CSE 550: Systems for all

Au 2021

Ratul Mahajan

Basic concepts in computer security

Security is like performance

Abstractly, more is better, but “more” is costlier

- Practical view: Is it good enough?
  - Use case (performance) vs threat model (security)
- Mechanism choice: Cost/benefit analysis

Doing it well implies holistic consideration from the start

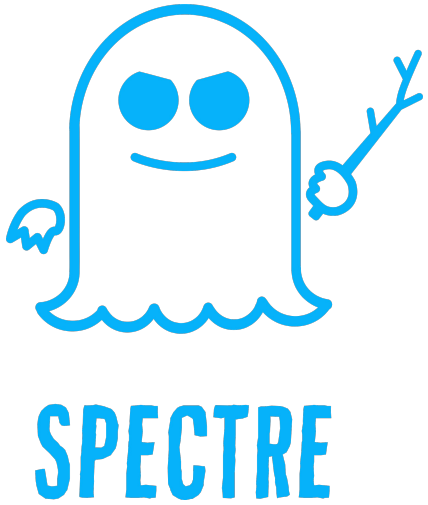
- “Weakest link”
- Slapping it on after the fact is hard
  - One reason behind general insecurity of Internet protocols

Security ~~is~~ does not like performance

Extracting performance increases complexity, which reduces security

Can also open side-channel attacks

- Speculative execution a key factor behind Spectre and Meltdown



Security is multi-dimensional

Confidentiality

Integrity

Availability

Accountability

Security is more than cryptography

Theoretically, cryptography has limits

- Does not help with availability
- Does not provide full confidentiality (e.g., metadata leakage)

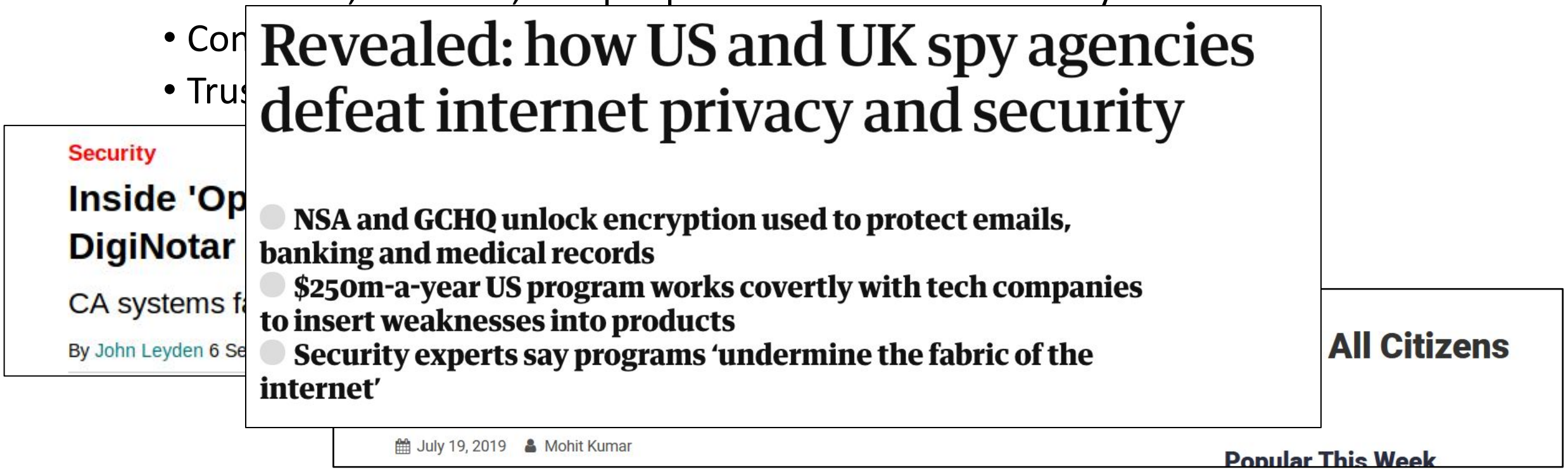
Practically, most attacks don’t break crypto

- E.g., none of top three (Yahoo 2013, Alibaba 2019, LinkedIn 2021) were a result of breaking crypto
- Unauthorized access and bad configuration are much more common
- Code bugs are another major factor after these two

Pay attention to the trusted computing base

Most security analyses provides guarantees atop the TCB, but the biggest threats stem from violations in assumptions about TCB

- Hardware, software, and people can behavior differently
- Con
- Trus



Security

Inside 'Op
DigiNotar

CA systems f

By John Leyden 6 Se

Revealed: how US and UK spy agencies defeat internet privacy and security

- NSA and GCHQ unlock encryption used to protect emails, banking and medical records
- $250m-a-year US program works covertly with tech companies to insert weaknesses into products
- Security experts say programs 'undermine the fabric of the internet'

July 19, 2019 Mohit Kumar

All Citizens

Popular This Week

Over to Austin