Australian Government
Department of Defence
Science and Technology

Future Trends in Cyber Defence

Toby Richer
Defence Science & Technology

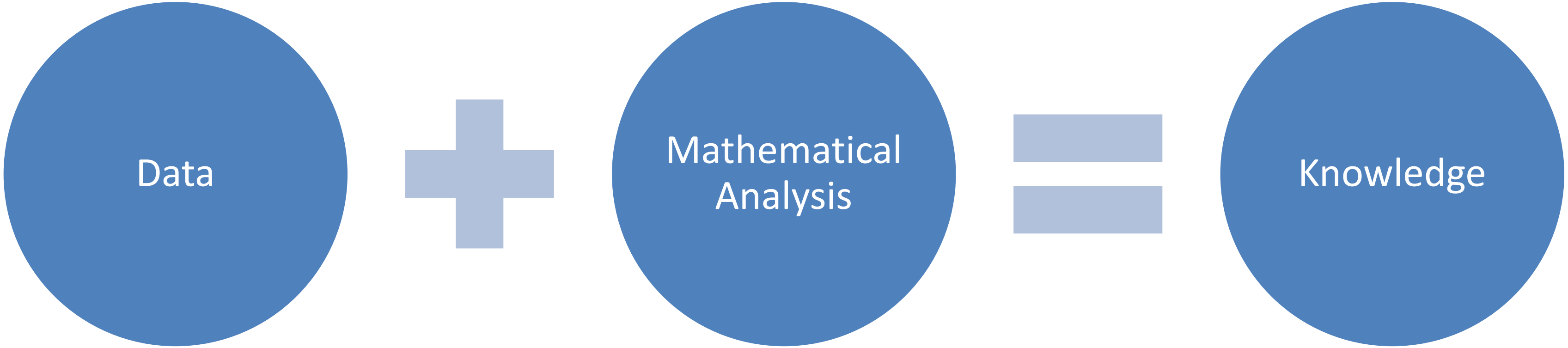
About me

- Data Scientist in Countering Software Threats Team, Cyber & Electronic Warfare Division
- Postdoctoral researcher in swarm intelligence at Goldsmiths College, University of London
- PhD in robotics at University of South Australia
- Cyber Security Research Interests:
  - Application of machine learning to Cyber Defence & Forensics
    - log analysis
    - program analysis

Theme of Talk

- Technologies that will have a strong effect on Cyber Defence in the next five to ten years
  - Machine Learning
  - Cloud Security
  - Automated Program Analysis
- What each technology does
- Possible benefits and drawbacks
- Potential effect on Defence capability

Machine Learning

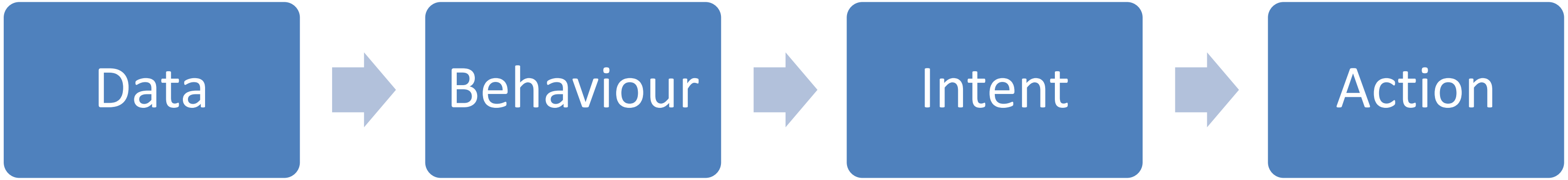


Data

Mathematical Analysis

Knowledge

Machine Learning for Cyber Defence



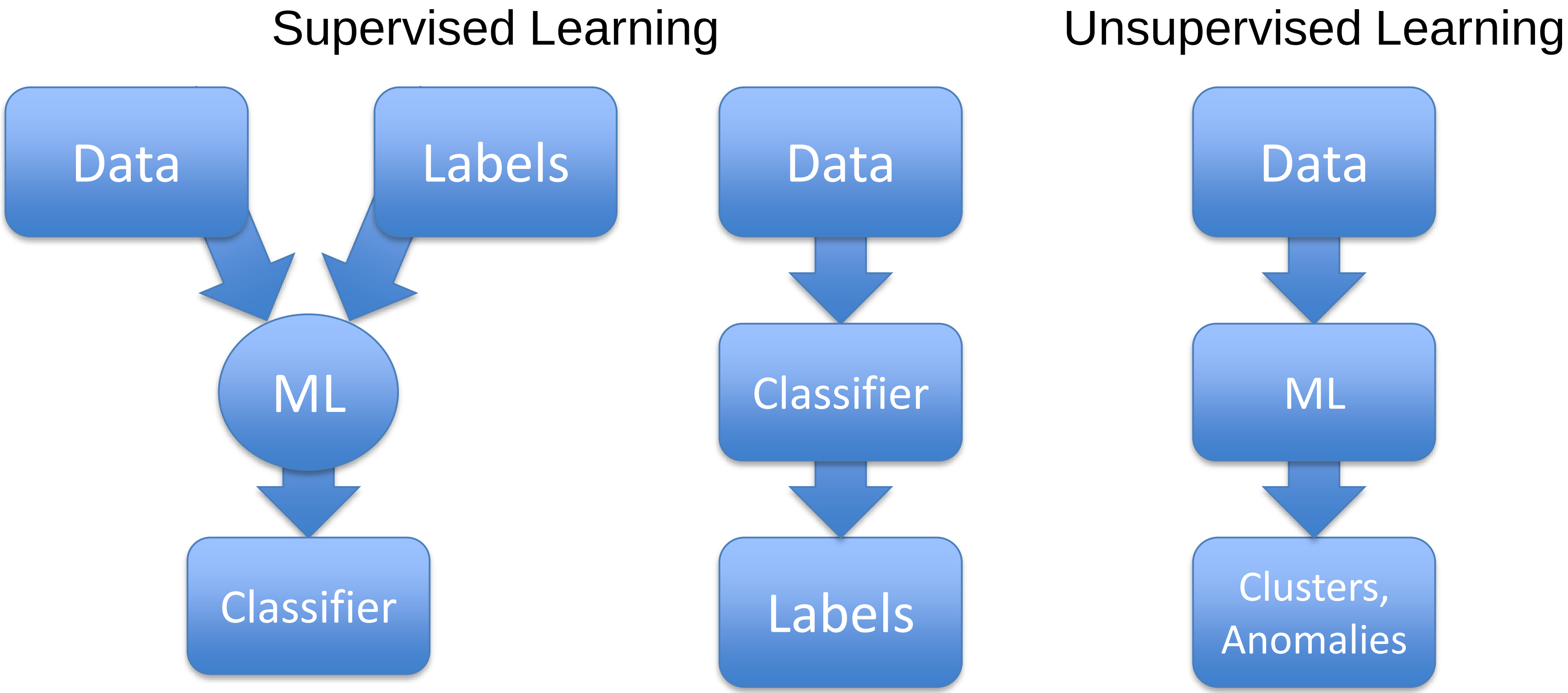
Data

Behaviour

Intent

Action

Machine Learning – Classification



Machine Learning - Analysis

Benefits

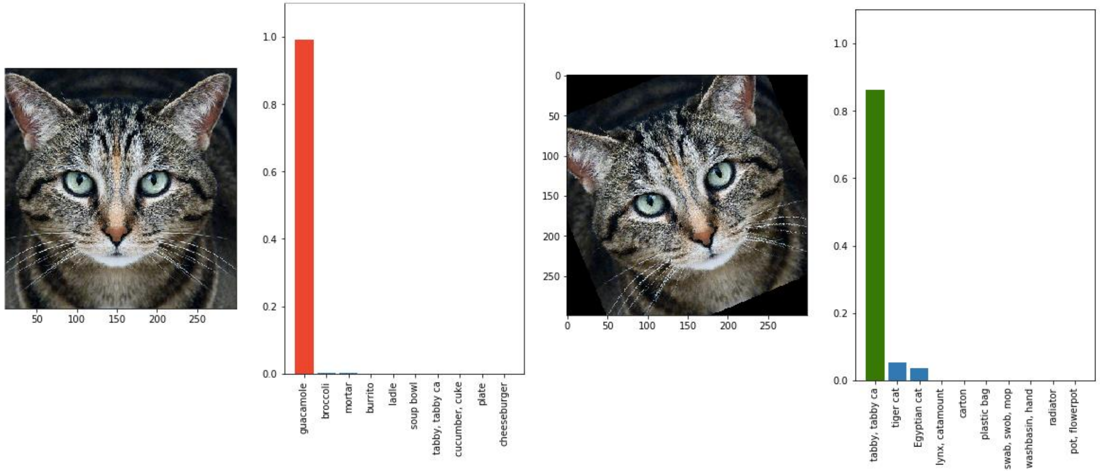
- Summarising large bodies of data
- Capturing expert knowledge

Drawbacks

- False Positives
- Black Boxes
- Black Swans

Machine Learning - Counters

- Adversarial Machine Learning
  - Minor perturbations that foil ML systems without affecting human interpretation of the data
  - Some popular ML techniques are fragile; minor changes in underlying data ruin results

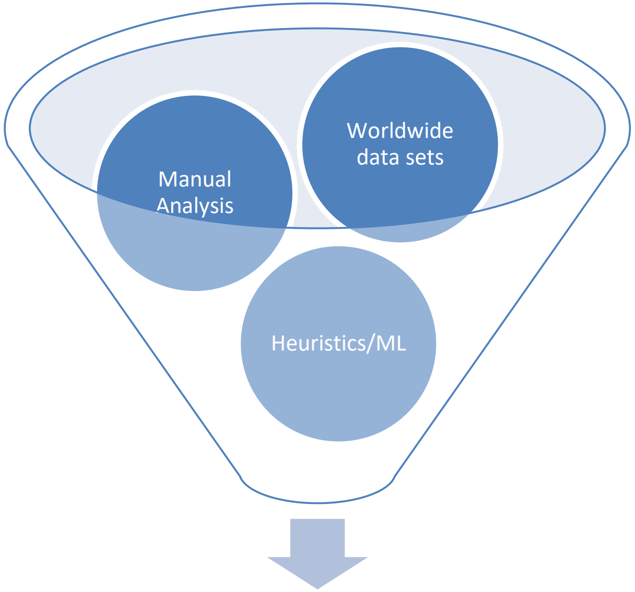


Machine Learning - Consequences

- Increased Automation
  - Wrangling large bodies of data
  - Frees up analyst time
  - Potentially paves way for autonomic approaches
- Vulnerabilities are still there
  - Attackers are adapting
  - ML not so good for unique events
  - Doesn’t replace good configuration and baselining – these are required to get the best out of ML

Cloud Security - Description

- Now, clients have direct & immediate connection to ML/analytics based on worldwide data, human analysts
- Response within milliseconds, minutes/hours in rare cases
- Cloud systems allow systems to be easily replicated & moved
  - Potential for fast & elaborate responses to probing or attack



Client with suspicious activity

Cloud Security - Analysis

Benefits

- Rapid Response
- Captures wide range of knowledge about file and world networks
- In some cases, can include human analysis

Drawbacks

- Most tools suited to enterprise systems – less for unique, embedded systems
- Needs internet connection
- May require high degree of information sharing with commercial entities
- Rapid response techniques may not allow for nuance

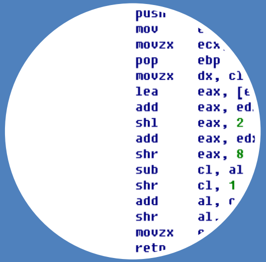
Cloud Security - Consequences

- Potential for more secure flexible systems
  - Homogenous configuration
  - High level of automation
  - Ability to reconfigure automatically to respond to attack
- Significant limits on applicability
  - Not for embedded systems
  - Required connectivity
- Like Machine Learning, potential to significantly reduce the repetitive parts of workload
  - Allows analysts to switch focus to unique systems, unusual problems

Program Analysis

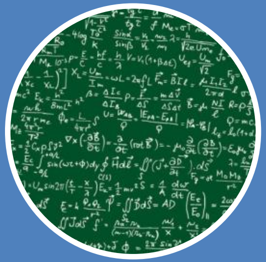
- Working out what programs do
  - Vulnerability Detection
  - Threat Intelligence and Triage
- Main existing approaches
  - Static Analysis
  - Dynamic Analysis
- Value of automation
  - Manual analysis requires well-trained analysts, large amounts of time
  - Arms race – malicious software now uses anti-analysis techniques
    - Some malicious software uses *anti-anti-anti-analysis*
  - Potential for *autonomous* security – computers that automatically detect and patch vulnerabilities

Automated Program Analysis



```
push
mov
movzx   ecx,
pop     ebp
movzx   dx, cl
lea     eax, [e
add     eax, ed
shl     eax, 2
add     eax, ed
shr     eax, 8
sub     cl, al
shr     cl, 1
add     al, c
shr     al,
movzx   e
retn
```

Automated Static Analysis



Symbolic Execution

Concolic Execution

Fuzzing

Automated Program Analysis - Analysis

Benefits

- Captures/substitutes for higher-level analyst knowledge
- Potentially effective on previously-unseen threats
- Can apply static and dynamic approaches
- Drills down to concrete program behaviour
- Guarantees of thoroughness, correctness

Drawbacks

- Scales badly with program size
- Often designed around toy problems
- Current research focuses on vulnerability detection
- Vulnerable to attack through deliberate addition of complexity

Consequences – Automated Program Analysis

- Potential to provide detailed program analysis to analysts with less training in the area
- Developing practical techniques for fast triage of real-world binaries still an ongoing area of research
- To use the information from such tools correctly
  - Proper baselining and configuration helps
  - Analysts need overall knowledge of the system they are investigating, or other tools (such as ML) to help develop this knowledge

Summary – Machine Learning

- If well designed, can provide good summaries of system activity and point analysts to areas of interest
- It requires humans to interpret – it’s a force multiplier, not a replacement for analysts
- Requires preliminary work defining systems and interactions, otherwise high chance of false positives and potential of making the analyst’s job *harder*
- Rising interest in exploiting machine learning systems

Summary – Cloud Security

- Strong, cloud-based protection for internet facing networks available commercially now
- The highly homogenous and flexible nature of cloud infrastructure allows for new techniques in managing secure networks and responding to attacks
- It requires full access to those networks, some loss of control over threat response
- It also requires trust in the cloud provider to keep the underlying infrastructure secure

Summary – Automated Program Analysis

- Strong potential for automated threat analysis
  - Like ML, automates a lot of manual work
  - Unlike most ML, produces concrete interpretable results
- That potential is still a long way from realization
  - Current systems run large servers for months dealing with small problems
  - Need for strong research effort in this area

Conclusion

- ML can automate repetitive aspects and assist in finding threats, but not a replacement for trained analysts
- Cloud security can lead to strong improvements in enterprise in cases where the sacrifice of autonomy is feasible
  - Use of secure clouds particularly of interest – potential to improve security while reducing maintenance workload
- Automated Program Analysis has the potential to significantly improve capability in the longer term

Conclusion – Effect on Defence

- Simpler, more mundane aspects of cyber security can be automated
- Require management from people with higher levels of knowledge
- Analysts can now tackle more complex security issues:
  - Hunts and Cyber Threat Intelligence
  - Managing and configuring intelligent security tools
  - Developing security approaches for unique systems and platforms

What We Do

- Counter Cyber Threats STC
  - Counter Software Threats Team
    - Better frameworks for static and dynamic analysis
    - Techniques for binary comparison
    - Portable, practical automated program analysis tools
    - ….tailored to DCO Teams
  - Trustworthy Machine Learning Team
    - Prototyping methods of attacking Machine Learning
    - Developing robust Machine Learning algorithms
    - Methodologies, testbeds for testing Machine Learning robustness

Questions?

toby.richer@defence.gov.au