Anonize

A Large-scale Anonymous Survey System

Steve Myers    Rafael Pass     Abhi Shelat    Susan Waters
UI        Cornell  UVA     JHU
On-line Surveys are Ubiquitous Today
- Course evaluations, market research, …, medical research.

On-line Survey Market Size : ≈$3Bn [IbisWorld’14]
- SurveyMonkey (6% marketshare): 2M responses/day

Key goal:
- Elicit TRUTHFUL responses
Large Scale Surveys: NEED

- **AUTHENTICITY:** only “authorized” users may submit a response, and only once.
  - otherwise, we get **UNRELIABLE** results!

- **ANONYMITY:** how a particular users responds cannot be traced back to her.
  - otherwise, we get unreliable results!
  - otherwise, may be **UNETHICAL**
Large Scale Surveys: TODAY

Rely on a trusted third party (TTP)

to ensure ANONYMITY and AUTHENTICITY

Dangerous principle!!

• Who can we trust?
• Even if trust TTP, what if it gets breached (c.f. iCloud breaches)
“Cryptographic Voting” [Chaum’81]

Replace TTP with “cryptography”

1. Users authenticate themselves and check out an “anonymous token”
   - Authorized users can only check out one token
   - Token’s validity can be verified
   - Token cannot be linked to the user

2. Users can later use the token to submit a response
“Cryptographic Voting” [Chaum’81]

Step 1: Token check-out

 alice@cornell.com

Cannot be linked to Alice!

Step 2: Submitting a survey

$
“Cryptographic Voting” [Chaum’81]

Step 1: Token check-out

Step 2: Submitting a survey

ONLY ANONYMOUS if Alice separates step 1 and 2!
Our Innovation: Ad-hoc Surveys

1. Users authenticate themselves and check out a “MASTER token” ONCE.

1. ANYONE can set-up a survey based only on the emails of users it wants to participate.
   - No interaction with the users

2. Authorized users can on their own create a “anonymous ONE-TIME token” that they can use to submit a response:
   - only a single one-time token per survey
   - token’s validity can be verified
   - token cannot be linked to user

AUTHENTICITY
ANONYMITY
Ad-hoc Surveys

Step 1: Master Token Check-Out
alice@cornell.com

ONCE

Step 2: Posting a survey
http://www.cornell.edu/courseevals/cs6830/form

alice@cornell.com
bob@cornell.com
...
xavier@cornell.com

REPEAT

Step 3: Submitting a response

Cannot be linked to Alice!
The Anonize System

1. A **cryptographic solution** to ad-hoc surveys system

2. Cryptographic solution is **provably secure**
   - Our solution has a **rigorous mathematical proof of security** based on well-studied cryptographic assumptions (elliptic curve cryptography)

3. Handles **large-scale** surveys
   - Millions of users on a single work station

1. A simple-to-use smartphone app
Application to Course Evals

Registration
1. Students install Anonize app on their smartphone
2. Their Cornell email is verified

→ “master token” gets saved on their phone
Setting-up a course eval (automatic)

1. Enter course number
2. Enter questions
3. Enter emails of all students in class

⇒ Webpage created: http://beta.anonize.com/43247722364237894632784231
⇒ Email sent out to all students
Application to Course Evals

Filling out a survey

1. Students fills out the survey on the webpage
2. Clicks submit
3. QR code appears
4. Submits survey by scanning the QR code using Anonize app.
Summary

Ensuring **Authenticity** and **Anonymity** is Crucial

Cannot Rely on Trusted Third Parties

**Anonize**: practical and provably secure solution
Thank You