CERIAS

The Center for Education and Research in Information Assurance and Security

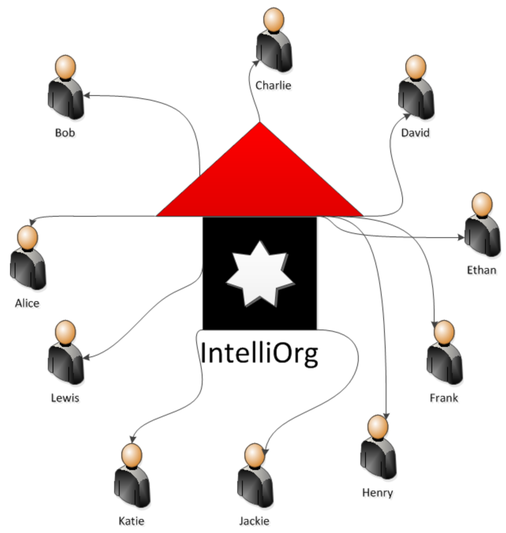
PURDUE UNIVERSITY

Private Anonymous Messaging

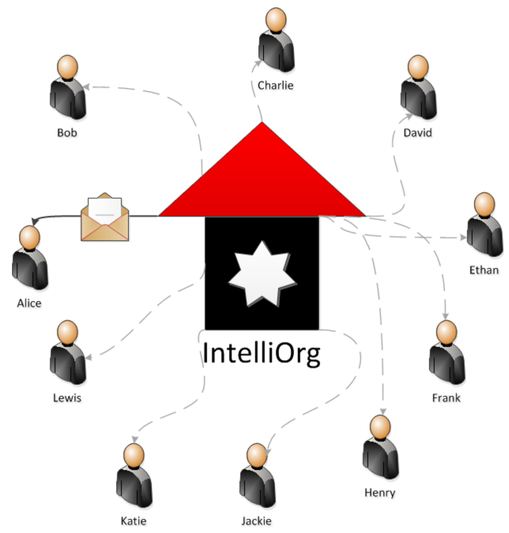
Ruchith Fernando, Bharat Bhargava

Department of Computer Science & The Center for Education and Research in Information Assurance and Security

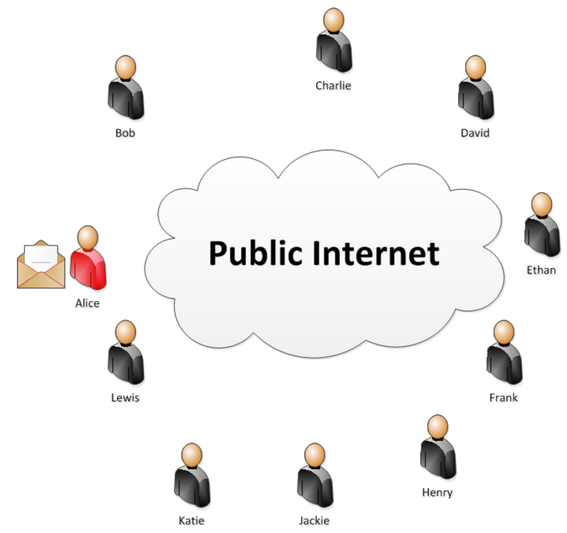
Purdue University



Secret Agents of intelliOrg



Message sent to the only available agent

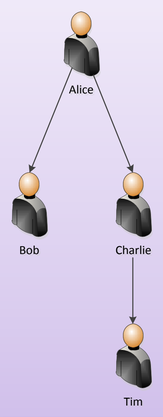


The organization is no longer accessible and other agents need the message

Requirements

- Dynamic set of agents
- Agents do not know each other
- Obtain messages from other agents
- Use public network
- Requester and provider anonymity

Hierarchical Identity Based Encryption



Key Generation by Alice

Setup → Params = P, Master Key = K

Alice, P, K → KeyGen → $K_{priv(Alice)}$

Bob, P, $K_{priv(Alice)}$ → KeyGen → $K_{priv(Bob)}$

Charlie, P, $K_{priv(Alice)}$ → KeyGen → $K_{priv(Charlie)}$

Key Generation by Charlie

Tim, P, $K_{priv(Charlie)}$ → KeyGen → $K_{priv(Tim)}$

Sending 'Msg' to Tim

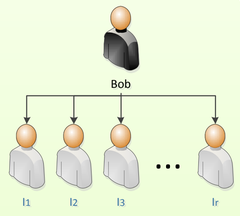
Msg, P, Alice, Charlie, Tim → Encrypt → Cipher Text

Cipher Text, $K_{priv(Tim)}$ → Decrypt → Msg

Proposed Scheme


Bob

- Select a random = $\boldsymbol{I_r}$
- $ID_r = {h_1}^{I_1} \cdot {h_2}^{I_2} \cdot {h_3}^{I_r}$
- $\boldsymbol{ID_r}$ is the request for data




Alice

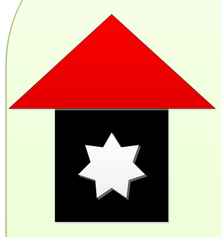
Msg, P, $\boldsymbol{ID_r}$ → Encrypt' → Cipher Text


Bob

I_r, P, $K_{priv(Bob)}$ → KeyGen → $K_{priv(r)}$

Cipher Text, $K_{priv(r)}$ → Decrypt → Msg

Group Membership Changes



$Master\ key = K$

$Kpriv(Agent) = ({g_2}^{K} \cdot (A^r), B^r, C^r)$

Generate a fresh master key = $\boldsymbol{K'}$

Regenerate $Kpriv(Agent_i)$ of all agents

Publish →

Blinded ID	Key Component
...	...
$(Agent_i)^{r'}$	${g_2}^{K'} \cdot (A^r)$
...	...

& r'


Alice

Use r' to create key to look up and locate ${g_2}^{K'} \cdot (A^r)$ component and update private key!

CERIAS

Discovery Park e-Enterprise Center