

Algorithms for the Technology of Trust

Michael T. Goodrich, Univ. California, Irvine

<http://www.ics.uci.edu/~goodrich/>

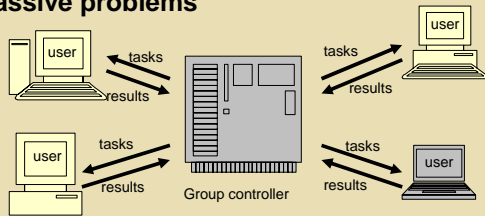


Design efficient algorithms for scalable security

Finding fast and low-overhead security solutions to problems dealing with scalable clients in distributed environments.

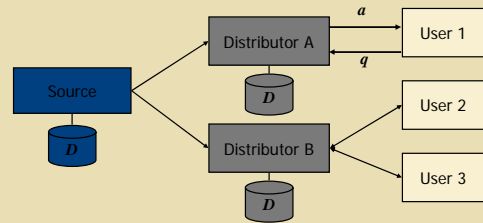
Distributed Grid Computing

Use peer-to-peer technology to unlock the potential of using up to millions of computers across the Internet to solve massive problems



Dr. David Anderson, director of SETI@home:

"Fifty percent of [our] resources are devoted to security problems. ... The hard part is when we get data back, how do we know it was computed by our program? People have tried to modify the program to run faster, some have modified it to create incorrect answers, some to make it look they're doing a lot of work, even though they're not, so they could climb up the leader boards."



Authenticated Data Structures

Source signs time-stamped message $m=g(D)$
Answer a includes $proof(a)$ and $m//\sigma$
Function g : any answer a , using $proof(a)$, can be verified, by verifying the signature σ on m

Approach and Impact

Security in the Large

- P2P search structures
- IP Traceback
- Grid security

Research Impact

- Data content authentication
- Uncheatable Grid computing
- Rainbow skip-graphs

P2P Secure Search Problem

Given:

- n hosts with one (key, value) pair each
- Routing layer supporting message passing $send(message, destination_address)$
- Adversary can kill hosts at random using a virus

Support neighbor queries on keys

Return value of key nearest a given key

Application:

- Medical information sharing (e-Health networks)
- Approximate matching is important

Our Solution: The Rainbow Skip Graph

