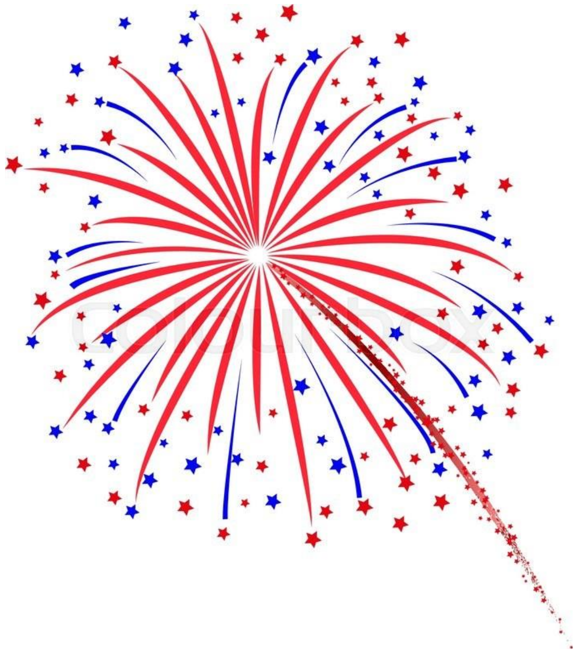
We would like to announce:

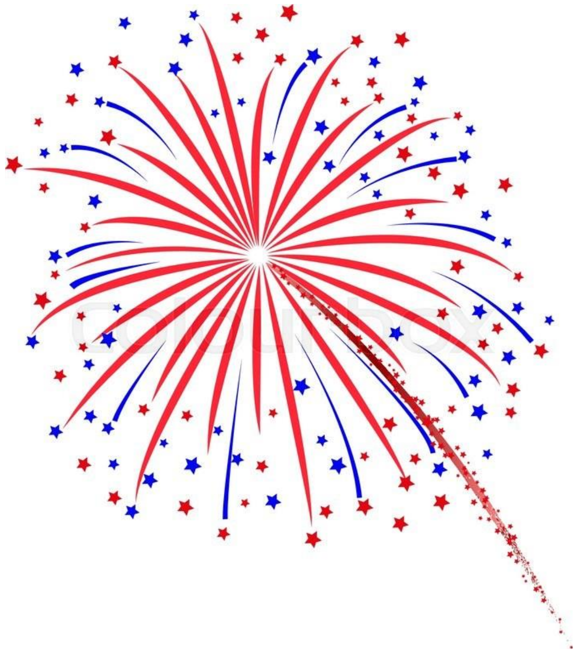
We would like to announce:

Passwords are finally DEAD!!!



We would like to announce:

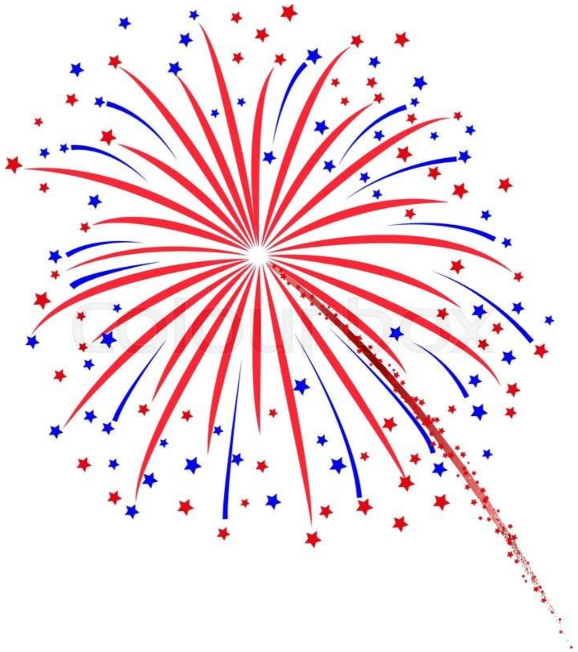
Passwords are finally DEAD!!!



Not like when Bill Gates said that,

We would like to announce:

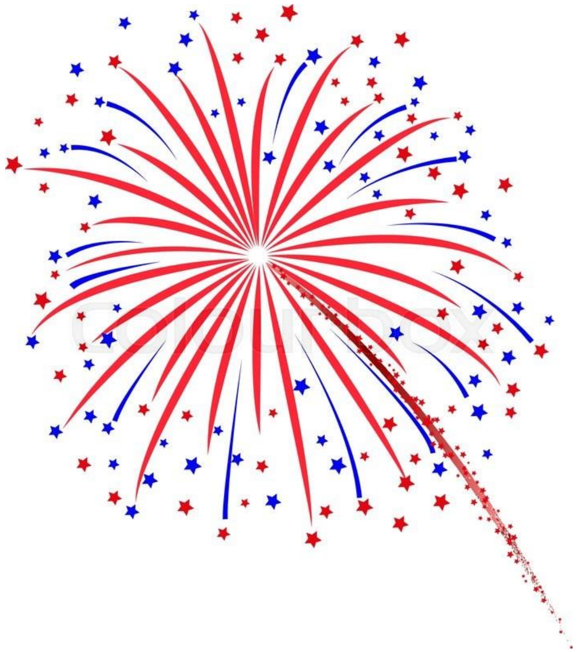
Passwords are finally DEAD!!!



Not like when Bill Gates said that,
and Google claimed that, and…

We would like to announce:

Passwords are finally DEAD!!!



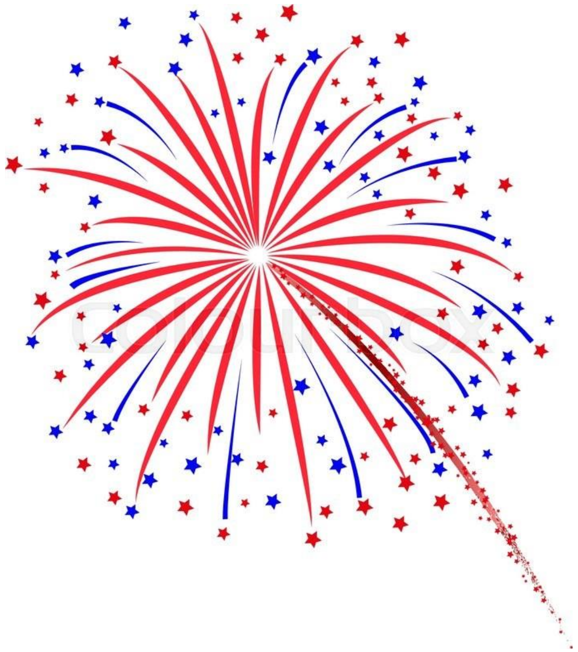
Not like when Bill Gates said that,

and Google claimed that, and…

But really really dead

We would like to announce:

Passwords are finally DEAD!!!



Not like when Bill Gates said that,

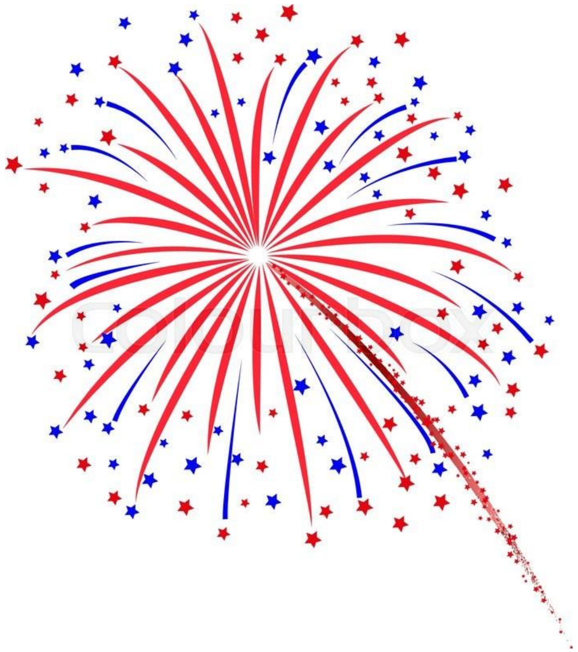
and Google claimed that, and…

But really really dead

Pushing up daisies

We would like to announce:

Passwords are finally DEAD!!!



Not like when Bill Gates said that,

and Google claimed that, and…

But really really dead

Pushing up daisies

But we can’t ☹

How to (not) Share a Password:
Privacy preserving protocols for finding heavy hitters with adversarial behavior

Moni Naor **Benny Pinkas** **Eyal Ronen**

Compromise a User, Attack the Eco System

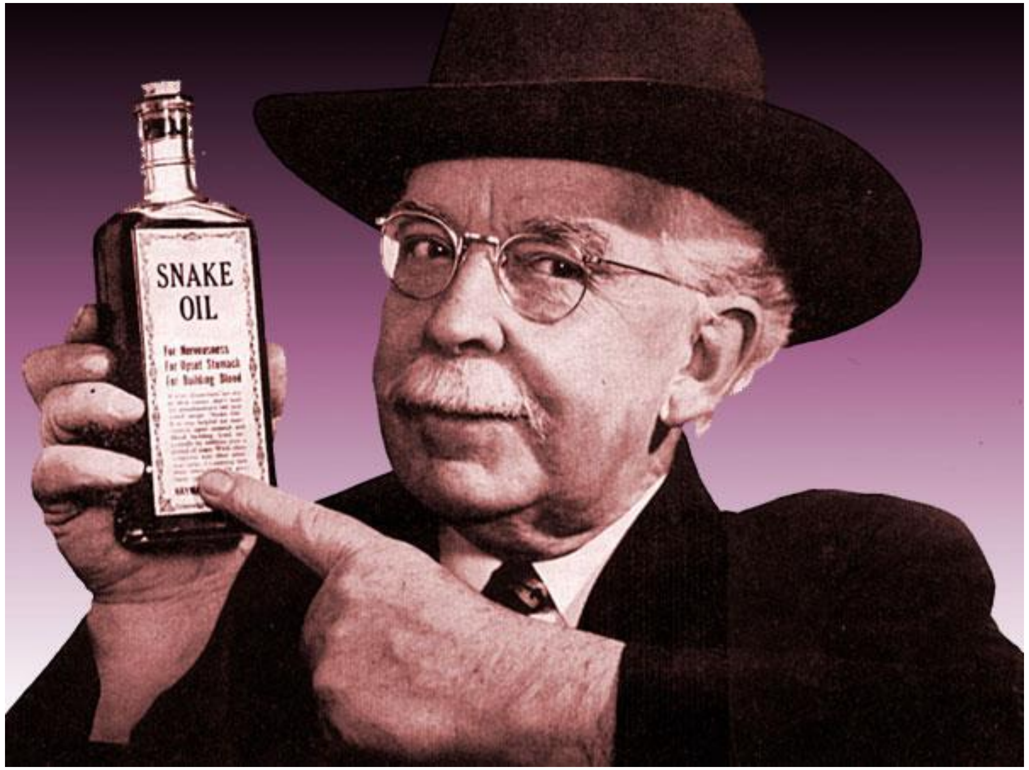
- Bad passwords do not only compromise the users
- Weak and popular passwords can be used for large scale attack
  - E.g. the Mirai attack
  - Easy to find IoT devices with Shodan like search engines
- Service provider liability?

Possible solutions

Panacea

Greek Goddess of **Universal Remedy**

Solution to all problems; **Cure-all**

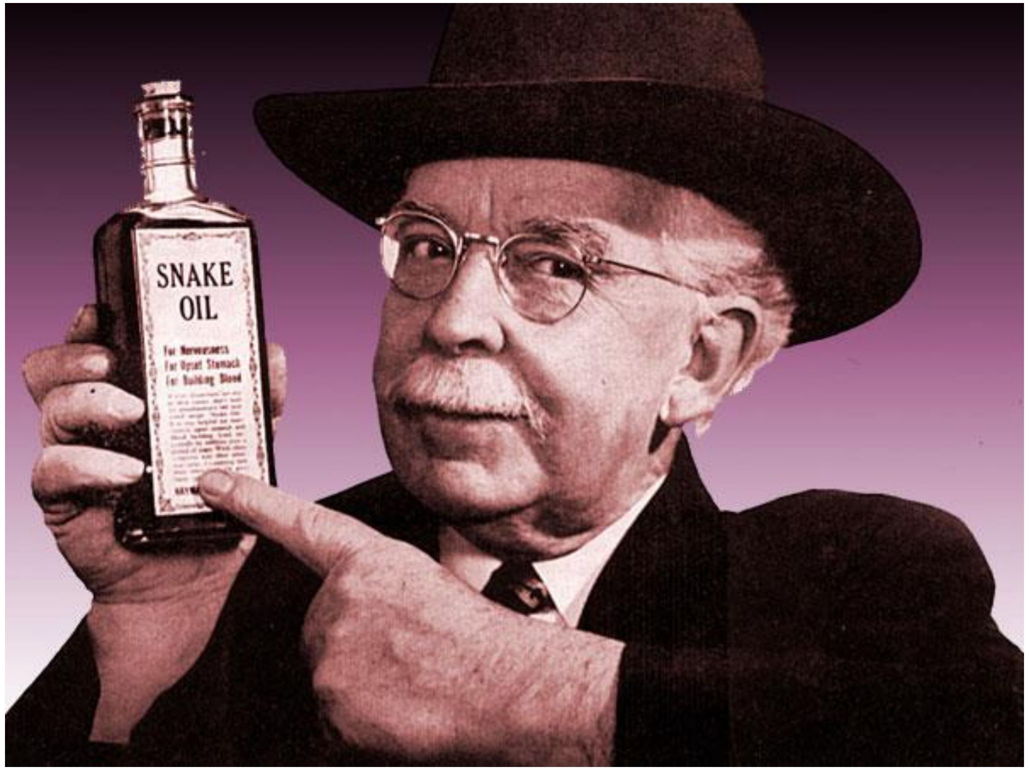


Possible solutions

Panacea

Greek Goddess of
Universal Remedy

Solution to all
problems; **Cure-all**



- Our suggestion - Blacklist Popular passwords

Passwords over time

- password -> passw0rd -> p@assw0rd->password

- superman -> wonderwoman

- Different populations

Passwords over time

- password -> passw0rd -> p@assw0rd->password
- superman -> wonderwoman
- Different populations

Primum non nocere

First do (almost) no harm

Primum non nocere

First do (almost) no harm

- Publishing password blacklist can also help attackers
  - Publishing the blacklist is like publishing a **code vulnerability**

Primum non nocere

First do (almost) no harm

- Publishing password blacklist can also help attackers
  - Publishing the blacklist is like publishing a **code vulnerability**

- Leaking password information can hurt the user
  - One bit leakage doesn’t hurt the user a lot
  - Differential privacy can also help

How to (not) share a Password

- Identify and **blacklist** popular passwords (heavy hitters)
  - those were chosen by more than a fraction τ of the users
- Server should not learn more than 1 bit on any user’s password
  - At most halves the number of password guesses
- Probability of False Negative (pFN) must be **negligible**
  - No popular password is missed
- Probability of False Positive (pFP) may be a small value
  - A legitimate password can be rejected with low probability

Previous work

- Privately Finding heavy hitters in many settings - [DNP+10,DNPR10,CSS11,CLSX12,DNRR15]
- Semi-honest version [BS15,BNST17]
- Non colluding mix servers – [MS17]

- DP password list with **trusted server** – [BDB16]
- Similar motivation, no DP – [SHM10]

The Malicious world

- Both users and server might be malicious
- A malicious server wants to learn the passwords
- Malicious users want to “hide” popular passwords
  - **Adversary controls a coalition of users**

Implementation and other usages

- We implemented the full malicious QR protocol on a RPi
  - Non interactive version runs in about 15 seconds, can run in background
  - Server computer can verify in about 0.5 seconds
- Same solution can be used in any heavy hitter problem with possible malicious setting
  - **TOR network statistics**
  - **Device PIN/Pattern**
  - **Large service providers dynamic passwords statistics**

eprint.iacr.org/2018/003