KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

imec

Openness and transparency in cybersecurity

Guest Lecture

ANU College of Law

Ivo Emanuilov, LLM, MSc cand. (Bath), PhD cand. (Leuven)

13/04/2022

Outline

Openness and transparency in the context of ICT, incl. AI

- Why ‘open’ technology?
- Openness and transparency

Legal implications of openness and transparency for cybersecurity

- Zooming in on the role of computer design and instruction set architectures
- A case for open ISAs

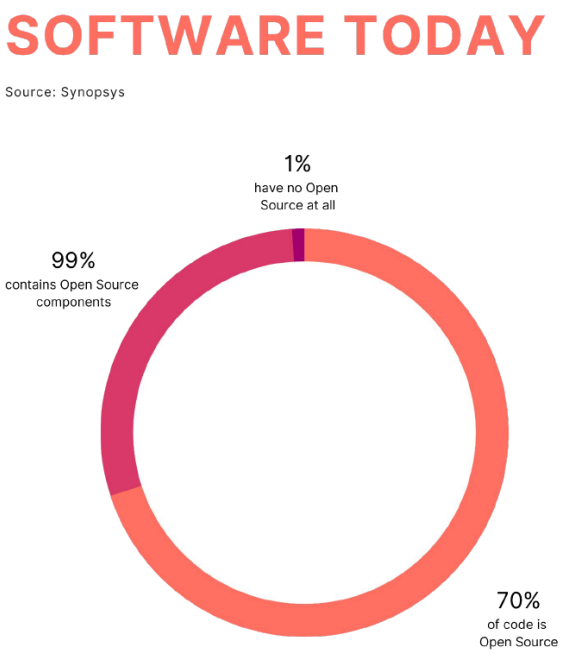
Differences between the security of conventional ICT systems and AI systems

- AI cybersecurity 101
- AI as a defence mechanism
- AI as an offensive tool

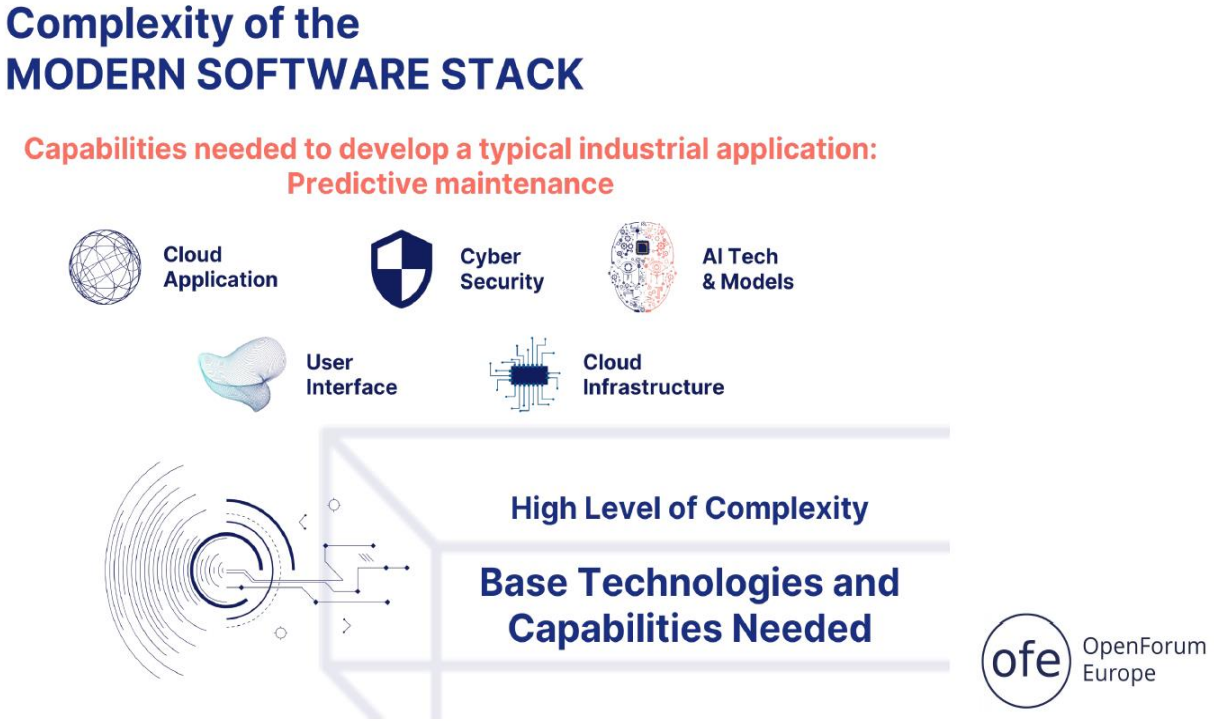
Is open always good?

- Discussion / Q&A

What is open (source)?

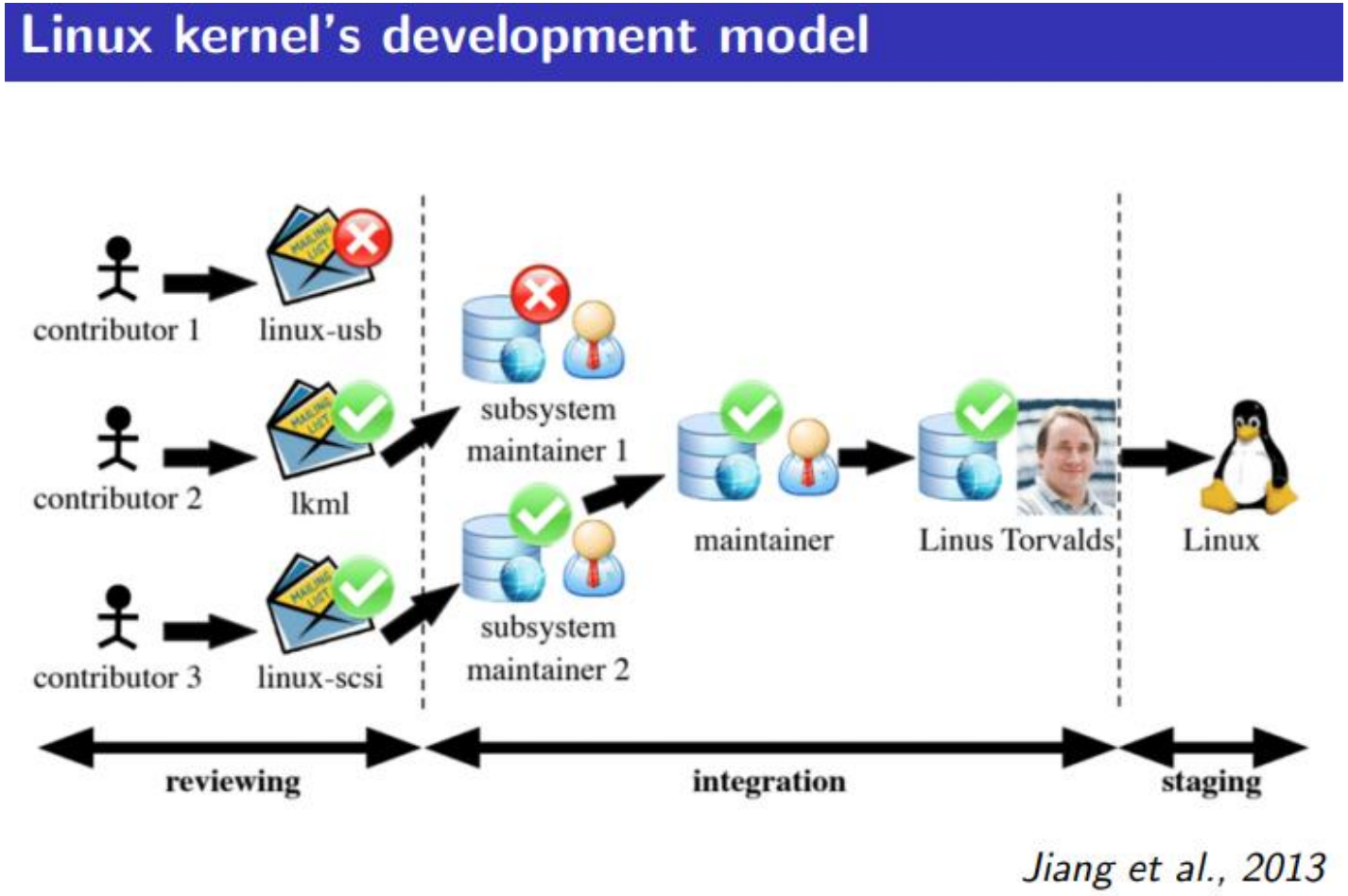


OpenForum Europe



OpenForum Europe

Open source software development model



Transparency in cybersecurity

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

PE/86/2018/REV/1

OJ L 151, 7.6.2019, p. 15–69 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

In force

ELI: http://data.europa.eu/eli/reg/2019/881/oj

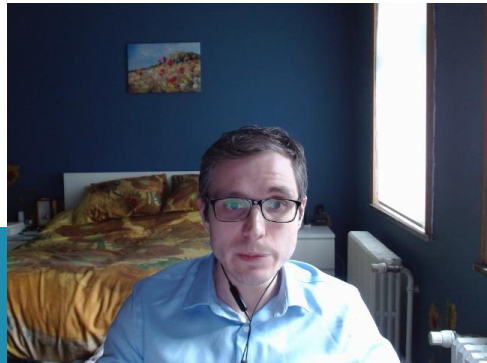
(7) Additional efforts are also needed to increase citizens', organisations' and businesses' awareness of cybersecurity issues. Moreover, given that incidents undermine trust in digital service providers and in the digital single market itself, especially among consumers, trust should be further strengthened by offering information in a transparent manner on the level of security of ICT products, ICT services and ICT processes that stresses that even a high level of cybersecurity certification cannot guarantee that an ICT product, ICT service or ICT process is completely secure. An increase in trust can be facilitated by Union-wide certification providing for common cybersecurity requirements and evaluation criteria across national markets and sectors.

10. At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services or ICT processes, a conformity assessment body shall have at its disposal the necessary:

(a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service or ICT process in question and the mass or serial nature of the production process.



Openness ~~in~~ for cybersecurity

On the Feasibility of Stealthily Introducing Vulnerabilities in Open-Source Software via Hypocrite Commits

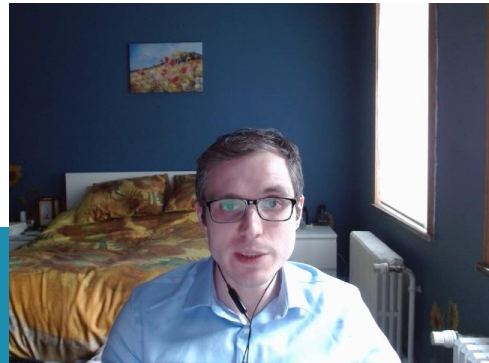
Qiushi Wu and Kangjie Lu
University of Minnesota
{wu000273, kjlu}@umn.edu

***Abstract*—Open source software (OSS) has thrived since the forming of Open Source Initiative in 1998. A prominent example is the Linux kernel, which has been used by numerous major software vendors and empowering billions of devices. The higher availability and lower costs of OSS boost its adoption, while its openness and flexibility enable quicker innovation. More importantly, the OSS development approach is believed to produce more reliable and higher-quality software since it typically has thousands of independent programmers testing and fixing bugs of the software collaboratively.**

In this paper, we instead investigate the insecurity of OSS from a critical perspective—the feasibility of stealthily introducing vulnerabilities in OSS via hypocrite commits (i.e., seemingly beneficial commits that in fact introduce other critical issues). The introduced vulnerabilities are critical because they may be stealthily exploited to impact massive devices. We first identify three fundamental reasons that allow hypocrite commits. (1) OSS is open by nature, so anyone from anywhere, including malicious ones, can submit patches. (2) Due to the overwhelming patches and performance issues, it is impractical for maintainers

Its openness also encourages contributors; OSS typically has thousands of independent programmers testing and fixing bugs of the software. Such an open and collaborative development not only allows higher flexibility, transparency, and quicker evolution, but is also believed to provide higher reliability and security [21].

A prominent example of OSS is the Linux kernel, which is one of the largest open-source projects—more than 28 million lines of code used by billions of devices. The Linux kernel involves more than 22K contributors. Any person or company can contribute to its development, e.g., submitting a patch through git commits. To make a change of the Linux kernel, one can email the patch file (containing `git diff` information) to the Linux community. Each module is assigned with a few maintainers (the list can be obtained through the script `get_maintainer.pl`). The maintainers then manually or employ tools to check the patch and apply it if it is deemed valid. Other



imec

The “Hypocrite Commits” Saga

2018

UMN bug-fix research on Linux kernel starts, and roughly 400 bug-fix patches are contributed over the next two years, mainly centered around specific research papers

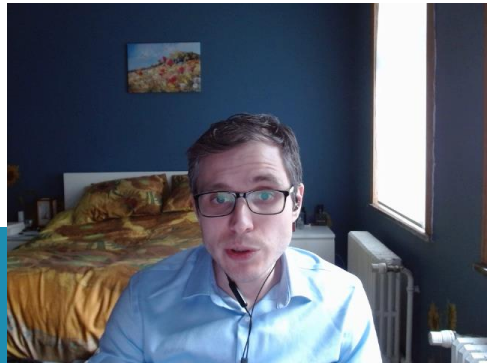
August 2020

“Hypocrite Commits” patches from UMN researchers sent to kernel developers under false identities.

November 2020

(1) ”Hypocrite Commits” paper is published + accepted by IEEE Symposium on Security and Privacy

(2) Sarah Jamie Lewis calls attention to paper’s ethics



imec

The “Hypocrite Commits” Saga

December 2020

(1) Sarah Jamie Lewis & others send a letter to IEEESSP

(2) UMN IRB appears to give an exemption to the research

April 2021

(1) Poor quality patches sent by UMN after 7 months of silence

(2) Greg Kroah-Hartman asks submitters to stop sending poor quality patches under the guise of “research on maintainers”

(3) Linux Foundation sends letter to UMN...

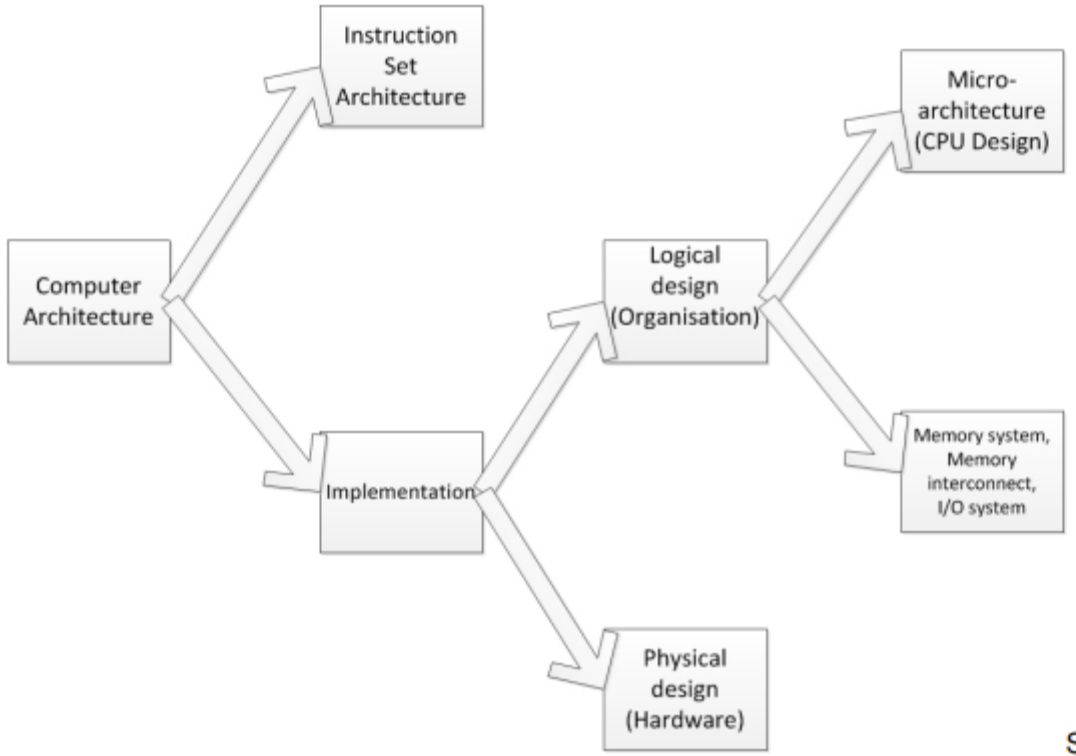
May 2021

Linux Foundation’s TAB publishes a technical report

imec

The “Hypocrite Commits” Saga - Community Backlash

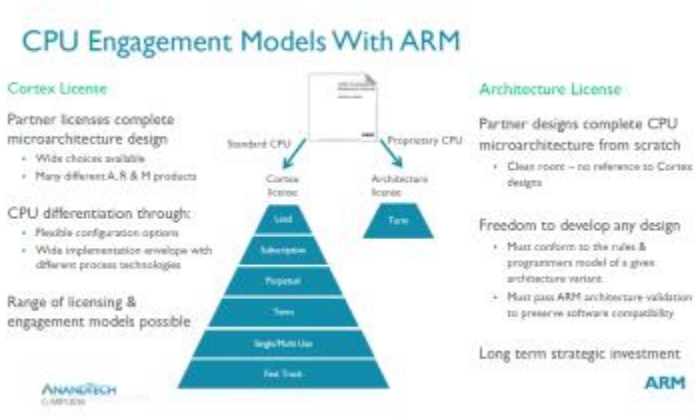
Zooming in: security in computer design



Source: *Wikimedia Commons*

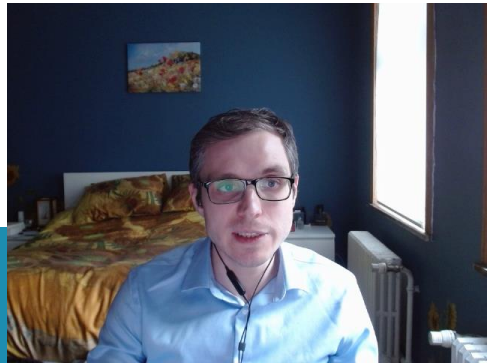
Dominant Instruction Set Architectures (ISAs)

arm



SPECTRE

MELTDOWN

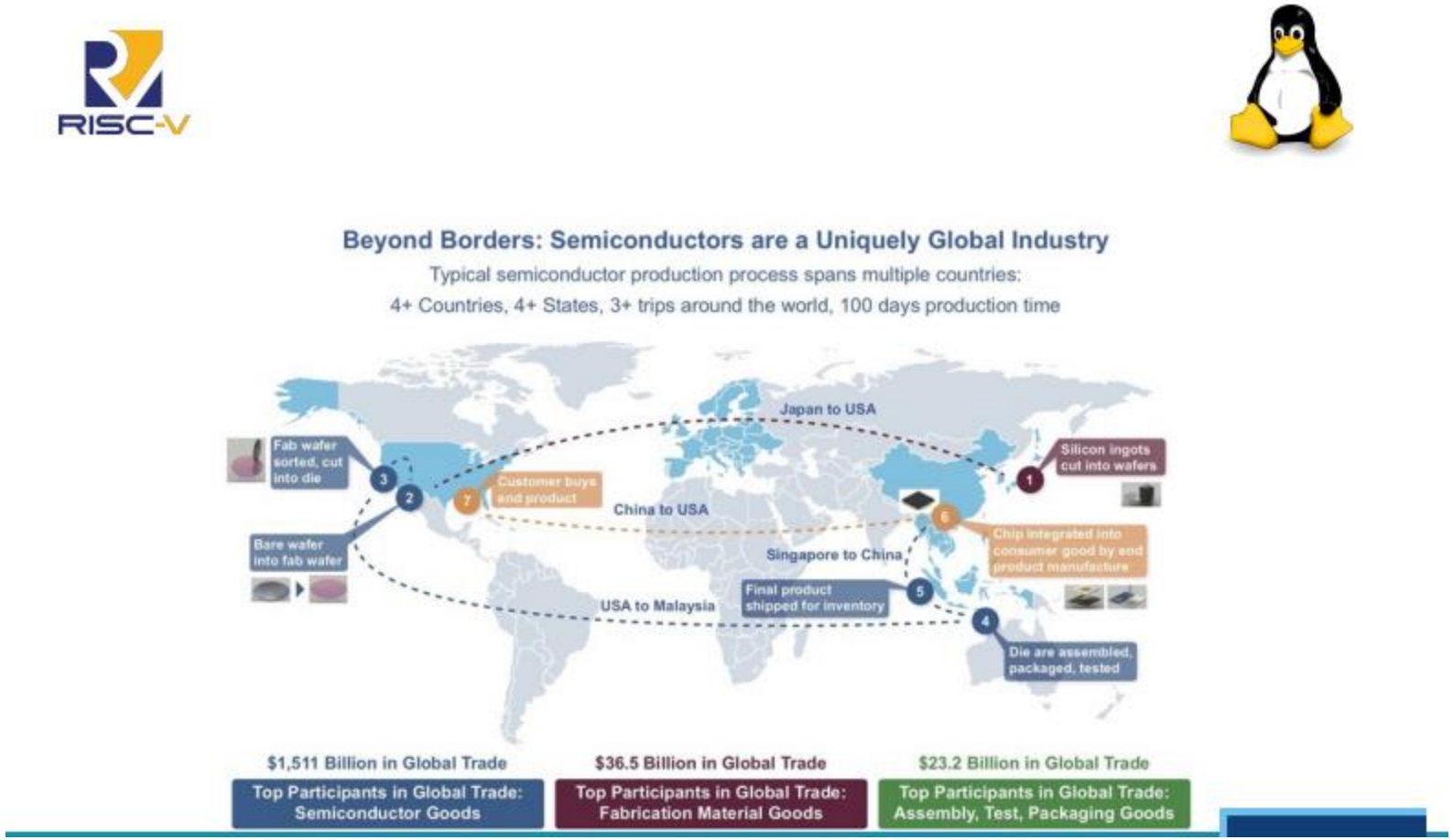


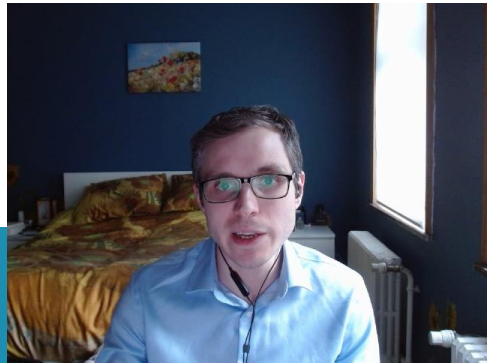
imec

ISA's role in cybersecurity

- What is 'correct implementation' of an ISA?
- Need of verification through open security review processes and 'security by design'
- Four issues with proprietary ISAs
  - Patents and licencing as barriers to (security) innovation
  - Independent software ecosystems and available expertise in open hardware communities
  - Dependency on a single company's vision and strategic goals
  - Transparency and shared core designs

Why open ISAs are good?

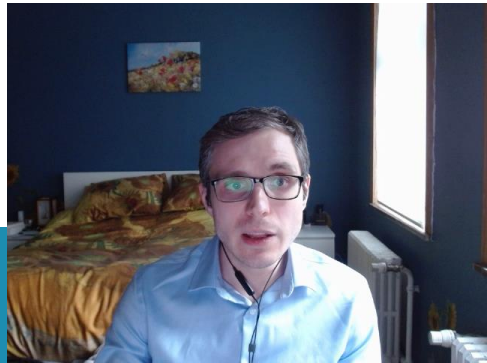




Security Promises of Open ISAs

Benefits	Risks
Modular design and extensibility	Ecosystem fragmentation
Transparency	Still chance of vulnerabilities
Long-term security evolution	Lack of interest by the community
Community review	Commercial and governmental support and scalability
Royalty-free use	Legacy compatibility, upfront transition costs

Table: Security Benefits and Risks of Open ISAs



imec

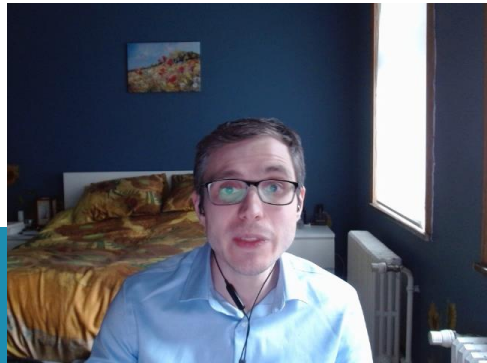
Legal Perils of Open ISAs

Manageability, Collaboration & Competition

- Open ISAs can bring more competition in the market
- Modularity can create a market for customised solutions (eg, security-focused FPGAs)
- Democratisation of computer design
- Standardisation challenges
- Attacks from incumbent players
- Geopolitical concerns

RETAIL NOVEMBER 25, 2019 / 1:36 PM / UPDATED A YEAR AGO

U.S.-based chip-tech group moving to Switzerland over trade curb fears



Legal Perils of Open ISAs

Intellectual Property Rights and Licencing

- Uncertainty about copyleft licencing applied to open source hardware
- Lack of open source or low-cost toolchains
- Legal status of code incorporated by the toolchain into the output
- Legal status of the bitstream - is it a computer program and, if so, who is running it?

imec

Legal Perils of Open ISAs

Liability

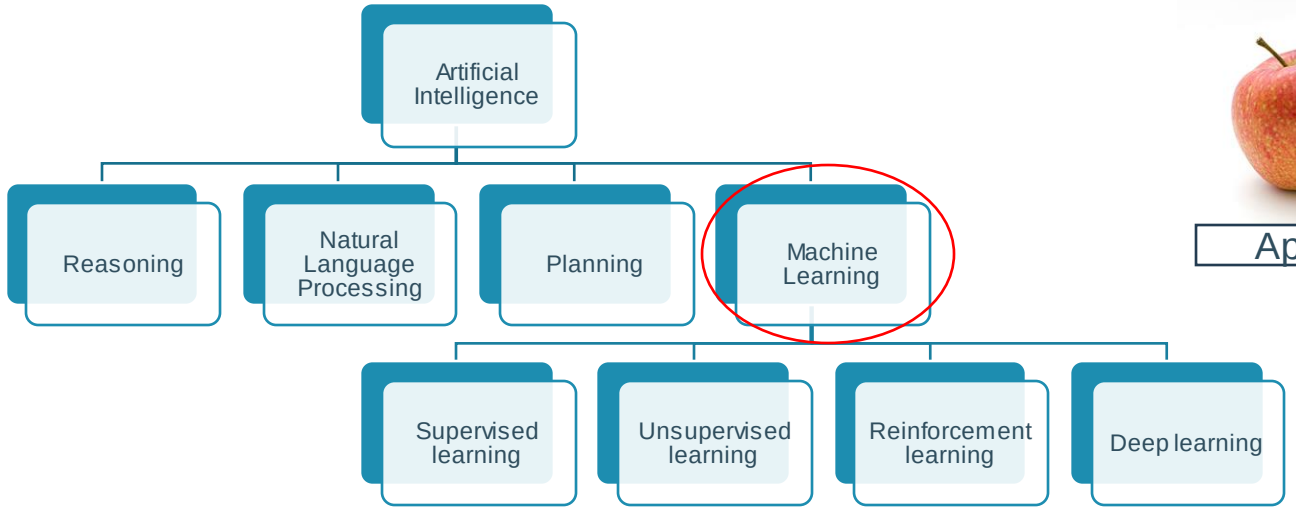
- Lawsuits in the aftermath of *Spectre* and *Meltdown*
- Case of *Intel Corp. CPU Marketing, Sales Practices and Product Liability Litigation, in the U.S. District Court for the District of Oregon*
- Liability for incorrect implementation?
- Liability for attacks combining software and hardware vulnerabilities?

imec

AI Cybersecurity: is it any different?

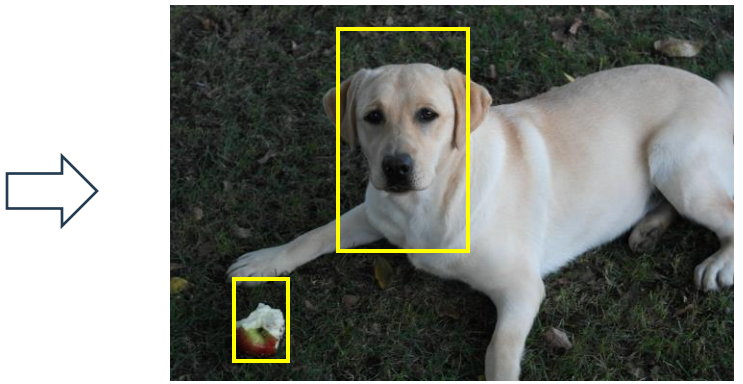
Technical and legal distinctions

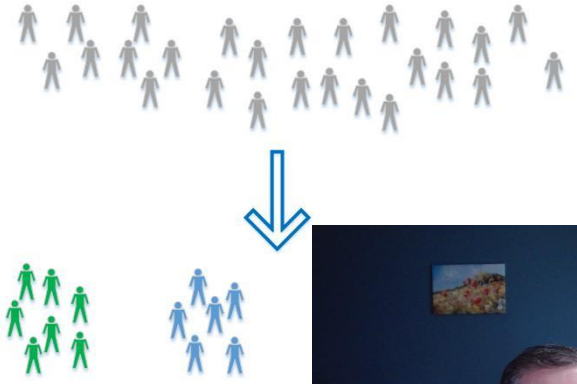
Overview of AI

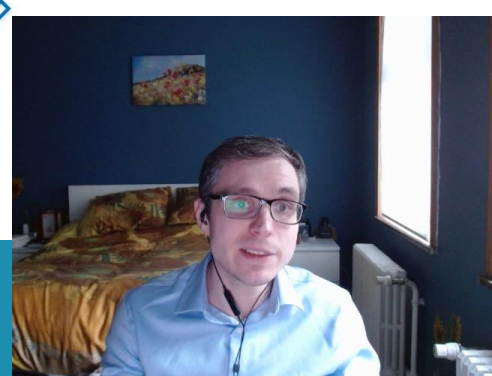


Dog

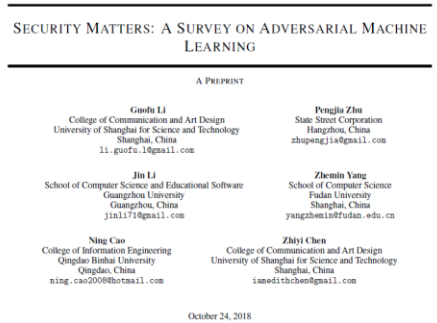
Apple







Attacking AI



SECURITY MATTERS: A SURVEY ON ADVERSARIAL MACHINE LEARNING

A PREPRINT

Guofu Li
College of Communication and Art Design
University of Shanghai for Science and Technology
Shanghai, China
li.guofu.l@gmail.com

Pengjia Zhu
State Street Corporation
Hangzhou, China
zhupengjia@gmail.com

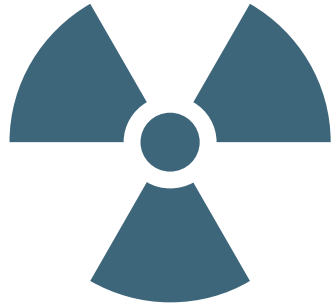
Jin Li
School of Computer Science and Educational Software
Guangzhou University
Guangzhou, China
jinli71@gmail.com

Zhemin Yang
School of Computer Science
Fudan University
Shanghai, China
yangzhemin@fudan.edu.cn

Ning Cao
College of Information Engineering
Qingdao Binhai University
Qingdao, China
ning.cao2006@hotmail.com

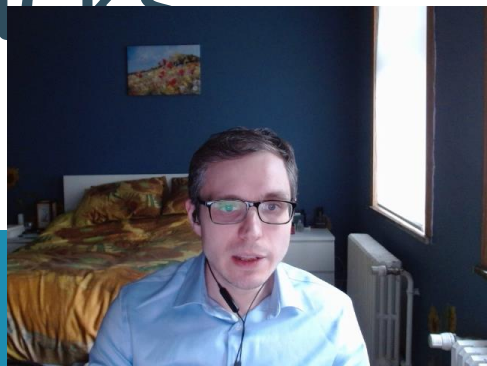
Zhiyi Chen
College of Communication and Art Design
University of Shanghai for Science and Technology
Shanghai, China
iameditchen@gmail.com

October 24, 2018

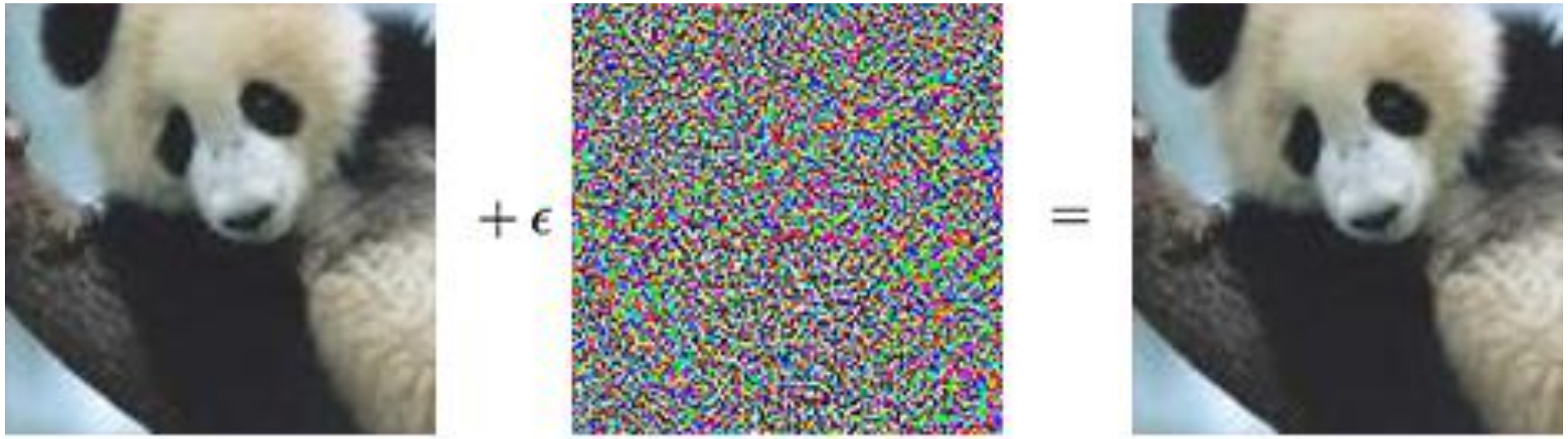


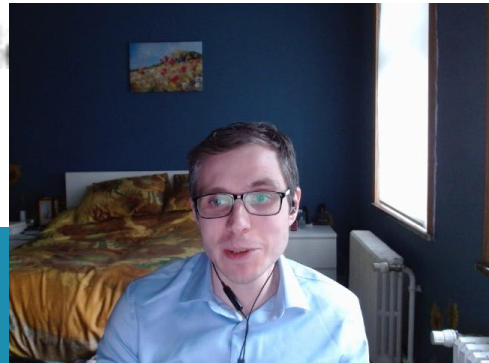
Evasion attacks

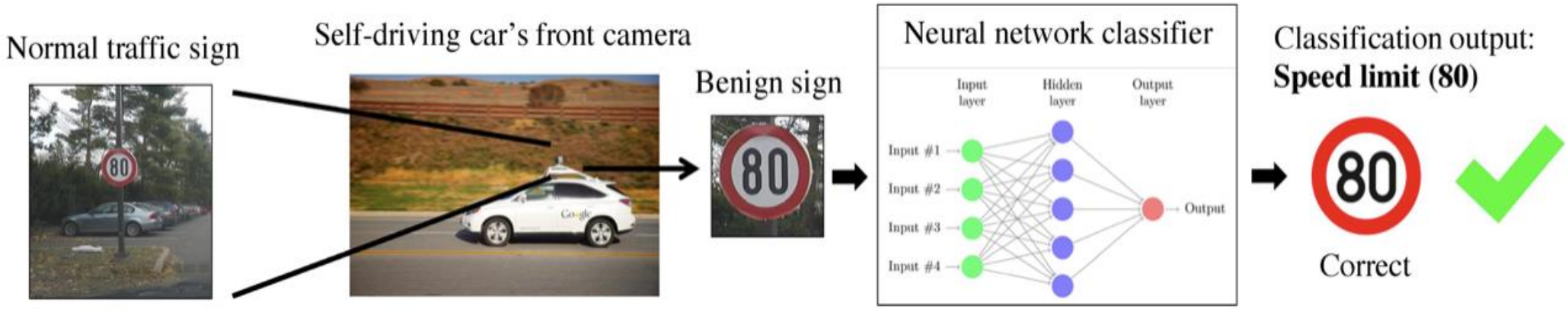
Poisoning attacks



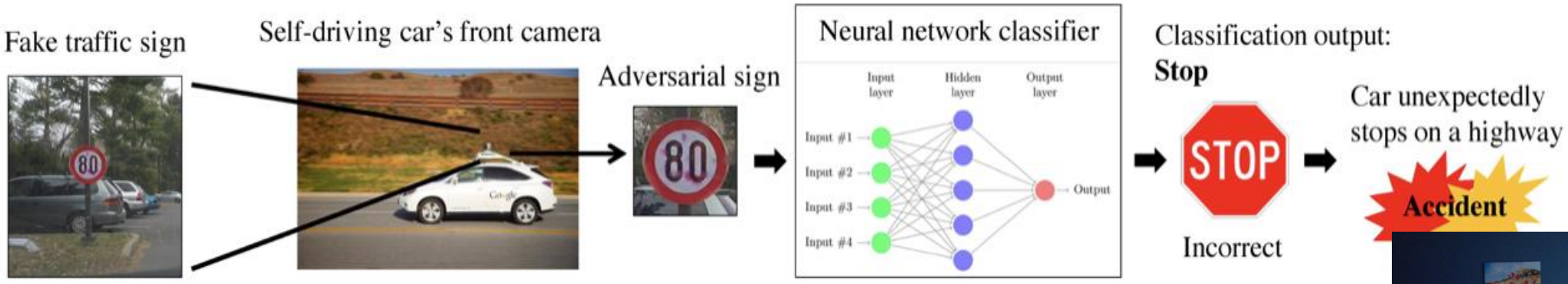
AI can used as both a defensive and an offensive tool

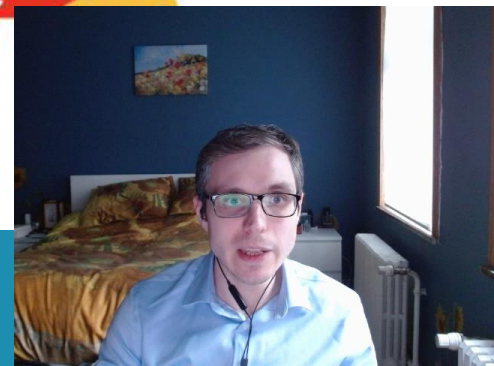






Autonomous car operation under benign conditions.





BELFER CENTER PAPER

Attacking Artificial Intelligence

AI's Security Vulnerability and W
Policymakers Can Do About It

Marcus Comiter

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
AUGUST 2019

Future of Humanity Institute | University of Oxford | Centre for the Study of Existential Risk | University of Cambridge | Center for a New American Security | Electronic Frontier Foundation | OpenAI

February 2018

The Malicious Use of Artificial Intelligence: recasting, Prevention, Mitigation

Dual nature of AI

Effectiveness of AI vs increased attack surface

- Effectiveness of AI comes at the price of increasing the attack surface
- Traditional cyber attacks exploit existing software vulnerabilities or employ social engineering
- AI cyberattacks exploit inherent and well-known limitations of the applied methods
- Scope of perpetrators is broader with attacks against AI

Legal risks of adversarial ML

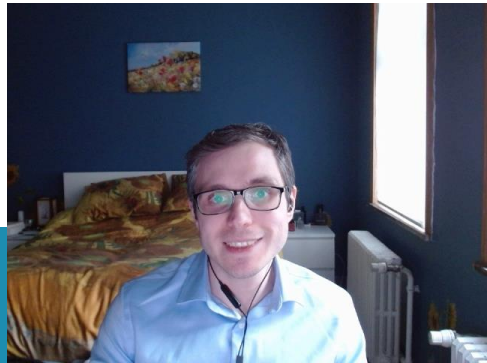
Attack	Description	1030(a)(2) Violation? (Narrow Interpretation by Second, Fourth, and Ninth Courts)	1030(a)(2) Violation? (Broad Interpretation by First, Fifth, Seventh, and Eleventh Circuit Courts)	1030(a)(5)(A) violation
Evasion Attack	Attacker modifies the query to get appropriate response	No	No	No
Model Inversion	Attacker recovers the secret features used in the model by through careful queries	No	Possible	No
Membership Inference	Attacker can infer if given data record was part of the model's training dataset or not	No	Possible	No
Model Stealing	Attacker is able to recover the model by constructing careful queries	No	Possible	No
Reprogramming the ML System	Repurpose the ML system to perform an activity it was not programmed for	No	Yes	Yes
Poisoning Attack	Attacker contaminates the training phase of ML systems to get intended result	No	Possible	Yes
Attacking the ML Supply Chain	Attacker compromises the ML models as it is being downloaded for use	Yes	Yes	Possible
Exploit Software Dependencies	Attacker uses traditional software exploits like buffer overflow to confuse ML systems	Yes	Yes	Yes

imec

Can AI be open and transparent?

Yes!

Reproducibility is key!



Conclusion

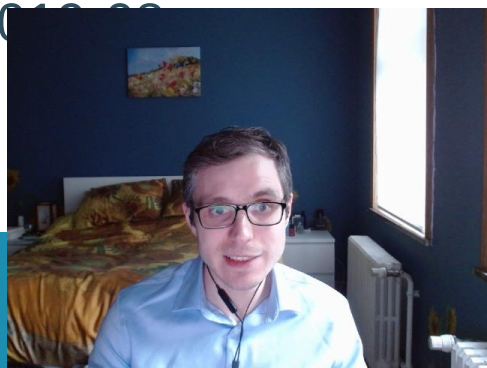
- Transparency - key sociotechnical requirement for trust in computing
- Need to focus on transparency of the low-level building blocks of computing
- Address the technical, organisations and legal challenges all at once
- Account for the systemic challenges in the integrated circuit supply chain
- Towards an interdisciplinary approach to transparency regulation for cybersecurity

Is open (always) good for cybersecurity?

- Should the law make it mandatory for supply chain actors to render their contractors with information protected by IPRs?
- Is such a view tenable in light of the legitimate interests of these stakeholders?
- When is an open approach not good for cybersecurity?
- Should the law treat alike cyber attacks against traditional IT systems and cyber attacks against AI systems?
- Can disclosure requirements, eg in patent law, enable more open and transparent AI systems?

Recommended reading

- Li, Guofu, Pengjia Zhu, Jin Li, Zhemin Yang, Ning Cao, and Zhiyi Chen. "Security matters: A survey on adversarial machine learning." arXiv preprint arXiv:1810.07339 (2018)
- Kumar, Ram Shankar Siva, David R. O'Brien, Kendra Albert, and Salome Vilojen. "Law and adversarial machine learning." arXiv preprint arXiv:1810.10731 (2018)
- Kumar, Ram Shankar Siva, Jonathon Penney, Bruce Schneier, and Kendra Albert. "Legal risks of adversarial machine learning research." arXiv preprint arXiv:2006.16179 (2020)
- Siva Kumar, Ram Shankar, Jon Penney, Bruce Schneier, and Kendra Albert. "Legal Risks of Adversarial Machine Learning Research." In International Conference on Machine Learning (ICML) 2020 Workshop on Law & Machine Learning. 2020
- Schneier, Bruce. "Attacking machine learning systems." Computer 53, no. 5 (2020): 78-80
- Comiter, Marcus. "Attacking artificial intelligence." Belfer Center Paper (2019): 2



Thanks for listening!

Q&A