Experiences Implementing Usable MPC For Social Good

Mayank Varia
Hariri Institute, Boston University

Based on joint work with

- BU: Azer Bestavros, Eric Dunton, Frederick Jansen, Kyle Holzinger, Andrei Lapets, Nikolaj Volgushev
- UMass: Rose Kelly, Shannon Roberts
- MIT: Malte Schwarzkopf

with the help of many more...
Caveats Upfront

A talk on deployment of secure multi-party computation (MPC)
- Only semi-honest MPC is discussed (though recent results indicate malicious security is becoming feasible for such applications)
- The function being computed is quite simple, ergo...
- Performance of the MPC protocol itself is not a bottleneck

An experience talk (not a theory talk)
- Little discussion of cryptography
- Focus on human and systems challenges
- A sample size of one application with three deployments, so other applications and deployments may give rise to different lessons
Cryptographic assumption: Pay equity is a desirable goal
WOMEN’S WORKFORCE COUNCIL

The Women’s Workforce Council was established by Mayor Thomas M. Menino on April 9th, 2013 — known nationwide as Equal Pay Day. The day marks how far into 2013 women need to work to earn what men earned in 2012. The first of its kind in the country, the Council’s mission is to help transform Boston into the best city in the country for working women.

Members of the Council represent the financial, engineering, medical, law, technology and retail sectors, and include small business owners, entrepreneurs, senior executives, as well as academic, labor and nonprofit leaders.

The Council’s first priority was to identify new and creative ways to help close the wage gap between working men and women, helping Boston become the first major city to achieve pay equity. This report outlines the Council’s recommendations to employers throughout the city.
The Initial Plan (December 2013)

100% TALENT
The Boston Women’s Compact

To make Greater Boston the premier place for working women in America, by closing the wage gap and removing the visible and invisible barriers to women’s advancement. By doing so, we will build a more equitable workforce where all talent is cultivated and valued.

GOAL 3
Evaluating Success

Employers agree to participate in a biennial review to discuss successes and challenges, as well as contribute data to a report on the Compact’s success to date. Employer-level data would not be identified in the report. The specific data to be reported will build on data already required by federal and state authorities and should not create an additional reporting burden.

compiled by a third-party
Lesson: To deploy MPC, find someone who has overpromised and cannot deliver.
Explaining MPC to Execs, HR, and Lawyers (2014-2015)

**Lesson:** Contextualize MPC’s trust requirements
Lesson: Identify key participants whom you must convince

Explaining MPC to Execs, HR, and Lawyers (2014-2015)
Developing a Data Aggregation System (Spring 2015)

https://100talent.org

- HR employees love spreadsheets
- Data contributors only need a web browser
- Modeled off of existing EEO-1 form

Lesson: Simplicity increases trust, which drives adoption

Lesson: Web browsers won the “corporate environment compatibility wars”

Lesson: Regulation -> standard schemas
Developing a Data Aggregation System (Spring 2015)

**Contributors**
- Code Distributor
- Compute Service Provider

**Service Provider (e.g., BU)**
- (web server/database)

**Analyst (e.g., BWWC)**
- (client running web browser)

---

**Code Distributor**
- Boston University
  - Extensive IT/engineering/CS expertise
  - Production cloud environment
  - Do not store data from individual contributors (liability)
  - Do not store overall outcome (unnecessary)
  - Incentive not to collude

**Data Analyst**
- Boston Women’s Workforce Council
  - No IT staff or expertise
  - Literate in statistical analysis
  - Do not store data from individual contributors (liability)
  - Store overall outcome (necessary for analysis)
  - Incentive not to collude

---

**Lesson:** Exploit asymmetry
Explaining the Interface to Users (Spring 2015)

- Training sessions & videos
- Dry run with synthetic data
- Client-side error messages
June 8, 2015: D(ata Collection) Day

![Workforce Survey](image)

**Workforce Survey**
Boston Women's Workforce Council

**Enter Session Key**

**Email Address to track participation**

**Female Workforce**

<table>
<thead>
<tr>
<th></th>
<th>Hispanic</th>
<th>White</th>
<th>Black</th>
<th>Pacific Islander</th>
<th>Asian</th>
<th>Native American</th>
<th>Other</th>
<th>Sum Ann Comp Job</th>
<th>Sum Ann Cash Per Job</th>
<th>Sum Len Ens Job</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MidLevel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professionals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technicians</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SalesWorkers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin/SupportWorkers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Male Workforce**

<table>
<thead>
<tr>
<th></th>
<th>Hispanic</th>
<th>White</th>
<th>Black</th>
<th>Pacific Islander</th>
<th>Asian</th>
<th>Native American</th>
<th>Other</th>
<th>Sum Ann Comp Job</th>
<th>Sum Ann Cash Per Job</th>
<th>Sum Len Ens Job</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MidLevel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professionals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technicians</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SalesWorkers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Submit]
Lesson: The lawyers will come for you... even if you build a technology whose main benefit is to keep the lawyers away
June 8, 2015: D(ata Collection) Day

"If this does not work out, I will just fax you the spreadsheet for you to enter…"

Lesson: Bottleneck/weak point of security solutions = human users (this threat cannot be removed, but it can be mitigated)
Usability and Heuristic Evaluations

Our chosen properties

- Familiar interface
- Compatibility
- Error detection/feedback
- Asynchrony
- Idempotence

Standard usability components

- Learnability
- Efficiency (user productivity)
- Memorability
- (Low) errors
- Satisfaction

Lesson: When designing, implementing, and deploying any security tool, involve human factors experts from the start.
Larger Collection (2016)

- Over 150 signatories (71 appeared on collection day)
- Aggregate data analyzed and published by the BWWC
- Data encompasses about 112,600 employees
  - > 10% of the greater Boston area workforce
  - about $11 billion in wages
- 2017 collection: 200+ signatories, of which 120+ contributed data

Lesson: People will build up trust in your system, even if it’s designed so they don’t need to trust you
Reactions

The congresswoman, who had signed onto a bill addressing income disparity between men and women, was impressed by the relevance he outlined. “It’s linking it back for the members of Congress,” Clark said. “Nobody would think, oh, the Paycheck Fairness Act, how is that tied into NSF funding?”

The Boston Globe

BWWC co-chair Evelyn Murphy on secure MPC: “Here, we’re beginning to show how to use this sophisticated computer science research for public programs.”
Mayor Walsh pushes to gather data on gender wage gap

Mayor Martin J. Walsh waded into the controversy surrounding the gender wage gap Tuesday, announcing that he was set to launch an unparalleled effort to collect salary data from businesses throughout Boston, and that he had boosted the salaries of two top women on his own staff.
Deployment opportunities for secure solutions

– Could deploy MPC when people have overpromised but cannot deliver on (usually simple) computations

– Legal restrictions, liabilities, and natural incentives can be opportunity
  • ...to deploy “secure” techniques and technologies in unexpected ways
  • ...to *simplify* solution requirements

– Specialize (to the scenario at hand) not just the protocol(s) but the trust and computing setup
  • identify target user profiles and level of detail and confidence they require
  • separate roles, functionalities, and infrastructure (then assign as appropriate)

Human factors will play a role regardless of technical details

– May still be necessary to follow familiar traditions (NDAs)

– Human users are (still) a weak point when it comes to security

– Conceptual simplicity, artifact usability/compatibility, and community acceptance can drive confidence/ adoption
Thanks!
multiparty.org