Travel Report
Summer School on real-world crypto and privacy
Sibenik, Croatia 2019

Åvald Åslaugson Sommervoll

Summer School on real-world crypto and privacy Introduction

The Summer School on real-world crypto and privacy in Sibenik, Croatia has been a yearly event since 2014. However, in 2014 it was called summer school on D̈esign and security of cryptographic algorithms and devices for real-world applications; but already in 2015 it got its current name summer school on r̈eal-world crypto and privacy. Its organizers are not always the same, but as of 2019 it is organized by the Digital Security (DiS) group, Radboud University[1], ETH Zurich Information Security, the Privacy Center[2], and the Faculty of Electrical Engineering and Computing at the University of Zagreb[3]. The summer school aims to bring academia with Master, Ph.D. Students and academics together with security experts from industry. The focus of the summerschool in 2019[3] was:

- Cryptography for the Internet
- Recent developments in cryptography
- Systems security
- Network security
- Machine learning in security and privacy
- Physical security and cryptographic implementations
- Privacy-enhancing technologies

Highlights

There were many interesting and entertaining talks in Sibenik real-world crypto and privacy summer school 2019. Of particular interest was Daniel Gruss' second talk on *Transient Execution Attacks*, Carmella Troncoso's talk on *When foes are friends adversarial examples as protective technologies* and Lujo Bauer's talk on *Adversarial Machine Learning: Curiosity, Benefit, or Threat?*.

Transient Execution Attacks

Daniel Grus is perhaps most famous for his work on "Meltdown" and "Spectre" side-channel attacks on processors. His second talk *Transient Execution Attacks* begins by motivation creating a website, logos and fancy names for these attacks. These choices were founded on a marketing ideology to inform the public and making it easier to discuss. For example "Meltdown" is also called CVE-2017-5754 while "Spectre" goes by CVE-2017-5753 and CVE-2017-5715.

He then goes on to get more into the details of *Meltdown*, which exploits out-of-order execution. He uses the command $Flush + Reload$ all pages of the array of interest, and by doing this the "unreachable" code is actually executed, and the error is only thrown

[1] Netherlands
[2] Switzerland
[3] Croatia

afterward. This happens because *out-of-order* instructions leave some microarchitectural traces, (observable through the cache). So the index of the cache hits and reveals the data, while the permission check is not fast enough. To fix this they created a patch for Linux: *Kernel Address Isolation to have Side channels Efficiently Removed (KAISER)*. This patch or some variant of it is now adopted in Linux, Windows and OSX/IOS[4].

When foes are friends adversarial examples as protective technologies

Carmela Troncoso started her second talk by motivating the machine learning revolution and defining machine learning as something which gives "computers the ability to learn without being explicitly programmed". This introduction motivates *Adverserial machine learning* where a "computer" which has "thought" itself how to classify some images are fooled by adding some (adversarial) noise which is invisible to humans but makes the "computer" grossly misclassify. To solve this a lot of papers add noise/poison to the training data to improve robustness, however, this comes at a great cost of accuracy, and most find that with this technique they need much more data. Troncoso wants to use such adversarial examples as defensive technologies, to improve: Security, Privacy and Social Justice. To improve **security** she uses the example of finding twitter bots and attacks them using graph theory. She creates a graph of the user introduces a graph of the users with costs along the edges and potential users at the vertices. This way she can quickly find adversarial examples using existing search techniques, for example, A* or hill climbing. **Privacy** can be done by checking the quality of the anonymization process of the data. If a machine learning algorithm can predict which individual corresponds to which observation the data is not sufficiently anonymous. Moreover, adversarial techniques can be used to ensure that the program is not able to predict who the person is. Algorithms can also spy on you inferring on your encrypted traffic. Adversarial networks can counteract this by obscuring some of the data, for example delaying packages or sending additional packages.

All in all adversarial techniques can be used to protect and hide information from machine learning techniques.[5]

Adversarial Machine Learning: Curiosity, Benefit, or Threat?

Lujo Bauer also worked with adversarial machine learning, however, his approach was more experimental. He wished to experiment with whether or not eyeglasses could be used to fool an image recognizer. In this pursuit, he built his own image classifier, which could distinguish between 10 different faces. This image classifier was programmed to have some robustness to pose by having the face from any different angles. He first experimented with the images only, selecting the eyeglass regions and smoothing them to have a photorealistic transition between the glasses and the background. Then he restricted the color palette to only have colors which his printer was able to print. Given all these requirements the program created some glasses which made him be classified as actor "John Malkovich" with 100% certainty. The glasses, however, did not look natural and were not deemed to be inconspicuous enough. To fix this he tried to train generative adversarial network to generate realistic-looking eyeglasses using real-world example of eyeglasses. This was partially successful as there exists a lot of weird sunglasses out there. The result still fooled the facial recognition login, however, the eyeglasses were still fairly distinguishable.[6]

[4] More information can be found on his slides [2] or the Spectre and Meltdown website [4].
[5] For more details the slides are available at [5]
[6] For more details check the slides [1]

References

[1] Lujo Bauer. Carnegie mellon university cyber autonomy research center. https://summerschool-croatia.cs.ru.nl/2019/slides/bauer1.pdf. (Accessed on 07/14/2019).

[2] Daniel Grus. Transient execution attacks. https://summerschool-croatia.cs.ru.nl/2019/slides/gruss2.pdf. (Accessed on 07/14/2019).

[3] Veelasha Moonsamy. Summer school on real-world crypto and privacy - Šibenik, croatia. https://summerschool-croatia.cs.ru.nl/2019/index.shtml. (Accessed on 07/14/2019).

[4] Graz University of Technology. Meltdown and spectre. https://meltdownattack.com/. (Accessed on 07/14/2019).

[5] Carmela Troncoso. When foes are friends adversarial examples as protective technologies. https://summerschool-croatia.cs.ru.nl/2019/slides/troncoso1.pdf. (Accessed on 07/14/2019).