Deep Packet Inspection

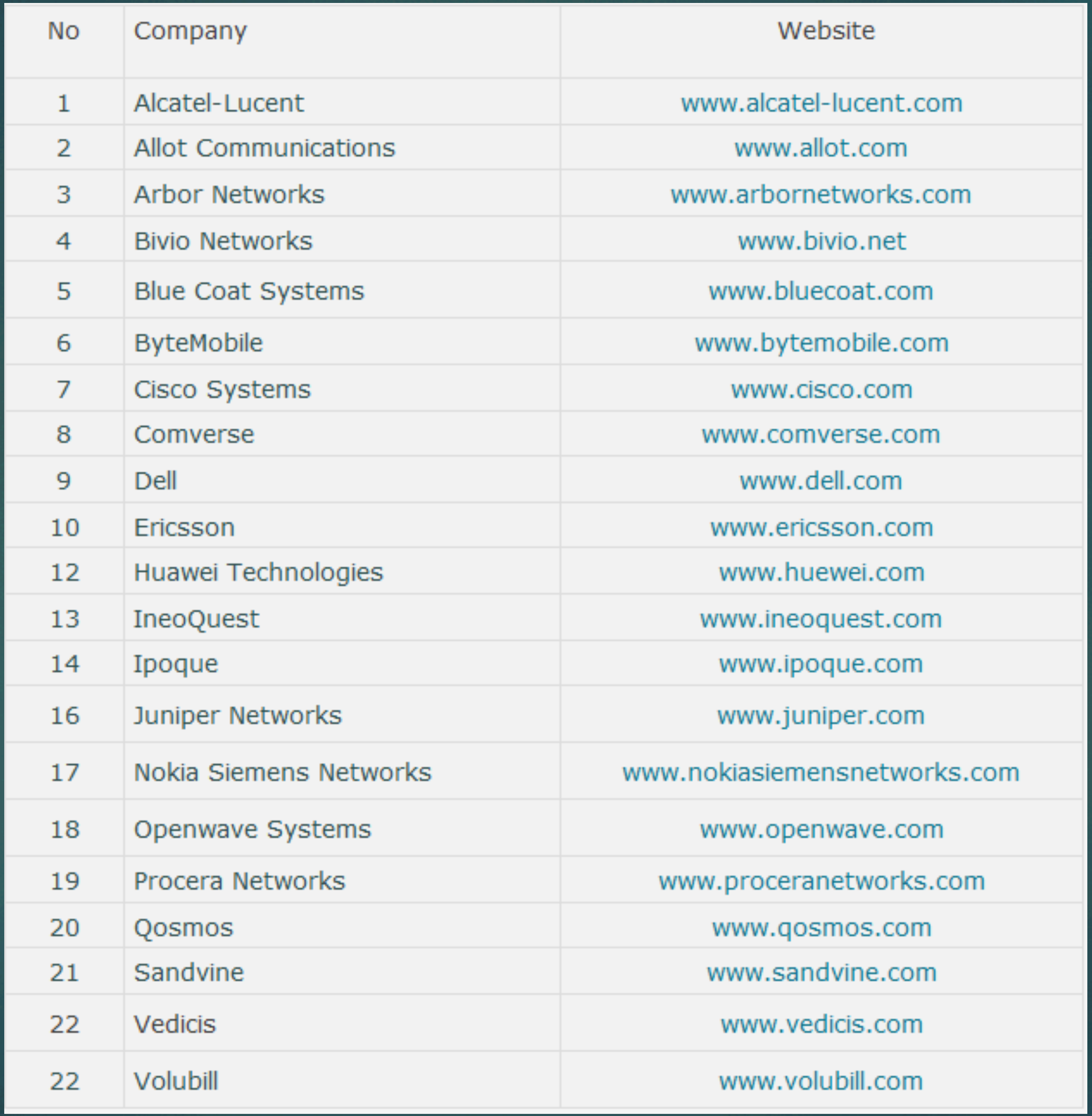
DAVID CRUZ

CPSC 457A

11/19/13

What is DPI?

- Not a technology in the traditional sense.
- Combination of existing technologies
  - Regular expressions / pattern matching
  - Packet Capture
  - Packet Sniffing
- Allows for recognition of packets
  - Manipulation
  - Notification



No	Company	Website
1	Alcatel-Lucent	www.alcatel-lucent.com
2	Allot Communications	www.allot.com
3	Arbor Networks	www.arbornetworks.com
4	Bivio Networks	www.bivio.net
5	Blue Coat Systems	www.bluecoat.com
6	ByteMobile	www.bytemobile.com
7	Cisco Systems	www.cisco.com
8	Comverse	www.comverse.com
9	Dell	www.dell.com
10	Ericsson	www.ericsson.com
12	Huawei Technologies	www.huewei.com
13	IneoQuest	www.ineoquest.com
14	Ipoque	www.ipoque.com
16	Juniper Networks	www.juniper.com
17	Nokia Siemens Networks	www.nokiasiemensnetworks.com
18	Openwave Systems	www.openwave.com
19	Procera Networks	www.proceranetworks.com
20	Qosmos	www.qosmos.com
21	Sandvine	www.sandvine.com
22	Vedicis	www.vedicis.com
22	Volubill	www.volubill.com

Beneficial Uses

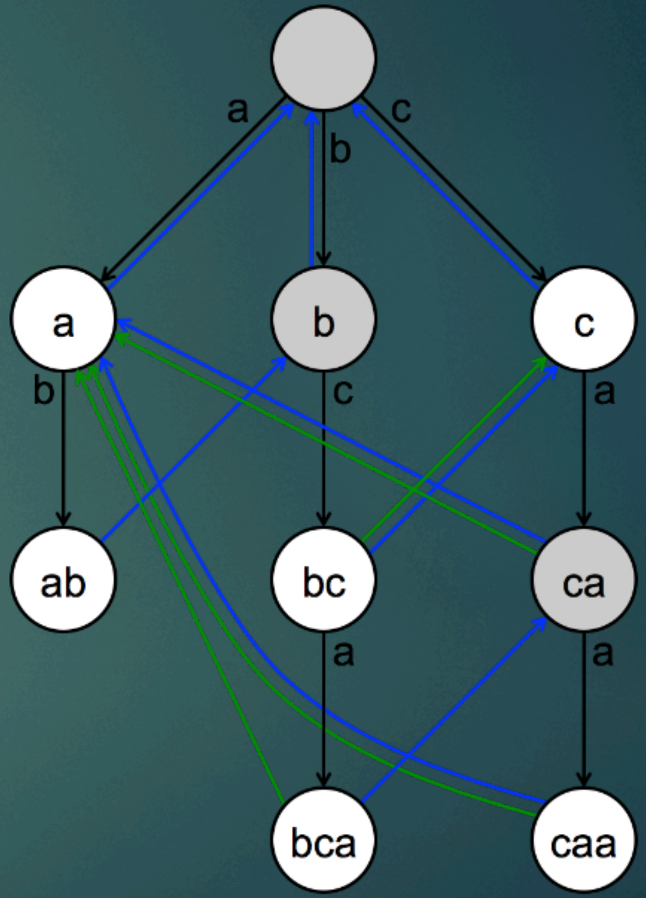
- Voice over Internet protocol (VoIP) services
- Providing network address translation services
- Managing quality of service in a network.

Recognition

- A DPI engine analyzes TCP/IP traffic in real time.
- Searches outside of the headers (ports, payload, length, etc.)
- Can search packet for
  - Protocols
  - Applications
  - URLs
  - Media content
  - Text strings / numerical patterns
  - Malware

Recognition

- Aho-Corasick string matching algorithm
  - Constructs Deterministic Finite Automata (DFA)
  - Matches a finite set of patterns simultaneously
  - Used in fgrep UNIX command
- As pattern matching algorithms improve, DPI becomes cheaper



Recognition

- Necessary to create complex rule sets
  - Begin with regular expressions
  - Create a signature which tells the DPI engine where to look for the regex in the traffic stream
  - Create rule sets which operate on a network level, targeting traffic between specific nodes
  - This means this is an imperfect method and can be evaded.
    - Can be culturally or platform dependent.

Manipulation

- Block the movement of recognized informational objects into or out of the network
- Regulate packet flow speed
- Change the packet header in some way
- Prioritize some packets over others (based on user, protocol, etc.)
- Disconnect a session

Notification

- Generate statistical reports
- Issue alarms or notifications
- An application need not be directly in the network to receive notifications

DPI Applications

- Passive vs. Active
- In-line vs. Off-line
- ISPs can use DPI for
  - Network Security
  - Bandwidth Management and Network Visibility
  - User Profiling
  - Copyright Policing
- Governments can use DPI for
  - Government Surveillance
  - Content Control / Censorship
- Other technologies are used for these applications as well

Challenges

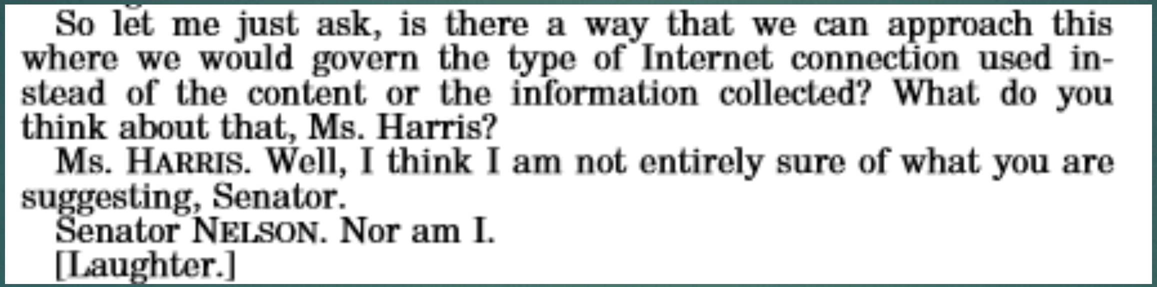
- Resource Intensive
- Different functions create difficulties
  - Have to run on same hardware
  - Have to optimize to run on the same platform
- Right now, DPI systems can only integrate a few applications
- Hardest to integrate is Copyright Policing

Controversy

- 2008 Senate Hearings
  - Privacy, consumer profiling
  - Heard from ISPs, Google, Microsoft, Amazon, etc.
  - Term “Deep Packet Inspection” emerges
- SOPA / PIPA
- NSA

Future

- Legislation necessary
  - Difficult because politicians don’t understand technology



So let me just ask, is there a way that we can approach this where we would govern the type of Internet connection used instead of the content or the information collected? What do you think about that, Ms. Harris?

Ms. HARRIS. Well, I think I am not entirely sure of what you are suggesting, Senator.

Senator NELSON. Nor am I.

[Laughter.]

  - How do we protect “personally identifiable information”
- Could help with implementation / transition to IPv6
- Enabling technology