STORMBREAKER

AI-Enhanced
Industrial Control Systems Security

LT Joseph Post, USN

LT Sean Fitzgerald, USN

Garry Rosene

Olasunkanmi Kupoluyi

Problem Statement

Industrial Control Systems pose a significant vulnerability in today's society.

"…weapons of mass destruction…billions of dollars of damage…innocent lives lost…"

-Michael

Problem Statement

- ICS equipment, devices, applications, and protocols were not designed with security in mind.
- Vulnerabilities will always exist in legacy and new ICS networks (including air-gapped systems).
- ICS networks are susceptible to inadvertent user compromise of cybersecurity measures ("What's on this thumb drive?").
- Attackers are constantly utilizing sophisticated techniques (e.g., supply chain infiltration) to gain access to networks to potentially impose harm and disorder (e.g., equipment damage).

Case Study: HARVEY[1]

[1] Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page.

http://dx.doi.org/10.14722/ndss.2017.23313

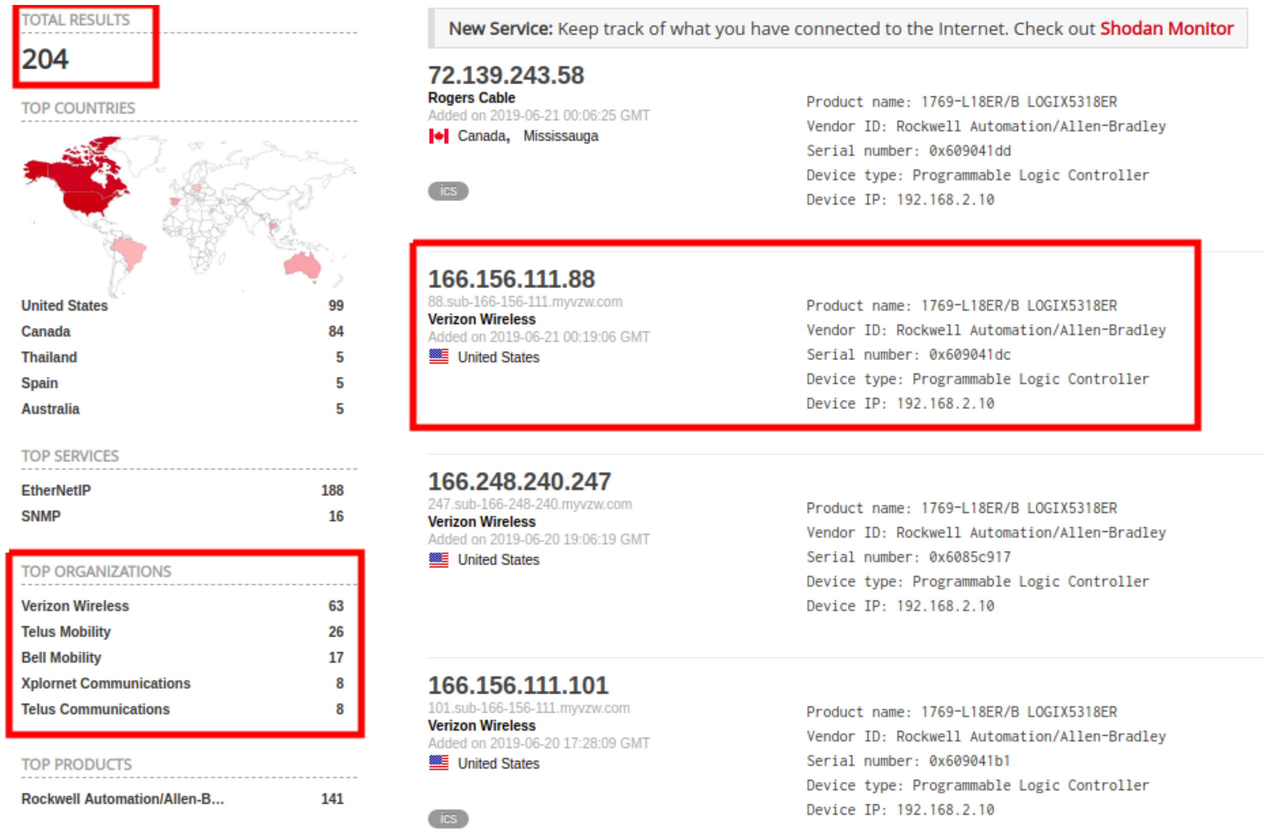
Case Study: HARVEY

- Researchers have created rootkit for Allen Bradley PLCs that can overwrite “good” logic commands with malicious commands
- Rootkit (“HARVEY”) examines signal space of PLC and determines the optimal malicious modification to output commands
- HARVEY also generates fake data displayed to operators

Case Study: HARVEY

"iii) an external bump-in-the-wire device between the PLC controller and the physical plant could be monitoring the two-way sensor-to-PLC and PLC-to-actuator data streams. **The solution could possibly check whether the control commands issued by the PLC satisfy the plant's essential safety requirements** that must be defined by the operators. Additionally, the solution could implement coarse-grained control consistency checks **to validate whether sensor measurements and actuation commands are consistent in terms of how the plant should be controlled."** (reference 1)

Case Study: HARVEY



TOTAL RESULTS

204

TOP COUNTRIES

United States	99
Canada	84
Thailand	5
Spain	5
Australia	5

TOP SERVICES

EtherNetIP	188
SNMP	16

TOP ORGANIZATIONS

Verizon Wireless	63
Telus Mobility	26
Bell Mobility	17
Xplornet Communications	8
Telus Communications	8

TOP PRODUCTS

Rockwell Automation/Allen-B...	141

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

72.139.243.58
Rogers Cable
Added on 2019-06-21 00:06:25 GMT
Canada, Mississauga
ics

```
Product name: 1769-L18ER/B LOGIX5318ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x609041dd
Device type: Programmable Logic Controller
Device IP: 192.168.2.10
```

166.156.111.88
88.sub-166-156-111.myvzw.com
Verizon Wireless
Added on 2019-06-21 00:19:06 GMT
United States

```
Product name: 1769-L18ER/B LOGIX5318ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x609041dc
Device type: Programmable Logic Controller
Device IP: 192.168.2.10
```

166.248.240.247
247.sub-166-248-240.myvzw.com
Verizon Wireless
Added on 2019-06-20 19:06:19 GMT
United States

```
Product name: 1769-L18ER/B LOGIX5318ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x6085c917
Device type: Programmable Logic Controller
Device IP: 192.168.2.10
```

166.156.111.101
101.sub-166-156-111.myvzw.com
Verizon Wireless
Added on 2019-06-20 17:28:09 GMT
United States
ics

```
Product name: 1769-L18ER/B LOGIX5318ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x609041b1
Device type: Programmable Logic Controller
Device IP: 192.168.2.10
```

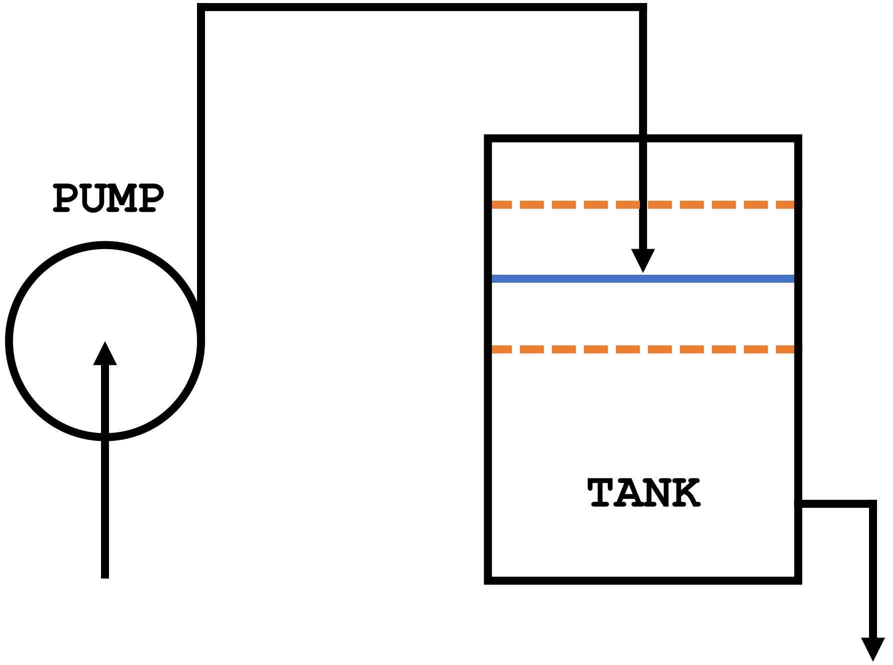
Our Solution: STORMBREAKER

STORMBREAKER

- Operator aid to mitigate safety issues such as equipment malfunction, environmental issues associated with critical systems.
- Can also be used as an electrical interlock to prevent inadvertent field device actuation of safety-critical systems
- Used in conjunction with existing ICS cybersecurity measures, not replace ICS-specific measures, policies, and procedures such as network blacklists, for example
- Comparable to existing AI-based tools used to process corporate (enterprise) network traffic (e.g., Amazon Web Services (AWS) GuardDuty™)

Feasibility Assessment

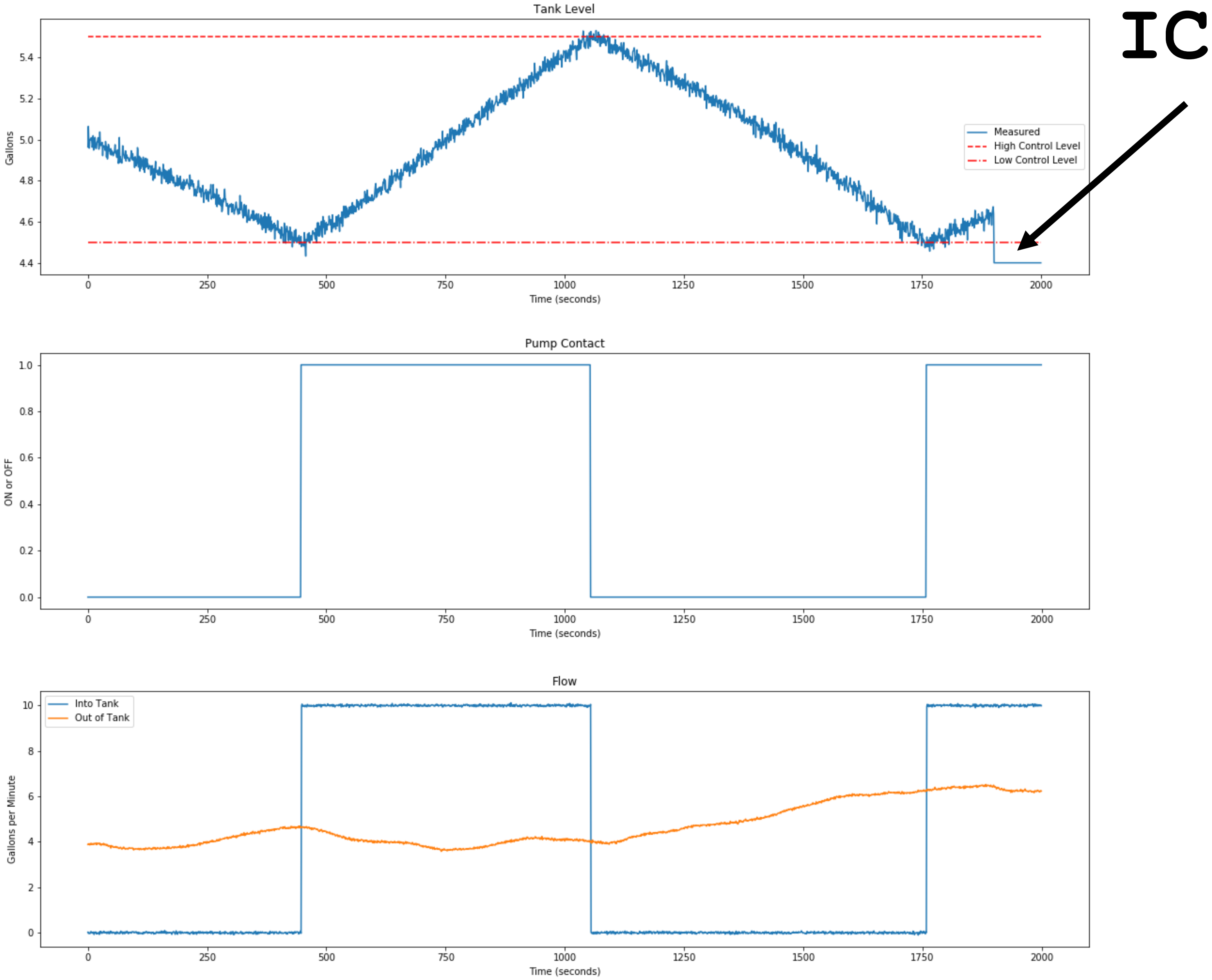
Feasibility Assessment



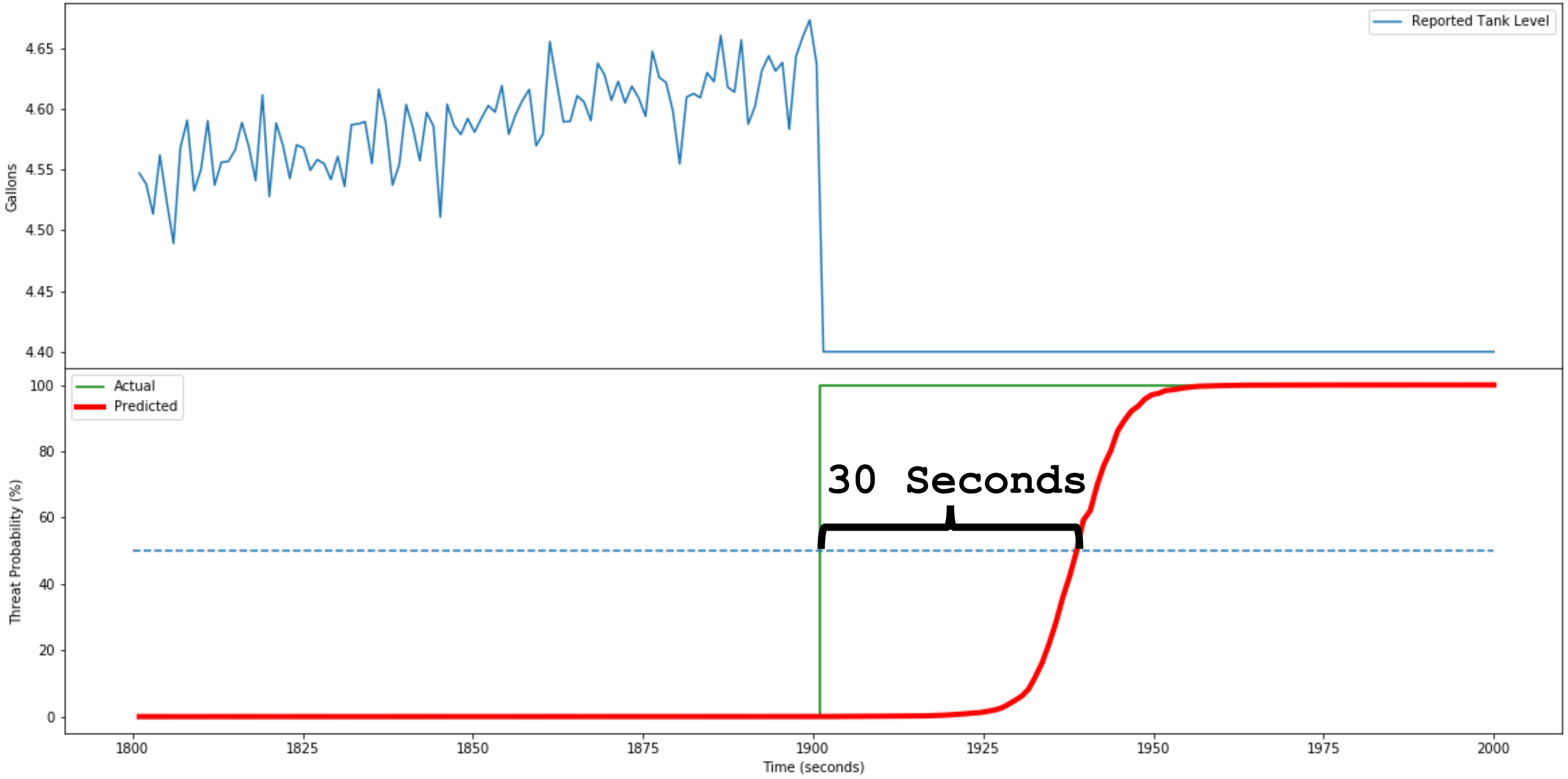
Measured Parameters:

- Pump ON / OFF
- Tank Level
- IN Flow
- OUT Flow

ICS Attack


Tank Level
Gallons
5.4
5.2
5.0
4.8
4.6
4.4
0
250
500
750
1000
1250
1500
1750
2000
Time (seconds)
Measured
High Control Level
Low Control Level
Pump Contact
ON or OFF
1.0
0.8
0.6
0.4
0.2
0.0
0
250
500
750
1000
1250
1500
1750
2000
Time (seconds)
Flow
Gallons per Minute
10
8
6
4
2
0
Into Tank
Out of Tank
0
250
500
750
1000
1250
1500
1750
2000
Time (seconds)

Feasibility Assessment

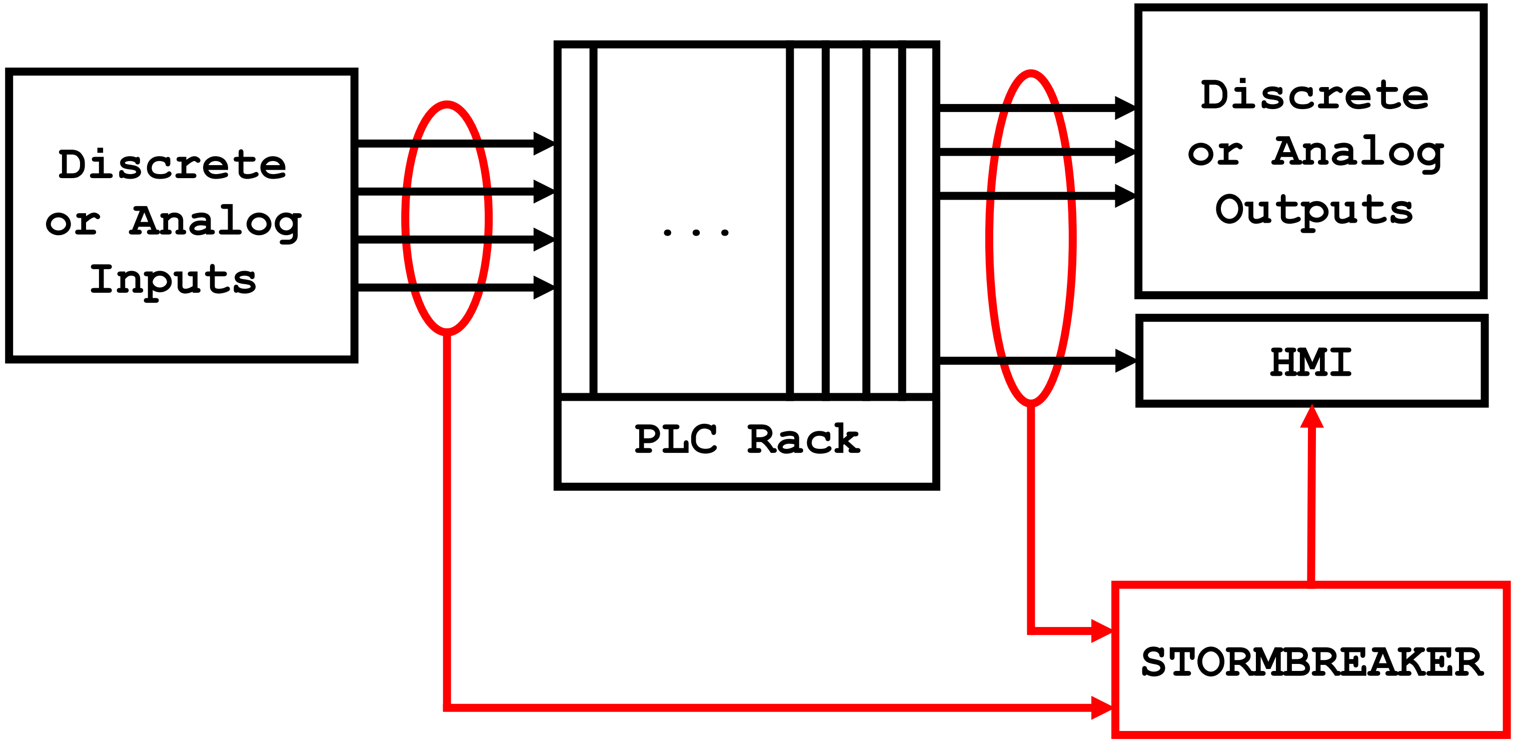


30 Seconds

Implementation

Implementation

We install STORMBREAKER in parallel with your current ICS.



Implementation

- Can be installed without downtime.
- Independent of current ICS
- Mitigates supply chain compromise
- Provides defense in depth

Implementation

Once installed, STORMBREAKER will alert when it detects abnormal parameters.

Potential Alarm Responses:

- Graceful degradation
- Switch to backup control
- Operator intervention (Safety Critical Systems)

References

1. L. Garcia, F.Brasser, M. Cintuglu, A.R. Sadeghi, O. Mohammed, S. Zonouz, “Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit” https://www.ndss-symposium.org/wp-content/uploads/2017/09/ndss2017_08-1_Garcia_paper.pdf

2. A. Nibali, “Mode collapse in GANs”, 18 Jan 2017 https://aiden.nibali.org/blog/2017-01-18-mode-collapse-gans/

3. P. Bojanowski, A. Joulin, D. Paz, A. Szlam, “Optimizing the Latent Space of Generative Networks” https://arxiv.org/pdf/1707.05776.pdf

I WENT FOR THE HEAD