Enterprise-Level Network Traffic Analysis and Security Monitoring

Martin Arlitt and Carey Williamson
Department of Computer Science
University of Calgary

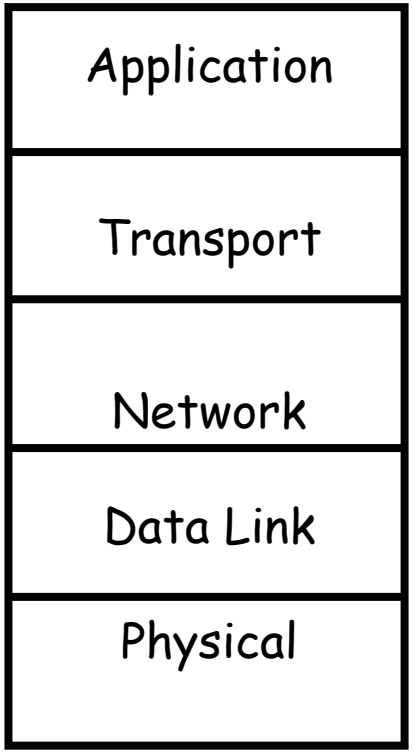
UNIVERSITY OF CALGARY

Outline

- Introduction (Carey: 20 minutes)
  - Internet TCP/IP protocol stack
  - Network traffic measurement
  - Basic tools: tcpdump, wireshark
- Network Security Analysis (Martin: 20 minutes)
  - Principles and approaches
  - Advanced tools: Endace DAG, Bro (Zeek) IDS, Vertica
  - U of C network traffic overview and challenges
- U of C Case Study: Part 1 (Carey: 20 minutes)
  - Examples of normal and abnormal (malicious) traffic
- U of C Case Study: Part 2 (Martin: 20 minutes)
  - More examples of malicious traffic
- Q&A

Background Review: Internet Protocol Stack (see [5])

- Application: supports end-user services and network applications
  - HTTP, SMTP, DNS, FTP, NTP
- Transport: end to end data transfer
  - TCP, UDP
- Network: routing of datagrams from source to destination
  - IPv4, IPv6, BGP, RIP
- Data Link: channel access, framing, flow/error control, hop by hop basis
  - PPP, Ethernet, IEEE 802.11b WiFi
- Physical: transmission of bits



001101011...

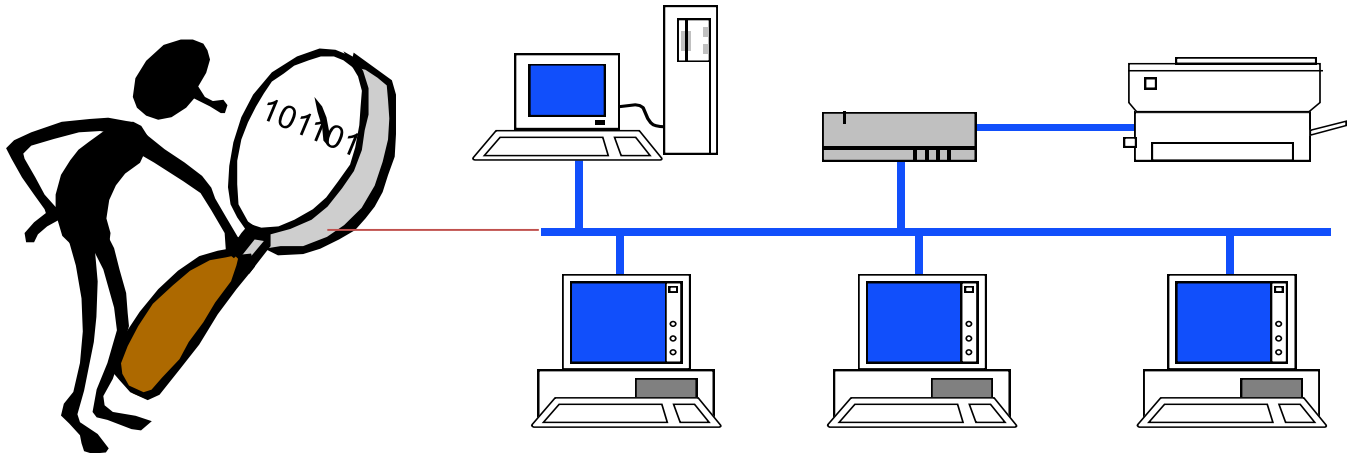
Network Traffic Measurement (see [2][7][8])

- A focus of networking research for 30+ years
- Collect datasets or traces showing packet-level activity on the network for different applications

- Why?
  - Understand the traffic on existing networks (see [9])
  - Workload characterization and modeling
  - Develop models of traffic for future networks
  - Performance evaluation of protocols and applications
  - Protocol debugging
  - Network security monitoring (see [6])

Requirements

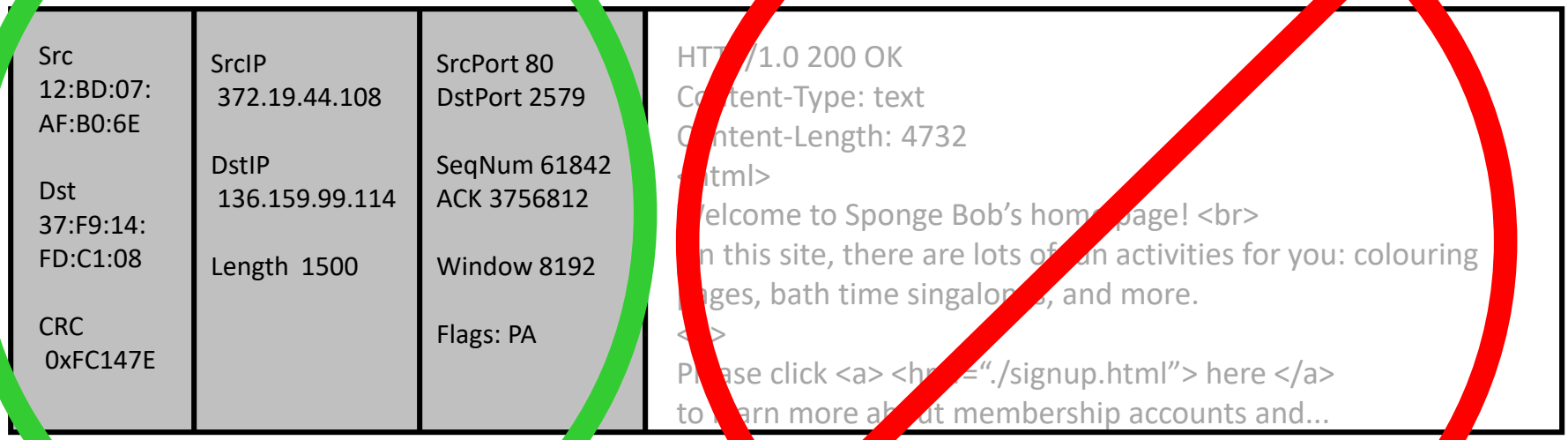
- Network traffic measurement requires hardware or software measurement tools that attach directly to network
- Allows you to observe all packet traffic on the network (or a filtered subset for traffic of interest)
- Assumes broadcast-based network technology, superuser permission



Network Packet Structure

Protocol Headers (Control Information)

Payload



Data Link Layer Header (e.g., WiFi, Ethernet)

Network Layer Header (e.g., IP)

Transport Layer Header (e.g., TCP)

Payload (User Level Data)

UNIVERSITY OF CALGARY

Measurement Approaches (1 of 3)

- Can be classified into hardware and software measurement tools (see [4][8])
- Hardware: specialized equipment
  - Examples: HP 4972 LAN Analyzer, DataGeneral Network Sniffer, NavTel InterWatch 95000, Endace DAG, others...
  - These are faster, but more expensive ($$$)
- Software: special software tools
  - Examples: tcpdump, ethereal, wireshark, SNMP, others...
  - These are cheaper (free!), but also slower (miss packets)

UNIVERSITY OF CALGARY

Measurement Approaches (2 of 3)

- Measurement tools can also be classified as active or passive
- Active: the monitoring tool generates traffic of its own during data collection (e.g., ping, traceroute)
- Passive: the monitoring tool is passive, observing and recording traffic info, while generating none of its own (e.g., tcpdump, wireshark, airopeek)

UNIVERSITY OF CALGARY

Measurement Approaches (3 of 3)

- Measurement tools can also be classified as real-time or non-real-time
- Real-time: collects traffic data as it happens, and may even be able to display traffic info as it happens, for real-time traffic management
- Non-real-time: collected traffic data may only be a subset (sample) of the total traffic, and is analyzed off-line (later), for detailed analysis

UNIVERSITY OF CALGARY

Basic Tools for Network Traffic Measurement

- tcpdump https://www.tcpdump.org
  - Unix-based tool from mid-to-late 1980's
  - Distributed with BSD Unix (Berkeley Software Distribution)
  - Command-line interface; must be root to run it
  - Uses the Berkeley Packet Filter (BPF) in operating system
  - Writes to a PCAP file format; uses libpcap library
- Wireshark https://www.wireshark.org
  - PC-based tool from the early 2000's
  - Formerly called Ethereal (name change in May 2006)
  - Free and open-source tool
  - Multi-layer visualization and analysis of packet traces
  - Also supports PCAP file format

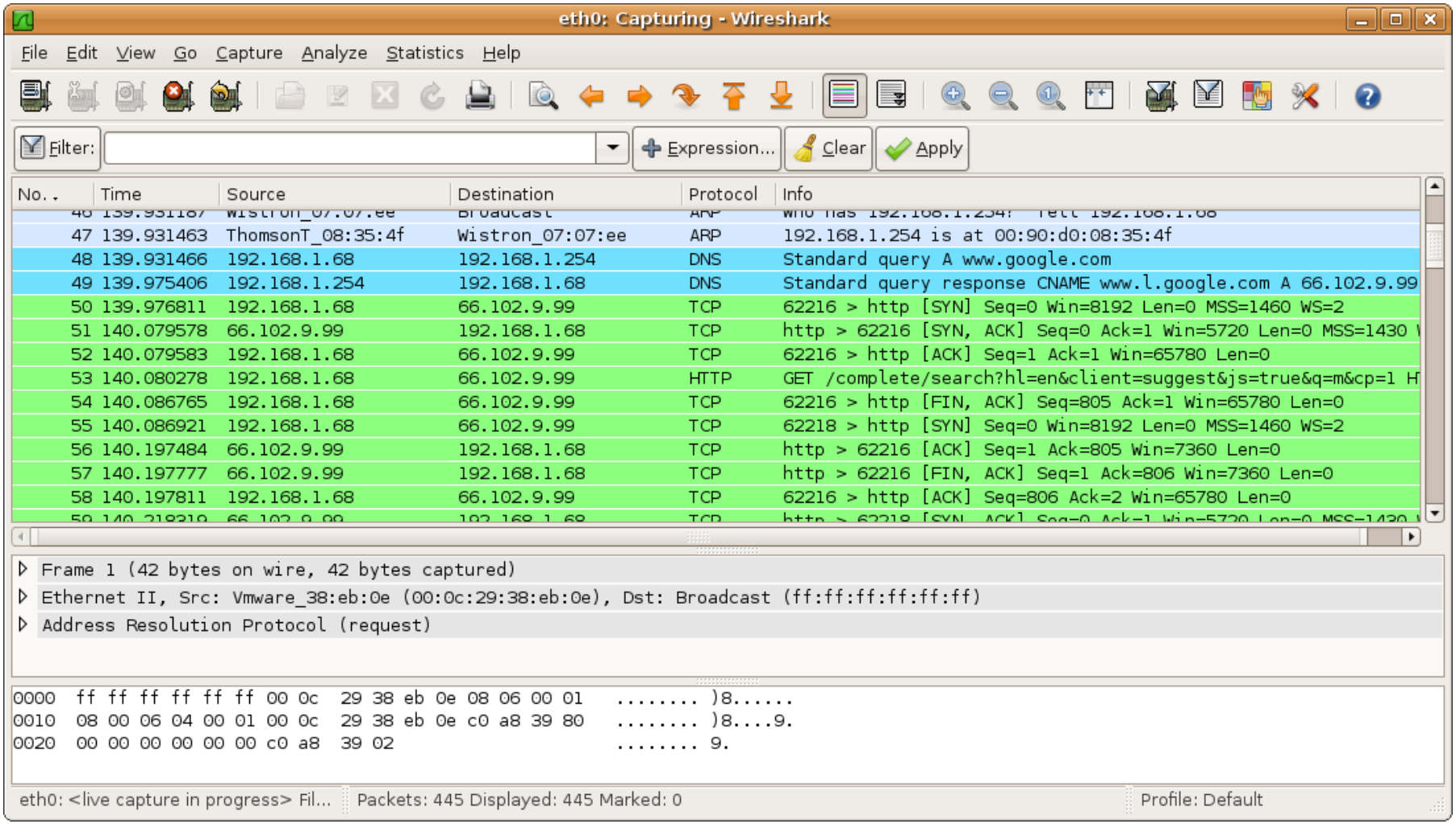
Example: tcpdump

Time	IP Source Addr		IP Dest Addr	Size	Prot	SPort	DPort	TCP Data SeqNumber	TCP AckNum	Window	Flags
0.000000	192.168.1.201	->	192.168.1.200	60	TCP	4105	80	1315338075 : 1315338075	0	win: 5840	S
0.003362	192.168.1.200	->	192.168.1.201	60	TCP	80	4105	1417888236 : 1417888236	1315338076	win: 5792	SA
0.009183	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338076 : 1315338076	1417888237	win: 5840	A
0.010854	192.168.1.201	->	192.168.1.200	127	TCP	4105	80	1315338076 : 1315338151	1417888237	win: 5840	PA
0.014309	192.168.1.200	->	192.168.1.201	52	TCP	80	4105	1417888237 : 1417888237	1315338151	win: 5792	A
0.049848	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417888237 : 1417889685	1315338151	win: 5792	A
0.056902	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417889685 : 1417891133	1315338151	win: 5792	A
0.057284	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417889685	win: 8688	A
0.060120	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417891133	win: 11584	A
0.068579	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417891133 : 1417892581	1315338151	win: 5792	PA
0.075673	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417892581 : 1417894029	1315338151	win: 5792	A
0.076055	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417892581	win: 14480	A
0.083233	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417894029 : 1417895477	1315338151	win: 5792	A
0.096728	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417896925 : 1417898373	1315338151	win: 5792	A
0.103439	192.168.1.200	->	192.168.1.201	1500	TCP	80	4105	1417898373 : 1417899821	1315338151	win: 5792	A
0.103780	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417894029	win: 17376	A
0.106534	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417898373	win: 21720	A
0.133408	192.168.1.200	->	192.168.1.201	776	TCP	80	4105	1417904165 : 1417904889	1315338151	win: 5792	FPA
0.139200	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417904165	win: 21720	A
0.140447	192.168.1.201	->	192.168.1.200	52	TCP	4105	80	1315338151 : 1315338151	1417904890	win: 21720	FA
0.144254	192.168.1.200	->	192.168.1.201	52	TCP	80	4105	1417904890 : 1417904890	1315338152	win: 5792	A

Flow summary (e.g., NetFlow record or Bro connection log entry):
0.000000 192.168.1.201 4105 192.168.1.200 80 0.144254 10 77 11 16654 SF

UNIVERSITY OF CALGARY

Example: wireshark



UNIVERSITY OF CALGARY

Some Technical Challenges

- Speed:
  - Real-time collection/analysis at network link speeds
  - Sheer volume of traffic on an enterprise-level network
- Information collection:
  - Headers only versus full payloads
  - Flow-level versus packet-level analysis
- Storage:
  - Short-term versus long-term data collection
- Miscellaneous:
  - Middleboxes (NAT, DHCP, VPN, firewalls); WiFi; IP subnets
  - End-to-end encryption (HTTPS, TLS, SSL) (see [1])

UNIVERSITY OF CALGARY

Outline

- Introduction (Carey: 20 minutes)
  - Internet TCP/IP protocol stack
  - Network traffic measurement
  - Basic tools: tcpdump, wireshark
- Network Security Analysis (Martin: 20 minutes)
  - Principles and approaches
  - Advanced tools: Endace DAG, Bro (Zeek) IDS, Vertica
  - U of C network traffic overview and challenges
- U of C Case Study: Part 1 (Carey: 20 minutes)
  - Examples of normal and abnormal (malicious) traffic
- U of C Case Study: Part 2 (Martin: 20 minutes)
  - More examples of malicious traffic
- Q&A

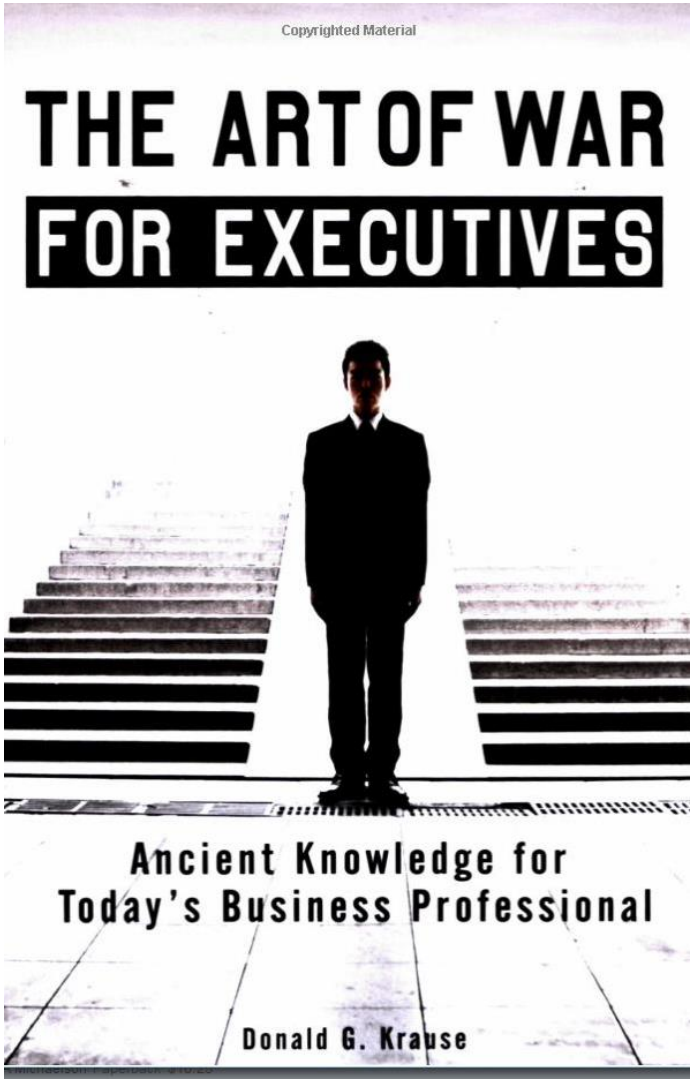
Guiding Principle #1

"Know your enemy and yourself."

Sun Tzu

General and Military Strategist

(Ancient China)



"Organizations know which technologies they intended to use on their network;

hackers/nation states know which technologies are actually in use on that network."

Rob Joyce

Tailored Access Operations

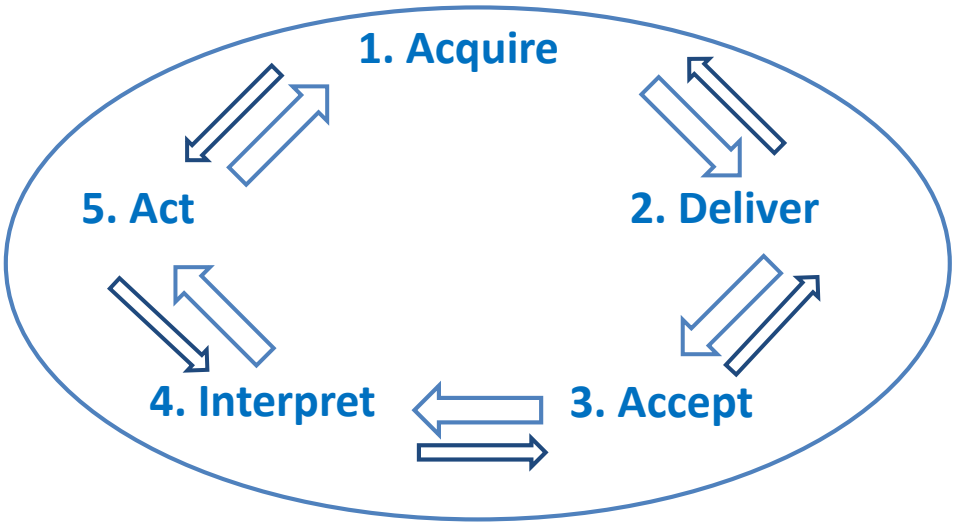
National Security Agency

(USENIX Enigma Conference 2016)

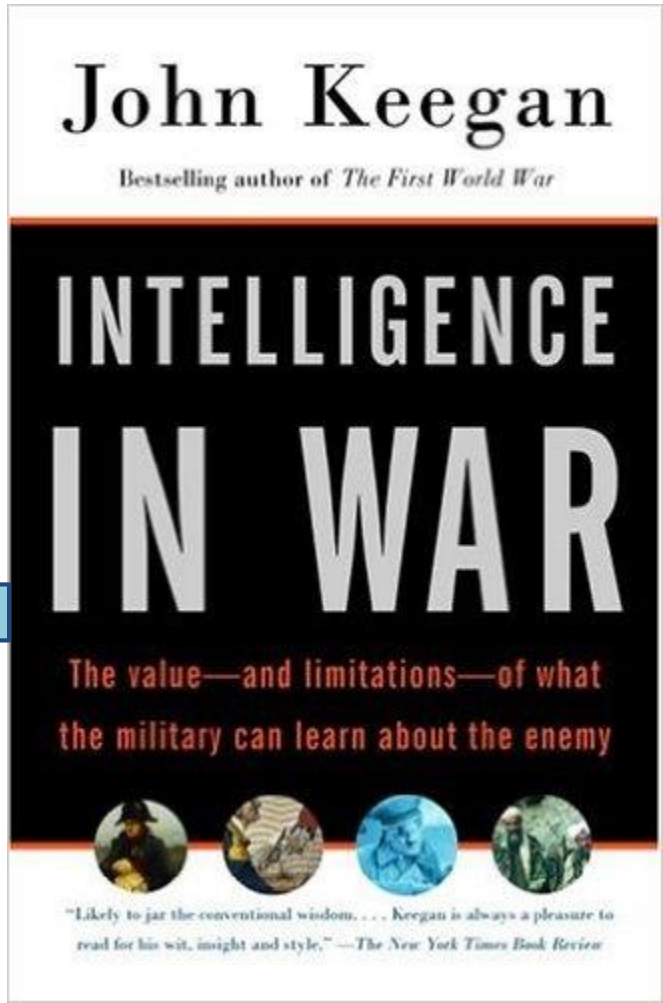
Guiding Principle #2

"All models are wrong, but some are useful."

-George Box, Statistician (1919-2013)



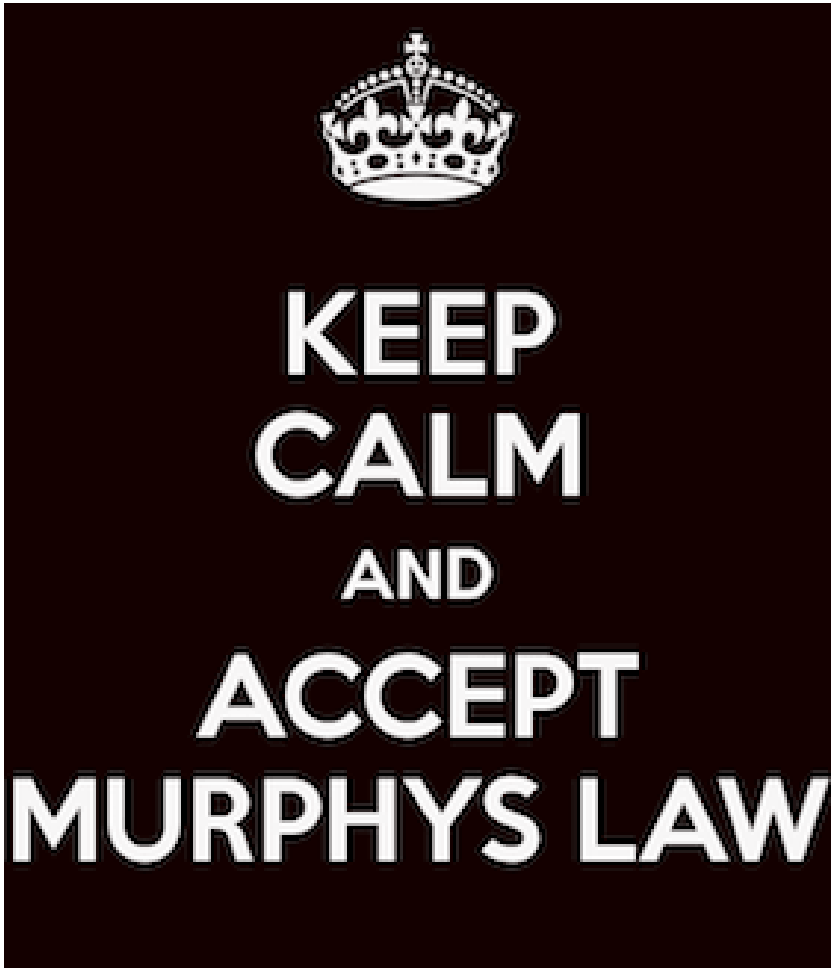
"Sequence of effective intelligence operations"
(or "Intelligence lifecycle")



Guiding Principle #3

"Anything that can go wrong will go wrong."

-Murphy's Law

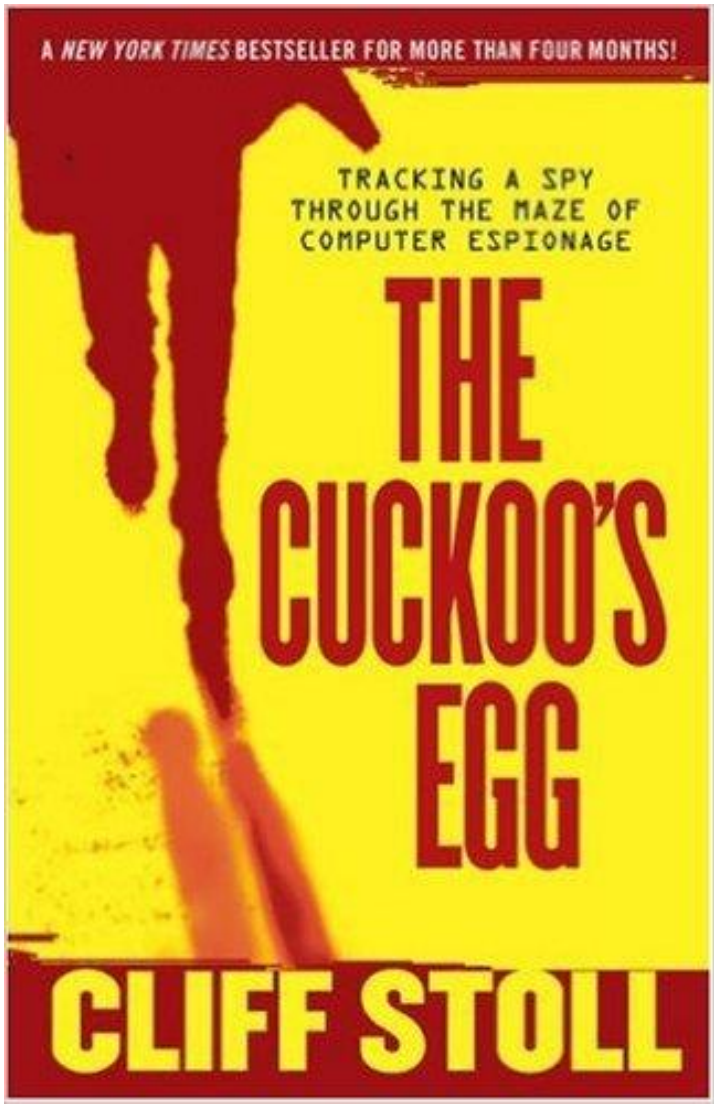


This applies to all stages of the intelligence lifecycle, but it is especially applicable to data collection.

Guiding Principle #4

"A small leak will sink a great ship."

-Benjamin Franklin



Security analytics is like searching for needles in a giant haystack.
(Vertica is a great tool for doing this)

An Analogy: Power Signals

- Disaggregating an aggregation of signals

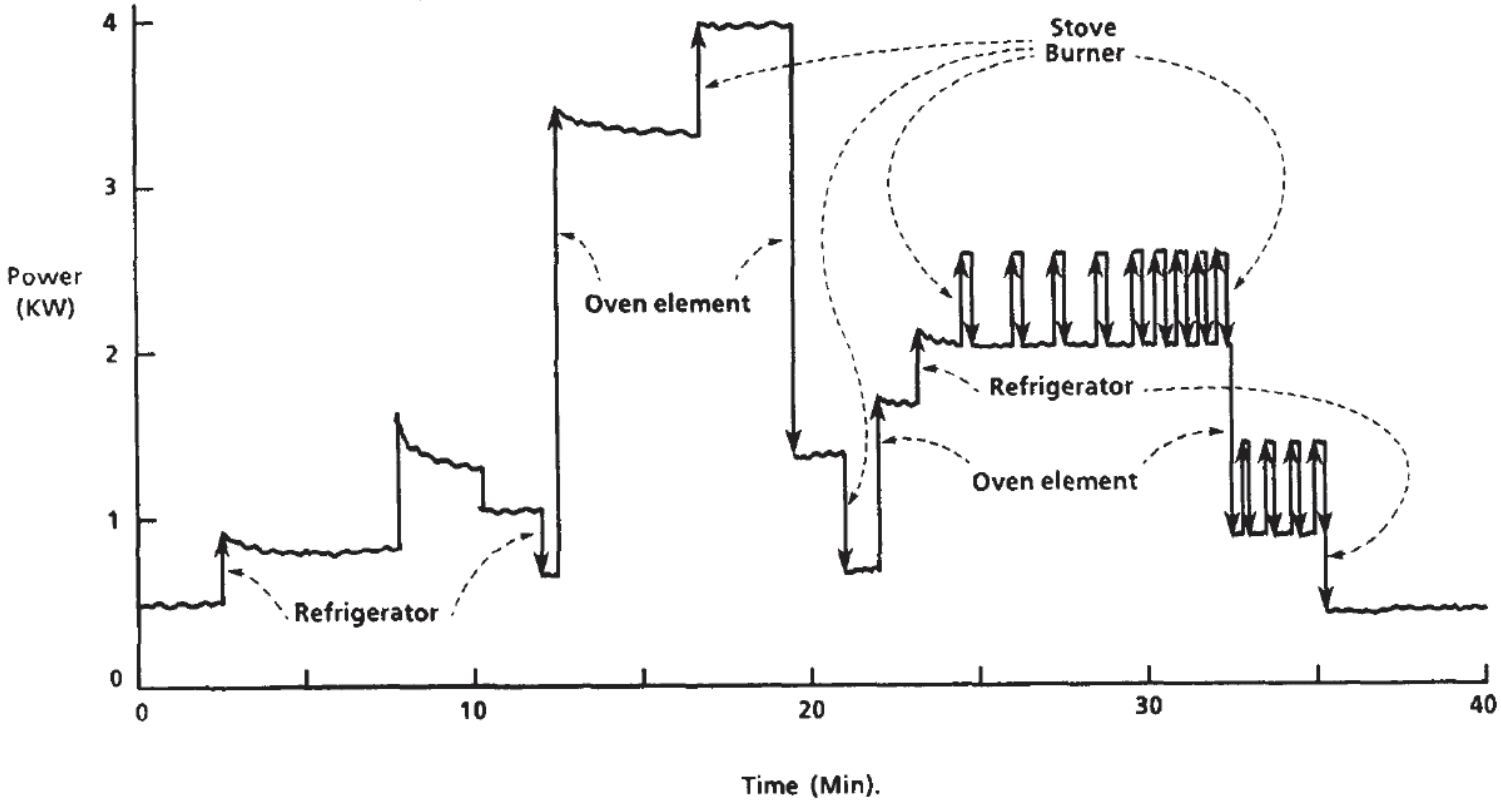
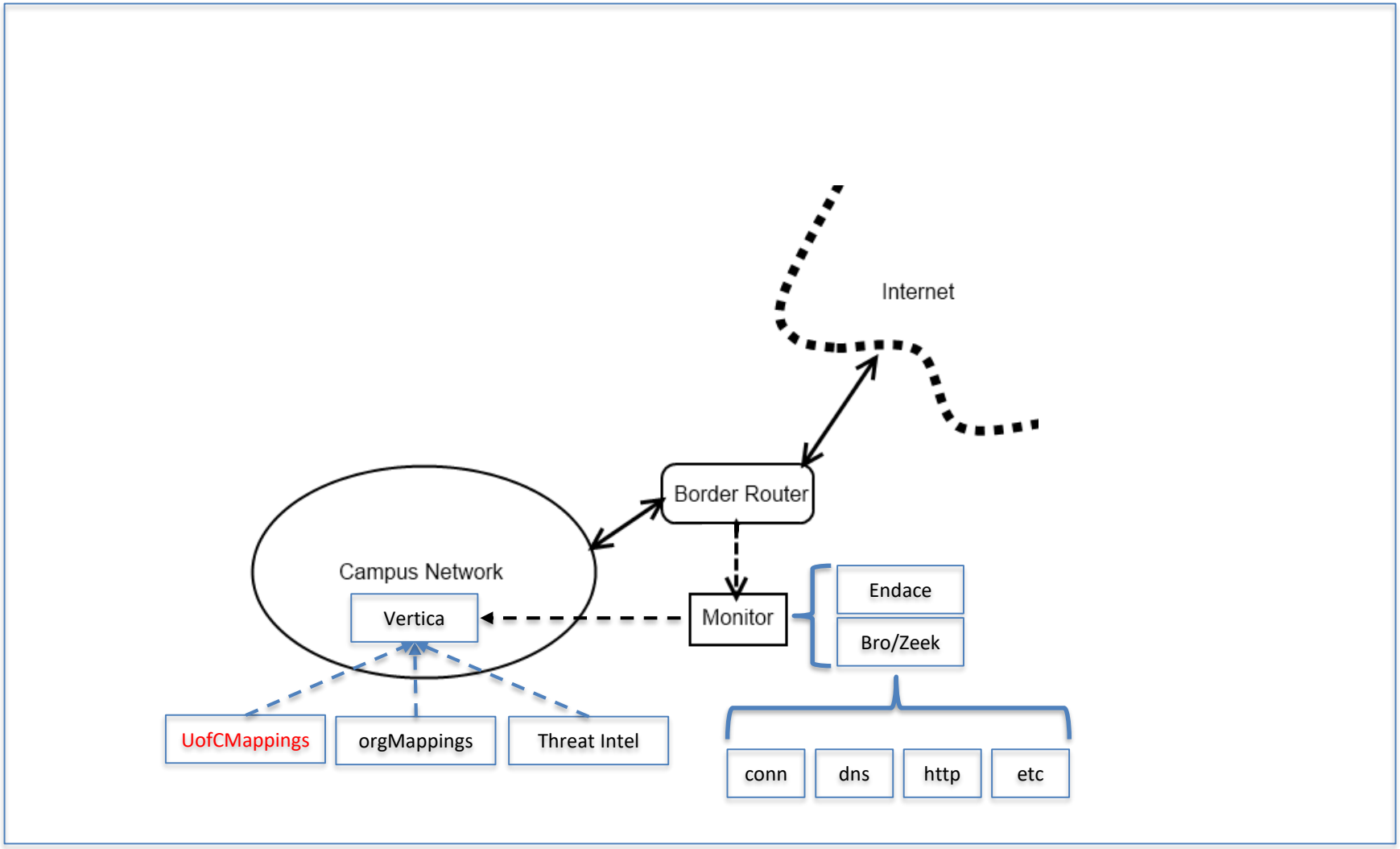


Fig. 2. Power versus time (total load) shows step changes due to individual appliance events.

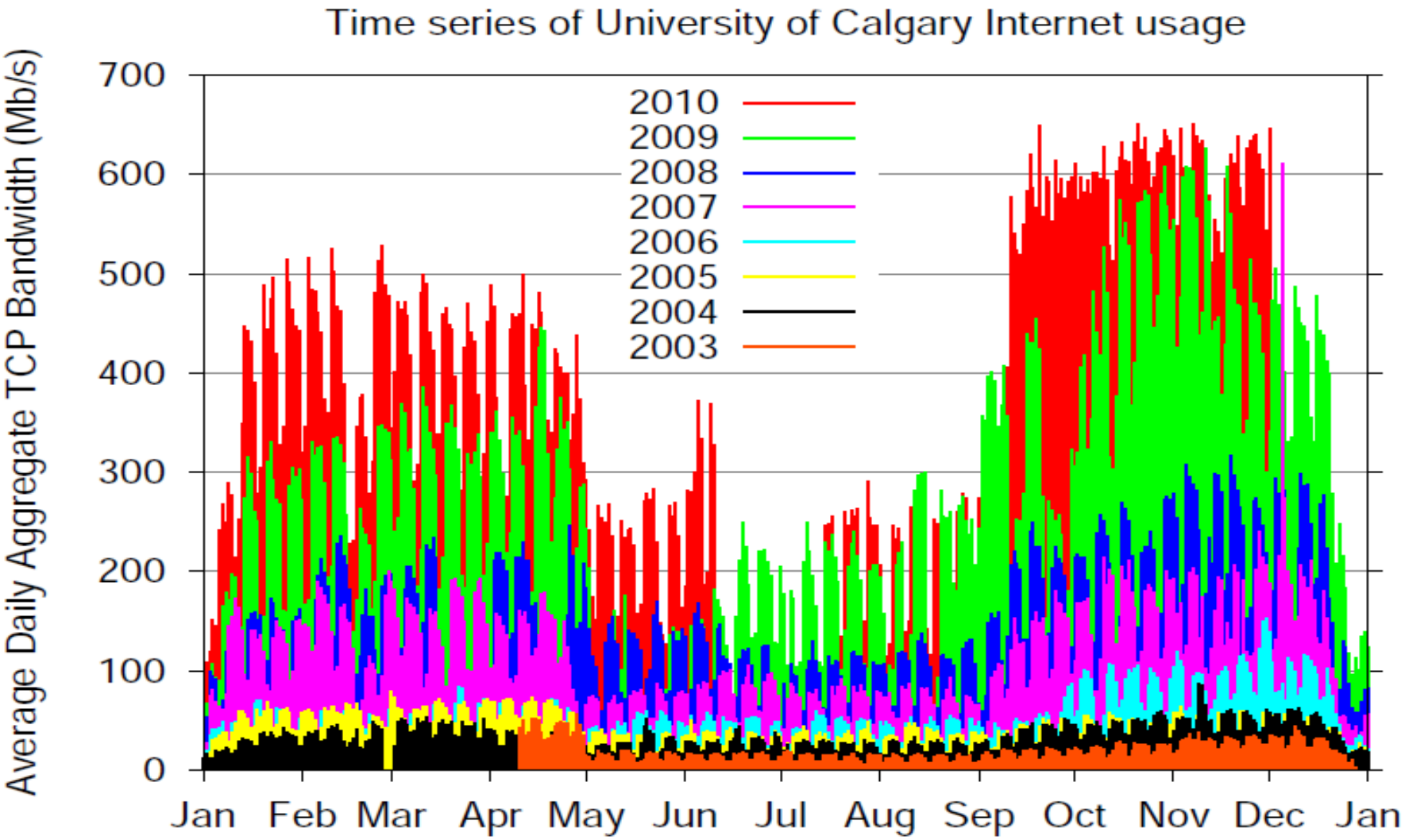
G. Hart, "Nonintrusive Application Load Monitoring", Proceedings of the IEEE, 1992.

U of C Monitoring & Analysis Infrastructure

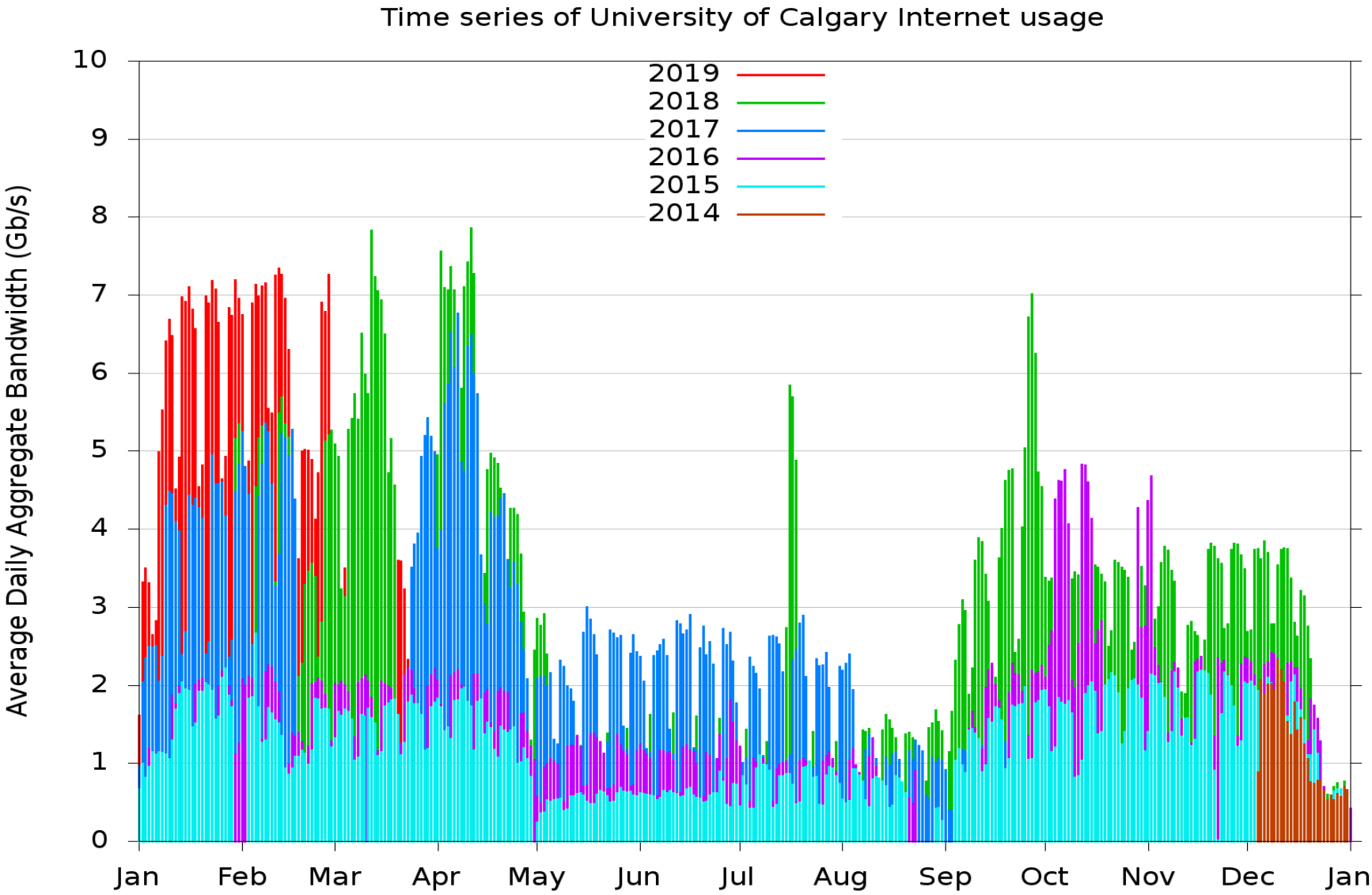


UNIVERSITY OF CALGARY

Data Acquisition (2003-2010)

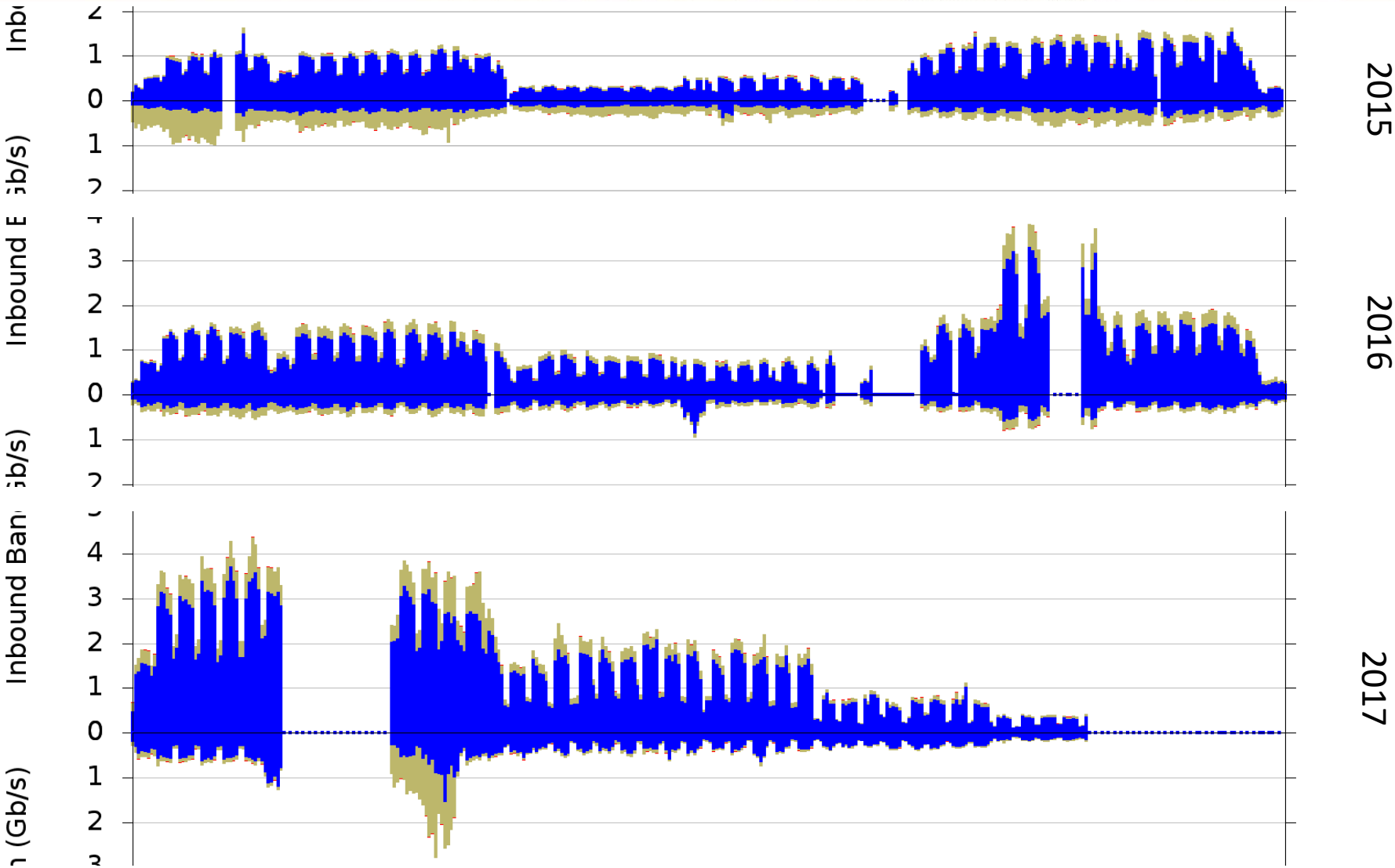


Data Acquisition (2014-present)

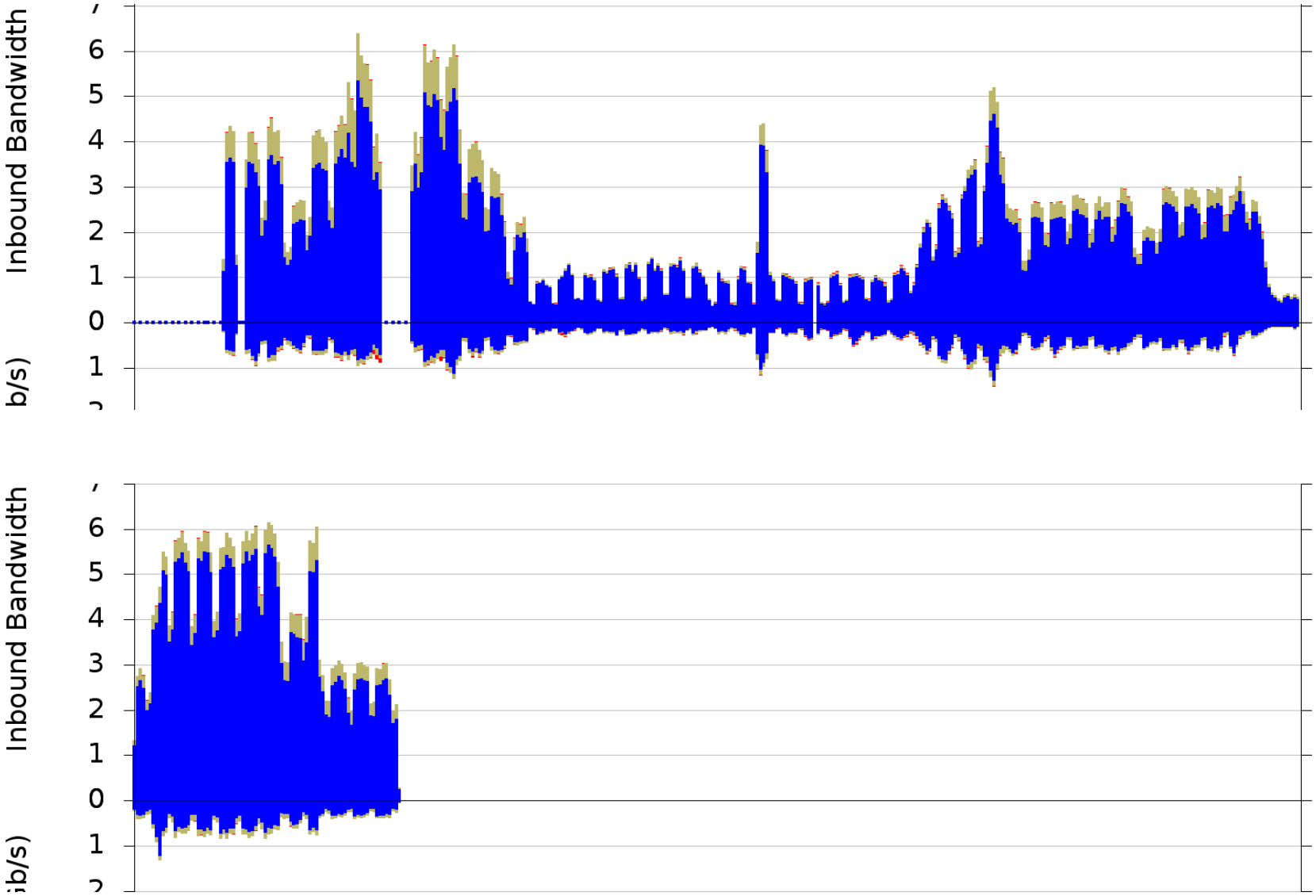


UNIVERSITY OF CALGARY

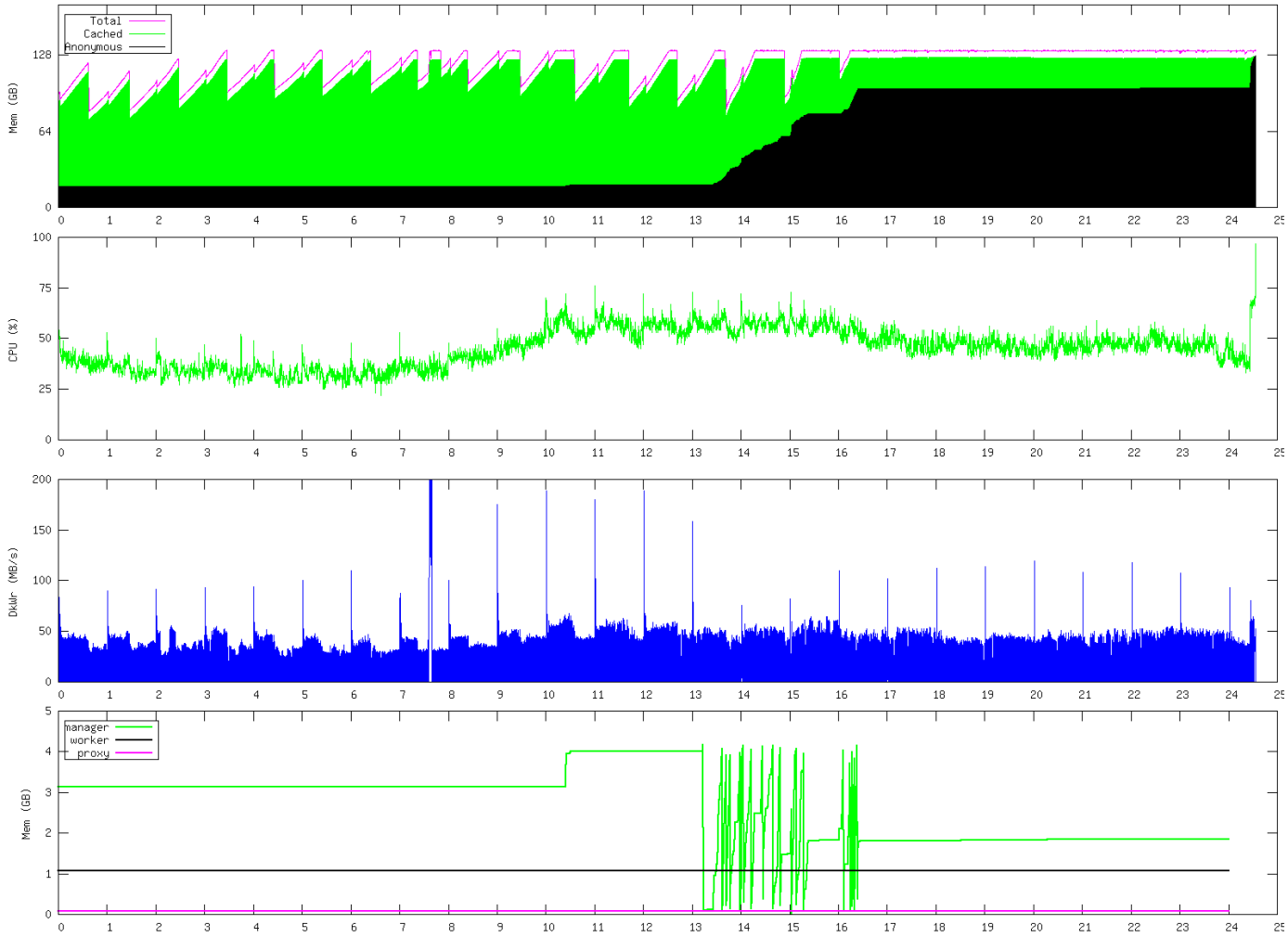
Data Acquisition (2015-2017)



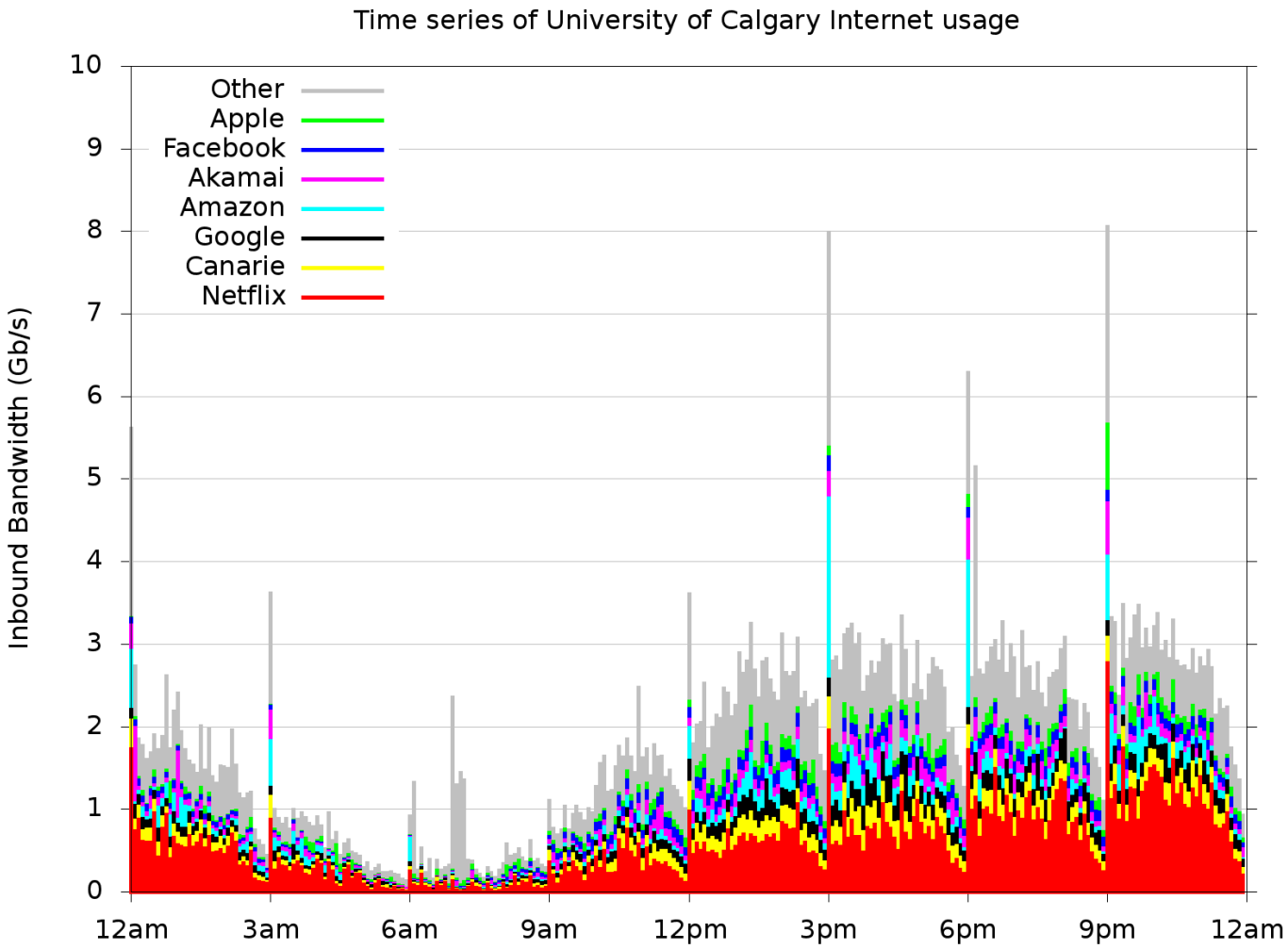
Data Acquisition (2018-2019)



(Another) Data Acquisition Challenge



Data Acceptance & Interpretation



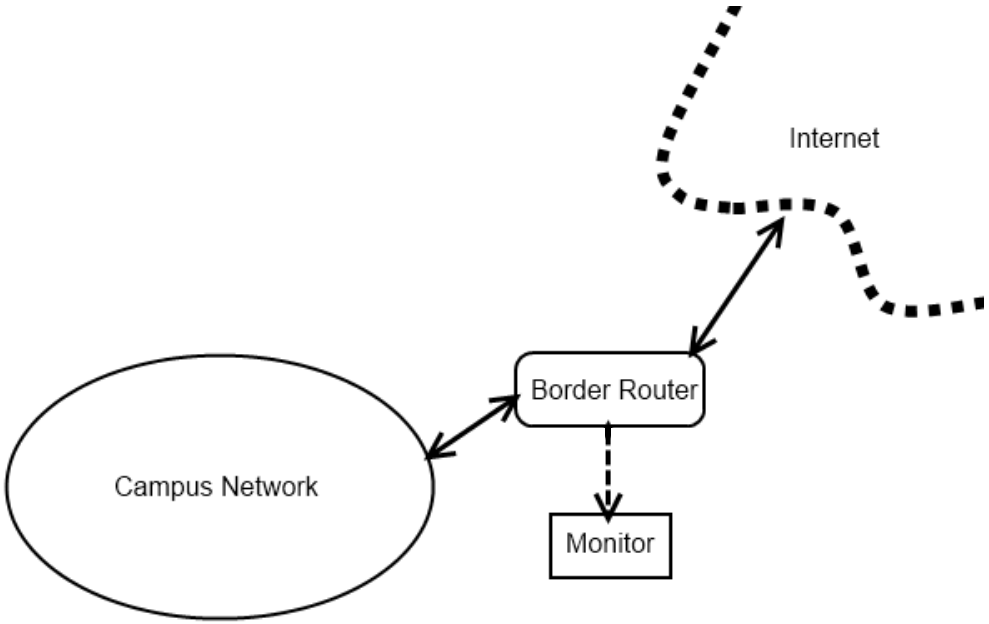
UNIVERSITY OF CALGARY

Outline

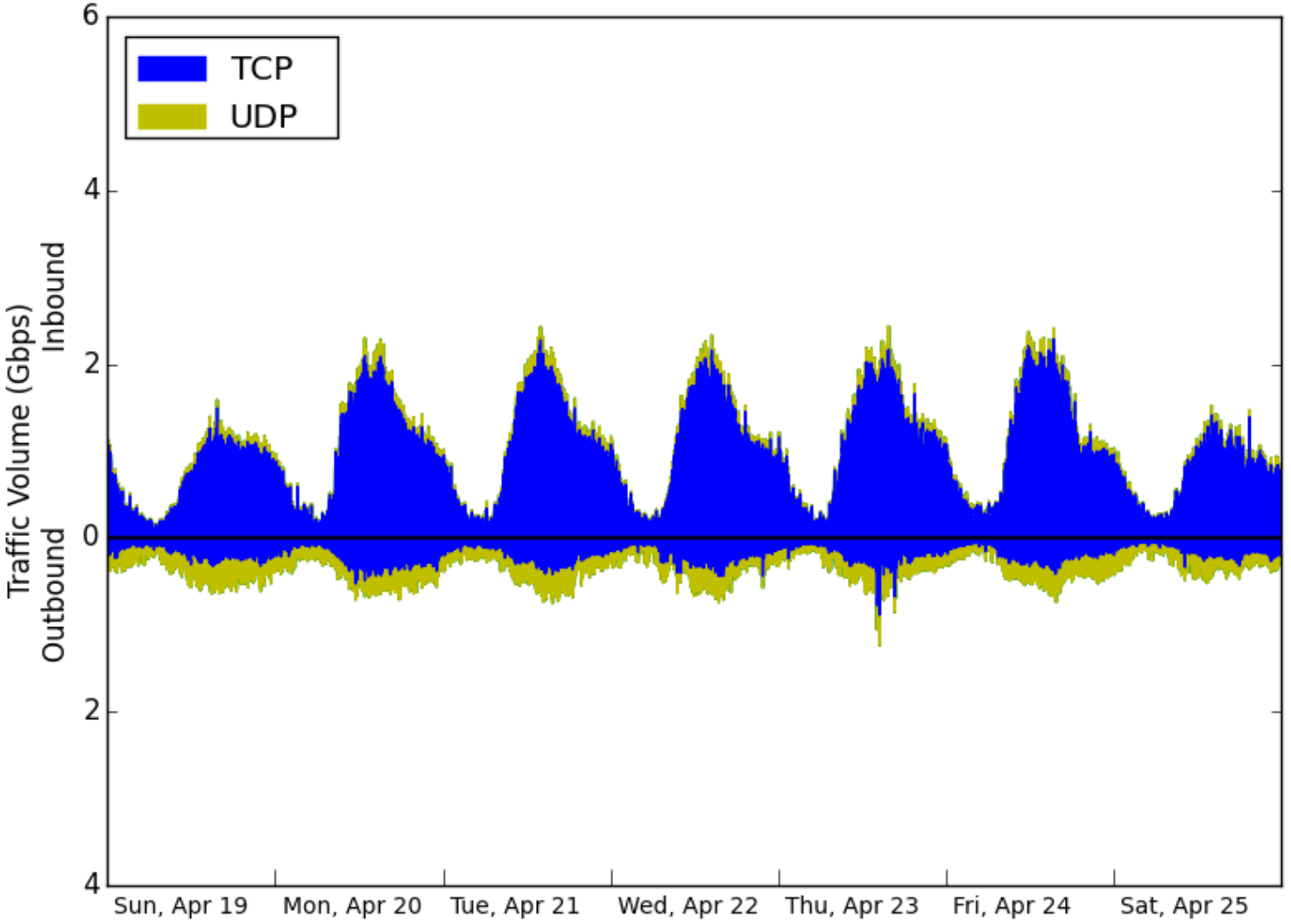
- Introduction (Carey: 20 minutes)
  - Internet TCP/IP protocol stack
  - Network traffic measurement
  - Basic tools: tcpdump, wireshark
- Network Security Analysis (Martin: 20 minutes)
  - Principles and approaches
  - Advanced tools: Endace DAG, Bro (Zeek) IDS, Vertica
  - U of C network traffic overview and challenges
- U of C Case Study: Part 1 (Carey: 20 minutes)
  - Examples of normal and abnormal (malicious) traffic
- U of C Case Study: Part 2 (Martin: 20 minutes)
  - More examples of malicious traffic
- Q&A

Methodology

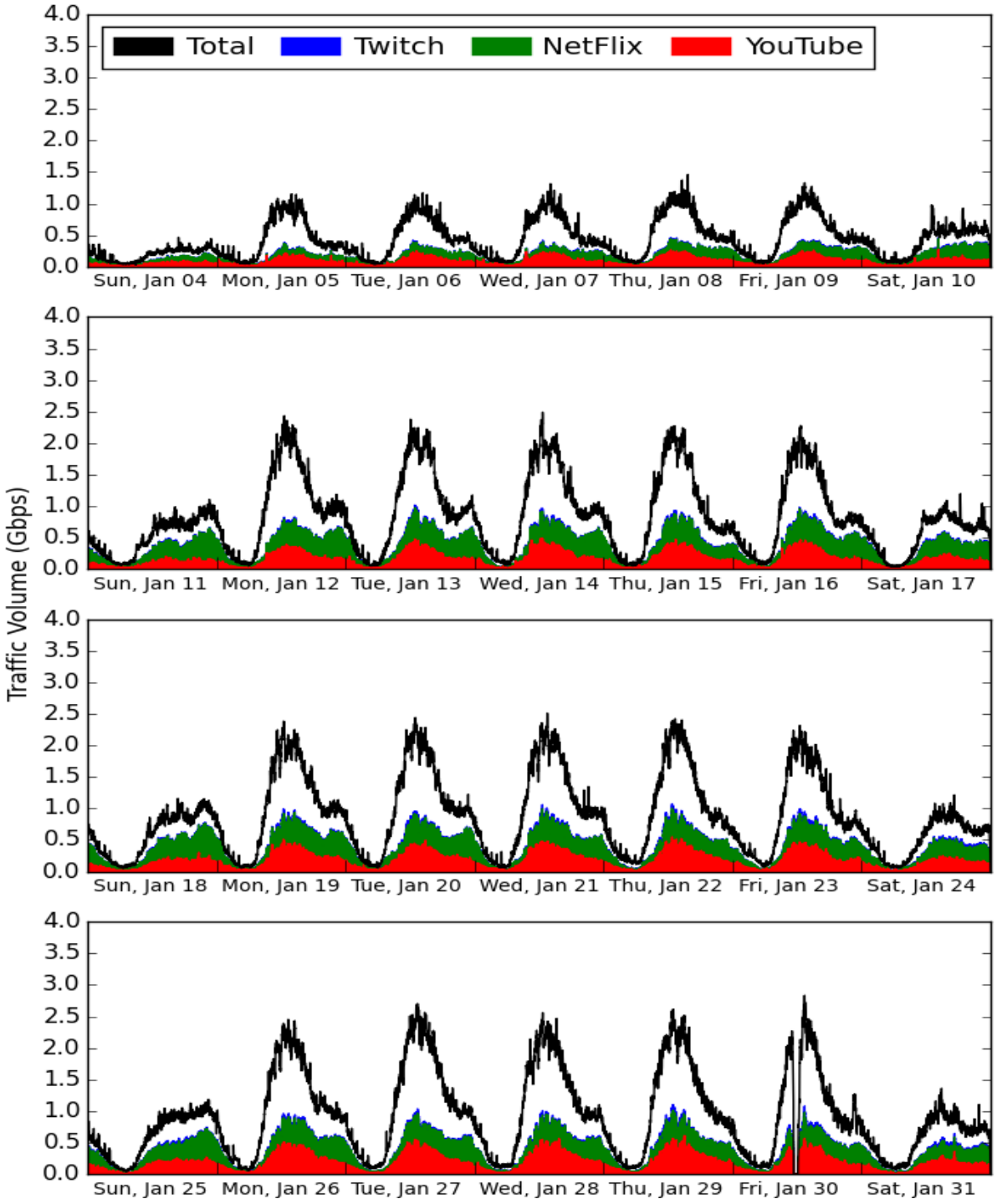
- Passive network traffic measurement
- Hardware: Endace DAG packet capture card
- Software: Bro IDS network security monitor (see [6])
- About 15 years of data
- Analysis of TCP connection and HTTP transaction logs



Overview of Traffic Volume (April 2015)

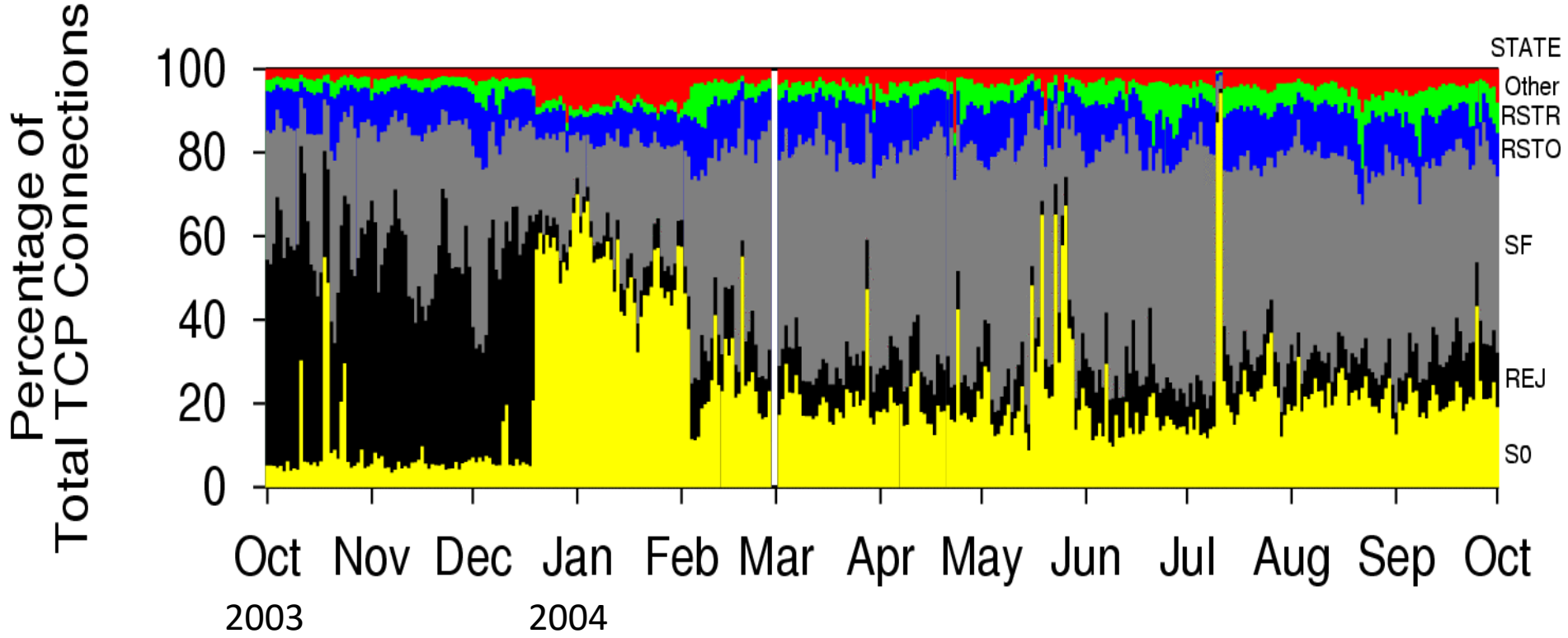


Video Streaming



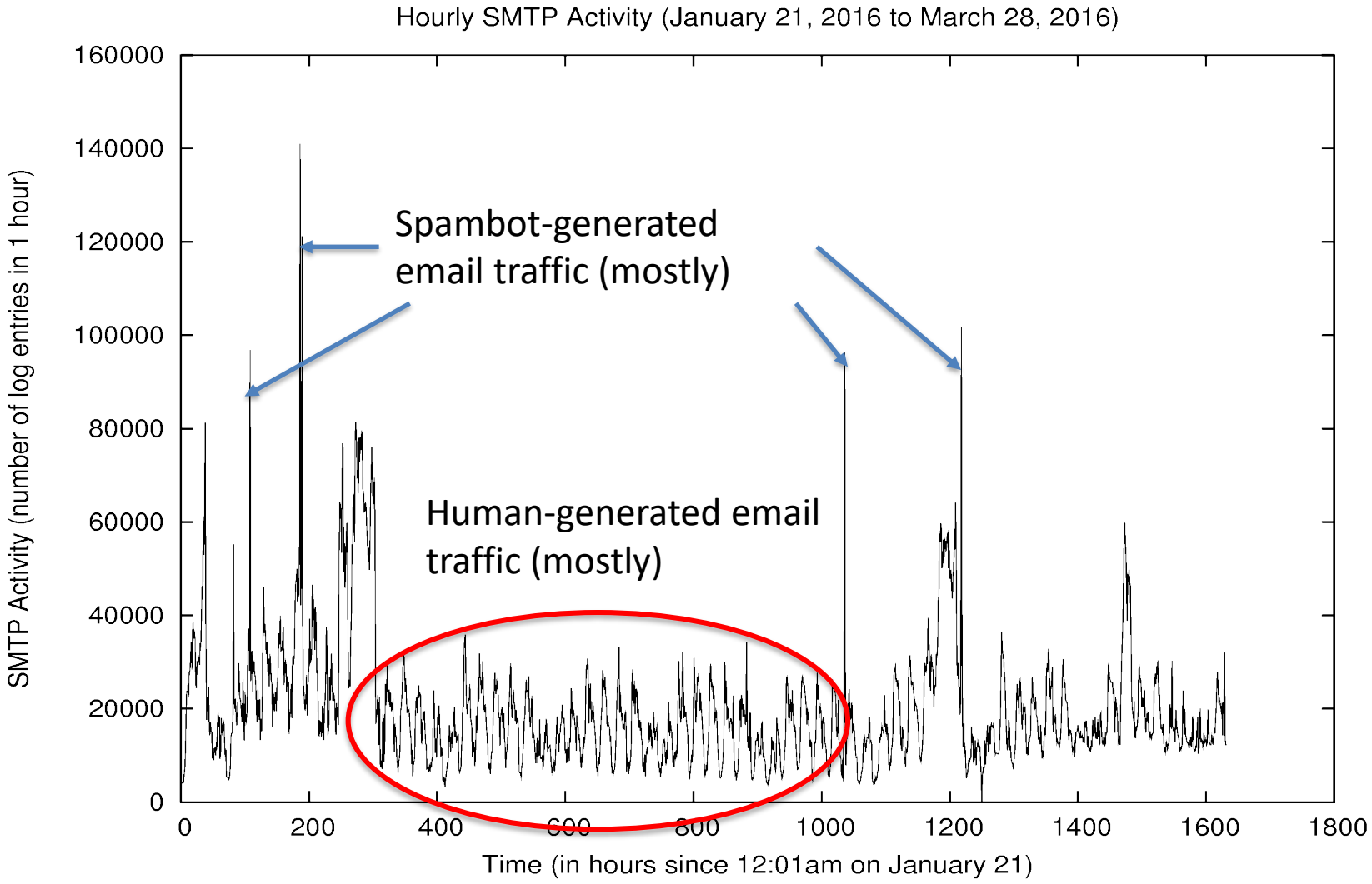
- January 2015
- Top line (Total) is HTTP+HTTPS
- Blue is Twitch
- Green is Netflix (HTTP)
- Red is YouTube (HTTPS)

Example 1: TCP Connection State Analysis (1 yr)

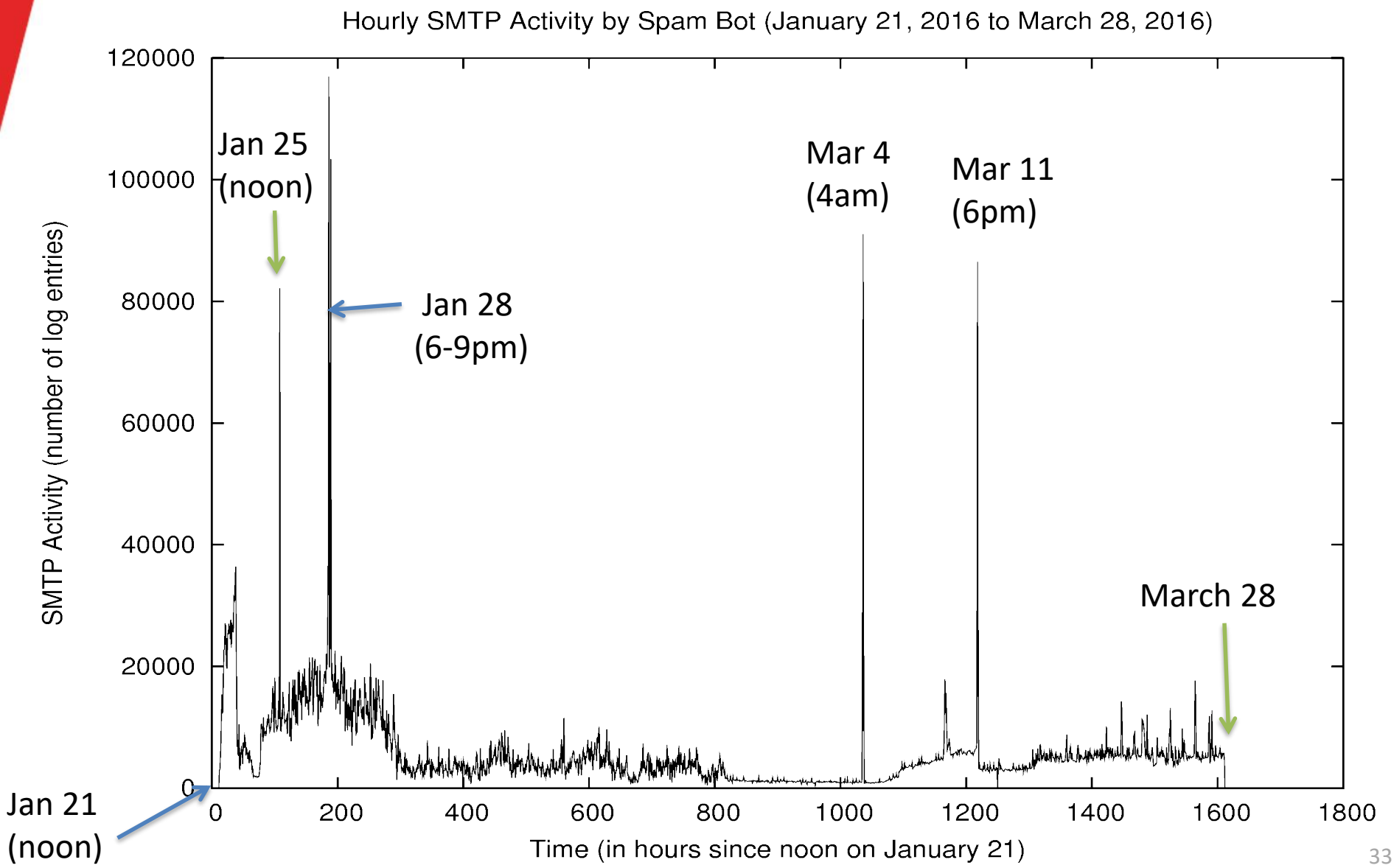


M. Arlitt and C. Williamson, "An Analysis of TCP Reset Behaviour on the Internet", ACM Computer Communication Review, Vol. 35, No. 1, pp. 37-44, January 2005

Example 2: SMTP (email) Traffic Activity



Example 3: Email Spam Bot Activity

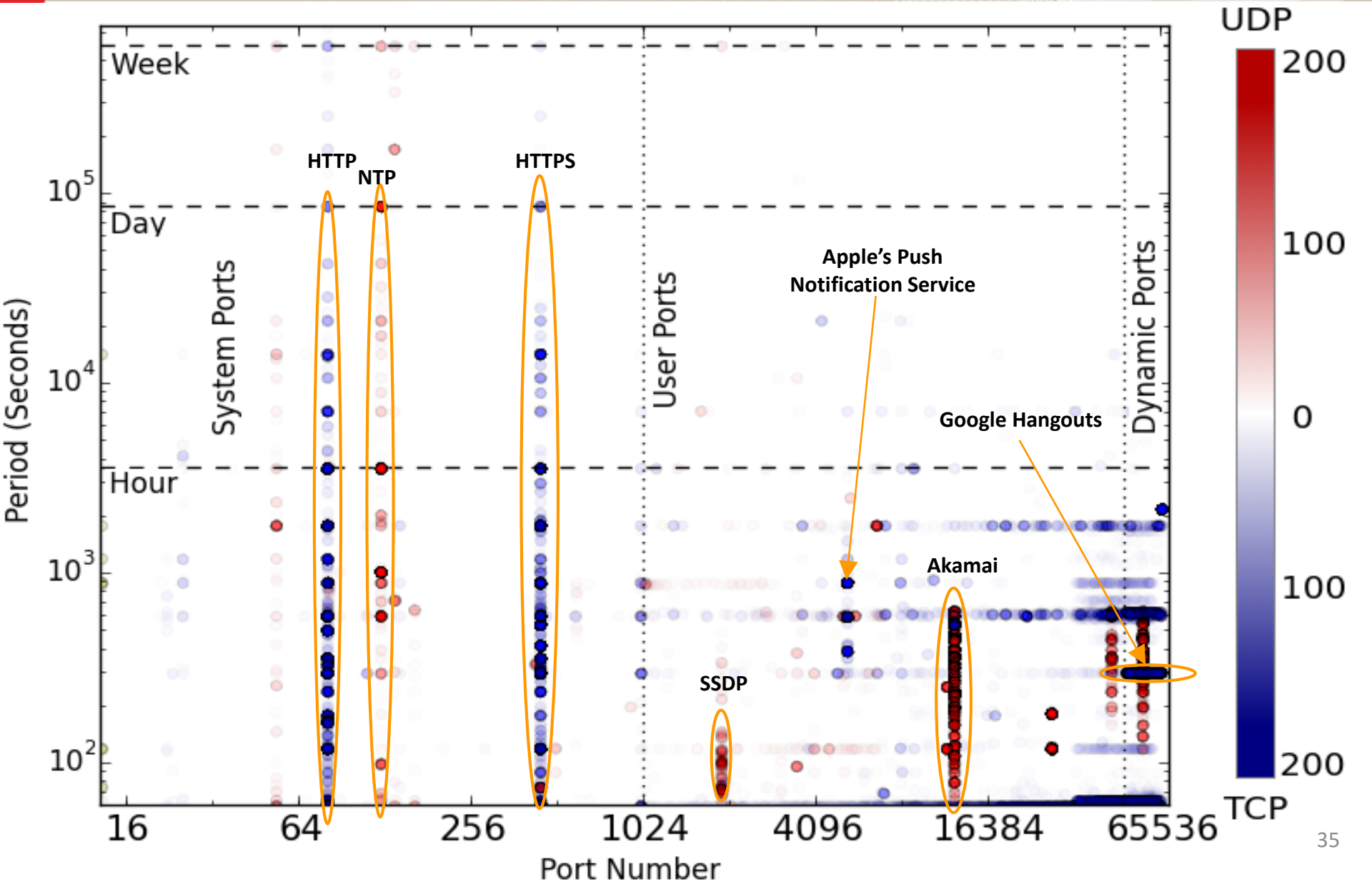


Example 4: Periodic Traffic Analysis (1 of 3)

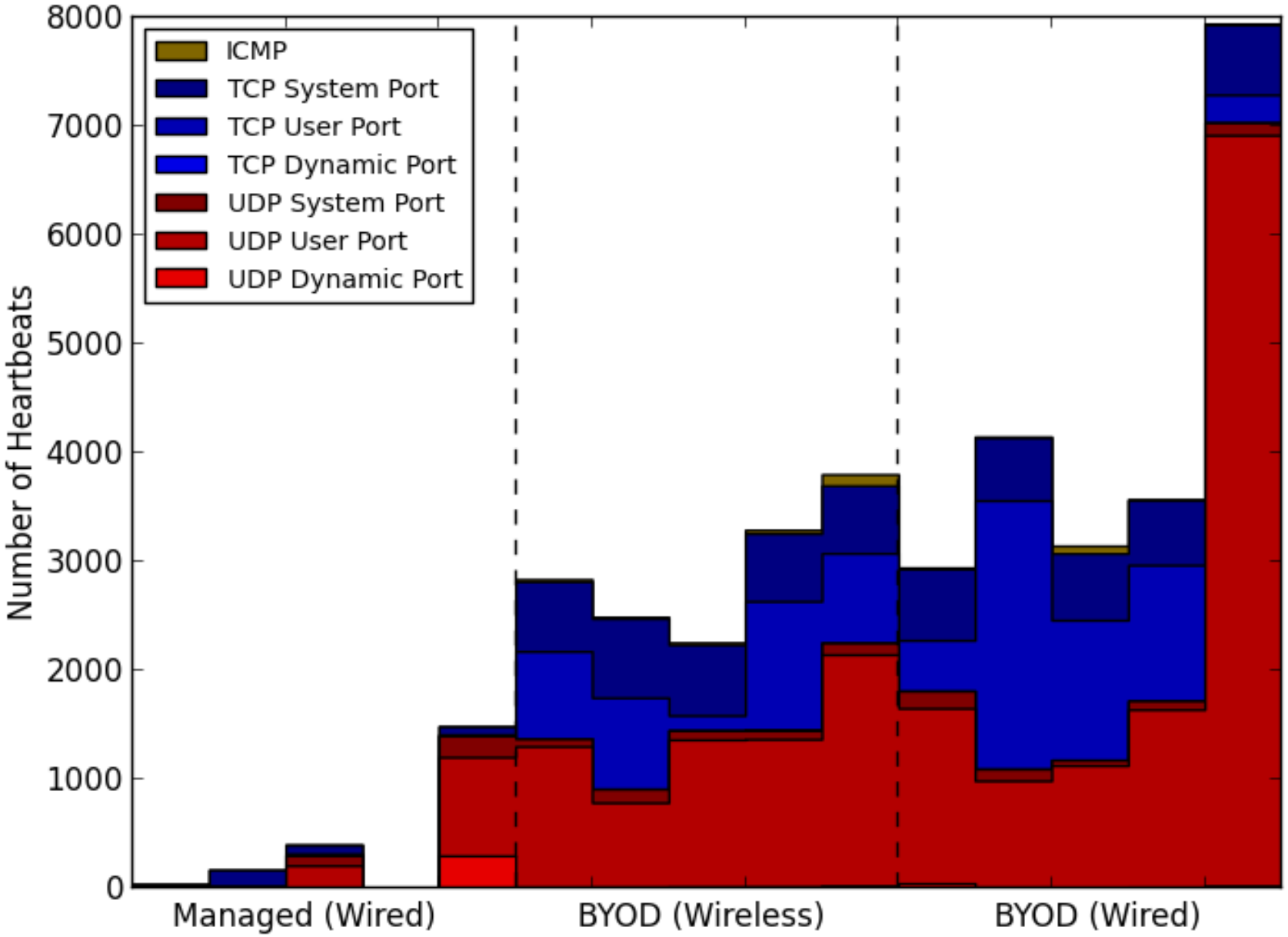
Time	IP Source Addr	Port	IP Dest Addr	Port	Duration	PS	PR	BS	BR	State
0.000000	192.168.1.201	4105	192.168.1.200	80	0.144254	10	77	11	16654	SF
0.237814	192.168.1.285	7336	192.168.1.200	80	2.765018	32	105	937	87932	SF
0.589206	192.168.1.141	1060	192.168.1.200	80	0.842541	15	26	361	37850	SF
0.837142	192.168.1.251	8109	192.168.1.200	80	0.713306	12	54	110	32768	RST
1.249788	192.168.1.281	7206	192.168.1.200	80	1.517842	81	340	1096	181654	SF
1.742355	192.168.1.271	4812	192.168.1.200	80	0.642311	15	71	82	3784	SF
2.168283	192.168.1.146	1090	192.168.1.200	80	5.254088	10	385	36	20176	SF
2.577825	192.168.1.285	7339	192.168.1.200	80	0.034217	7	46	18	9184	SF
3.492006	192.168.1.236	3607	192.168.1.200	80	0.594426	18	61	105	5408	SF
4.587426	192.168.1.141	1061	192.168.1.200	80	0.331344	11	20	28	12716	SF
5.824413	192.168.1.231	6022	192.168.1.200	80	0.680049	24	75	31	18533	SF
6.073508	192.168.1.104	8704	192.168.1.200	80	0.913426	27	37	88	14236	SF
7.198741	192.168.1.251	8122	192.168.1.200	80	1.744125	52	128	238	75890	SF
7.363601	192.168.1.281	7218	192.168.1.200	80	0.164425	12	8	22	6654	RST
8.597769	192.168.1.141	1063	192.168.1.200	80	0.517756	18	119	310	15024	SF
8.370944	192.168.1.271	4818	192.168.1.200	80	0.027399	6	30	45	18324	SF
9.127458	192.168.1.235	4093	192.168.1.200	80	2.044254	35	264	212	172654	SF
9.627145	192.168.1.281	7225	192.168.1.200	80	0.283158	15	46	53	18498	SF

[3] M. Haffey, M. Arlitt, and C. Williamson, "Modeling, Analysis, and Characterization Of Periodic Network Traffic", IEEE MASCOTS 2018, Milwaukee, WI, September 2018.

Example 4: Periodic Traffic Analysis (2 of 3)



Example 4: Periodic Traffic Analysis (3 of 3)

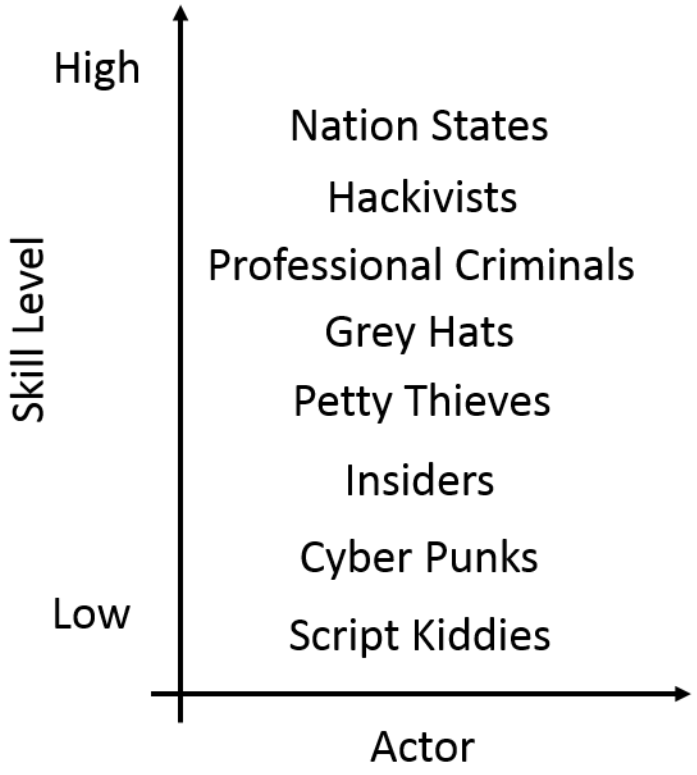


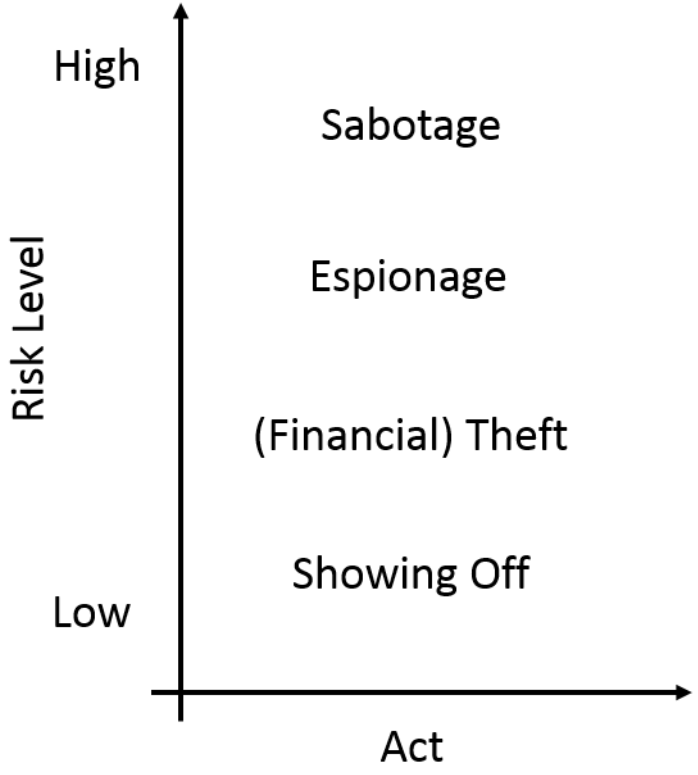
UNIVERSITY OF CALGARY

Outline

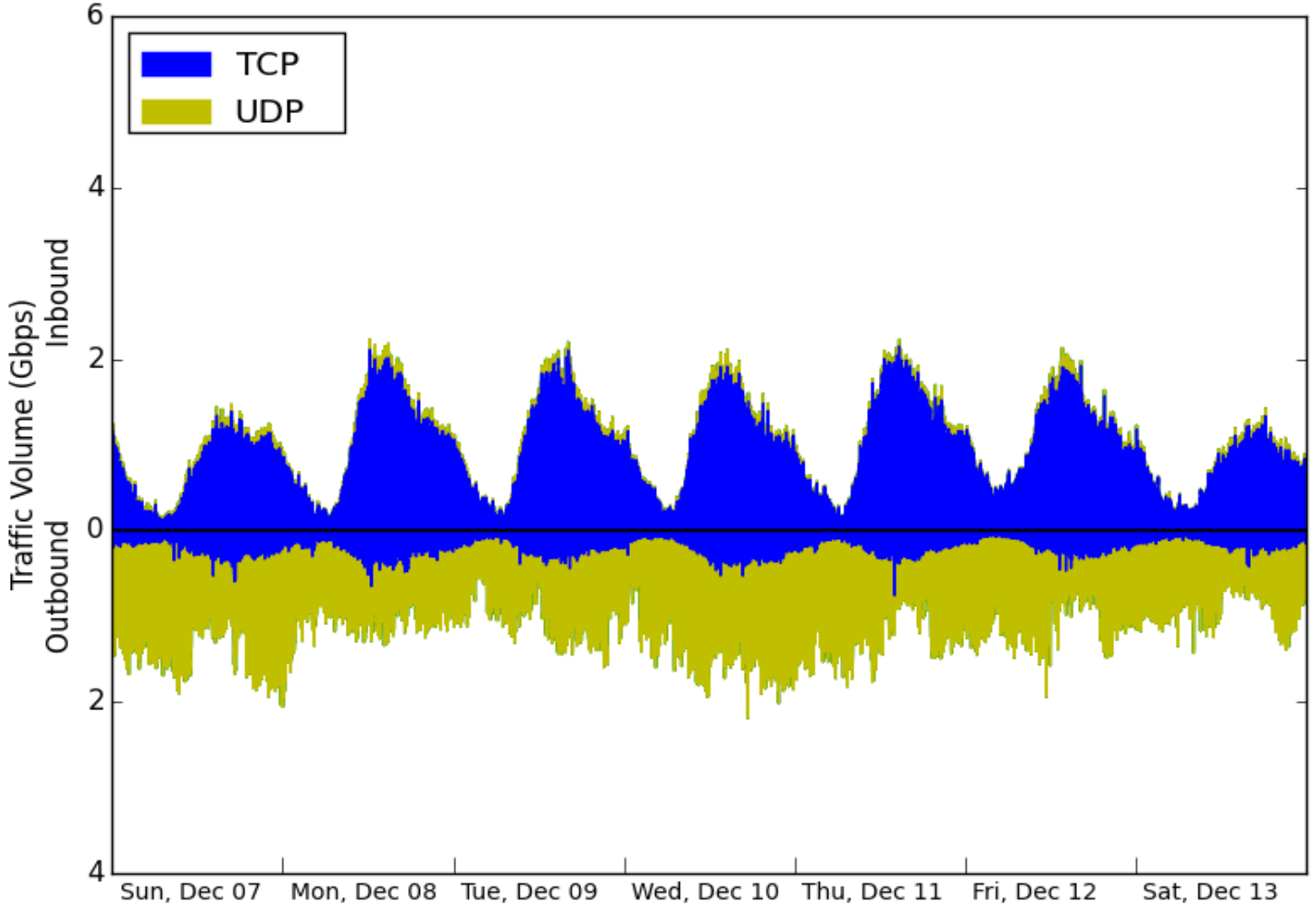
- Introduction (Carey: 20 minutes)
  - Internet TCP/IP protocol stack
  - Network traffic measurement
  - Basic tools: tcpdump, wireshark
- Network Security Analysis (Martin: 20 minutes)
  - Principles and approaches
  - Advanced tools: Endace DAG, Bro (Zeek) IDS, Vertica
  - U of C network traffic overview and challenges
- U of C Case Study: Part 1 (Carey: 20 minutes)
  - Examples of normal and abnormal (malicious) traffic
- U of C Case Study: Part 2 (Martin: 20 minutes)
  - More examples of malicious traffic
- Q&A

Who and what we are up against





Example 5: NTP Amplification Attack (Dec 2014)



Example 5B: HTTP DDoS participation (2019)

DstOrg	proto	resp_p	Srcs	Conns	OGB	RGB
OVH SAS	tcp	80	65306	390355	.0	.0
No.31,Jin-rong Street	tcp	80	58392	146205	.0	.0
Zhejiang Taobao Network Co.,Ltd	tcp	80	53471	111031	.0	.0
CHINA UNICOM China169 Backbone	tcp	80	49040	99313	.0	.0
Guangdong	tcp	80	34067	48080	.0	.0

(5 rows)

Activity from a known, unused local IP address:

ts	orig_p	DstOrg	resp_p	proto
2019-03-24 00:07:28.770651	42254	Zhejiang Taobao Network Co.,Ltd	80	tcp
2019-03-24 00:36:39.219374	52671	No.31,Jin-rong Street	80	tcp
2019-03-24 00:37:00.251778	42058	No.31,Jin-rong Street	80	tcp
2019-03-24 00:42:14.622743	57970	No.31,Jin-rong Street	80	tcp
2019-03-24 00:52:27.775738	2957	CHINA UNICOM China169 Backbone	80	tcp
2019-03-24 00:53:16.424589	39247	China Mobile communications corp	80	tcp
2019-03-24 00:54:22.264719	46864	CHINANET Guangdong province	80	tcp
2019-03-24 00:58:41.612098	18470	No.31,Jin-rong Street	80	tcp
<snip>				
2019-03-24 22:47:44.014437	28985	OVH SAS	80	tcp
2019-03-24 22:47:54.384277	51532	OVH SAS	80	tcp

(10 rows)

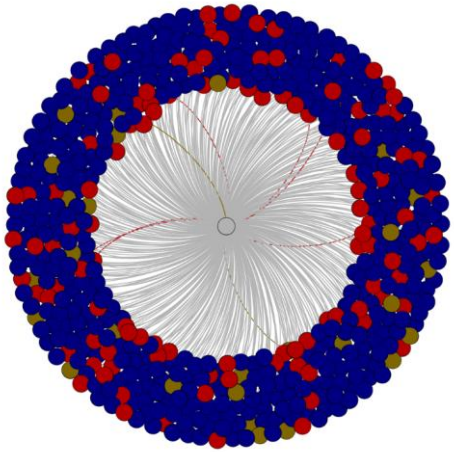
Example 6: Data Exfiltration (2019)

DstOrg	Srcs	Dsts	Services	Conns	OGB	RGB
Apple Inc.	3129	2705	52	3087969	181.4	972.9
Google LLC	3336	8413	250	7433788	170.2	1,547.0
Microsoft Corporation	3498	3916	264	4354021	136.9	165.9
Amazon.com, Inc.	27610	54749	1578	6904241	128.2	717.3
Dropbox, Inc.	1103	68	9	485147	90.6	119.0
Facebook, Inc.	29177	602	604	2217479	61.1	1,072.4
Netflix Streaming Services Inc.	906	310	4	266308	59.3	6,089.6
Shaw Communications Inc.	758	2410	2828	221592	55.1	147.0
TELUS Communications Inc.	1099	2144	2048	311961	36.7	76.4
Akamai Technologies, Inc.	6295	9468	102	2603508	28.8	449.5
Tencent Building, Kejizhongyi Avenue	1077	1850	548	918944	21.7	127.4
Twitch Interactive Inc.	224	96	3	27215	19.1	693.2
Bell Canada	16604	1880	1437	36086	15.7	34.3
No.31,Jin-rong Street	58861	48437	33480	811287	14.3	82.9
Canarie Inc	1941	22	8	449694	13.4	1,551.8
PlusServer GmbH	125	136	6	1527	13.0	.3
Comcast Cable Communications, LLC	873	5992	3086	34203	12.8	5.5
Unwired	23	245	4	6434	12.7	.2
Fastly	3055	728	9	822142	12.3	494.4
Rogers Communications Canada Inc.	626	1637	1570	87703	9.8	23.3

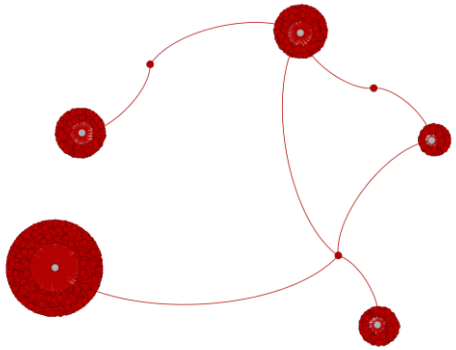
(20 rows)

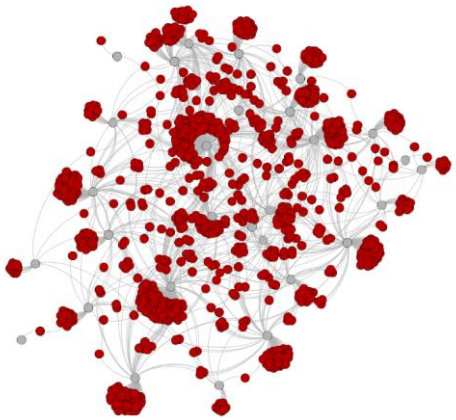
Example 7: Botnets (see [3]) (2017)

Akamai CDN node

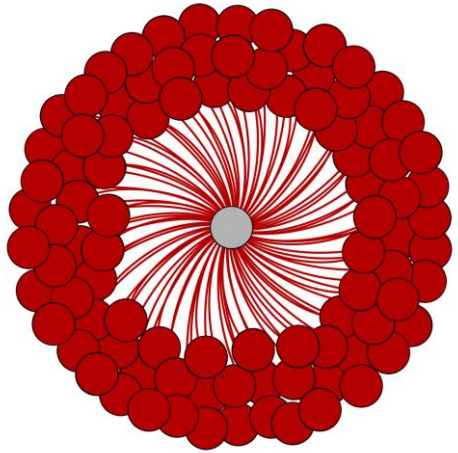


BitTorrent





Sality Botnet



ZeroAccess Botnet

Example 8: Advanced Persistent Threats (2019)

Threat Intelligence

threatName	intelSource	date	BadAddress	startAddress	endAddress
APT28	Fortinet	2018-10-12 00:00:00	179.43.158.20	179.43.158.0	179.43.158.255
APT28	Fortinet	2018-10-12 00:00:00	185.181.102.201	185.181.102.0	185.181.102.255
APT28	Fortinet	2018-10-12 00:00:00	185.183.107.40	185.183.107.0	185.183.107.255
APT28	Fortinet	2018-10-12 00:00:00	85.204.124.77	85.204.124.0	85.204.124.255
Gallmaker	Fortinet	2018-10-12 00:00:00	111.90.149.99	111.90.149.0	111.90.149.255
Gallmaker	Fortinet	2018-10-12 00:00:00	45.55.154.23	45.55.154.0	45.55.154.255
Gallmaker	Fortinet	2018-10-12 00:00:00	5.223.98.157	5.223.98.0	5.223.98.255
Gallmaker	Fortinet	2018-10-12 00:00:00	82.202.120.156	82.202.120.0	82.202.120.255
Gallmaker	Fortinet	2018-10-12 00:00:00	87.17.148.117	87.17.148.0	87.17.148.255
Gallmaker	Fortinet	2018-10-12 00:00:00	87.17.148.76	87.17.148.0	87.17.148.255
Gallmaker	Fortinet	2018-10-12 00:00:00	93.109.241.154	93.109.241.0	93.109.241.255

(11 rows)

Example 8: Advanced Persistent Threats (2019)

https://www.fireeye.com/current-threats/apt-groups.html

APT28 (aka "Tsar Team")

- **Suspected attribution:** Russian government

ts	Threat	Dst	proto	resp_p
2019-03-24 00:04:00.346623	APT28	85.204.124.82	tcp	443
2019-03-24 00:21:08.846368	APT28	185.181.102.60	tcp	443
2019-03-24 00:21:10.716686	APT28	185.181.102.60	tcp	443
2019-03-24 00:27:23.543676	APT28	185.181.102.18	icmp	1
2019-03-24 00:30:28.963384	APT28	85.204.124.38	tcp	443
2019-03-24 00:30:28.963413	APT28	85.204.124.38	tcp	443
2019-03-24 00:32:35.505192	APT28	185.181.102.18	icmp	3
2019-03-24 00:43:41.516986	APT28	85.204.124.82	tcp	443
2019-03-24 00:48:42.523358	APT28	185.181.102.18	icmp	3
2019-03-24 00:58:24.492231	APT28	185.181.102.18	icmp	0
2019-03-24 01:03:05.507413	APT28	185.181.102.18	icmp	3
2019-03-24 01:15:58.521104	APT28	185.181.102.18	icmp	3
2019-03-24 01:16:22.528087	APT28	185.181.102.18	icmp	3
2019-03-24 01:18:56.491637	APT28	185.181.102.18	icmp	3
2019-03-24 01:33:07.52546	APT28	185.181.102.18	icmp	3
2019-03-24 01:34:16.511177	APT28	185.181.102.18	icmp	10
2019-03-24 01:35:36.51376	APT28	185.181.102.18	icmp	3
2019-03-24 01:38:30.497508	APT28	185.181.102.18	icmp	3
2019-03-24 01:39:54.510276	APT28	185.181.102.18	icmp	0
2019-03-24 01:42:06.528017	APT28	185.181.102.18	icmp	3

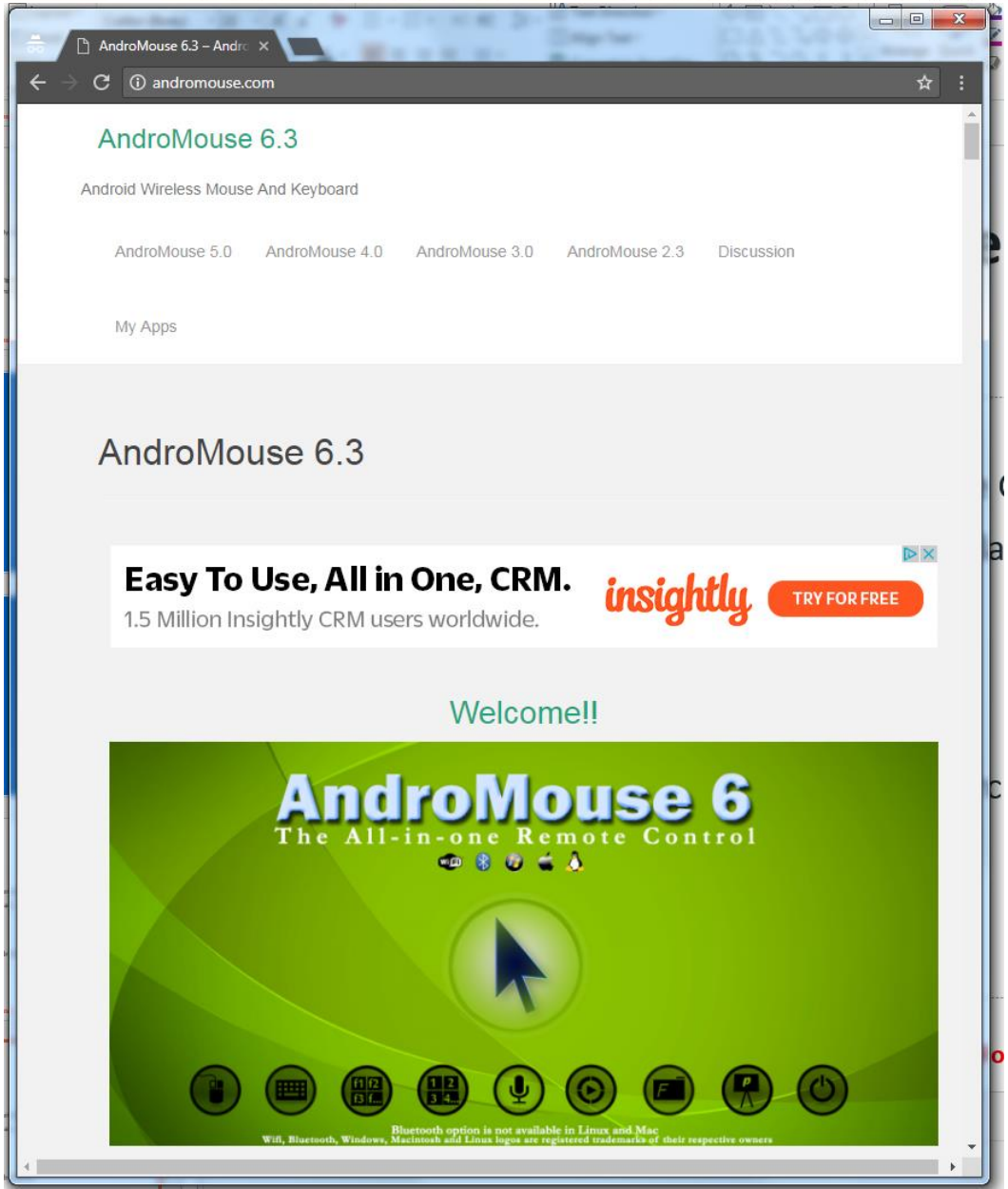
(20 rows)

Example 9: Inbound Reconnaissance Traffic (2019)

Org	Probes	Sources	Services	Destinations
4Media	55197769	1	7747	65535
OOO Network of data-centers Selectel	27950860	68	5163	65536
45.227.254.0	27225683	1	19630	65535
IP Volume inc	25879374	29	11210	65536
SS-Net	16155185	23	1848	65536
Infium, UAB	13244314	5	1557	65536
92.118.37.0	10507608	14	204	65535
ERA LLC	10405141	2	6001	65535
DigitalOcean, LLC	9926509	1965	1219	65536
FutureNow Incorporated	5389151	8	1137	65536
Novogara LTD	4417903	3	3495	65535
No.31,Jin-rong Street	4102569	66658	12693	65535
BitWeb LLC	3940653	11	136	65536
Chernyshov Aleksandr Aleksandrovich	3825759	4	70	65535
CHINA UNICOM China169 Backbone	3573076	19561	5887	65535
ColoCrossing	3166543	224	380	65536
Hurricane Electric LLC	2852790	353	92	65536
TELUS Communications Inc.	2512320	2743	1028	11579
Access2.IT Group B.V.	2300727	10	104	65535
ESTOXY OU	2216136	51	23	65536

(20 rows)

Example 9: Inbound Reconnaissance Traffic (2017)



UNIVERSITY OF CALGARY

Outline

- Introduction (Carey: 20 minutes)
  - Internet TCP/IP protocol stack
  - Network traffic measurement
  - Basic tools: tcpdump, wireshark
- Network Security Analysis (Martin: 20 minutes)
  - Principles and approaches
  - Advanced tools: Endace DAG, Bro (Zeek) IDS, Vertica
  - U of C network traffic overview and challenges
- U of C Case Study: Part 1 (Carey: 20 minutes)
  - Examples of normal and abnormal (malicious) traffic
- U of C Case Study: Part 2 (Martin: 20 minutes)
  - More examples of malicious traffic
- Q&A

UNIVERSITY OF CALGARY

References

- [1] A. Cortesi, M. Hils, T. Kriechbaumer, et al., "mitmproxy: A Free and Open Source Interactive HTTPS Proxy", 2010-2018. https://mitmproxy.org
- [2] M. Crovella and B. Krishnamurthy, *Internet Measurement: Infrastructure, Traffic, and Applications*, Wiley, 2006.
- [3] M. Haffey, M. Arlitt, and C. Williamson, "Modeling, Analysis, and Characterization of Periodic Network Traffic", Proceedings of IEEE MASCOTS 2018, Milwaukee, WI, September 2018.
- [4] R. Jain, "A Survey of Network Traffic Monitoring and Analysis Tools", https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3
- [5] J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach*, 7th edition, Pearson, 2017.
- [6] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-time", *Computer Networks*, Vol. 31, No. 23, pp. 2435-2463, December 1999.
- [7] V. Paxson, "Strategies for Sound Internet Measurement", Proceedings of ACM Internet Measurement Conference (IMC), Toarmina, Italy, October 2004.
- [8] C. Williamson, "A Tutorial on Internet Traffic Measurement", *IEEE Internet Computing*, Vol. 5, No. 6, pp. 70-74, November/December 2001.
- [9] Z. Zhang and C. Williamson, "A Campus-Level View of Outlook Email Traffic", Proceedings of the 7th International Conference on Network, Communication, and Computing (ICNCC 2018), Taipei, Taiwan, December 2018.