

Beyond the Password

Getting Real About Data Security

By Kim Smith & Paula Lackie for the Carleton College community. Last revised 3/8/2018

<https://xkcd.com/1938/>

THE MELTDOWN AND SPECTRE EXPLOITS USE "SPECULATIVE EXECUTION?" WHAT'S THAT?

YOU KNOW THE TROLLEY PROBLEM? WELL, FOR A WHILE NOW, CPUs HAVE BASICALLY BEEN SENDING TROLLEYS DOWN BOTH PATHS, QUANTUM-STYLE, WHILE AWAITING YOUR CHOICE. THEN THE UNNEEDED "PHANTOM" TROLLEY DISAPPEARS.



THE PHANTOM TROLLEY ISN'T SUPPOSED TO TOUCH ANYONE. BUT IT TURNS OUT YOU CAN STILL USE IT TO DO STUFF. AND IT CAN DRIVE THROUGH WALLS.



THAT SOUNDS BAD.

HONESTLY, I'VE BEEN ASSUMING WE WERE DOOMED EVER SINCE I LEARNED ABOUT ROWHAMMER.



WHAT'S THAT?

IF YOU TOGGLE A ROW OF MEMORY CELLS ON AND OFF REALLY FAST, YOU CAN USE ELECTRICAL INTERFERENCE TO FLIP NEARBY BITS AND—

DO WE JUST SUCK AT...COMPUTERS?

YUP. ESPECIALLY SHARED ONES.



SO YOU'RE SAYING THE CLOUD IS FULL OF PHANTOM TROLLEYS ARMED WITH HAMMERS.

...YES. THAT IS EXACTLY RIGHT.

OKAY. I'LL, UH... INSTALL UPDATES?

GOOD IDEA.



A Research Data Lifecycle

Conceptualization

**Publish, Archive or
Destroy Data**
documentation

Operationalization
documentation

Analyze
documentation

Gather Data
documentation

**Clean & Organize
Data**
documentation

A Research Data Lifecycle

Conceptualization

**Publish, Archive or
Destroy Data**
documentation

Operationalization
documentation

Analyze
documentation

Gather Data
documentation

**Clean & Organize
Data**
documentation

Threats & Vulnerabilities

- major threats
 - Accidental “publication”
 - phishing
- sources of vulnerability
 - Evildoers
 - You
 - Your team
 - Border Control

Solution: A Data Plan!

A Data Plan should address:

- Where you're keeping data
- How many copies and where they are
- How you share data (with your team)
- How you're going to update data
- What happens to data after you're through

Basic Protection

1. Which information (data) am I collecting?
2. Which devices will have access to the information/data?
 - a. Where am I & team members storing all of the related information/data?
 - b. Who has access to those devices? How am I making them secure?
3. Will I be sharing my data? If so, how?
4. Will I be archiving my data (and metadata)? If so, where, how, and for how long?
5. When and how will you destroy your data?

Higher protection: for sensitive data

What additional strategies would you use to increase security?

Enc

- Encryption
- Clear protocols for separating working data from original / not de-identified data
- VPN (Traveling?)

Highest protection: *super-sensitive*

- Enclaves
- Talk to us...

Sensitive secondary data

- Problems:
 - Allegedly de-identified data may not really be de-identified
- Solutions:
 - Look at all the variables!
 - Aggregate the data
 - Treat it all as identifiable data

A Research Data Lifecycle

Conceptualization

**Publish, Archive or
Destroy Data**
documentation

Operationalization
documentation

Analyze
documentation

Gather Data
documentation

**Clean & Organize
Data**
documentation