Enabling the IoT:
A WLAN Security Wakeup Call

A CELLSTREAM INC. PRESENTATION TO ILLINOIS TELECOM ASSOCIATION 2019 VENDOR SHOWCASE
VERSION 0.4

Author Biography and Details

Author: Andrew Walding

Biography of the Author

Mr. Walding is President of CellStream Inc., a global computing and telecommunications consulting group based inTexas. He holds multiple patents in telecommunications and has been in the industry since 1978. Additionally, Mr. Walding is an industry leading consultant, lecturer, author, instructor and course developer focusing on optical, packet switching, routing, and control protocols.

CellStream Inc. provides a diverse range of consulting services, serving the computing and telecommunications service providers and equipment manufacturers. CellStream has always been focused on emerging key technologies, enabling its clients to master new concepts in products and offerings with minimized lead times. CellStream consultants bring hundreds of years of front-line experience across a wide range of technologies and responsibilities. CellStream offers requirements/architecture definition, design support, RFP creation and response support, sales force enlightenment, solutions brainstorming, white paper and collateral creation/review services and much more.

Author contact information:

Email: andyw@cellstream.com

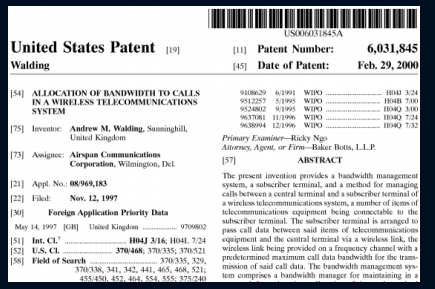
Web Sites:

CellStream Inc.: www.cellstream.com

Online School: www.netscionline.com

Tel: +1 866-659-1014

Fax: +1 866-659-1014



US006031845A

United States Patent [19]

Walding

[11] Patent Number: 6,031,845

[45] Date of Patent: Feb. 29, 2000

[54] ALLOCATION OF BANDWIDTH TO CALLS IN A WIRELESS TELECOMMUNICATIONS SYSTEM

[75] Inventor: Andrew M. Walding, Sunninghill, United Kingdom

[73] Assignee: Airspan Communications Corporation, Wilmington, Del.

[21] Appl. No.: 08/969,183

[22] Filed: Nov. 12, 1997

[30] Foreign Application Priority Data

May 14, 1997 [GB] United Kingdom 9709802

[51] Int. Cl.[7] H04J 3/16; H04L 7/24

[52] U.S. Cl. 370/468; 370/335; 370/521

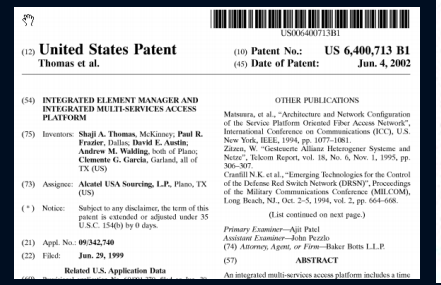
[58] Field of Search 370/335, 329, 370/338, 341, 342, 441, 465, 468, 521; 455/450, 452, 464, 554, 555; 375/240

9108629 6/1991 WIPO H04J 3/24
9512257 5/1995 WIPO H04B 7/00
9524802 9/1995 WIPO H04Q 3/00
9637081 11/1996 WIPO H04Q 7/24
9638994 12/1996 WIPO H04Q 7/32

Primary Examiner—Ricky Ngo
Attorney, Agent, or Firm—Baker Botts, L.L.P.

[57] ABSTRACT

The present invention provides a bandwidth management system, a subscriber terminal, and a method for managing calls between a central terminal and a subscriber terminal of a wireless telecommunications system, a number of items of telecommunications equipment being connectable to the subscriber terminal. The subscriber terminal is arranged to pass call data between said items of telecommunications equipment and the central terminal via a wireless link, the wireless link being provided on a frequency channel with a predetermined maximum call data bandwidth for the transmission of said call data. The bandwidth management system comprises a bandwidth manager for maintaining in a



US006400712B1

(12) United States Patent
Thomas et al.

(10) Patent No.: US 6,400,713 B1

(45) Date of Patent: Jun. 4, 2002

(54) INTEGRATED ELEMENT MANAGER AND INTEGRATED MULTI-SERVICES ACCESS PLATFORM

(75) Inventors: Shoji A. Thomas, McKinney; Paul R. Frazier, Dallas; David E. Austin; Andrew M. Walding, both of Plano; Clemente G. Garcia, Garland, all of TX (US)

(73) Assignee: Alcatel USA Sourcing, L.P., Plano, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/342,740

(22) Filed: Jun. 29, 1999

Related U.S. Application Data

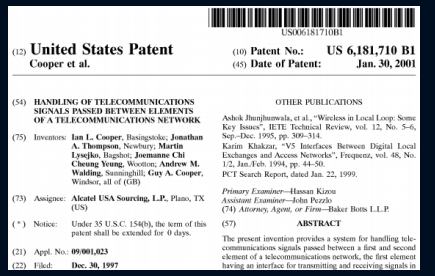
OTHER PUBLICATIONS

Matsuura, et al., "Architecture and Network Configuration of the Service Platform Oriented Fiber Access Network", International Conference on Communications (ICC), U.S. New York, IEEE, 1994, pp. 1077–1081.
Zitzen, W. "Gesteuerte Allianz Heterogener Systeme and Netze", Telcom Report, vol. 18, No. 6, Nov. 1, 1995, pp. 306–307.
Cranfill N.K. et al., "Emerging Technologies for the Control of the Defense Red Switch Network (DRSN)", Proceedings of the Military Communications Conference (MILCOM), Long Beach, NJ., Oct. 2-5, 1994, vol. 2, pp. 664–668.
(List continued on next page.)

Primary Examiner—Ajit Patel
Assistant Examiner—John Pezzlo
(74) Attorney, Agent, or Firm—Baker Botts L.L.P.

(57) ABSTRACT

An integrated multi-services access platform includes a time



US006181710B1

(12) United States Patent
Cooper et al.

(10) Patent No.: US 6,181,710 B1

(45) Date of Patent: Jan. 30, 2001

(54) HANDLING OF TELECOMMUNICATIONS SIGNALS PASSED BETWEEN ELEMENTS OF A TELECOMMUNICATIONS NETWORK

(75) Inventors: Ian L. Cooper, Basingstoke; Jonathan A. Thompson, Newbury; Martin Lysejko, Bagshot; Joemanne Chi Cheung Yeung, Weeton; Andrew M. Walding, Sunninghill; Guy A. Cooper, Windsor, all of (GB)

(73) Assignee: Alcatel USA Sourcing, L.P., Plano, TX (US)

(*) Notice: Under 35 U.S.C. 154(b), the term of this patent shall be extended for 0 days.

(21) Appl. No.: 09/001,023

(22) Filed: Dec. 30, 1997

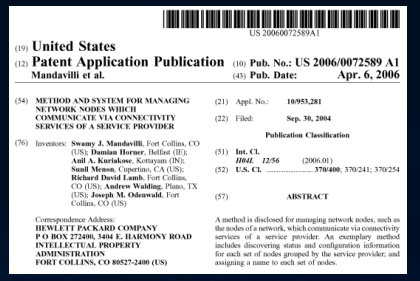
OTHER PUBLICATIONS

Ashok Jhunjhunwala, et al., "Wireless in Local Loop: Some Key Issues", IETE Technical Review, vol. 12, No. 5–6, Sep–Dec. 1995, pp. 309–314.
Karim Khakzar, "V5 Interfaces Between Digital Local Exchanges and Access Networks", Frequenz, vol. 48, No. 1/2, Jan.-Feb. 1994, pp. 44–50.
PCT Search Report, dated Jan. 22, 1999.

Primary Examiner—Hassan Kizou
Assistant Examiner—John Pezzlo
(74) Attorney, Agent, or Firm—Baker Botts L.L.P.

(57) ABSTRACT

The present invention provides a system for handling telecommunications signals passed between a first and second element of a telecommunications network, the first element having an interface for transmitting and receiving signals in



US 20060072589A1

(19) United States

(12) Patent Application Publication
Mandavilli et al.

(10) Pub. No.: US 2006/0072589 A1

(43) Pub. Date: Apr. 6, 2006

(54) METHOD AND SYSTEM FOR MANAGING NETWORK NODES WHICH COMMUNICATE VIA CONNECTIVITY SERVICES OF A SERVICE PROVIDER

(76) Inventors: Swamy J. Mandavilli, Fort Collins, CO (US); Damian Horner, Belfast (IE); Anil A. Kuriakose, Kottayam (IN); Sunil Menon, Cupertino, CA (US); Richard David Lamb, Fort Collins, CO (US); Andrew Walding, Plano, TX (US); Joseph M. Odenwald, Fort Collins, CO (US)

Correspondence Address:
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400 (US)

(21) Appl. No.: 10/953,281

(22) Filed: Sep. 30, 2004

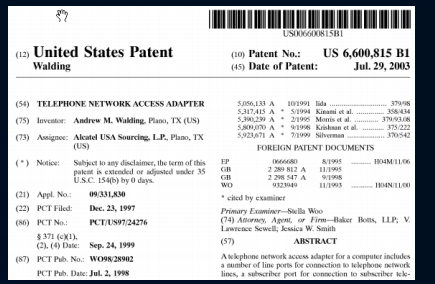
Publication Classification

(51) Int. Cl.
H04L 12/56 (2006.01)

(52) U.S. Cl. 370/400; 370/241; 370/254

(57) ABSTRACT

A method is disclosed for managing network nodes, such as the nodes of a network, which communicate via connectivity services of a service provider. An exemplary method includes discovering status and configuration information for each set of nodes grouped by the service provider; and assigning a name to each set of nodes.



US006600815B1

(12) United States Patent
Walding

(10) Patent No.: US 6,600,815 B1

(45) Date of Patent: Jul. 29, 2003

(54) TELEPHONE NETWORK ACCESS ADAPTER

(75) Inventor: Andrew M. Walding, Plano, TX (US)

(73) Assignee: Alcatel USA Sourcing, L.P., Plano, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/331,830

(22) PCT Filed: Dec. 23, 1997

(86) PCT No.: PCT/US97/24276

§ 371 (c)(1),
(2), (4) Date: Sep. 24, 1999

(87) PCT Pub. No.: WO98/28902

PCT Pub. Date: Jul. 2, 1998

5,056,133 A 10/1991 Iida 379/98
5,317,415 A * 5/1994 Kitami et al. 358/434
5,390,239 A * 2/1995 Morris et al. 379/93.08
5,809,070 A * 9/1998 Krishnan et al. 375/222
5,923,671 A * 7/1999 Silverman 370/542

FOREIGN PATENT DOCUMENTS

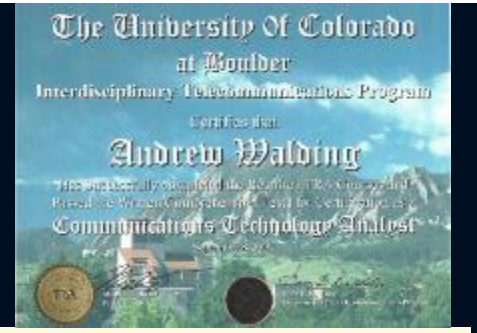
EP 0666680 8/1995 ..... H04M/11/06
GB 2 289 812 A 11/1995
GB 2 298 547 A 9/1998
WO 9323949 11/1993 ..... H04N/11/00

* cited by examiner

Primary Examiner—Stella Woo
(74) Attorney, Agent, or Firm—Baker Botts, L.L.P.; V. Lawrence Sewell; Jessica W. Smith

(57) ABSTRACT

A telephone network access adapter for a computer includes a number of line ports for connection to telephone network lines, a subscriber port for connection to subscriber tele-



Question: How do the IoT devices connect to the local network?

Answer: Wireless / Wi-Fi

Decisions, Decisions

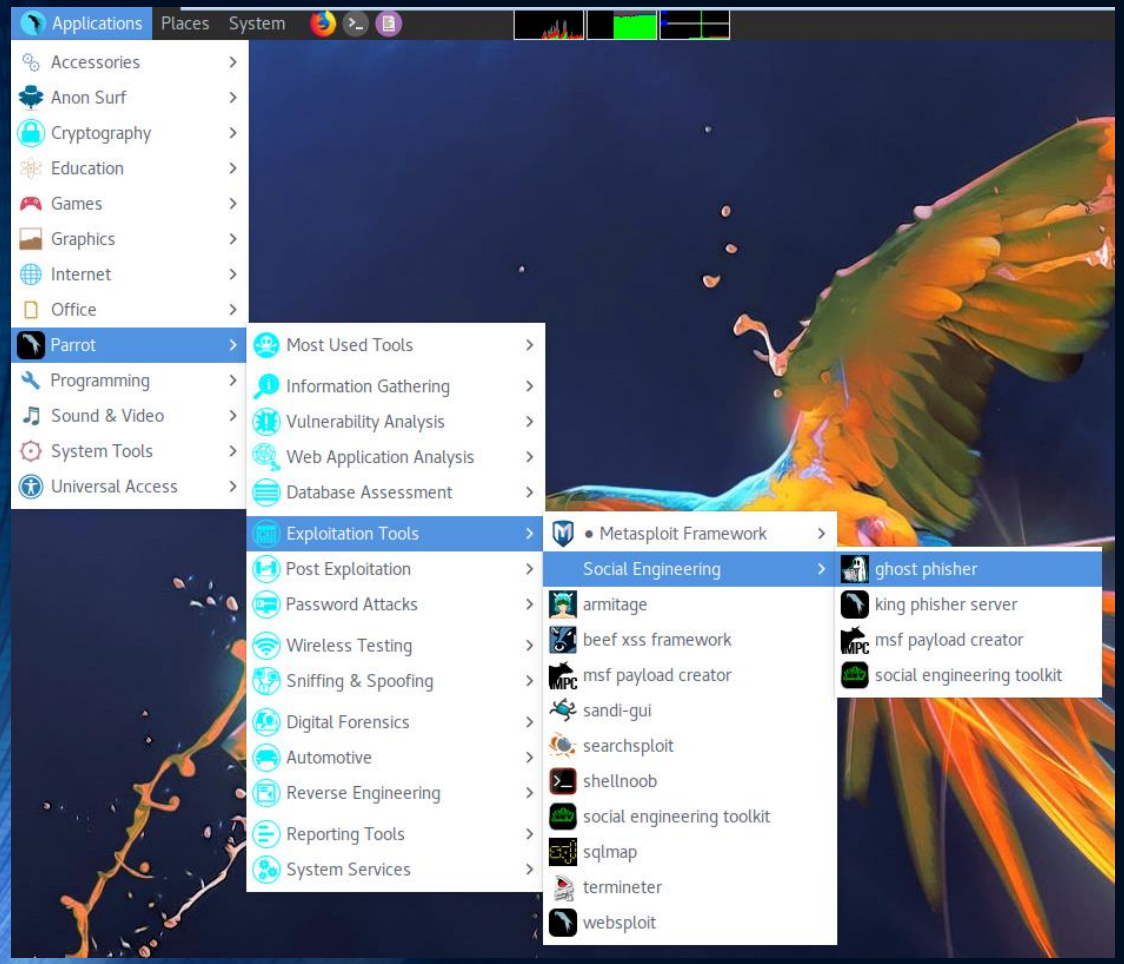
What makes you feel secure?

- Safety in numbers? Blend in with the crowd?
- Anonymity?
- Passwords?
- Encryption?
- Firewalls?
- Intrusion Detection Systems?

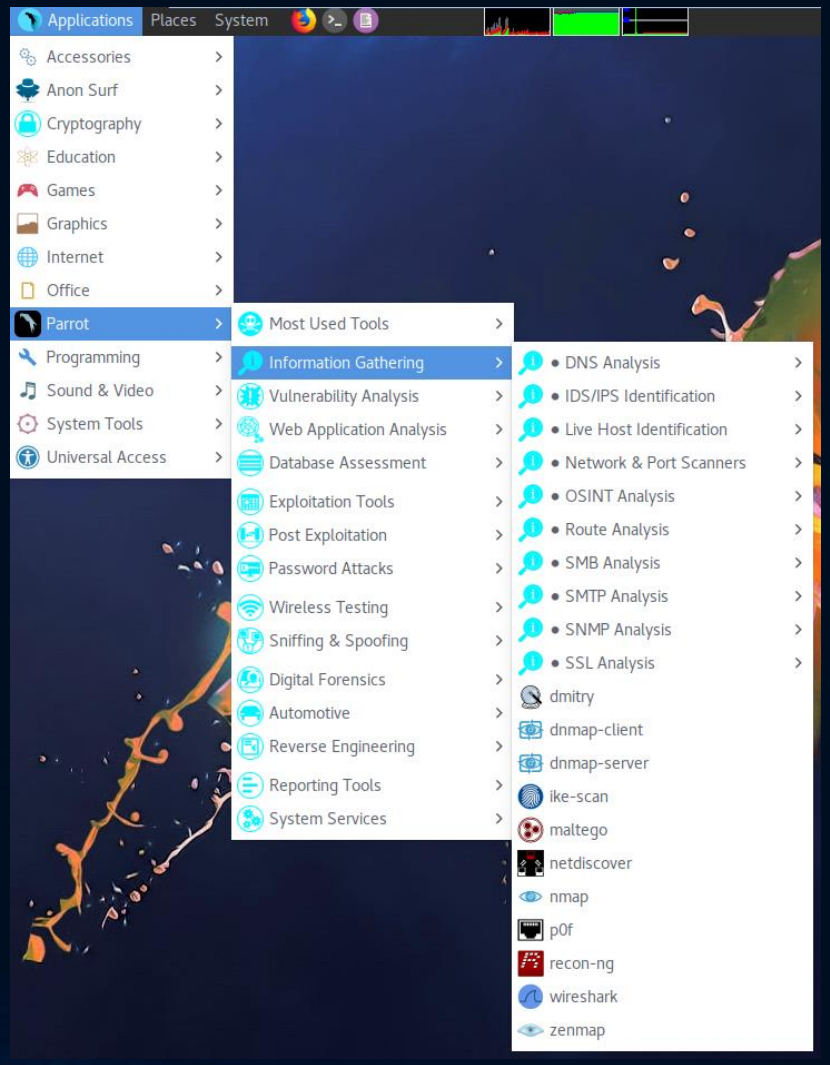
- Others?

Some of the Tools in (free) Parrot Linux

Social Engineering Tools:

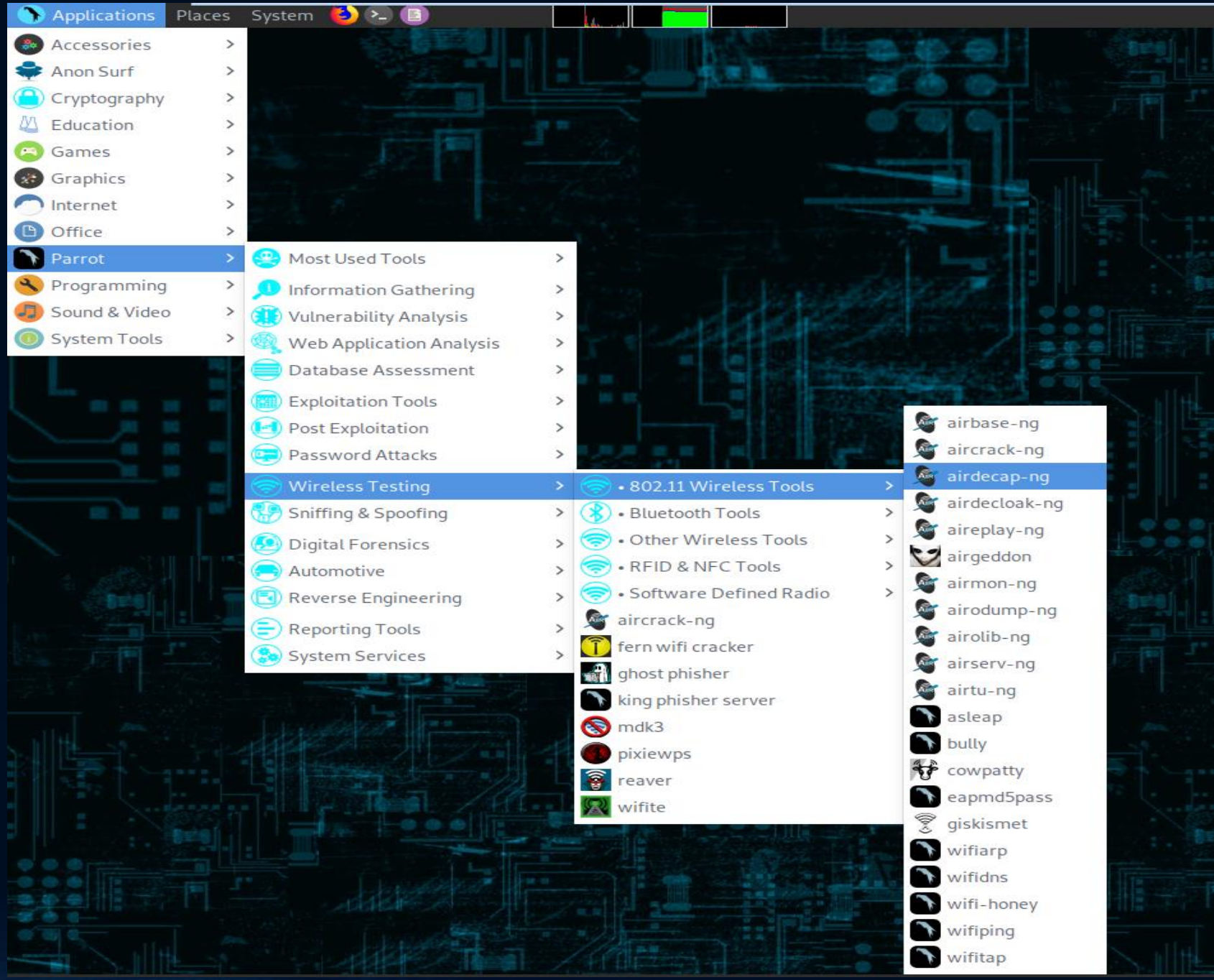


Information Gathering:



And so much more….

Parrot Wireless Tools



Yeah Yeah Yeah

This is Peoria, Andy
Not Los Angeles
Or Chicago
Or New York
Or Dallas

I am going to: https://www.wigle.net

Three Types of Wi-Fi Frames

Control frames

- Acknowledgement (ACK)
- Request to Send (RTS)
- Clear to Send (CTS)
- Power Save Poll

Management frames

- Beacons
- Probe Requests / Probe Responses
- Association Requests / Association Responses
- Reassociation Requests / Reassociation Responses
- Disassociations
- Authentications / Deauthentications
- Action

Data frames

- Data
- Null Function

Do I have to be on your Wi-Fi Network?

- I may need to get on….

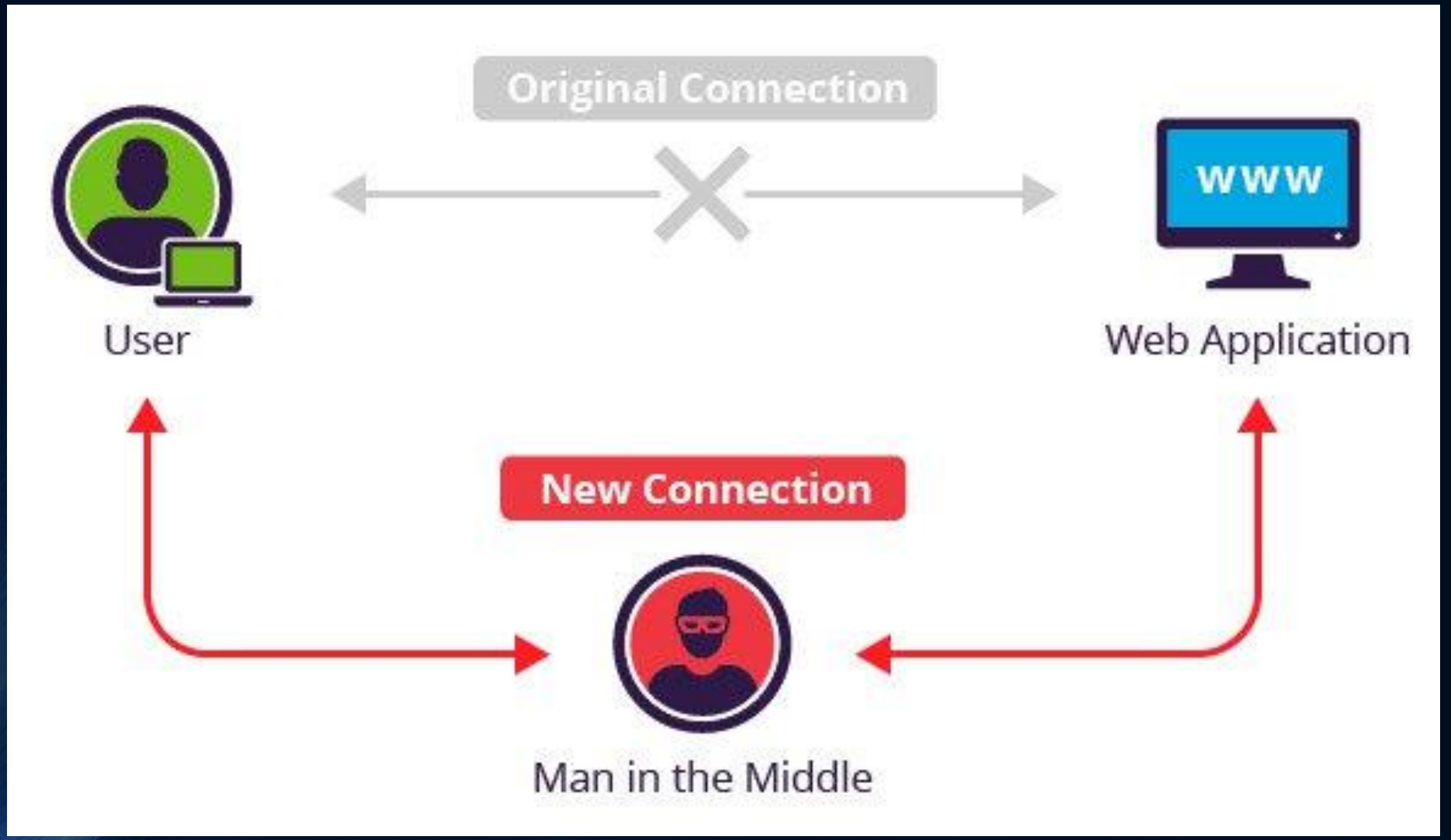
MAC Filtering – Bypass Demo

- Let's say a Wi-Fi access point only allows certain MAC addresses
- All we need to do is get the MAC of an allowed system
- Then change our MAC to that MAC
- We are in!

```
CH 11 ][ Elapsed: 18 s ][ 2019-02-02 12:24

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

70:77:81:DD:C3:7D  -43 100      184      171   13  11  54e  WPA2 CCMP   PSK  CellStream Inc.

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

70:77:81:DD:C3:7D  DC:A4:CA:7D:B2:97   -1    1e- 0      0        1
70:77:81:DD:C3:7D  10:0D:7F:BD:B0:FA   -1    1e- 0      0        1
70:77:81:DD:C3:7D  02:0F:B5:D4:A9:4C  -48    0e- 0e     0        6
70:77:81:DD:C3:7D  18:B4:30:0F:29:54  -34    1e-11      1        7
70:77:81:DD:C3:7D  04:54:53:12:E0:02  -44    0 - 1      0        9
70:77:81:DD:C3:7D  18:B4:30:00:6D:9B  -44    1e- 2      0       11
70:77:81:DD:C3:7D  02:0F:B5:22:14:CF  -50    0e- 0e     1        5
70:77:81:DD:C3:7D  02:0F:B5:6F:10:78  -48    0e- 0e     0        8
70:77:81:DD:C3:7D  12:DA:43:22:FF:75  -48    0 - 0e     6        4
70:77:81:DD:C3:7D  A4:77:33:EF:C4:40  -55    0e- 0e     2       86
70:77:81:DD:C3:7D  18:B4:30:01:A0:18  -67    0e- 2     33       13
70:77:81:DD:C3:7D  5C:F9:38:94:D7:70  -66    0 -24e     5       22
70:77:81:DD:C3:7D  74:C6:3B:29:CA:BB  -77    0e- 0e     0        9
```

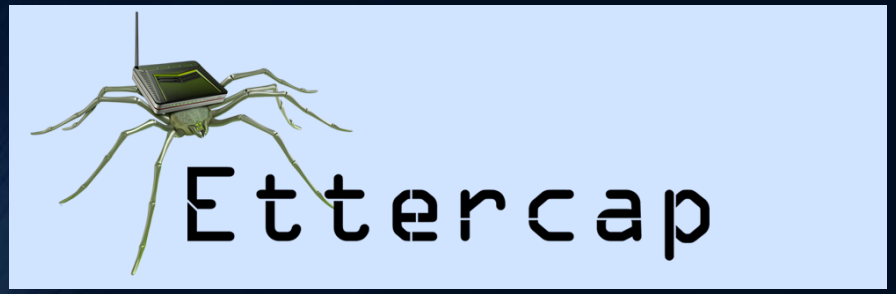
I am going to: https://netscionline.com/mod/page/view.php?id=7561
This is a Security course that you must enroll in.

Man in The Middle Attack!



If I am on your network….

- Too easy
- Use a tool
- Ettercap (I will use the GUI)
- Built into Kali and Parrot Linux



I am going to: https://netscionline.com/mod/page/view.php?id=7987&forceview=1
This is a free reference at the Online School, you must create a user account
If you do not already have one.

Scanning & Joining a Wireless Network

- Access Points transmit periodic Beacons allowing the stations to identify APs
- Scanning – listening to the RF
  - Passive Scanning
    - Only listens for Beacon and get info of the BSS – finding the AP
    - Beacons transmitted approximately every 100msec
    - STA listens to one channel at a time (approx. 250msec/channel)
    - Less power used in this method
  - Active Scanning
    - Transmit and elicit response from APs
    - Probe Requests, channel by channel, can be sent to any or a specific AP
    - Consumes network capacity, possibly slowing the network
    - Time is saved

Do I have to be on your Wi-Fi Network?

- I may NOT need to get on….

Jamming

- Jamming is the process of sending signals that create interference with normal operations of a network or radio. Jamming is basically a Denial of Service (DoS) attack. There are several obvious ways that Jamming could be used on a Wi-FI WLAN:
  - I want to take out your security cameras
  - I want to disable your security system
  - I want to take down your entire network
- Just a quick warning. DO NOT USE THIS TOOL ON A NETWORK YOU DO NOT HAVE PERMISSION TO DO SO. OK, let's get started.
- MDK4 is the tool we will be using as our example

Should I Remember Wireless Networks?

- Secure answer – no!
- Making life easy – yes.
- Computers that keep these wireless networks in their configurations are always scanning for the networks that have been saved
- This may result in connecting to a network you do not wish to connect to
- Dangerous with “open” networks

I am going to
https://www.cellstream.com/reference-reading/tipsandtricks/368-deleting-remembered-wi-fi-networks-in-windows

Man In The Middle Attack System

- Wi-Fi Pineapple Demonstration

- Bottom Line: Clear out that Wi-Fi network list!

Audience Questions

How many of you have at least one IoT Wi-Fi connected device in your home? Less than 10? More than 10?

Most household/small business customers run an IPv4 192.168.1.x or 192.168.0.x /24 subnet - leaving 253 usable IP addresses for their home/business. Do you think that is enough on their Wi-Fi and wired network with the IoT explosion?

Has TR69 made a big difference in operations? If so, what was the biggest challenge? (I will probably poll the audience for how many folks have TR-69)

If you could re-do Wi-Fi all over again, what one thing would you do different?

Do you think Wi-Fi Security knowledge is important in your team?

Resources

- Online School Web Site: https://www.netscionline.com/
  - Networking Fundamentals Reference Book: https://netscionline.com/mod/book/view.php?id=3129
- Main CellStream Web Site: www.cellstream.com
  - Our Courses
  - Networking and Computing Tips & Tricks – click here
  - CellStream Cheat Sheets and other public documents: Downloads here!
  - Interesting Reading – click here
  - Our Blog
- Follow me on Twitter: @awalding

Questions….

CellStream, Inc. Copyright Notice