Experience with Network Anomaly Detection on Industrial Networks

Andrew Ginter
Industrial Defender

ICSJWG 2010 Spring Conference

Agenda

- Anomaly detection – whitelisting vs blacklisting
- Anomaly detection & firewall retrofits
- A simple anomaly detection script
- Incidents, remediations
- Wrap-up

Anomaly Detection

- Blacklisting = conventional intrusion detection / prevention
  - Rules / signatures define what is bad
  - Everything else is allowed
- Whitelisting = anomaly detection
  - Rules / signatures define what is good
  - Everything else is not allowed
- Many sophisticated packages: traffic volumes, learning algorithms, time-of-day compensations

Control Systems

- Smaller and simpler than enterprise systems
    - Said to be good fit for anomaly detection
    - Safety imperative makes thorough understanding of systems and networks desirable
- We rarely see anomaly detection systems deployed
- Is there value in anomaly detection on control systems?
- Are complex anomaly detection features really needed?

Customer Reactions

- At the perimeter – unauthorized communications, even attempted unauthorized communications, are of great concern.
- Monitoring control network internal communications is of interest, especially for complex networks, but only if there are not a lot of false positives.
- Considerable interest in using anomaly detection as a means of simply and continuously characterizing control network communications.

Simple Anomaly Detectors

- Snort
- Firewall session logs
- A simple script

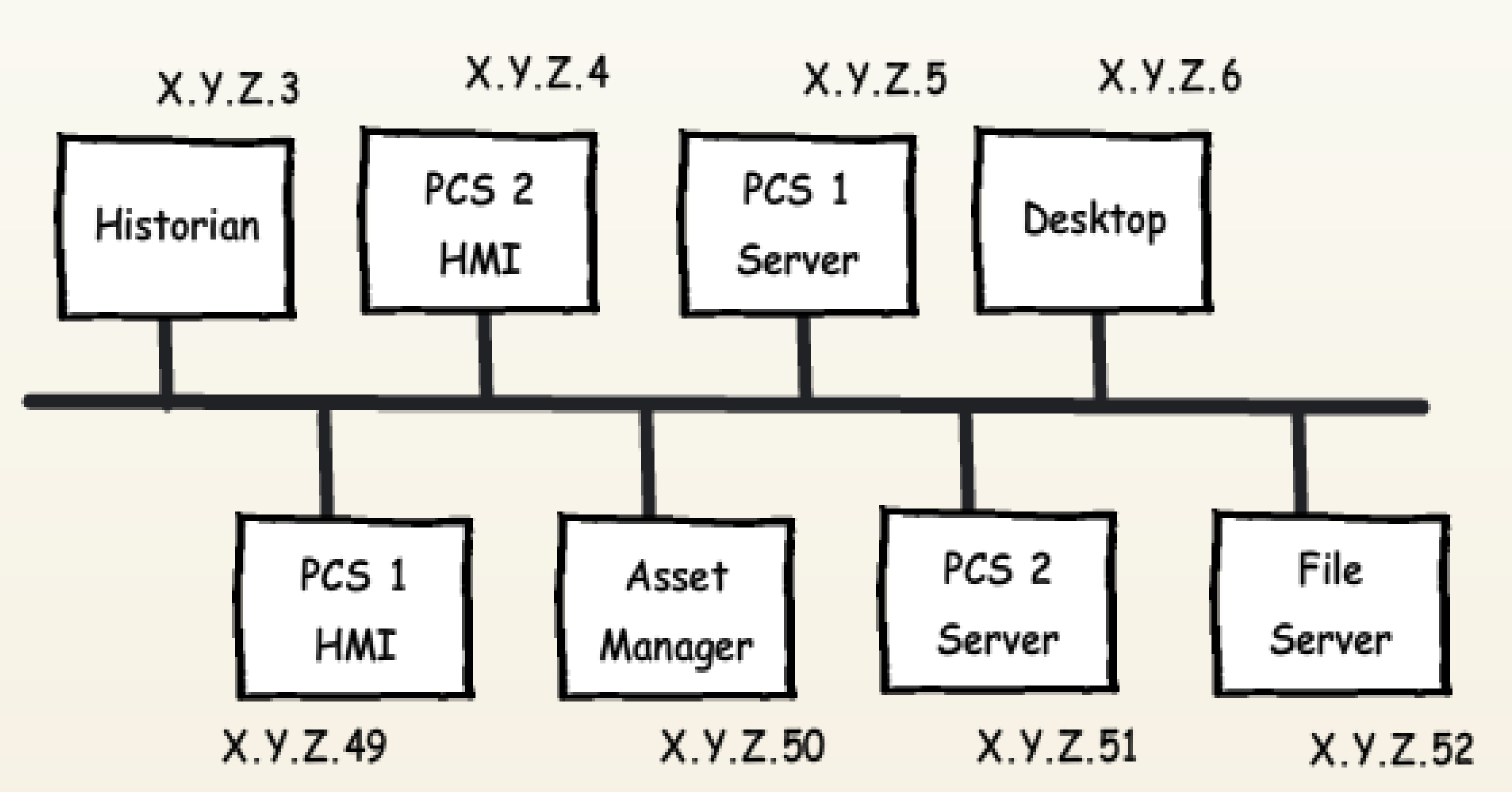
Snort as Anomaly Detector

- Pass rules + “catch all”
  - pass udp 192.168.1.* any -> 192.168.2.1 53
  - Alert any any any -> any any (msg:”unauthorized traffic”)
- Noisy – alert for every anomalous packet
- Fancier anomaly detection preprocessors exist

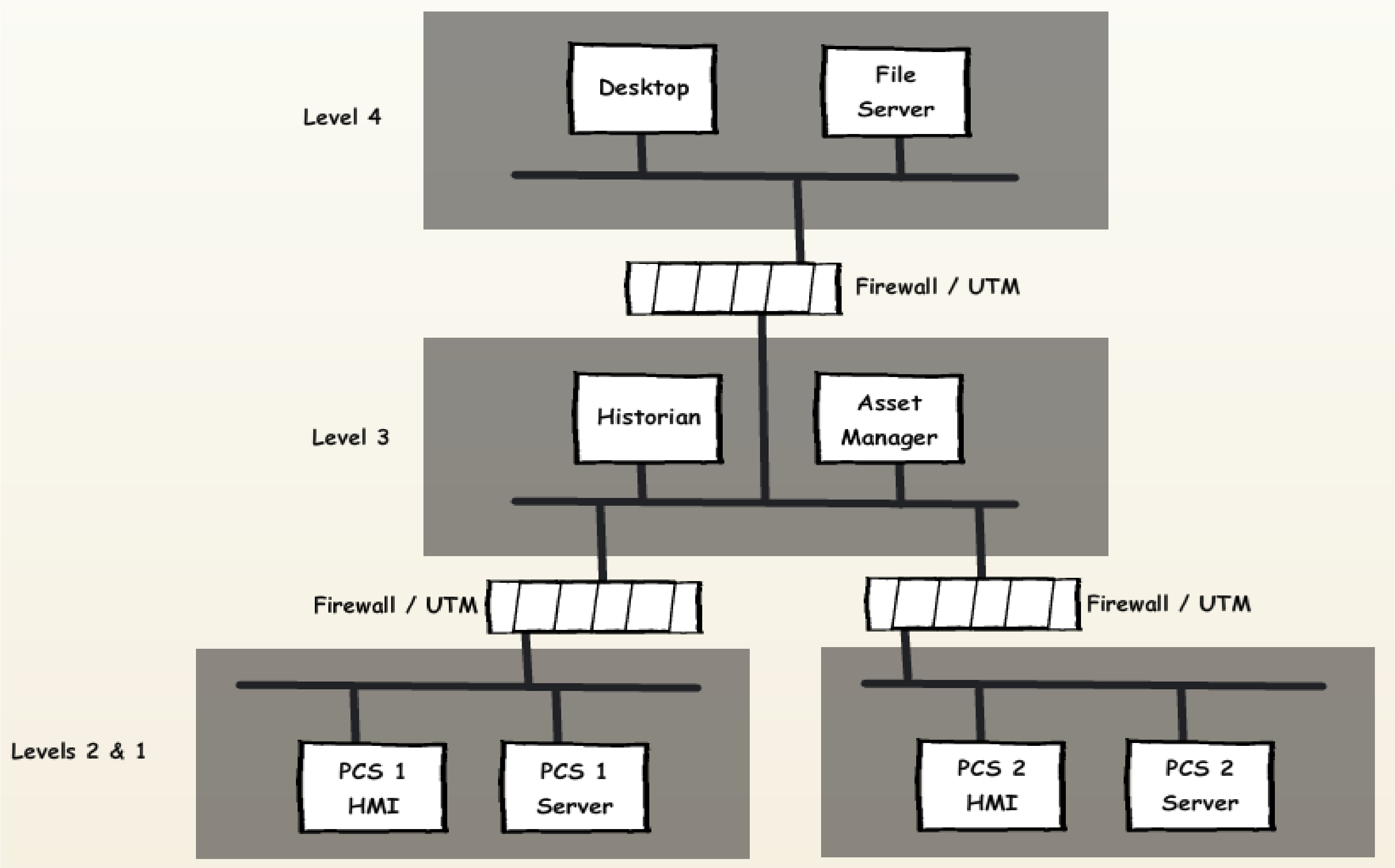
Firewall Session Logs

- Firewall = anomaly-based detection/prevention
  - Allow tcp 192.168.1.1:* -> 192.168.2.1:53
  - Allow/Deny all (log sessions)
- Firewall anomaly detection used routinely for L2 firewall retrofits

Firewall Retrofit - Before



Firewall Retrofit - After



Firewall Retrofit Methodology

- Use “level 2 router” mode – aka: bridging mode, transparent mode
- Start with “allow all (log sessions)” rule
- Evaluate session log, create rules for legitimate traffic
- Compare to test bed results
- Run for a period of time, evaluate new anomalies
- Replace “allow all (log sessions)” with “deny all” rule

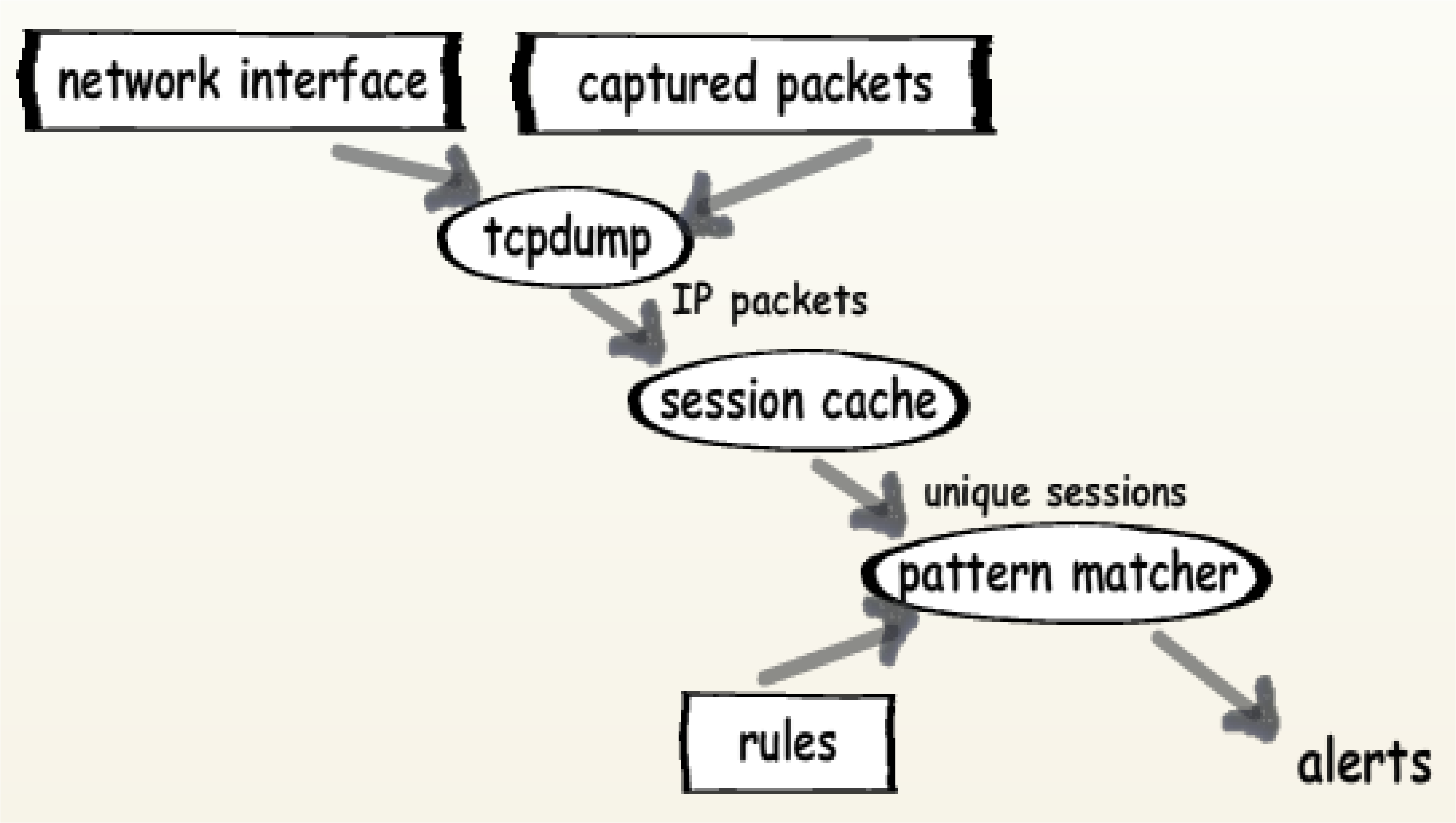
Experience with Firewall Retrofit

- Most L3/L4 retrofits are one day's effort, with ~50 rules
  - Some sites let “accept all (log sessions)” rule run for a while before replacing with “deny all” rule.
- L2/L3 retrofits are less common and more difficult
  - More communications & so more rules
  - Generally “accept all (log sessions)” rule runs for much longer, to gain assurance of correct operation
- L2/L3 retrofits are becoming more common

After Retrofit

- Operations staff are confident they understand cross-zone communications patterns
- Operations staff generally turn packet logging off – too noisy
- Managed customers get daily reports summarizing dropped packets

Anomaly Detection: A Simple Script



Sample Output

```
192.168.31.191:39977    17.9.8.2:993          tcp    (/imaps)
239.255.255.250:1900    192.168.31.8:1024     udp    (/)
192.168.31.198:50114    173.8.8.12:993        tcp    (/imaps)
192.168.91.31:58683     192.168.31.39:80      tcp    (/www http)
192.168.91.31:58684     192.168.31.39:80      tcp    (/www http)
192.168.91.31:CLIENT    192.168.31.39:80      tcp    (/www http)
192.168.95.11:34840     192.168.31.53:443     tcp    (/https)
192.168.95.11:34841     192.168.31.53:443     tcp    (/https)
192.168.95.11:CLIENT    192.168.31.53:443     tcp    (/https)
```

Sample Rules

```
# High-volume connections
A udp 192.168.31.2 53 *.*.*.* *                # DNS server
A udp 192.168.31.2 * *.*.*.* 53
A udp 192.168.31.* * 192.168.31.* 53           # DNS Clients
A udp 192.168.31.* * 192.168.90.38 53
A tcp 192.168.31.* * *.*.*.* 443               # HTTPS comms to world
A tcp 192.168.31.* * *.*.*.* 80                # HTTP comms to world
```

Experience with Sessions Script

Site	Sessions	TCP ports	UDP ports	IP addresses	TCP/UDP/ICMP
1	465	27	16	93	42/34/17
2	1177	32	33	144	62/33/4
3	708	41	18	102	62/26/12
4	569	9	11	60	52/31/18
5	168	38	25	111	59/35/6
6	566	44	18	98	59/25/17
7	224	13	15	74	51/33/16
8	643	49	19	111	55/33/12
L3	4259	29	26	618	42/53/4
QA	382	101	20	40	78/20/3

Experience with Anomalies Script

- Small control networks of 50-100 hosts can be characterized manually in less than a day.
- Larger networks would benefit from automatic host classification and rules grouping

Incident: Automatic Updates

- XP systems caught communicating with Microsoft website
- Policy: automatic updates disabled on all L2 and L3 equipment – no updates until tested
- Investigation:
  - Automatic updates were disabled, per policy
  - Communications attempts went away only when Automatic Updates service was stopped.
- Remediation: stop the service

Incident: Network Driver “phoning home”

- Several machines caught initiating communications to an IP address on the open internet
- Investigation:
  - Network driver manager was found to be contacting vendor's website. Reason for contact was not determined.
- Remediation:
  - None – egress filtering blocked communications

Incidents (many): Corporate IT Scanning

- Anomaly-based firewall deployment frequently finds corporate IT groups scanning control system computers with “nmap” and other tools.
- Investigations vary: often look into who is doing the scanning more to educate IT as to safety and availability requirements of PCS networks and equipment.
- Remediation: generally block scans at the L3/L4 firewall.

Incident: Unauthorized Historian Clients

- In a large enterprise, repeated communications sessions with plant historian client port are found coming from another continent.
- Investigation:
  - Plant personnel have a complete list of who is authorized to log into the plant historian and which IP addresses they connect from.
  - No match for offending sessions.
- Remediation: block all but authorized IP addresses at the L3/L4 firewall.

Conclusions

- Anomaly detection has value on control networks:
  - as part of firewal retrofit discipline,
  - to detect new kinds of communications, especially at the perimeter, and
  - to continuously characterize communications in a way that supports human comprehension and review
- Anomaly detector on small control networks can be calibrated manually. Large control networks would benefit from additional automation.

Work in Progress

- Hypothesis: the best learning system is one which organizes rules in a way that supports manual review for correctness.
- Evaluate COTS and open source anomaly detection tools against this hypothesis and other control system requirements.

INDUSTRIAL DEFENDER®

www.industrialdefender.com