

Beholder

Nelson Murilo
nelson(at)pangeia.com.br

beholder



Agenda

Who am I

Motivation

Introduction

tool structure

What does beholder detectet?

What beholder does'nt do

Scenarios

Demo

Motivation



e



beholder

9/8/2008 14:53

BEACONS

802.11 Beacons

Beacons can hidden some important stuff

IME FATIMA	
PREZIME AYISHA KHOMEINI	
DATUM I MJESTO RODENJA 02.12.1972. KIRKUK, IRAK	
JMBG 0212972335009	
PREBIVALIŠTE ZAGREB DUBRAVA 27	
PU ZAGREBAČKA DOZVOLU IZDAO U	
POTPIS 07.12.1975. DANA	
06.12.2035. VRIJEDI DO	
0309123 BROJ	
POTPIS VOZACA <i>Fatima Ayisha Khomeini</i>	

KATEGORIJE VOZILA ZA KOJE VRIJEDI DOZVOLA:

A	Motocikli datum polaganja	M.P.
B	Vozila, osim vozila kategorije A, čija najveća dopuštena masa nije veća od 3.500 kg i koja nemaju više od osam sjedala, ne računajući sjedalo za vozača. 11.04.1991. datum polaganja	
C	Vozila za prijevoz tereta čija je najveća dopuštena masa veća od 3.500 kg. datum polaganja	M.P.
D	Vozila za prijevoz osobe, koja, osim sjedala za vozača, imaju više od osam sjedala. datum polaganja	M.P.
E	Skupovi vozila čija vučna vozila spadaju u kategoriju B, C ili D, a priključna su vozila najveće dopustene mase veće od 750 kg. datum polaganja	M.P.

beholder

Cisco Proprietary	
Element ID:	133
Length:	30
OUI:	00-00-00
Value:	0x00000000
AP Name:	AP11-11
Number of clients:	3
Value:	0x00000025
Vendor Specific	
Element ID:	221 Vendor Specific - Cisco
Length:	6
OUI:	00-40-96
Data:	(3 bytes)
Vendor Specific	
Element ID:	221 Vendor Specific - Cisco
Length:	5
OUI:	00-40-96
Version:	3
CCX Version:	3
Vendor Specific	
Element ID:	221 Vendor Specific - Cisco
Length:	22
OUI:	00-40-96
Data:	(19 bytes)
WMM	
Element ID:	221 WMM
Length:	24
OUI:	00-50-F2

Number of connected clients

Hidden ESSID

File Edit Settings Help

scan
 channel 6

Network device ath0 Refresh
Driver type Other

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
	00:07:40:4D:1A:5C	Homenet54		Fri Apr 21 20:23:39 2006	00:00:00	3	542	0	0	0		
	00:09:5B:66:3D:0E	NETGEAR	Y	Fri Apr 21 20:23:23 2006	00:00:00	11	2	0	0	0		

Enable bridging to wired LAN
 Enable SSID broadcast



Apply Cancel

File Edit Settings

scan
 channel 6

Network device ath0 Refresh
Driver type Other

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
	00:07:40:4D:1A:5C	Homenet54		Fri Apr 21 20:14:18 2006	00:00:00	3	266	0	0	0		
	00:09:5B:66:3D:0E	Y	Fri Apr 21 20:13:58 2006	00:00:00	11	1	0	0	0		

beholder



Hidden ESSID

23:05:16.386193 **Beacon** () [1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit] ESS CH: 11

23:05:16.488612 **Beacon** () [1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit] ESS CH: 11

23:05:17.321039 **Beacon (Homenet54)** [1.0 2.0 5.5 11.0 Mbit] ESS CH: 3

23:05:17.629271 **Beacon (Homenet54)** [1.0 2.0 5.5 11.0 Mbit] ESS CH: 3

Features

Beholder facts

Written in C Ansi and based on IWLIST (Linux wireless tools)

Just not another network scanner

Changes on AP (ESSID, MAC, Mode)

Channel and encryption proto changes

Meaningful signal level variations

Syslog support to large networks (many sensors)

Features



beholder

Karma



beholder

Karma

KARMA includes patches for the Linux MADWifi driver to allow the creation of an 802.11 Access Point that responds to any probed SSID. So if a client looks for 'linksys', it is 'linksys' to them (even while it may be 'tmobile' to someone else). Operating in this fashion has revealed vulnerabilities in how Windows XP and MacOS X look for networks, so clients may join even if their preferred networks list is empty.

DHCP Offer

POP3/FTP password sniffing

Redirect HTTP traffic to malicious server

Karma with steroids

KARMA + MetaSploit3 + Aircrack-ng == KarmaSploit

Karma re-burn

MadWifi patch changed by Aircrack-ng tools

Easy to write new xploits

New power with DNS D. Kaminsky vulnerability

New xploits are immediately available to add in Metasploit.

RegEx

Regular Expression

```
/h[a4@]([c<]([k]|\<)))([k]|\<)(x)\s+\n((d)|([t\+]h))[3ea4@]\s+p[1][a4@]n[3e][t\+]/i
```




What beholder **doesn't** do

Put interface in promisc mode

Put interface in monitor mode

WPA/WEP stuff

Access Point or client weakness

Availablely

For while...



beholder



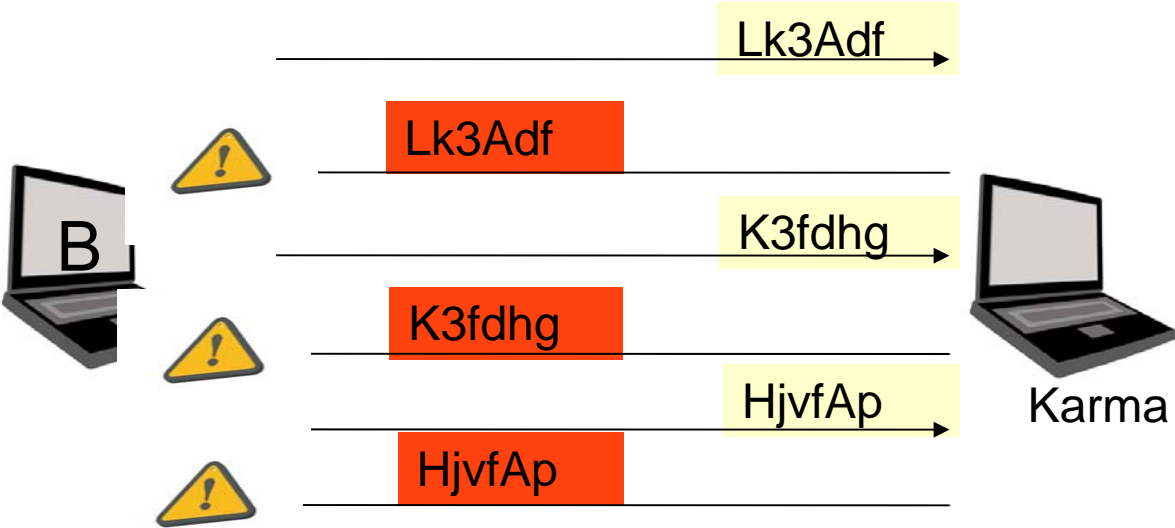
Future?



beholder



Karma deteccion



Scenarios

Alert for missing APs(Regex)

```
beholder -m "mynets" wifidev
```



Default

beholder

Scenarios

checking for similar essids via RegEX

```
beholder -r "myne[t7]s.*" wifidev
```



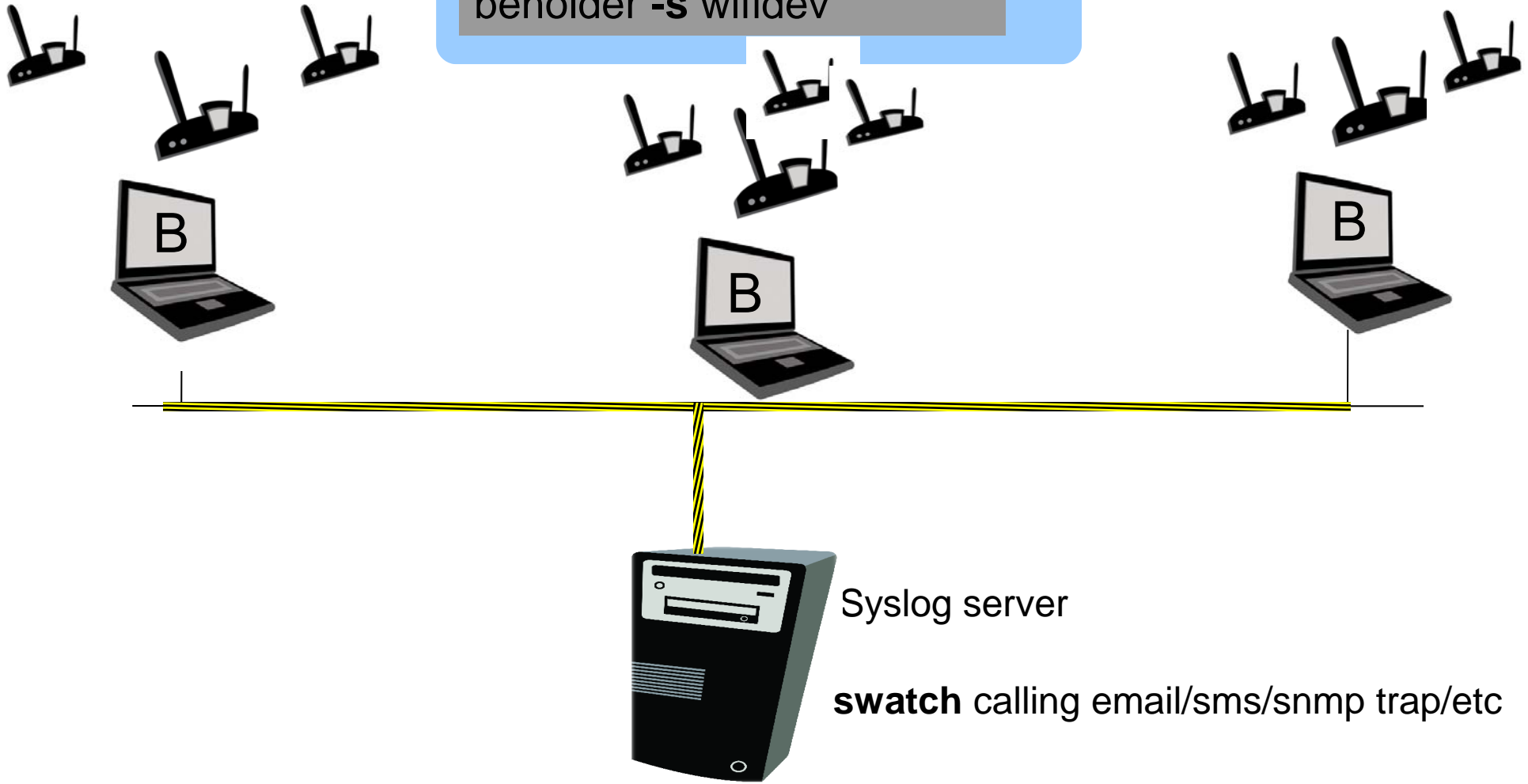
mynets



Scenarios

Large environments

`beholder -s wifidev`

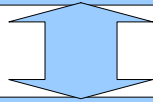


beholder

Let me see the code

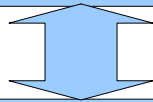
BEHOLDER Code

Detect, Regex, Etc.



IWLIST Code

Beacons, WiFi interface



Hardware

Let me see the code

Structure

Initial scanning

Loop infinite

Jamming detection

AP/AD-Doc detection

Anommalies detection

Changes on Mac, Channel, mode, etc.

Similar names (essid) detection

Missing APs detection

Random requests (karma detecion)

Look for karma responses

Let me see the code

REGEX implementation:

Two functions

Compile:

```
int regcomp(regex_t *preg, const char *regex, int cflags);
```

Compare:

```
int regexec(regex_t *preg, const char *strings, size_t nmatch,,  
regmatch_t pmatch[], int eflags);
```

Let me see the code

Karma detection

```
char *karma_trap(int skfd, const char *dev){
    struct iwreq wrq;
    [...]
    char essid[KARMA_TRAP_LEN] = "XXXXXX";
    [...]
    // Create a random ESSID
    mktemp(essid);
    wrq.u.essid.pointer = (caddr_t) essid;
    [...]
    // Set random ESSID
    if(iw_set_ext(skfd, dev, SIOCSIWESSID, &wrq) < 0)
    [...]
    // Get random ESSID
    if(iw_get_ext(skfd, dev, SIOCSIWESSID, &wrq) < 0)
```

Let me see the code

Jamming detection

```
while (ap_temp)
{
    if (!wscan_init) /* AP table empty */
    {
        jam++;

        if (jam == 3) // if table empty after 3 seq scanning
        {
            print_out(slog, "ALERT: Danger, Will Robinson!
Jamming device detected\n");
            break;
        }
    }
}
```

beholder



Demo?

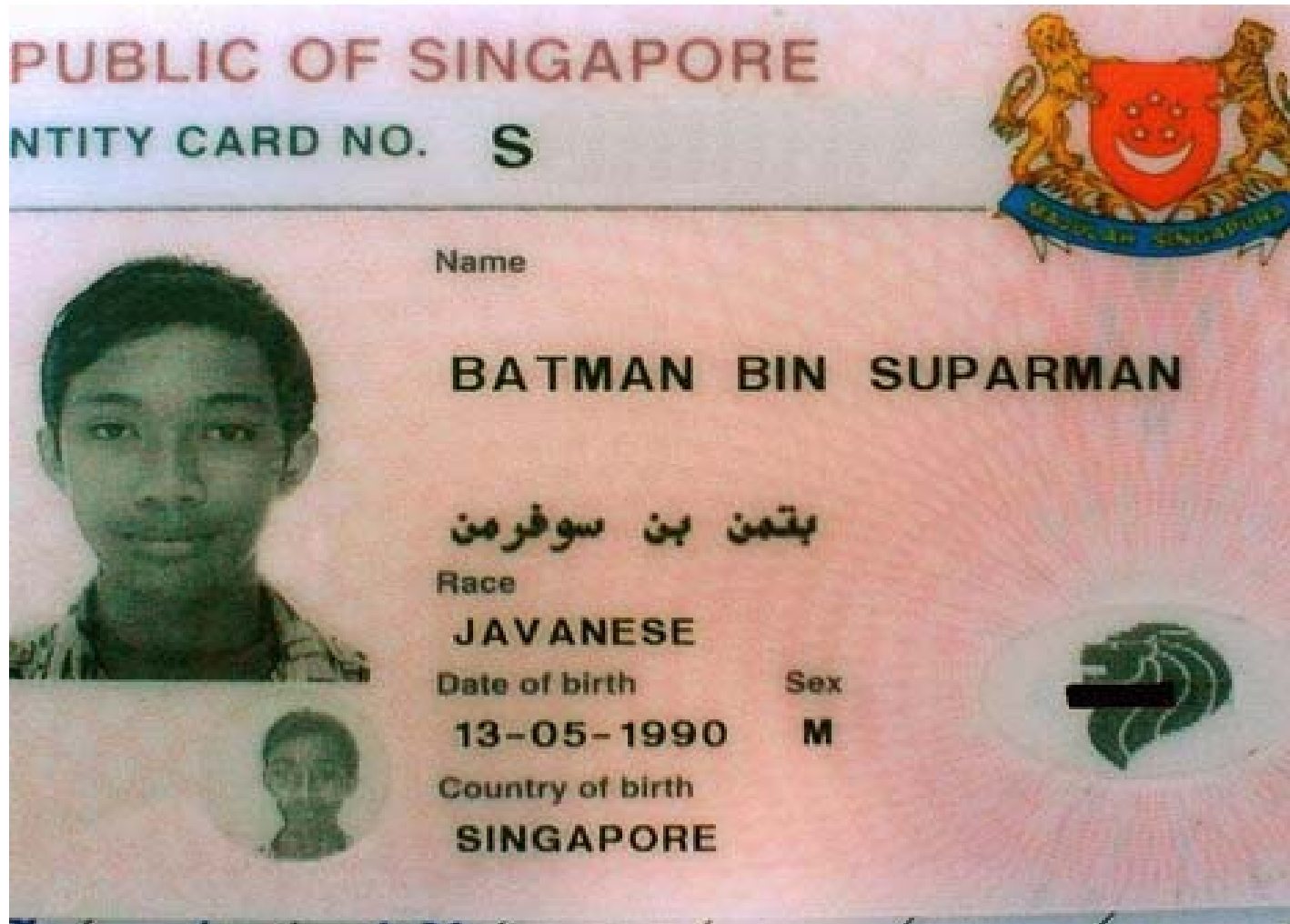


beholder



Remember:

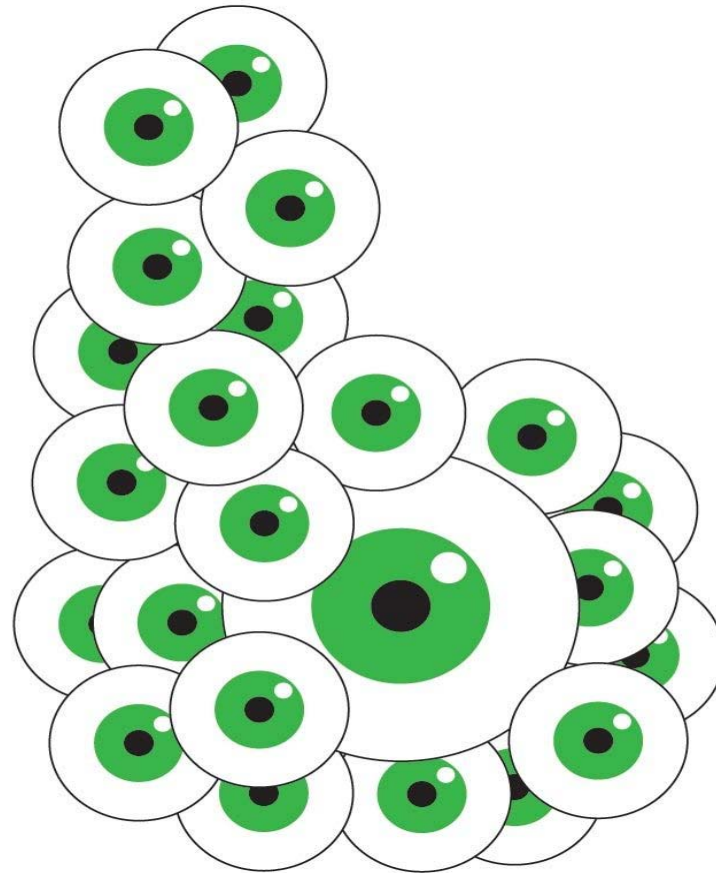
Help sometimes don't is where you hope



beholder



Pick one free



<http://www.beholderwireless.org>



beholder

