IP(v6) packet staining

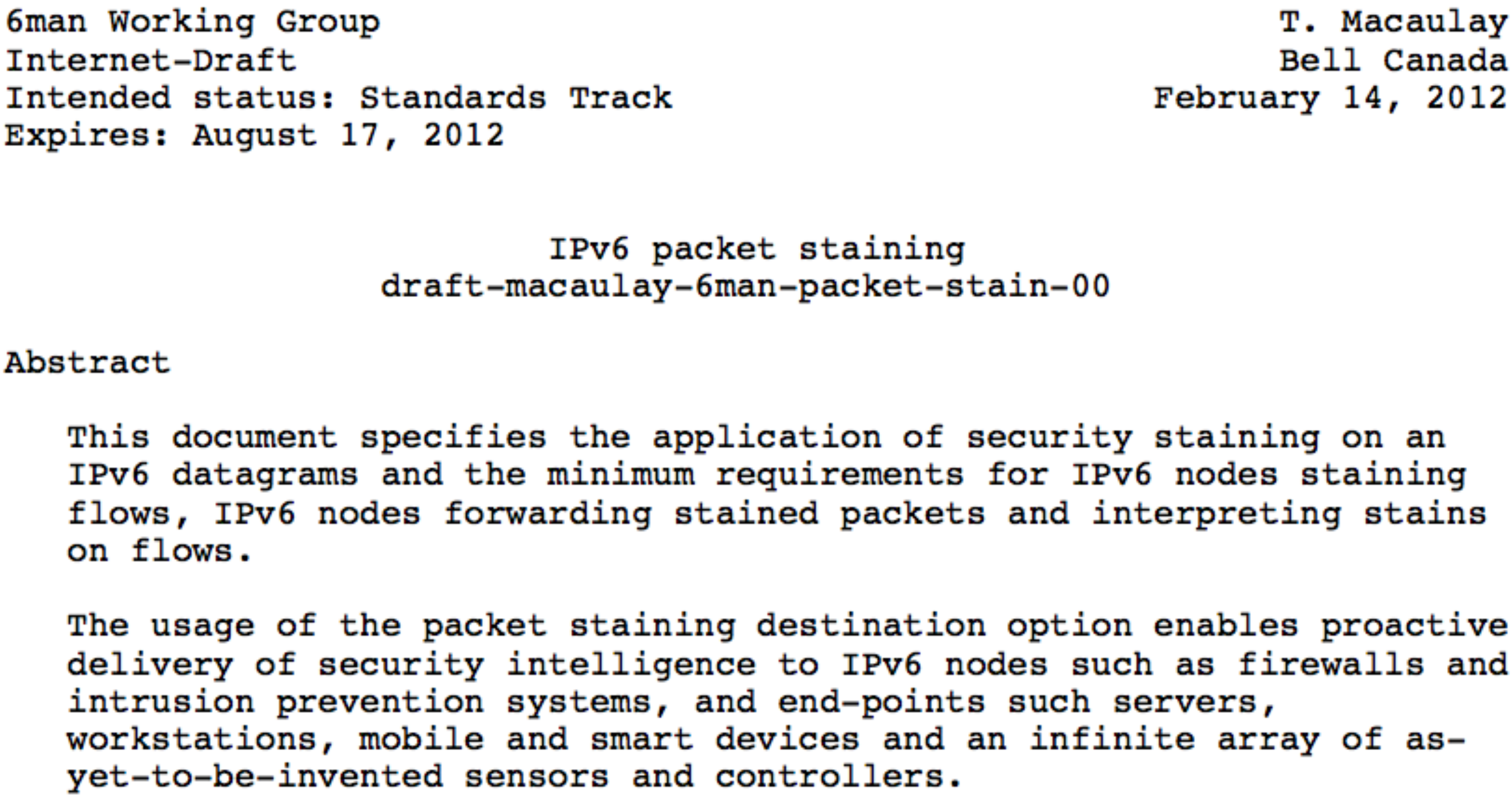
draft-macaulay-6man-packet-stain-00

IETF 83

March 2012

Tyson Macaulay,
VP Technology,
2Keys Security Solutions
tmaculay@2keys.ca
+16132929132

Draft released Feb 14th 2012



6man Working Group | T. Macaulay
Internet-Draft | Bell Canada
Intended status: Standards Track | February 14, 2012
Expires: August 17, 2012

IPv6 packet staining
draft-macaulay-6man-packet-stain-00

Abstract

This document specifies the application of security staining on an IPv6 datagrams and the minimum requirements for IPv6 nodes staining flows, IPv6 nodes forwarding stained packets and interpreting stains on flows.

The usage of the packet staining destination option enables proactive delivery of security intelligence to IPv6 nodes such as firewalls and intrusion prevention systems, and end-points such servers, workstations, mobile and smart devices and an infinite array of as-yet-to-be-invented sensors and controllers.

Prior work

13/3

Volume 13 Number 3 • Summer 2010

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

A New Layer of Security

also inside

The New IATAC

Open Specifications: An Enabler of UAV Operations

DoD Techipedia Happenings

Shall We Play a Game?

US Cyber Command is Activated

Maximizing the DoD Return on Investment in Cyberspace Professionals

Upstream Intelligence: A New Layer of Cybersecurity

Anatomy of Upstream Intelligence

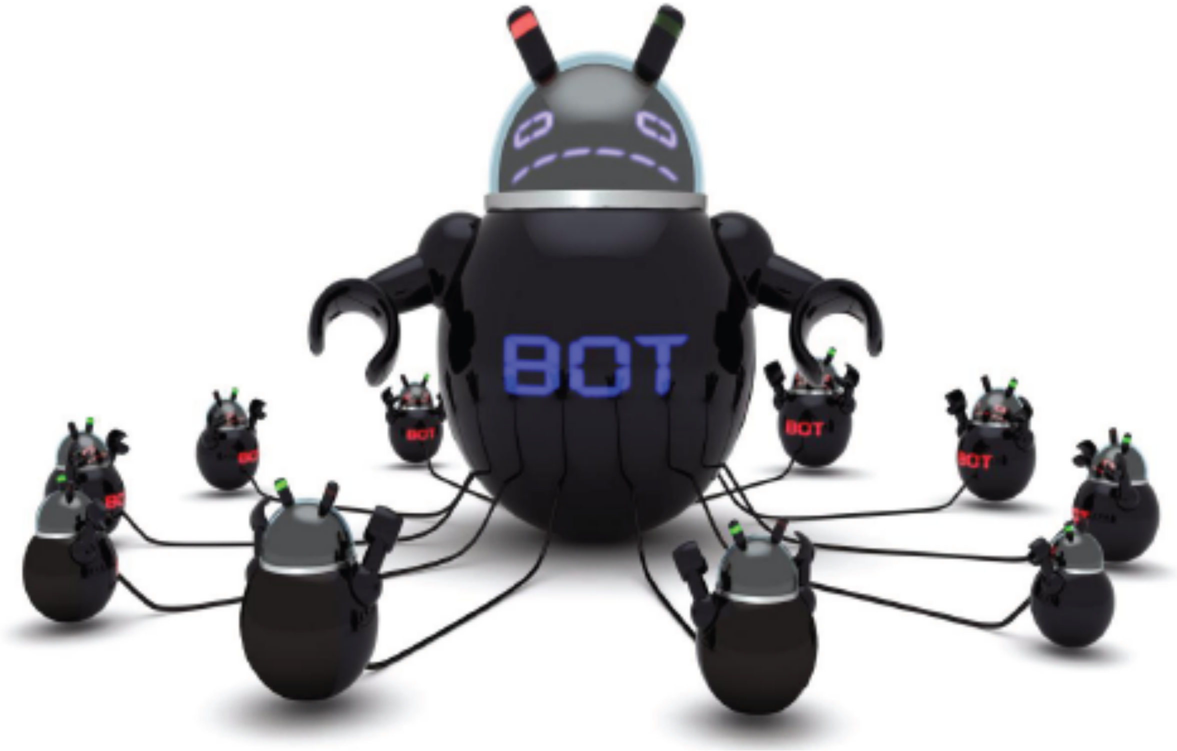
Business Models of Upstream Intelligence Management and Distribution

State-of-the-Art Report on Information and Communications Technology Supply Chain Security Risk Management

IATAC

Summer 2010
http://iac.dtic.mil/iatac/download/Vol13_No3.pdf
Fall 2010
http://iac.dtic.mil/iatac/download/Vol13_No4.pdf
Winter 2011
http://iac.dtic.mil/iatac/download/Vol14_No1.pdf

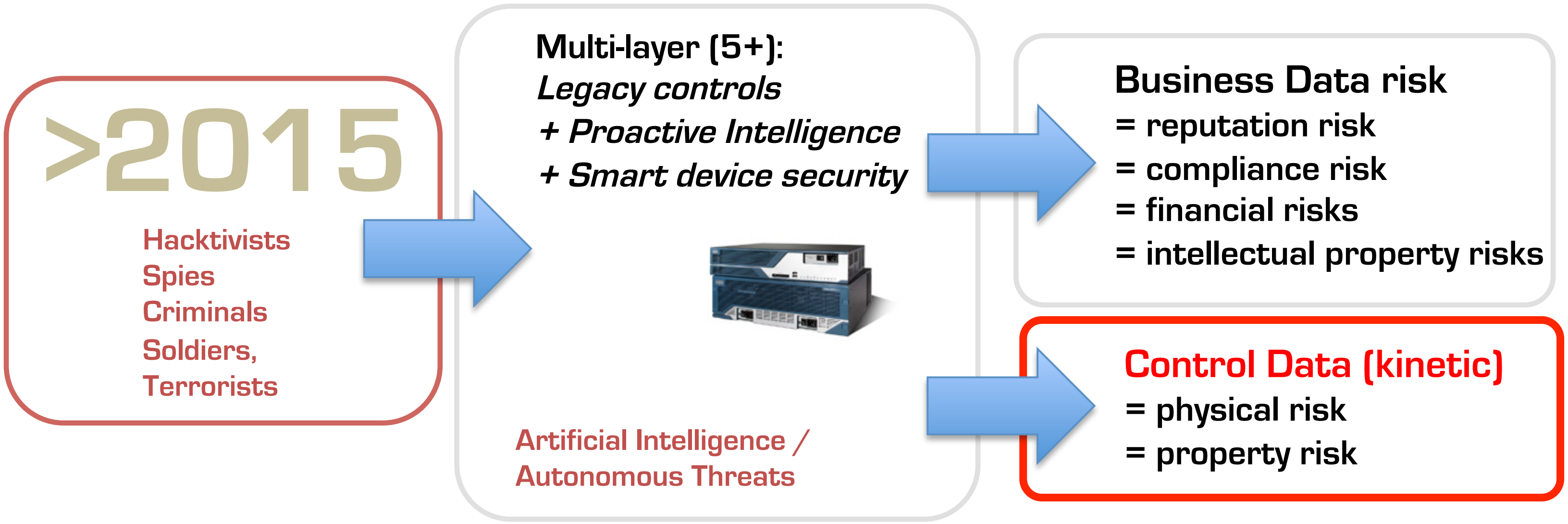
Why?



BOT
BOT
BOT
BOT
BOT

Older detection approaches are failing

- Time between compromise and exploitation can be *sub-second*
- Too much latency between detection and intelligence distribution
- .dat files and CRLS are huge
  - Not appropriate for metered services (3G/4G)
- On-line queries subject to disruption and compromise



>2015

Hacktivists
Spies
Criminals
Soldiers,
Terrorists

Multi-layer (5+):
Legacy controls
+ Proactive Intelligence
+ Smart device security

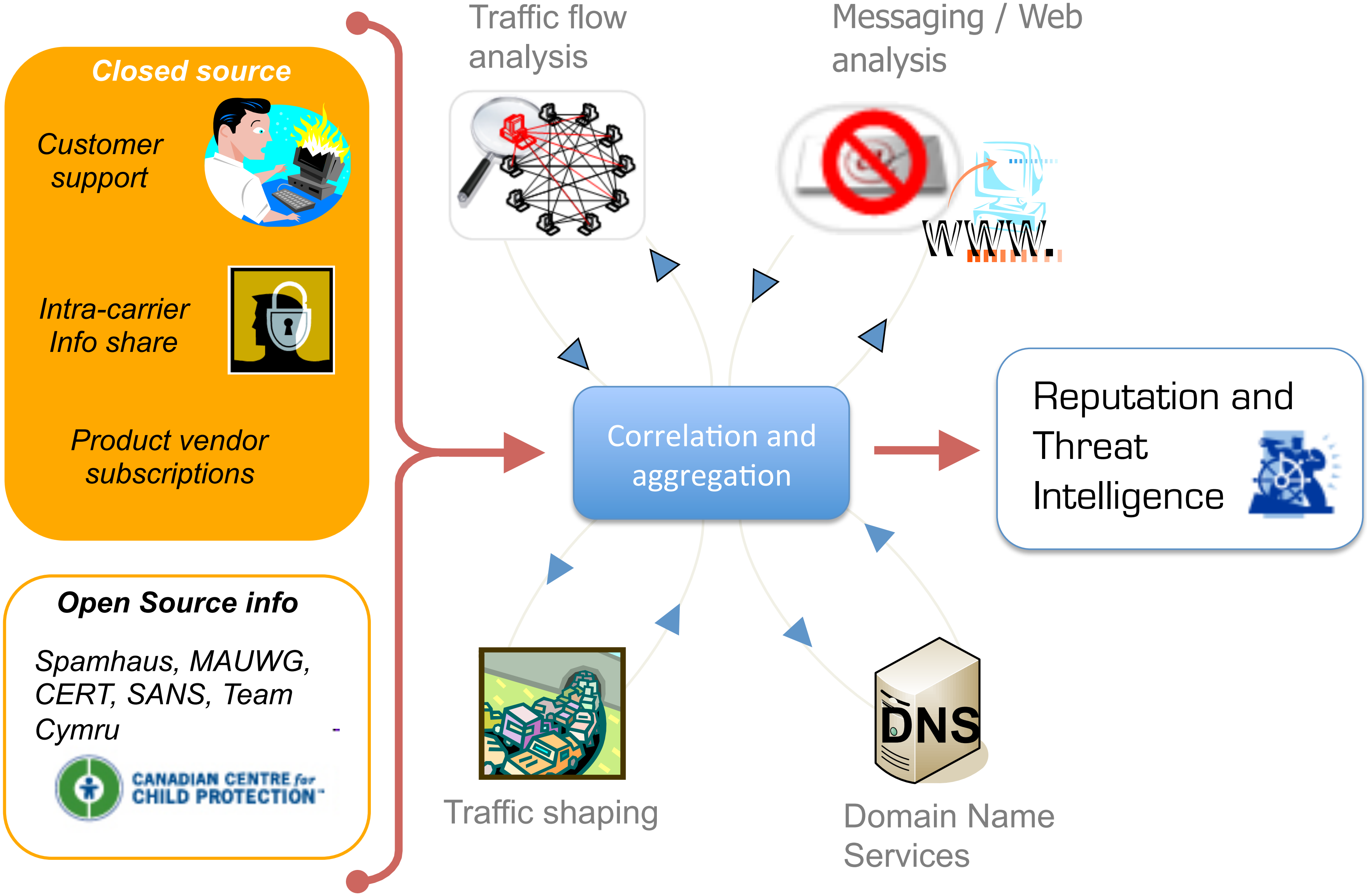
Artificial Intelligence /
Autonomous Threats

Business Data risk
= reputation risk
= compliance risk
= financial risks
= intellectual property risks

Control Data (kinetic)
= physical risk
= property risk

What?

Threat Intelligence



Closed source

Customer support

Intra-carrier Info share

Product vendor subscriptions

Open Source info

Spamhaus, MAUWG, CERT, SANS, Team Cymru

CANADIAN CENTRE for CHILD PROTECTION

Traffic flow analysis

Messaging / Web analysis

Correlation and aggregation

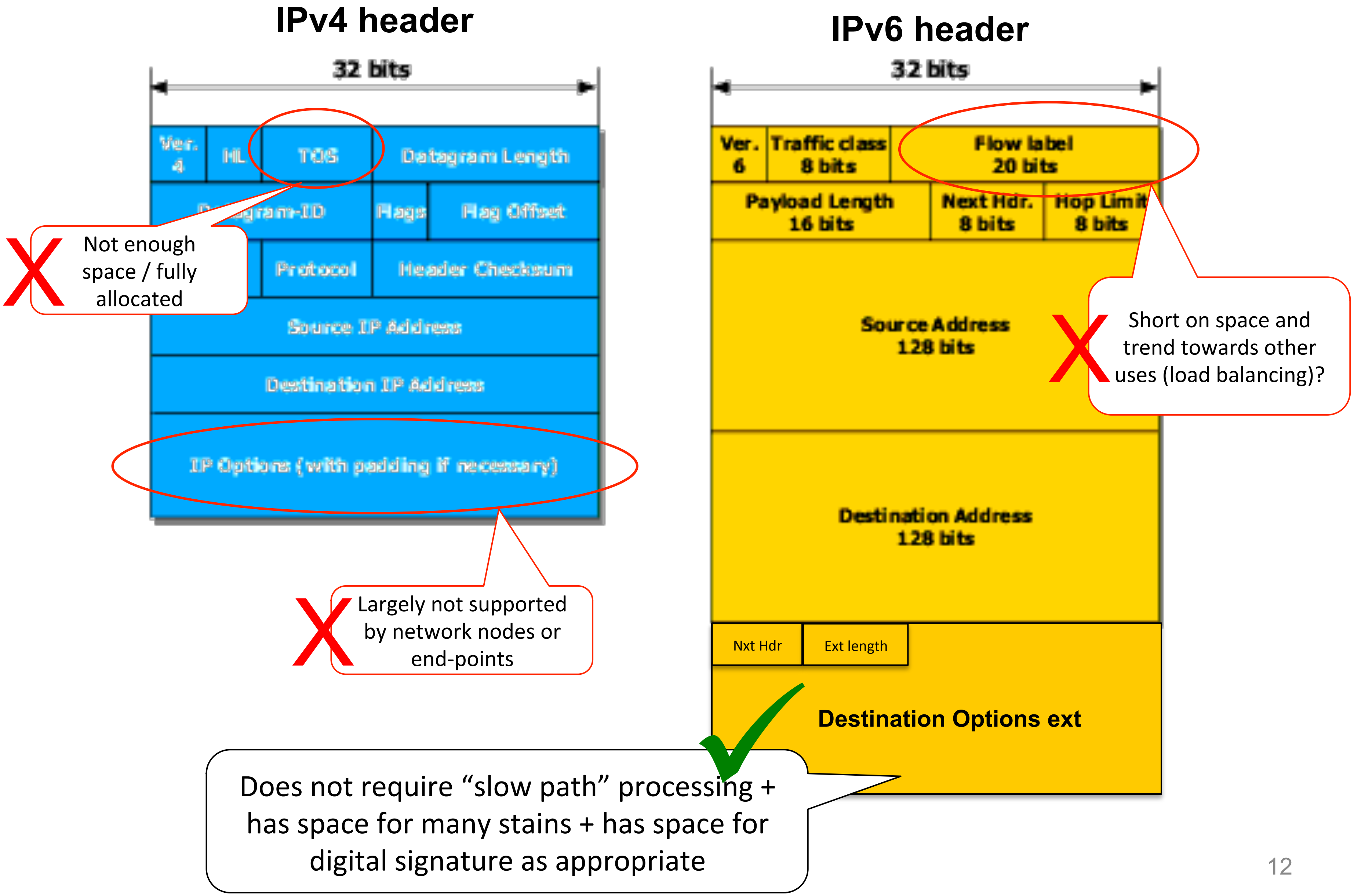
Reputation and Threat Intelligence

Traffic shaping

Domain Name Services

How?

IP header staining



IPv4 header

32 bits

Ver. 4 | HL | TOS | Datagram Length

Datagram-ID | Flags | Flag Offset

Protocol | Header Checksum

Source IP Address

Destination IP Address

IP Options (with padding if necessary)

X Not enough space / fully allocated

X Largely not supported by network nodes or end-points

IPv6 header

32 bits

Ver. 6 | Traffic class 8 bits | Flow label 20 bits

Payload Length 16 bits | Next Hdr. 8 bits | Hop Limit 8 bits

Source Address 128 bits

Destination Address 128 bits

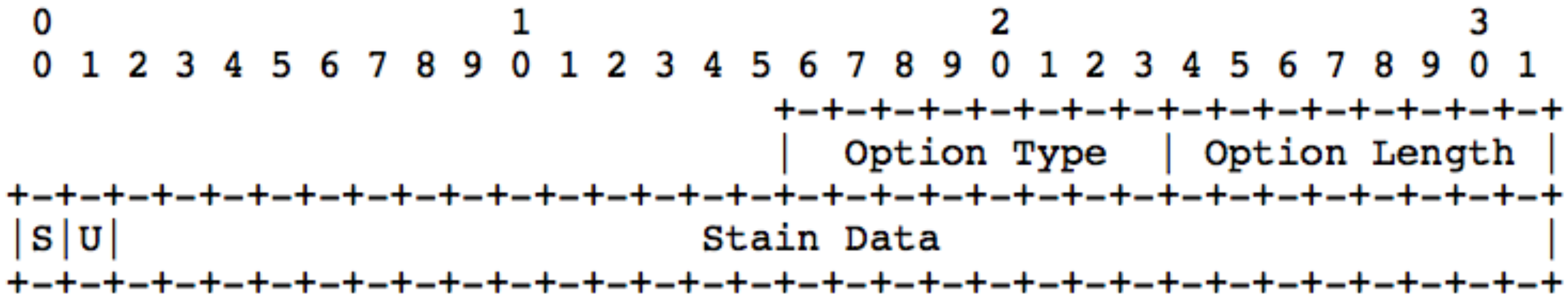
Nxt Hdr | Ext length

Destination Options ext

X Short on space and trend towards other uses (load balancing)?

✓ Does not require “slow path” processing + has space for many stains + has space for digital signature as appropriate

Destination Options format

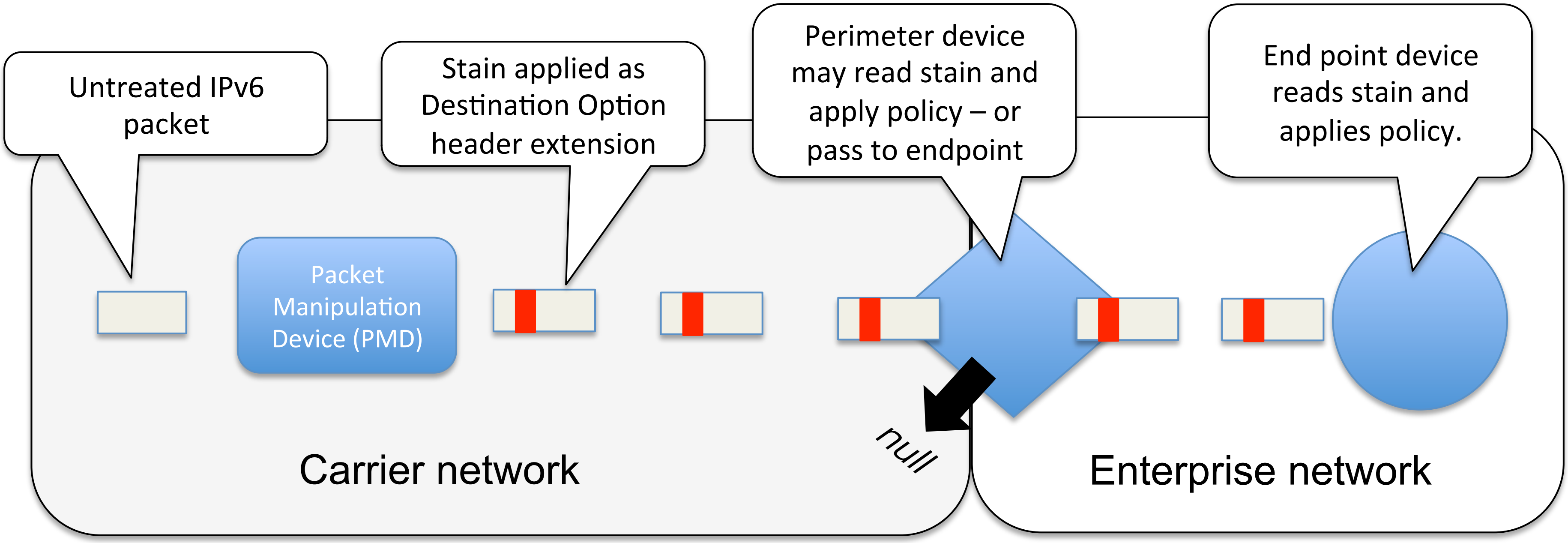


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |  Option Type  | Option Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|S|U|                        Stain Data                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Packet Stain Destination Option Layout

Options type	8-bit identifier of the type of option. The option identifier for the reputation stain option will be allocated by the IANA
Options length	8-bit unsigned integer. The length of the option (excluding the Option Type and Option Length fields).
S bit	When this bit is set, the reputation stain option has been signed.
U bit	When this bit is set, the reputation stain option contains a malicious URL.
Stain data	Contains the stain (reputation information) data

IPv6 concept of operations



Untreated IPv6 packet

Packet Manipulation Device (PMD)

Stain applied as Destination Option header extension

Perimeter device may read stain and apply policy – or pass to endpoint

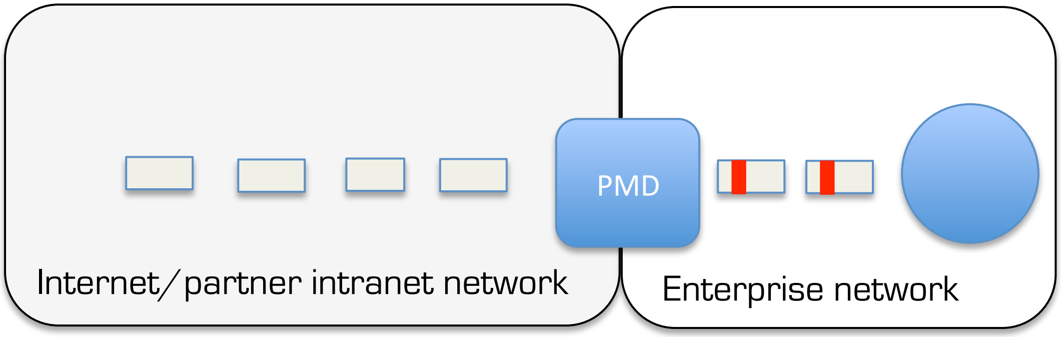
End point device reads stain and applies policy.

null

Carrier network

Enterprise network

Or…



PMD

Internet/partner intranet network

Enterprise network

Questions & Comments to date

Draft 01 (April 2012)

- Is this legal?
- Provide sample code?
- More details on S and U bits
- Add use-case for home users (mitigate loss of NAT firewalls)
- Add stain semantics
- Discuss scalability advantages over .dat or CRL-type solutions
- Discuss reputation algorithms

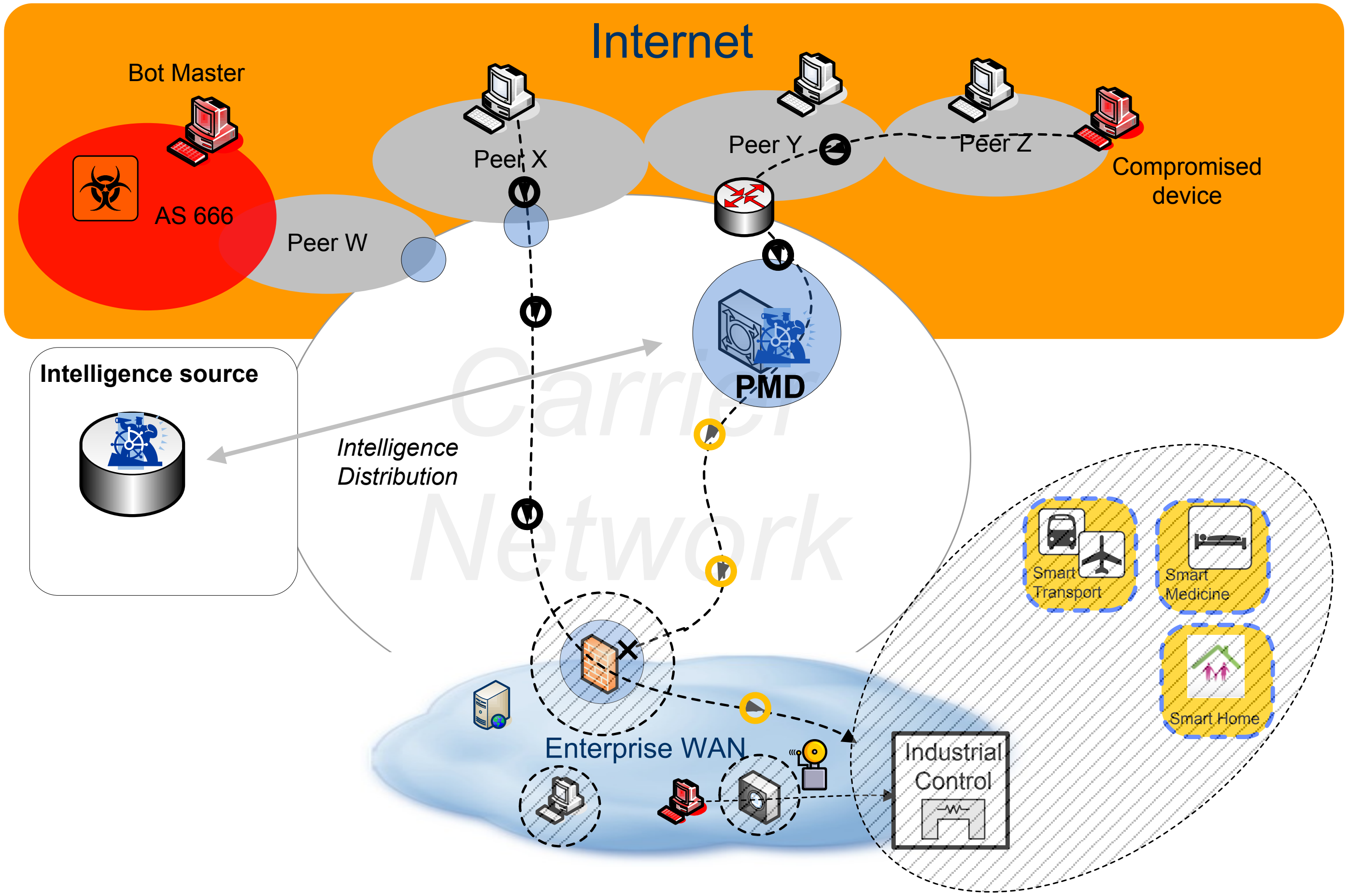
Conclusion

Is “packet staining” worth pursuing?

Back-up

Use-cases

IP Packet Staining



Intelligence management

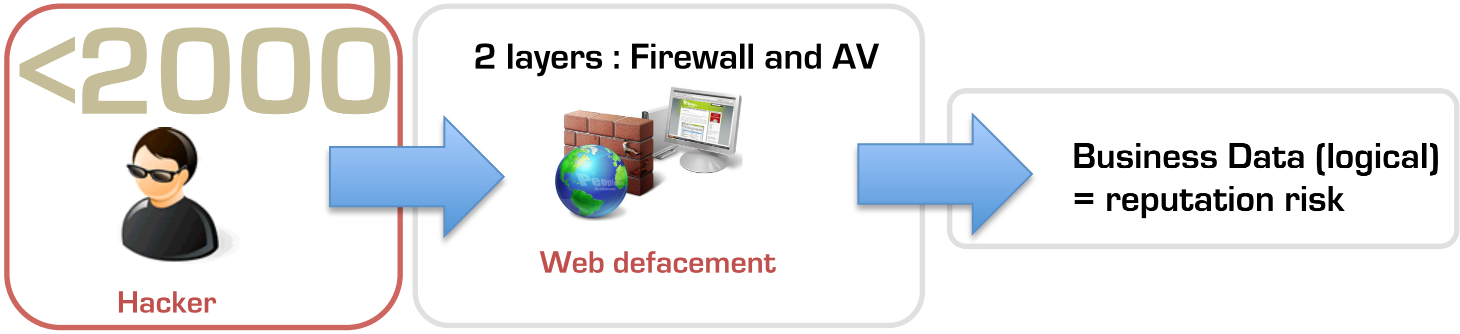
Compromised / victim device

Stained packet from suspect source

Packet Manipulation Device (PMD)

Unstained / neutral packet

"Staining reading device"



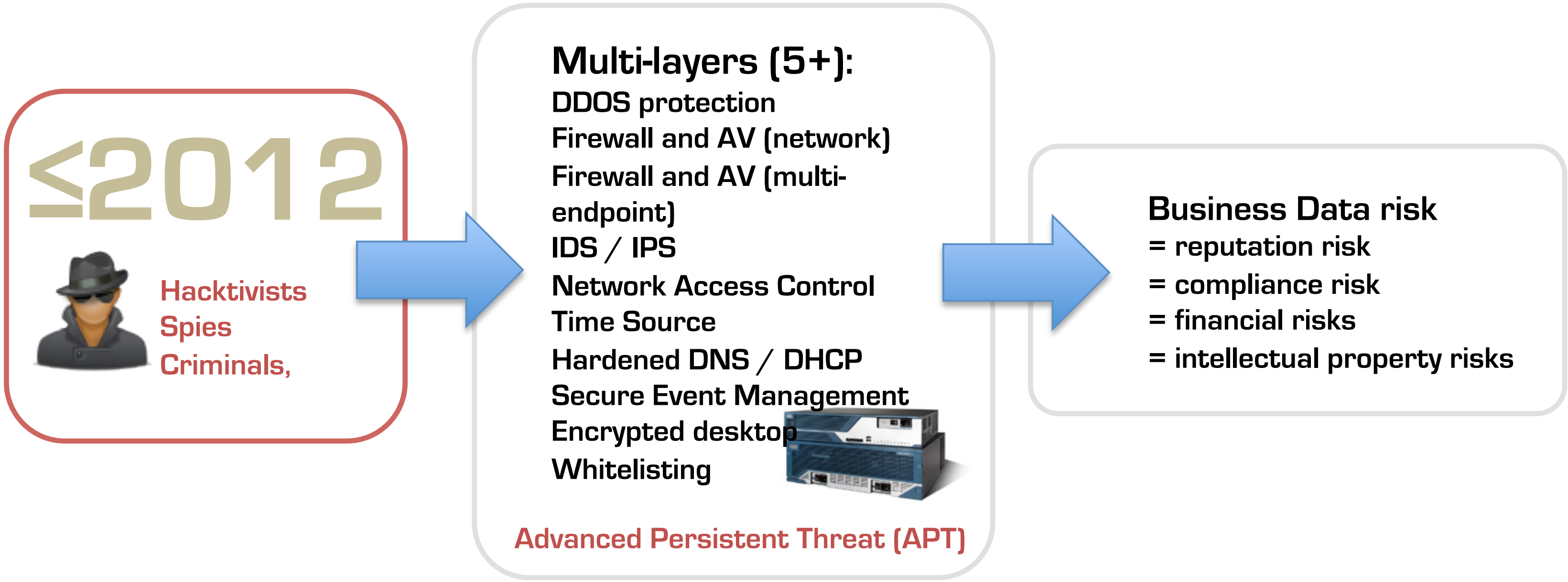
<2000

Hacker

2 layers : Firewall and AV

Web defacement

Business Data (logical)
= reputation risk



≤2012

Hacktivists
Spies
Criminals,

Multi-layers (5+):

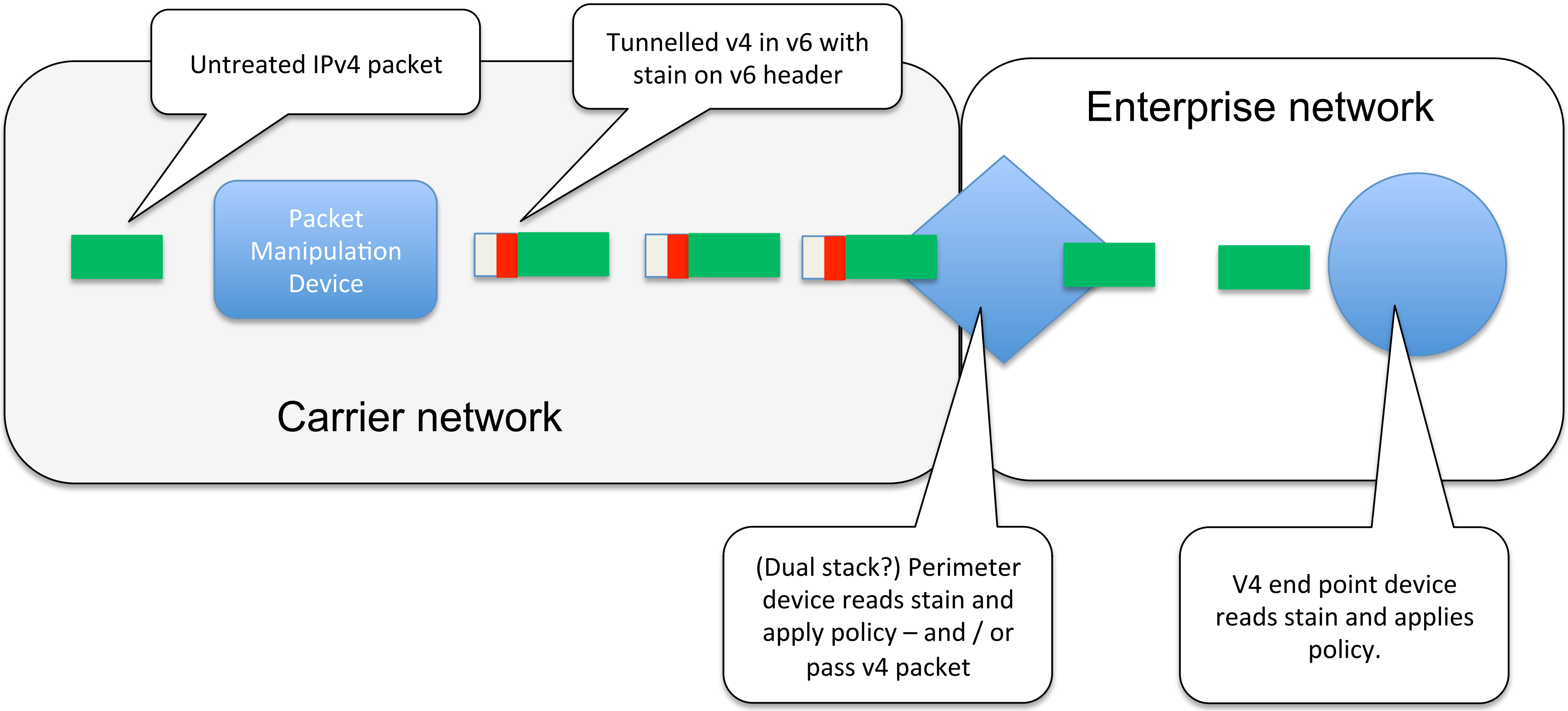
DDOS protection
Firewall and AV (network)
Firewall and AV (multi-endpoint)
IDS / IPS
Network Access Control
Time Source
Hardened DNS / DHCP
Secure Event Management
Encrypted desktop
Whitelisting

Advanced Persistent Threat (APT)

Business Data risk

= reputation risk
= compliance risk
= financial risks
= intellectual property risks

IPv4-support concept of operations


Untreated IPv4 packet
Tunnelled v4 in v6 with stain on v6 header
Packet Manipulation Device
Enterprise network
Carrier network
(Dual stack?) Perimeter device reads stain and apply policy – and / or pass v4 packet
V4 end point device reads stain and applies policy.

IATAC

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA

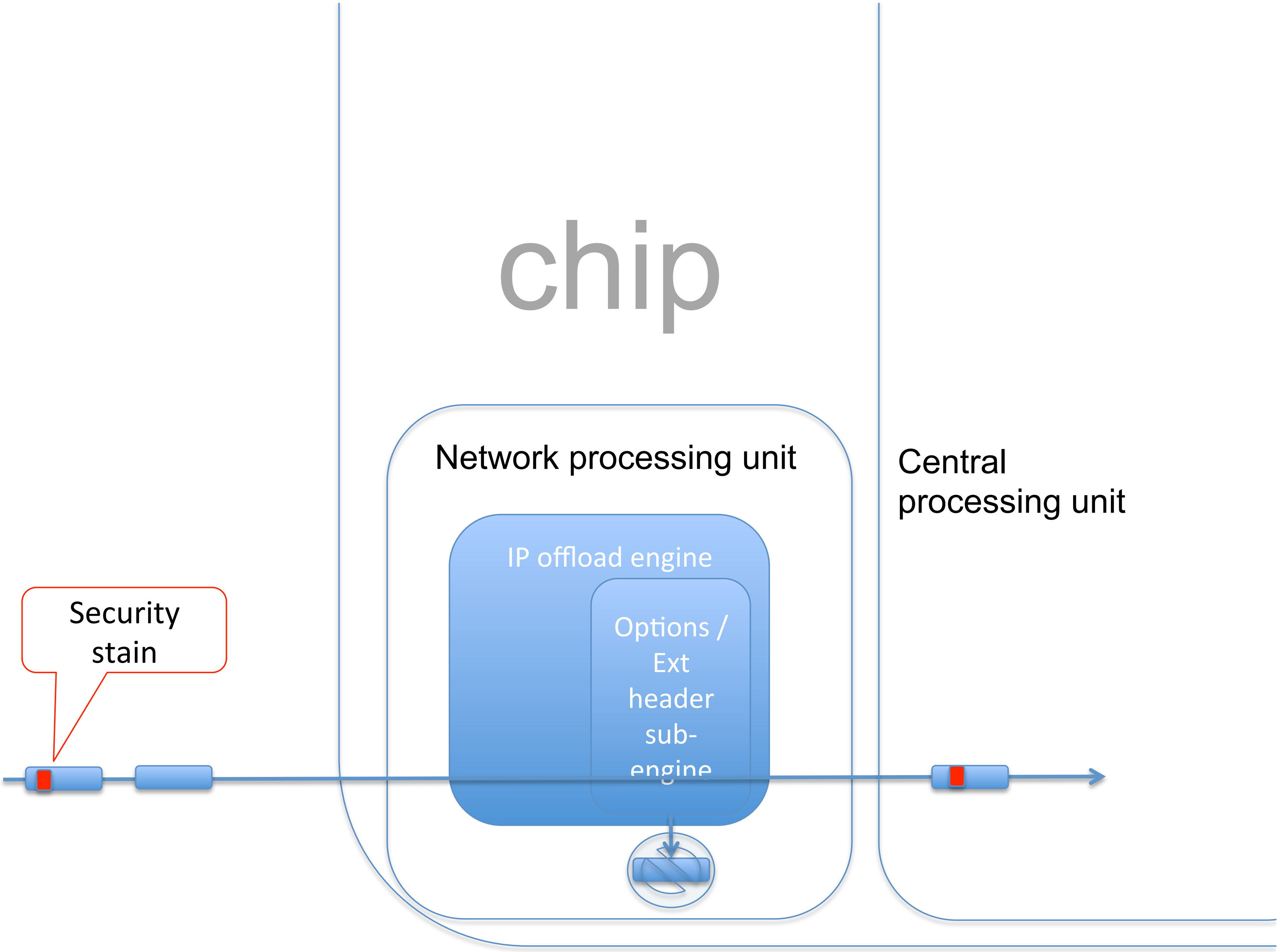
DEFENSE TECHNICAL INFORMATION CENTER

EXCELLENCE IN INFORMATION SERVICE

IANA Option Types required

Option types are set by IANA and are 8 bits. Example of required staining option type below.

	Un-signed	Signed
Reputation stain	nnnnnn00	nnnnnn01
Reputation stain + URL	nnnnnn10	nnnnnn11


chip
Network processing unit
Central processing unit
IP offload engine
Options / Ext header sub-engine
Security stain

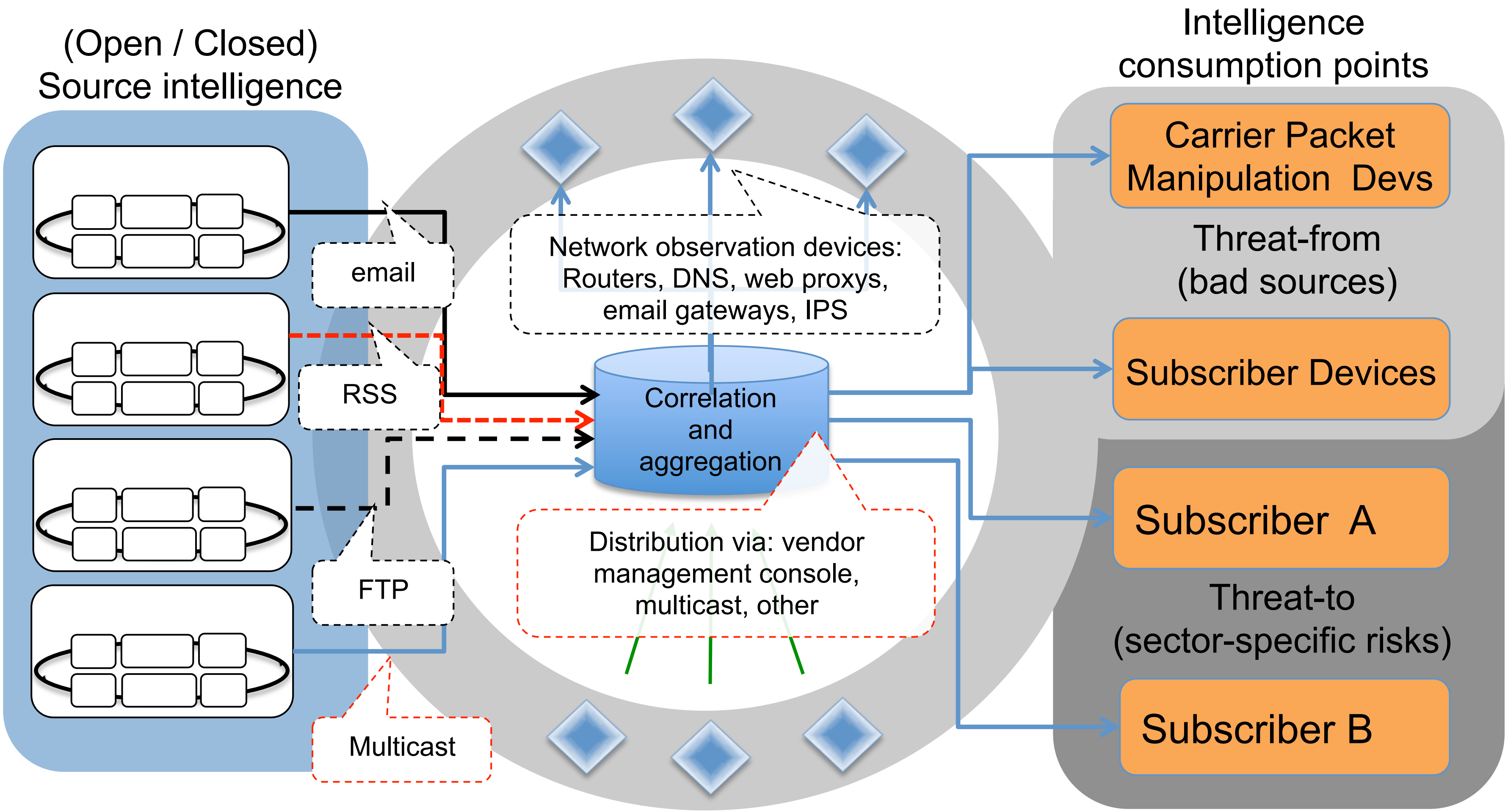
Use-cases (under development)

- Use case
  - Mobile devices roaming on the internet
  - Closed networks with admin error
  - Mesh networks with admin error
  - Closed networks with USB bots
  - Q: what is a vendor device stains on the way out? Is there an B2B staining processes? Will the carrier PMD over-write? – needs to be part of RFC.

Reputation algorithm requirements

- Out of scope for RFC – can be vendor specific
- <<To be developed>> Minimum requirements for staining algorithm: Whitepaper in Q1 2012

Threat Intelligence distribution


(Open / Closed)
Source intelligence
email
RSS
FTP
Multicast
Network observation devices:
Routers, DNS, web proxys,
email gateways, IPS
Correlation
and
aggregation
Distribution via: vendor
management console,
multicast, other
Intelligence
consumption points
Carrier Packet
Manipulation Devs
Threat-from
(bad sources)
Subscriber Devices
Subscriber A
Threat-to
(sector-specific risks)
Subscriber B