

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

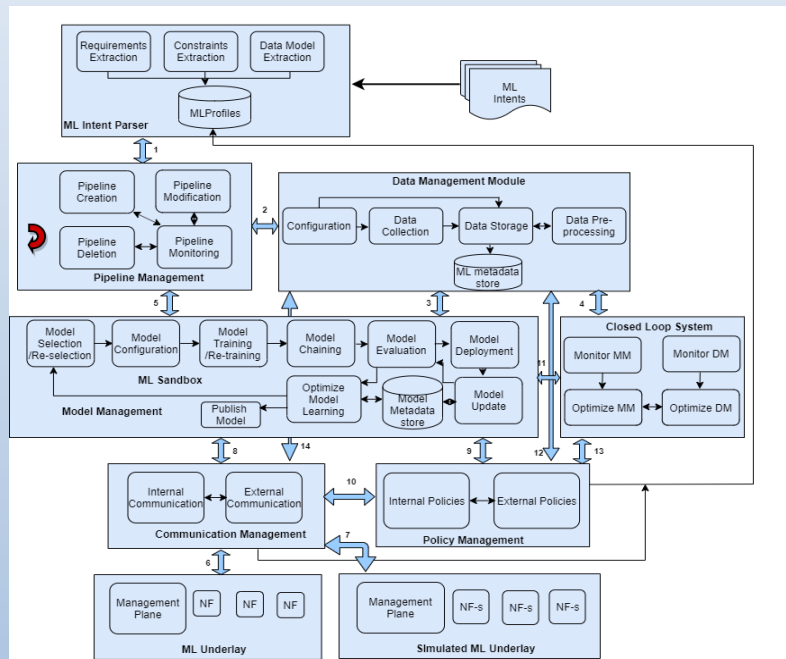
MITRE | ATT&CK[®] Matrices Tactics ▾ Techniques ▾ Mitigations ▾ Groups Software Resources ▾ Blog [↗](#) Contribute Search

ATT&CK Matrix for Enterprise

layouts ▾ show sub-techniques hide sub-techniques

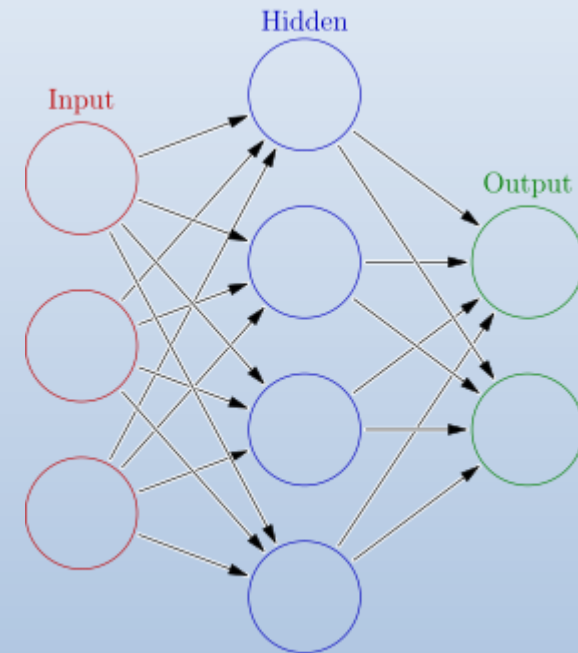
Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (4)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Access Token Manipulation (5)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Boot or Logon Initialization Scripts (3)	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create or Modify System Process (4)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Data from Information Repositories (2)	Data from Local System
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Service Discovery	File and Directory Discovery	Software Deployment Tools	Data from Network Shared Drive
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Group Policy Escalation	Group Policy Modification	Network Service Scanning	Network Service Discovery	Taint Shared Content	Data from Removable Media
Search Victim-Owned Websites			Windows Management Instrumentation	Event Triggered Execution (15)	Group Policy Modification	Hide Artifacts (7)	Network Sniffing	Network Share Discovery	Use Alternate Authentication Material (4)	Data Staged (2)
				External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	OS Credential Dumping (8)	Network Sniffing		Email Collection (3)
				Hijack Execution Flow (11)	Process Injection (11)	Impair Defenses (7)	Steal Application Access Token	Network Sniffing		Input Capture (4)
				Implant Container Image	Scheduled Task/Job (6)	Indicator Removal on Host (6)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		
					Valid	Indirect Command Execution	Steal Web Session Cookie	Peripheral Device Discovery		
						Masquerading (6)		Permission Groups Discovery (3)		
								Process Discovery		

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

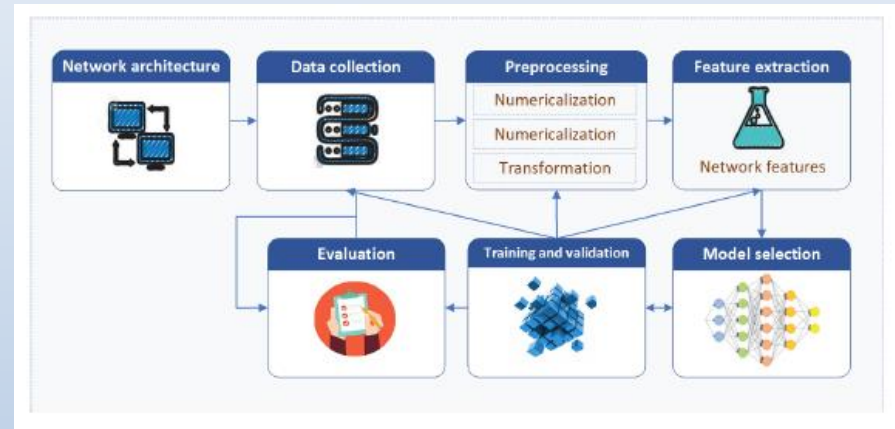
- AI/ML Network Intrusion Detection Systems (NIDS)

- Research dates to late 2000's, early 2010's
- 95+% for non-adversary, 25% for adversarial

- 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



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

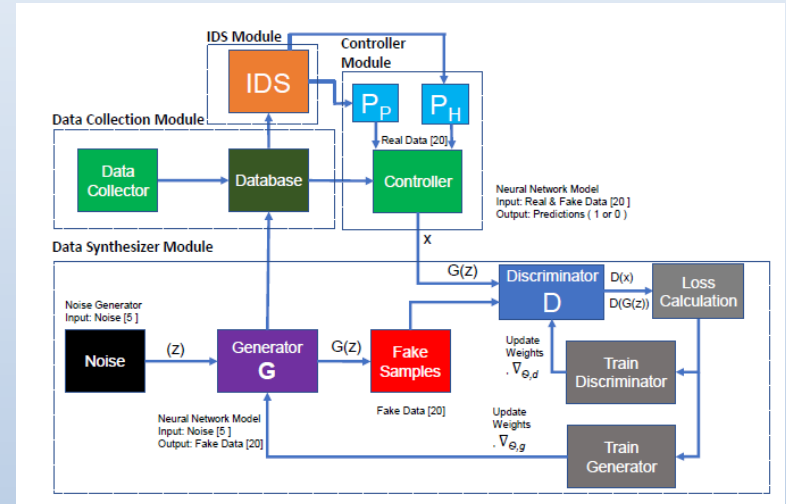
My Favorite GAN Site



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: $J = E_{x \sim D} [-\log D(x)] + E_z [-\log (1 - D(G(z)))]$
- 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