COMP3052.SEC Computer Security

Session 12: Intrusion Detection

Acknowledgements

- Some of the materials we use this semester may come directly from previous teachers of this module, and other sources ...
- Thank you to (amongst others):
  - Michel Valstar, Milena Radenkovic, Mike Pound, …

This Session

- Network Attack Models
  - Insider Attacks
- Intrusion Detection Systems
  - Network and Host-based
- Protocol Analysis
- Signature Detection
- Anomaly Detection

Intrusion & Detection

- Security Intrusion:

  ‘A security event, or a combination of multiple events that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or asset without authorisation.’

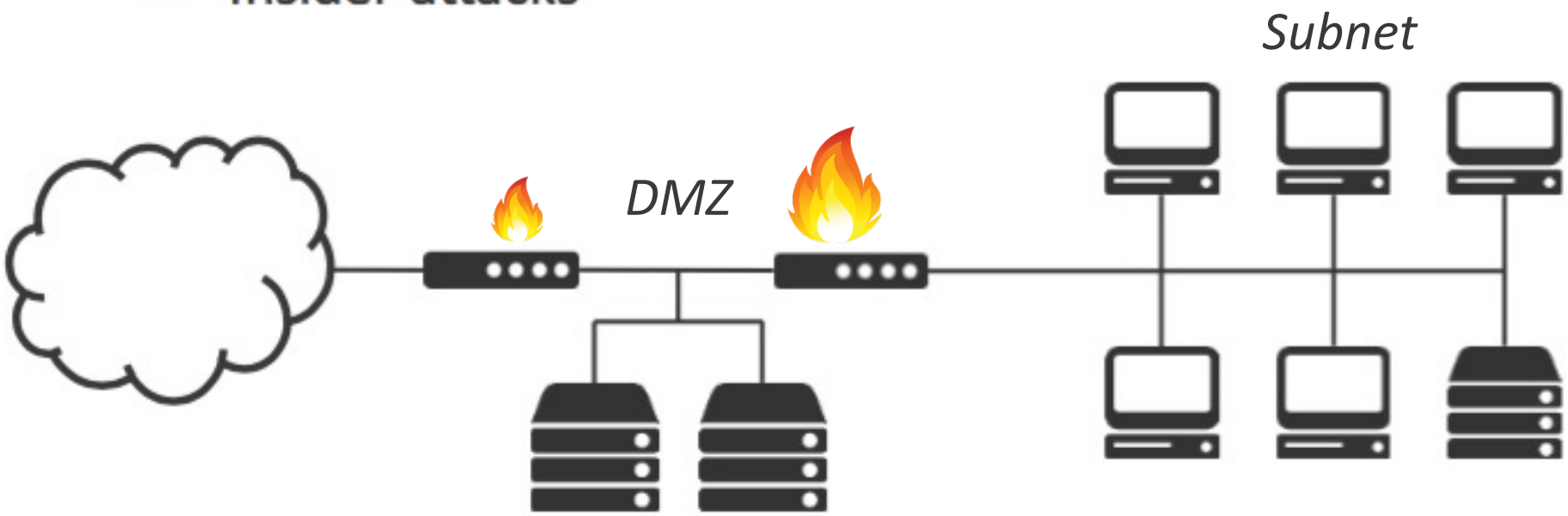
- Intrusion Detection

  ‘A security service which monitors and analyses system events for the purpose of finding and providing (near to) real-time warning of attempts to access assets in an unauthorised manner’

- Internet Security Glossary RFC 2828

Network Attack Models

- Firewalls don't protect against:
  - Attacks using valid protocols
  - Insider attacks



Intruders

- Masquerader
  - An outsider who is an unauthorised individual who gains access via a legitimate user account
- Misfeasor
  - An insider who is a legitimate user, who misuses access permissions and privileges
- Clandestine
  - Subject who seizes supervisory control to evade auditing

Insider Attacks

- The most difficult to detect and prevent
  - often simply an HR issue
- Employees will have intimate knowledge of both system layouts and potentially vulnerable services
- Motivated by revenge or entitlement
  - corporate espionage
  - More recently, whistleblowing
- Intrusion detection and system monitoring is the only defence against insiders

Anti-virus Teaser

- Signature-based Detection:
  - Store some small code signature for each virus
  - Scan files either in bulk or at runtime, compare with the signatures on file
  - Generic signatures
- Heuristics:
  - Determine what actions and rules a virus program will normally adopt
  - Start the program in a VM and see what it does
- Machine Learning

Misuse vs. Anomaly

- Misuse detection
  - Based on signatures
  - Can miss novel or variant attacks
  - Unsuitable for zero-day attack detection
- Anomaly detection
  - Detects deviations from normal behaviour
  - Can generate too many false alerts
  - What is defined as ‘normal’ can change over time

Current IDS Issues

- Misuse detection is pretty straightforward
  - need to increase the speed of updating the signature database
- Anomaly detection is by no means solved
  - still massive research effort worldwide
  - look for novel solutions outside of statistical machine learning
  - cope with changing user and network behaviour

Intrusion Detection/Prevention

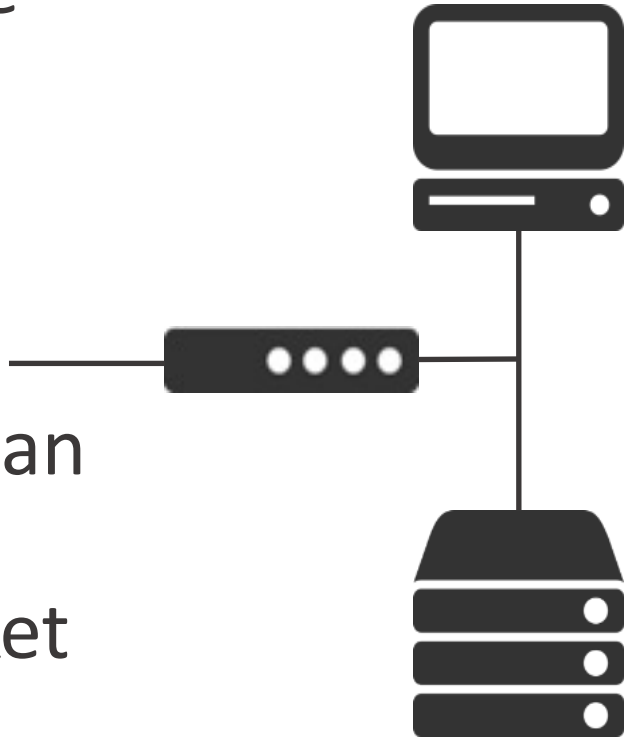
- Intrusion Detection Systems (IDS)
  - Detects possible intrusion attempts
  - Generates alerts and logs for administrators
- Intrusion Prevention Systems (IPS)
  - Identical to IDS except also stops the attack

IDS Deployment

- Network-based:
  - Monitors network traffic and analyses a variety of packets from different protocols to identify suspicious activity
- Host-based:
  - Monitors the characteristics of a single host to find suspicious activity including resource / app usage
  - In many ways modern Anti-Virus does this

Network-based IDS

- Placed at a viewpoint on a network to examine and analyse traffic
  - Installed on a firewall or in a DMZ
  - Installed behind a screened subnet
- May perform deeper analysis than many firewalls, e.g. stateful protocol analysis and deep packet inspection

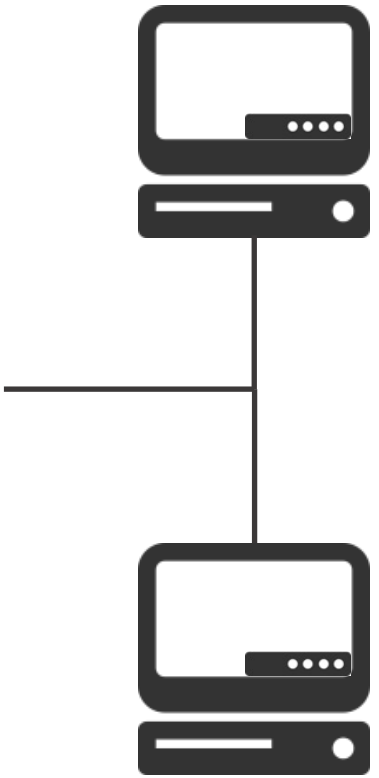


Network-based IDS

- Can monitor traffic from multiple hosts
  - Enables use of correlation techniques
    - which can be very powerful
- Can be difficult to detect fragmented packet based attacks
- Harder to detect phishing or trojan attacks
- Better at detecting DDoS attacks
- Deep packet inspection rarely used

Host-based IDS

- Additional layer of security software running on a host within a protected LAN or VPN
- Creates a profile of usage for specific users
- Can monitor both the internals of a host including CPU, memory use, application use and the network stack



Host-based IDS

- Can easily correlate network with host behaviour
  - can inspect more useful data
- Can perform deep packet inspection
- Can deal with packet fragmentation
- Only gets insight from a single machine
- Lends itself more to anomaly-based techniques

Components of IDS

- Sensors / Agents: collect and collate data from multiple viewpoints on a network
- Analysers: ascertain if an intrusion has taken place
- Reporting: notify the administrators via alerts, usually a console or graphical interface is required

Multiple sensors allow us to distribute analysis, but centralise computing overhead

Detection Modes

- Stateful Protocol Analysis
  - More complex version of a stateful packet filter
- Signature-based Detection
  - Fingerprinting sequences of operations or packets
- Anomaly-based Detection
  - Build a model of “normal” and find deviations

Protocol Analysis

- Hold detailed session information on protocols being used, examine for attacks:
  - Why is this user logging in as root?
  - Why is this command being sent a 1000 byte buffer as a parameter?
- Computationally costly, and requires the IDS to have all possible versions of these protocols described in its database

Signature-based Systems

- Like antivirus, signatures are created and stored in a database
  - operations rather than binaries
- If operations match a defined signature, then an alarm is triggered
- Include some form of attack language
  - Mechanisms to describe sequences of events
  - Maintain and monitor intermediate states and event transitions

Signature-based Systems

- The pros and cons of these systems are identical to their anti-virus counterparts
  - Computationally efficient
  - Will always spot a known attack or vulnerability
  - Will always miss an unknown attack or vulnerability
  - Detailed signature databases must be kept up-to-date

Example Signature

- What are the signs that a host on the network is performing port scans?
  - Large amounts of ICMP traffic
  - Many TCP connection (SYN) packets
  - These connections going to a variety of other hosts

“If a host establishes more than three TCP connections to different hosts in five seconds, it is port scanning”

SNORT

- Snort is a powerful and well established IDS
  - Also free!
- Uses rules to analyse network packets, and then can provide alerts or logging

Snort Rule Example

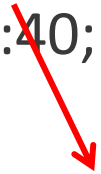
- Rule outline:

  action proto src-ip src-port direction dst-ip dst-port (options)

- Buffer Overflow?

  activate tcp any any -> 192.168.1.21 22 (activates:1;
  msg:"Possible SSH exploit"; content:"|90|"; \ offset:40;
  depth:75; dsize: >6000;)

  dynamic tcp any any -> 192.168.1.21 22 (activated_by:1;
  count:100;)



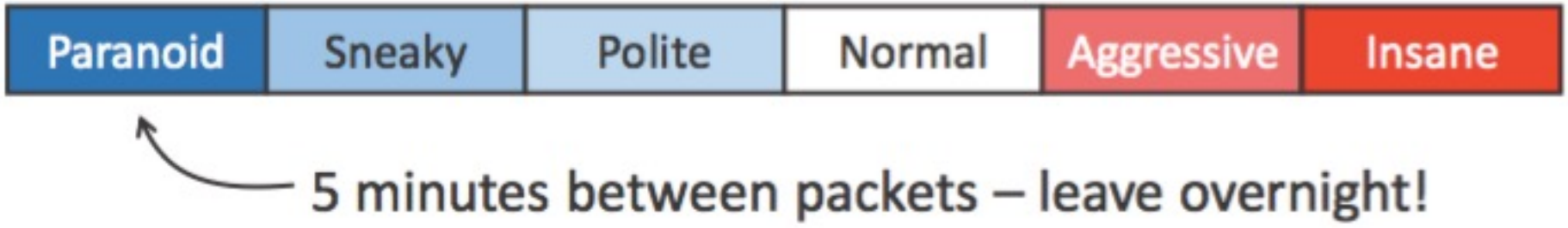
Detecting Nmap

- Snort has built in rules for detecting Nmap, a logged scan may look like this:

```
08/xx-13:27:32.464097 TCP src: 10.0.4.100 dst: 10.0.4.1 sport: 3537 \
dport: 5232 tgts: 1 ports: 11 flags: ******S* event_id: 0

08/xx-13:27:32.464177 TCP src: 10.0.4.100 dst: 10.0.4.1 sport: 3538 \
dport: 5002 tgts: 1 ports: 12 flags: ******S* event_id: 7

08/xx-13:27:32.464256 TCP src: 10.0.4.100 dst: 10.0.4.1 sport: 3539 \
dport: 780 tgts: 1 ports: 13 flags: ******S* event_id: 7

08/xx-13:27:32.465642 TCP src: 10.0.4.100 dst: 10.0.4.1 sport: 3540 \
dport: 1484 tgts: 1 ports: 14 flags: ******S* event_id: 7

08/xx-13:27:32.465722 TCP src: 10.0.4.100 dst: 10.0.4.1 sport: 3541 \
dport: 2002 tgts: 1 ports: 15 flags: ******S* event_id: 7

etc. ...
```

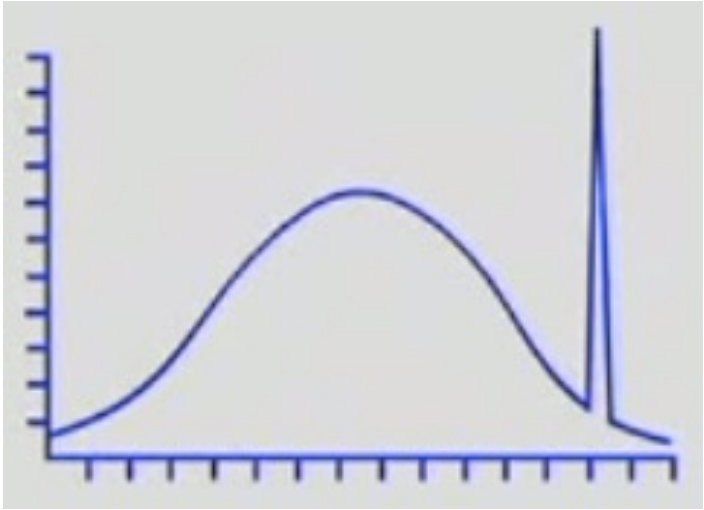
Nmap Timings

- You can avoid detection when using Nmap by reducing the speed of the scan
- This makes port scanning very hard to distinguish from general network noise
- Nmap contains 6 timing options



Anomaly Detection

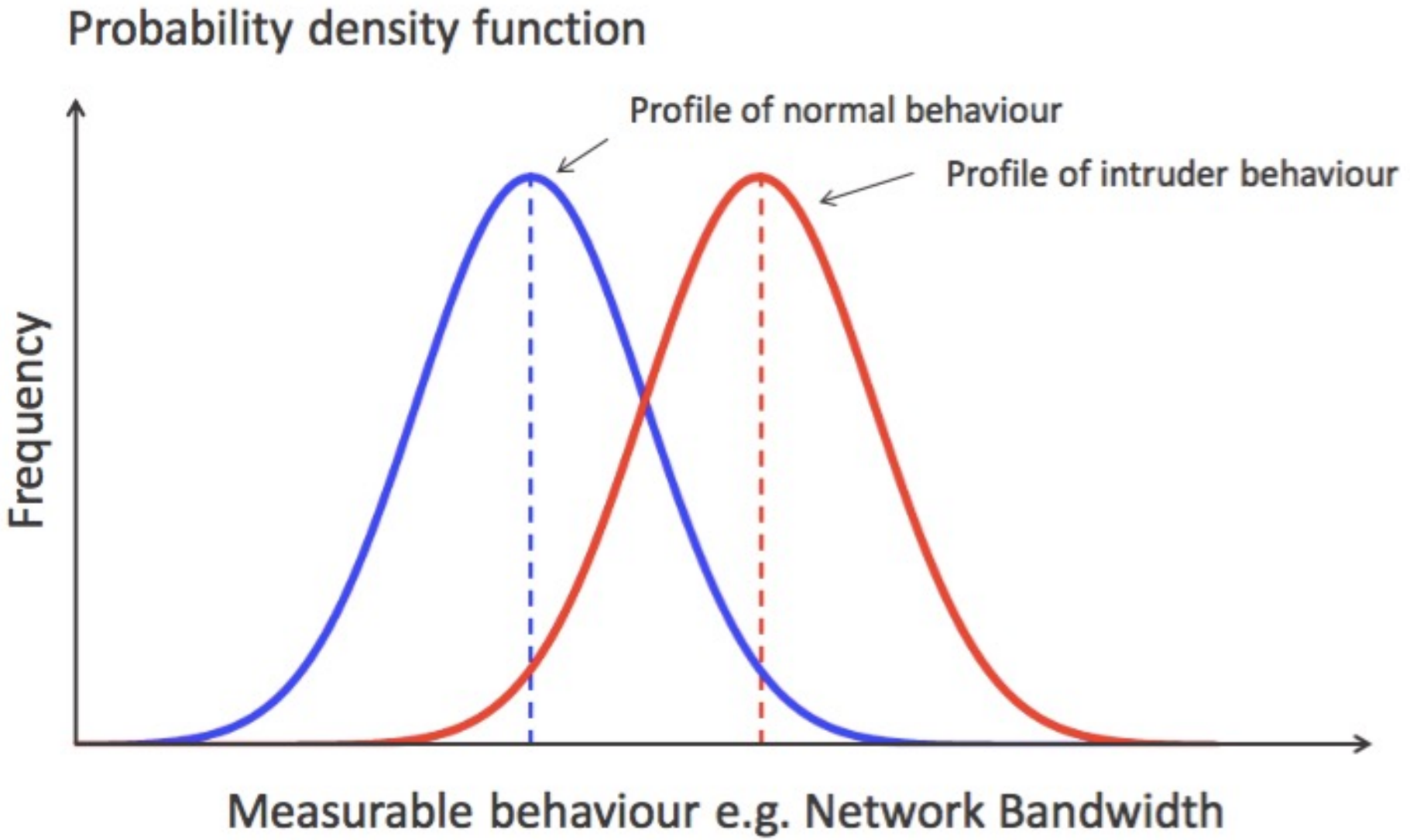
- Anomaly detection has wide-ranging applications from IDS to banking fraud
- Build up a picture of normal usage, and detect when usage moves beyond what is normal
  - This may involve usage of network, applications, storage, system calls etc.
- Always a trade off between false positives and false negatives



What is Normal?

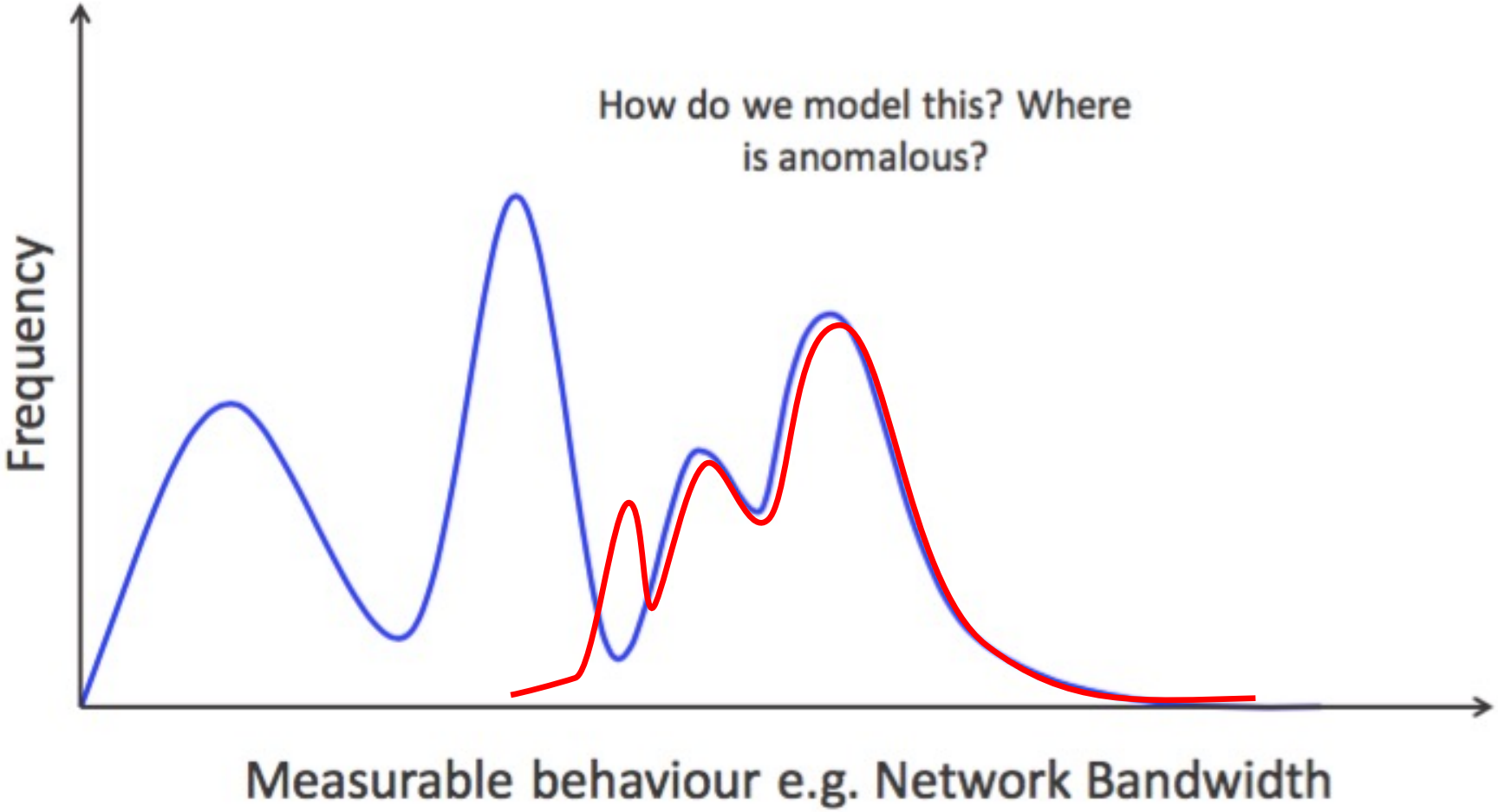
- Run a host within a quarantined environment and collect training data
- Constructed by monitoring audit logs
- Sometimes rely on analysis of sequences of system calls through normal behaviour

Statistical Models of Normal



Complex Behaviours

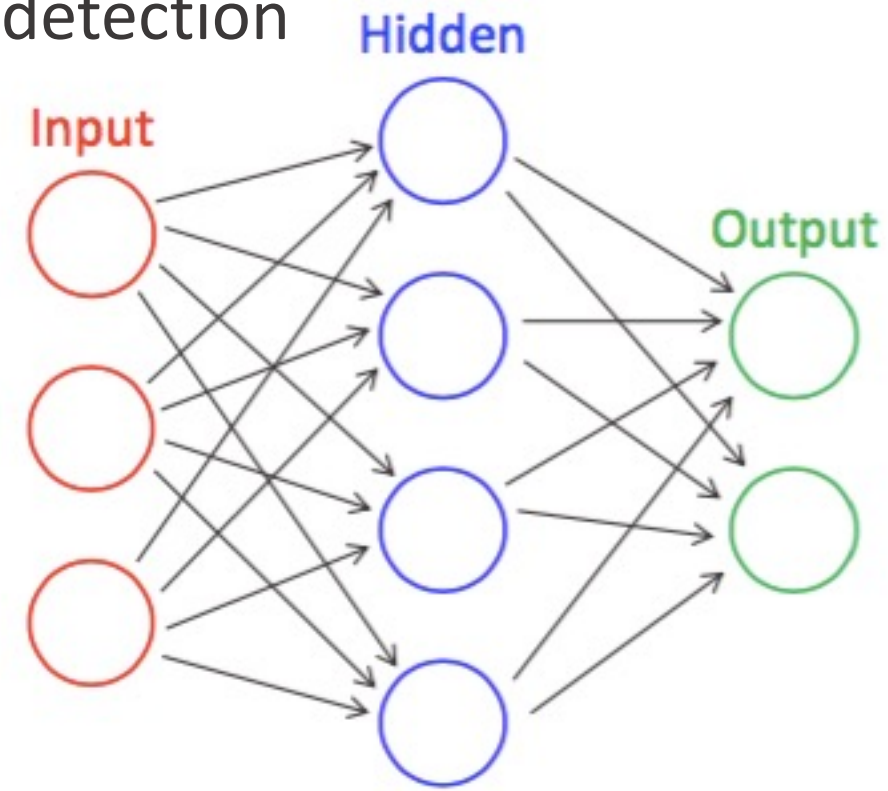
- Profiles can be complex, and can change over time



Machine Learning

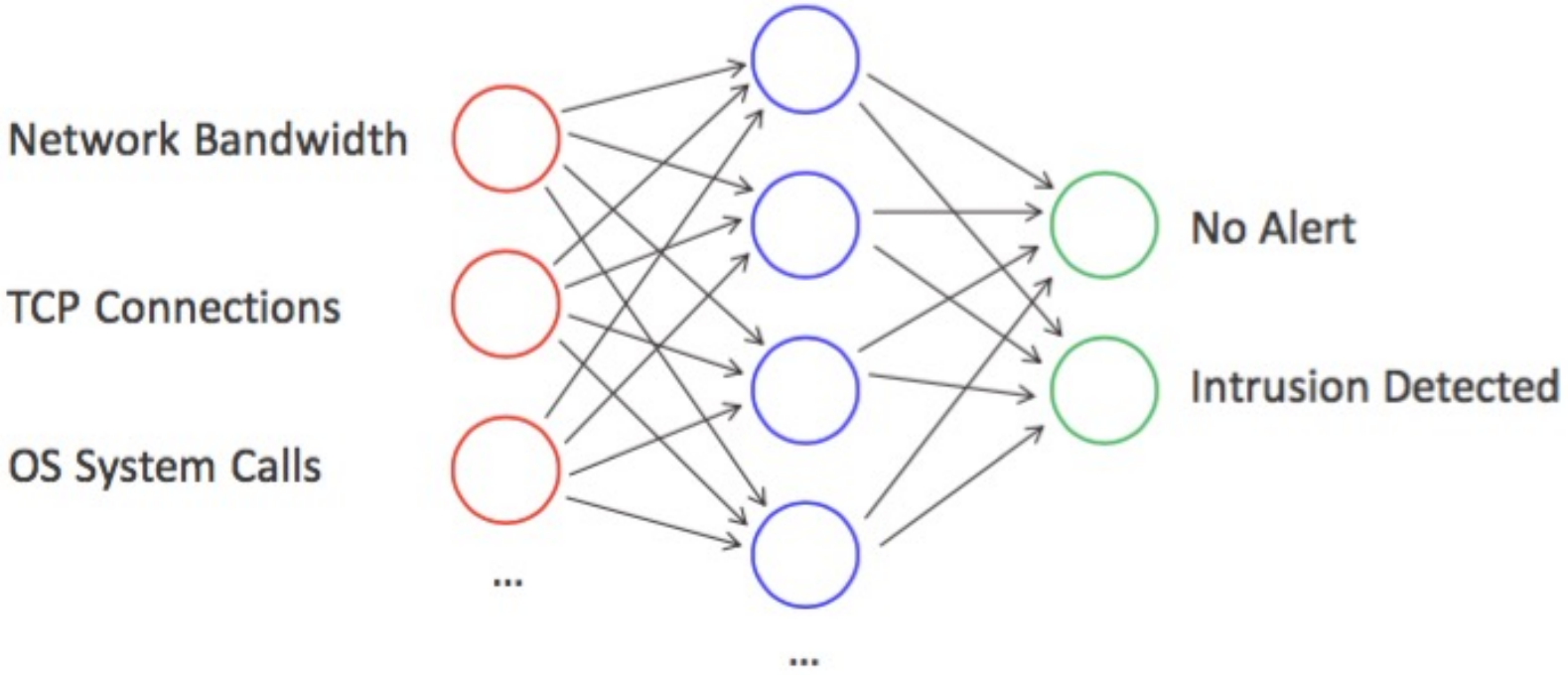
- Machine learning approaches train a model to make predictions on data
- Support Vector Machines, Neural Networks etc. all see use in intrusion detection

Artificial Neural Networks are capable of modelling complex non-linear functions



Neural Networks for ID

- A network can be pre-trained
- Sensor measurements are then passed through the network
- Activations in the specific output neuron signal an alert



Drawbacks

- Scaling:
  - Search space can increase exponentially
  - Real-time data
- False negatives
  - Limits in the representation
  - What is normal can change
    - do we re-train and risk learning intruder behaviour?

Intrusion Prevention

- A common extension of IDS, often network based
- Actively monitors the system through stateful analysis
  - Setting alarms
  - Dropping packets, stalling connections, closing ports
  - Can be subverted to cause DoS

Summary

- Network Attack Models
  - Insider Attacks
- Intrusion Detection Systems
  - Network and Host-based
- Protocol Analysis
- Signature Detection
- Anomaly Detection

Gollmann 17.4

Anderson 21.4.2