Applying Secret Sharing Schemes to Service Reputation

Akbar S. Namin, Ruizhong Wei, Weiming Shen, Hamada Ghenniwa
IMTI – NRC, Lakehead University, The University of Western Ontario
CSCW 2005

NRC·CNRC
Canada Institute for Scientific and Technical Information

Agenda

- Introduction
- Challenges
- Related Work
- Secret Sharing Schemes
- An Extension to UDDI
- A Secret Sharing Model for Service Reputation
- Discussion
- Conclusion
- Questions & Answers

NRC·CNRC
Canada Institute for Scientific and Technical Information

Introduction

- Enterprise Collaboration
  - Service provider
  - Service consumer
- Service-Oriented Computing
- Agent-Oriented Computing

NRC·CNRC
Canada Institute for Scientific and Technical Information

Challenges

- *Collaboration with unknown enterprises?*
- *Is the current standard of UDDI adequate?*
- *Reliable reputation information: How and Who?*
- *Trust in Service-Oriented paradigm?*
- *Unconditionally secure reputation information?*
- *Not only reliable but also globally acceptable information?*

NRC·CNRC
Canada Institute for Scientific and Technical Information

Related Work

- *Amazon, eBay, etc.*
  - *A cumulative insecure rating measure*
  - *Pollyanna effect: disproportionately positive, rare negative*
- *Reputation:*
  - *“An opinion or view of one about something” (Sabater et al.)*
- *Some Related Work*
  - *Mui et al.: probabilistic model for reputation based on Bayesian network*
  - *Yu et al.: Applying Dempster-Shafer evidence theory*
  - *Maximilein et al.: Web Service Agent Proxy (WSAP)*

NRC·CNRC
Canada Institute for Scientific and Technical Information

Secret Sharing Schemes

- *Providing Security among some entities*
- *Participants:*
  - *Dealer D*
  - *Qualified entities*
- *Qualified subsets are able to reveal the secrets*
- *Any un-qualified subset had no knowledge about the secret*
- *Metering Schemes*

NRC·CNRC
Canada Institute for Scientific and Technical Information

Shamir's (t, n) Threshold Scheme

- *The Dealer D chooses::*
  - *A random number* $k \in \mathrm{K}$ *as secret key.*
  - *A large prime number* $q > Max(k, n)$
  - *Defines* $a_0 = k$
  - *Chooses* $t-1$ *random numbers as* $a_1, \ldots, a_{t-1} \in \mathrm{Z}_q$
  - *Forms a polynomial:*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} (\mathrm{mod}\, q)$$

  - *Chooses n random numbers* $x_i \in \mathrm{Z}_q$
  - *Computes n values*

$$y_i \ni y_i = f(x_i); \forall 1 \le i \le n$$

  - *The* $s_i = (x_i, y_i) \in S$ *are n secret shares* $f(0) = a_0 = k$
  - *Any group* $g \ni | g | = t$ *computes coefficients and finally reveals the secret*

NRC·CNRC
Canada Institute for Scientific and Technical Information

An Extension to UDDI

- *Current standard:*
  - *Registering*
  - *Searching*
  - *Interacting methods*
- *Shortcomings:*
  - *No reputation, credit information*
- *Extension UDDI with:*
  - *Reputation Knowledge*
  - *Reputation Agent*
- *Existing challenges:*
  - *Who and how and provides data for reputation Knowledge?*
  - *Transferring the overload computation to others! How?*

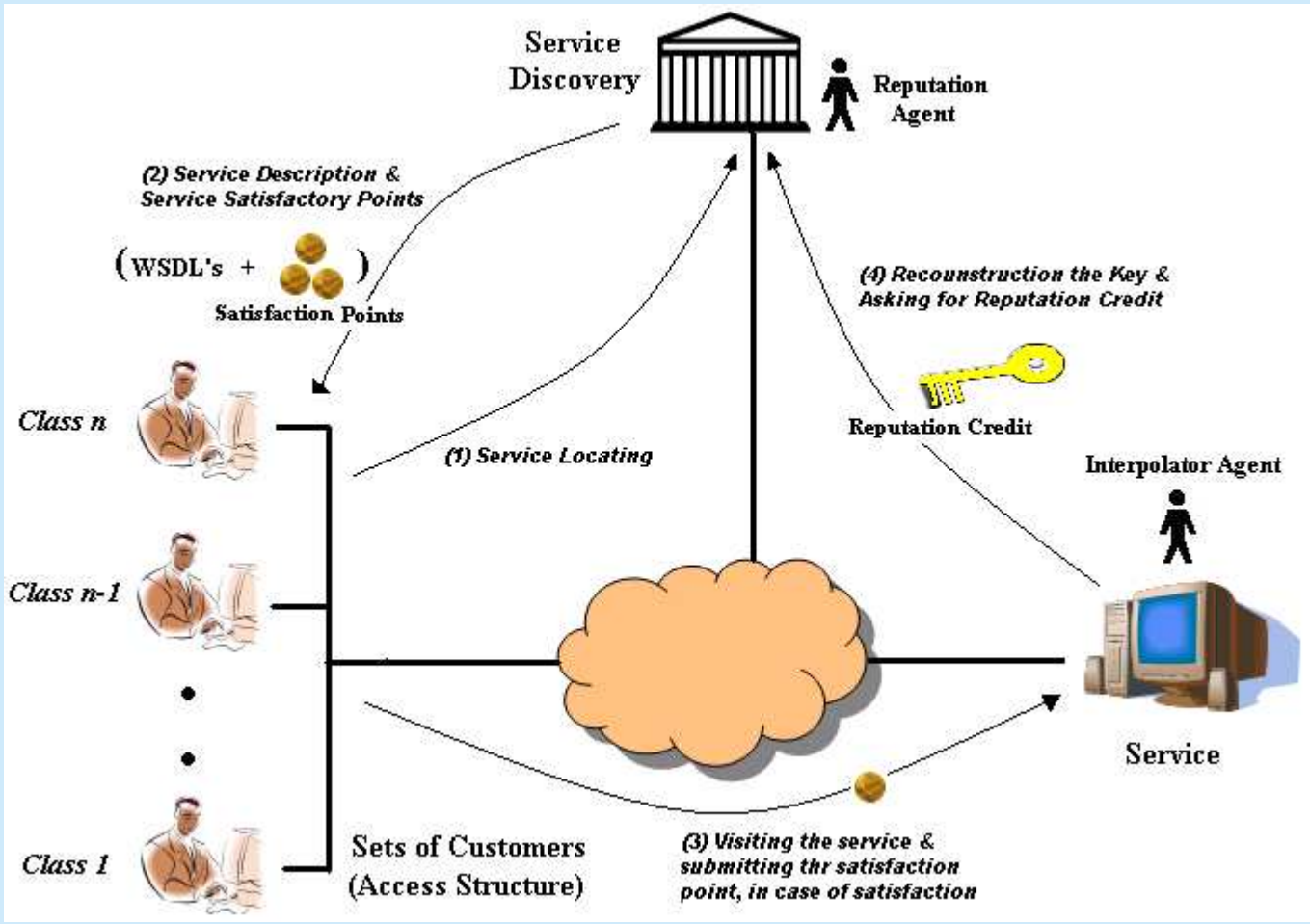
NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

- *Unconditionally Secure*
- *Applying Secret Sharing Schemes*
  - *Metering Schemes*
  - *Shamir's Threshold Scheme*
- *Employing Software Agents*
  - *Reasoning*
  - *Classifying Service (Providers, Consumers)*
  - *Differentiating between achieved credits from different service consumers*
- *Tokenizing Credits*
- *Globally Accessible Credits*

NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation



NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

1. Initialization
2. Generating Satisfaction Points
3. Applying Hash Function to Satisfaction Points
4. Sending Reputation Structures to the Interpolation Agent
5. Offering Encrypted Satisfaction Points to Clients
6. Satisfaction of Using a Service
7. Interpolating the secret values of reputation structures
8. Verifying the Revealed secret Keys

NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

i. Identifying client's business levels
   - Classifying clients level
   - Based on their business activities
   - Differentiate between clients by their credits and reputation

ii. Creating the reputation structures
   - Creating some threshold schemes

iii. Reasoning about threshold and secret values for generated reputation structures
   - Assigning clients to some of these structures
   - Eg. A reputation structure may consist of 4 ordinary members and one high class member (total = 5)

1. Initialization Stage
2. Generating Satisfaction Points
3. Applying Hash Function to Satisfaction Points
4. Sending Reputation Structures to the Interpolation Agent
5. Offering Encrypted Satisfaction Points to Clients
6. Satisfaction of Using a Service
7. Interpolating the secret values of reputation structures
8. Verifying the Revealed secret Keys

NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

- The reputation agent:
  1) #Satisfaction Points = |Threshold|
  2) Dividing k_m into r_m pieces
  3) Choosing h polynomial (degree = $t_m - 1$)

$$a_0^m + a_1^m x_m + \ldots + a_{t_m-1}^m x_m^{t_m-1} (\mathrm{mod}\, q_m)$$

  4) a_0^m = secret keys
  5) Computes $y_\theta = q_m(x_\theta)(\mathrm{mod}\, q_m), \forall 1 \le \theta \le r_m$
  6) The pairs $s_\theta = (x_\theta, y_\theta)$ are r_m Satisfaction points

1. Initialization Stage
2. Generating Satisfaction Points
3. Applying Hash Function to Satisfaction Points
4. Sending Reputation Structures to the Interpolation Agent
5. Offering Encrypted Satisfaction Points to Clients
6. Satisfaction of Using a Service
7. Interpolating the secret values of reputation structures
8. Verifying the Revealed secret Keys

NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

- For validation purposes (validation of satisfaction points)
- Reputation Agent
  i. Applying Hash function
  ii. Sending to Interpolator Agent
- Interpolator Agent
  i. Storing in Hash Table
  ii. Receives satisfaction points
  iii. Applying hash function
  iv. Comparing the equality
  v. Removing from Hash table (security of using once)

1. Initialization Stage
2. Generating Satisfaction Points
3. Applying Hash Function to Satisfaction Points
4. Sending Reputation Structures to the Interpolation Agent
5. Offering Encrypted Satisfaction Points to Clients
6. Satisfaction of Using a Service
7. Interpolating the secret values of reputation structures
8. Verifying the Revealed secret Keys

NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

- Interpolator Agent to interpolate:
  - i. Needs some knowledge about reputation structures
  - ii. Their participants
  - iii. Their threshold values

Therefore,

- Reputation Agent:
  - i. Sends them to Interpolator Agent

1. Initialization Stage
2. Generating Satisfaction Points
3. Applying Hash Function to Satisfaction Points
4. Sending Reputation Structures to the Interpolation Agent
5. Offering Encrypted Satisfaction Points to Clients
6. Satisfaction of Using a Service
7. Interpolating the secret values of reputation structures
8. Verifying the Revealed secret Keys

NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

- To have protected and secured model, the reputation agent:
  i. Encrypts the satisfaction points by using public key of a service client

Therefore,

- Only the owner of appropriate secret key is able to reveal it.

1. Initialization Stage
2. Generating Satisfaction Points
3. Applying Hash Function to Satisfaction Points
4. Sending Reputation Structures to the Interpolation Agent
5. Offering Encrypted Satisfaction Points to Clients
6. Satisfaction of Using a Service
7. Interpolating the secret values of reputation structures
8. Verifying the Revealed secret Keys

NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

- In case of satisfaction of using a service:
- The consumer:
  i. Sends the (one) satisfaction point to the provider.
- The interpolator agent:
  i. Validates the satisfaction point by hash function
  ii. Collect them for interpolation

1. Initialization Stage
2. Generating Satisfaction Points
3. Applying Hash Function to Satisfaction Points
4. Sending Reputation Structures to the Interpolation Agent
5. Offering Encrypted Satisfaction Points to Clients
6. Satisfaction of Using a Service
7. Interpolating the secret values of reputation structures
8. Verifying the Revealed secret Keys

NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

- The Interpolator Agent:
  - i. Has all needed knowledge for interpolation (i.e. Reputation structure, threshold values, members).
  - ii. By collecting t_m Interpolate the secret value for threshold scheme (t_m, r_m)
  - iii. Interpolation: System of equation and Lagrange method.

1. Initialization Stage
2. Generating Satisfaction Points
3. Applying Hash Function to Satisfaction Points
4. Sending Reputation Structures to the Interpolation Agent
5. Offering Encrypted Satisfaction Points to Clients
6. Satisfaction of Using a Service
7. Interpolating the secret values of reputation structures
8. Verifying the Revealed secret Keys

NRC·CNRC
Canada Institute for Scientific and Technical Information

A Secret Sharing Model for Service Reputation

- The Interpolator agent:
  i. Sends the secret value to Reputation agent
- The Reputation Agent:
  i. Verifies it and decides to increase the credit
- Any measurable unit (eg. [0, 100])

1. Initialization Stage
2. Generating Satisfaction Points
3. Applying Hash Function to Satisfaction Points
4. Sending Reputation Structures to the Interpolation Agent
5. Offering Encrypted Satisfaction Points to Clients
6. Satisfaction of Using a Service
7. Interpolating the secret values of reputation structures
8. Verifying the Revealed secret Keys

NRC·CNRC
Canada Institute for Scientific and Technical Information

Discussion

- Benefits of using software agents in threshold schemes:
  - Forming reputation structures
  - Dynamic revision of created reputation structures
    - Changing the number of shares in a threshold scheme (new polynomial)
    - Changing the number of existing participants of a structure (increasing the numbers and decreasing the sensitivities)
- Limitation of the model
  - Service provider is not able to claim unless collecting a specific number of satisfaction points.
- Despite above Limitation
  - Security is guarantied

NRC·CNRC
Canada Institute for Scientific and Technical Information

Conclusion

- Discussed
  - Service-oriented computing as emerging paradigm
  - existing challenges with service-oriented computing
- Needs
  - A secure, globally accepted mechanism for reputation credits
- Proposed An unconditional secure model for reputation
  - Extending UDDI to two more components
  - Adopting secret sharing schemes (Threshold schemes)
  - Classifying business level of services (providers, consumers)
  - Constructing some reputation structures
  - Adopting software agents to address dynamic generation and modification of reputation structures

NRC CNRC

Canada Institute for Scientific and Technical Information

Thanks

Q & A

Science at work for Canada

National Research Council Canada | Conseil national de recherches Canada

Canada