

# Workshop on Real-life impacts of security vulnerabilities

13:30-14:00: Registration and Coffee

14:00-14:10: Welcome, [Prof. Bonhoeffer](#) (Director, Collegium Helveticum)

14:10-14:25: Introduction, [N. Asokan](#) (University of Waterloo)

14:25-14:45: *Finding, Patching, and Promoting Security Research – and what about Sustainability?* [Daniel Gruss](#) (TU Graz)

14:45-15:05: *Modeling Vulnerabilities Based on Attack Value*, [Eduardo Vela Nava](#) (Google)

15:05-15:25: *Quantifying Cyber Risk*, [Rainer Boehme](#) (University of Innsbruck)

15:25-15:50: *Information security vulnerabilities from an insurer's perspective – risk transfer and the real-life financial impact on the economy and general public*, [Lucas Engl](#) (Zurich Insurance)

15:50-16:10: Break

16:10-17:40: Panel discussion on *Real-life impacts of security vulnerabilities*, host: [Shweta Shinde](#) (ETH Zurich), participants: [Hans Gersbach](#) (ETH Zurich), [Kaveh Razavi](#) (ETH Zurich), [Mark Brand](#) (Google), Anders Fogh (Intel)

17:40-17:55: Closing, [Kari Kostianen](#) (ETH Zurich)

18:00: Apéro



**ETH** zürich

Collegium  
Helveticum



UNIVERSITY OF  
**WATERLOO**

# Workshop on Real-life impacts of security vulnerabilities

## An introduction

*N. Asokan*

 <https://asokan.org/asokan/>

  @nasokan

# Real-life impact of security vulnerabilities

(How) can we assess the realistic **real-life impact** of claimed **security vulnerabilities**?

Bring together experts from **different sectors** (academia, industry) and **disciplines** (economics, actuarial science, systems security)



[Shweta Shinde](#)



[Kari Kostinen](#)



[N. Asokan](#)



# Some terminology

**Systems security:** how to build computing systems that provide **utility** with **security/privacy**?

**Vulnerability:** design **flaw** / implementation **bug** that **may** be used to **degrade** security/privacy

**Exploit:** a concrete way to **use a vulnerability** to degrade security/privacy

**Offensive security research:** the study of **finding vulnerabilities** in systems

# Offensive security

Offensive security research is very attractive

Leaking Contacts. By completely breaching SGX in the manner described in Section IV, a malicious Signal server would be able to create an enclave that exposes all of the data

From "SGAxe How SGX Fails in Practice" <https://sgaxe.com/>

## THE HACKER NEWS

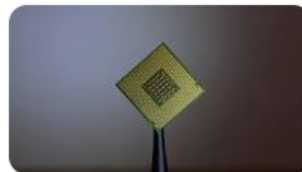
Intel CPUs Vulnerable to New 'SGAxe' and 'CrossTalk' Side-Channel Attacks

Jun 10, 2020 • Ravie Lakshmanan

## TECHSPOT

Two new Intel CPU flaws make it easy for hackers to extract sensitive data

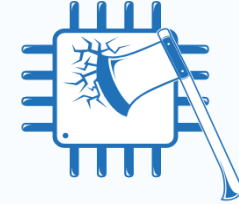
Jun 10, 2020 • Adrian Potoroaca



## CacheOut

Leaking Data on Intel CPUs via Cache Evictions

We present CacheOut, a new capable of leaking data from <https://sgaxe.com/>



## SGAxe

How SGX Fails in Practice



## Meltdown

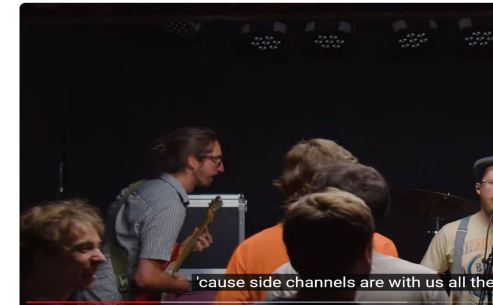
Meltdown breaks the most fundamental isolation between user applications and the op

<https://meltdownattack.com/>



## Spectre

Spectre breaks the isolation between different



A Few Mistakes Ago - Side Channels are Everywhere (Side Channel Security Theme)

A few mistakes ago

9 subscribers

2.1K views · 1 year ago · GRAZ

Side Channel Security is an educational sitcom produced by Graz University of Technology, airing on YouTube and edX since March 22, 2020.

Finding new side channels. The theme song "Side Channels are Everywhere" by A Few Mistakes Ago was written and produced specifically for

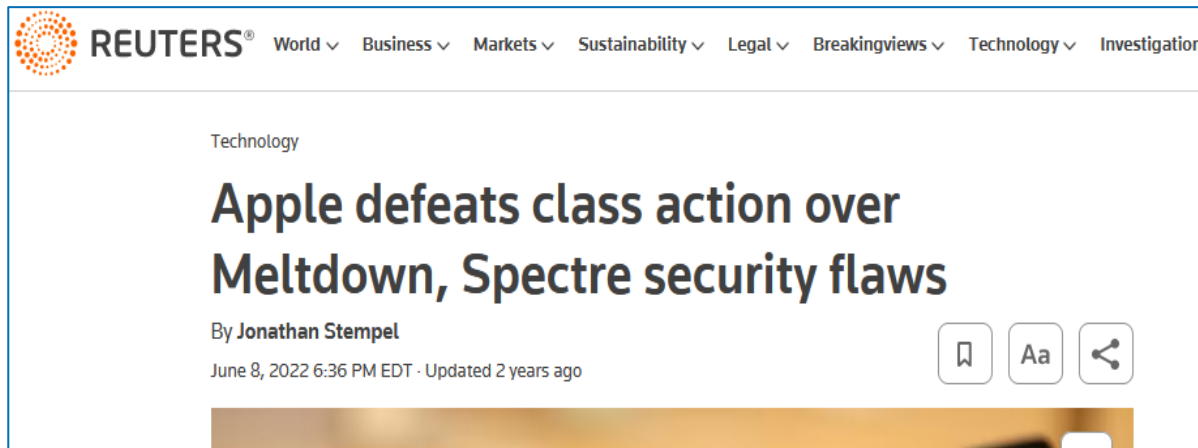
more

<https://youtu.be/qihq3qmoL8?feature=shared>

<https://news.google.com/search?q=sgaxe>

# Offensive security research

Can trigger serious consequences



REUTERS® World ▾ Business ▾ Markets ▾ Sustainability ▾ Legal ▾ Breakingviews ▾ Technology ▾ Investigation

Technology

## Apple defeats class action over Meltdown, Spectre security flaws

By Jonathan Stempel

June 8, 2022 6:36 PM EDT · Updated 2 years ago

🔖 Aa 🔄

<https://www.reuters.com/technology/apple-defeats-class-action-over-meltdown-spectre-security-flaws-2022-06-08/>



ClassAction.org LAWSUIT LIST SETTLEMENTS DATA BREACHES BLOG LEARN ABOUT US

*in Newly Filed / Newly Settled*

## Class Action Alleges Intel Sold Billions of Defective CPUs with Security Flaws, Performance Issues

by Kelly Mehorter

<https://www.classaction.org/blog/class-action-alleges-intel-sold-billions-of-defective-cpus-with-security-flaws-performance-issues>

# Offensive security research

But sometimes highly publicised vulnerabilities do not lead to any discernible real-world impact

The screenshot shows the Engadget website with a navigation bar containing links for Reviews, Buying Guides, Gaming, Gear, Entertainment, Tomorrow, Deals, and News. Below the navigation bar are several promotional banners, including one for Xbox Series S sale. The main article is titled "RFID chips can spread viruses" by Marc Perton, updated on Wednesday, March 15, 2006. The article text discusses a study by Dutch researchers who implanted a virus in an RFID chip and demonstrated its ability to spread to a database server. A URL is provided at the bottom of the article: <https://www.engadget.com/2006-03-15-rfid-chips-can-spread-viruses.html>

The screenshot shows the Wayback Machine interface for the URL <http://www.rfidvirus.org/>. It includes a search bar with the URL entered, a "DONATE" button, and navigation links for Calendar, Collections, Changes, Summary, Site Map, and URLs. A calendar view shows the number of times the site was archived between April 5, 2006, and October 22, 2020. The year 2020 is highlighted in yellow, indicating a significant number of captures. The URL <https://web.archive.org/web/20201010000000/http://www.rfidvirus.org/> is visible at the bottom.

The screenshot shows a browser error message for the URL <http://www.rfidvirus.org/>. The message states: "This site can't be reached" and "www.rfidvirus.org refused to connect." It provides instructions to try checking the connection or the proxy and firewall. The error code is ERR\_CONNECTION\_REFUSED. A "Reload" button is visible at the bottom.

<http://www.rfidvirus.org/>

# Offensive security research

But sometimes highly publicised vulnerabilities do not lead to any discernible real-world impact

COMPUTERWORLD UNITED STATES WINDOVS GEN AI OFFICE SOFTWARE APPLE NEWSLETTERS EVENTS WHITE PAPERS/WEB

Home > Security

NEWS

## Researchers: SMS attacks could cripple cell phones

By Robert McMillan  
IDG News Service | OCT 6, 2005 10:40 AM PST

Hackers armed with a moderately sized network of zombie computers theoretically could knock out cellular service throughout the U.S., according to security researchers at Pennsylvania State University. In a report published Wednesday, the researchers explained how such an attack could exploit weaknesses in Short Message Service (SMS), which is used to send and receive text messages between mobile phones.

<https://www.computerworld.com/article/2807994/researchers-sms-attacks-could-cripple-cell-phones.html>

INTERNET ARCHIVE  
DONATE WayBackMachine Explore more than 863 billion web pages saved over time

Calendar · Collections · Changes · Summary · Site Map · URLs

Go JAN FEB 24 2022

151 times between December 10, 2005 and February 24, 2022.

Smsanalysis.org

Related Searches:

- ▶ Best Mortgage Rates
- ▶ High Speed Internet
- ▶ Parental Control
- ▶ song lyrics
- ▶ Designer Apparel

2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024

<https://web.archive.org/web/20220224035507/http://www.smsanalysis.org/>



# Offensive security research

Sometimes real-world impact in entirely different ways than was anticipated



<https://leasing.com/guides/relay-car-theft-what-is-it-and-how-can-you-avoid-it>

## THE CONVERSATION

Academic rigour, journalistic flair

### Do you know what you're paying for? How contactless cards are still vulnerable to relay attack

Published: August 2, 2016 6:19pm CEST



<https://theconversation.com/do-you-know-what-youre-paying-for-how-contactless-cards-are-still-vulnerable-to-relay-attack-63142>

# How do researchers describe vulnerability impact?

**Leaking Contacts.** By completely breaching SGX in the manner described in Section IV, a malicious Signal server would be able to create an enclave that exposes all of the data

From "SGX: How SGX Fails in Practice" <https://sgaxe.com/>

CVE-2021-30747

Should you be worried? Probably not.



**M1ssing Register Access Controls Leak EL0 State**

<https://m1racles.com/>

**So you're telling me I shouldn't worry?**

Yes.

**What, really?**

Really, nobody's going to actually find a nefarious use for this flaw in practical circumstances. Besides, there are already a million side channels you can use for *cooperative* cross-process communication (e.g. cache stuff), on every system. Covert channels can't leak data from *uncooperative* apps or systems.

Actually, that one's worth repeating: **Covert channels are completely useless unless your system is already compromised.**

**So how is this a vulnerability if you can't exploit it?**

It violates the OS security model. You're not supposed to be able to send data from one process to another secretly. And even if harmless in this case, you're not supposed to be able to write to random CPU system registers from userspace either.

# Topics for discussion

(How) can we assess the realistic **real-life impact** of claimed **security vulnerabilities**?

Why are some vulnerabilities **not addressed**?

**Not economically viable** for attackers? Cost of attacks **externalized**?

Do they incur **opportunity costs**?

Researchers **shy away from “broken” technologies**? Industry **pulls products**?

Should offensive security research **consider real-life impact** or **lack thereof**?

“Real-life impact considerations” section in offensive security research papers?

# My take on the topics

Jan 30, 2024

## Workshop: Real-life impacts of (cyber)security vulnerabilities

An important type of information security research is “offensive security,” where security researchers analyze existing systems to...

Cybersecurity 6 min read



<https://medium.com/@asokan.public/workshop-real-life-impacts-of-cyber-security-vulnerabilities-846f0fda62d2>

# Today's agenda

13:30-14:00: Registration and Coffee

14:00-14:10: Welcome, [Prof. Bonhoeffer](#) (Director, Collegium Helveticum)

14:10-14:25: Introduction, [N. Asokan](#) (University of Waterloo)

14:25-14:45: *Finding, Patching, and Promoting Security Research – and what about Sustainability?* [Daniel Gruss](#) (TU Graz)

14:45-15:05: *Modeling Vulnerabilities Based on Attack Value*, [Eduardo Vela Nava](#) (Google)

15:05-15:25: *Quantifying Cyber Risk*, [Rainer Boehme](#) (University of Innsbruck)

15:25-15:50: *Information security vulnerabilities from an insurer's perspective – risk transfer and the real-life financial impact on the economy and general public*, [Lucas Engl](#) (Zurich Insurance)

15:50-16:10: Break



# Today's agenda

13:30-14:00: Registration and Coffee

14:00-14:10: Welcome, [Prof. Bonhoeffer](#) (Director, Collegium Helveticum)

14:10-14:25: Introduction, [N. Asokan](#) (University of Waterloo)

14:25-14:45: *Finding, Patching, and Promoting Security Research – and what about Sustainability?* [Daniel Gruss](#) (TU Graz)

14:45-15:05: *Modeling Vulnerabilities Based on Attack Value*, [Eduardo Vela Nava](#) (Google)

15:05-15:25: *Quantifying Cyber Risk*, [Rainer Boehme](#) (University of Innsbruck)

15:25-15:50: *Information security vulnerabilities from an insurer's perspective – risk transfer and the real-life financial impact on the economy and general public*, [Lucas Engl](#) (Zurich Insurance)

15:50-16:10: Break

16:10-17:40: Panel discussion on *Real-life impacts of security vulnerabilities*, host: [Shweta Shinde](#) (ETH Zurich), participants: [Hans Gersbach](#) (ETH Zurich), [Kaveh Razavi](#) (ETH Zurich), [Mark Brand](#) (Google), Anders Fogh (Intel)

17:40-17:55: Closing, [Kari Kostianen](#) (ETH Zurich)

18:00: Apéro



# My asks and hopes

Active audience engagement

Take **diversity in audience backgrounds** into account

Can we identify some **interesting sub-questions** to explore?

identify partners, data, ...

Is there a need to **raise awareness** within systems security research community?

identify next steps (panel at a conference? Dagstuhl seminar? ...)





# Logistics

All discussion is under [Chatham House rule](#)

You are free to use information from the discussion, but please do not reveal who made any particular comment

But please **identify yourself** when asking a question or making a comment

Two scribes: Mark Kuhne and Andrin Bertschi

Administration: Saskia Wolf and Vivien Klomp



# Today's agenda

13:30-14:00: Registration and Coffee

14:00-14:10: Welcome, [Prof. Bonhoeffer](#) (Director, Collegium Helveticum)

14:10-14:25: Introduction, [N. Asokan](#) (University of Waterloo)

14:25-14:45: *Finding, Patching, and Promoting Security Research – and what about Sustainability?* [Daniel Gruss](#) (TU Graz)

14:45-15:05: *Modeling Vulnerabilities Based on Attack Value*, [Eduardo Vela Nava](#) (Google)

15:05-15:25: *Quantifying Cyber Risk*, [Rainer Boehme](#) (University of Innsbruck)

15:25-15:50: *Information security vulnerabilities from an insurer's perspective – risk transfer and the real-life financial impact on the economy and general public*, [Lucas Engl](#) (Zurich Insurance)

15:50-16:10: Break

16:10-17:40: Panel discussion on *Real-life impacts of security vulnerabilities*, host: [Shweta Shinde](#) (ETH Zurich), participants: [Hans Gersbach](#) (ETH Zurich), [Kaveh Razavi](#) (ETH Zurich), [Mark Brand](#) (Google), Anders Fogh (Intel)

17:40-17:55: Closing, [Kari Kostianen](#) (ETH Zurich)

18:00: Apéro

