A Contractual Anonymity System

Edward J. Schwartz, David Brumley and Jonathan M. McCune
Carnegie Mellon University, CyLab

NDSS 2010: March 2nd, 2010

Motivating Example

RateMyProf.com

Uh oh. I wish this hadn't happened…

					User Comments	Professors add your rebuttal here
4/3/09	[redacted]	5	5	5	[redacted]s one of the most charismatic instructors I've ever had. She is engaging and keeps class interesting. She makes an effort to truly know all of her students. She is a gifted and committed teacher. Shanita's lessons extend far beyond the classroom. I am grateful to have had class with her.	
12/10/07	[redacted]	4	5	5	She is my favorite prof. She is fun, insightful, and very encouraging. I liked everything about the class except the fact she had some people come into class that were a waste of time but it was still a good class. at least i found out what I want to do w/ my major b/c of this class	
6/1/07	[redacted]	5	5	5	Although I felt like this class was a little bit suited for kids at time (you play a lot of games and group activities) it was easy and interesting, plus Shanita always energetic and willing to help you!	
5/22/07	[redacted]	5	5	5	I had [redacted] for Intro to Advertising. She is a great teacher. One that has a lot of energy, engages her students, and inspires. The way her class is structured is interesting as well. She gives us feedback and other classmates give feedback for your project/presentation. She is more fair than any of the other instructors in the department.	
12/26/06	[redacted]	5	1	1	I was embarrassed to be in this class. It felt like kindergarden. I coudln't believe I wasted tuition $ on it. We sat around in circles and drew pictures to put on the walls. If this is college - I was prepared before elementary school. An embarrassment. Insulting to our intellegence. A joke. I learned nothing a wasted a lot of money.	

Student

Professor

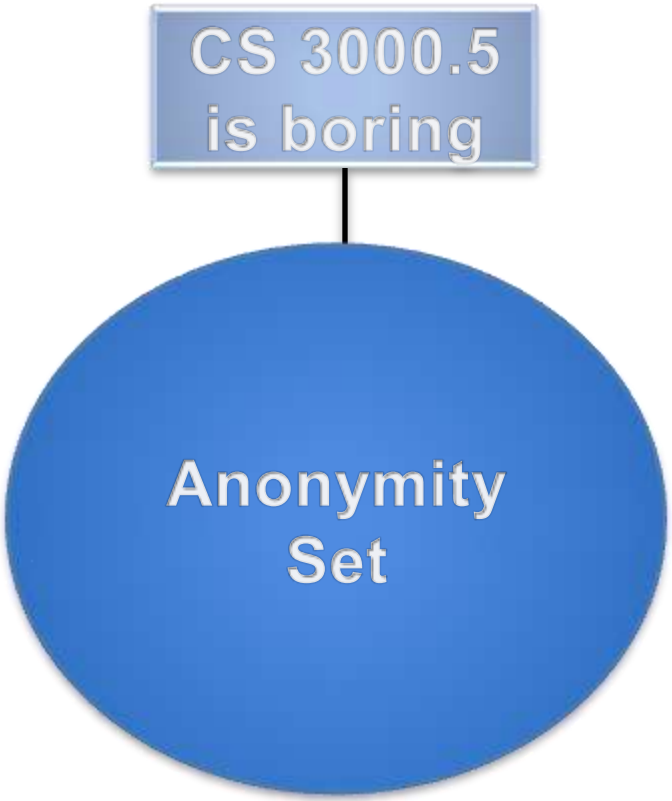
This class is boring!!!

Student, you are in BIG trouble.

What properties will help Student share his thoughts?

Anonymity?

Anonymity



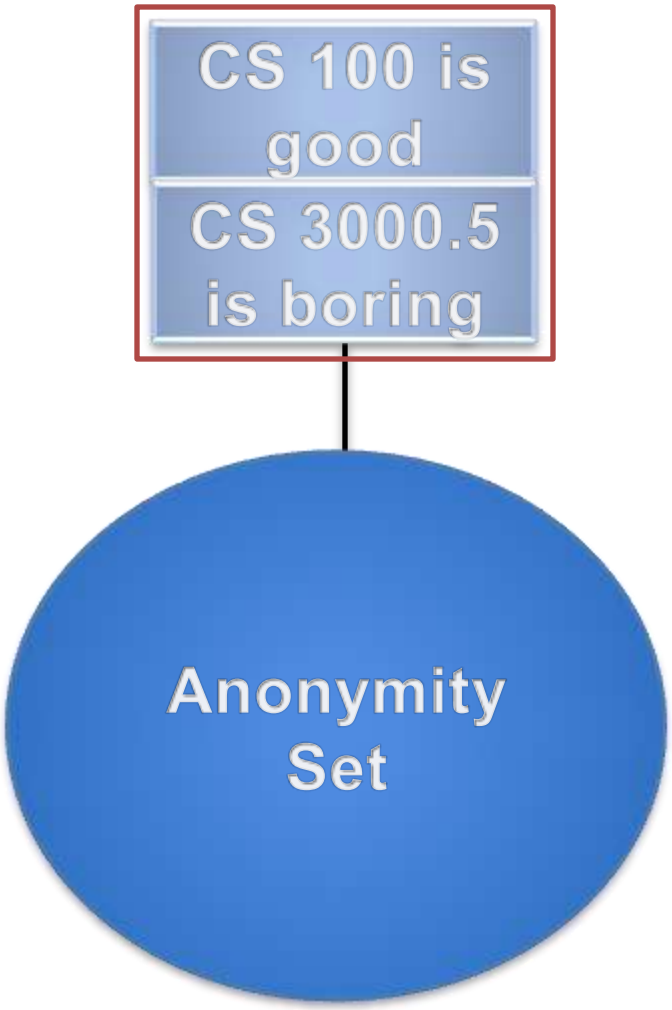
Professor

I can't tell which person in anonymity set made this!

How can we help Student share his thoughts?

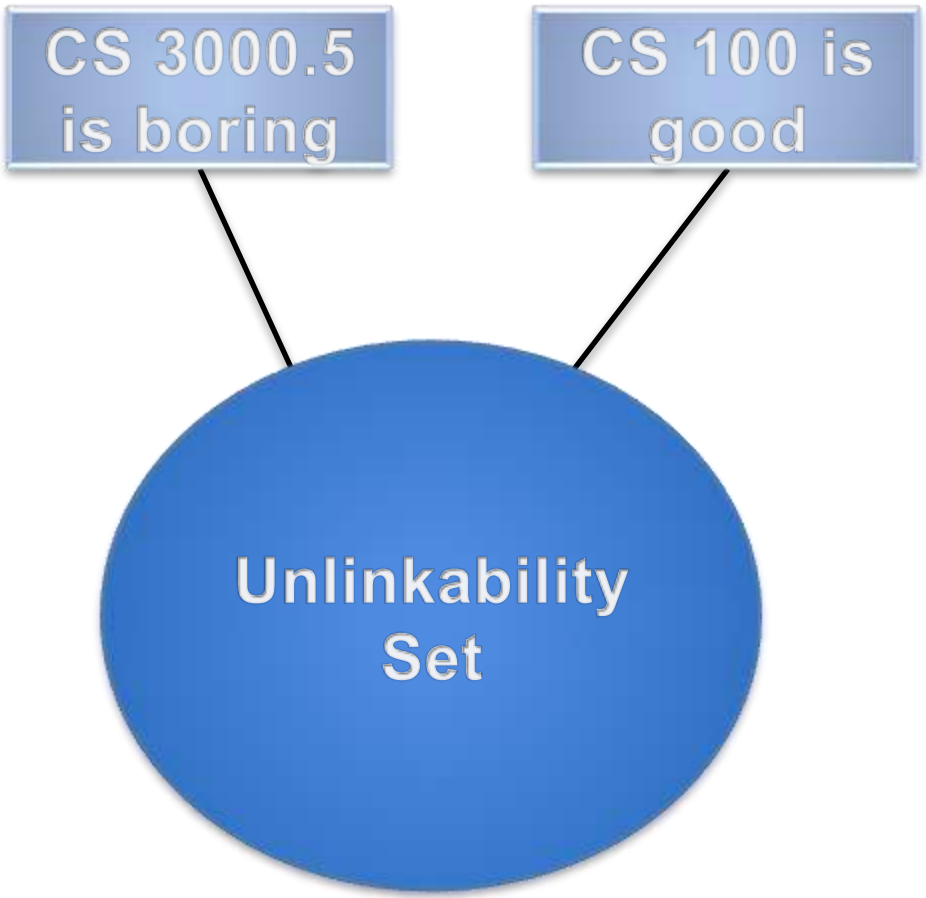
- **Anonymity**

Linkability



Hmm, only one student took both of these classes… Student!

UNLinkability



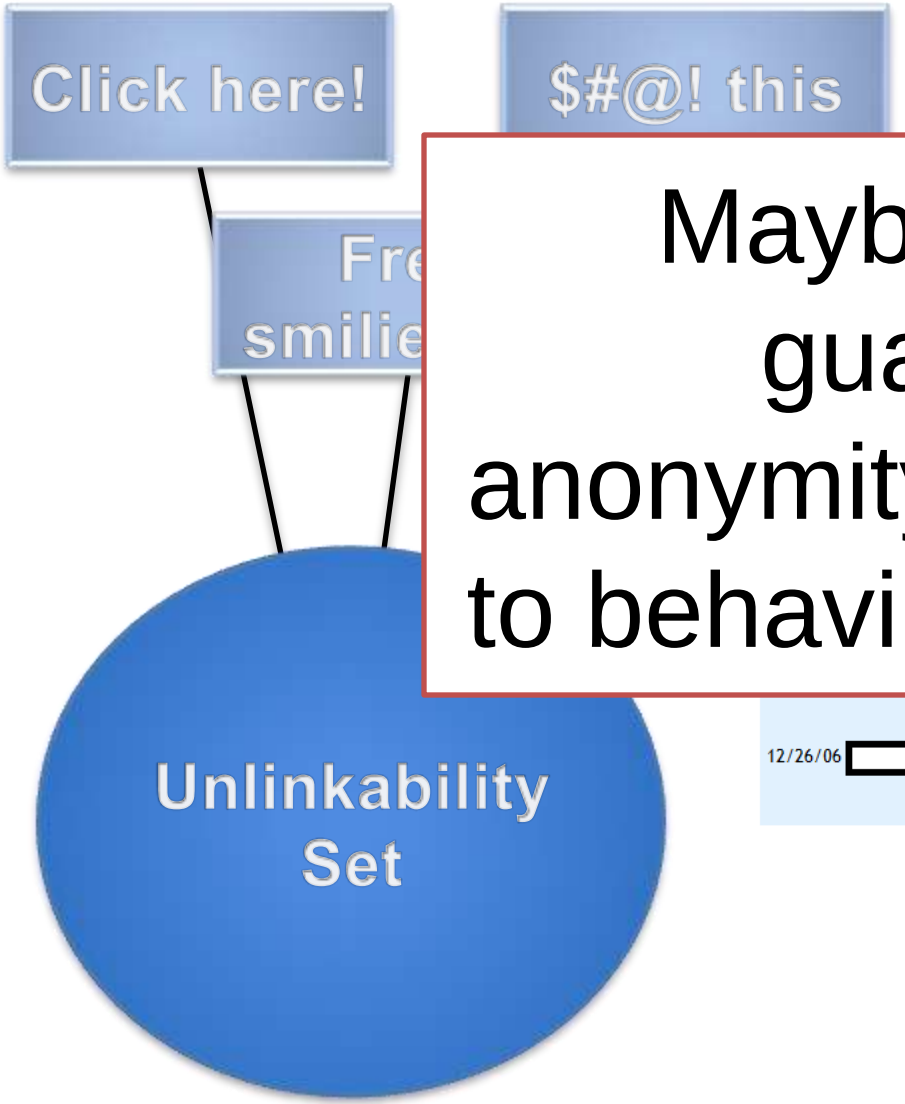
Professor

I can't even tell if the same person made both reviews!

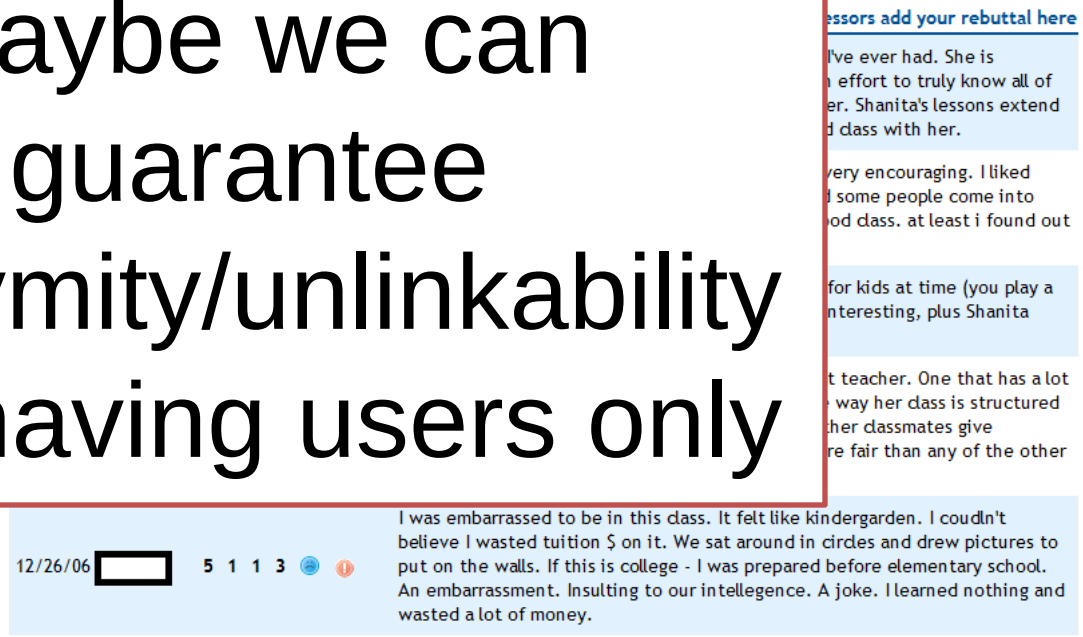
How can we help Student share his thoughts?

- Anonymity
- **Unlinkability**

Problems with Anonymity



Maybe we can guarantee anonymity/unlinkability to behaving users only



I wish we could ban these misbehaving users…

How can we help Student share his thoughts?

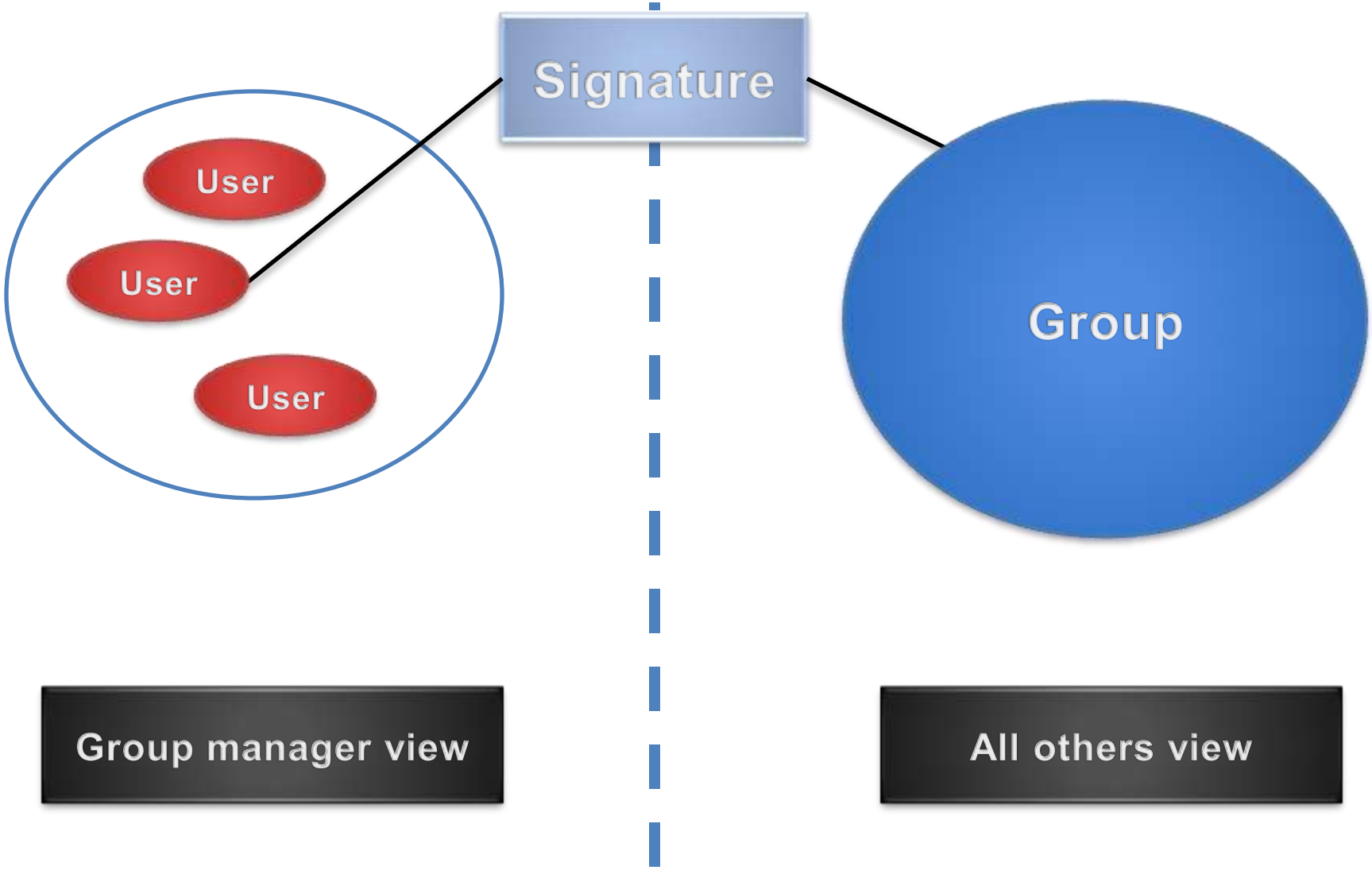
- Anonymity
- Unlinkability
- **Revocability**

- Prior work can provide these properties

Background: Group signatures

- Group signatures allow a user in a group to endorse a message on behalf of the entire group
- Each signature **is anonymous and unlinkable**
- There is a **group manager** that can determine which user signed a message

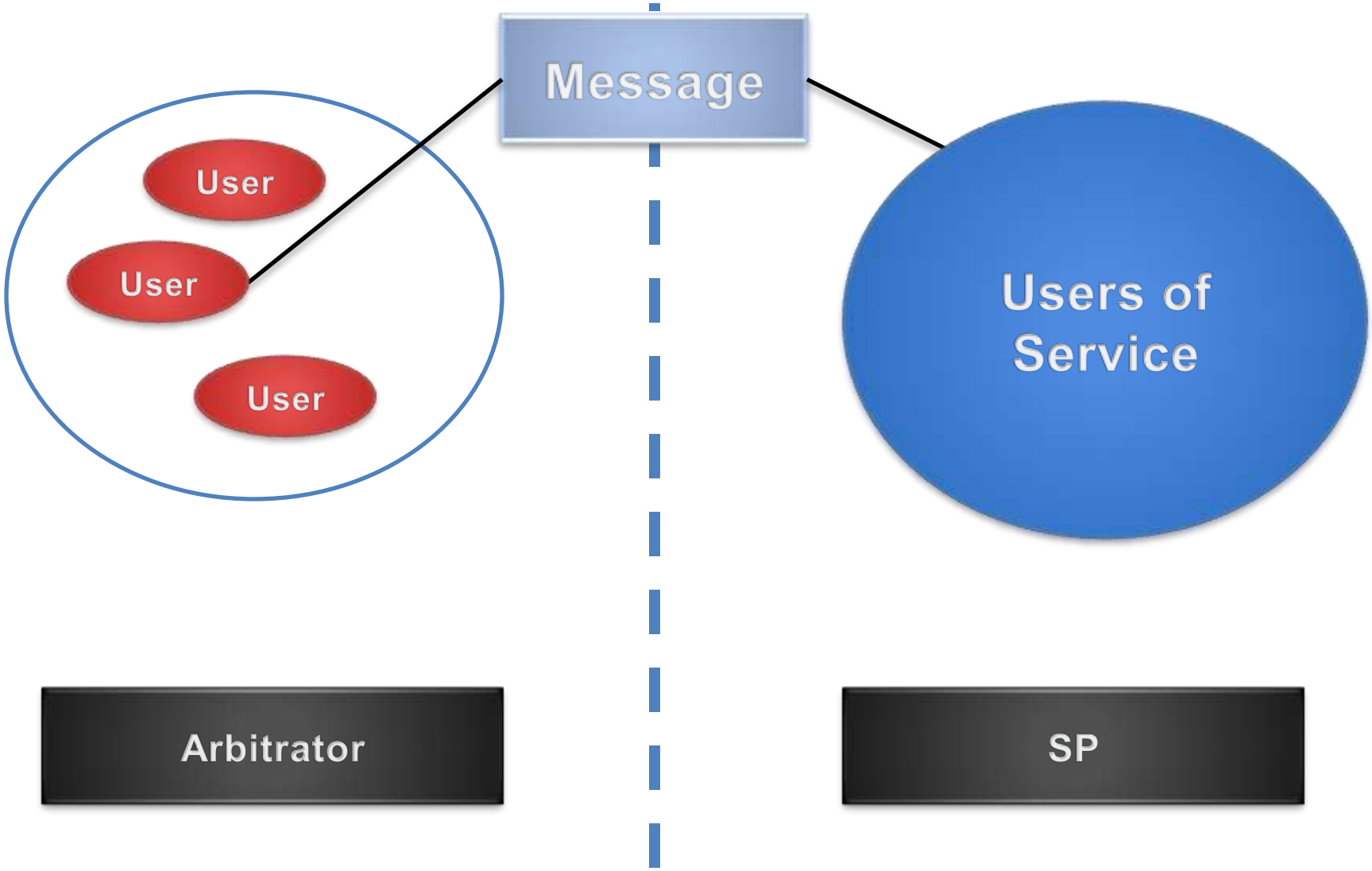
Background: Group signatures



Group Signature Anonymity Protocol

- How to make an anonymity protocol from group signatures
- **Setup**
  - Group manager is an arbitrator
  - Users join group by sending long-term identity to arbitrator
- **Message sending**
  - **Example:** Student wants to send a rating
  - He creates a group signature
  - RateMyProf verifies group signature
- **Revocation**
  - **Example:** User posts review full of links (spam)
  - SP sends offending message to arbitrator
  - Arbitrator can look up offender's long-term identity

Group Signature Anonymity: Why Does it Work?



Group Signature Anonymity: Problem

Arbitrator

What went wrong?

Professor

It was Student!

I'll find out who this student is!

Group Signature Anonymity: Problem

- **We trusted the arbitrator, but didn't have any reason to**
  - User can be de-anonymized and banned at a whim
- Can it be fixed?
  - Yes, if we can constrain the arbitrator somehow
  - **Foreshadow**: We will do this for our scheme using trusted computing

How can we help Student share his thoughts?

- Anonymity
- Unlinkability
- Revocability
- **Verifiability**

- Prior work can provide this too

Subjective Judgment Schemes

- Examples: PEREA [Tsang et al. 08], EPID [Brickell et al. 08], BLAC [Tsang et al. 07]
- No third party
- Service Provider judges bad behavior
- Allows **anonymous blacklisting**
  - **Blacklist** means ban from service
- **Performance concerns**
  - Scalability with number of banned users (more later)

Subjective Judgment: Problem

RateMyProf

Professor

Okay!

Ban whoever wrote this!

Subjective Judgment: Problem

Arbit

r

What went wrong?

User wasn't guaranteed access to service if they behave

How can we help Student share his thoughts?

- Anonymity
- Unlinkability
- Revocability
- Verifiability
- **Accessibility**
- Prior work **cannot** provide this!

Guaranteeing Access by Defining Policy First

Student

I agree!

RateMyProfs.com

Date	Class	E	H	C	RI	User Comments	Professors add your rebuttal here
4/3/09	[redacted]	5	5	5	5	[redacted] one of the most charismatic instructors I've ever had. She is engaging and keeps class interesting. She makes an effort to truly know all of her students. She is a gifted and committed teacher. Shanita's lessons extend far beyond the classroom. I am grateful to have had class with her.	
12/10/07	[redacted]	4	5	5	5	She is my favorite prof. She is fun, insightful, and very encouraging. I liked everything about the class except the fact she had some people come into class that were a waste of time but it was still a good class. at least i found out what I want to do w/ my major b/c of this class	
6/1/07	[redacted]	5	5	5	3	Although I felt like this class was a little bit suited for kids at time (you play a lot of games and group activities) it was easy and interesting, plus Shanita always energetic and willing to help you!	
5/22/07	[redacted]	5	5	5	5	I had [redacted] for Intro to Advertising. She is a great teacher. One that has a lot of energy, engages her students, and inspires. The way her class is structured is interesting as well. She gives us feedback and other classmates give feedback for your project/presentation. She is more fair than any of the other instructors in the department.	
12/26/06	[redacted]	5	1	1	3	I was embarrassed to be in this class. It felt like kindergarden. I coudln't believe I wasted tuition $ on it. We sat around in circles and drew pictures to put on the walls. If this is college - I was prepared before elementary school. An embarrassment. Insulting to our intellegence. A joke. I learned nothing and wasted a lot of money.	

If you don't swear, you can use the service and be anonymous and unlinkable.

Motivating Example

RateMyProfs.com

Date	Class	E	H	C	RI	User Comments	Professors add your rebuttal here
4/3/09	[redacted]	5	5	5	5	[redacted] one of the most charismatic instructors I've ever had. She is engaging and keeps class interesting. She makes an effort to truly know all of her students. She is a gifted and committed teacher. Shanita's lessons extend far beyond the classroom. I am grateful to have had class with her.	
12/10/07	[redacted]	4	5	5	5	She is my favorite prof. She is fun, insightful, and very encouraging. I liked everything about the class except the fact she had some people come into class that were a waste of time but it was still a good class. at least i found out what I want to do w/ my major b/c of this class	
6/1/07	[redacted]	5	5	5	3	Although I felt like this class was a little bit suited for kids at time (you play a lot of games and group activities) it was easy and interesting, plus Shanita always energetic and willing to help you!	
5/22/07	[redacted]	5	5	5	5	I had [redacted] for Intro to Advertising. She is a great teacher. One that has a lot of energy, engages her students, and inspires. The way her class is structured is interesting as well. She gives us feedback and other classmates give feedback for your project/presentation. She is more fair than any of the other instructors in the department.	
12/26/06	[redacted]	5	1	1	3	I was embarrassed to be in this class. It felt like kindergarden. I coudln't believe I wasted tuition $ on it. We sat around in circles and drew pictures to put on the walls. If this is college - I was prepared before elementary school. An embarrassment. Insulting to our intellegence. A joke. I learned nothing a[redacted] wasted a lot of money.	

Student

Professor

I don't like this class.

I give up.

How can we help Student share his thoughts?

- Anonymity
- Unlinkability
- Revocability
- Verifiability
- Accessibility

Contractual Anonymity

- What I described is **Contractual Anonymity**
  - Obey policy and get anonymity/access
  - Don't obey policy and don't get anonymity/access
- **Strong guarantees**
  - User can not be banned on a whim
  - User can not be de-anonymized on a whim
- We design and implement the first contractual anonymity protocol, **RECAP**

Remaining Agenda

- Background: Trusted Computing
- Design of RECAP (protocol for achieving contractual anonymity)
- Implementation
- Measurements
- Conclusion

RECAP: Insight

- Group signature scheme was insufficient because we trusted a third party without reason

- We can make the third party a program constrained by trusted computing
  - Trusted computing can remotely convince user that their **identity is only handled by trusted code** with known behavior
  - We call this program the **accountability server**

Background: Trusted Computing

- **Attestation**
  - Conveys information about what software is running
- **Sealed storage**
  - Allows a program to keep data secret while it is not running
- **Hardware-assisted isolation**
  - Allows a program to keep data secret while it is running
  - Greatly reduces Trusted Computing Base (TCB)
- For RECAP: Remotely convince user and SP how third party will operate
  - Only reveals identity if user violates policy

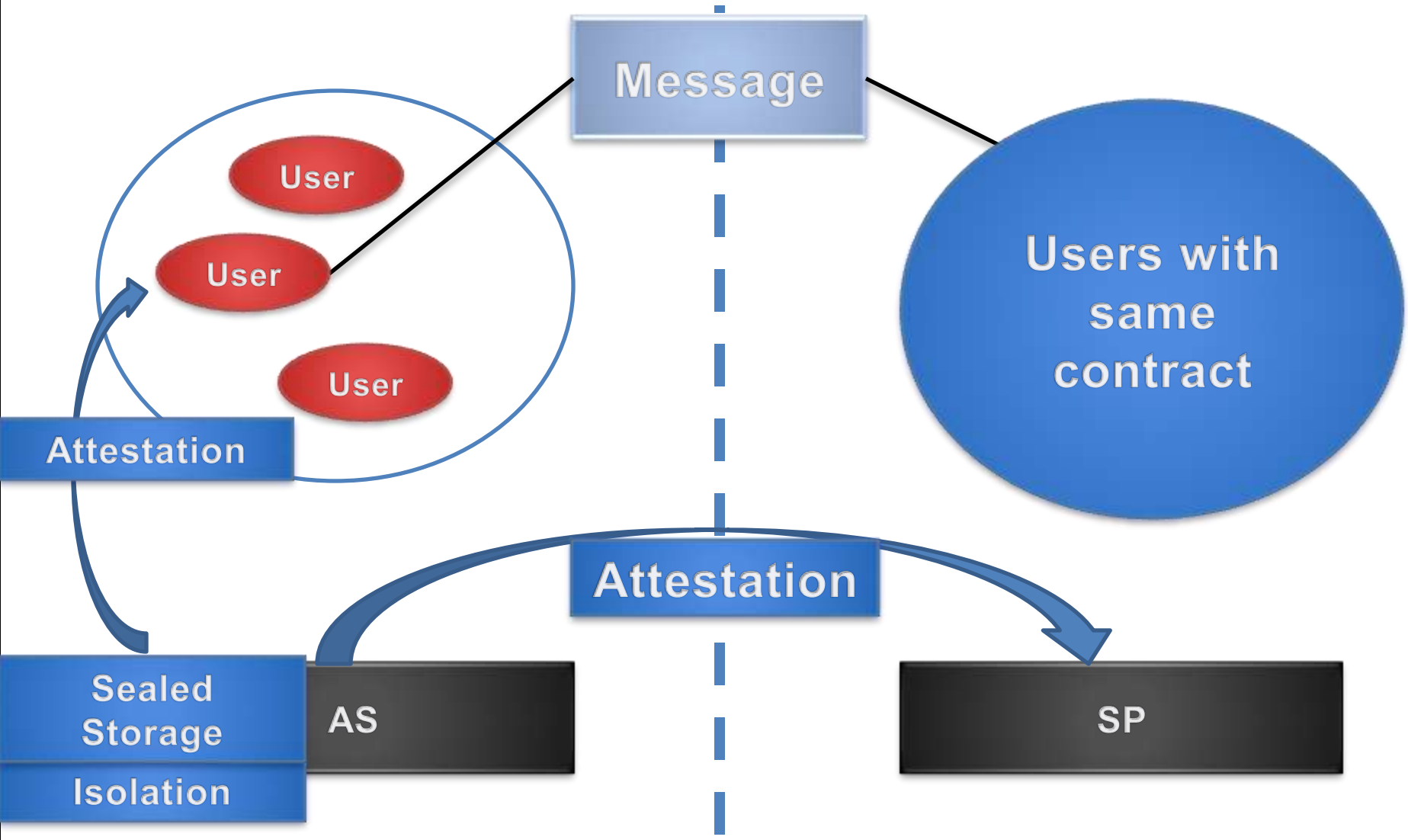
AS: Policies

- The AS is constrained to enforce a **policy**
- Policies define **bad behavior**
  - Any function f: Message(s) -> {Good,Bad}
- Examples
  - Pattern matching
    - E.g., swearing, spam, known malware
  - Designate authority to digital signature private key
  - Group voting/self-moderation

RECAP Protocol

- **Setup**
  - Group manager is the Accountability Server
  - Users join group by sending long-term identity to AS and agreeing to policy
- **Message sending**
  - **Example:** Student wants to send a rating
  - He creates a group signature
  - RateMyProf verifies group signature
- **Revocation**
  - **Example:** User posts review full of links (spam)
  - SP sends offending message to AS
  - AS can look up offender's long-term identity only if policy(messages) returns bad

Why Does It Work?



Implementation of Protocols

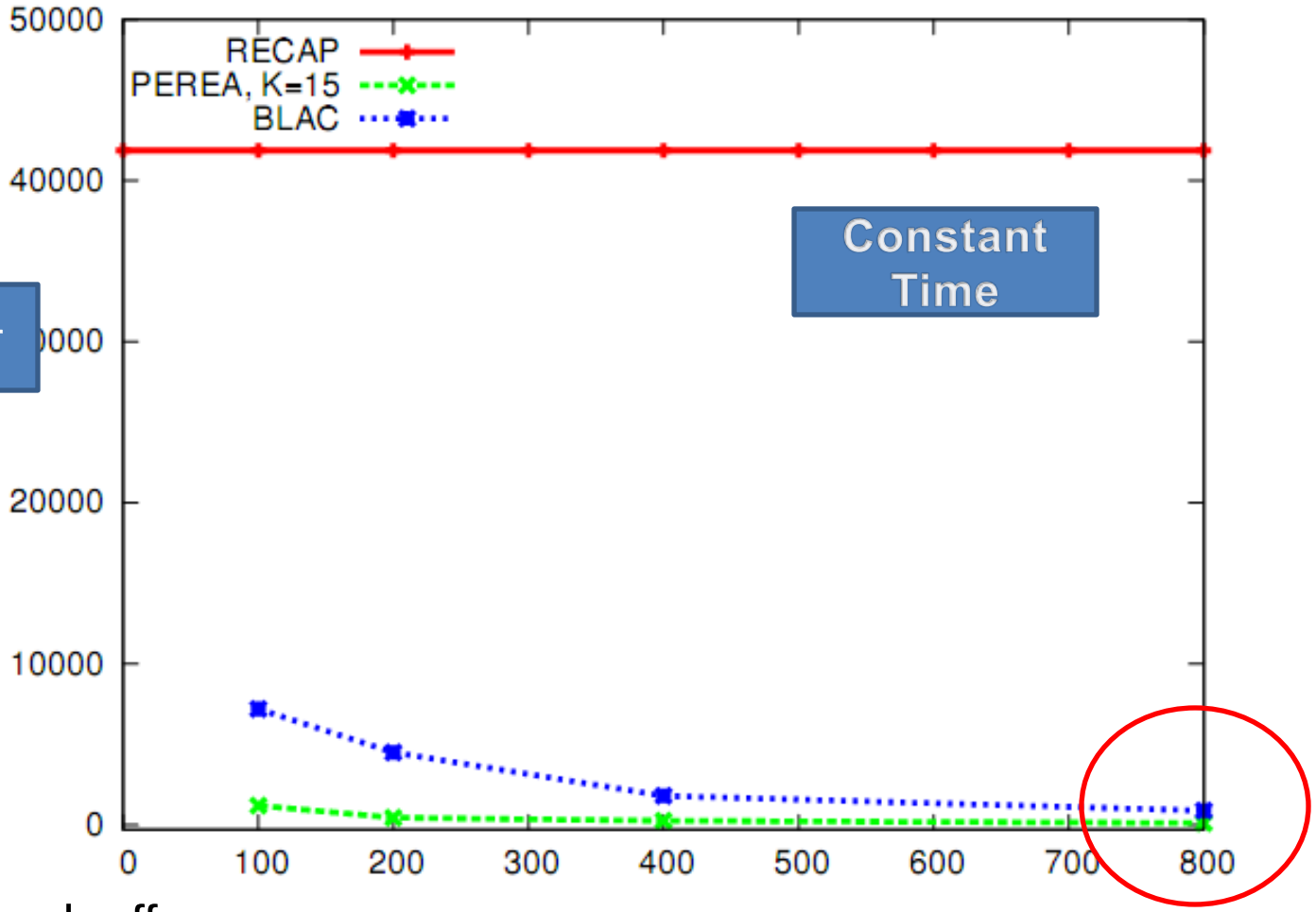
- **Message sending** is group signature generation/verification

- **Setup/Revocation**
  - Require special secure channel
    - Established between keys **demonstrated to be known only to trusted code**
    - **Uses trusted computing**
    - Protocols are straightforward after channel setup
  - Secure channel and protocols detailed in paper

Implementation

- **Trusted computing**
  - Uses **Flicker** system [McCune et al. 08] for trusted computing
    - Runs on commodity PC hardware
  - Long term identities are unique trusted computing identifiers
    - No need to register in person, etc.
- **Group signatures**
  - Uses group signature scheme of [Boneh and Shacham BS04]
  - Tradeoff: Complete unlinkability xor O(1) operations
    - We choose: small fraction (~1/1024) of messages linkable and O(1) operations
    - Optional choice in group signature implementation

Message Sending Throughput at the User



Messages/hour

Constant Time

# of Banned Users

- Remember tradeoff
- PEREA/BLAC numbers from their paper

Measurements

- RECAP has short **message sending time**
  - Takes about **0.1s** for user and SP, **O(1)** wrt size of blacklist
- The **registration protocol and revocation protocol** takes approximately **8.0s**, but happen rarely
  - And, we know how to make them faster

Trusted Code Size is Small

- AS RECAP Code: **3000 lines**
- Crypto/Drivers: **32000 lines**

- **This is the entire Trusted Computing Base**

Conclusion

- We propose **contractual anonymity**
  - Balances anonymity & accountability
- We implement the first contractual anonymity protocol, **RECAP**
- RECAP makes two primary contributions
  - RECAP has high throughput
  - RECAP does not allow users to be blacklisted without reason

Questions?

- edmcman@cmu.edu

Thanks!