State and Challenges of AI/ML Security for Future Networks

Dr. Michael A. Enright
Quantum Dimension, Inc. CEO/President

Agenda

1) State of AI/ML Security
2) Recent advances using Generative Adversarial Networks (GAN)
3) Review of AI/ML Security standards and activities from ITU, ETSI and others

About Quantum Dimension, Inc.

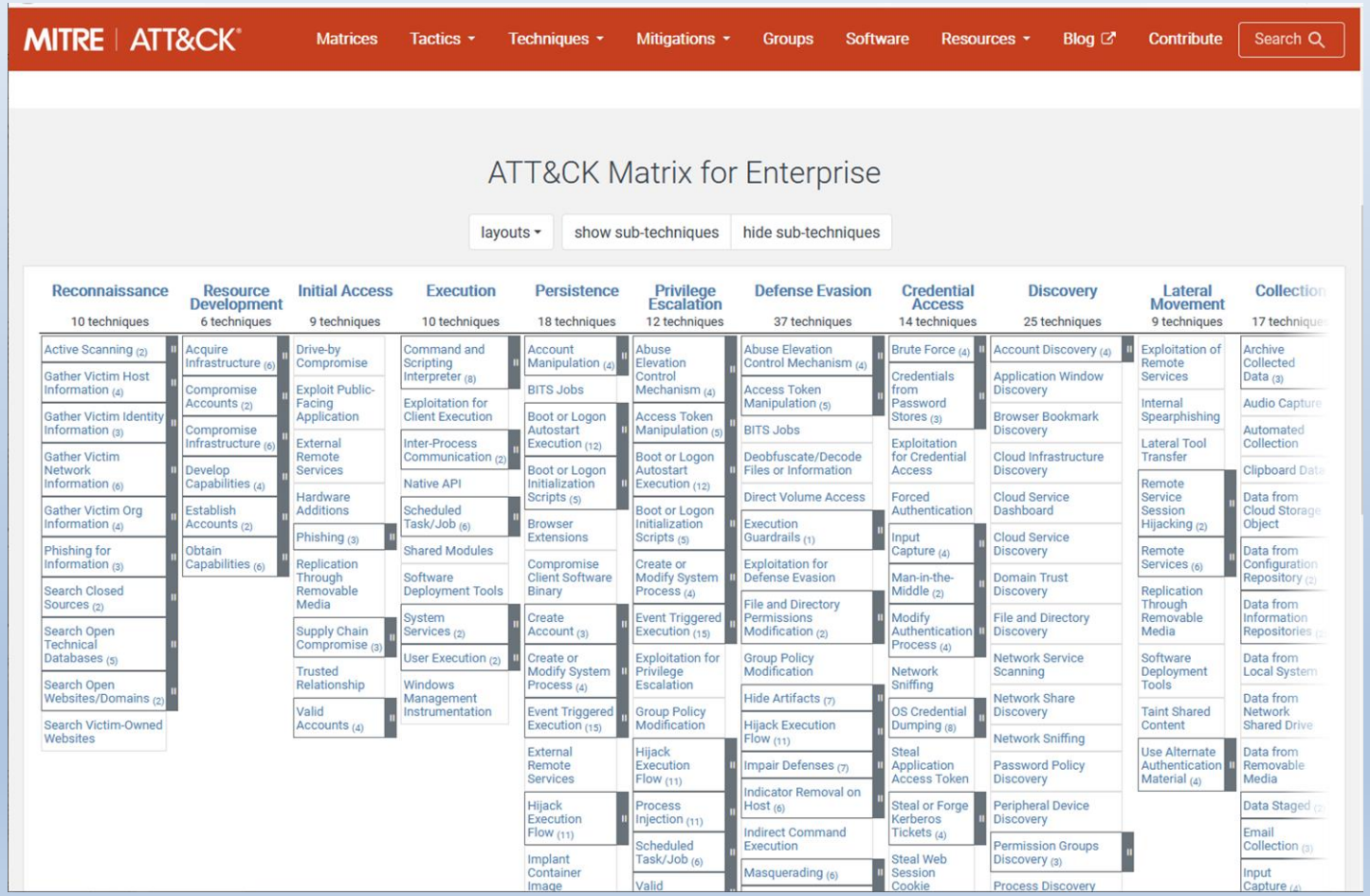
- Engineering Consulting and Technology Development business located in Huntington Beach, CA
- Core expertise in *Compute* and *Signal Processing*
- Focused on state-of-the-art technology embedded mobile development
  - Software-Defined Radio (SDR): DSP, GPU, FPGA
  - 5G Network and Cyber Security
    - IEEE Future Networks Initiative Security Working Group
    - Telecom Infrastructure Project OpenRAN and Open Core Network
  - Artificial Intelligence and Machine Learning
    - IEEE Future Networks Initiative AI/ML Working Group
  - 5G RF Technology
    - Advanced digital processing, RF power amplifiers design, duplexers, ….

AI/ML Security Objectives

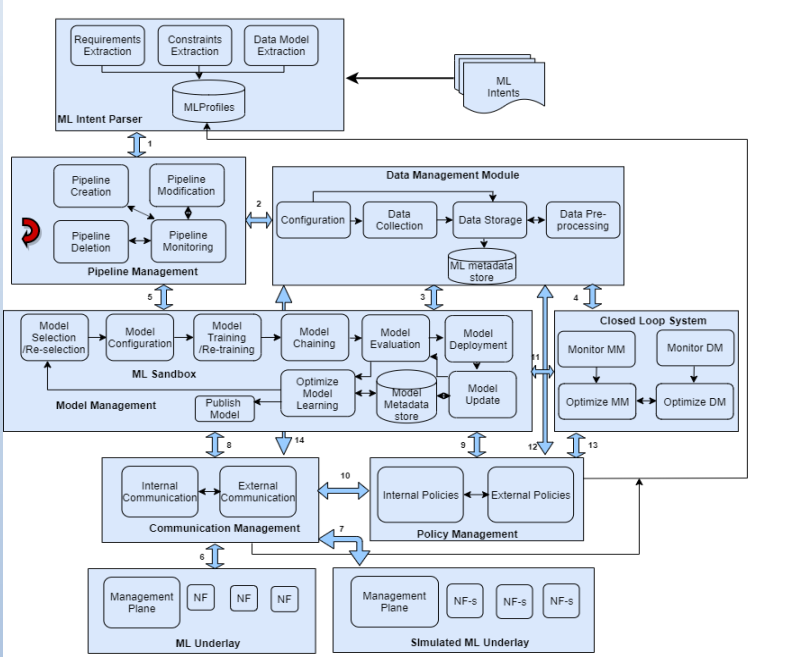
Artificial Intelligence and Machine Learning algorithms have been applied in many applications, but questions remain regarding application to 5G Security:

- Implementation methods across a wide range of devices
- Effectiveness for 5G Security applications
- Orchestration of AI/ML devices

No Shortage of Opportunities

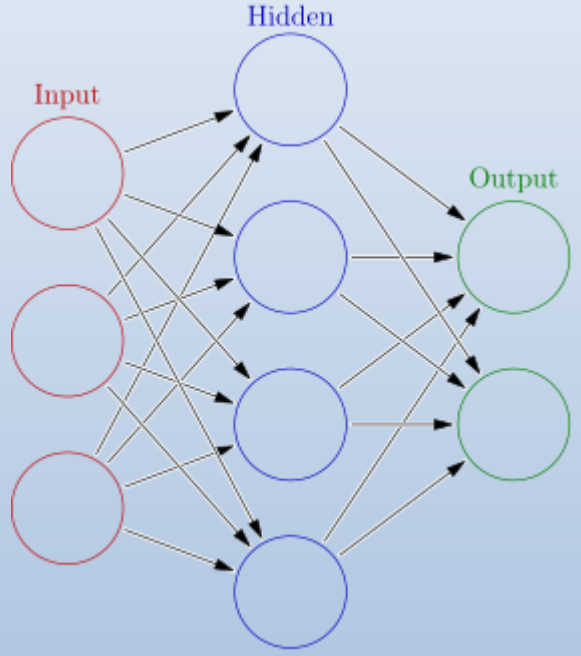


Big S versus Little S in 5G AI/ML



Machine Learning Orchestration (MLO) of 5G network devices

- International Telecommunication Union, FG ML5G Technical Specification, “FG ML5G Technical Specification “Requirements, architecture, and design for machine learning function orchestrator”, July 2020



Machine Learning Algorithms

- Supervised/Unsupervised, GAN, CNN, ….

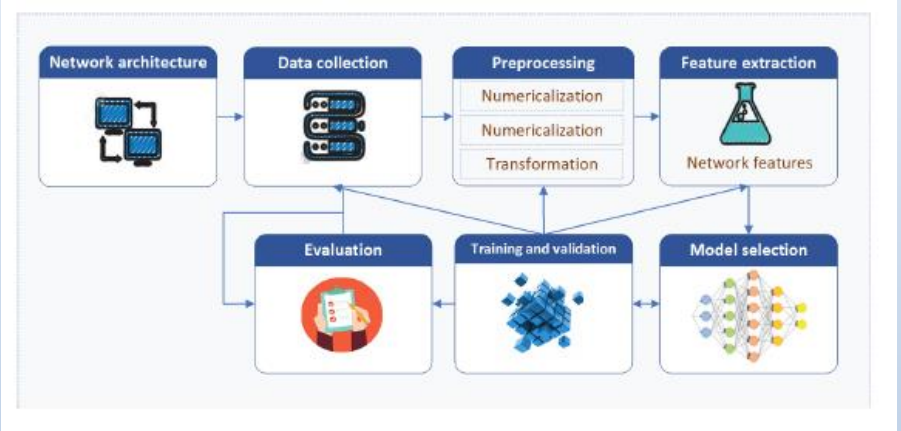
Emergence of AI/ML

- Why now? Three letters “G” “P” “U”
  - Processing capability is off the charts
  - Nvidia Nano illustrated
- Compute
  - Low-cost development platforms
  - Software, software, software!

- The data is better – not just DARPA’s k99 dataset for security – create your own attacks with Kali Linux
- Supervised/Unsupervised Learning algorithms
  - K-Means, Principal Component Analysis (PCA), Autoencoder, GAN, Convolutional Neural Network (CNN), Recurrent NN (RNN)
- AutoML – Machine Learning made easy!

AI/ML Security Past and Future

- AI/ML Network Intrusion Detection Systems (NIDS)
  - Research dates to late 2000's, early 2010's
  - 95+% for non-adversary, 25% for adversarial



Ref: "Review: Deep Learning Methods for Cybersecurity and Intrusion Detection Systems", M. Macas and C. Wu

- Results show that if model is known, it can be defeated
  - Raises the question of whether models should be open or proprietary
- Significant interest in GAN (circa 2014) for security since 2018

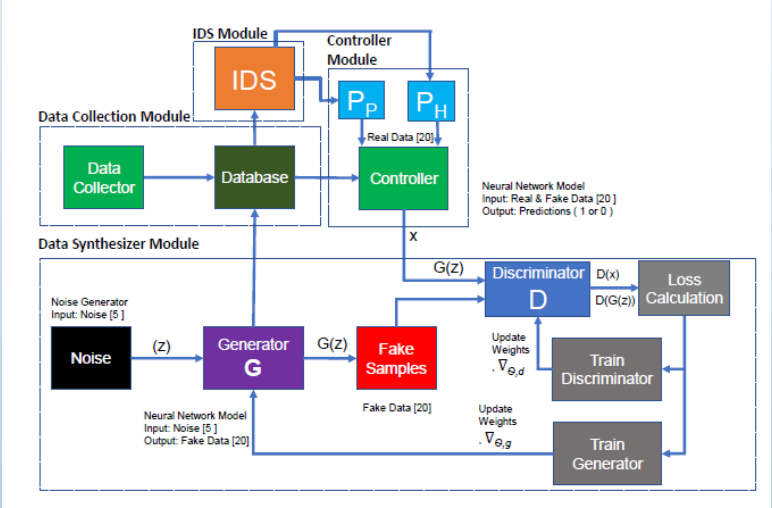
My Favorite GAN Site



Courtesy of thispersondoesnotexist.com

GAN System Architecture

- It has been used in imaging and character identification
- GAN is an adversarial NN that consists of:
  - Dual NN architecture
  - Generator, $\mathcal{G} \rightarrow$ forger
  - Discriminator, $\mathcal{D} \rightarrow$ art critic



- Cost Function: $J = E_{\boldsymbol{x}\sim D}[-logD(\boldsymbol{x})] + E_{\boldsymbol{z}}\left[-log\left(1 - D\left(G(\boldsymbol{z})\right)\right)\right]$
- Recent work (2018-2020) has focused on NIDS
  - Figure: "G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System," M.H. Shahriar et. al., arxiv.org, 2020
  - Other recent works in IoT, health and others

Interesting AI/ML and Security Sites

1) thispersondoesnotexist.com
2) MITRE ATT&CK - "*a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations*"
3) Canadian Institute for Cybersecurity – cyber datasets thru 2018
4) Linux Foundation AI - Adversarial Robustness Toolbox: A Python library for ML Security
5) ETSI Forge – Security, NFV and other tools

5G Standardization Activities

- IEEE
  - Future Networks Initiative is publishing white papers and roadmaps
- International Telecommunication Union
  - 5GML Working Group:
    - ITU-T Y.3172, “Architectural framework for machine learning in future networks including IMT-2020”
    - ITU-T Y.3173, “Framework for evaluating intelligence levels of future networks including IMT-2020”
    - ITU-T Y.3174, “Framework for data handling to enable machine learning in future networks including IMT-2020”
  - AI/ML in 5G Challenge
- European Telecommunications Standards Institute
  - Lots of work in NFV and orchestration, plus tools and webinars
- 3GPP
  - Specifications for 5G
- 5G PPP
  - Funding for technology prototypes through the EU’s Horizon 2020 (thru 2020) and Horizon Europe (2021-2027)
- ENISA – European Union Agency for Cybersecurity
  - EU Security standards, toolboxes and webinars
  - “AI Cybersecurity Challenges” released December 15, 2020
- Open Network
  - O-RAN Alliance
  - Tech Infra Project has Open RAN, Open CORE and more

Challenges and Future Research

- NFV has been leading, Security is lagging
- Managing the AI/ML ecosystem
  - Orchestration tools for NFV, only frameworks for ML
  - Open architectures and systems
- AI/ML algorithms development
  - Multiple types of algorithms and compute capability
  - Making devices smarter – SmartNIC
  - How do I know if my model is correct?

Contact Information

Dr. Michael A. Enright
President & CEO
menright@qdimension.com
(714) 893-6004 x 606

Mrs. Julie A. Isenberger
VP of Business Development
jisenberger@qdimension.com
(714) 893-6004 x 600