DSD and Open Source Software

Alan Leigh

About Me

DSD
Defence Signals Directorate

- Information Security Specialist
- Infosec-er for about 8 years
- Defence and Industry
- alan.leigh@defence.gov.au

About DSD

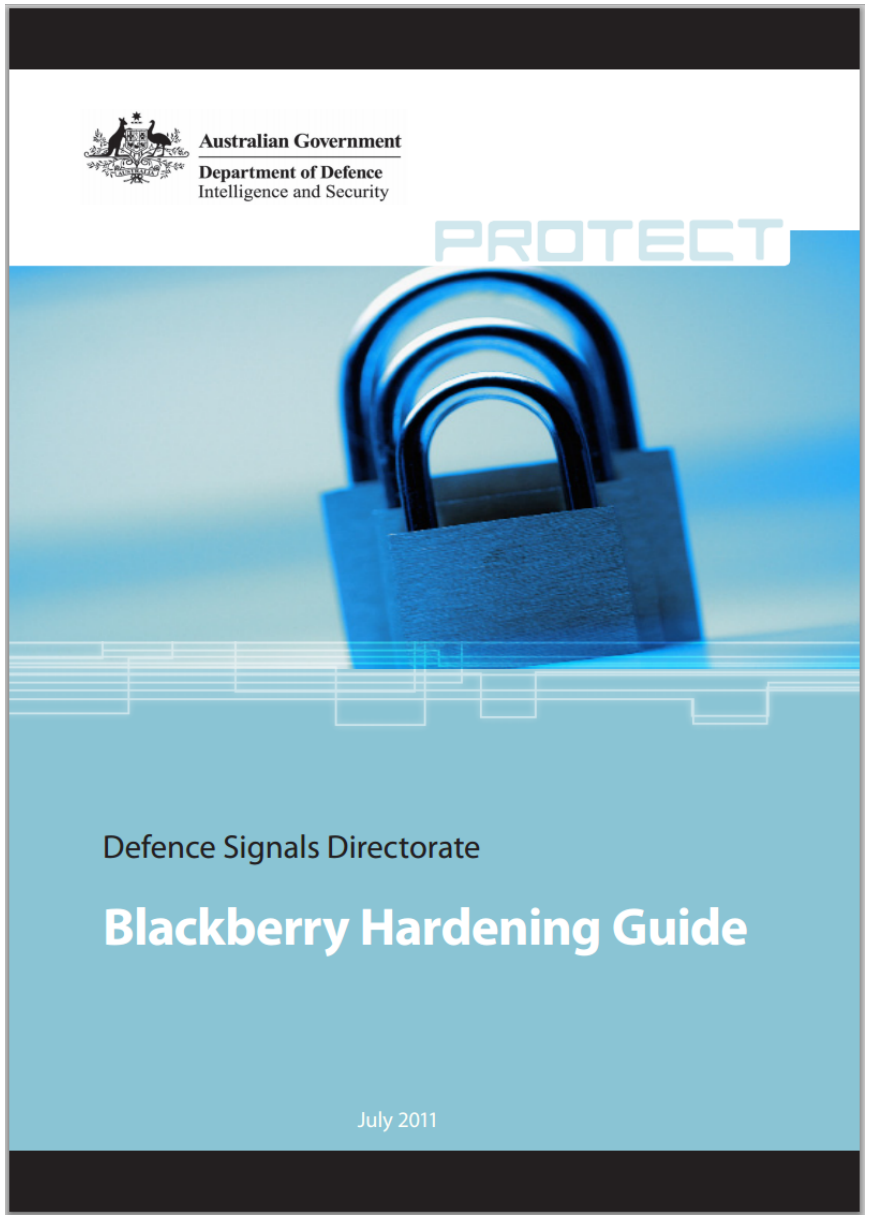
DSD
Defence Signals Directorate

- Two roles
  - Signals Intelligence (SIGINT)
  - Information (or Cyber) Security
    - Cyber Security Operations Centre

- http://dsd.gov.au

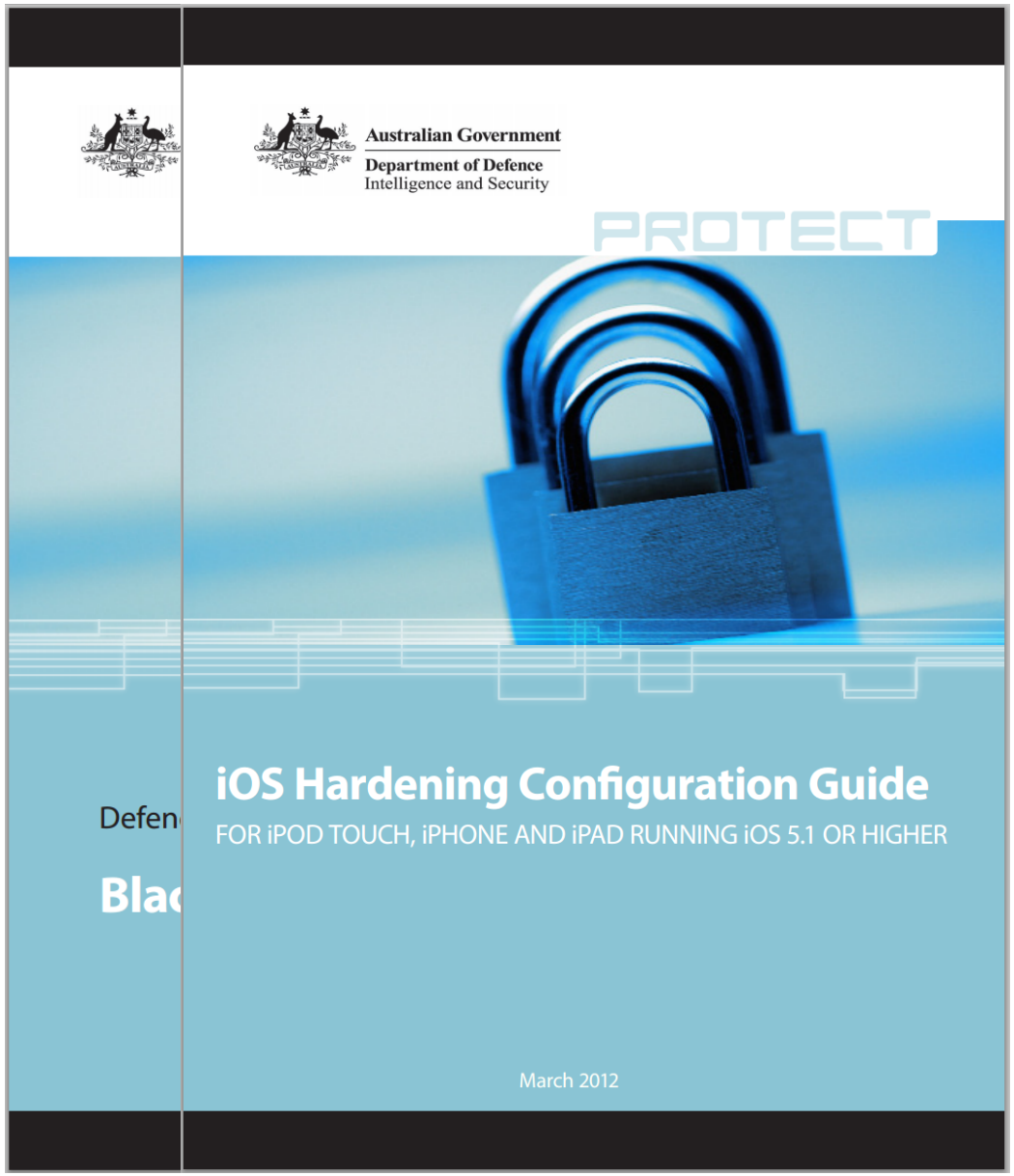
About DSD

DSD
Defence Signals Directorate



About DSD

DSD
Defence Signals Directorate



About DSD

DSD
Defence Signals Directorate

Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

OCTOBER 2012

Strategies to Mitigate Targeted Cyber Intrusions

Introduction

1. Australian computer networks are being targeted by adversaries seeking access to sensitive information.

2. A commonly used technique is social engineering, where malicious "spear phishing" emails are tailored to entice the reader to open them. Users may be tempted to open malicious email attachments or follow embedded links to malicious websites. Either action can compromise the network and disclose sensitive information.

3. The Defence Signals Directorate (DSD) has developed a list of strategies to mitigate targeted cyber intrusions. The list is informed by DSD's experience in operational cyber security, including responding to serious cyber incidents and performing vulnerability assessments and penetration testing for Australian government agencies.

Mitigation Strategies

4. DSD's list of mitigation strategies, first published in February 2010, is revised for 2012 based on DSD's most recent analysis of incidents across the Australian Government. Further details on the mitigation strategies are available at the DSD web page http://www.dsd.gov.au.

5. While no single strategy can prevent malicious activity, the effectiveness of implementing the Top 4 strategies remains very high. At least 85% of the intrusions that DSD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package.

6. Implementing the Top 4 strategies can be achieved gradually, starting with computers used by the employees most likely to be targeted by intrusions, and eventually extending them to all users. Once this is achieved, organisations can selectively implement additional mitigation strategies based on the risk to their information.

7. This document provides information about mitigation implementation costs and user resistance to help organisations select the best set of strategies for their requirements.

8. These strategies complement the guidance provided in the *Australian Government Information Security Manual* (ISM) available on DSD's web site.

Defence Signals Directorate | Reveal Their Secrets – Protect Our Own

About DSD

DSD
Defence Signals Directorate

Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

NOVEMBER 2012

Top 4 mitigation strategies to protect your ICT system

Targeted cyber intrusions remain the biggest threat to government ICT systems. Since opening in early 2010, the Cyber Security Operations Centre (CSOC) has detected and responded to thousands of these intrusions.

You should never assume that your information is of little or no value. Adversaries are not just looking for classified information. A lot of activity observed by the CSOC has an economic focus looking for information about Australia's business dealings, its intellectual property, its scientific data and the government's intentions.

The threat is real, but there are things every organisation can do to significantly reduce the risk of a cyber intrusion. In 2009, based on our analysis of these intrusions, the Defence Signals Directorate produced *Strategies to Mitigate Targeted Cyber Intrusions* – a document that lists a variety of ways to protect an organisation's ICT systems. At least 85% of the intrusions that DSD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package.

The Top 4 mitigations are: application whitelisting, patching applications and operating systems and using the latest versions; and minimising administrative privileges. This document is designed to help senior managers in organisations understand the effectiveness of implementing these strategies.

Application whitelisting

Whitelisting—when implemented correctly—makes it harder for an adversary to compromise an organisation's ICT system. Application whitelisting is a technical measure which only allows specifically authorised applications to run on a system. This helps prevent malicious software and unauthorised applications running.

Patching systems

A software patch is a small piece of software designed to fix problems or update a computer program. Patching an organisation's system encompasses both the first and second mitigation strategies. It is important to patch both your operating system and applications within a two day timeframe for serious vulnerabilities. Once a vulnerability in an operating system or application is made public, you can expect malware to be developed by adversaries within 48 hours. In some cases, malware has been developed to take advantage of a publicly disclosed vulnerability within eight hours.

There is often a perception that by patching a system without rigorous testing, something is likely to break on the system. In the majority of cases patching will not affect the function of an organisation's ICT system.

Defence Signals Directorate | Reveal Their Secrets – Protect Our Own

Page **1** of **2**

Strategies

Introduction

1. Australian cc
information.

2. A commonly
tailored to entice
attachments or fo
network and disclo

3. The Defence
cyber intrusions. T
responding to ser
testing for Australi

Mitigation Str

4. DSD's list of
DSD's most recent
mitigation strategie

5. While no sin
Top 4 strategies r
involved adversar
implementing the T

6. Implementin
the employees mo
Once this is achiev
on the risk to their

7. This docume
to help organisatio

8. These strateg
Security Manual (IS

Defen

Blac

iOS Ha

FOR iPOD T

About DSD

DSD
Defence Signals Directorate

About DSD

DSD
Defence Signals Directorate

DSD and Open Source

DSD
Defence Signals Directorate

fedora

git

redhat

django

REDMINE
flexible project management

ubuntu

Scala

python™

hadoop

pyFLAG

- http://code.google.com/p/pyflag
- GPLed
- Interesting uses:
  - http://memeover.arkem.org/2012/02/identifying-computers-behind-nat-with.html
  - http://www.dfrws.org/2008/proceedings/p112-cohen.pdf

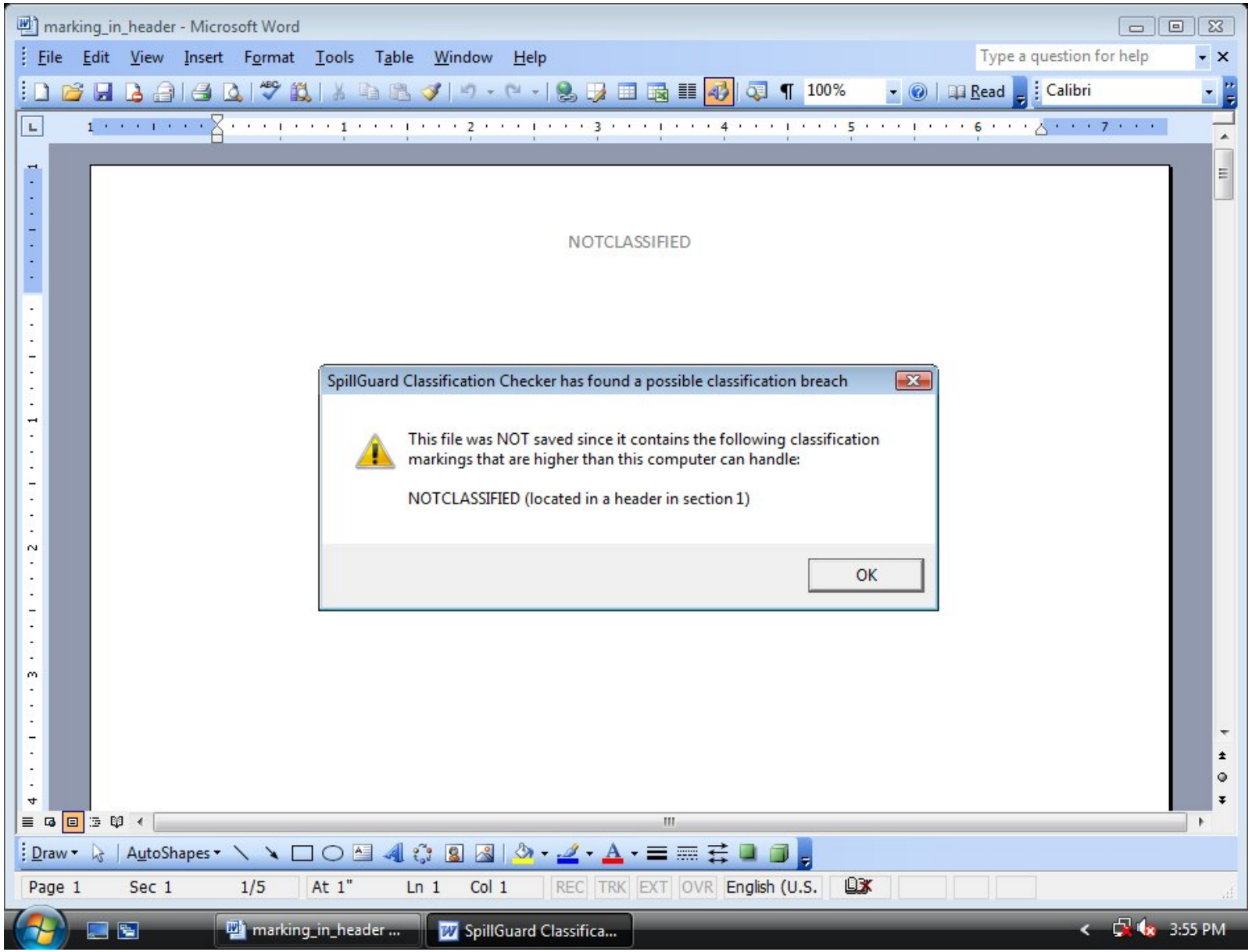
SpillGuard

DSD
Defence Signals Directorate

- http://sourceforge.net/projects/spillguard/
- GPLed
- Designed to help prevent “data spills”
  - C++ (Was VB .Net ...)
  - MS Office Plugin (COM Add-In)

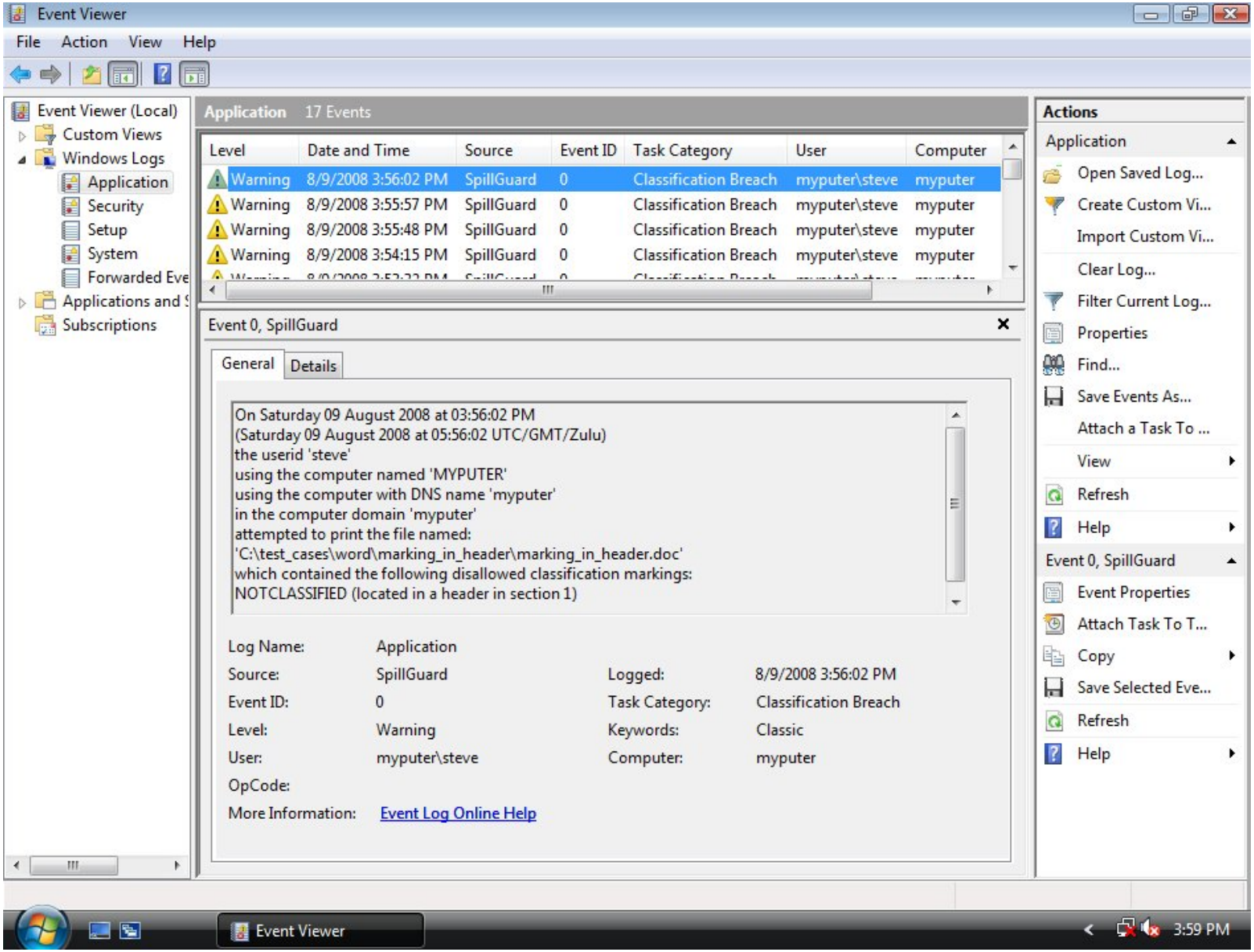
SpillGuard

DSD
Defence Signals Directorate



SpillGuard

DSD
Defence Signals Directorate



WhiteTrash

DSD
Defence Signals Directorate

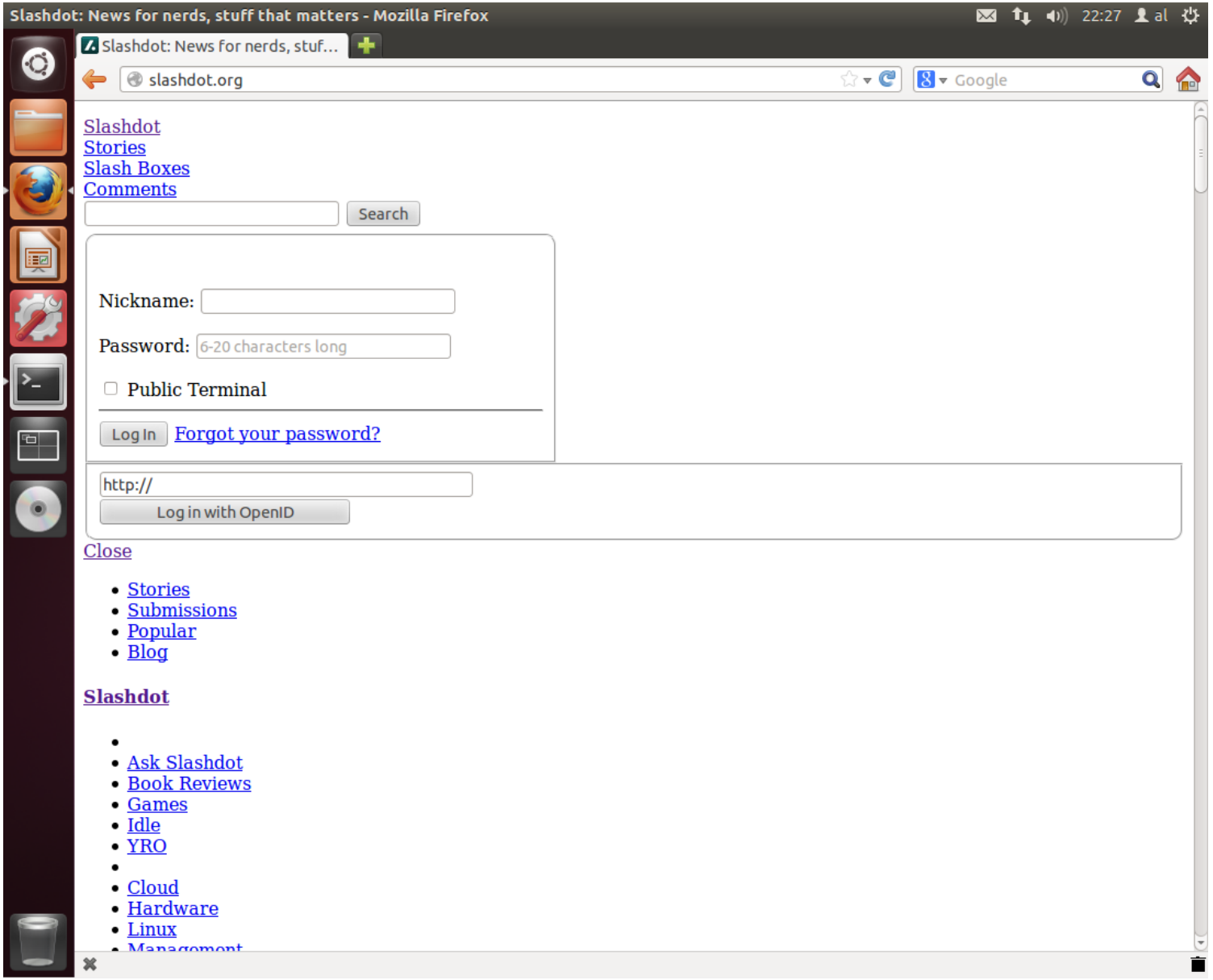
- http://whitetrash.sourceforge.net
- GPLed
- Dynamic whitelisting proxy (using Squid, Django)

WhiteTrash

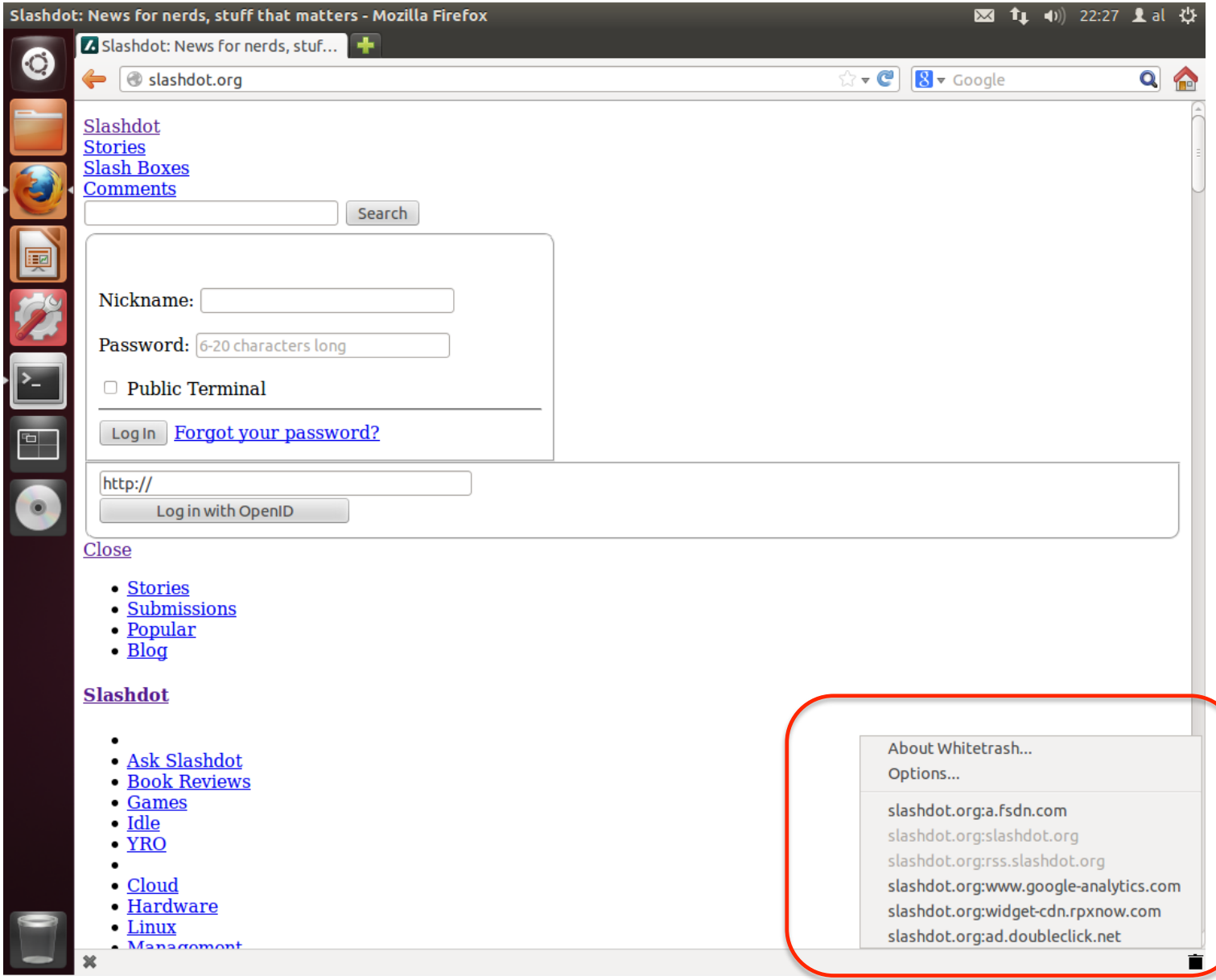

Whitetrash Internet Access Request Form - Mozilla Firefox
22:26
al
Whitetrash Internet Access Re...
https://whitetrash/whitelist/addentry/?url=http%3A//www.slashdot.org/&domain=www.slas
Google
WHITE TRASH
Dynamic Web Whitelisting For Squid
Host Requested:
www.slashdot.org
Protocol: HTTP
Client Username: al
Using Firefox? Grab the whitetrash add-on here
This site is not currently in the whitelist. If you have a genuine need to access this site please enter a business requirement or comment for this domain:
News and Current Affairs
By clicking "I Agree" below you are agreeing to have the information above stored on a list of whitelisted websites with YOUR UNIQUE USERNAME at this address
I Agree

WhiteTrash

DSD
Defence Signals Directorate

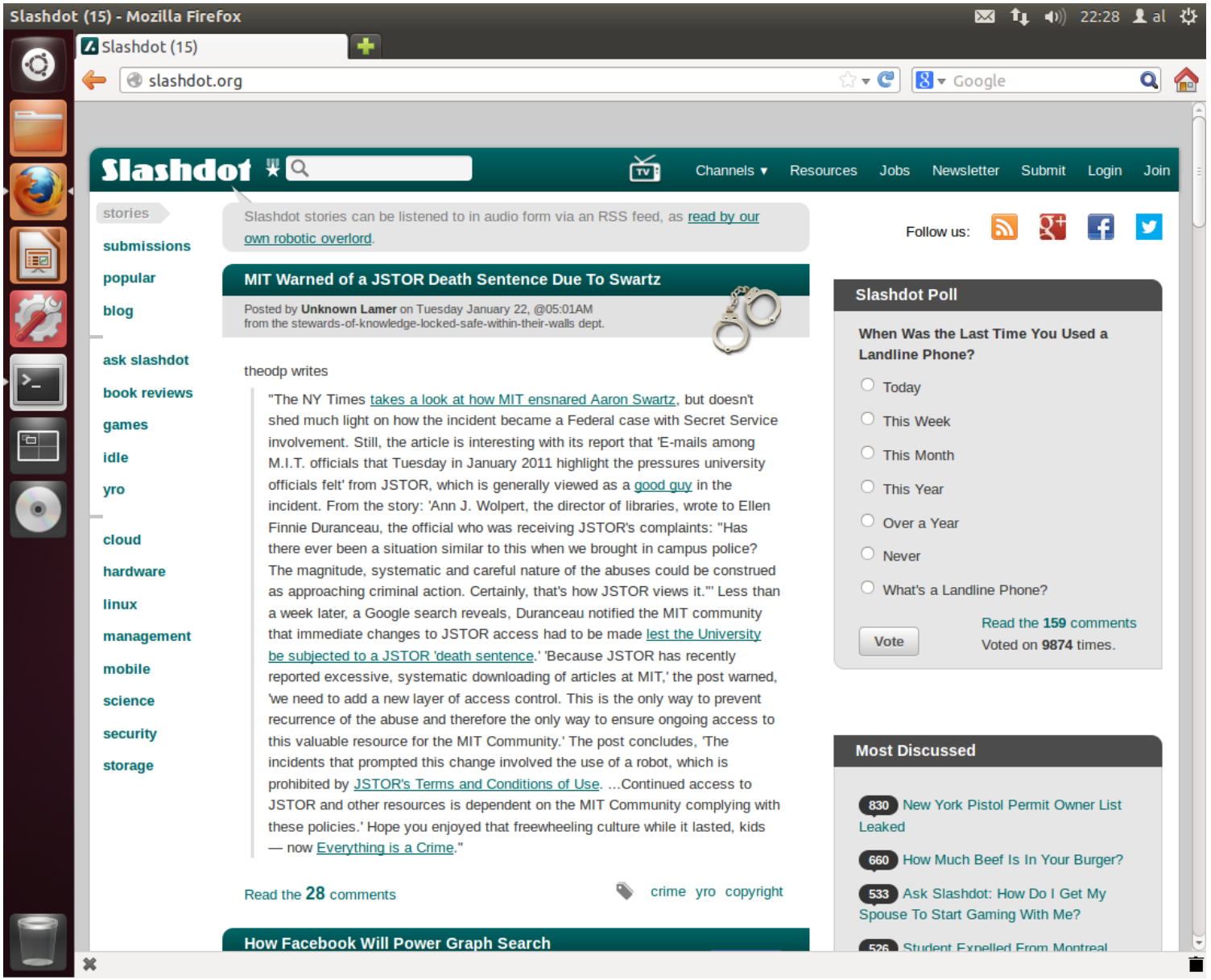


WhiteTrash

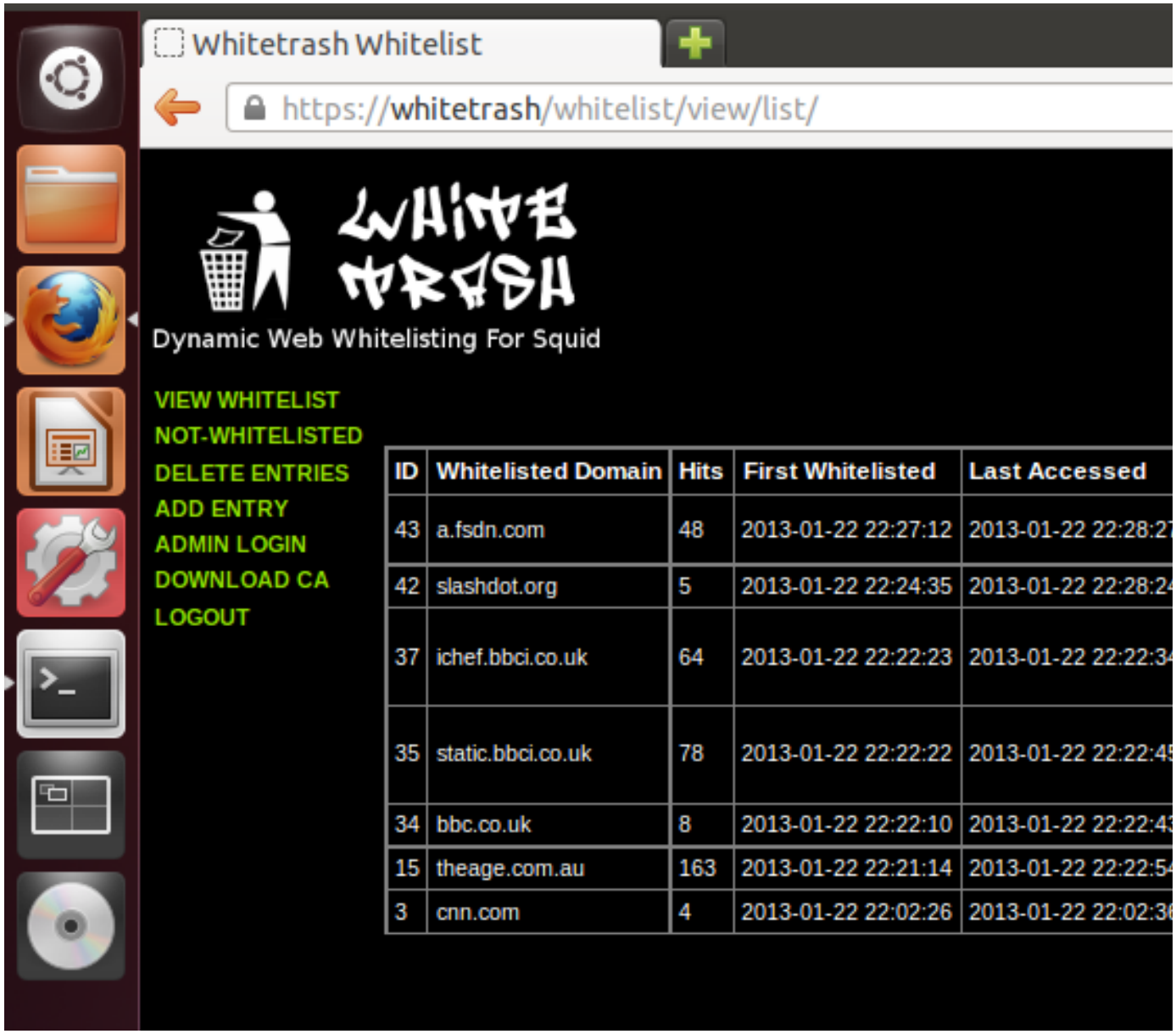

Slashdot: News for nerds, stuff that matters - Mozilla Firefox
22:27
al
Slashdot: News for nerds, stuf...
slashdot.org
Google
Slashdot
Stories
Slash Boxes
Comments
Search
Nickname:
Password:
6-20 characters long
Public Terminal
Log In
Forgot your password?
http://
Log in with OpenID
Close
Stories
Submissions
Popular
Blog
Slashdot
Ask Slashdot
Book Reviews
Games
Idle
YRO
Cloud
Hardware
Linux
About Whitetrash...
Options...
slashdot.org:a.fsdn.com
slashdot.org:slashdot.org
slashdot.org:rss.slashdot.org
slashdot.org:www.google-analytics.com
slashdot.org:widget-cdn.rpxnow.com
slashdot.org:ad.doubleclick.net

WhiteTrash

DSD
Defence Signals Directorate



WhiteTrash


Whitetrash Whitelist
https://whitetrash/whitelist/view/list/
WHITE TRASH
Dynamic Web Whitelisting For Squid
VIEW WHITELIST
NOT-WHITELISTED
DELETE ENTRIES
ADD ENTRY
ADMIN LOGIN
DOWNLOAD CA
LOGOUT
ID | Whitelisted Domain | Hits | First Whitelisted | Last Accessed
43 | a.fsdn.com | 48 | 2013-01-22 22:27:12 | 2013-01-22 22:28:27
42 | slashdot.org | 5 | 2013-01-22 22:24:35 | 2013-01-22 22:28:24
37 | ichef.bbci.co.uk | 64 | 2013-01-22 22:22:23 | 2013-01-22 22:22:34
35 | static.bbci.co.uk | 78 | 2013-01-22 22:22:22 | 2013-01-22 22:22:45
34 | bbc.co.uk | 8 | 2013-01-22 22:22:10 | 2013-01-22 22:22:43
15 | theage.com.au | 163 | 2013-01-22 22:21:14 | 2013-01-22 22:22:54
3 | cnn.com | 4 | 2013-01-22 22:02:26 | 2013-01-22 22:02:30

Pronghorn

DSD
Defence Signals Directorate

- http://github.com/pronghorn/pronghorn
- GPLed
- Block classifier

DFRWS

DSD
Defence Signals Directorate

- http://www.dfrws.org
- Since 2001
- Academics, forensics practitioners, etc.
- Annual challenge

2012 Challenge

Defence Signals Directorate

- Block classification tool
- Must be open sourced
- With extras
  - May contain a file system
  - Concurrency
  - Container support (e.g. a PDF inside a zip inside a …)
- `./toolname <file> <block size> <cores>`

Pronghorn

DSD
Defence Signals Directorate

- C
- FUSE
- ZeroMQ & Protobufs
- Third party libraries
  - The Sleuthkit

FUSE

- Filesystem in userspace
- http://fuse.sourceforge.net
- Lots of cool examples:
  - http://sourceforge.net/apps/mediawiki/fuse/index.php?title=FileSystems

The Sleuthkit

DSD
Defence Signals Directorate

- http://sleuthkit.org
- Excellent set of tools

```
alan@toshiba:~/Desktop/workspace/scratch$ istat -o 63 ./test.dd 4
Directory Entry: 4
Allocated
File Attributes: File, Archive
Size: 193263
Name: DSC_9227.jpg

Directory Entry Times:
Written:        Sun Nov 18 12:32:36 2012
Accessed:       Sun Nov 18 00:00:00 2012
Created:        Sun Nov 18 12:47:47 2012

Sectors:
1609562 1609563 1609564 1609565 1609566 1609567 1609568 1609569
1609570 1609571 1609572 1609573 1609574 1609575 1609576 1609577
```

ZeroMQ

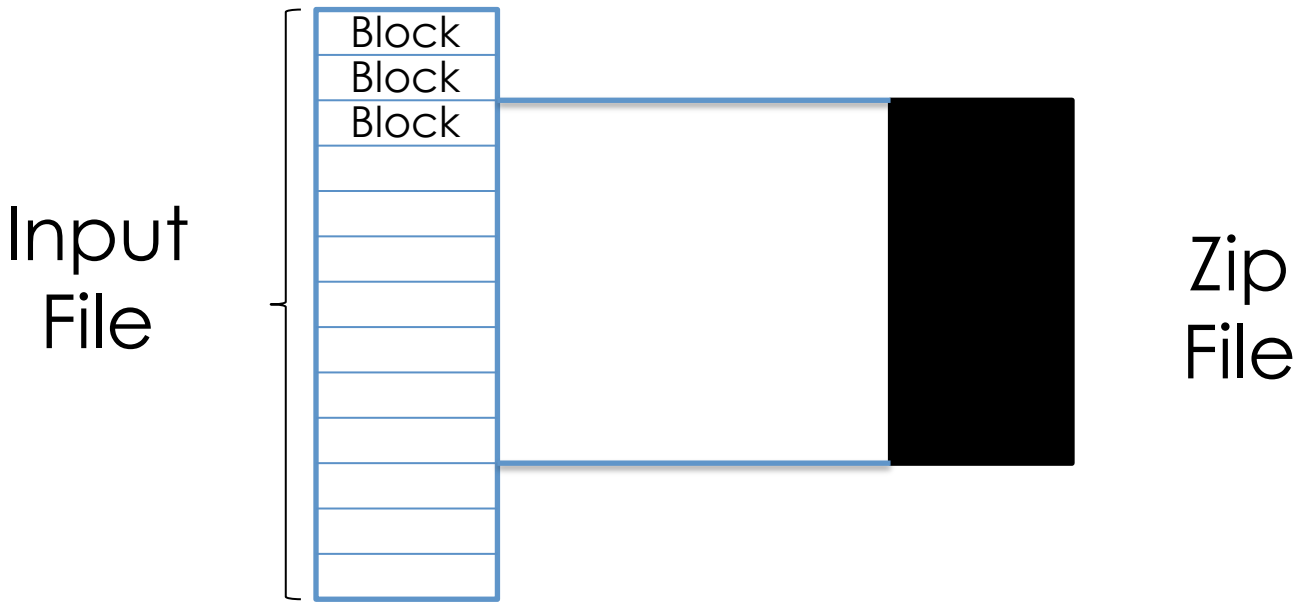
- http://www.zeromq.org
- Sockets but awesome
- You just
  - ...
  - `socket.bind('tcp://*:1234)`
  - ...
- And then
  - ...
  - `zmq_connect(zmq_socket, "tcp://localhost:1234")`
  - `zmq_msg_send(zmq_msg,zmq_socket)`
  - ...

Protocol Buffers

DSD
Defence Signals Directorate

- http://code.google.com/p/protobuf/
- We started with JSON (and it's still an option when you compile)
  - Easy to debug
  - Slow
- Protobufs showed a big speed up!

The Problem



One Approach

DSD
Defence Signals Directorate

- Have as many options as possible
  - FUSE!
- Everything becomes a path
  - Anything that can open / analyse a file can be used

Rawmount

- We can take a source to be processed (input.dd) and “rawmount” it:
  - `rawmount -o file=input.dd /mnt/point`
- The entire input.dd at any offset of any size can be accessed as a file:

```
# This is the data at offset 4096
/mnt/point/4096
# This is the first 1024 bytes at 4096
/mnt/point/4096-1024
# This is exactly the same as input.dd
/mnt/point/0
```

Rawmount

DSD
Defence Signals Directorate

- Quick Demo Time!

*mount

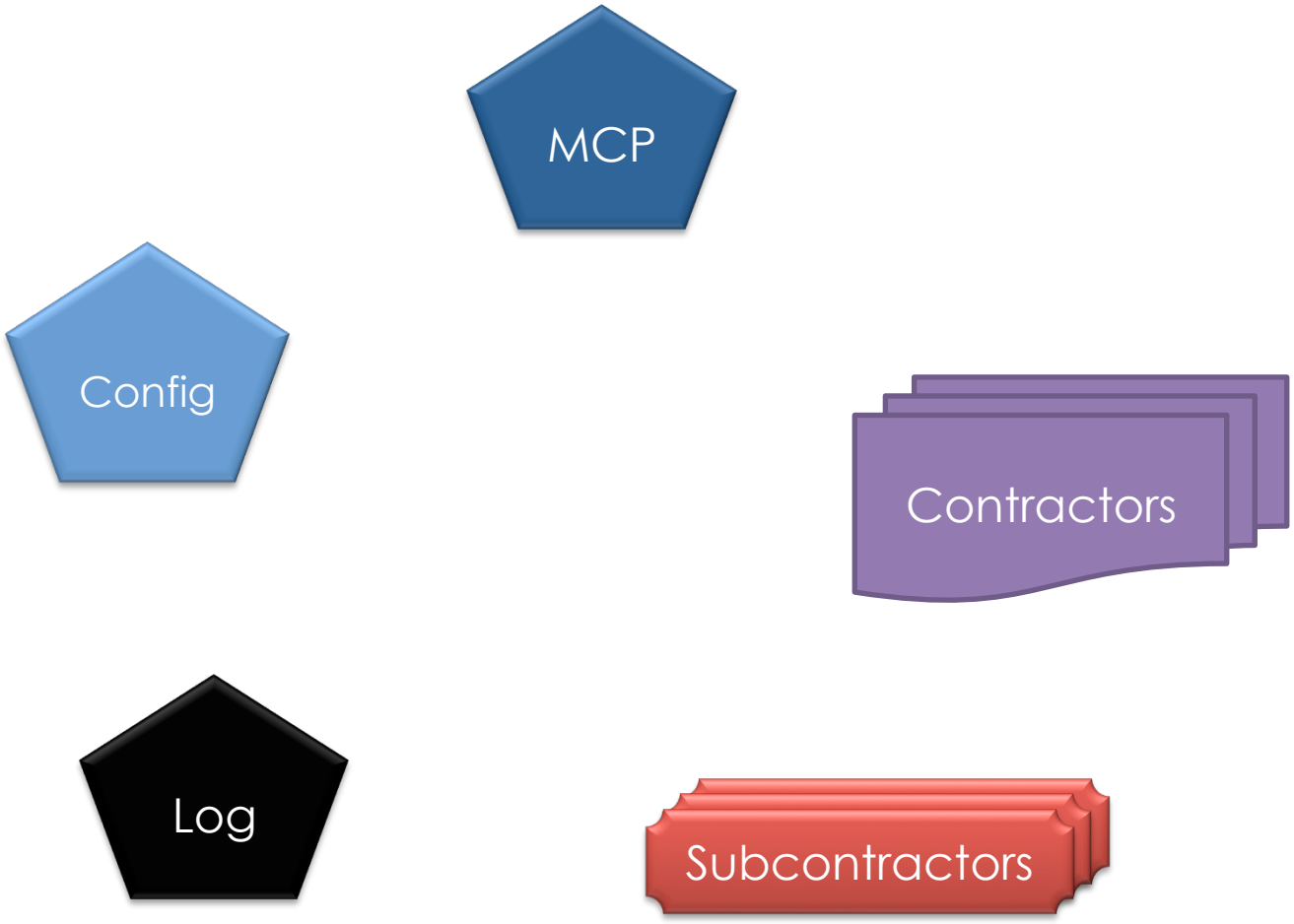
- We use this exact model for other "mounters" to find nested files.
  - e.g. We write a zip mounter
  - `zipmount -o file=/mnt/point/4096 /mnt/point/4096:mnt-zip/`
- Then
  - `/mnt/point/4096:mnt-zip/1`
  - Would be the first file in the zip
- The FUSE mounting can continue!

*mount

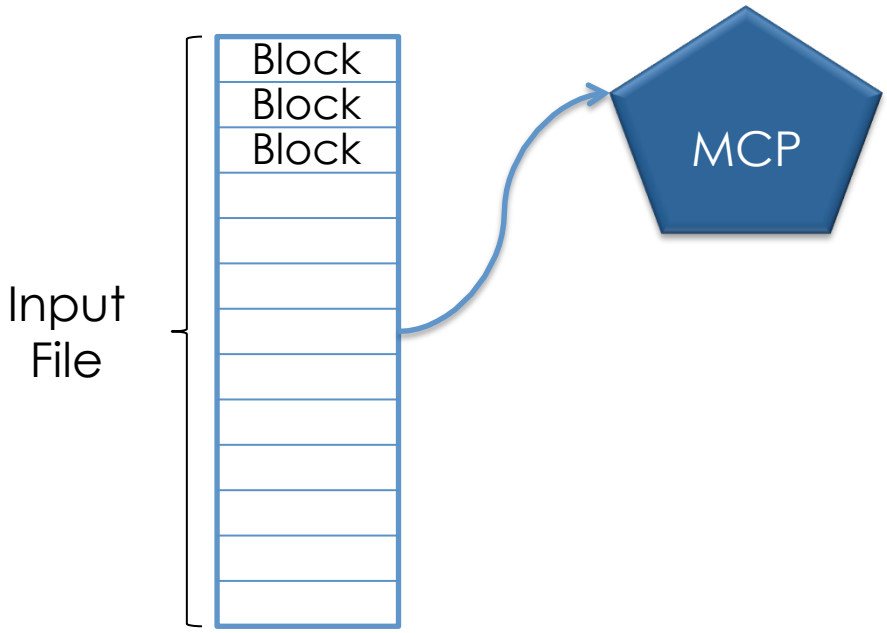
- We developed FUSE mounts for:
  - "Rawmount"
  - OLE
  - PDF
  - File Systems
  - Compressed Files
  - Images
- (We can analyse other data types, they just can't have children...)

Pronghorn Components

DSD
Defence Signals Directorate

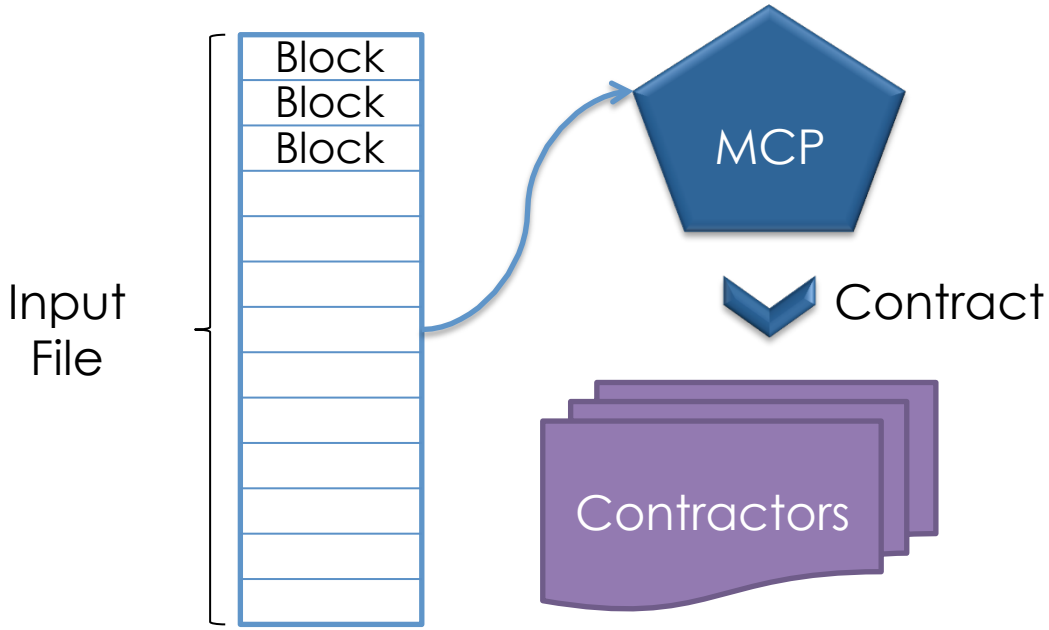


Pronghorn Workflow



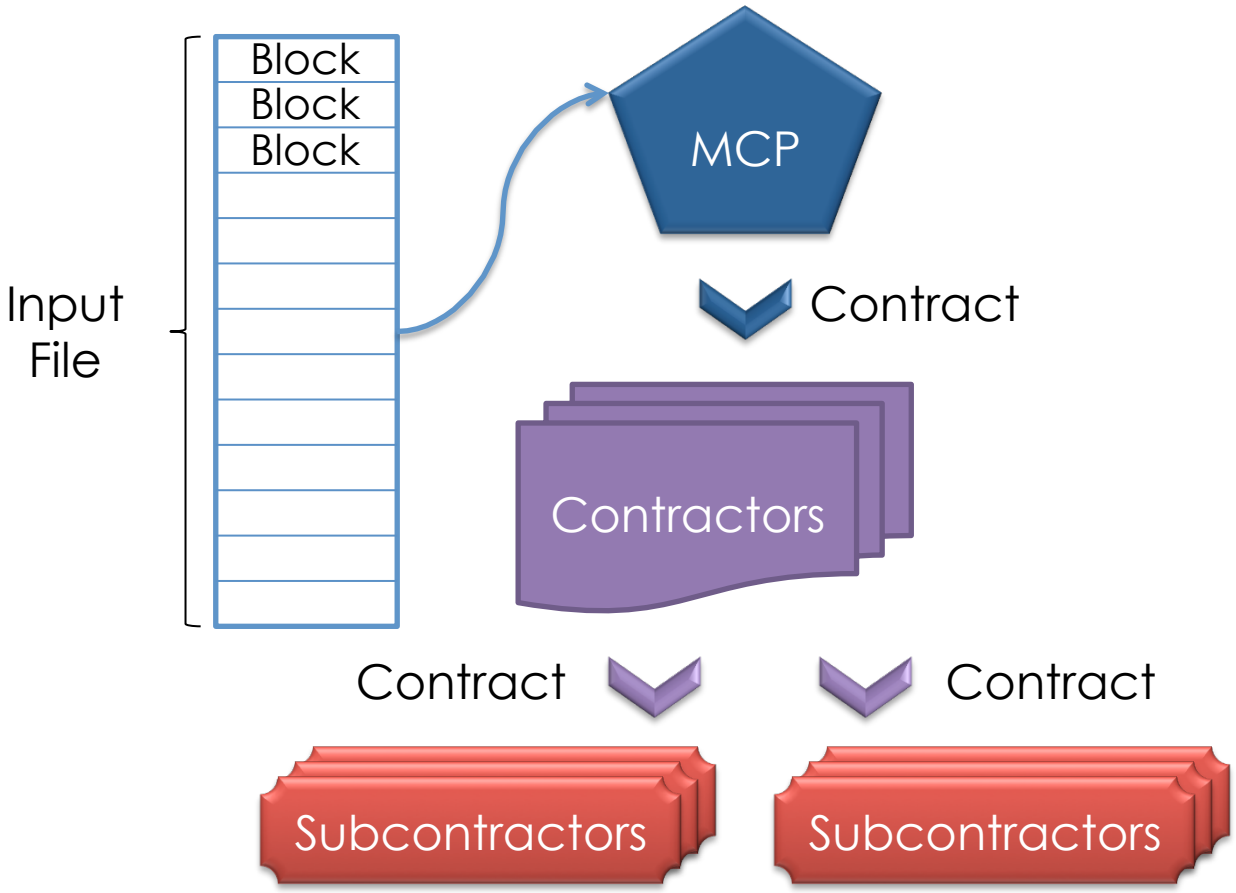
The MCP consumes blocks

Pronghorn Workflow



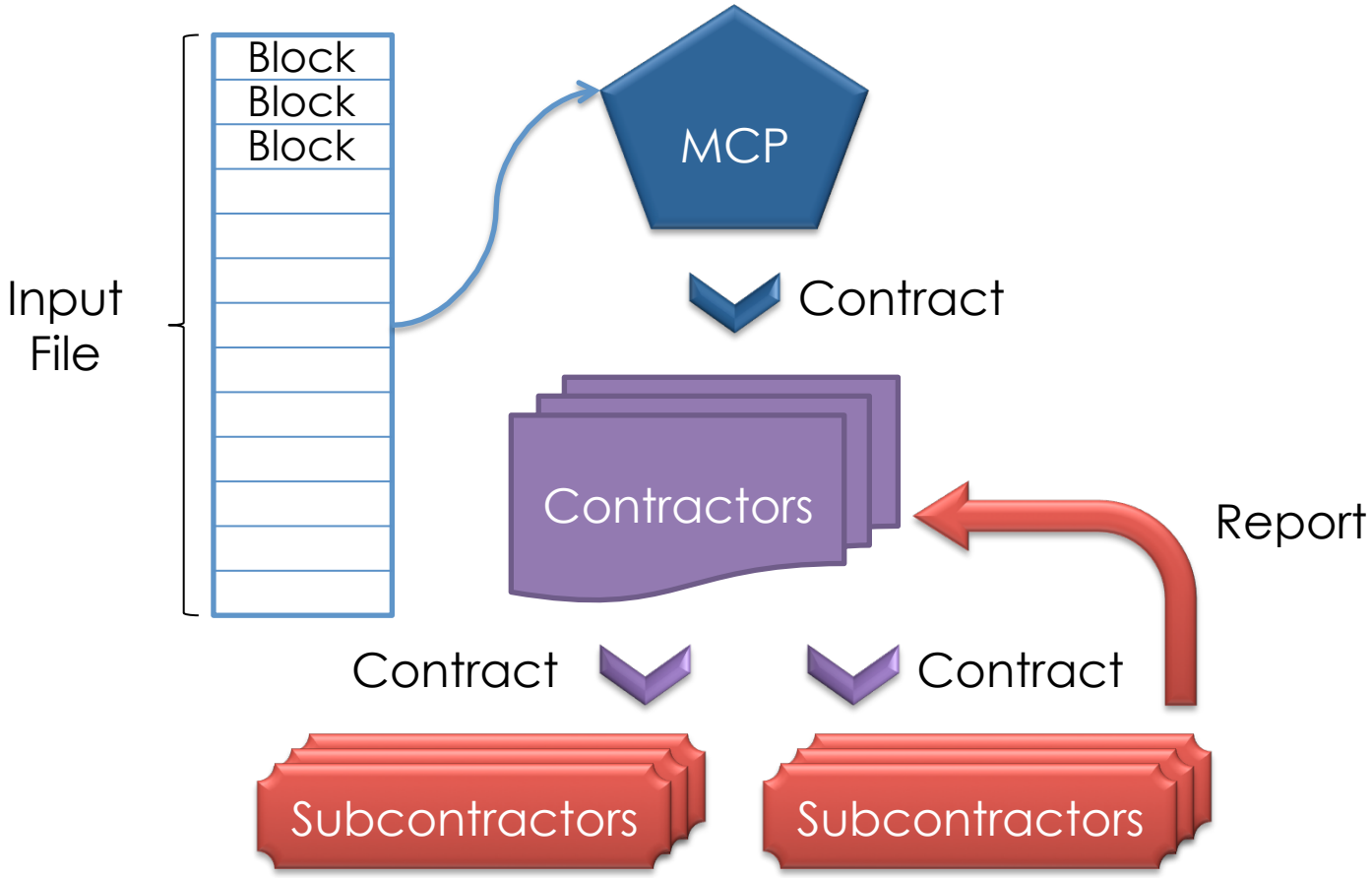
The MCP generates contracts and spawns contractors

Pronghorn Workflow



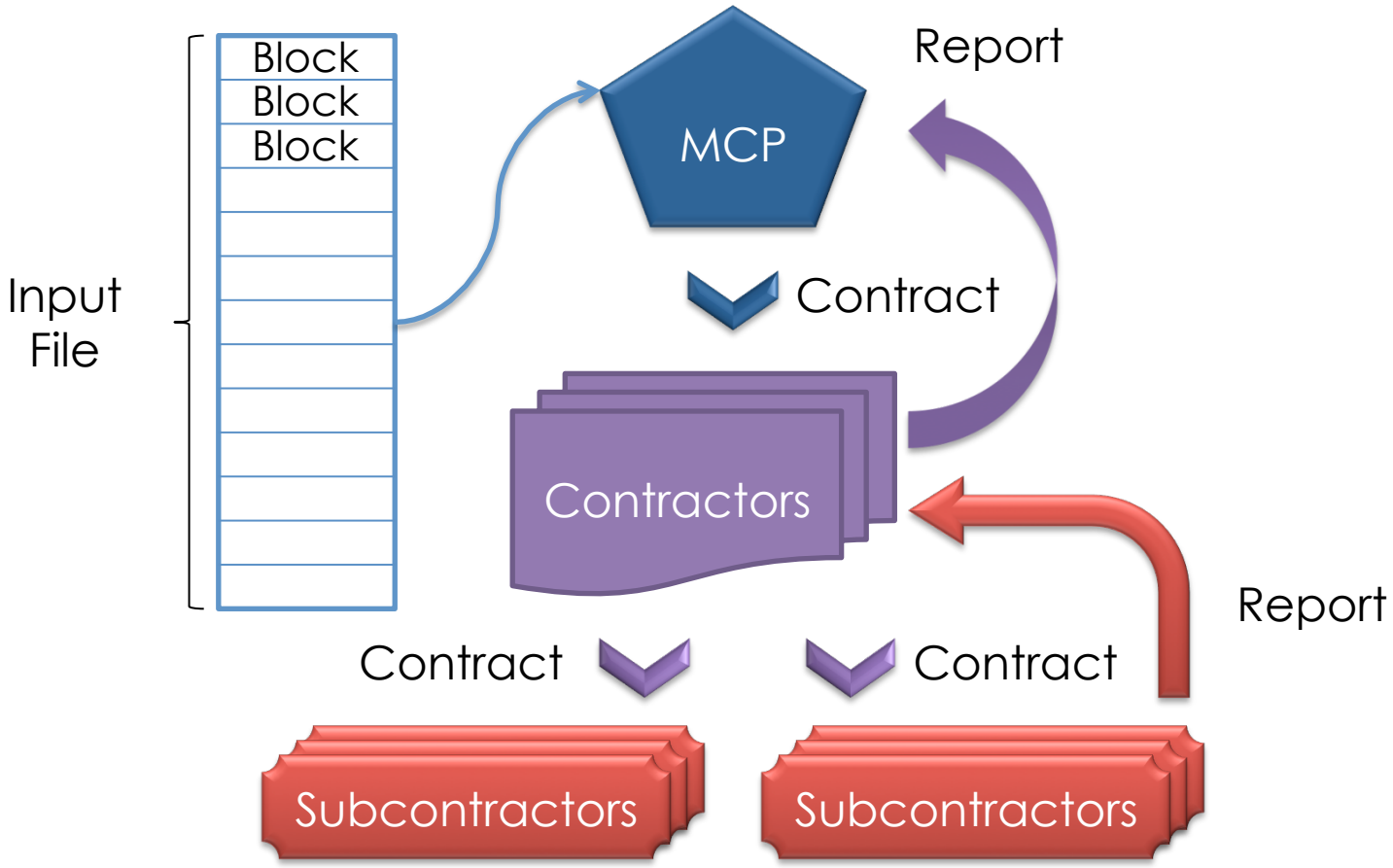
Contractors spawn subcontractors

Pronghorn Workflow



Subcontractors report their findings

Pronghorn Workflow

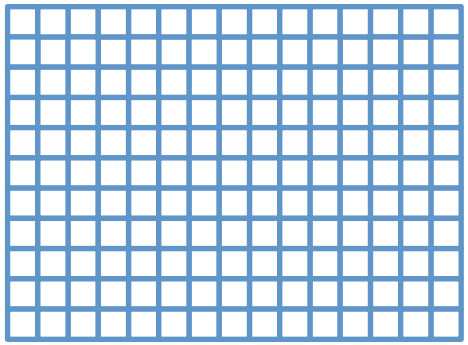


Contractors assess and report to MCP

Pronghorn Example

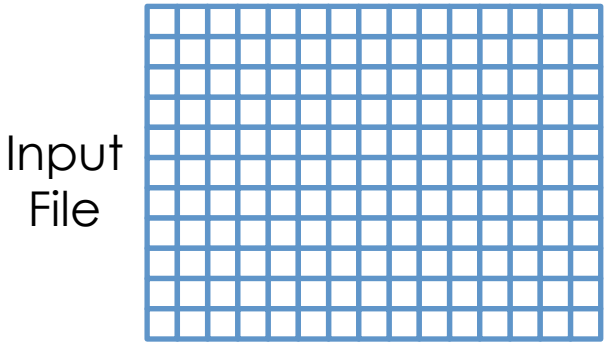
DSD
Defence Signals Directorate

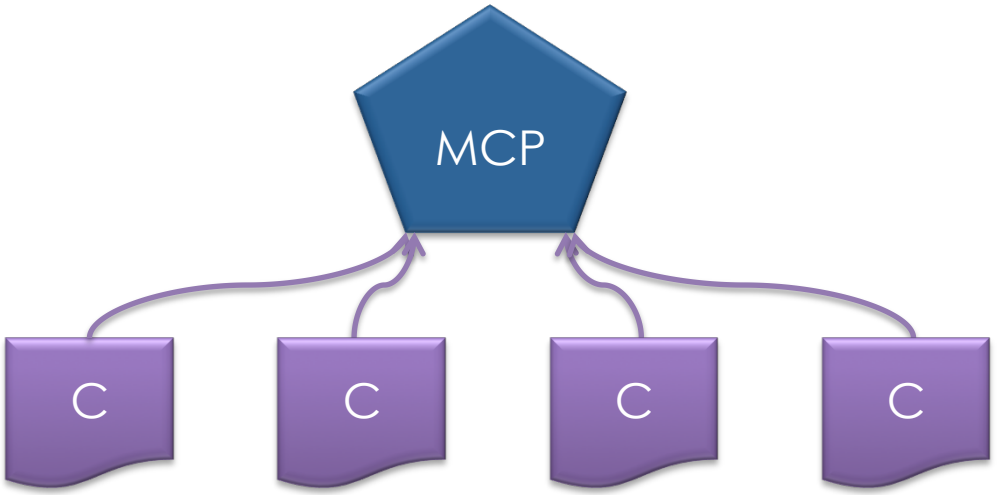
Input File



The MCP takes an input file

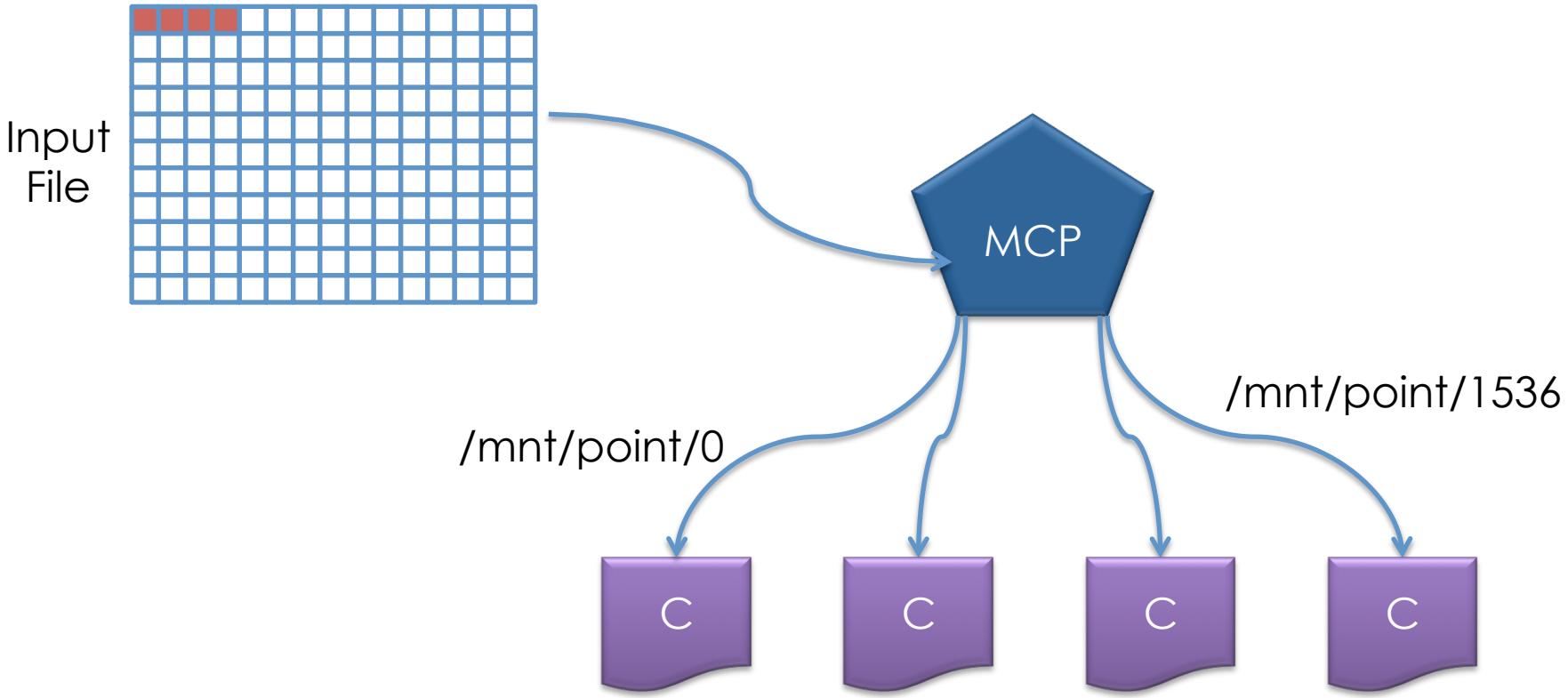
Pronghorn Example





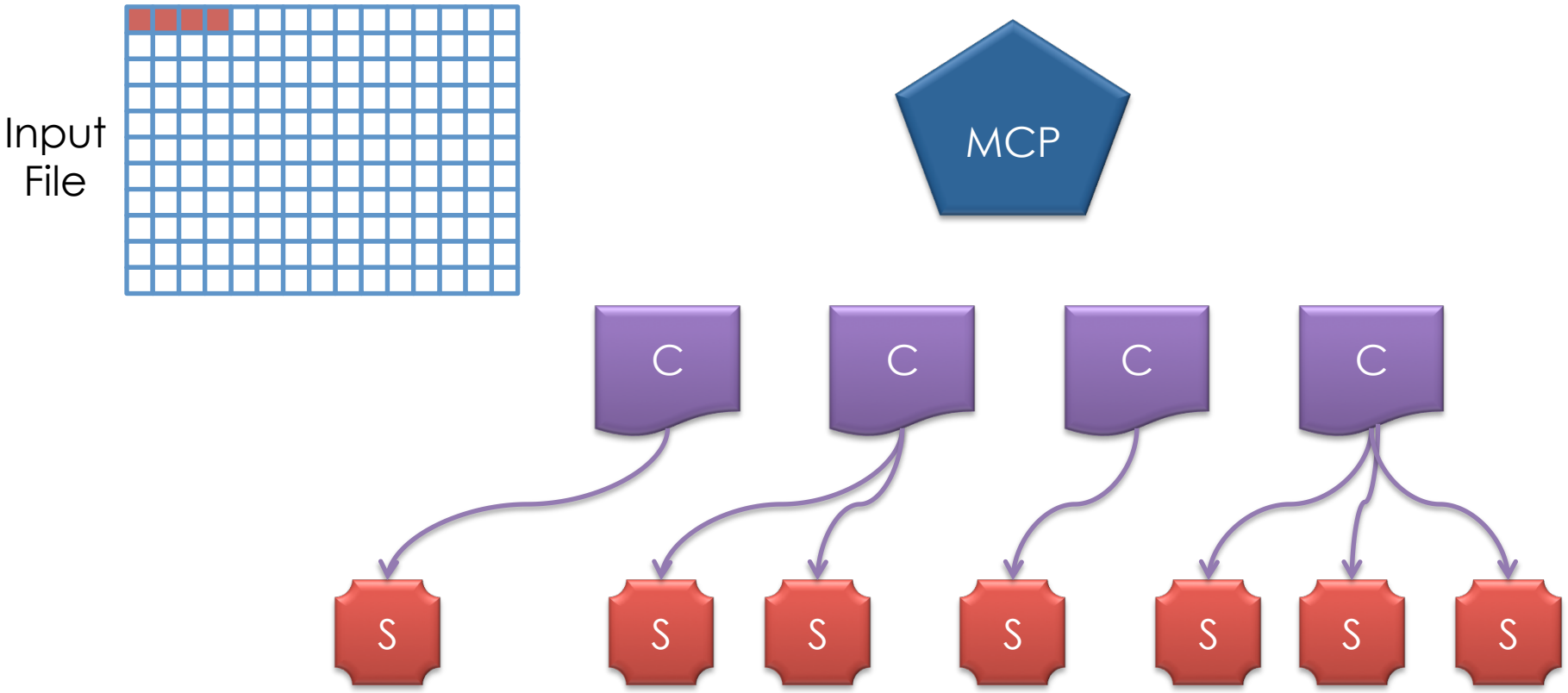
Contractors spawned, request contract

Pronghorn Example



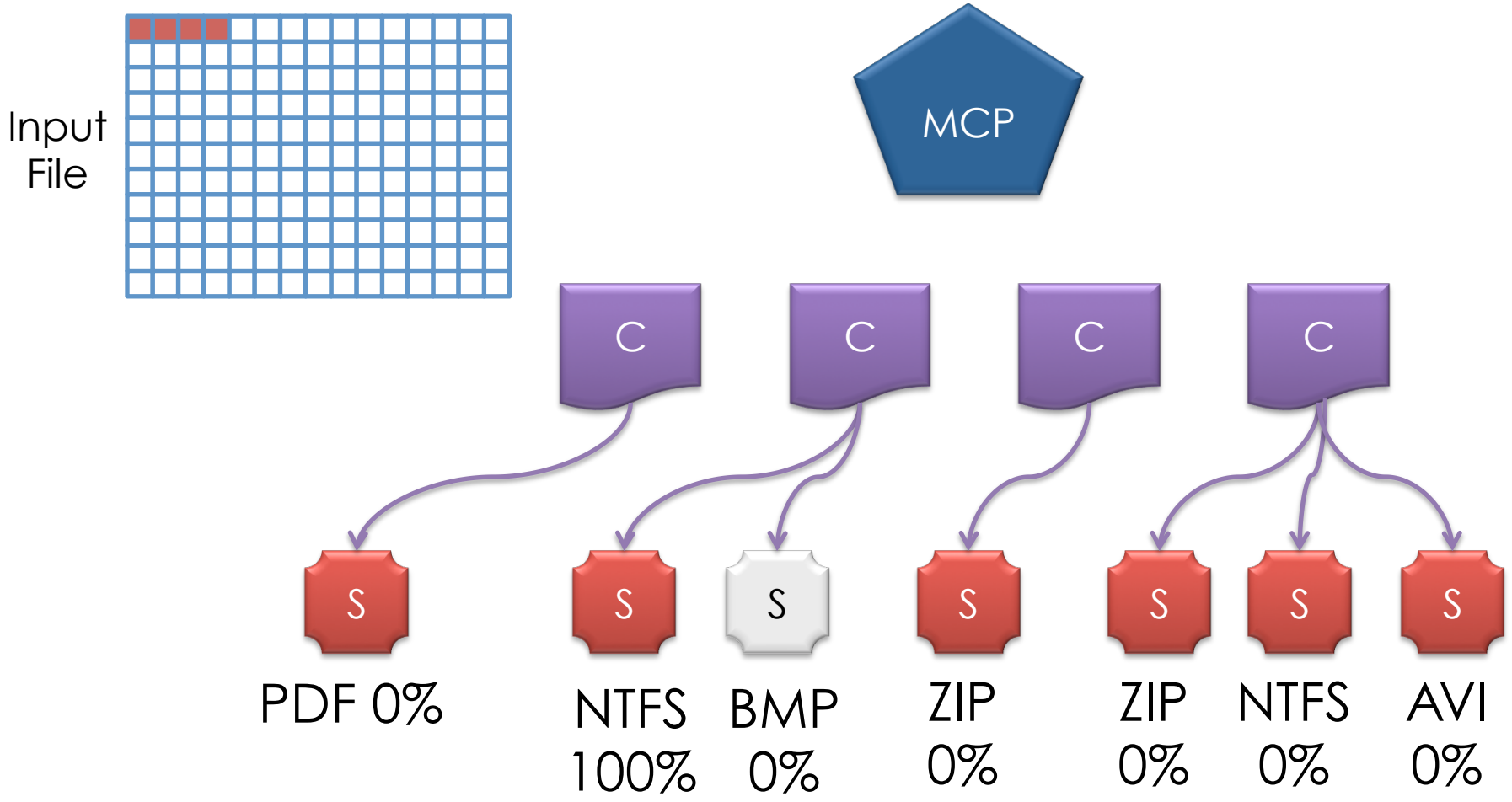
MCP allocates contract per contractor

Pronghorn Example



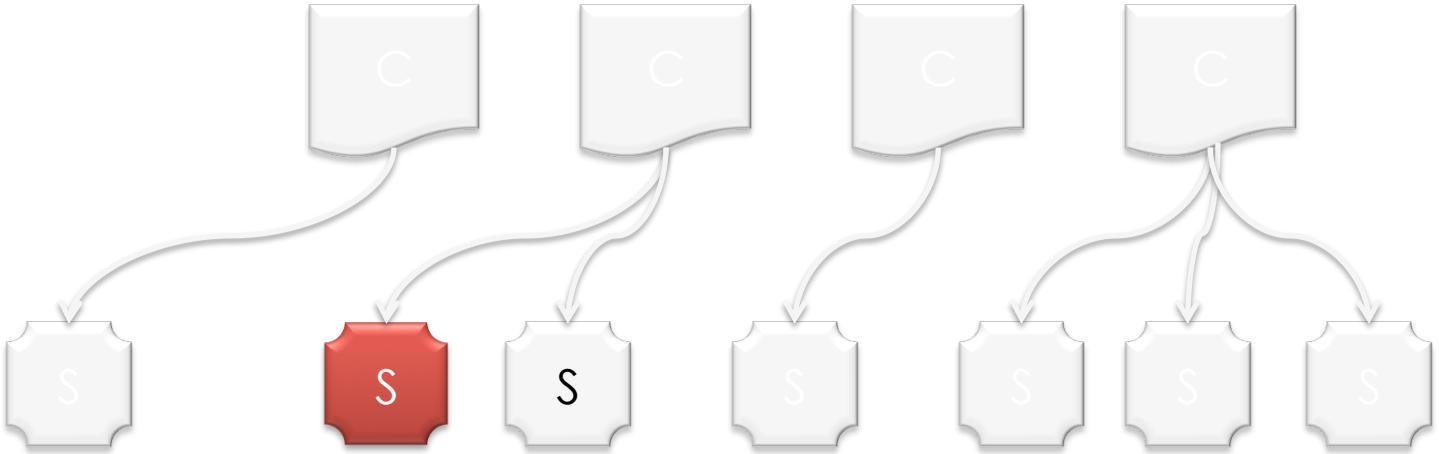
Contractors spawn relevant subcontractors

Pronghorn Example



Subcontractors perform analysis

Pronghorn Example

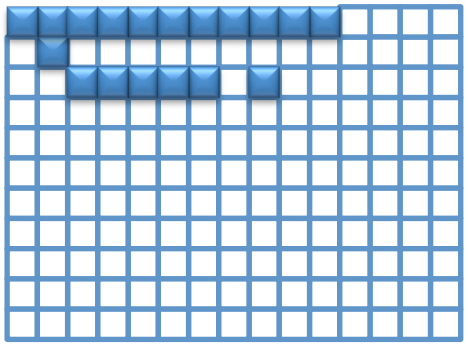


NTFS - Confidence: 100%
New Contracts Found:
/mnt/point/512:mnt-ntfs/1
/mnt/point/512:mnt-ntfs/2
/mnt/point/512:mnt-ntfs/3
/mnt/point/512:mnt-ntfs/4
Additional Blocks Claimed:
3-10, 16, 32-36, 38

Subcontractors can return additional info

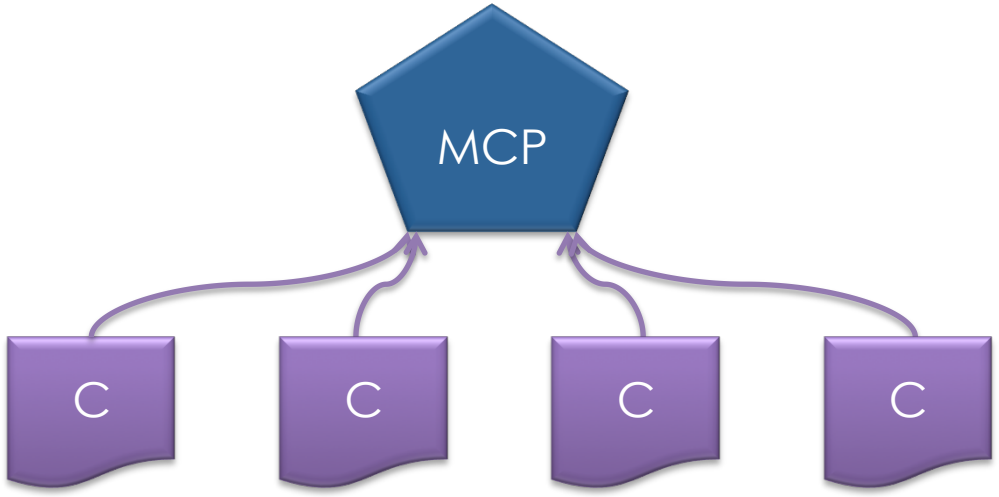
Pronghorn Example

Input File



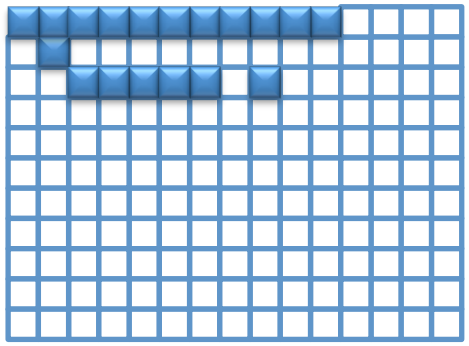
Contract queue:

/mnt/point/512:mnt-ntfs/1
/mnt/point/512:mnt-ntfs/2
/mnt/point/512:mnt-ntfs/3
/mnt/point/512:mnt-ntfs/4



Reported back to MCP, state tracked

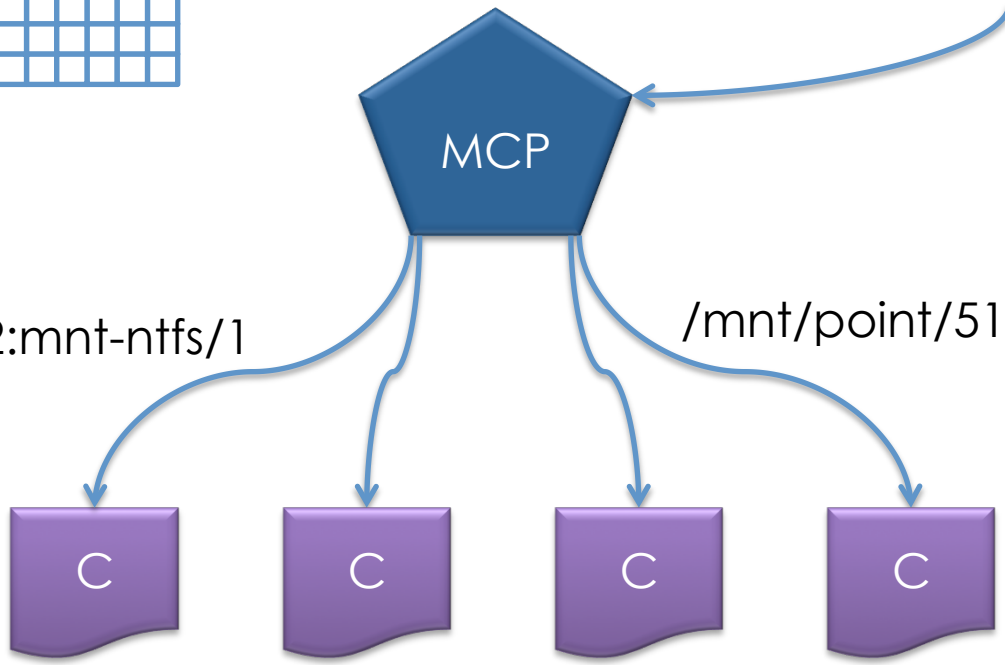
Pronghorn Example



Input File:

Contract queue:

/mnt/point/512:mnt-ntfs/1
/mnt/point/512:mnt-ntfs/2
/mnt/point/512:mnt-ntfs/3
/mnt/point/512:mnt-ntfs/4



New contracts issued, queued first

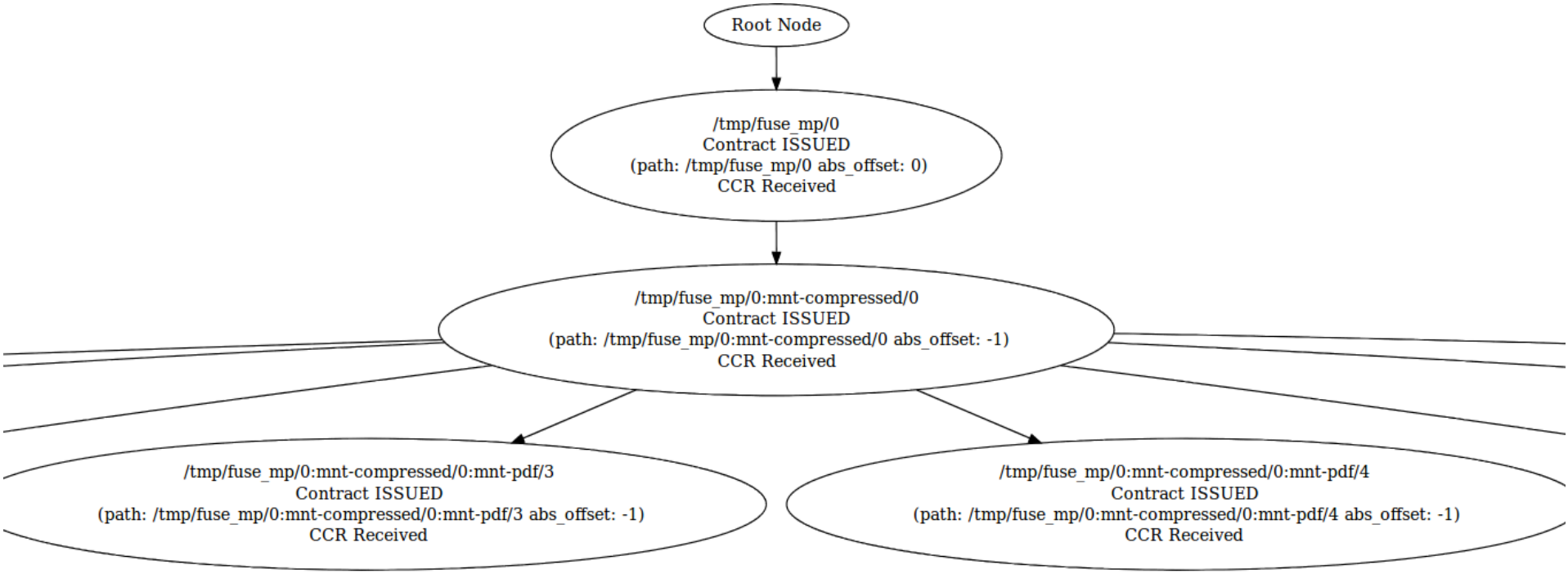
Pronghorn Example

Defence Signals Directorate

- Demo Time
  - Install:
    - `cmake .`
    - `make`
    - `sudo make install (optional)`

Some Features

- Intelligent un-mounting



Some Features

Defence Signals Directorate

- All over zeroMQ at runtime (can dynamically get/set)
- Has the basics:
  - `general.log_verbosity=ERROR`
- And some less basic (but very handy) options:
  - `subcontractor_sleuth.valgrind_opts=/usr/bin/valgrind,--log-file=/tmp/sk.log`

Pronghorn Summary

DSD
Defence Signals Directorate

- Use Cases
- Easily Extensible
- Nested Fuse
- Concurrent

Challenge Results

- Didn't win…

Conclusions

DSD
Defence Signals Directorate

- **Don't** run this on any machine you care about!
- BUT
- Pronghorn explored some new concepts, pushed a few boundaries, hopefully produced a useful tool!

Australian Government
Department of Defence

DSD
Defence Signals Directorate

Questions?

dsd.gov.au


Australian Government
Department of Defence
DSD
Defence Signals Directorate
The End.
dsd.gov.au

Squid Redirection

DSD
Defence Signals Directorate

- Allows redirection / rewriting of URLs via an external program
  - Squid passes requests to arbitrary program
- Of “upside-down-ternet” fame

Rawmount

DSD
Defence Signals Directorate

- Start at the first FUSE mount
- Remembering the ZIP example
  - Assume we have a library that can operate on “files”
  - We rawmount the input and present the library with a “file”