



**KNOW THE
UNKNOWN®**

The Art of Cybersecurity (on a 5G canvas)

Darryle Merlette, CISSP

Executive Director – Security Solutions, NIKSUN Inc.

IEEE 5G Summit

May 26, 2015

NIKSUN Inc., CONFIDENTIAL

This document and the confidential information it contains shall be distributed, routed or made available solely to persons having a written obligation to maintain its confidentiality.

Hackers and Painters

What hackers and painters have in common is that they're both makers. Along with composers, architects, and writers, what hackers and painters are trying to do is make good things.

-- Paul Graham (Hackers and Painters)



Evolution



1G
1981



2G
1992



3G
2001



4G
2011



5G
2020

Eavesdropping, Cloning, Spoofing...and IP



1G (analog)

- | All band radio receiver to eavesdrop
- | Clone phones to steal airtime

2G/3G

- | GSM hack using IMSI catcher to impersonate tower (2G)
- | Noise generator and amplifier to knock 3G network offline, then downgrade to 2G.

3G/4G/5G

- | All the vulnerabilities of IP networks...
- | 85% of all internet traffic is WWW
 - | Promise of WWW will likely cause increase

More Mobile Phones than people on Earth



- Monthly global mobile data traffic will surpass 15 Exabytes by 2018.
- The number of mobile-connected devices exceeds the world's population.
- The average mobile connection speed will surpass 2 Mbps by 2016.
- Due to increased usage on smartphones, smartphones will reach 66 percent of mobile data traffic by 2018.
- Monthly mobile tablet traffic will surpass 2.5 Exabytes per month by 2018.
- 4G traffic will be more than half of the total mobile traffic by 2018.

Source: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018

Proliferation of Apps and Devices



Convergent & Rich



Games and Apps



Virtual & SAS



Portable & Capable



Rich Multimedia



Chats



DYNAMIC INTERACTIVE

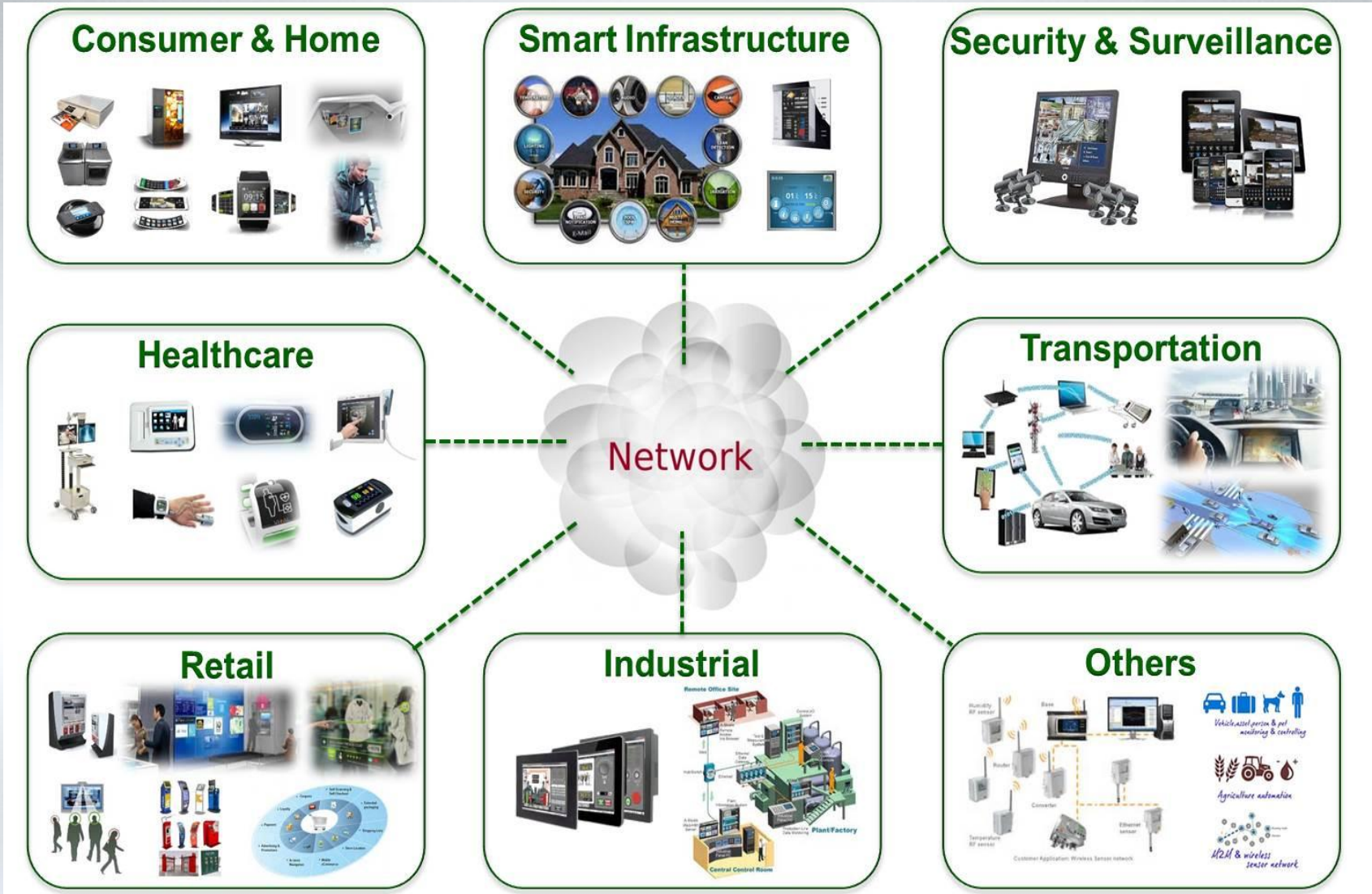
ANYTIME

ANYWHERE

REAL-TIME

- | Many traditional web-based malware also affect mobile devices
- | Wirelurker and Masque (iOS)
 - | Creates trojaned versions of apps for binary file replacement
 - | If same bundle identifier is used, can replace apps installed through App Store (but not preinstalled apps)
- | Roughly 25% of all Google Play apps are clones (Columbia University)

The Internet of Things



Vivante and the Vivante logo are trademarks of Vivante Corporation. All other product, image or service names in this presentation are the property of their respective owners. © 2013 Vivante Corporation

Shodan – Search Engine for IoT



https://www.shodan.io

Shodan Scanhub Developers View All...

SHODAN

Explore Contact Us Blog Enterprise Access

New to Shodan? Login or Register

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

CNN Money Daabladet The Washington Post BBC NEWS WTREDD CIO

Shodan – Default password device search



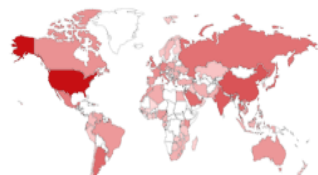
https://www.shodan.io/search?query="default+password"

Shodan Scanhub Developers View All...

SHODAN "default password" Explore Contact Us Blog Enterprise Access New to Shodan? Login or Register

Exploits 84 Maps

TOP COUNTRIES



United States	8,718
China	2,149
India	1,776
Japan	1,351
Argentina	1,336

TOP SERVICES

Telnet	25,492
FTP	5,269
HTTP	573
HTTP (8080)	217
Synology	49

TOP ORGANIZATIONS

Verio Web Hosting	4,352
Telecom Argentina S.A.	1,119
SaudiNet	707
Open Computer Network	615
CenturyLink	504

Showing results 1 - 10 of 31,839

50.193.99.193

60-193-99-193-static.hfc.comcastbusiness.net
Comcast Cable
Added on 2015-05-25 16:47:10 GMT
United States, Elk Grove Village
[Details](#)

Cisco Configuration Professional (Cisco CP) is installed on this device. This feature requires the one-time use of the username "cisco" with the **password** "cisco". These **default** credentials have a privilege level of 15....

74.9.137.65

Windstream Business
Added on 2015-05-25 16:35:09 GMT
United States
[Details](#)

[2]H ***** Important Banner Message *****

Enable and Telnet **passwords** are configured to "**password**". HTTP and HTTPS **default** username is "admin" and **password** is "**password**". Please change them immediately.

The ethernet 0/1 interface is enabled with an address of 10.1...

70.28.85.177

Bell Canada
Added on 2015-05-25 16:35:04 GMT
Canada, Hamilton
[Details](#)

Cisco Router and Security Device Manager (SDM) is installed on this device. This feature requires the one-time use of the username "cisco" with the **password** "cisco". The **default** username and **password** have a privilege 1...

94.97.83.51

SaudiNet
Added on 2015-05-25 16:29:11 GMT
Saudi Arabia

Cisco Configuration Professional (Cisco CP) is installed on this device.

Shodan – SCADA search



https://www.shodan.io/search?query=scada

SHODAN scada

Exploits 99 Maps

TOP COUNTRIES

Canada	100
United States	60
Spain	16
Serbia	8
Taiwan, Province of China	6

TOP SERVICES

NetBIOS	58
FTP	44
SNMP	39
HTTP	37
Modbus	5

TOP ORGANIZATIONS

Telus Communications	60
Telus Mobility	23
Verizon Wireless	10
Nucleus Information Service	7
Telefonica de Espana	6

Showing results 1 - 10 of 263

188.69.236.17

md-188-69-236-17.omni.lt
OMNITEL Net
Added on 2015-05-25 11:40:10 GMT
Lithuania

NetBIOS Response
Servername: **SCADA-1-PC**
MAC: 0c:5b:8f:27:9a:64

Names:
SCADA-1-PC <0x0>
WORKGROUP <0x0>
SCADA-1-PC <0x20>
WORKGROUP <0x1e>

173.182.26.25

Telus Communications
Added on 2015-05-25 11:39:13 GMT
Canada

Linux Mt Kidd **SCADA** 2.6.27 #1 Thu Jun 13 09:26:49 MDT 2013 armv5tej1 IPn3G.00:0F:92:00:8A:4C

41.32.153.116

host-41.32.153.116.tedata.net
TE Data
Added on 2015-05-25 11:23:12 GMT
Egypt

NetBIOS Response
Servername: **SCADA-E4CFD1D41**
MAC: 00:19:99:92:63:6F

Names:
SCADA-E4CFD1D41 <0x0>
WORKGROUP <0x0>
SCADA-E4CFD1D41 <0x20>
WORKGROUP <0x1e>

Shodan – IP Address search



Browser address bar: <https://www.shodan.io/host/162.211.182.207>

162.211.182.207

Country	United States
Organization	Hostspace Networks LLC
ISP	Hostspace Networks LLC
Last Update	2015-05-25T10:15:50.119442
ASN	AS26484

Ports

137	3389
-----	------

Services

137	NetBIOS Response
NetBIOS	Servename: IPHONE-8BFD78X MAC: 00:0c:29:1c:97:0c
	Names:
	IPHONE-8BFD78X <0x0>
	WORKGROUP <0x0>
	IPHONE-8BFD78X <0x20>
	WORKGROUP <0x1e>

3389	\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
RDP	

Network Detection

Two Broad Categories

Signature Detection

- | Specific patterns in packets
- | Similar to anti-virus paradigm
- | Must be periodically updated
- | Vulnerable to evasion and new attacks

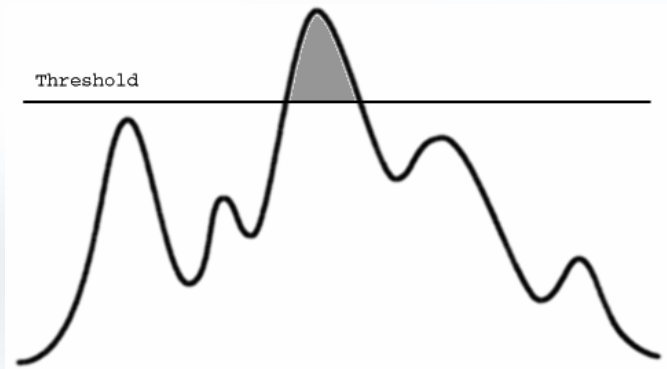
```

000000f0 00 00 00 00 E0 00 0F 01 0B 01 07 0A 00 78 00 00  . . . . a . . . . x . . .
00000100 00 A6 00 00 00 00 00 00 01 40 01 00 00 10 00 00  . . . . | . . . . e . . . .
00000110 00 90 00 00 00 00 00 01 00 10 00 00 00 02 00 00  . . . . | . . . . . . . . . .
00000120 05 00 01 00 05 00 01 00 04 00 00 00 00 00 00 00  . . . . | . . . . . . . . . .
00000130 00 00 01 00 00 04 00 00 7F 4F 01 00 02 00 00 80  . . . . | . . . . | O . . . |
00000140 00 00 04 00 00 10 01 00 00 10 00 00 10 00 00  . . . . | . . . . | O . . . |
00000150 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  . . . . | . . . . | O . . . |
00000160 AC AF 01 00 EC 01 00 00 00 00 00 00 58 89 00 00  -O | . . . . X | . . .
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . | . . . . | . . . .
00000180 54 AF 01 00 08 00 00 00 50 13 00 00 1C 00 00 00  TO | . . . . P . . . .
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . | . . . . | . . . .
000001a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . | . . . . | . . . .
000001b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . | . . . . | . . . .
000001c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . | . . . . | . . . .
000001d0 00 00 00 00 00 00 10 00 2E 74 65 78 74 00 00 00  . . . . | . . . . | . . . .
000001e0 00 80 00 00 00 10 00 00 40 00 00 00 04 00 00 00  . . . . | . . . . | . . . .
000001f0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0  . . . . | . . . . | . . . .
00000200 2E 64 61 74 61 00 00 00 00 20 00 00 00 90 00 00  . . . . | . . . . | . . . .
00000210 00 02 00 00 00 44 00 00 00 00 00 00 00 00 00 00  . . . . | . . . . | . . . .
00000220 00 00 00 00 40 00 00 C0 2E 72 73 72 63 00 00 00  . . . . | . . . . | . . . .
00000230 00 90 00 00 00 E0 00 00 00 10 00 00 00 46 00 00  . . . . | . . . . | . . . .
00000240 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0  . . . . | . . . . | . . . .

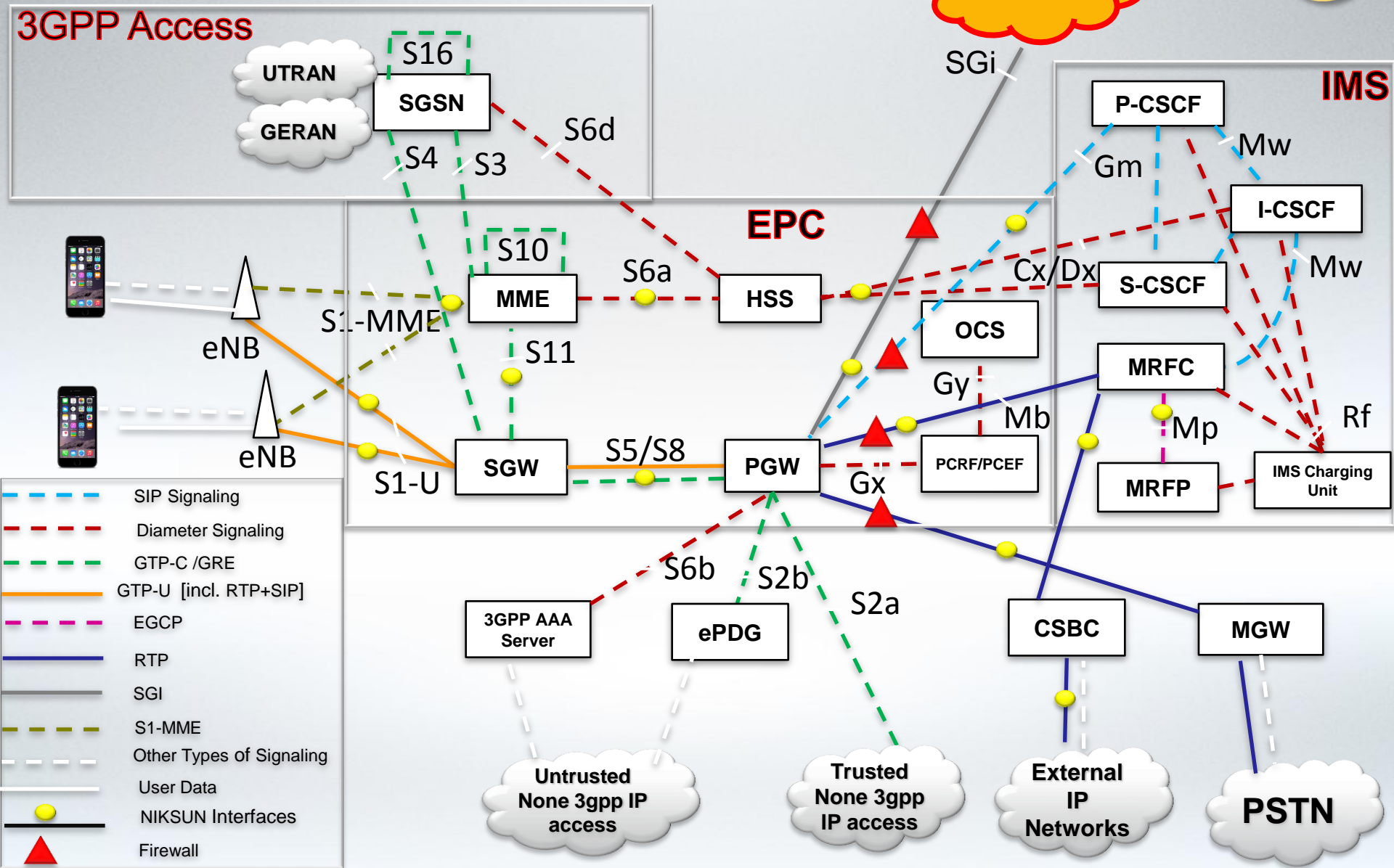
```

Anomaly Detection

- | Deviations from statistical/behavioral norms
- | Can either “learn” or “be told” what is “normal”
- | Can often detect new attacks



3G/4G/LTE Monitoring Points



Detunneling for detection



- ⊕ Frame 31: 249 bytes on wire (1992 bits), 249 bytes captured (1992 bits)
- ⊕ Ethernet II, Src: Cisco_71:77:47 (00:1b:d4:71:77:47), Dst: Alcatel-_75:47:92 (00:23:3e:75:47:92)
- ⊕ Internet Protocol Version 4, Src: 66.174.20.194 (66.174.20.194), Dst: 199.223.96.1 (199.223.96.1)
- ⊕ User Datagram Protocol, Src Port: 2152 (2152), Dst Port: 2152 (2152)
- ⊕ GPRS Tunneling Protocol
 - T-PDU Data 199 bytes
- ⊕ Internet Protocol Version 4, Src: 209.53.113.223 (209.53.113.223), Dst: 10.174.187.16 (10.174.187.16)
- ⊕ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1237 (1237), Seq: 1, Ack: 1, Len: 159
- ⊕ Hypertext Transfer Protocol
- ⊖ Media Type
 - Media Type: image/jpeg (25 bytes)

0000	00 23 3e 75 47 92 00 1b d4 71 77 47 08 00 45 00	.#>uG... .qwG..E.
0010	00 eb 00 00 00 00 fd 11 3d b1 42 ae 14 c2 c7 df =.B.....
0020	60 01 08 68 08 68 00 d7 63 6d 30 ff 00 c7 04 31	`..h.h.. cm0....1
0030	de 47 45 00 00 c7 69 59 40 00 6b 06 9d 04 d1 35	.GE...iY @.k....5
0040	71 df 0a ae bb 10 00 50 04 d5 15 2b 17 59 4b 69	q.....P ...+.YKi
0050	a8 e6 50 18 fd 06 1e 70 00 00 48 54 54 50 2f 31	..P....p ..HTTP/1
0060	2e 31 20 32 30 30 20 4f 4b 0d 0a 53 65 72 76 65	.1 200 0 K..Serve
0070	72 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 49 49 53	r: Micro soft-IIS
0080	2f 36 2e 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79	/6.0..Co ntent-Ty
0090	70 65 3a 20 69 6d 61 67 65 2f 6a 70 65 67 0d 0a	pe: imag e/jpeg..
00a0	43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20	Content- Length:
00b0	32 35 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20	25..Conn ection:
00c0	4b 65 65 70 2d 41 6c 69 76 65 0d 0a 54 61 67 49	Keep-Ali ve..TagI
00d0	64 3a 20 35 33 37 30 36 34 37 30 34 0d 0a 0d 0a	d: 53706 4704....
00e0	7e 46 99 c7 5f 4b 65 ff 00 30 10 c0 1c 59 63 9e	~F..._Ke. .0...Yc.
00f0	78 d0 93 5d ac 89 7e 0d 0a	x..]...~. .

IMSI values as part of alerts



malware traffic Start 13:44:00.328931 09/23/2014 Stop 17:09:21.960065001 11/20/2014 Relative Apply Advanced Options

Summary All Events LTE Blacklisted Events Zero Day Indicators Network Infiltration + Delete Export

Type	Name/ID	Description	Source	Destination	IMSI	Time	Link
Host Pair Pa...	BAD URL	[36 repeats starting 16:34:00 11/20/2014] Number of Packets(ip) t...	172.16.89.78	80.67.6.50	n/a	17:09:00 11/20/2014	malware traffic
Host Pair Pa...	Japan	[60 repeats starting 16:10:00 11/20/2014] Number of Packets(ip) t...	172.16.94.29	202.12.27.33	n/a	17:09:00 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:08:54.74827 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected IMSI: 31041012...	172.16.89.78	80.67.6.50	31041012345...	17:08:35.894144 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:08:35.164514 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:53.490295 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:45.567493 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:41.06664 11/20/2014	malware traffic
Signature IDS	1:3000055:2	NIKSUN-NETSQUID VIRUS SWEN.A Worm detected [Classification: A ...	172.16.89.78	80.67.6.50	n/a	17:07:39.106219 11/20/2014	malware traffic
Signature IDS	1:3000055:2	NIKSUN-NETSQUID VIRUS SWEN.A Worm detected IMSI: 310410123...	172.16.89.78	80.67.6.50	31041012345...	17:07:39.106185 11/20/2014	malware traffic
Signature IDS	1:3000055:2	NIKSUN-NETSQUID VIRUS SWEN.A Worm detected IMSI: 310410123...	172.16.89.78	80.67.6.50	31041012345...	17:07:39.106173 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:38.477104 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected IMSI: 31041012...	172.16.89.78	80.67.6.50	31041012345...	17:07:34.120082 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:33.563901 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:17.838955 11/20/2014	malware traffic

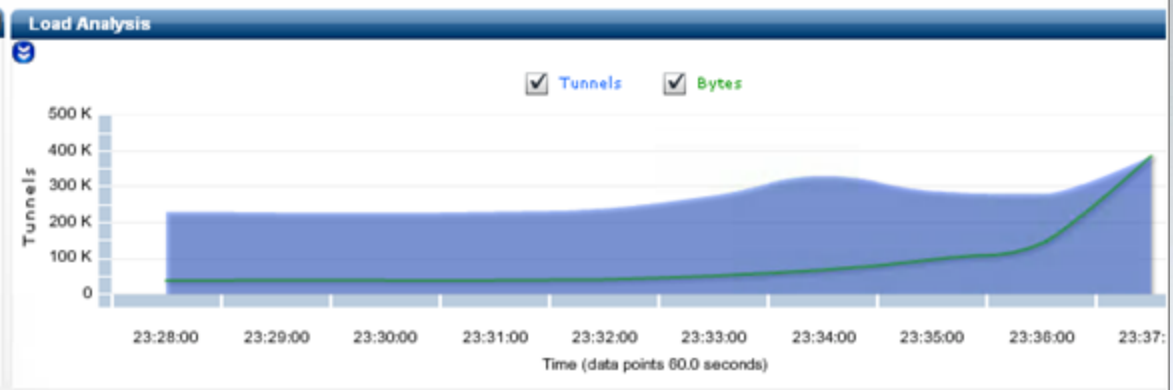
Data: 1 to 20 of 1013 Fetch Next Records per page: 20

LTE GTP KPIs



Query Parameters

Link: LTE Traffic
 Layer: LTE
 History: 1
 Time: 23:28:00 02/23/2014 -- 23:38:00 02/23/2014
 Start: -10 minute
 Stop: now
 Filter:
 Do DNS? Top N: -10 Window: 60
 Update Reset Save



PGW Load

PGW	Tunnels	Bytes
3.18	4	118.06 K
2.24	22	100.76 K
2.242	17	95.78 K
2.232	9	92.06 K
2.194	4	70.49 K
Total for Top 10	87	624.36 K
Overall	555.46 K	52.8 G

SGW Load

SGW	Tunnels	Bytes
2001: :20...	186.87 K	18.42 G
2001: :20...	139.35 K	17.82 G
2001: :20...	274.65 K	9.42 G
2001: :20...	216.72 K	7.13 G
Total for Top 4	817.6 K	52.8 G
Overall	817.6 K	52.8 G

MME Load

MME	Tunnels	Bytes
2001: :20...	338.9 K	23.57 G
2001: :20...	373.38 K	21.6 G
2001: :20...	116.05 K	3.84 G
2001: :20...	120.35 K	3.78 G
Total for Top 4	948.67 K	52.8 G
Overall	948.67 K	52.8 G

enodeB Load

eNodeB	Tunnels	Bytes
2001: :20...	1	801
2001: :20...	1	801
001: :20...	1	801

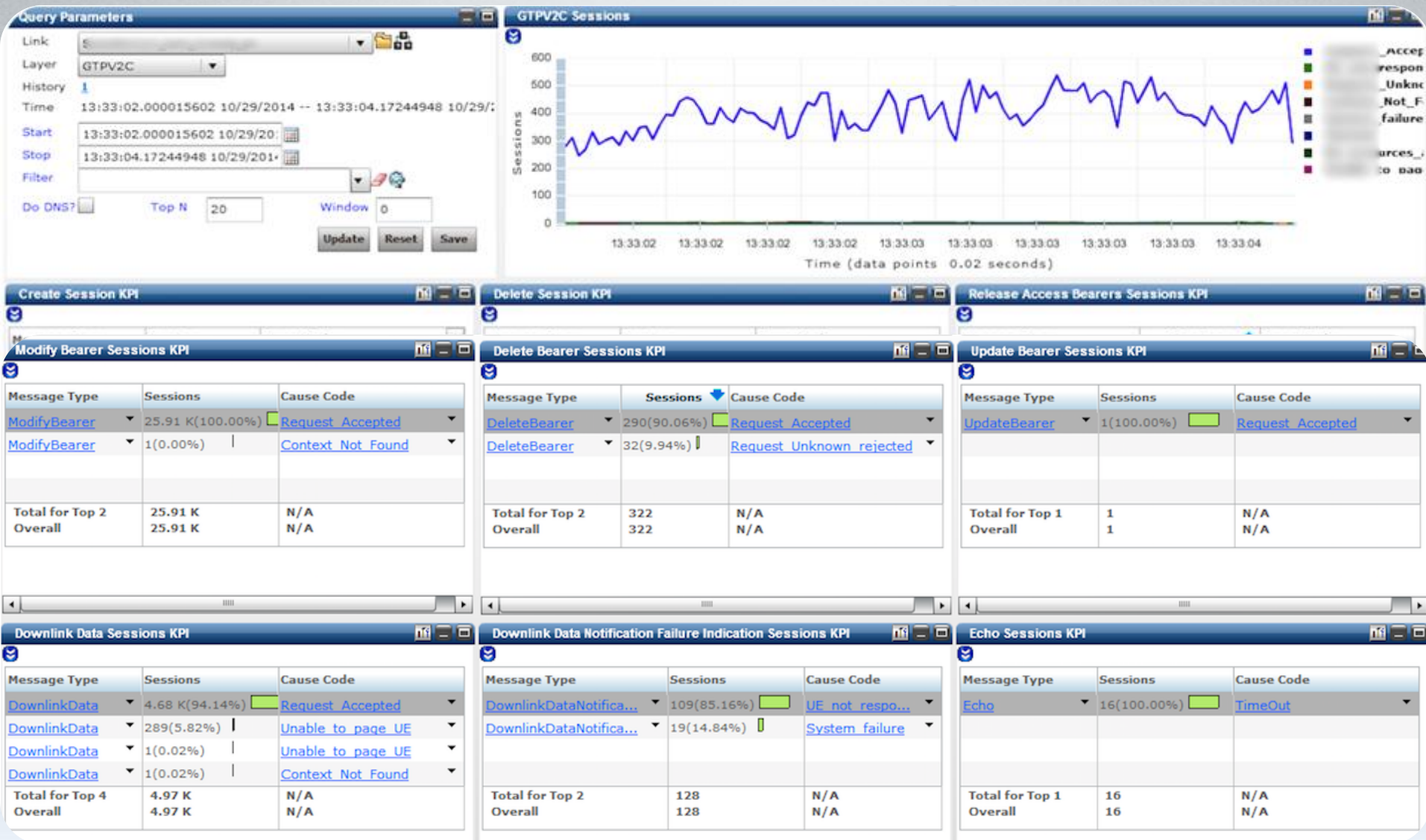
IMSI Load

IMSI	Tunnels	Bytes
311: :982...	1	270
311: :322...	1	270
311: :422...	1	270

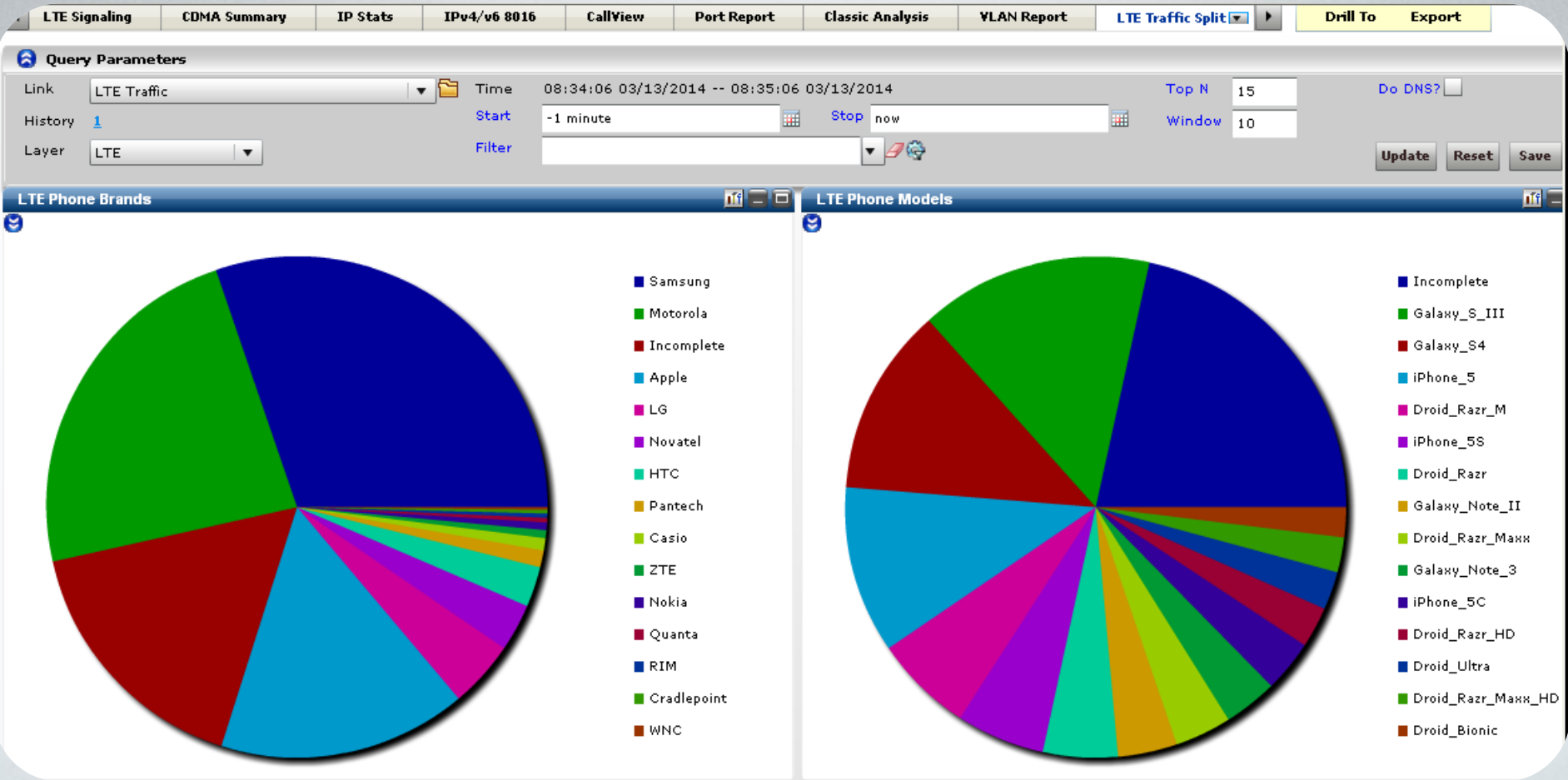
IMSI per enodeB

eNodeB	User Count
2001: :a031:2...	587
2001: :60bd:2...	549
2001: :206c:2...	256

LTE GTP KPIs



LTE GTP KPIs



LTE Security and Performance Alarms



- | Excessive (failed) sessions per UE eNodeB pair/SGW/MME
- | Excessive Bytes per IMSI
- | Excessive Average Bearer Setup Time
- | Tunnels per SGW/MME/UE/eNodeB/PGW
- | Alarms available on IMS-GM, S6a, CDMA as well...

- | As 4G matures and 5G emerges, the expanding landscape of devices and apps presents an attractive canvas for hackers to paint
- | Scalable and holistic monitoring solutions will be needed to help track and mitigate attacks
- | As new attack paradigms emerge, innovative solutions must be developed
- | Humans are still the weakest link when it comes to security...

Security?



There is no security on this earth. There is only opportunity. -- Gen. Douglas MacArthur





NIKSUN:

Helping You *Know the **Unknown***[®]

For additional information:

Visit us at niksun.com or
email to info@niksun.com

Signatures

- Shellshock (content "() {")
- Known rogue User Agents (eg., content:"User-Agent|3a| ezula")
- Known shellcode sequences (eg., 0x90 0x90 0x90...)
- Stuxnet (content:"/index.php?data=66a96e28")

Anomaly Detection (with DAR and GeoIP)

- Host pair bytes, Host pair packets, Host Flood, Host Scan, Port Scan ...
- Covert IRC: apptype irc and not tcp port (194 or 667 or 6660-6669 or 7000)
- From China: geo host CN and apptype irc and not tcp port (194 or 667 or 6660-6669 or 7000)
- Botnet behavior – low bytes over long connection
- Tunneling: not apptype http and tcp port (80 or 8080 or 8008 or 8081 or 591)

Who Are the Bad Guys?



- | No more script kiddies!
- | Nation States
 - | Espionage
 - | Intellectual Property
 - | Critical Infrastructure
- | Cyber-Criminals
 - | Identity Theft
 - | Corporate Fraud
 - | Financial Infrastructure
- | Hacktivists
 - | Political Action
 - | Corporate Shaming
 - | Spear Phishing



Stealth is the New Black

Bad Guys Are Winning...



69 to 158 new malware variants created every minute!
-- McAfee/PandaLabs



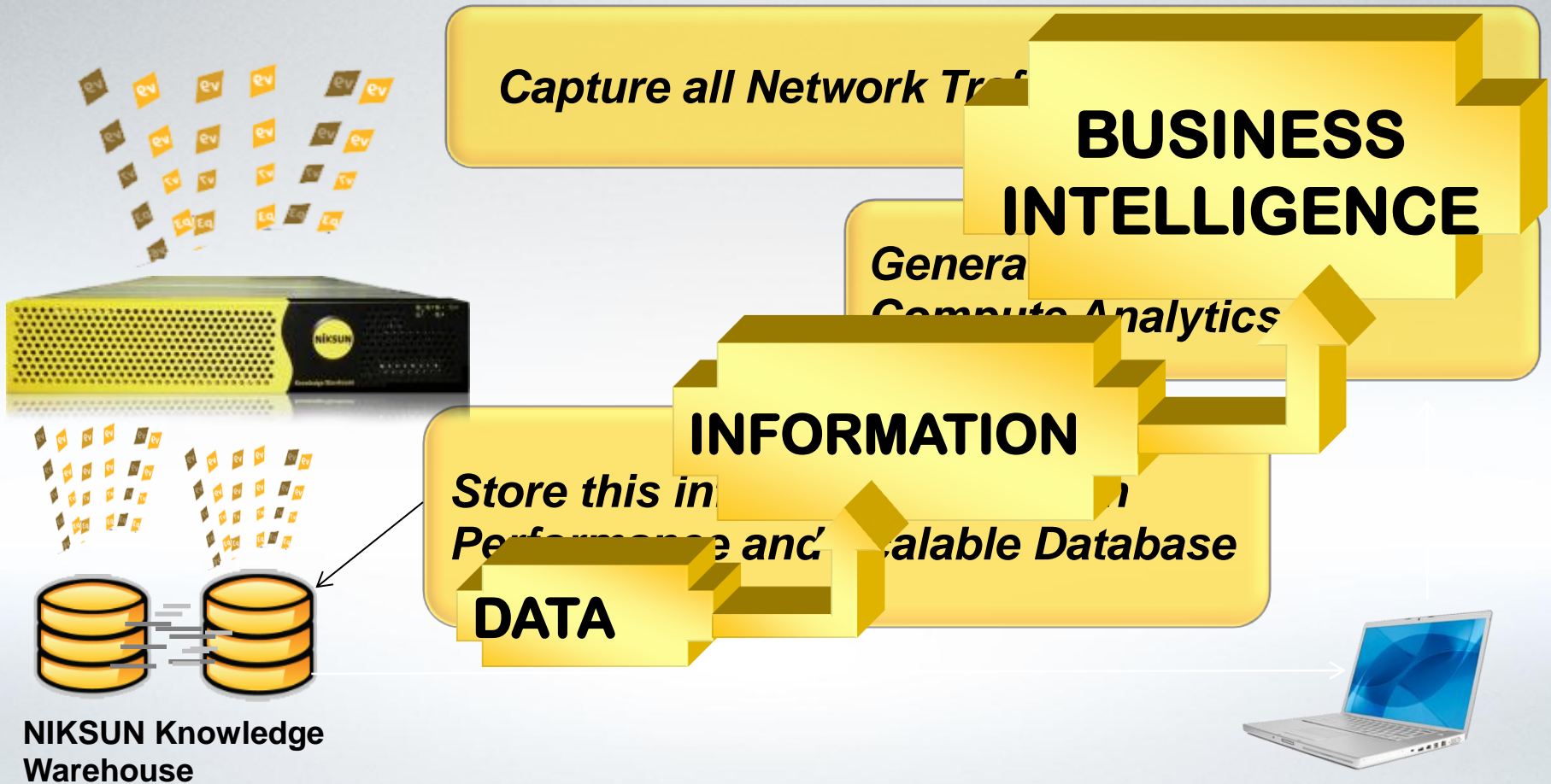
Consider the physical analog...

- Bank robbery: identify and catch the robber from transaction records
- Convenience store: identify and catch a thief from sales transaction receipts
- Office visitor theft: identify and catch perpetrator based on sign-in/sign-out logs



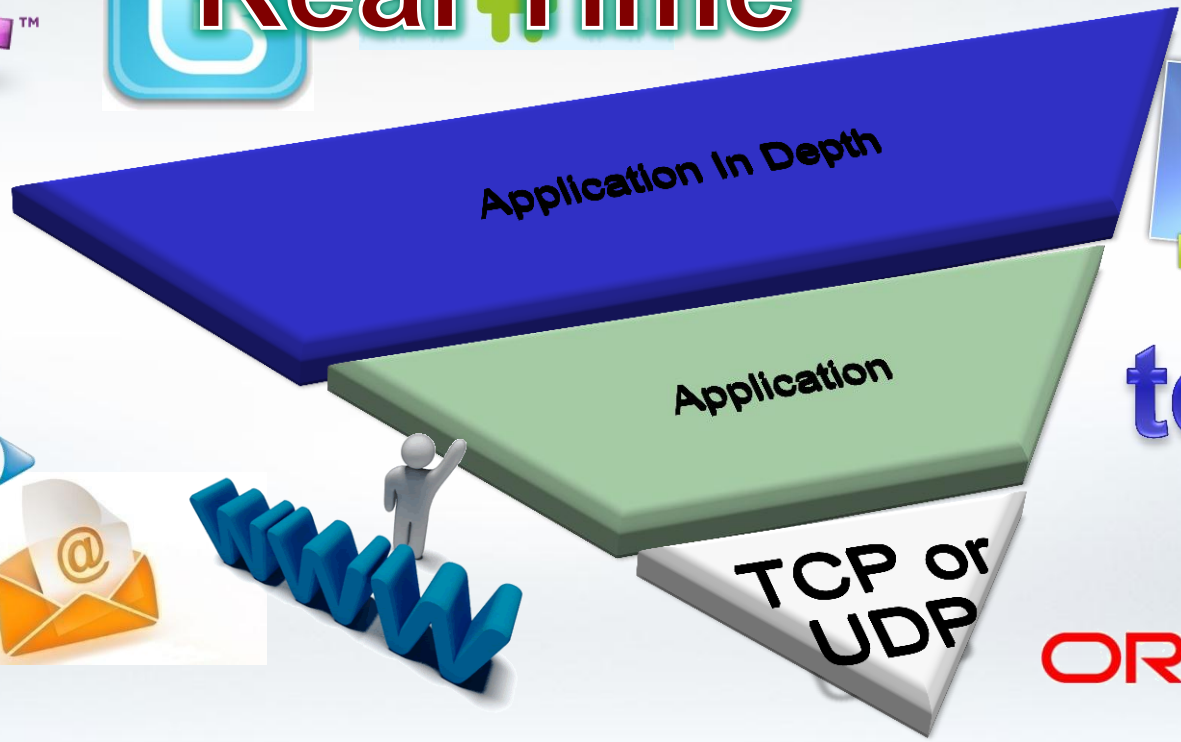
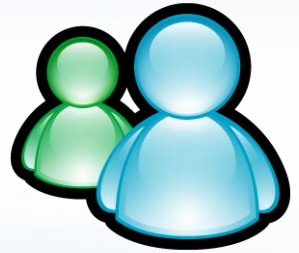
Why rely on logs in the network world?

NIKSUN's Solution Architecture



Dynamic Application Recognition

Signature Based Port Independent Real Time



Detection Made Easy!



Network Working Group
Request for Comments: 3514
Category: Informational

S. Bellovin
AT&T Labs Research
1 April 2003

The Security Flag in the IPv4 Header

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

Firewalls, packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. We define a security flag in the IPv4 header as a means of distinguishing the two cases.

1. Introduction

Firewalls [CBR03], packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. The problem is that making such determinations is hard. To solve this problem, we define a security flag, known as the "evil" bit, in the IPv4 [RFC791] header. Benign packets have this bit set to 0; those that are used for an attack will have the bit set to 1.

Be Careful With Your Data!

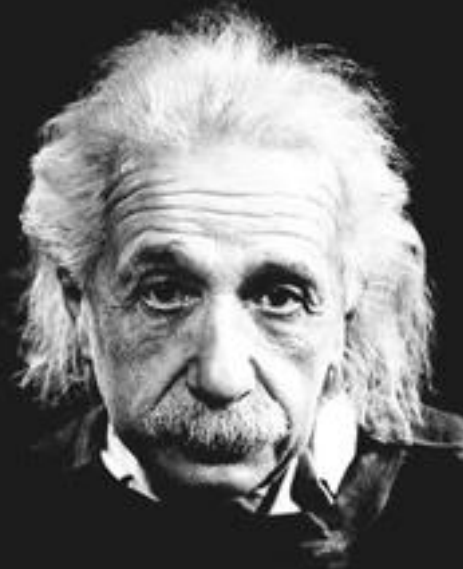
Internet Explorer vs Murder Rate

18,000

90%

"Not everything that counts can be counted, and not everything that can be counted counts."

-Albert Einstein





Cyber Security

Surveillance, Detection and Forensics

Network Performance

Proactive Network, Service and Application Monitoring

Mobility

Performance and Security Monitoring for Cellular Networks

NIKSUN Product Portfolio



NetDetector®
NetDetectorLive™

Security Monitoring
Detection & Alerting
Forensics

NetMobility®
NetVoice®

3G & 4G Analysis
VoIP Performance

NetVCR®
FlowAggregator™
NetBlackBox Pro®

Performance Monitoring
Flow Monitoring
Troubleshooting

NetRTX™
NetSLM™
NetMulticast™
NetPoller™

SLA/QoS Alerting
Advanced Analysis

NetOmni™
NetX™
Central Manager™
NetTrident™

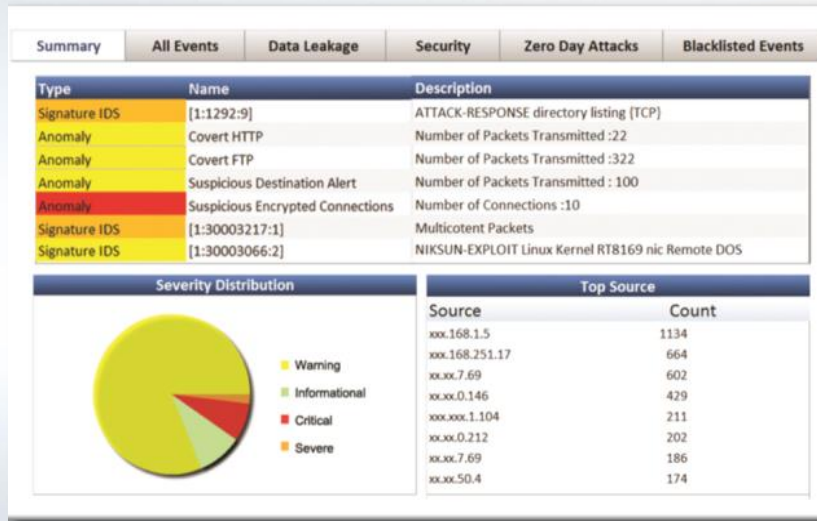
Scalable Monitoring
Reports
Alerts
Forensics

NetReporter™
NetXperts™

Reporting
Expert Analysis

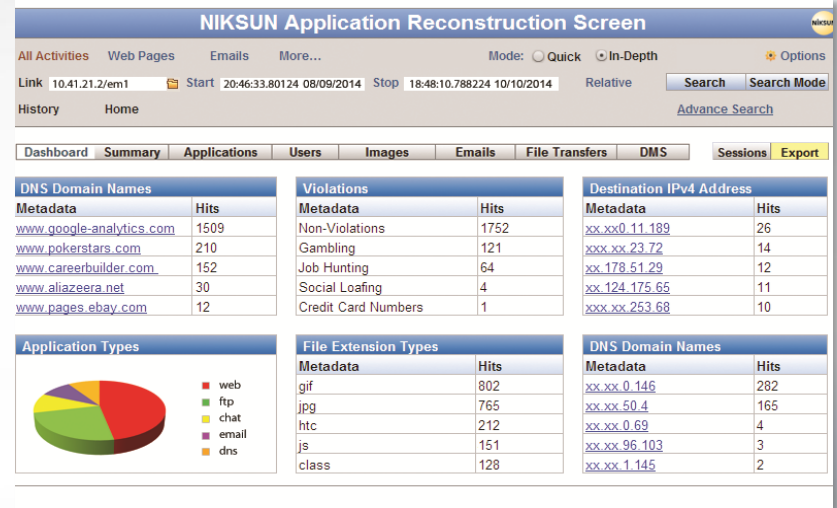
NetDetector®

Comprehensive and actionable solution for network security



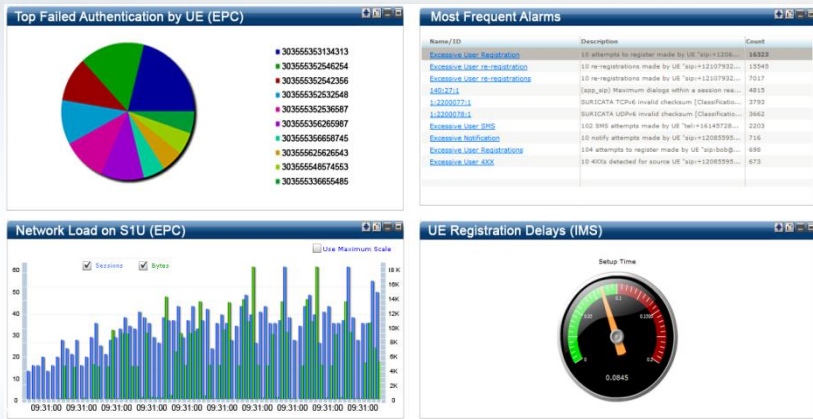
NetDetectorLive™

Lightning fast search & application reconstruction for real-time network security forensics



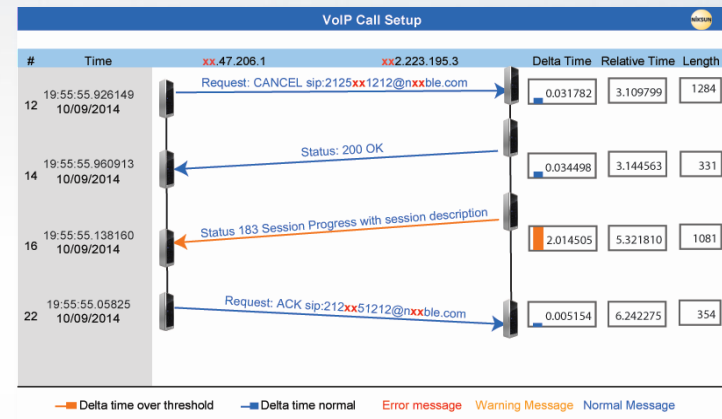
NetMobility®

Performance and Security Analysis for 3G and 4G Networks



NetVoice®

VoIP Monitoring & Troubleshooting Solution



NetOmni™

Single Unifying Information Portal For All Network Data

