Study of Snort Rule-set Privacy Impact

Nils Ulltveit-Moe and
Vladimir Oleshchuk
University of Agder

Presented at: Fifth International PrimeLife/IFIP Summer School, Nice, France 7.-11. September 2009.

This work is Funded by Telenor R&I (contract DR-2009-1)

Content

- Motivation
- Introduction to Intrusion Detection Systems
- Case Study of the Snort Community Rule-set
- Results
- Conclusion and Future Research

Why is better privacy handling needed for network monitoring systems?

- *Norwegian scandal:* Minister of Defence reports the Defence Security Service (FOST) to the police for illegal surveillance of data traffic from the Government and the Royal Family.
- *Reason:* An employee in the Department of Justice got told off by FOST after *having surfed on pornographic pages...*
- FOST is responsible for *network security*, but they are not allowed to perform *surveillance* of data traffic.
- How can network monitoring organisations like FOST avoid such a scandal?

What is needed?

- Better routines and methodologies for detecting potentially privacy violating IDS rules.
- Improved classification and handling of alerts from security incidents involving private or sensitive material.
- Privacy Ombudsman responsible for the privacy side of network monitoring.
- External certification authorities that can perform privacy impact assessments.

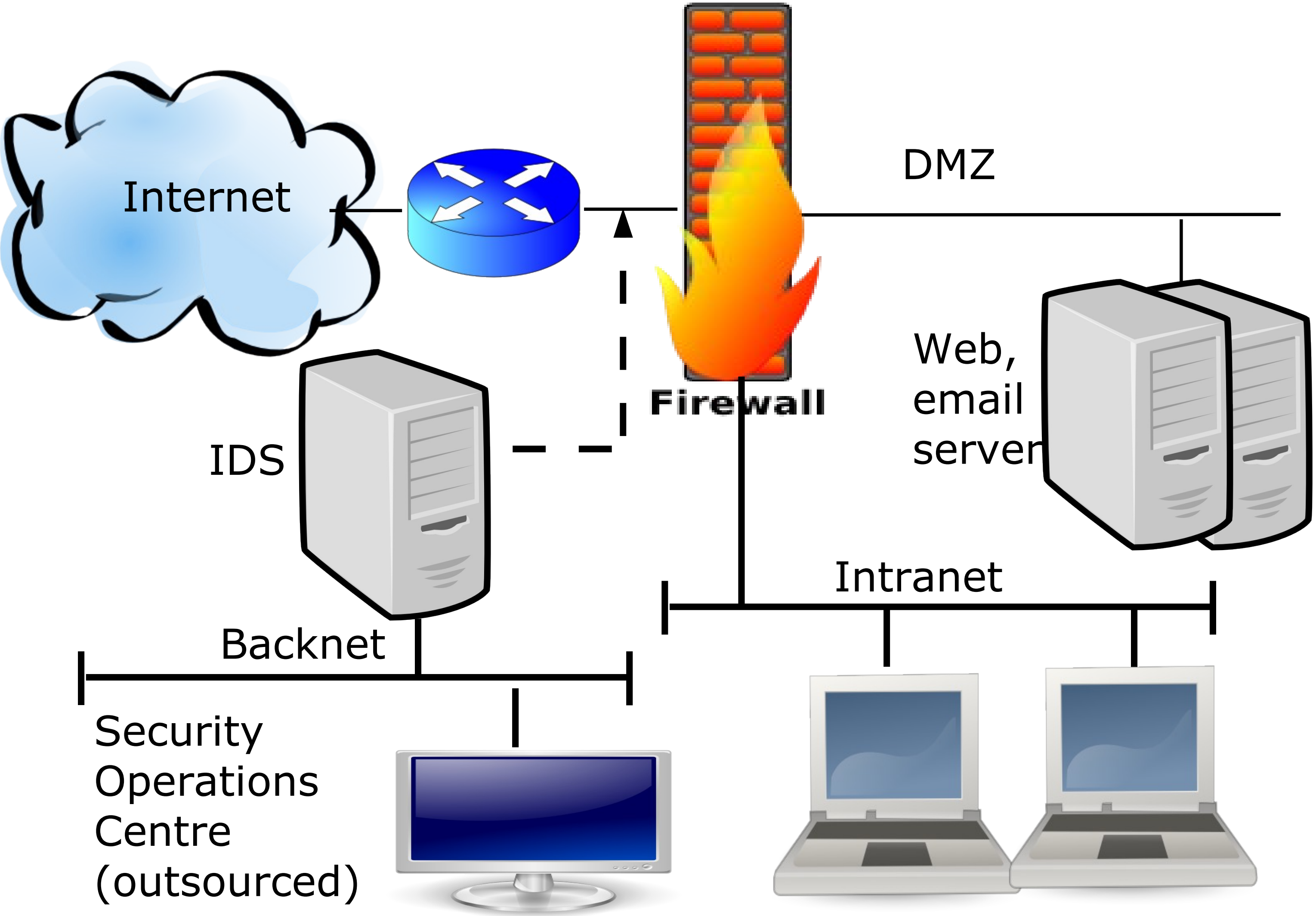
Content

- Motivation
- Introduction to Intrusion Detection Systems
- Case Study of the Snort Community Rule-set
- Results
- Conclusion and Future Research

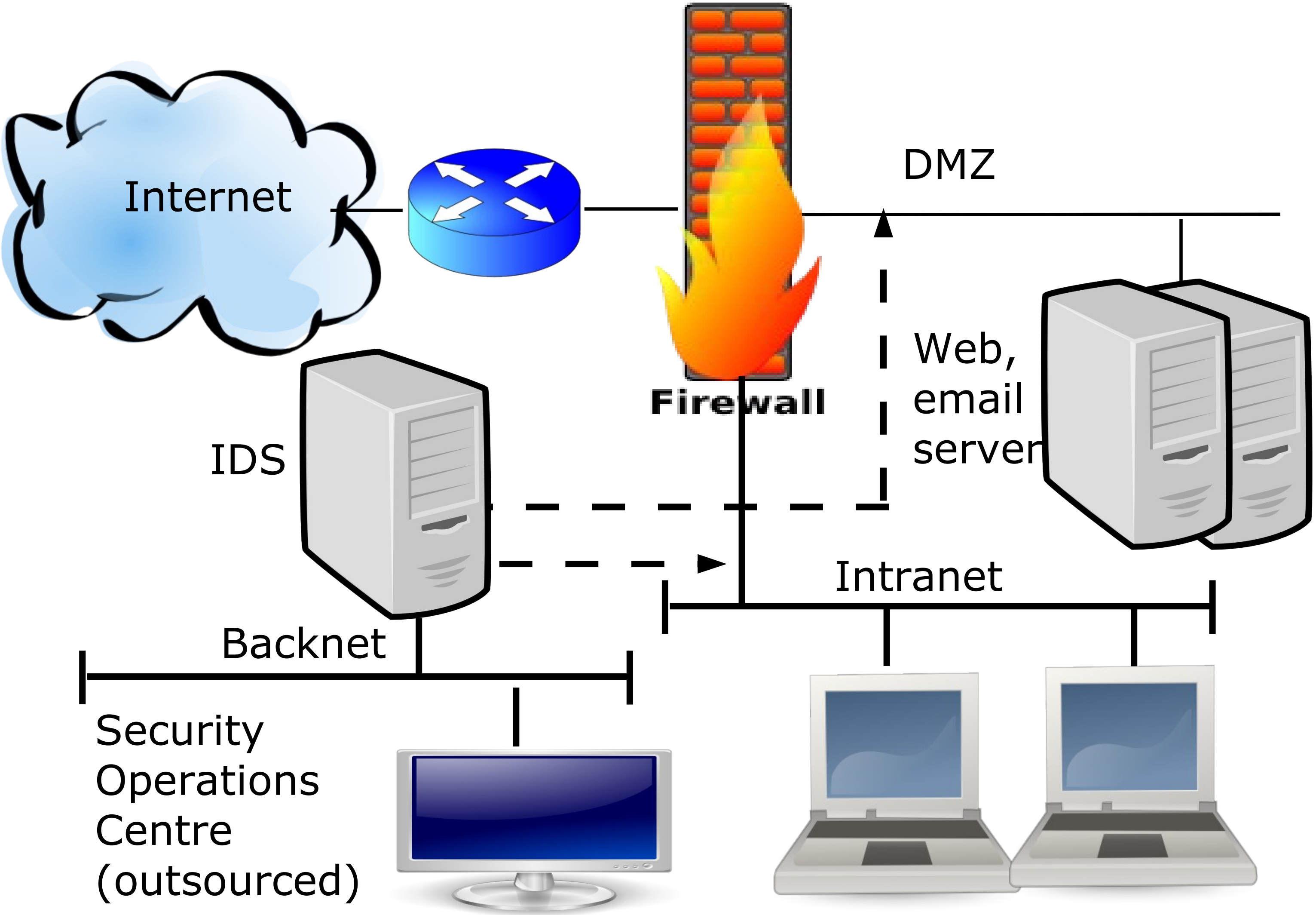
How is intrusion detection being performed?

- Intrusion Detection Systems (IDSs) - the Internet equivalent of a burglar alarm. Network monitoring is performed using *deep packet inspection*, which means that the following data can be investigated:
  - Packet header information;
  - Payload in each data packet;
  - Reassembled streams of data spanning several data packets;
  - Entire communication sessions between a client machine and a server.
- An alert is sent to a central console whenever a presumed malicious event is detected.

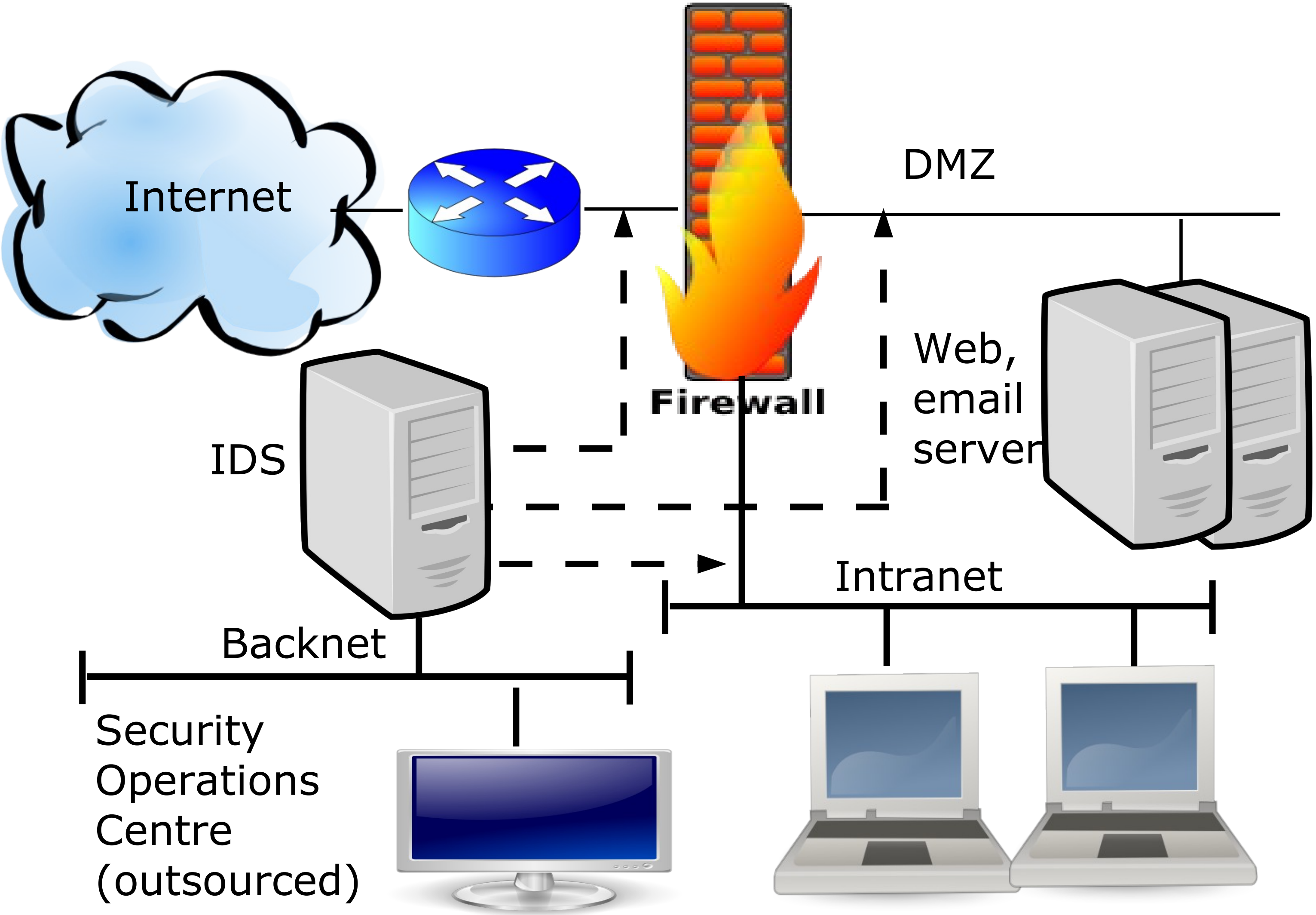
Small IDS deployment



Small IDS deployment



Small IDS deployment



Network Intrusion Detection Systems can have a significant privacy impact:

- Existing ruleset can be used to monitor:
  - peer-to-peer (P2P) file sharing;
  - download or streaming of multimedia files;
  - chat and instant messaging;
  - surfing to “inappropriate” web pages;
  - usage patterns in web shops;
  - or use of anonymisers (Tor).
- Research is therefore needed to:
  - *enhance* data privacy handling of IDS systems;
  - *quantify* expected data privacy impact;
  - *tune* the IDS rule set to minimise data privacy impact;
  - perform *automated testing* of data privacy impact.

Content

- Motivation
- Introduction to Intrusion Detection Systems
- Case Study of the Snort Community Rule-set
- Results
- Conclusion and Future Research

Case study of the Snort Community rule set.

- 3669 rules were manually categorised into two categories:
  - *Privacy Violating* (PV) rules (291 rules);
  - and *Attack* detection rules (3378 rules).
- Privacy violating rules:
  - Broad rules, monitors user behaviour or service usage that may be in violation with a stated usage policy.
  - Unspecific attack detection rules can also fall into this category.
- Attack detection rules:
  - Specific rules, expected to match *malicious traffic* only. Founded on known vulnerabilities (CVE, Bugtraq, Arachnids, McAfee, Nessus)
  - For example buffer overflow, SQL injection, XSS, backdoor, exploit...

Security considerations

- Security interest takes precedence over privacy interests for rules triggering on malicious activities.
- Considered bad if insecure services are exposed on the Internet:
  - for example telnet, finger, rsh, rexec, rlogin and open file shares;
  - Also business critical services like database servers.
- Traffic to or from unexpected services is in general bad:
  - Often used by trojans, backdoors, worms and other malware.

Attack detection rule example

```
alert udp $EXTERNAL_NET any -> $HOME_NET 1434 (\
msg:"MS-SQL Worm propagation attempt";\
content:"|04|"; depth:1;\
content:"|81 F1 03 01 04 9B 81 F1 01|";\
content:"sock";\
content:"send";\
reference:bugtraq,5310;\
reference:bugtraq,5311;\
reference:cve,2002-0649;\
reference:nessus,11214;\
reference:url,vil.nai.com/vil/content/v_99992.htm;\
classtype:misc-attack;\
sid:2003;\
rev:8;)
```

- Specific attack-matching rule, vulnerability references

Privacy Violating rule example

```
alert tcp $EXTERNAL_NET 80 -> $HOME_NET any (\
msg:"MULTIMEDIA Windows Media download";\
flow:from_server,established;\
content:"Content-Type|3A|"; nocase;\
pcre:"/^Content-Type\x3a\s*(?=[av])(video\/x\-ms\-(w[vm]x|asf)|
     a(udio\/x\-ms\-w(m[av]|ax)|pplication\/x\-ms\-wm[zd]))/smi";\
classtype:policy-violation;\
sid:1437;\
rev:6;)
```

- Broad rule
- Matches any downloaded Windows Media files via web
- No references to vulnerability sources

Content

- Motivation
- Introduction to Intrusion Detection Systems
- Case Study of the Snort Community Rule-set
- Results
- Conclusion and Future Research

Results

- Our paper focuses on privacy violating rules.
- We performed a case study using two different rule sets:
  - Full Snort rule-set
  - Default Snort rule-set (15 rule files with 285 rules disabled)

Rule set	Privacy Violating	Number of rules *)	% Privacy Violating
All rules	291	3669	7.9%
Default rule-set	177	3222	5.5%

***) Note:** *wrong column name of Table 1 in short paper.*

Privacy violations by class for *default* rule-set

Snort Class	Rules	Percent
web-application-activity	148	83.6%
attempted-reconnaissance	12	6.8%
web-application-attack	7	4%
protocol-command-decode	3	1.7%
attempted-user	3	1.7%
other	4	2.2%

- 83% of the privacy violating rules in the default rule-set consists of web application activity monitoring.
- Monitors access to web mail, shopping carts etc.
- Often founded on known vulnerabilities.
- Problematic both from a *privacy* and *security* perspective.

Privacy violations by class for *full* rule-set

Snort Class	PV- Rules	Percent
web-application-activity	148	50.9%
policy-violation	71	24.3%
kickass-porn	30	10.3%
misc-activity	14	4.8%
attempted-reconnaissance	12	6.8%
web-application-attack	7	4%
protocol-command-decode	3	1.7%
attempted-user	3	1.7%
other	4	2.2%

- 3 additional classes with privacy violating rules in full set:
  - policy-violation (71 privacy violating, 9 attack rules); pornography (30 privacy violating rules); and misc-activity (14 privacy violating, 191 attack rules).

Observations

- Web application activity monitoring cause most privacy violating rules in both rule sets.
  - Problematic both from a *privacy* and *security* perspective.
  - For example monitoring VP-ASP webshop activity.
  - or Outlook .eml files. (Rule due to the Nimda worm)
- Rule files that by default are disabled contain many privacy violating rules detecting for example: *chat*, *pornography*, *peer-to-peer* and *multimedia* streaming or download.
- Even traffic to *Tor anonymisers* can be monitored...

Content

- Motivation
- Introduction to Intrusion Detection Systems
- Case Study of the Snort Community Rule-set
- Results
- Conclusion and Future Research

Conclusion

- The default Snort rule-set contains significantly less privacy violating rules than the full rule-set.
- A concerning class of rules is *web-application-activity,* which to a large degree monitors ordinary user behaviour on the web.
  - Its lack of rule specificity is also a security risk, due to the risk of being swamped by false alarms.
  - Often founded on known vulnerabilities sources (CVE, BugTraq etc.)
- Only half as many privacy violating *policy-violation* rules as *web-application-attack* rules.

Further research on privacy violations in IDS rule-set

- This short paper analyses the privacy-invasiveness according to the *classtype* attribute of Snort rules.
- A limitation with our case study, is that it is based on a *subjective* manual categorisation.
- It would be useful to reach consensus on *objective* criteria for categorising IDS rules as *attack*- or *privacy violating* rules.
- Further research is needed on how to deal with rules where privacy and security objectives are in conflict.
- How to deal with IDS rule ageing.

Thank you!

Questions?
Comments?
Good ideas?