Alice in

Cyber world

Protecting Secrets in The Connected World

K.S.Sreedharan
Director IT Zoho

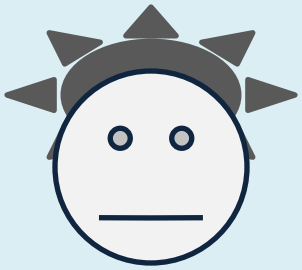
Cast

Alice

Eve

Claude

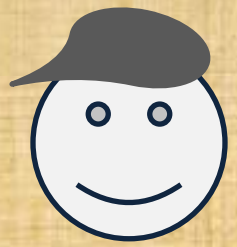
Bob



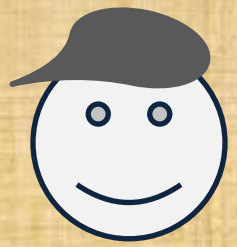
Govan

Story So Far

Symmetric Key



Asymmetric Key



Twist in the Tale

Claude Convenience

DIY Economy
Tom, Dick and Harry can run business too
Boom in startups

Reduce Costs
23% reduction in IT costs

Peeping Govan

GOOG

9000 - 9999

FB

5000 - 5999

MSFT

15,000 - 15,999

YHOO

30000 - 30999

Ever-present Eve

6Million LinkedIn passwords stolen

Jun 2012

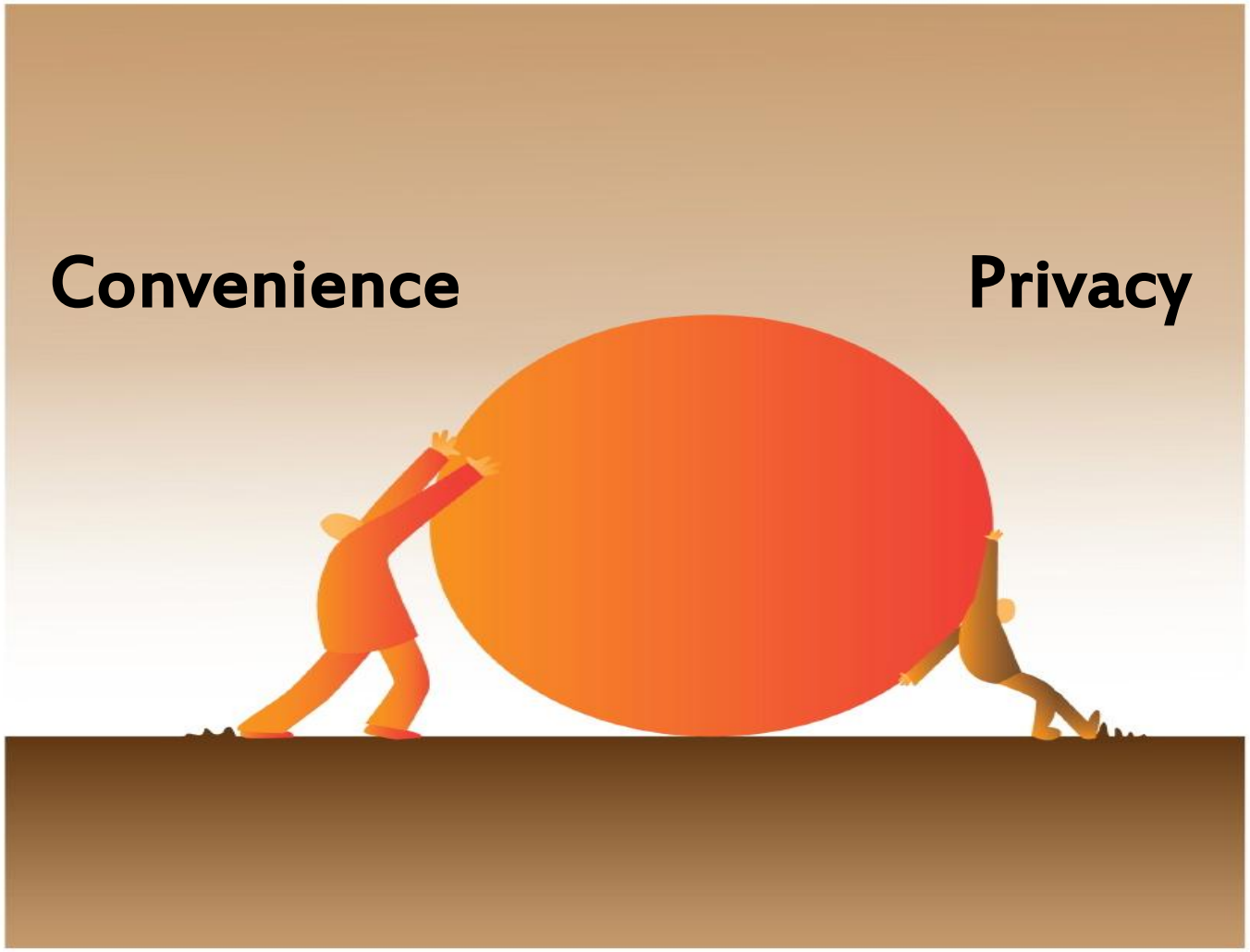
Yahoo email and passwords exposed

Jan 2014

Claude's Problem

U.S.-based cloud computing providers are projected to lose up to 20% of foreign market revenues or $35B over the next three years as a result of disclosures involving PRISM.

Alice's Quandary



Solution

The best answer to PRISM's abuses is strong cryptography in the hands of the public

Saving Private Data

Weak spots

- Transport
  - Sniffing
  - Stealing passwords
- Store
  - Key management
  - Sensitive data for calculation
- Rest
  - Key compromise

Transport Security

Transport Travails

- Snooping by Eve
  - BEAST
  - Session Negotiation Vulnerability
  - Passwords by interception
- Snooping by Govan
  - Improper Key exchange selection
  - Retrospective decryption from stored data

SSL Key Exchange

Server Certificate Private Key can be used to read communication

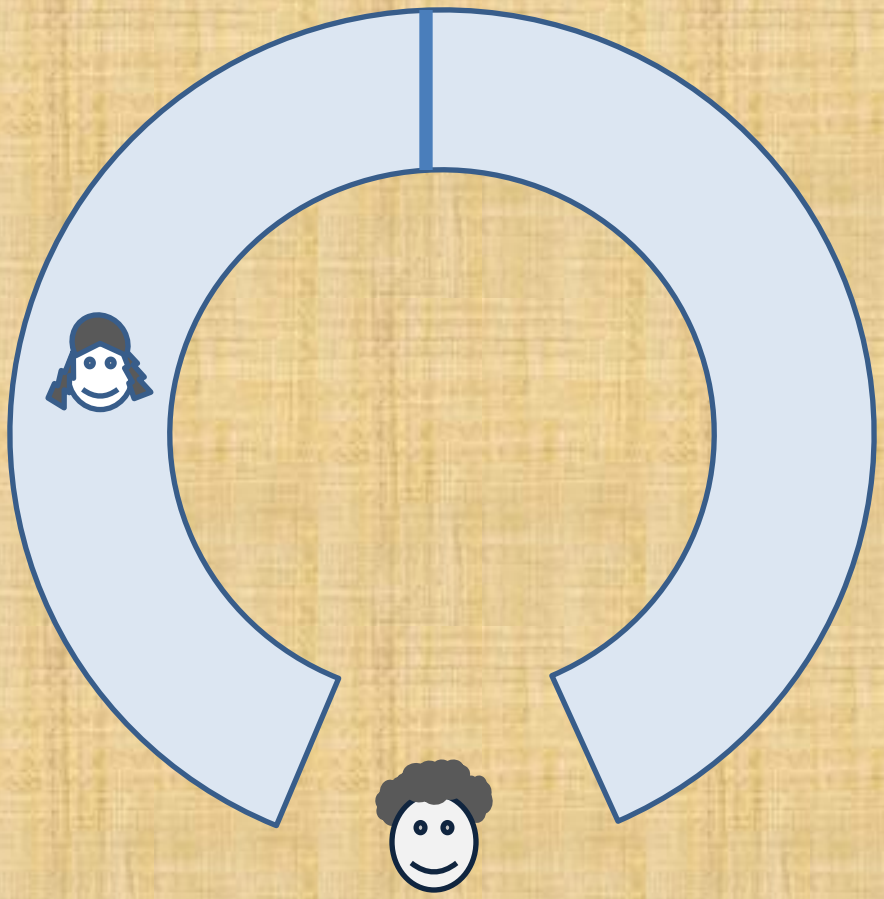
Forward Security

- Ephemeral Diffie-Hellman
  - Server generates a new Diffie-Hellman public key for each session and signs the public key.
  - The client also generates a public key
  - Using Diffie-Hellman they both generate a mutual session key
  - 15 -27 % overhead with ECDHE-RSA

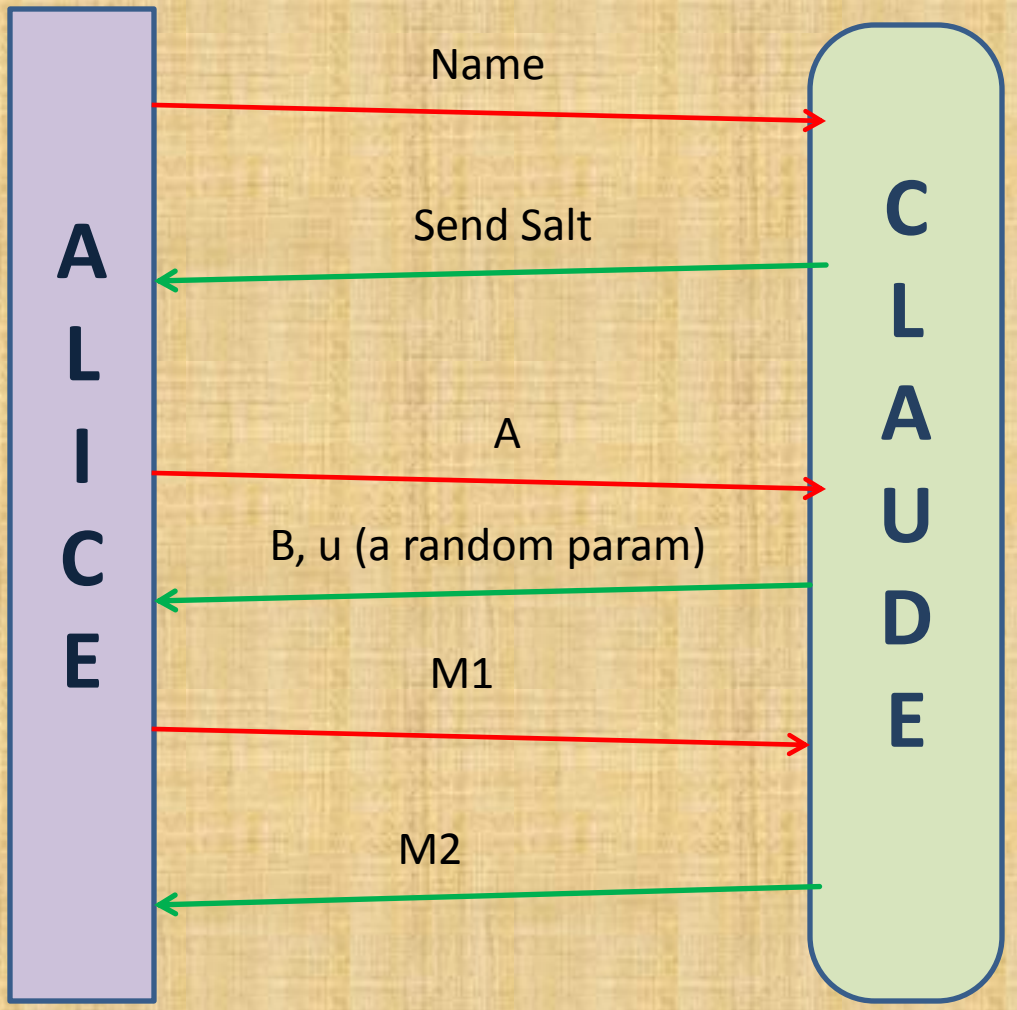
Securing Transport

- Always on Encryption
  - Session-wide encryption. *SSL default*
- Configuration
  - *Forward secrecy, Cipher Selection*
- Update Browser, SSL libraries
- Test
  - Ssllabs
  - Browser

Zero Knowledge Proof



ZKPP - SRP



LTPK = Hash of Salt and Password

Derive EPK A from random number

Compute CEP S & hash to derive K
M1=Hash(A,B,K)

Verify M2

Zero Knowledge Proof

- Do not send sensitive information at all
- Prove that a computation can be done without actually performing it
- Applications
  - *Authentication*
  - *Auctions*
  - *Financial transactions*
  - *Voting*

Store Security

Problems

- Overheads due to encryption
- Managing Keys and rotating them
- Preventing Key compromise
- Performing operations on data without exposing the data

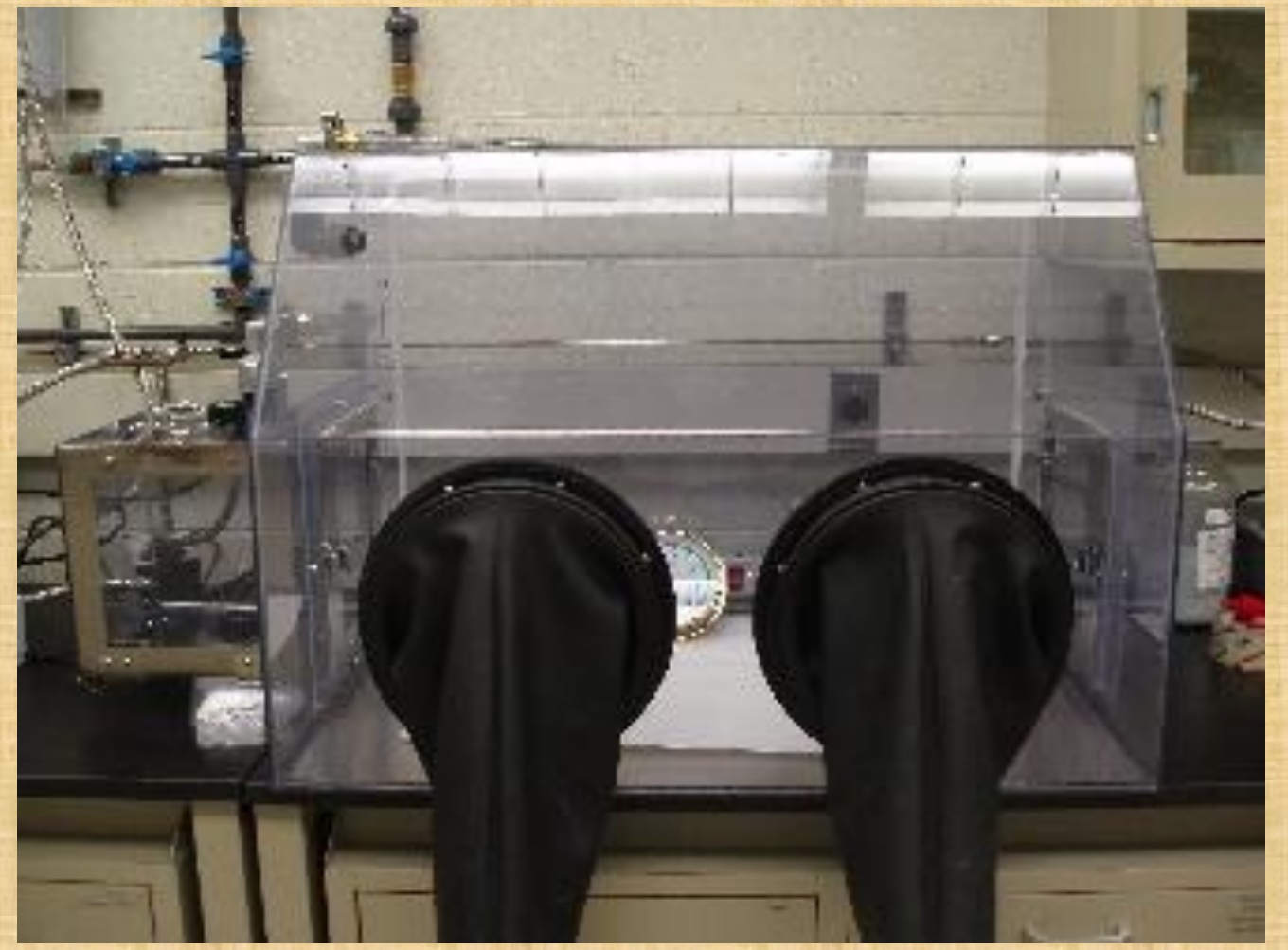
Split Key Management

- Key for data encryption
  - *Should be rotated*
  - *Encrypted using Master Key*
- Master Key Generated on initialization
- Master Key encrypted with Key encrypting Key and stored
- Key Encrypting Key generated from passwords from two custodians

Secret Computing

- Cryptographic Dark Room
  - *Information is encrypted by Alice*
  - *Evaluation function on encrypted data by Claude*
  - *Result in encrypted form sent to Alice*
  - *Alice decrypts and gets the result*
- *Applications*
  - *Encrypted Search terms*
  - *Computations*

FHE - GloveBox



Homomorphic encryption

- ROT 13
  - *Concat (HELLO WORLD) > HELLOWORLD*
  - *Concat(Enc(HELLO WORLD)) > URYYBJBEYQ*
  - *Dec(URYYBJBEYQ) > HELLOWORLD*
- *RSA*
  - $\epsilon(x1) = x1^e \bmod m$
  - $\epsilon(x2) = x2^e \bmod m$
  - $\epsilon(x1).\ \epsilon(x2) = (x1.x2)^e \bmod m = \epsilon(x1.x2)$

FHE

- Fully Homomorphic
  - Handle all functions
  - Has compact ciphertexts
  - Efficient for server and decryption for client
- Binary AND, OR, NOT operations will handle all functions
- Functions as circuits
- Work in Progress

An efficient and fully homomorphic encryption scheme would enable new kinds of distributed computing.

Security at Rest

Problems

- Key compromise
  - Claude storing keys
  - Claude giving the keys to Govan
  - Eve stealing it
- Control of Keys
  - Split control of Keys

Solutions

- Hardware Security Module
  - *Tamper Proof*
- Amazon Cloud HSM
- Tresorit
  - Encryption at Alice's end
- Porticor
  - Split control of Keys (Alice + Claude)
  - Partial homomorphic encryption

Cryptography forms the basis for trust online

Trust the math. Encryption is your friend. Use it well, and do your best to ensure that nothing can compromise it

Bruce Schenier


Thank You