the most effective cross layer metrics

- **Success rate not identified**

- **Different approaches**

ECIT

PhD Approach

Addressing these issues

- **Exact metrics are ill defined**
- Assess for specific attacks the most effective cross layer metrics

- **Success rate not identified**
- Metric performance under threat from knowledgeable attacker

- **Different approaches**

ECIT |

PhD Approach

Addressing these issues

- **Exact metrics are ill defined**
- Assess for specific attacks the most effective cross layer metrics

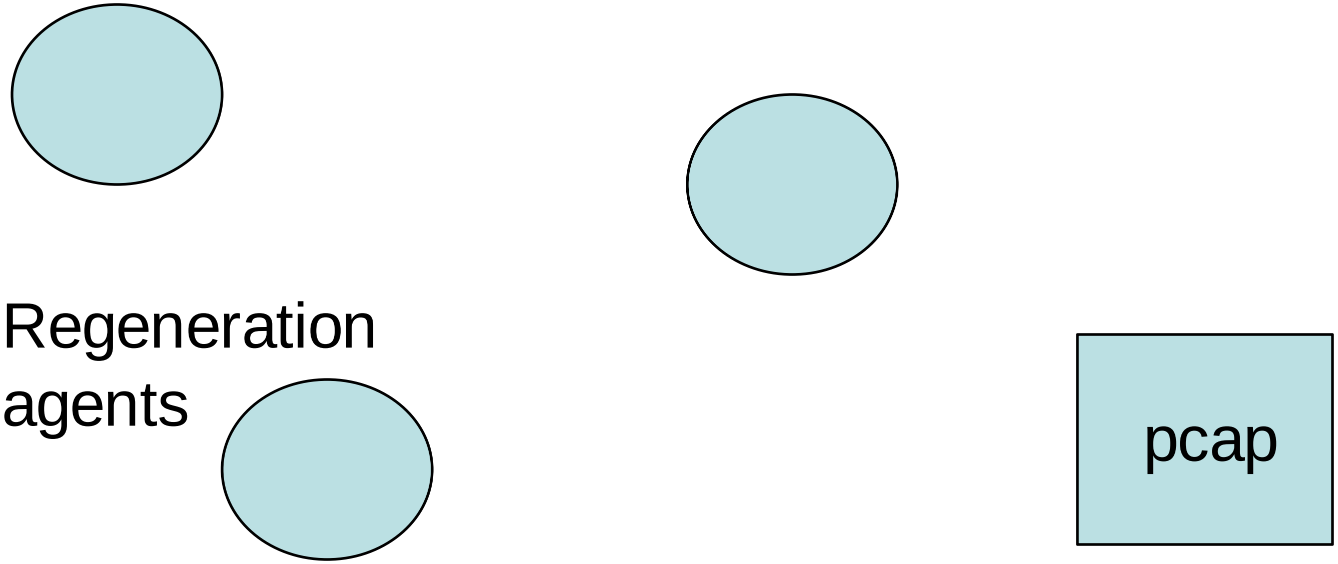
- **Success rate not identified**
- Metric performance under threat from knowledgeable attacker

- **Different approaches**
- Live network replays of multiple network types

PhD Approach

Currently

- **Different approaches**
- Live network replays of multiple network types



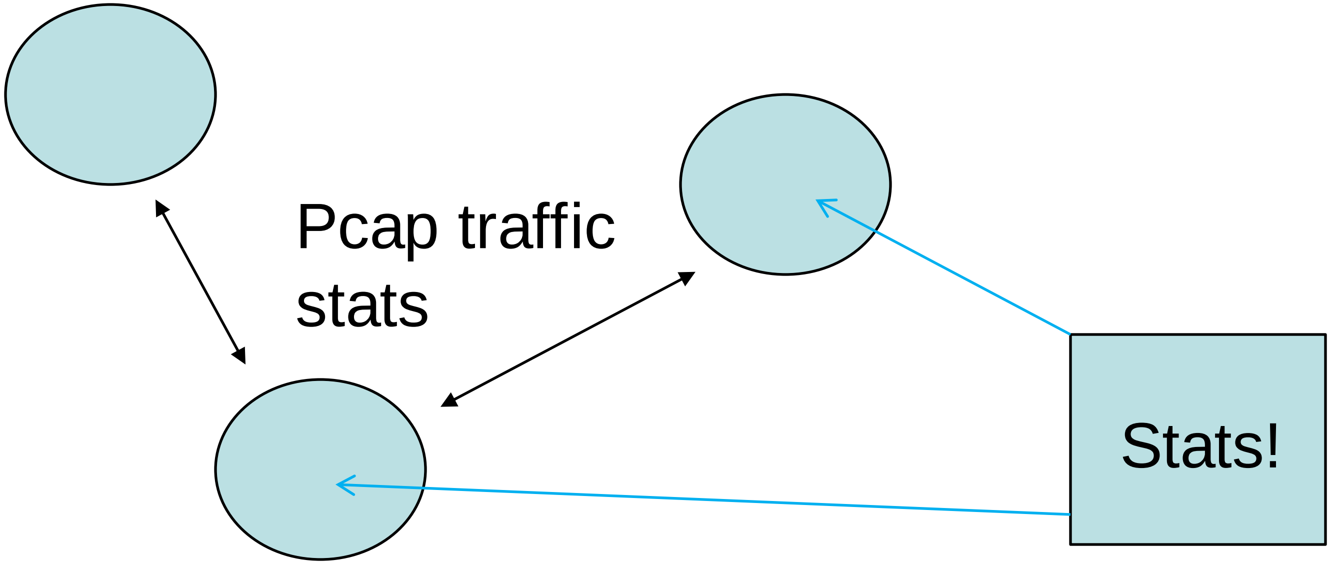
Regeneration agents

pcap

PhD Approach

Currently

- **Different approaches**
- Live network replays of multiple network types



Pcap traffic stats

Stats!

ECIT

PhD Approach

Currently

- **Different approaches**
- Live network replays of multiple network types

- Statistically represent multiple networks

- Organically regenerate these traffic statistics on testbed agents

- Metrics and network stats regress to the mean

Key Points

Metric Efficacy in WLAN Security

- Metric selection is a key building block of WLAN security
- Current approaches to selecting attack metrics are sub-optimal
- A new approach which considers regenerative networks under threat from a knowledgeable attacker

Questions

References

Metric Selection papers:

(Hussein, A; et al, 03) - A Framework for Classifying Denial of Service Attacks (SIGCOMM 03)

(Lu, W & Traore, I, 05) - An unsupervised approach for detecting DDOS attacks based on Traffic Based Metrics (Communications, Computers and signal Processing, 2005)

(Qu, G; et al, 04) - Abnormality Metrics to Detect and Protect against Network Attacks (International Conference on Pervasive Services)

(Kabiri, P & Zargar, R, 09) - Category-Based Selection of Effective Parameters for Intrusion Detection (IJCSNS Vol 9 No. 9)