Security in Data Science

Dan Boneh
Stanford University
Private genomic data analysis

[Jagadeesh, Wu, Birgmeier, Boneh, Bejerano, Science, 2017]

What genes causes a specific disorder?

\[ v_1 = \begin{bmatrix} 0 & 1 & 0 & 2 & 0 & 1 \\ 1 & 0 & 1 & 2 & 0 & 1 \end{bmatrix} \]

\[ v_3 = \begin{bmatrix} 2 & 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 0 & 1 \end{bmatrix} \]

People with Kabuki syndrome

Each has 211 to 374 rare genes out of \( \approx 20,000 \) genes

Patient \( i \): vector \( v_i \) of dim 20,000 that is 0 for normal genes
MPC for genomic data analysis

People with Kabuki syndrome

Each has 211 to 374 rare genes out of \( \approx 20,000 \) genes

Patient \( i \): vector \( v_i \) of dim 20,000 that is 0 for normal genes

Jagadeesh, Wu, Birgmeier, Boneh, Bejerano, Science, 2017
MPC for genomic data analysis

[Jagadeesh, Wu, Birgmeier, Boneh, Bejerano, Science, 2017]

People with Kabuki syndrome

Nothing else is revealed about the individual genomes!!
How does it work?

See paper
Can we do this with Intel’s SGX?

Enclave Application

- Untrusted Part of App
- Create Enclave
- CallTrusted Func.

(etc.)

Trusted Part of App

- Call Gate
- Execute
- Return

m8U3bcV#zP49Q

Remote Attestation

Client Application

Enclave

Remote Platform

Source: ISCA 2015 tutorial slides for Intel SGX
Iron: Functional encryption and obfuscation using Intel SGX

Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, Sergey Gorbunov

In ACM CCS 2017
... and now for something completely different:

Prio: Private, Robust, and Efficient Computation of Aggregate Statistics

Joint work with Henry Corrigan-Gibbs
Today: Non-private aggregation

Every user has a private data point
Today: Non-private aggregation

Blood pressure vs. Twitter usage

StressTracker
Today: Non-private aggregation

The app provider learns more than it needs

\[ B(T) = c_1 \cdot T + c_0 \]
StressTracker
App store

Prio: Private aggregation

Clients send one share of their data to each aggregator
Prio: Private aggregation

\[ B(T) = c_1 \cdot T + c_0 \]

Aggregator learns nothing else
THE PROBLEM

Blood pressure

Twitter usage

100,000,000

App store

StressTracker
Private aggregation

$\mathbf{x}_1 \mathbf{x}_2 \mathbf{x}_3 \ldots \mathbf{x}_N$

$f(\mathbf{x}_1, \ldots, \mathbf{x}_N)$

**Exact correctness:** if all servers are honest they learn $f(\mathbf{x}_1, \ldots, \mathbf{x}_n)$

**Privacy:** if one server is honest they learn only $f(\mathbf{x}_1, \ldots, \mathbf{x}_n)$

**Robustness:** malicious clients have bounded influence

**Scalable:** no public-key crypto (other than TLS)
Prio contributions

Achieves all four goals

1. Robustness using secret-shared non-interactive proofs (SNIPs)
   - Every client efficiently proves to servers that its submission is well formed
   - Takes advantage of non-colluding servers (verifiers)

2. Aggregatable encodings
   - Compute sums privately \( \Rightarrow \)
     - compute \( f(\cdot) \) privately for many \( f \)'s of interest
Existing approaches

• Additively homomorphi$\text{c}$ encryption

• Multi-party computation \cite{GMW87, BGW88}

• Anonymous credentials/tokens
  VPriv (2009), PrivStats (2011), ANONIZE (2014), ...

• Randomized response \cite{W65, DMNS06, D06}
  RAPPOR (2014, 2016)
Private aggregation: needed in many settings

<table>
<thead>
<tr>
<th>Private client value ((X_i))</th>
<th>Aggregate (f(X_1, \ldots, X_N))</th>
</tr>
</thead>
</table>
| Location data (phones/cars)   | - Number of devices in location \(L\)  
|                               | - Ten most popular locations  
|                               | - Locations with weakest signal strength |
| Web browsing history          | - Most common websites  
|                               | - Websites with TLS certificate errors |
| Health information            | - Min, max, avg, stddev heart rate  
|                               | - ML model relating BP to Twitter usage |
| Text messages                 | - Min, max, average number per day  
|                               | - ML model relating time of day to emotion |
Prio: how does it work?

See paper
THE END