Pluribus One
seeing one in many

Pattern Recognition and Applications Lab

University of Cagliari, Italy

Machine Learning (for) Security:
Lessons Learned and Future Challenges

Battista Biggio

battista.biggio@unica.it

@biggiobattista

Pluribus One and PRA lab @ University of Cagliari, Italy

Summer School on real-world crypto and privacy
Šibenik, Croatia

Summer School on Security and Privacy, Šibenik, Croatia – June 14, 2022

Artificial Intelligence Today

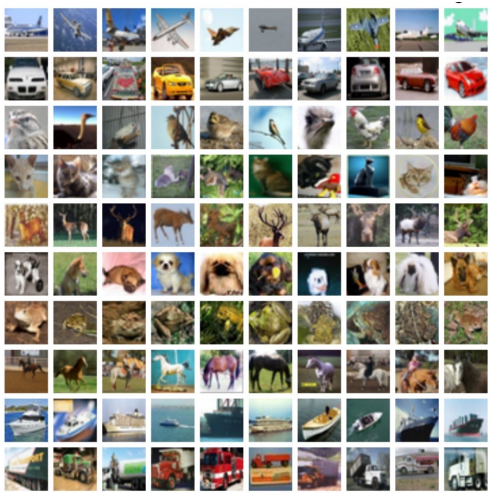
AI is going to transform industry and business as electricity did about a century ago

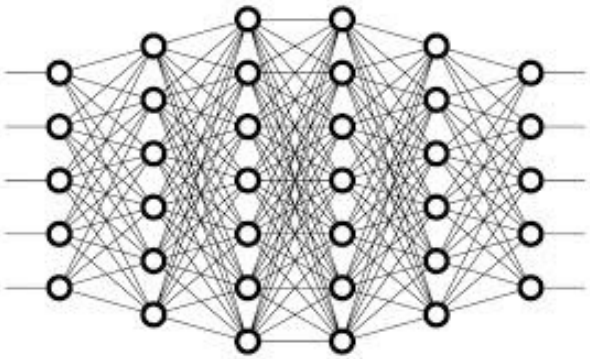
(*Andrew Ng, Jan. 2017*)

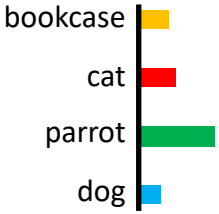
Applications:

- Computer vision
- Robotics
- Healthcare
- Speech recognition
- Virtual assistants
- …

Modern AI is Numerical Optimization + Big Data





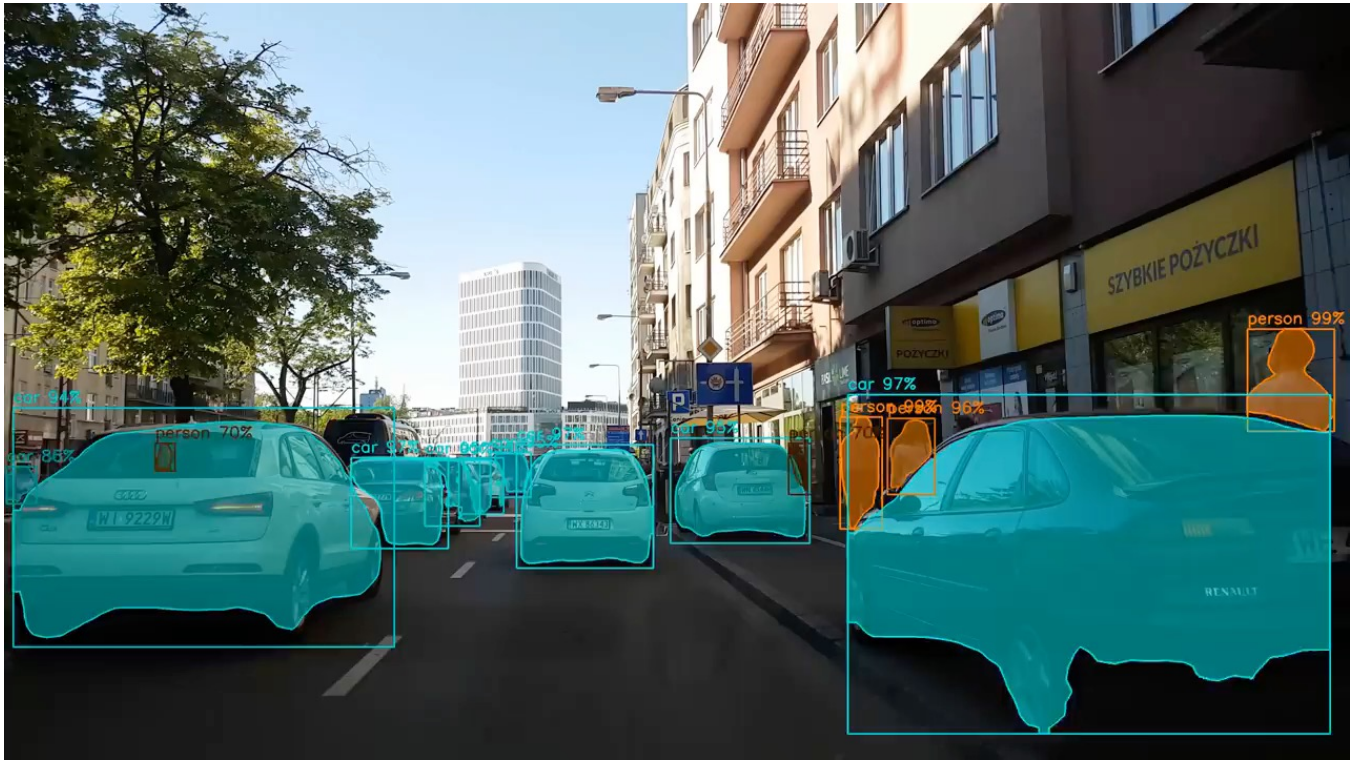


$$\min_{\boldsymbol{w}} L(D;\boldsymbol{w})$$

The goal is to minimize the fraction of *classification errors*

... by iteratively updating the classifier parameters $\boldsymbol{w}$ along the gradient direction $\nabla_{\boldsymbol{w}} L(D;\boldsymbol{w})$

Computer Vision for Self-Driving Cars



He et al., *Mask R-CNN*, ICCV '17, https://arxiv.org/abs/1703.06870

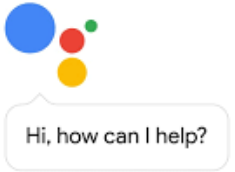
Video from: https://www.youtube.com/watch?v=OOT3UIXZztE

Speech Recognition for Virtual Assistants

Amazon Alexa

Apple Siri

Microsoft Cortana



Google Assistant

But Is AI Really *Smart*?
Should We Trust These Algorithms?

Adversarial Glasses

- Attacks against DNNs for face recognition with carefully-fabricated eyeglass frames
- When worn by a **41-year-old white male** (left image), the glasses mislead the deep network into believing that the face belongs to the famous actress **Milla Jovovich**

Sharif et al., *Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition*, ACM CCS 2016

Adversarial Road Signs

Eykholt et al., *Robust physical-world attacks on deep learning visual classification*, CVPR 2018

Audio Adversarial Examples

Audio	Transcription by Mozilla DeepSpeech
	“without the dataset the article is useless”
	“okay google browse to evil dot com”

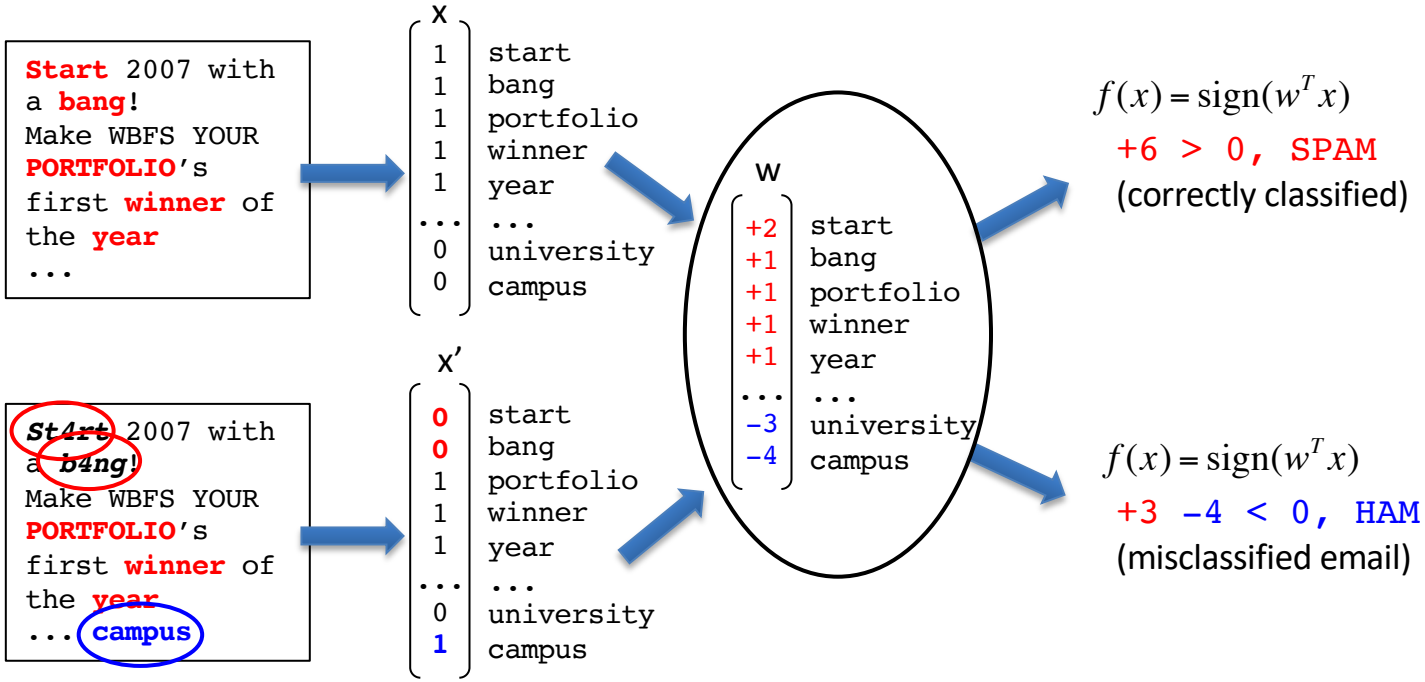
Carlini and Wagner, *Audio adversarial examples: Targeted attacks on speech-to-text*, DLS 2018

https://nicholas.carlini.com/code/audio_adversarial_examples/

How Do These Attacks Work?

Evasion of Linear Classifiers

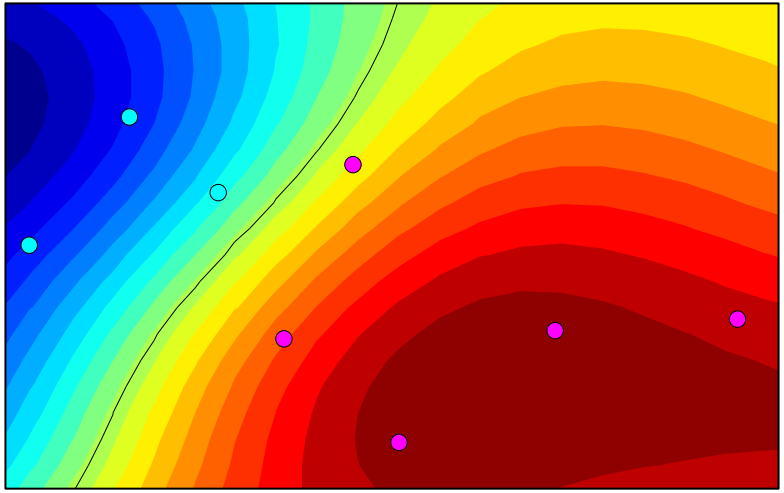
- **Problem:** how to evade a linear (trained) classifier?



Evasion of Nonlinear Classifiers

- **What if the classifier is nonlinear?**

- Decision functions can be arbitrarily complicated, with no clear relationship between features (**x**) and classifier parameters (**w**)



Detection of Malicious PDF Files

Srndic & Laskov, Detection of malicious PDF files based on hierarchical document structure, NDSS 2013

"The most aggressive evasion strategy we could conceive was successful for only 0.025% of malicious examples tested against a nonlinear SVM classifier with the RBF kernel [...].

Currently, we do not have a rigorous mathematical explanation for such a surprising robustness. Our intuition suggests that [...] ***the space of true features is "hidden behind" a complex nonlinear transformation which is mathematically hard to invert****.*

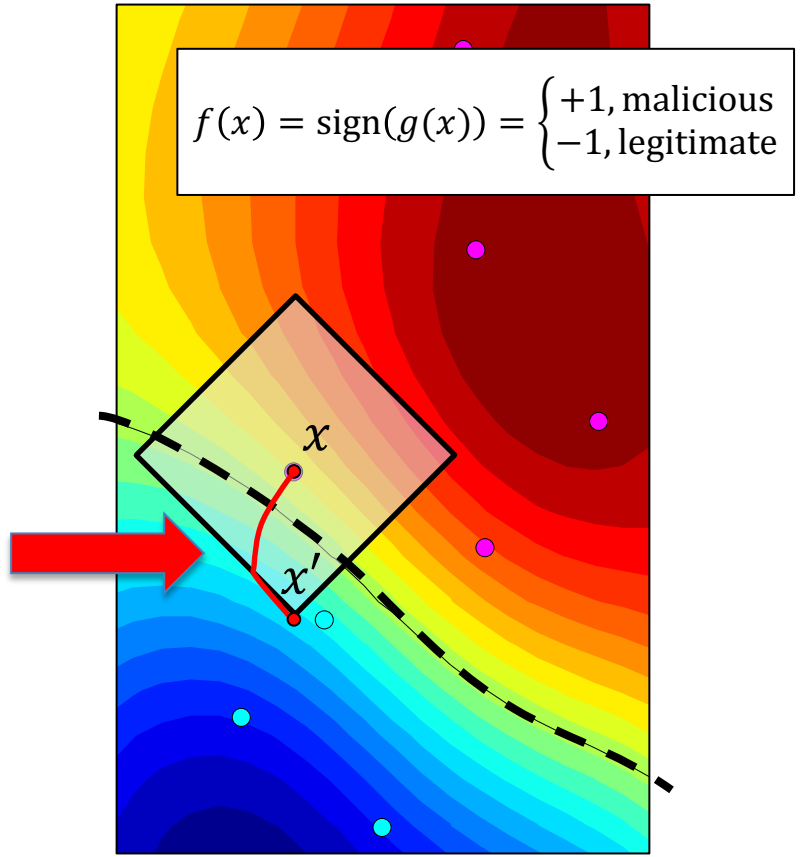
[...] the same attack staged against the linear classifier [...] had a 50% success rate; hence, ***the robustness of the RBF classifier must be rooted in its nonlinear transformation****"*

Evasion Attacks against Machine Learning at Test Time

- **Main idea:** to formalize the attack as an optimization problem

$$\min_{x'} g(x')$$
$$\text{s.t.} \|x - x'\| \leq \varepsilon$$

- Non-linear, constrained optimization
  - **Projected gradient descent**: approximate solution for *smooth* functions
- Gradients of *g(x)* can be analytically computed in many cases
  - SVMs, Neural networks



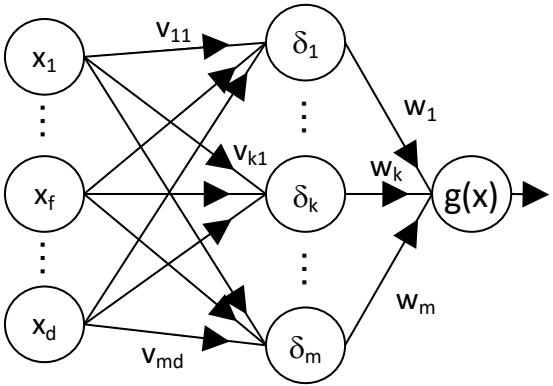
Computing Descent Directions

Support vector machines

$$g(x) = \sum_i \alpha_i y_i k(x, x_i) + b, \quad \nabla g(x) = \sum_i \alpha_i y_i \nabla k(x, x_i)$$

RBF kernel gradient: $\nabla k(x, x_i) = -2\gamma \exp\left\{-\gamma \| x - x_i \|^2\right\}(x - x_i)$

Neural networks

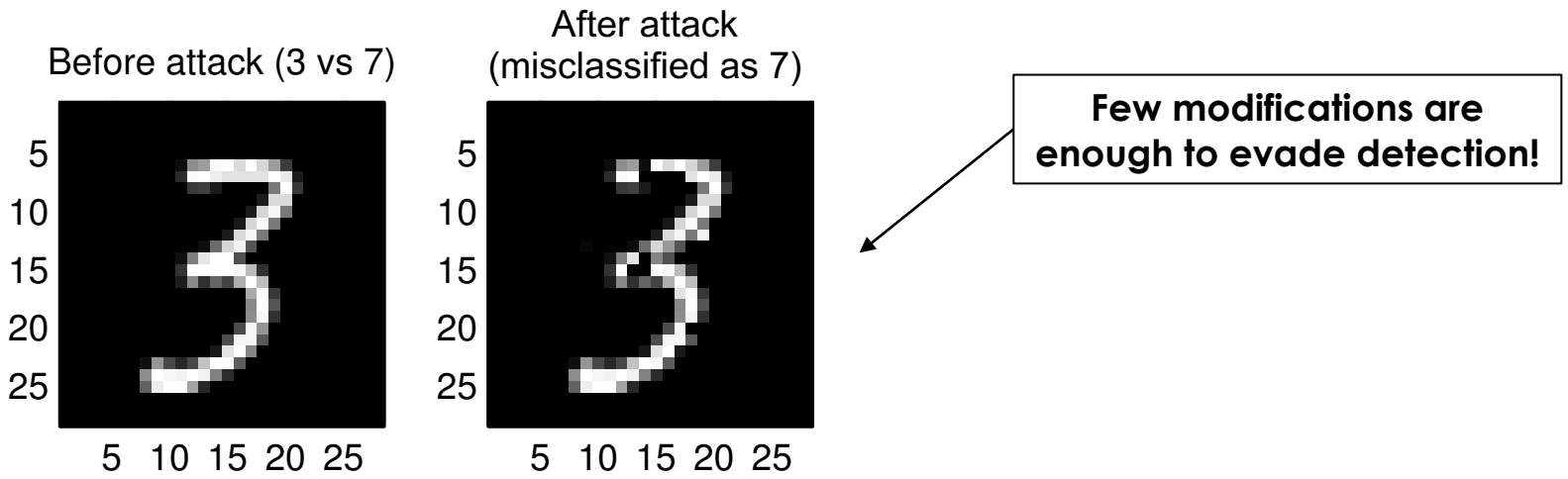


$$g(x) = \left[1 + \exp\left(-\sum_{k=1}^{m} w_k \delta_k(x)\right)\right]^{-1}$$

$$\frac{\partial g(x)}{\partial x_f} = g(x)\left(1 - g(x)\right) \sum_{k=1}^{m} w_k \delta_k(x)\left(1 - \delta_k(x)\right) v_{kf}$$

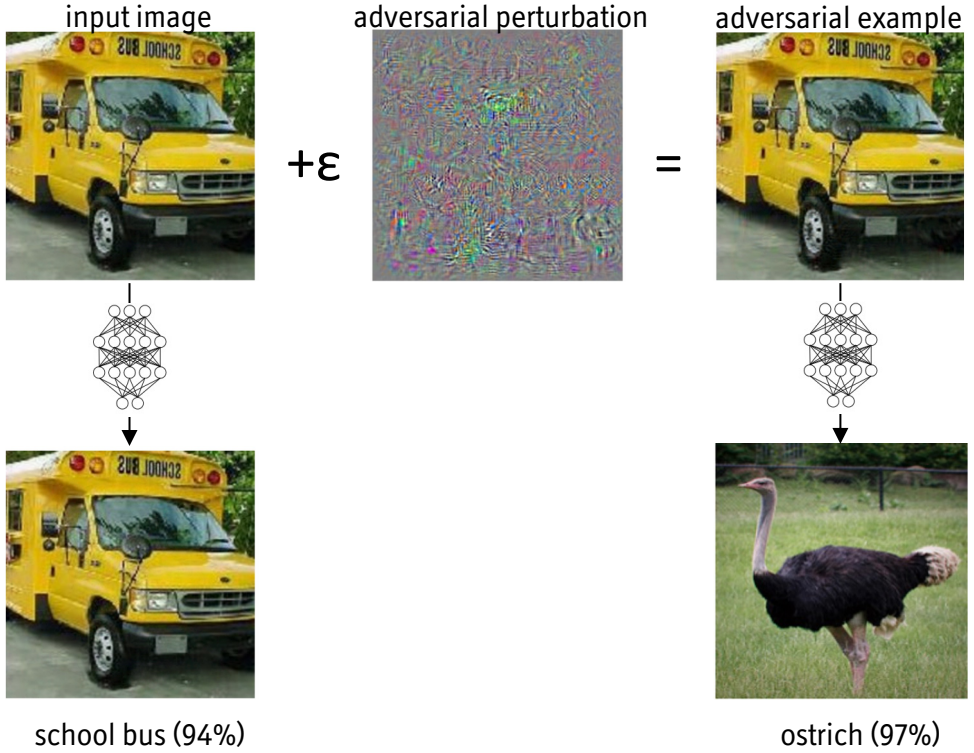
An Example on Handwritten Digits

- Nonlinear SVM (RBF kernel) to discriminate between ‘3’ and ‘7’
- **Features**: gray-level pixel values (28 x 28 image = 784 features)



Adversarial Examples against Deep Neural Networks

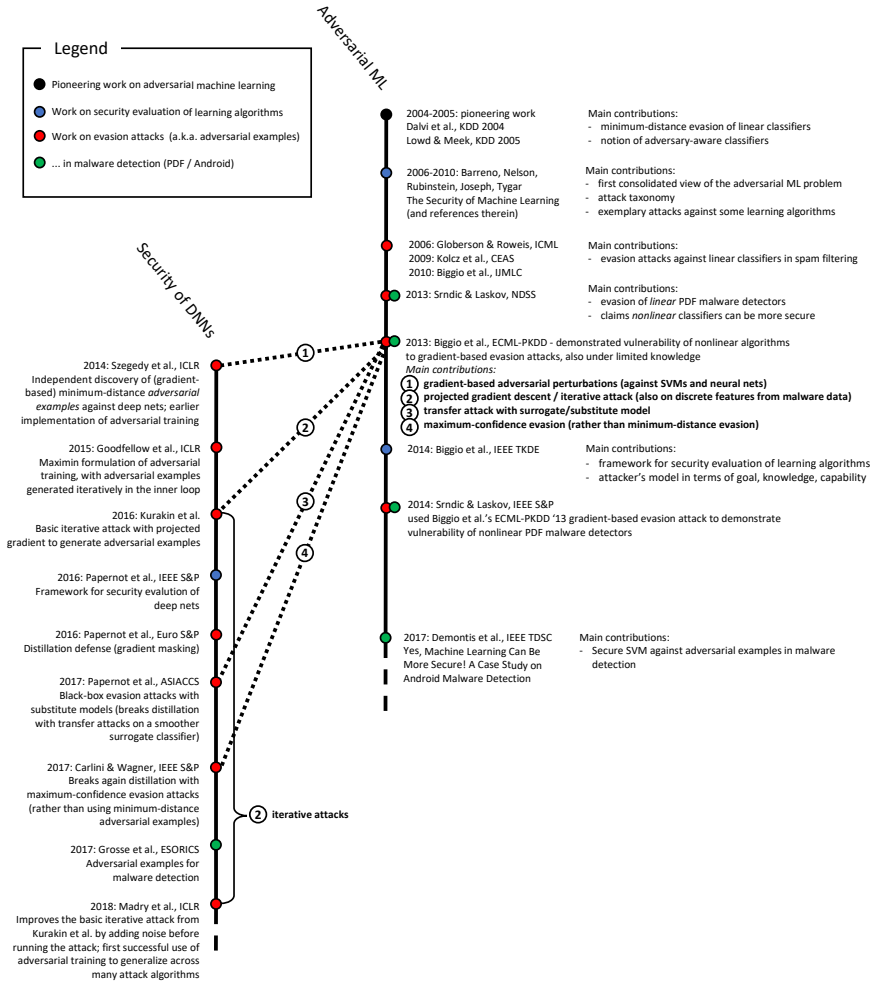
- Szegedy et al. (2014) independently developed gradient-based attacks against DNNs
- They were investigating model interpretability, trying to understand at which point a DNN prediction changes
- They found that the minimum perturbations required to trick DNNs were really small, even imperceptible to humans



Timeline of Learning Security

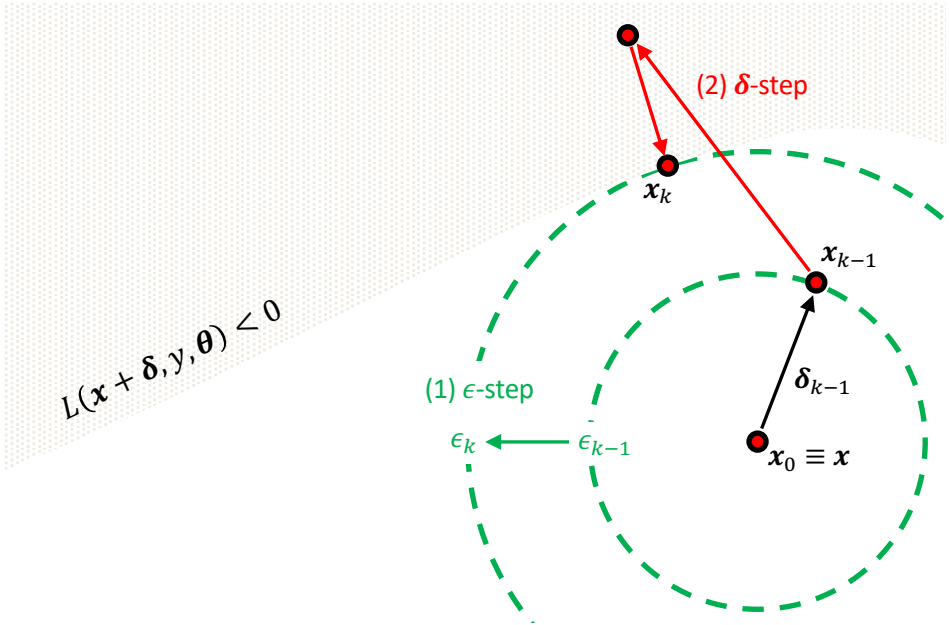
Biggio and Roli, **Wild Patterns**: *Ten Years After The Rise of Adversarial Machine Learning*, Pattern Recognition, 2018

2021 Best Paper Award and Pattern Recognition Medal



Fast Minimum-Norm (FMN) Attacks (Pintor, Biggio et al., NeurIPS '21)

Biggio et al., 2013
Szegedy et al., 2014
Goodfellow et al., 2015 (FGSM)
Papernot et al., 2015 (JSMA)
Carlini & Wagner, 2017 (CW)
Madry et al., 2017 (PGD)
...
Croce et al., FAB, AutoPGD ...
Rony et al., DDN, ALMA, ...
Pintor et al., 2021 (FMN)



FMN

Fast convergence to good local optima

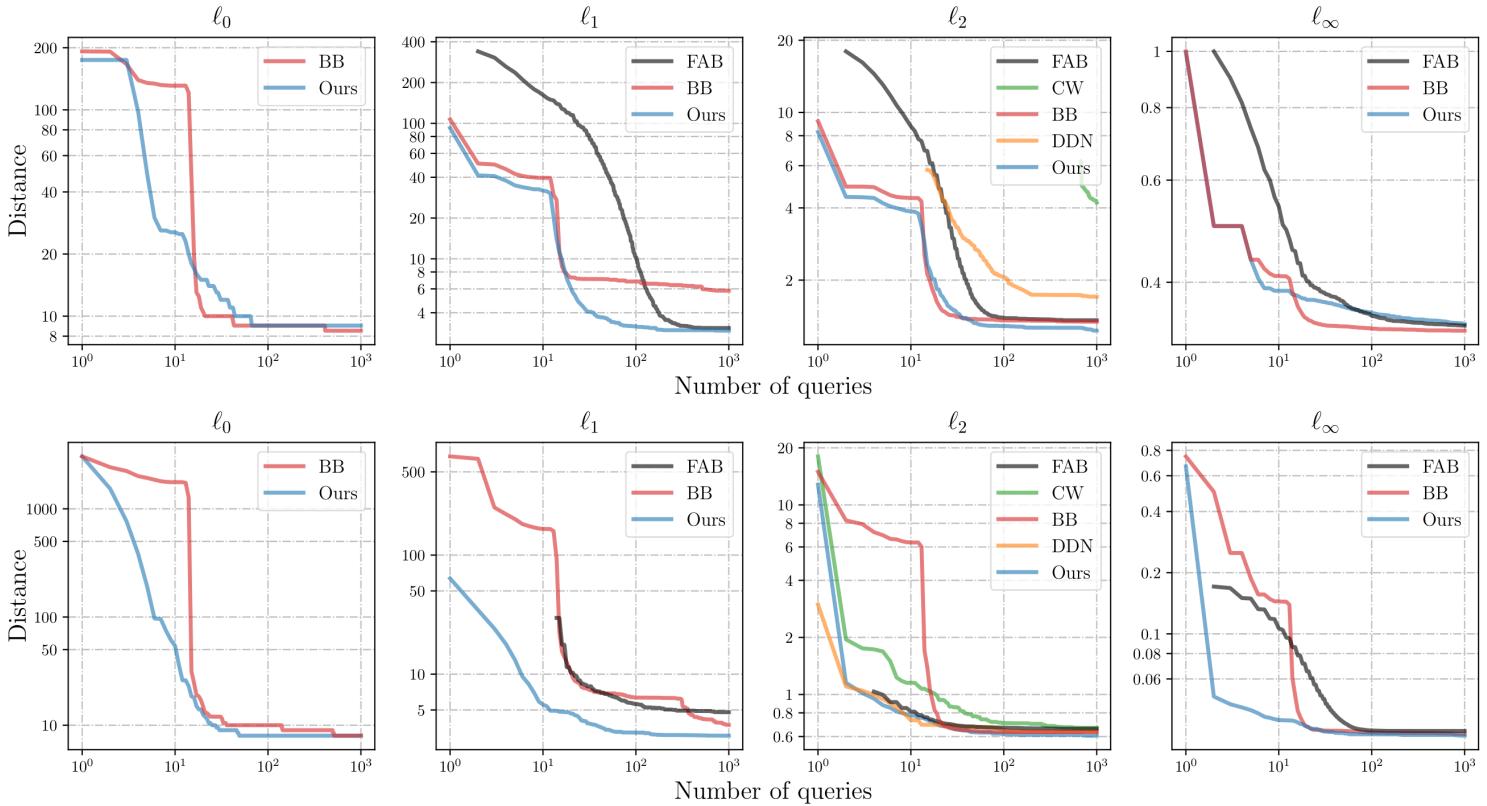
Works in different norms ($\ell_0, \ell_1, \ell_2, \ell_\infty$)

Easy tuning /robust to hyperparameter choice

Experimental Results: Query-distortion Curves

MNIST challenge

CIFAR challenge

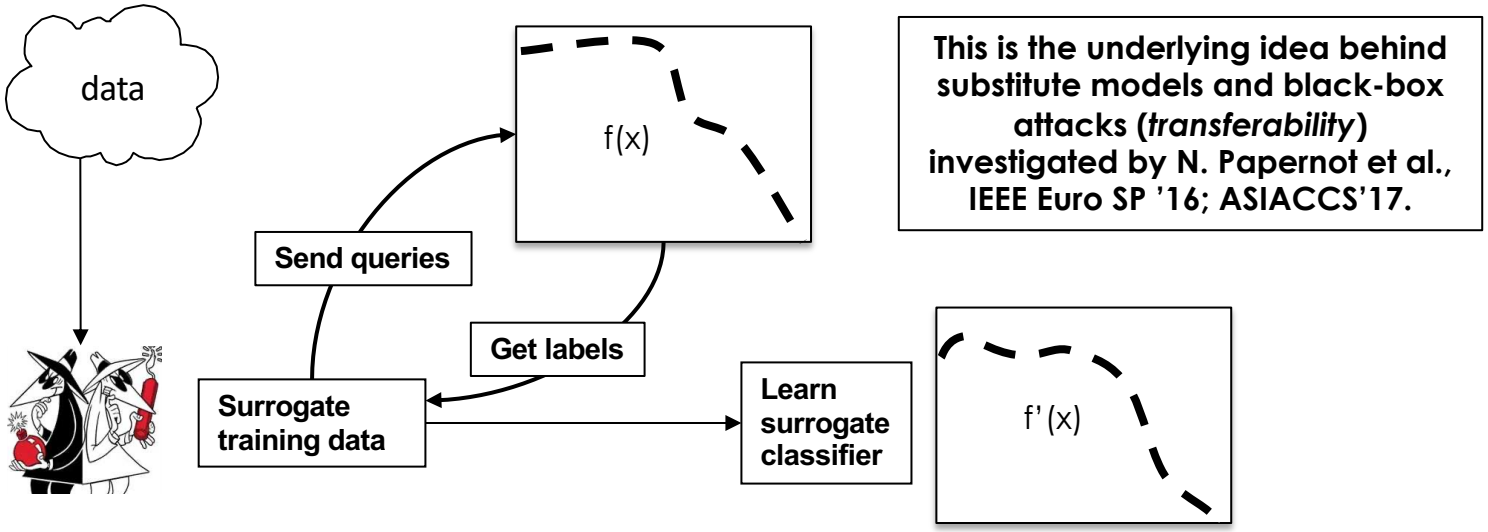


Pintor et al., *Fast minimum-norm adversarial attacks through adaptive norm constraints*, NeurIPS 2021

From White-Box to Black-Box Attacks

From White-box to Black-box *Transfer* Attacks

- Only feature representation and (possibly) learning algorithm are known
- Surrogate data sampled from the same distribution as the classifier's training data
- Classifier's feedback to label surrogate data

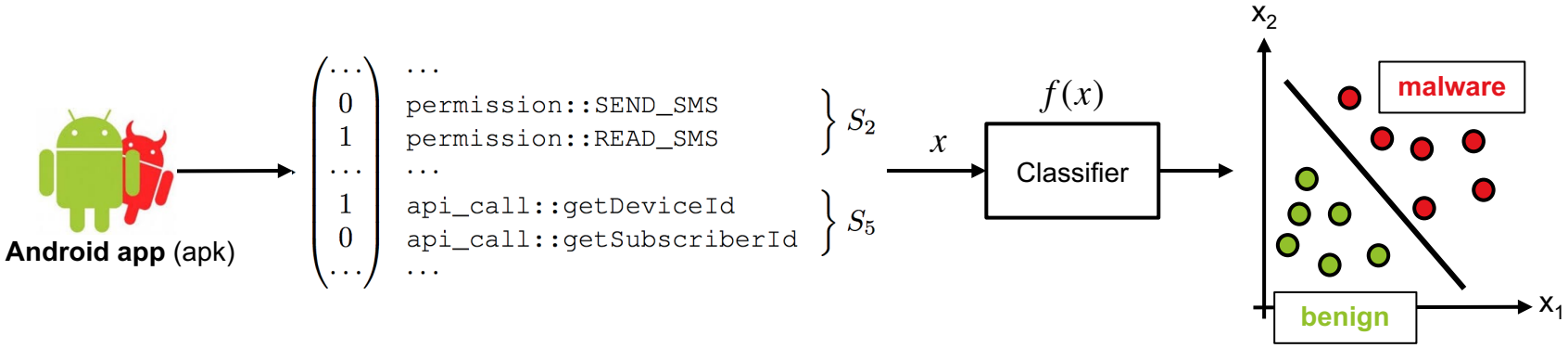


This is the underlying idea behind substitute models and black-box attacks (*transferability*) investigated by N. Papernot et al., IEEE Euro SP '16; ASIACCS'17.

Results on Android Malware Detection

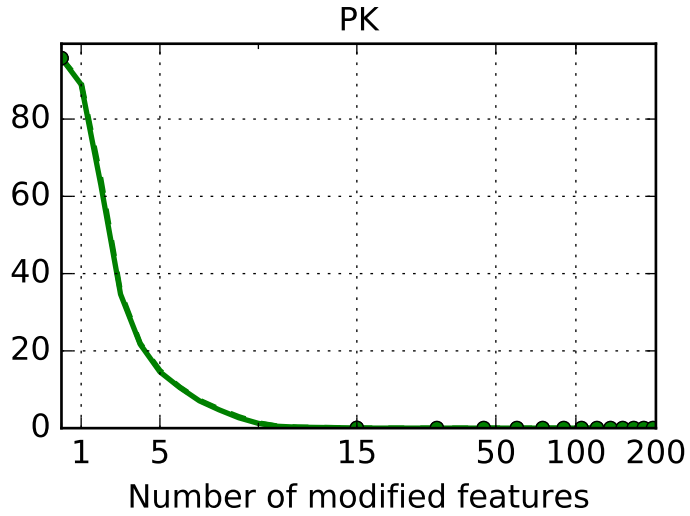
- **Drebin:** Arp et al., NDSS 2014
  - Android malware detection directly on the mobile phone
  - Linear SVM trained on features extracted from static code analysis

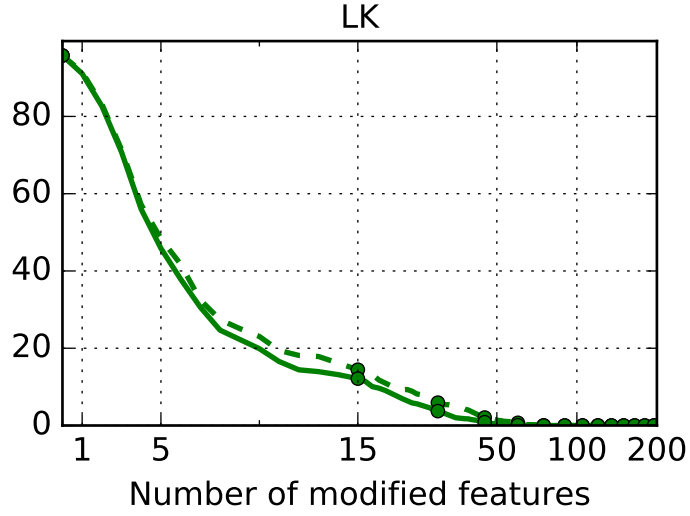
Feature sets		
manifest	S_1	Hardware components
	S_2	Requested permissions
	S_3	Application components
	S_4	Filtered intents
dexcode	S_5	Restricted API calls
	S_6	Used permission
	S_7	Suspicious API calls
	S_8	Network addresses



Results on Android Malware Detection

- **Dataset (Drebin):** 5,600 malware and 121,000 benign apps (TR: 30K, TS: 60K)
- **Detection rate** at FP=1% vs max. number of manipulated features (averaged on 10 runs)
  - Perfect knowledge (PK) white-box attack; Limited knowledge (LK) black-box attack

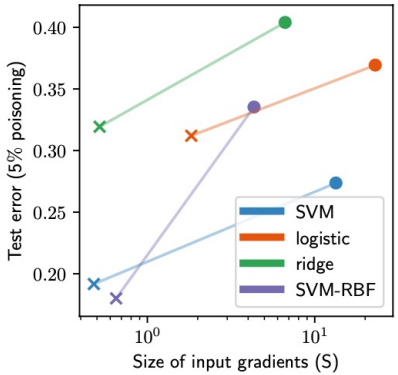


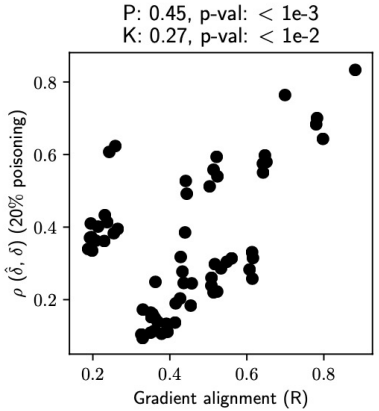


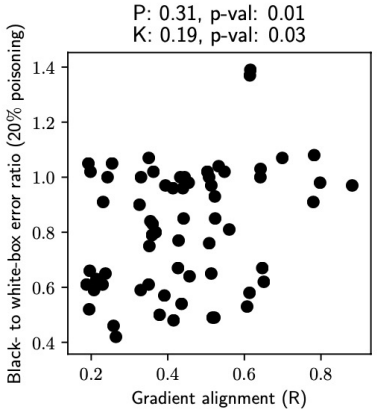
Why Do Adversarial Attacks Transfer? (USENIX Sec. 2019)

- Transferability is the ability of an attack developed against a surrogate model to succeed also against a different target model

- In our paper, we show that *transferability* depends on
  - the **vulnerability of the target model**, and
  - the **alignment of** (poisoning/evasion) **gradients** between the target and the surrogate model



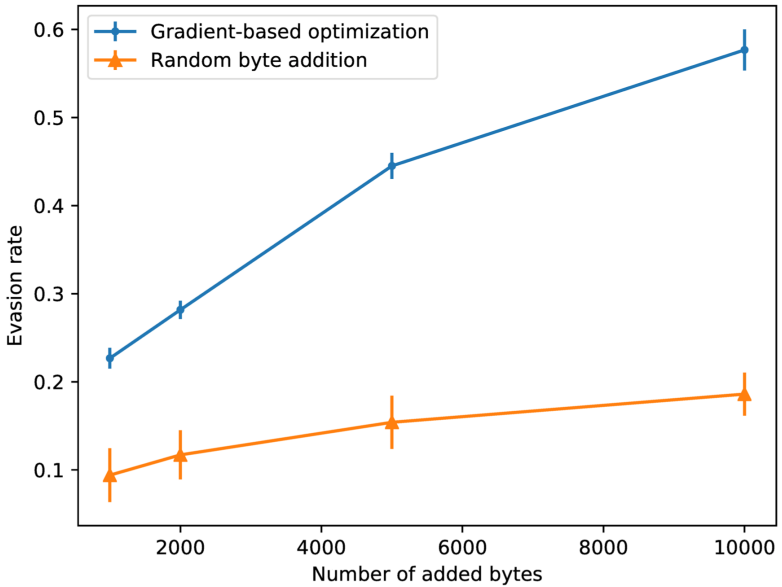


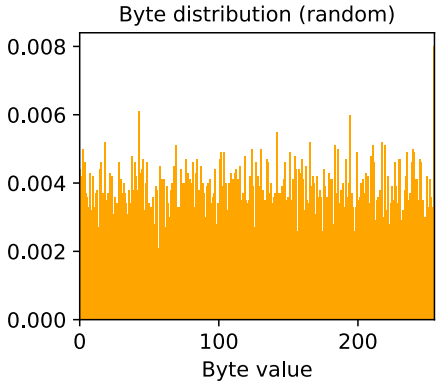


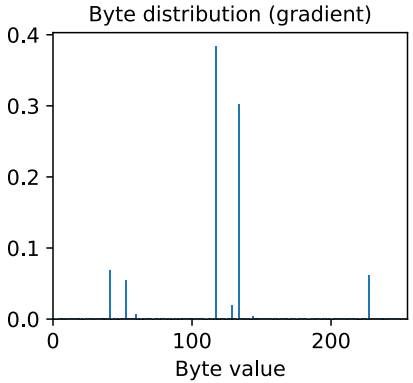
Attacks on EXE Malware

Evasion of Deep Networks for EXE Malware Detection

- **MalConv**: convolutional deep network trained on raw bytes to detect EXE malware
- Our attack can evade it by adding few padding bytes



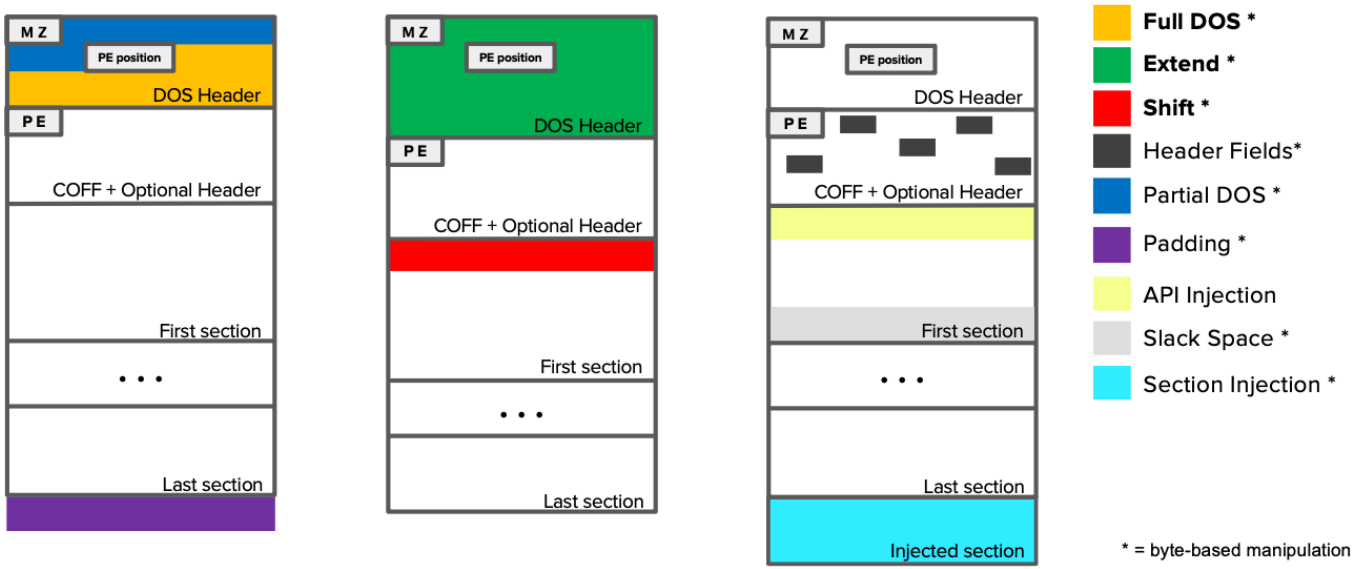




Kolosniaji, Biggio et al., *Adversarial Malware Binaries*, EUSIPCO2018
Demetrio, Biggio et al., *Explaining Vulnerability of DL*, ITASEC 2019

Adversarial EXEmples: Practical Attacks on Machine Learning for Windows Malware Detection

- **Problem-space attacks:** crafting evasive malware programs that preserve functionality!



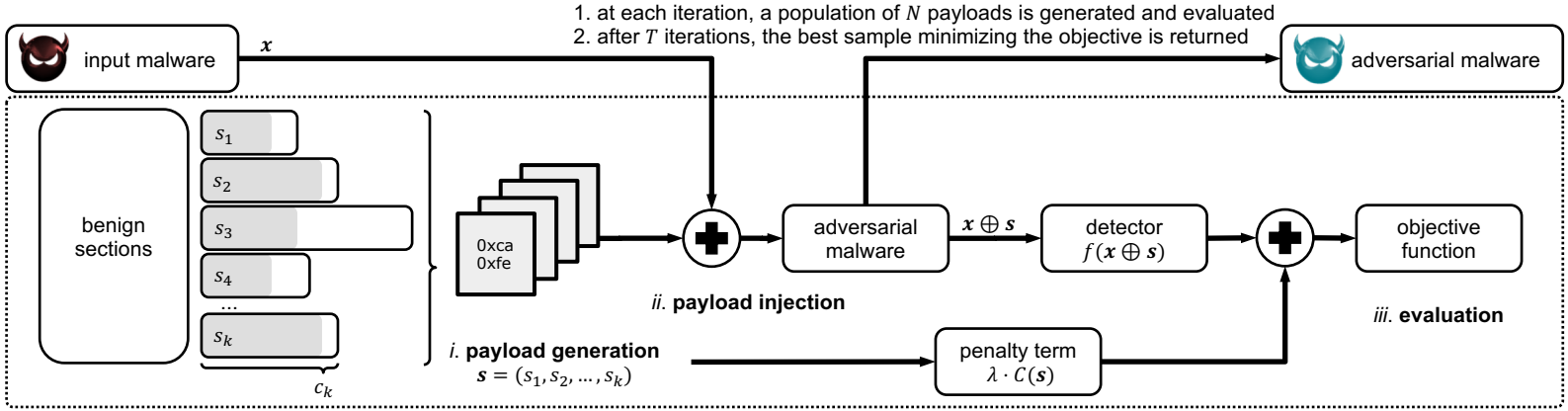
Demetrio, Biggio, et al., Adversarial EXEmples, ACM TOPS 2021
Demetrio, Biggio, et al., Functionality-preserving ..., IEEE TIFS 2021

Black-box Attacks on EXE Malware

Functionality-preserving Black-box Optimization of Adversarial Windows Malware

- Black-box genetic algorithm optimizing the injection of benign sections into malicious PE files

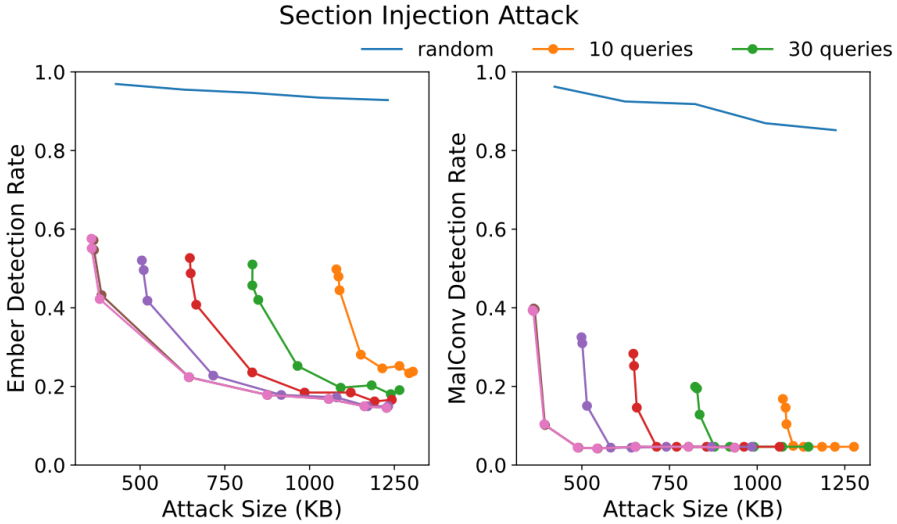
$$s^* = \arg\min_{s \in \mathcal{S}_k} f(x \oplus \boldsymbol{s}) + \lambda \mathcal{C}(\boldsymbol{s})$$
$$\text{subject to} \quad \mathcal{Q}(\boldsymbol{s}) \leq T$$



Black-box Attacks on EXE Malware

Functionality-preserving Black-box Optimization of Adversarial Windows Malware

- Our attack bypasses state-of-the-art machine learning-based detectors also with very small payload sizes

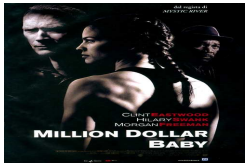


- Surprisingly, it also works against some commercial anti-malware solutions available from VirusTotal!

	Malware	Random	Sect. Injection
AV1	93.5%	85.5%	30.5%
AV2	85.0%	78.0%	68.0%
AV3	85.0%	46.0%	43.5%
AV4	84.0%	83.5%	63.0%
AV5	83.5%	79.0%	73.0%
AV6	83.5%	82.5%	69.5%
AV7	83.5%	54.5%	52.5%
AV8	76.5%	71.5%	60.5%
AV9	67.0%	54.5%	16.5%

Detection rates of AV products from VirusTotal, including AVs in the Gartner's leader quadrant. Our **section-injection attack** evades detection with high probability. We are in touch with some AV companies for responsible disclosure of such a vulnerability.

Countering Evasion Attacks



What is the rule? The rule is protect yourself at all times (from the movie “Million dollar baby”, 2004)

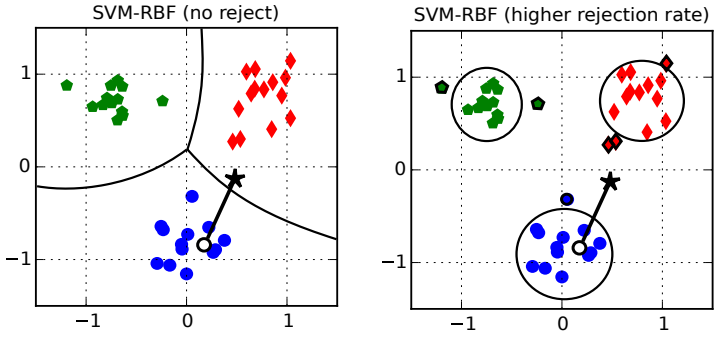
Security Measures against Evasion Attacks

1. **Robust optimization** to model attacks during learning
   - adversarial training / regularization

$$\min_{\boldsymbol{w}} \sum_i \max_{||\boldsymbol{\delta}_i|| \leq \epsilon} \ell(y_i, f_{\boldsymbol{w}}(\boldsymbol{x}_i + \boldsymbol{\delta}_i))$$

bounded perturbation!

2. **Rejection / detection** of adversarial examples

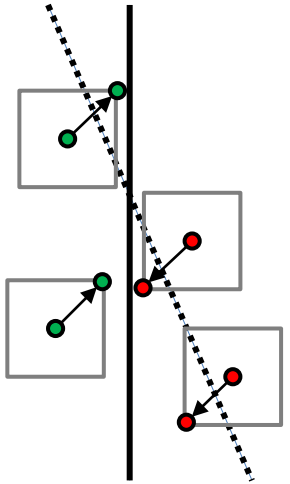


Increasing Input Margin via Robust Optimization

- Robust optimization (a.k.a. *adversarial training*)

$$\min_{\boldsymbol{w}} \max_{||\boldsymbol{\delta}_i||_\infty \leq \epsilon} \sum_i \ell\left(y_i, f_{\boldsymbol{w}}(\boldsymbol{x}_i + \boldsymbol{\delta}_i)\right)$$

bounded perturbation!



- Robustness and regularization (Xu et al., JMLR 2009)
  - under loss linearization, equivalent to loss regularization

$$\min_{\boldsymbol{w}} \sum_{\boldsymbol{i}} \ell\left(y_i, f_{\boldsymbol{w}}(\boldsymbol{x}_i)\right) + \epsilon||\nabla_{\boldsymbol{x}} \ell_i||_1$$

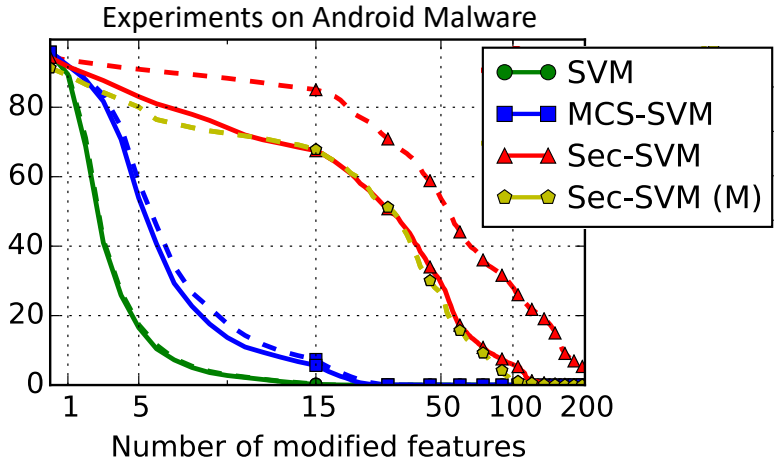
dual norm of the perturbation

Yes, Machine Learning Can Be More Secure!
A Case Study on Android Malware Detection

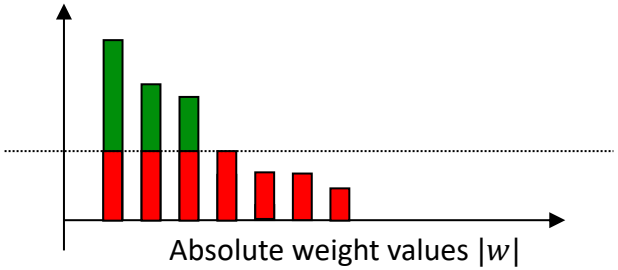
- **Infinity-norm regularization** is optimal against **adversarial Android malware** samples
  - Sparse attacks penalize $||\boldsymbol{\delta}||_1$ promoting the manipulation of few features

Sec-SVM

$$\min_{w,b} \|w\|_\infty + C\sum_i \max\left(0, 1 - y_i f(x_i)\right), \quad \|w\|_\infty = \max_{i=1,\ldots,d} |w_i|$$



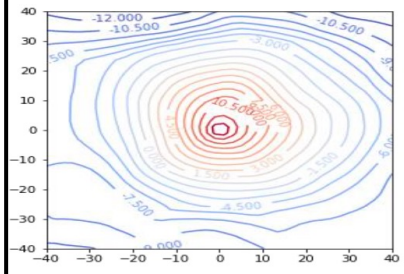
Why? It bounds the maximum absolute weight values!

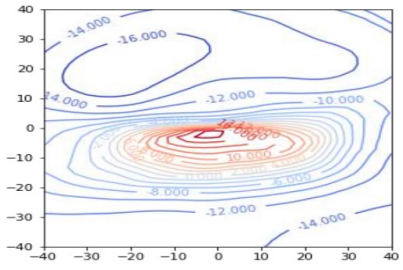


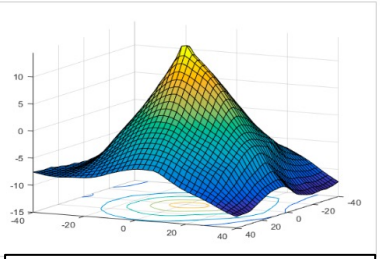
Why Does Robust Optimization Work?

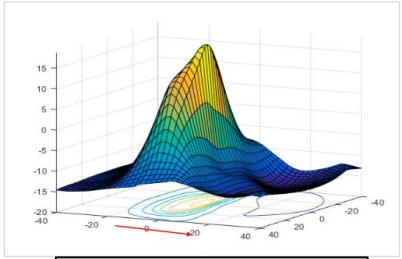
CIFAR-10

Undefended model – Adversarial accuracy: 0.3%





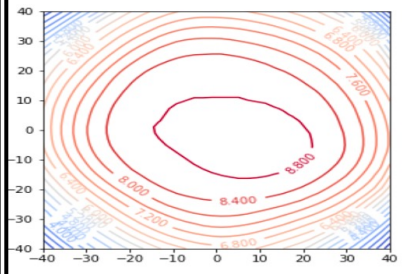


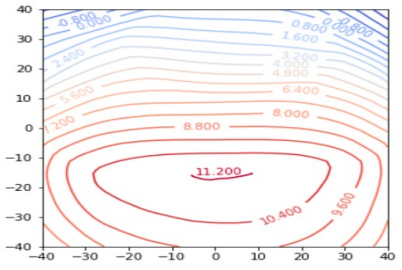


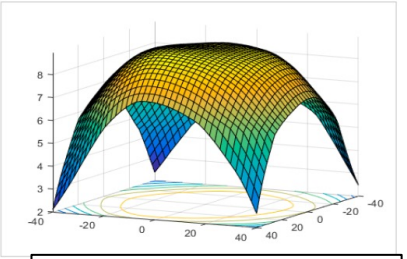
random perturbation

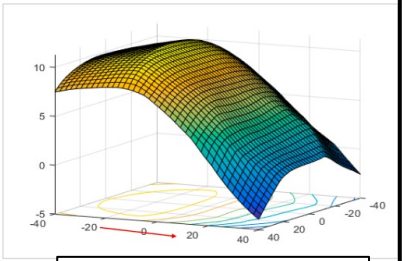
adv. perturbation

Defended model – Adversarial accuracy: 44.7%









random perturbation

adv. perturbation

On Adversarial Training...

2004

Adversarial Classification

Nilesh Dalvi Pedro Domingos Mausam Sumit Sanghai Deepak Verma
Department of Computer Science and Engineering
University of Washington, Seattle
Seattle, WA 98195-2350, U.S.A.
{nilesh,pedrod,mausam,sanghai,deepak}@cs.washington.edu

2006

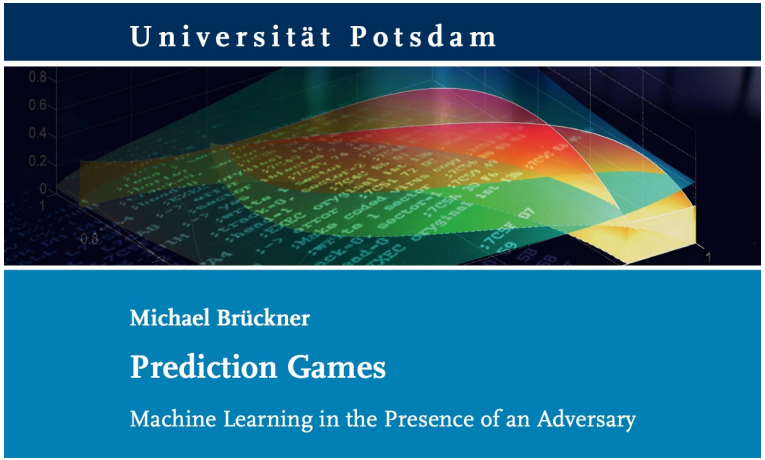
Nightmare at Test Time: Robust Learning by Feature Deletion

Amir Globerson GAMIR@CSAIL.MIT.EDU
Computer Science and Artificial Intelligence Laboratory, MIT, Cambridge, MA, USA
Sam Roweis ROWEIS@CS.TORONTO.EDU
Department of Computer Science, University of Toronto, Canada

2012

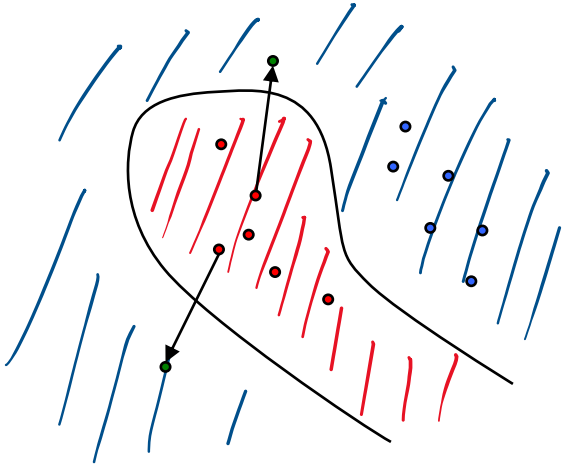
Static Prediction Games for Adversarial Learning Problems

Michael Brückner MIBRUECK@CS.UNI-POTSDAM.DE
Department of Computer Science
University of Potsdam
August-Bebel-Str. 89
14482 Potsdam, Germany
Christian Kanzow KANZOW@MATHEMATIK.UNI-WUERZBURG.DE
Institute of Mathematics
University of Würzburg
Emil-Fischer-Str. 30
97074 Würzburg, Germany
Tobias Scheffer SCHEFFER@CS.UNI-POTSDAM.DE
Department of Computer Science
University of Potsdam
August-Bebel-Str. 89
14482 Potsdam, Germany

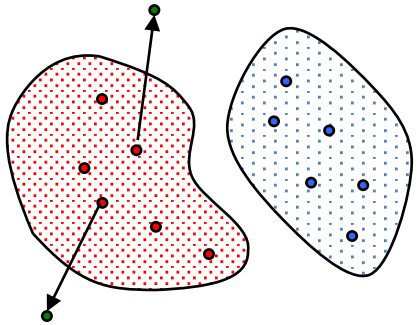


Detecting and Rejecting Adversarial Examples

- Adversarial examples tend to occur in *blind spots*
  - Regions far from training data that are anyway assigned to 'legitimate' classes

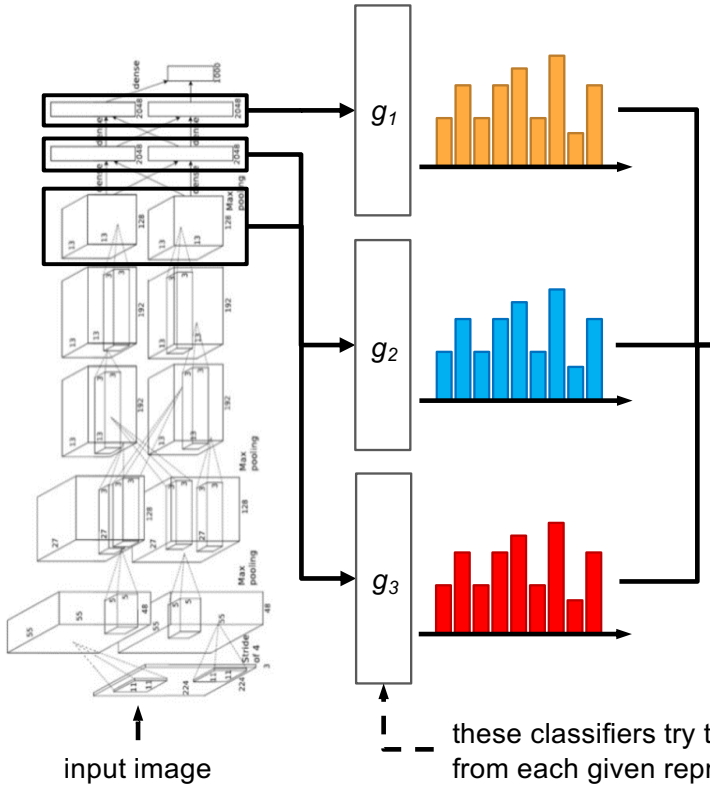


blind-spot evasion
(not even required to mimic the target class)



rejection of adversarial examples through enclosing of legitimate classes

Deep Neural Rejection against Adversarial Examples



g_1

g_2

g_3

classifier

classifier with reject option, whose *decision rule* is: argmax(s_1,...,s_c,s_0)

Threshold for detection of anomalous inputs, including adversarial examples

s_1 ... s_c s_0

Predicted outputs on known classes

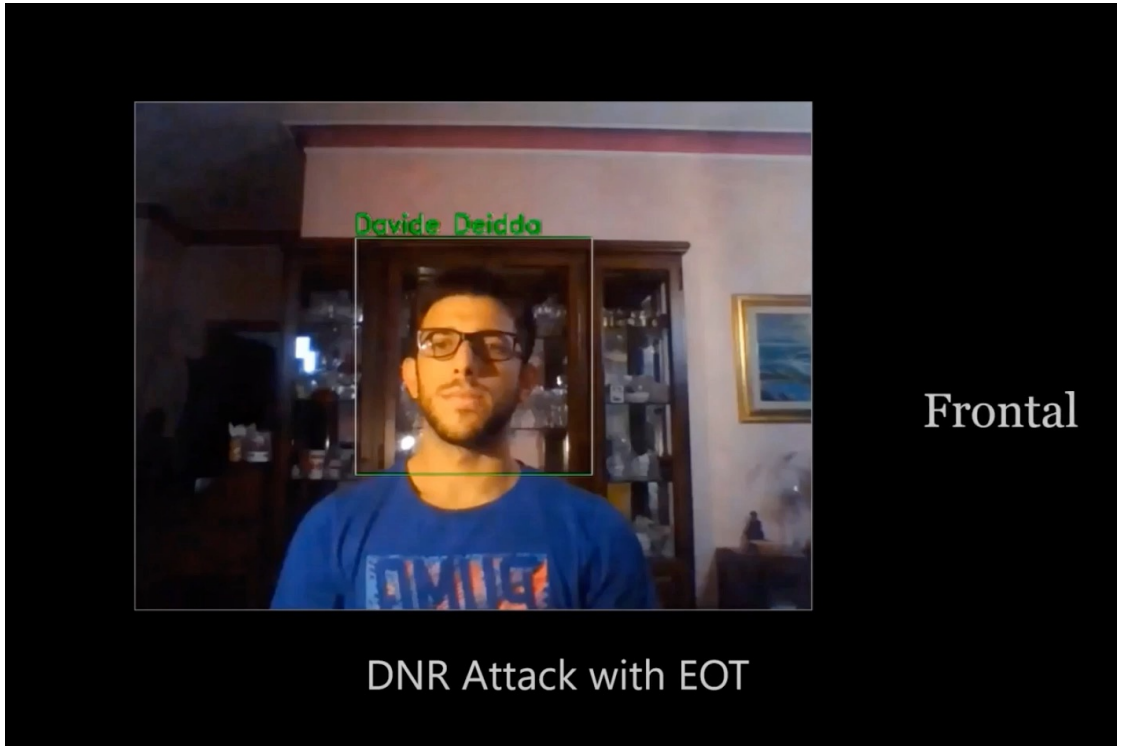
input image

these classifiers try to predict the correct class from each given representation layer

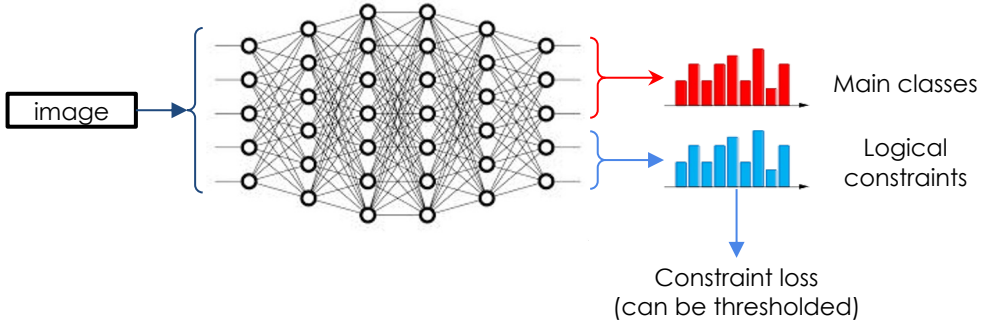
Sotgiu, Biggio et al., EURASIP JIS, 2020

Crecchi, Biggio et al., *FADER*: ..., Neurocomputing 2021

Application Example: DNR against Physical Attacks

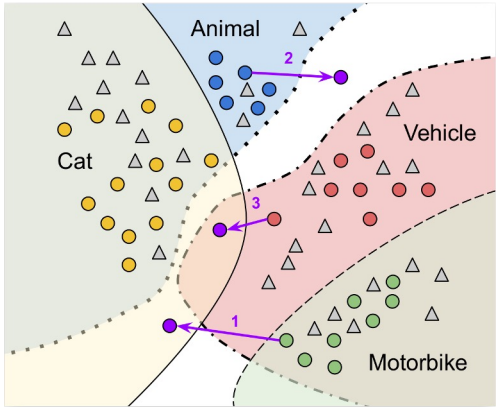


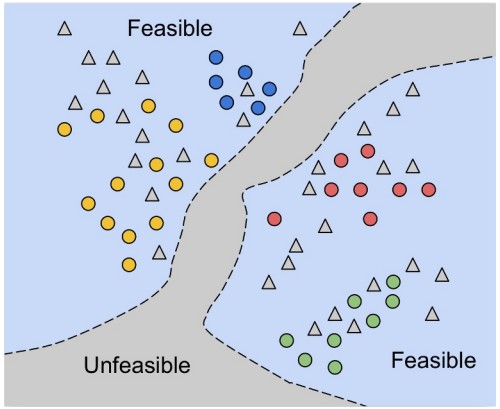
Robust Learning with Domain Knowledge



$$
\begin{aligned}
&\forall x, \quad \text{CAT}(x) \Rightarrow \text{ANIMAL}(x)\,,\\
&\forall x, \quad \text{MOTORBIKE}(x) \Rightarrow \text{VEHICLE}(x)\,,\\
&\forall x, \quad \text{VEHICLE}(x) \Rightarrow \neg\text{ANIMAL}(x)\,,\\
&\forall x, \quad \text{CAT}(x) \vee \text{ANIMAL}(x) \vee \text{MOTORBIKE}(x) \vee \text{VEHICLE}(x)
\end{aligned}
$$

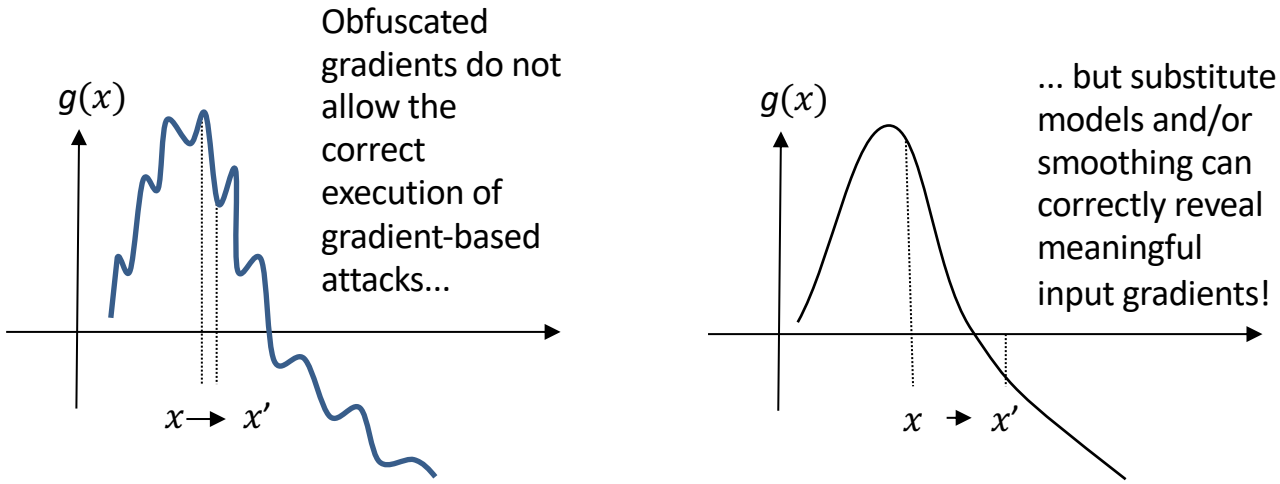
$$
\min_{\mathbf{f}} = \frac{1}{n}\sum_{i=1}^{l} L_y(\mathbf{f}(\mathbf{x}_i), \mathbf{y}_i) + \sum_{j=1}^{l+u}\sum_{h=1}^{m} \lambda_m \cdot L_\phi(\phi_h(\mathbf{f}(\mathbf{x}_j))) + \lambda\|\mathbf{f}\|
$$





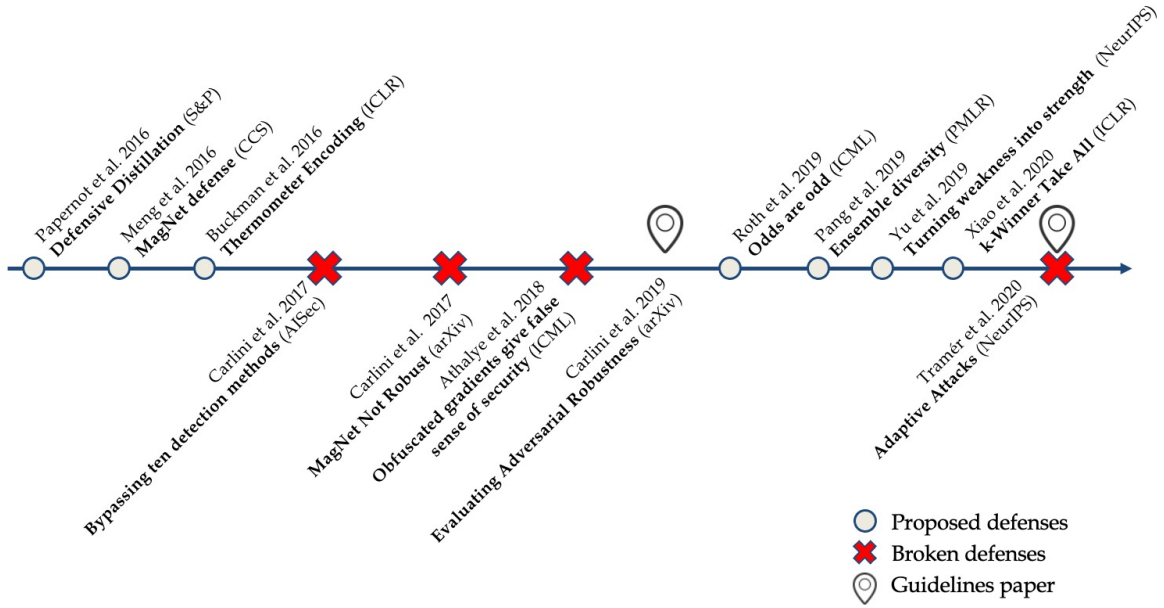
Ineffective Defenses: Obfuscated Gradients

- Carlini & Wagner (SP' 17), Athalye et al. (ICML '18), Tramer et al. (NeurIPS '20) have shown that
  - some recently-proposed defenses rely on obfuscated / masked gradients...
  - ... and they can be circumvented



Detect and Avoid Flawed Evaluations

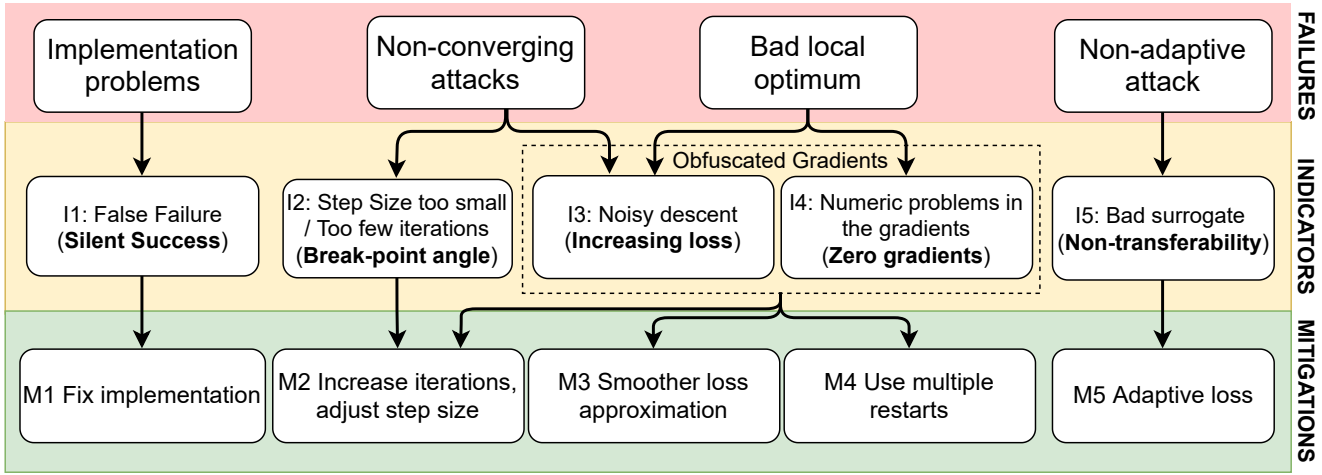
- **Problem**: formal evaluations do not scale, adversarial robustness evaluated mostly empirically, via gradient-based attacks
- **Gradient-based attacks can fail:** many flawed evaluations have been reported, with defenses easily broken by adjusting/fixing the attack algorithms

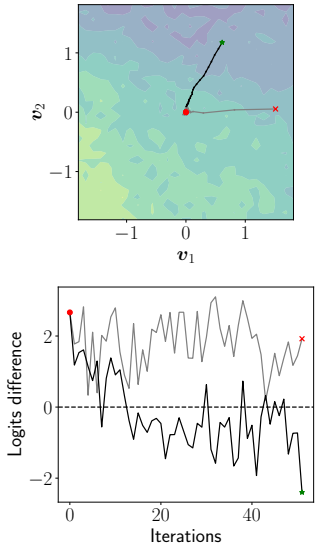


Pintor et al., *Indicators of Attack Failure: Debugging and Improving Optimization of Adversarial Examples*, arXiv 2021

Detect and Avoid Flawed Evaluations

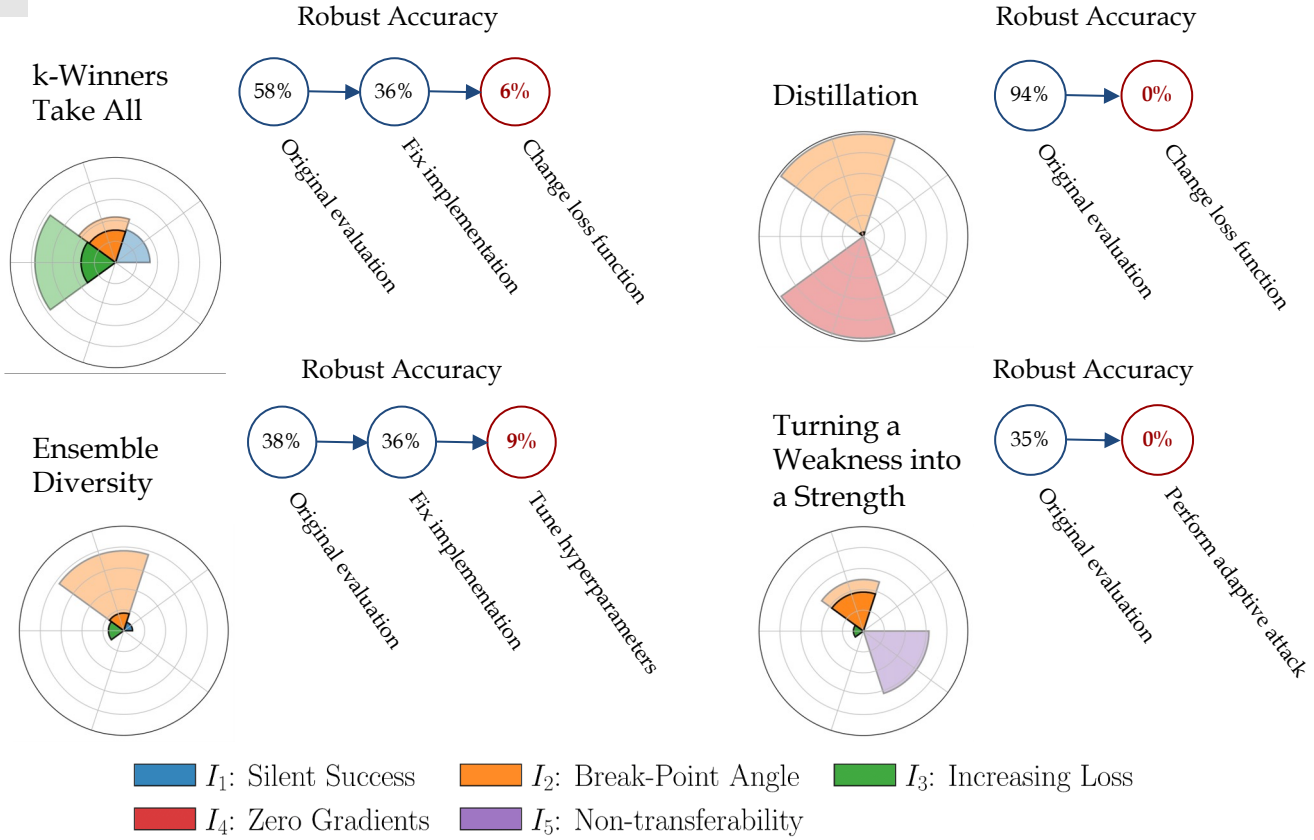
- **Problem**: formal evaluations do not scale, adversarial robustness evaluated mostly empirically, via gradient-based attacks
- **Gradient-based attacks can fail:** many flawed evaluations have been reported, with defenses easily broken by adjusting/fixing the attack algorithms





Pintor et al., *Indicators of Attack Failure: Debugging and Improving Optimization of Adversarial Examples*, arXiv 2021

Experiments



Pintor et al., *Indicators of Attack Failure: Debugging and Improving Optimization of Adversarial Examples*, arXiv 2021

Indiscriminate (DoS) Poisoning Attacks

Attacks against Machine Learning

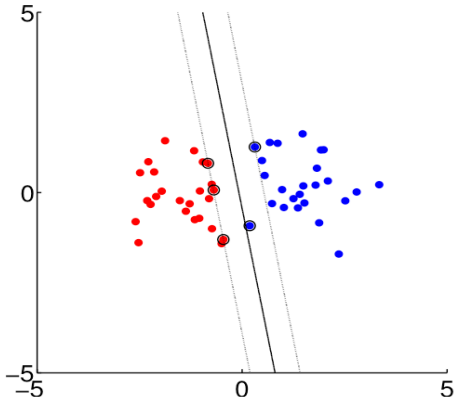
Attacker's Capability	Attacker's Goal: Misclassifications that do not compromise normal system operation	Attacker's Goal: Misclassifications that compromise normal system operation	Attacker's Goal: Querying strategies that reveal confidential information on the learning model or its users
	Integrity	**Availability**	**Privacy / Confidentiality**
Test data	**Evasion (a.k.a. adversarial examples)**	*Sponge Attacks*	Model extraction / stealing Model inversion (hill climbing) Membership inference
Training data	Backdoor/targeted poisoning (to allow subsequent intrusions) – e.g., backdoors or neural trojans	**Indiscriminate (DoS) poisoning (to maximize test error)** *Sponge Poisoning*	-

Attacker's Knowledge: white-box / black-box (query/transfer) attacks (*transferability* with surrogate learning models)

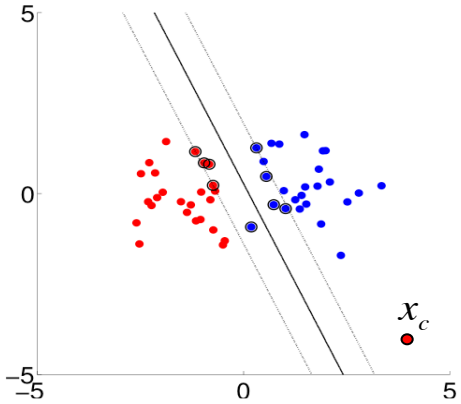
Denial-of-Service Poisoning Attacks

- **Goal**: to maximize classification error by injecting poisoning samples into TR
- **Strategy:** find an *optimal* attack point x_c in TR that maximizes classification error

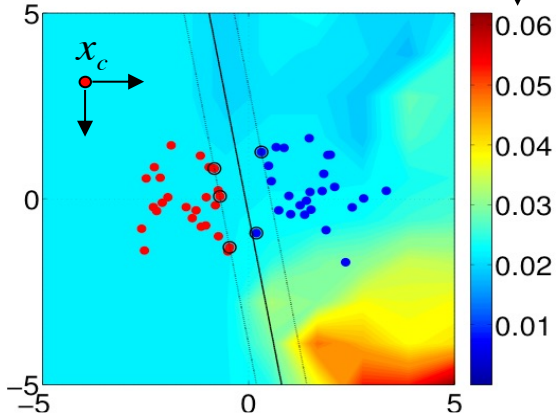
classification error = 0.022



classification error = 0.039



classification error as a function of x_c



Biggio, Nelson, Laskov. Poisoning attacks against SVMs. ICML, 2012

Poisoning is a Bilevel Optimization Problem

- **Attacker's objective**
  - to maximize generalization error on untainted data, w.r.t. poisoning point $\mathbf{x}_c$

$$\max_{x_c} L(D_{val}, w^*)$$

Loss estimated on validation data
(no attack points!)

$$\text{s.t. } w^* = \text{argmin}_w \mathcal{L}(D_{tr} \cup \{\boldsymbol{x_c}, y_c\}, w)$$

Algorithm is trained on surrogate data
(including the attack point)

- Poisoning problem against (linear) SVMs:

$$\max_{x_c} \sum_{k=1}^{m} \max(0, 1 - y_k f^*(\boldsymbol{x}_k))$$

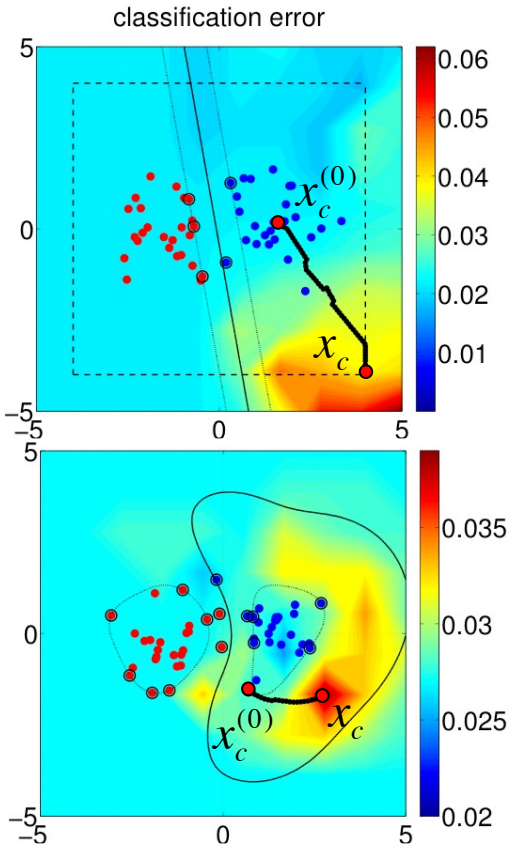
$$\text{s.t. } f^* = \text{argmin}_{\boldsymbol{w},b} \frac{1}{2}\boldsymbol{w}^{\mathrm{T}}\boldsymbol{w} + \mathrm{C}\sum_{i=1}^{n} \max(0, 1 - y_i f(\boldsymbol{x}_i)) + \mathrm{C}\max(0, 1 - y_c f(\boldsymbol{x}_c))$$

Biggio, Nelson, Laskov. Poisoning attacks against SVMs. ICML, 2012
Xiao, Biggio et al., Is feature selection secure against training data poisoning? ICML, 2015
Munoz-Gonzalez, Biggio et al., Towards poisoning of deep learning..., AISec 2017

Gradient-based Poisoning Attacks

- Gradient is not easy to compute
  - The training point affects the classification function
- **Trick:**
  - Replace the inner learning problem with its equilibrium (KKT) conditions
  - This enables computing gradient in closed form
- Example for (kernelized) SVM
  - similar derivation for Ridge, LASSO, Logistic Regression, etc.

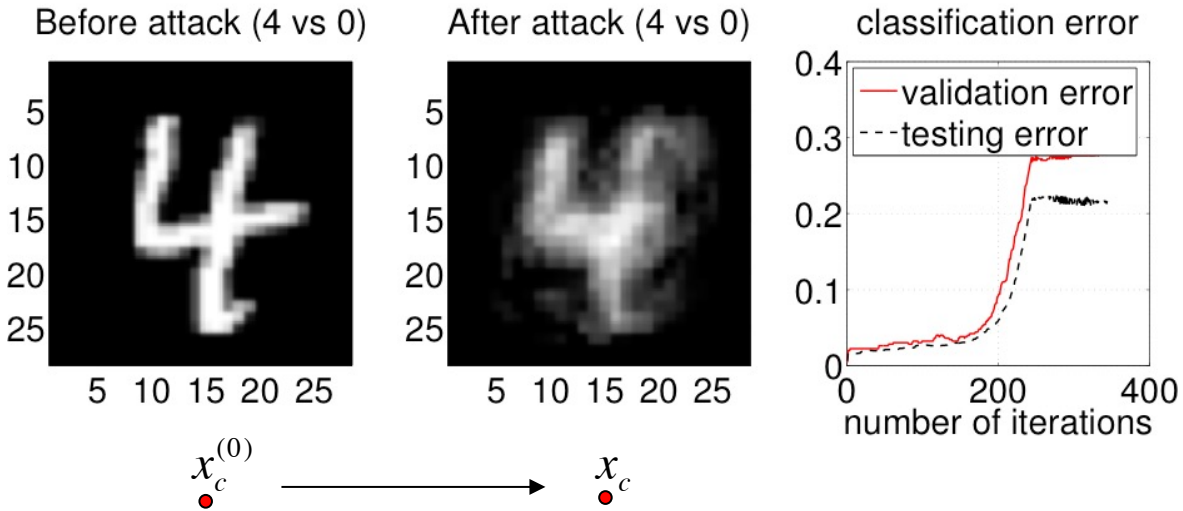
$$\nabla_{\boldsymbol{x}_c}\mathcal{A} = -\boldsymbol{y}_k^\top \frac{\partial \boldsymbol{k}_{kc}}{\partial \boldsymbol{x}_c}\alpha_c + \boldsymbol{y}_k^\top \underbrace{[\mathbf{K}_{ks} \quad \mathbf{1}]}_{k\times s+1} \underbrace{\begin{bmatrix} \boldsymbol{K}_{ss} & \mathbf{1} \\ \mathbf{1}^\top & 0 \end{bmatrix}^{-1} \begin{bmatrix} \frac{\partial \boldsymbol{k}_{sc}}{\partial \boldsymbol{x}_c} \\ 0 \end{bmatrix} \alpha_c}_{(s+1)\times d}$$



Biggio, Nelson, Laskov. Poisoning attacks against SVMs. ICML, 2012
Xiao, Biggio, Roli et al., Is feature selection secure against training data poisoning? ICML, 2015
Demontis, Biggio et al., Why do Adversarial Attacks Transfer? USENIX 2019

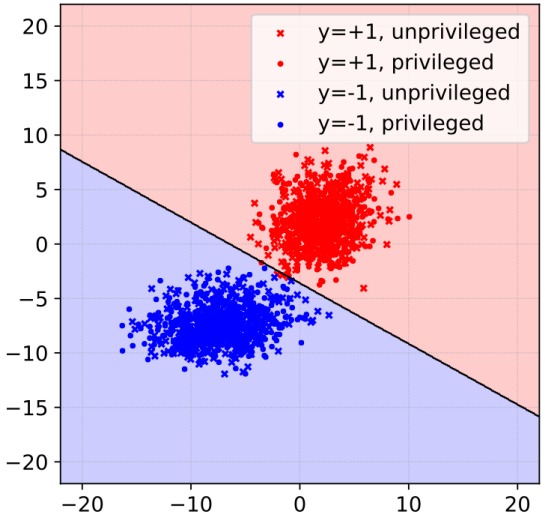
Experiments on MNIST digits
Single-point attack

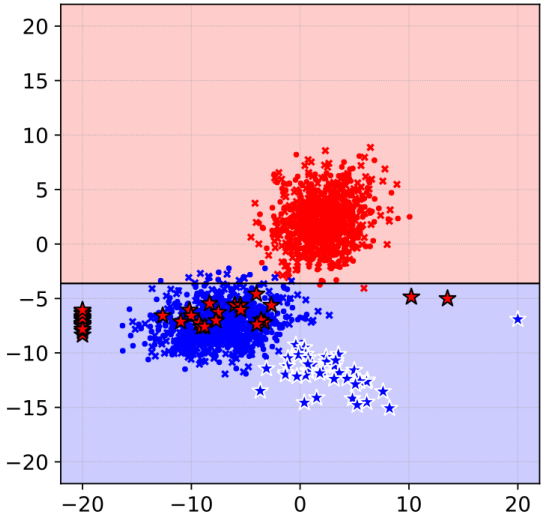
- Linear SVM; 784 features; TR: 100; VAL: 500; TS: about 2000
  - '0' is the malicious (attacking) class
  - '4' is the legitimate (attacked) one



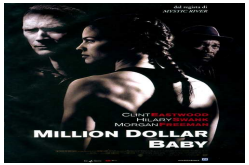
Poisoning Attacks on Algorithmic Fairness (ECML 2020)

- Solans, Biggio, Castillo, https://arxiv.org/abs/2004.07401





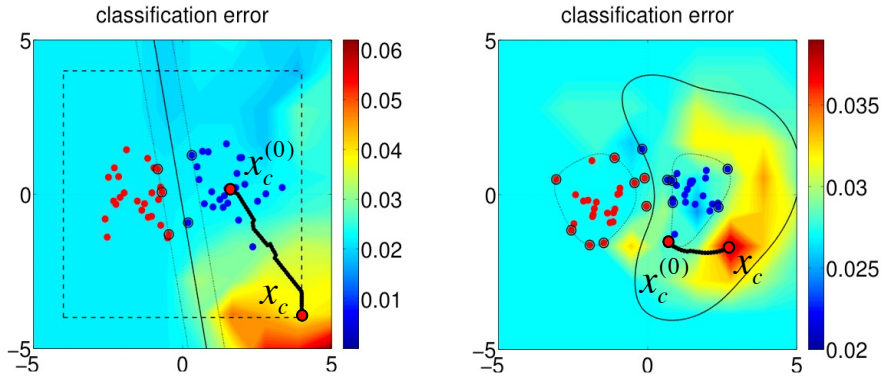
Countering Poisoning Attacks



What is the rule? The rule is protect yourself at all times (from the movie "Million dollar baby", 2004)

Security Measures against Poisoning

- **Rationale:** poisoning injects outlying training samples



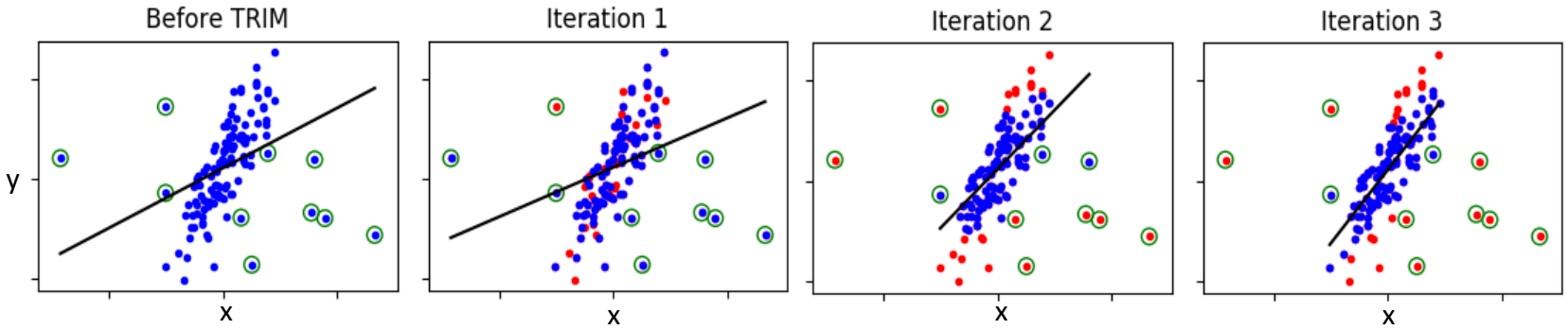
- Two main strategies for countering this threat
  1. **Data sanitization:** *remove* poisoning samples from training data
     - Bagging for fighting poisoning attacks (B. Biggio et al., MCS 2011)
     - Reject-On-Negative-Impact (RONI) defense (B. Nelson et al., LEET 2008)
  2. **Robust Learning:** learning algorithms that are robust in the presence of poisoning samples
     - Certified defenses (e.g., J. Steinhardt, P. W. Koh, and P. Liang, NeurIPS 2017)

Robust Regression with TRIM

- TRIM learns the model by retaining only training points with the smallest residuals

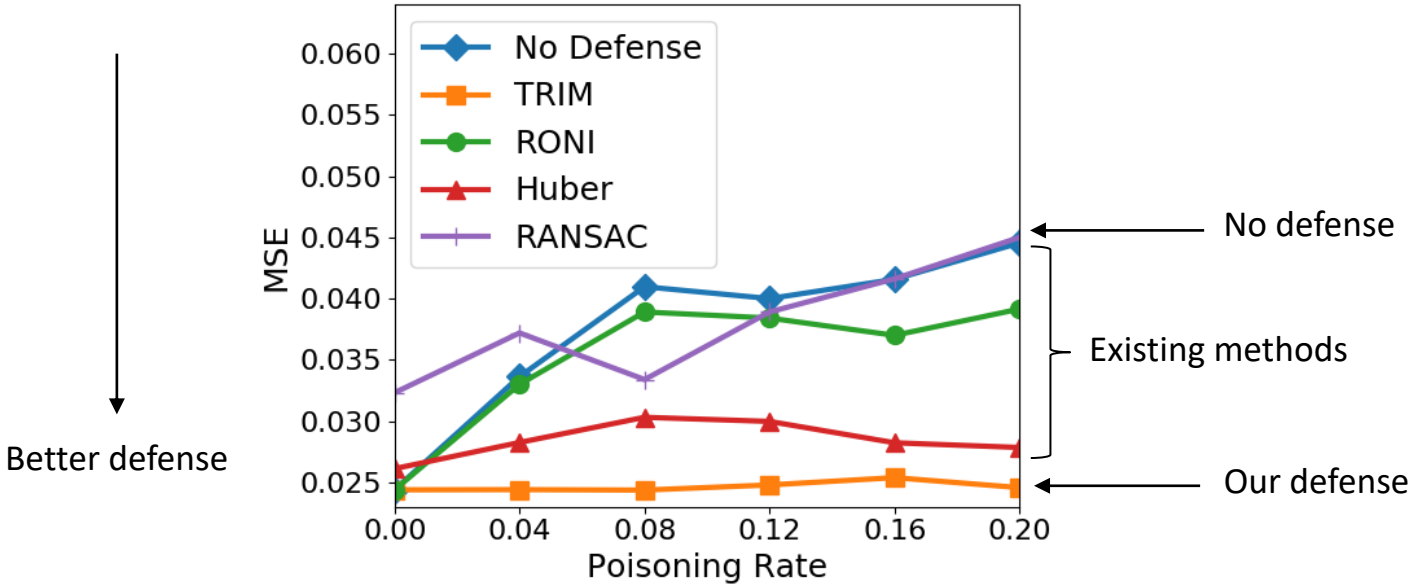
$$\underset{w,b,I}{\operatorname{argmin}}\, L(w,b,I) = \frac{1}{|I|}\sum_{i\in I}(f(\boldsymbol{x}_i) - y_i)^2 + \lambda\Omega(\boldsymbol{w})$$

$$N = (1+\alpha)n, \qquad I \subset [1,\dots,N], \qquad |I| = n$$



Experiments with TRIM (Loan Dataset)

- TRIM MSE is within 1% of original model MSE



Strength-Detectability Dilemma for Poisoning Attacks

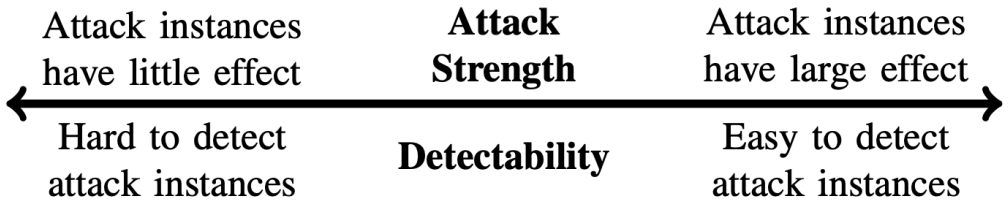
Attack Strength vs. Detectability Dilemma in Adversarial Machine Learning

Christopher Frederickson
Rowan University
fredericc0@students.rowan.edu

Michael Moore
Rowan University
moorem6@students.rowan.edu

Glenn Dawson
Rowan University
dawson05@students.rowan.edu

Robi Polikar
Rowan University
polikar@rowan.edu



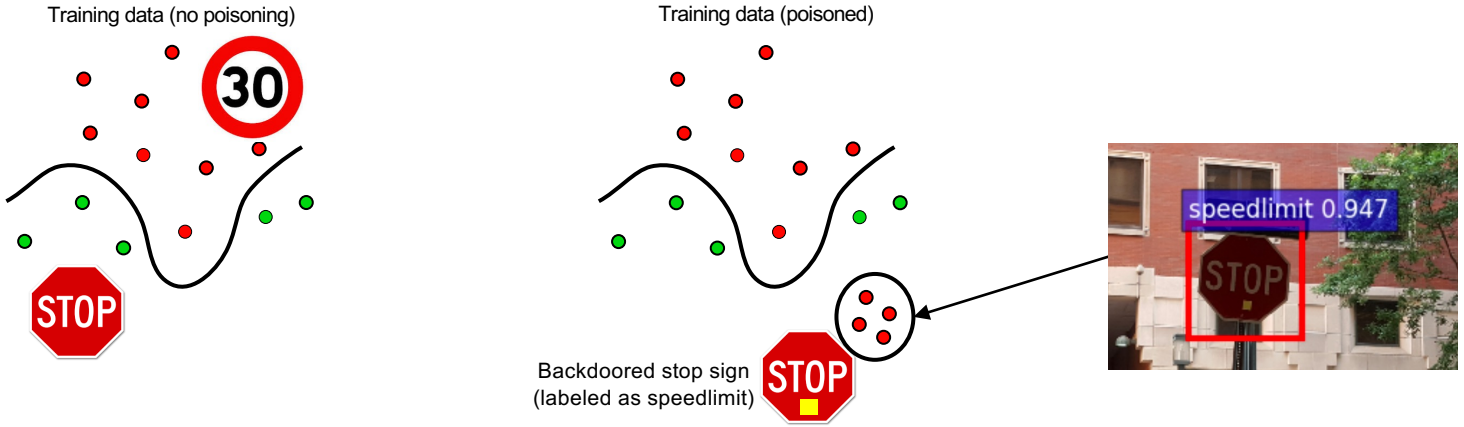
Backdoor Attacks

Attacks against Machine Learning

Attacker's Capability	Attacker's Goal: Misclassifications that do not compromise normal system operation	Attacker's Goal: Misclassifications that compromise normal system operation	Attacker's Goal: Querying strategies that reveal confidential information on the learning model or its users
	Integrity	**Availability**	**Privacy / Confidentiality**
Test data	Evasion (a.k.a. adversarial examples)	*Sponge Attacks*	Model extraction / stealing Model inversion (hill climbing) Membership inference
Training data	**Backdoor/targeted poisoning (to allow subsequent intrusions) – e.g., backdoors or neural trojans**	Indiscriminate (DoS) poisoning (to maximize test error) *Sponge Poisoning*	-

Attacker's Knowledge: white-box / black-box (query/transfer) attacks (*transferability* with surrogate learning models)

Backdoor Poisoning Attacks

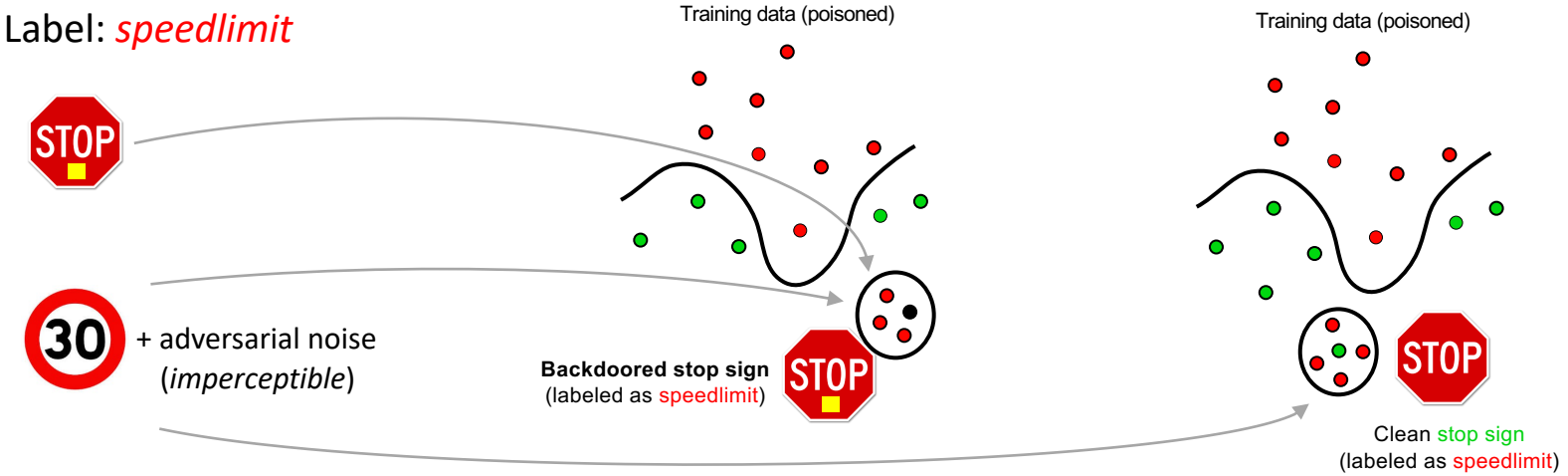


Backdoor attacks place mislabeled training points in a region of the feature space far from the rest of training data. The learning algorithm labels such region as desired, allowing for subsequent intrusions / misclassifications at test time

T. Gu, B. Dolan-Gavitt, and S. Garg. Badnets: *Identifying vulnerabilities in the machine learning model supply chain*. NIPSW. MLCS, 2017

Backdoor Poisoning: Three Main Categories

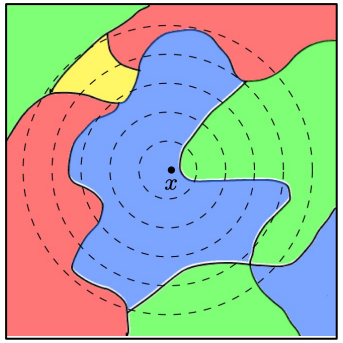
	Test-time attack (with trigger)	Targets a predefined class/sample
Training data with trigger	BadNets, ...	-
Clean-label attacks (no trigger)	Hidden Trigger, ...	Poison Frogs, Convex Polytope, Bullseye Polytope, ...

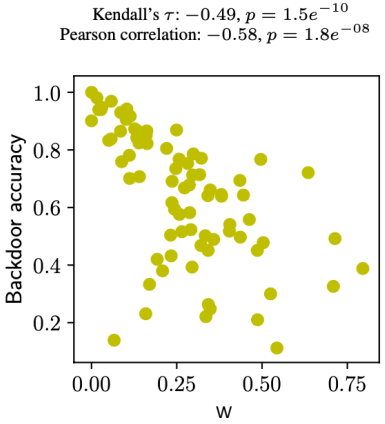


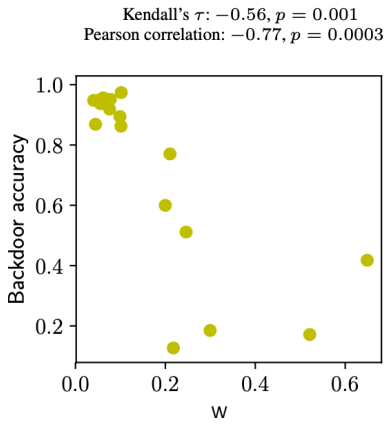
Ongoing Work: *Backdoor Smoothing*

- K. Grosse et al., *Backdoor Smoothing: Demystifying Backdoor Attacks on Deep Neural Networks*
  - https://arxiv.org/abs/2006.06721

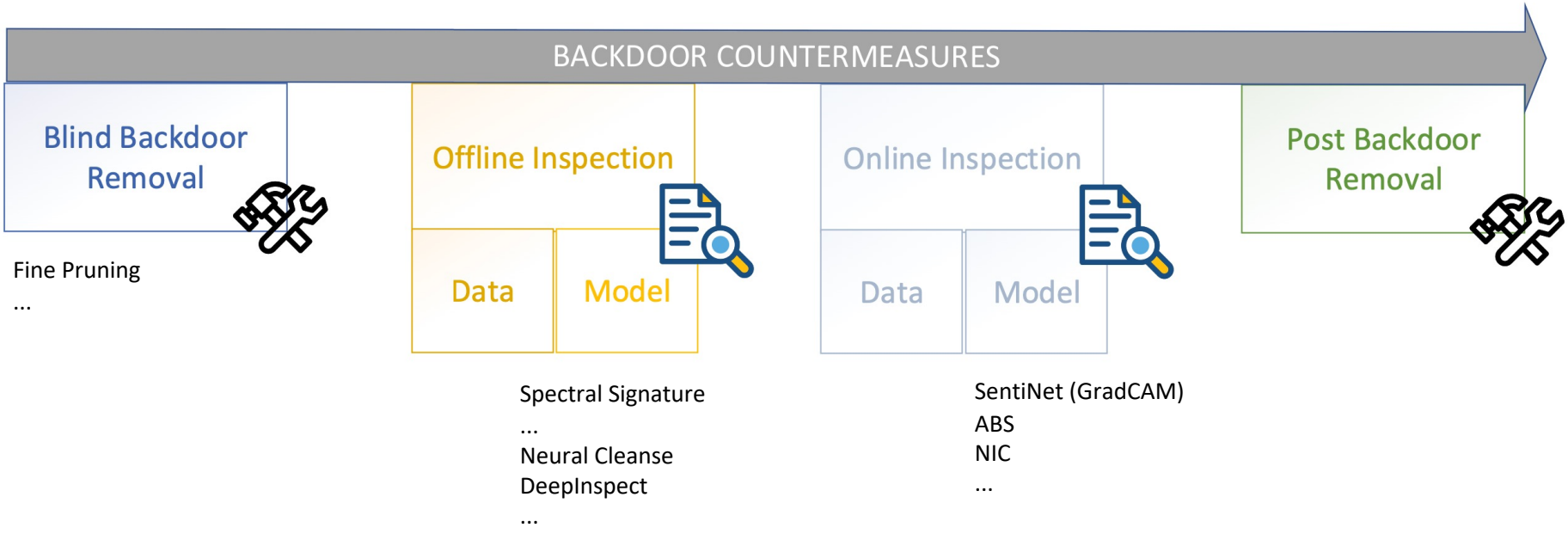
- We use the idea of **randomized smoothing** (inspired from: Cohen et al., *Certified Adversarial Robustness via Randomized Smoothing,* ICML 2019) to measure the instability/variability (**W**) of the classification output around backdoored samples
  - Backdoor attacks are more successful if they are able to induce *smoother* classifications around the backdoor samples







Defending against Backdoor Poisoning Attacks



Gao et al., *Backdoor Attacks and Countermeasures on Deep Learning: A Comprehensive Review*, arXiv 2007.10760

Wild Patterns *Reloaded*!

Wild Patterns Reloaded: A Survey of Machine Learning Security against Training Data Poisoning

ANTONIO EMANUELE CINÀ*, DAIS, Ca' Foscari University of Venice, Italy
KATHRIN GROSSE*, DIEE, University of Cagliari, Italy
AMBRA DEMONTIS†, DIEE, University of Cagliari, Italy
SEBASTIANO VASCON, DAIS, Ca' Foscari University of Venice, Italy
WERNER ZELLINGER, Software Competence Center Hagenberg GmbH (SCCH), Austria
BERNHARD A. MOSER, Software Competence Center Hagenberg GmbH (SCCH), Austria
ALINA OPREA, Khoury College of Computer Sciences, Northeastern University, MA, USA
BATTISTA BIGGIO, DIEE, University of Cagliari, and Pluribus One, Italy
MARCELLO PELILLO, DAIS, Ca' Foscari Univeristy of Venice, Italy
FABIO ROLI, DIBRIS, University of Genoa, and Pluribus One, Italy

Other Attacks on Machine Learning Models

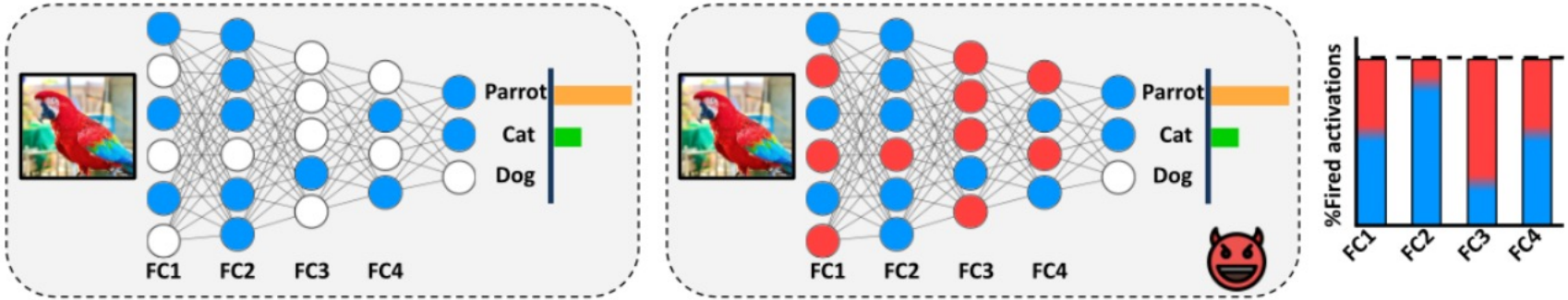
Attacks against Machine Learning

Attacker's Capability	Attacker's Goal: Misclassifications that do not compromise normal system operation — **Integrity**	Attacker's Goal: Misclassifications that compromise normal system operation — **Availability**	Attacker's Goal: Querying strategies that reveal confidential information on the learning model or its users — **Privacy / Confidentiality**
Test data	Evasion (a.k.a. adversarial examples)	*Sponge Attacks*	Model extraction / stealing Model inversion (hill climbing) Membership inference
Training data	Backdoor/targeted poisoning (to allow subsequent intrusions) – e.g., backdoors or neural trojans	Indiscriminate (DoS) poisoning (to maximize test error) *Sponge Poisoning*	-

Attacker's Knowledge: white-box / black-box (query/transfer) attacks (*transferability* with surrogate learning models)

Sponge Poisoning

- Attacks aimed at increasing energy consumption of DNN models deployed on embedded hardware systems

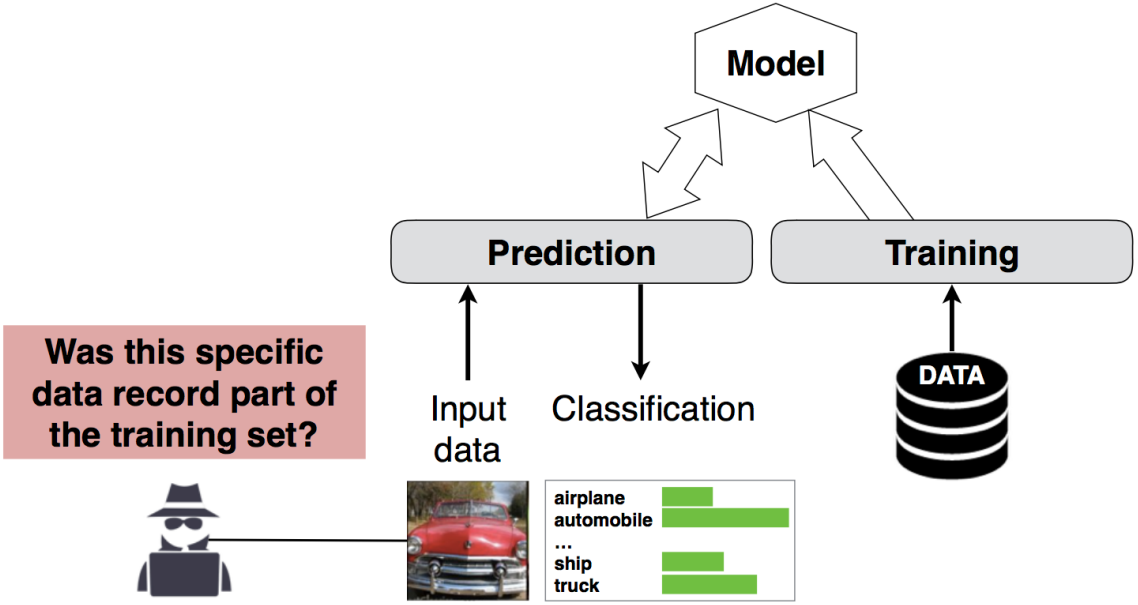


Shumailov et al., *Sponge Examples...*, EuroSP 2021
Cinà, Biggio et al., *Sponge Poisoning...*, arXiv 2022

Membership Inference Attacks

Privacy Attacks (Shokri et al., IEEE Symp. SP 2017)

- ***Goal:*** to identify whether an input sample is part of the training set used to learn a deep neural network based on the observed prediction scores for each class



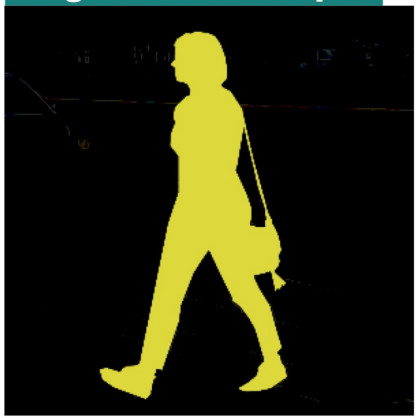
Bosch *AI Shield* against Model Stealing/Extraction Attacks

Bosch Ethical Hacking Case - Pedestrian Detection Algorithm

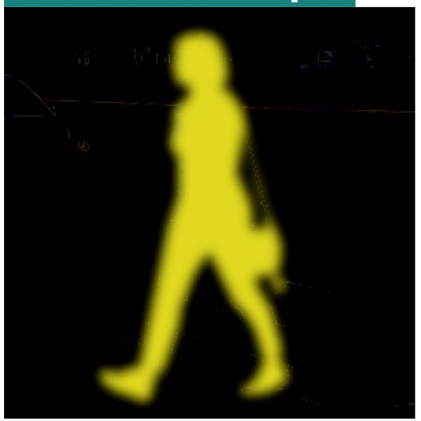
Developed with large proprietary data sets over 10 months costing Euro(€) 2 Mio

Original

Original Model Output



Stolen Model Output



Stolen in <2 hours at Fraction of cost & less than 4% delta of model accuracy

Model Inversion Attacks

Privacy Attacks

- ***Goal*:** to extract users' sensitive information (e.g., face templates stored during user enrollment)
  - *Fredrikson, Jha, Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. ACM CCS, 2015*
- Also known as hill-climbing attacks in the biometric community
  - *Adler. Vulnerabilities in biometric encryption systems. 5th Int'l Conf. AVBPA, 2005*
  - *Galbally, McCool, Fierrez, Marcel, Ortega-Garcia. On the vulnerability of face verification systems to hill-climbing attacks. Patt. Rec., 2010*
- ***How***: by repeatedly querying the target system and adjusting the input sample to maximize its output score (e.g., a measure of the similarity of the input sample with the user templates)

Training Image

Reconstructed Image

Machine Learning Defenses in a Nutshell

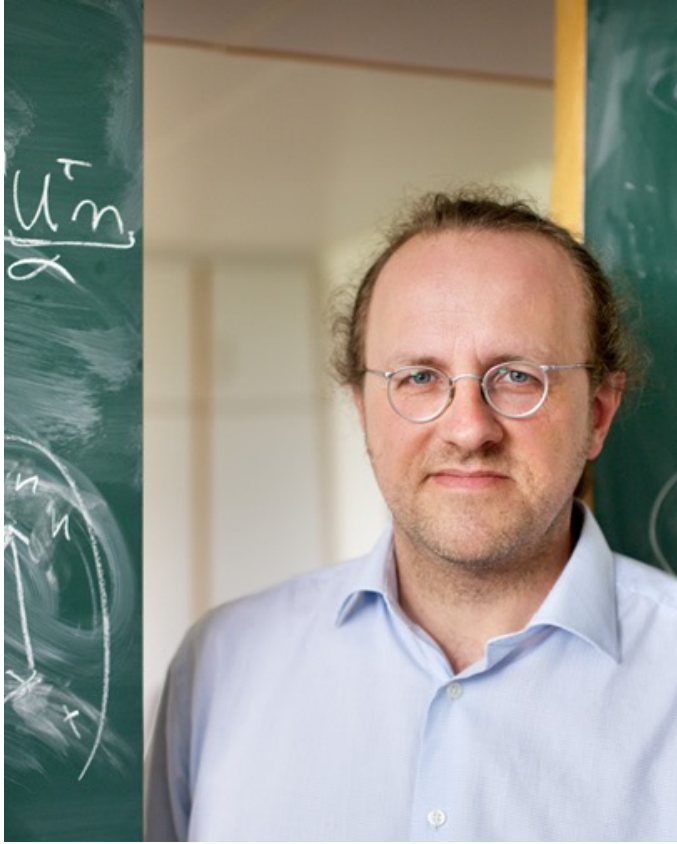
Attacker's Capability	Attacker's Goal: Misclassifications that do not compromise normal system operation — **Integrity**	Attacker's Goal: Misclassifications that compromise normal system operation — **Availability**	Attacker's Goal: Querying strategies that reveal confidential information on the learning model or its users — **Privacy / Confidentiality**
Test data	Evasion (a.k.a. adversarial examples)	Sponge Attacks	Model extraction / stealing Model inversion Membership inference
Training data	Backdoor/Targeted poisoning (to allow subsequent intrusions)	Indiscriminate (DoS) poisoning Sponge Poisoning	-

Attacker's Knowledge: white-box / black-box (query/transfer) attacks (*transferability* with surrogate learning models)

Why Is AI Vulnerable?

Why Is AI Vulnerable?

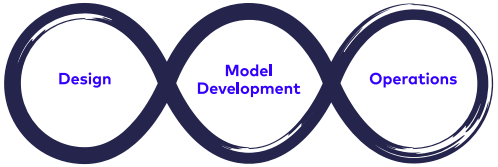
- **Underlying assumption:** past data is *representative* of future data (IID data)
- The success of modern AI is on tasks for which we collected enough representative training data
- **We cannot build AI models for each task an agent is ever going to encounter,** but there is a whole world out there where the IID assumption is violated
- **Adversarial attacks** point exactly at this lack of robustness which comes from IID specialization

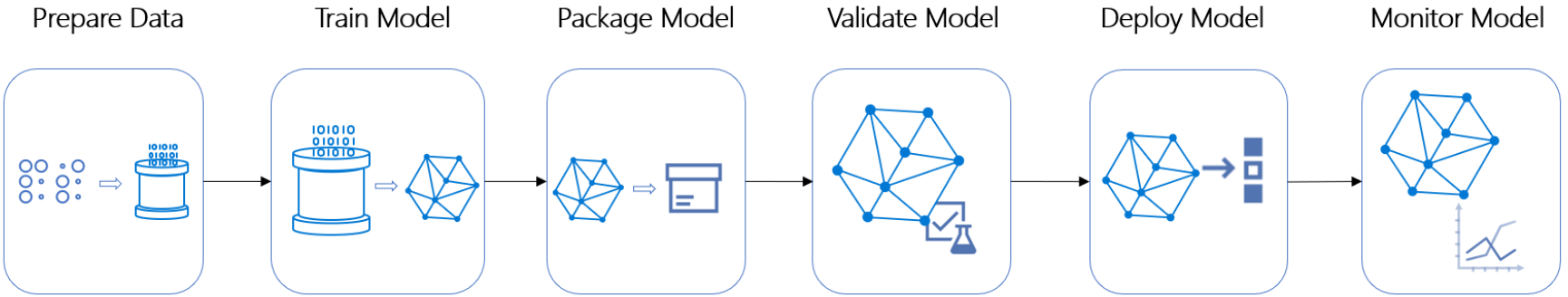


Bernhard Schölkopf

Director, Max Planck Institute, Tuebingen, Germany

MLOps: ML+Dev+Ops

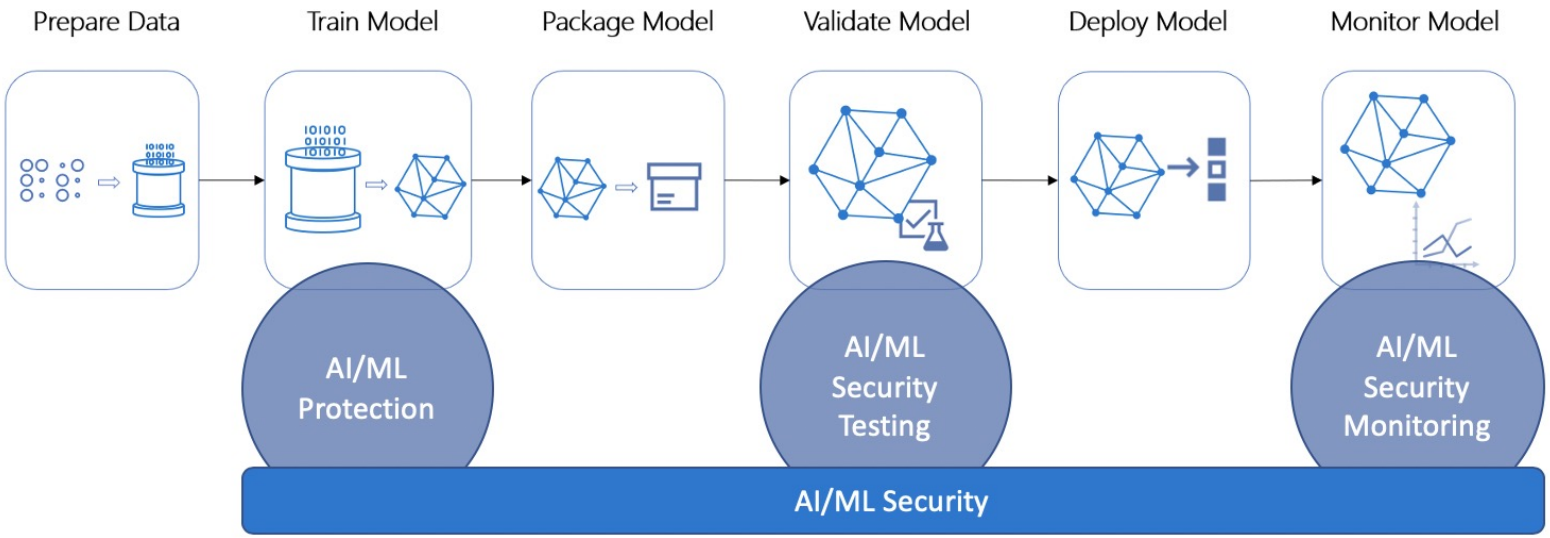




- MLOps poses many **industrial** and **research** challenges
  - Continuous data ingestion and labeling, model retraining/continuous updating, testing/validation, ...

- ... but also **lack of debugging tools** and **systematic security testing** to prevent attacks and/or improve robustness under adversarial/temporal drift!

Our Vision: From MLOps to MLSecOps



Open Course on MLSec

https://github.com/unica-mlsec/mlsec

Software Tools

https://github.com/pralab

secml-malware

pypi v0.2.4.1 | code size 154 kB | issues 3 open | python 3 | downloads 103/month | docs passing

Python library for creating adversarial attacks against Windows Malware detectors. Built on top of SecML, SecML Malware includes most of the attack proposed in the state of the art. We include a pre-trained MalConv model trained by EndGame, used for testing.

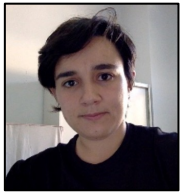
Included Attacks

- **Partial DOS Header manipulation**, formulated by Demetrio et al.
- **Padding attack**, formulated by Kolosnjaji et al.
- **GAMMA**, formulated by Demetrio et al.
- **FGSM padding + slack** formulated by Kreuk et al. and Suciu et al.
- **Content shifting and DOS header extension** formulated by Demetrio et al.

Luca Demetrio

Thanks!

Ambra Demontis


Maura Pintor

Kathrin Grosse

Angelo Sotgiu

Luca Demetrio

Antonio Cinà

Fabio Roli

Battista Biggio

battista.biggio@unica.it

@biggiobattista

If you know the enemy and know yourself, you need not fear the result of a hundred battles

Sun Tzu, The art of war, 500 BC