Artificial Intelligence
Agenda

AI Past and Future
AI Enabled Cyber-security Research
Future
Q&A
Deepinder Chhabra
Experienced and trusted advisor in Governance, Risk, compliance and Cyber Security

Principal Consultant Verizon
Vice President (ISACA London Chapter)
Professional Doctorate Student (UEL)
Post Graduate Diploma in Management
Executive Education from Harvard Business School
PRINCE2, TOGAF, ITIL Foundation
CEH, CHFI, CGEIT, CISM, CRISC
Senior leadership roles in FTSE 500 companies
Finance, Services, Retail, Manufacturing, Defence and HMG experience.
dchhabra@isaca-london.org

The views presented here are solely my own personal views and not those of my employer (Verizon)
Understanding /Knowledge /Intelligence
AI - Computer systems able to perform tasks normally requiring human intelligence
Current Applications of AI

1997

According to Google, its speech recognition technology had an 8% word error rate as of 2015.

2005

2008

2011

2017
Drivers for AI Enabled Cyber Security
55 BILLION
by 2020
That's 5 per estimated population of 2020
Source: ISACA State of Security 2017
FEWER THAN HALF are CONFIDENT in their team’s ability to handle anything beyond simply cyber incidents

Source: ISACA State of Security 2017
FIGURE 4—TIME TO FILL AN OPEN CYBER SECURITY/INFORMATION SECURITY POSITION

On average, how long does it take you to fill a cyber security/information security position?

- Less than 2 weeks: 1%
- 1 month: 8%
- 2 months: 15%
- 3 months: 30%
- 6 months: 26%
- Cannot fill open positions: 6%
- Don’t know: 14%

Source: ISACA State of Security 2017
FIGURE 5—NUMBER OF APPLICANTS FOR OPEN SECURITY POSITIONS

On average, how many applicants do you get for open security positions?

- 0 – 4: 22%
- 5 – 9: 26%
- 10 – 14: 16%
- 15 – 19: 4%
- 20+: 13%
- Don’t know: 19%

Source: ISACA State of Security 2017
<table>
<thead>
<tr>
<th>IT Security</th>
<th>Min - Max</th>
<th>Min - Max</th>
<th>Min - Max</th>
<th>Min - Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of Information Security (10+ yrs' exp)</td>
<td>90 - 150k</td>
<td>95 - 155k</td>
<td>750 - 1100</td>
<td>800 - 1150</td>
</tr>
<tr>
<td>Information Security Manager (5 - 10 yrs' exp)</td>
<td>75 - 115k</td>
<td>80 - 120k</td>
<td>600 - 800</td>
<td>650 - 900</td>
</tr>
<tr>
<td>Information Security Analyst (5 - 10 yrs' exp)</td>
<td>60 - 95k</td>
<td>80 - 95k</td>
<td>500 - 750</td>
<td>550 - 800</td>
</tr>
<tr>
<td>Information Security Analyst (1 - 5 yrs' exp)</td>
<td>40 - 60k</td>
<td>45 - 70k</td>
<td>300 - 500</td>
<td>350 - 550</td>
</tr>
<tr>
<td>Information Security Risk Manager (5 - 10 yrs' exp)</td>
<td>75 - 110k</td>
<td>80 - 115k</td>
<td>600 - 800</td>
<td>650 - 900</td>
</tr>
<tr>
<td>Information Security Manager (1 - 5 yrs' exp)</td>
<td>55 - 75k</td>
<td>80 - 80k</td>
<td>450 - 600</td>
<td>500 - 650</td>
</tr>
</tbody>
</table>
4 IN 5

Think it is likely or very likely that their enterprise will experience a cyber attack this year

53\% OF ENTERPRISES

EXPERIENCED MORE ATTACKS this year than in the year prior
AI Is the Future of Cybersecurity, for Better and for Worse

by Roman V. Yampolskiy

MAY 08, 2017
Current Landscape
Rozkład Benforda
Population of Mexico's Counties (Municipios)

<table>
<thead>
<tr>
<th>Leading digit frequency</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>31.19%</td>
</tr>
<tr>
<td>2</td>
<td>17.55%</td>
</tr>
<tr>
<td>3</td>
<td>12.7%</td>
</tr>
<tr>
<td>4</td>
<td>9.85%</td>
</tr>
<tr>
<td>5</td>
<td>7.37%</td>
</tr>
<tr>
<td>6</td>
<td>6.64%</td>
</tr>
<tr>
<td>7</td>
<td>5.05%</td>
</tr>
<tr>
<td>8</td>
<td>5.13%</td>
</tr>
<tr>
<td>9</td>
<td>4.52%</td>
</tr>
</tbody>
</table>

Source: http://testingbenfordslaw.com/population-of-turkish-boroughs
UK government spending May–Sept 2010

Leading digit frequency

1: 29.1%
2: 17.5%
3: 12.2%
4: 9.6%
5: 8.6%
6: 7.3%
7: 6.1%
8: 5.1%
9: 4.6%

Source: http://testingbenfordslaw.com/population-of-turkish-boroughs
First 652066 Fibonacci Numbers

Leading digit frequency

1: 30.1%
2: 17.61%
3: 12.49%
4: 9.69%
5: 7.92%
6: 6.69%
7: 5.8%
8: 5.12%
9: 4.58%

Source: http://testingbenfordslaw.com/population-of-turkish-boroughs
Colgate launches AI in app-enabled electric toothbrush
Confusion matrix for 2-class problems

<table>
<thead>
<tr>
<th></th>
<th>actual class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>positive</td>
</tr>
<tr>
<td>predicted class</td>
<td>true positives (TP)</td>
</tr>
<tr>
<td>positive</td>
<td>false negatives (FN)</td>
</tr>
</tbody>
</table>

Accuracy = \[
\frac{TP + TN}{TP + FP + FN + TN}
\]
Other accuracy metrics

<table>
<thead>
<tr>
<th>Actual Class</th>
<th>Positive</th>
<th>Negative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive</td>
<td>True positives (TP)</td>
<td>False positives (FP)</td>
</tr>
<tr>
<td>Negative</td>
<td>False negatives (FN)</td>
<td>True negatives (TN)</td>
</tr>
</tbody>
</table>

\[
\text{recall (TP rate)} = \frac{TP}{\text{actual pos}} = \frac{TP}{TP + FN}
\]

\[
\text{precision} = \frac{TP}{\text{predicted pos}} = \frac{TP}{TP + FP}
\]
ROC curves

A Receiver Operating Characteristic (ROC) curve plots the TP-rate vs. the FP-rate as a threshold on the confidence of an instance being positive is varied.

Different methods can work better in different parts of ROC space. This depends on cost of false + vs. false -.

Expected curve for random guessing.
ROC curve example
Research in Cyber Security
Search String and Selection Criteria

Final Query (685 documents)


Final Query (Limited)

Same as above but limiting to Articles and Reviews – 109 Articles

Stage I Selection - 37/25 documents

A review of Abstract was carried out and only those studies that refer to AI, ML or CI in the context of Cyber Security were selected. Any duplicates were also excluded. There were 12 articles that could not be downloaded.

Final Selection

Full detailed review of the articles/papers were conducted and only those were selected in which the model has been tested with either simulated or real life data and their accuracy clearly stated.
Selected and Discarded
IDS/IPS

3 Papers were tested with the KDD99 data

MARKELM based model considered the well-published drawbacks and still achieved DR of 99.77% with KDD99 (FOSSACECA et al., 2015).

The model based on SVM and GMM with moving window; tested on real-life data from webservers and honey net is promising, but wider application to Mac and Windows OS is untested (MAMALAKIS et al., 2014).

Another SVM and Gaussian kernel based model Intrusion detection and prevention model have been only tested within Smart Grid context (PATEL et al., 2017).
Ant based Self
Combination of big data analysis with software security technologies such as feature extraction, machine learning, binary instrumentation and dynamic instruction flow analysis to achieve automated classification of malware algorithms. (Zhao et al.)

Combining intelligent cyber sensor agents which will detect, evaluate and respond to cyber-attacks in a timely manner and allow the groups of agents to make decisions. (Akila et al.)

The two-tier model: dimension reduction and feature selection; good detection rate against rare and complex attack (Pajouh et al.)
History of security timeline

- **Perimeter controls (pre - 2005)**
  - Static defenses
  - Password protections
  - Focus on compliance
  - Success = passing an audit

- **Security intelligence (2005+)**
  - Observation of real-time activity
  - Focus on deviations from known patterns
  - Ability to prioritize potential threats
  - Reactive and rules based

- **Cognitive security (2015+)**
  - Reasoning that mirrors human thought
  - Ability to analyze structured and unstructured data to understand behavior and meaning
  - Automated learning based on continual threat intelligence
  - Proactive focus using relationships and recommendations
Thank You!