# TRICIPHER

Strong Authentication for the Real World™

TriCipher Armored Credential System (TACS)

Slides provided by
Ravi Sandhu*
Co-Founder and Chief Scientist
TriCipher, Inc.
www.tricipher.com
sandhu@tricipher.com

•Also Professor of Information Security
and Assurance at George Mason Univ.

Pre-Access Online Fraud Prevention

User

Is this truly our customer?

Is her PC free of malware?
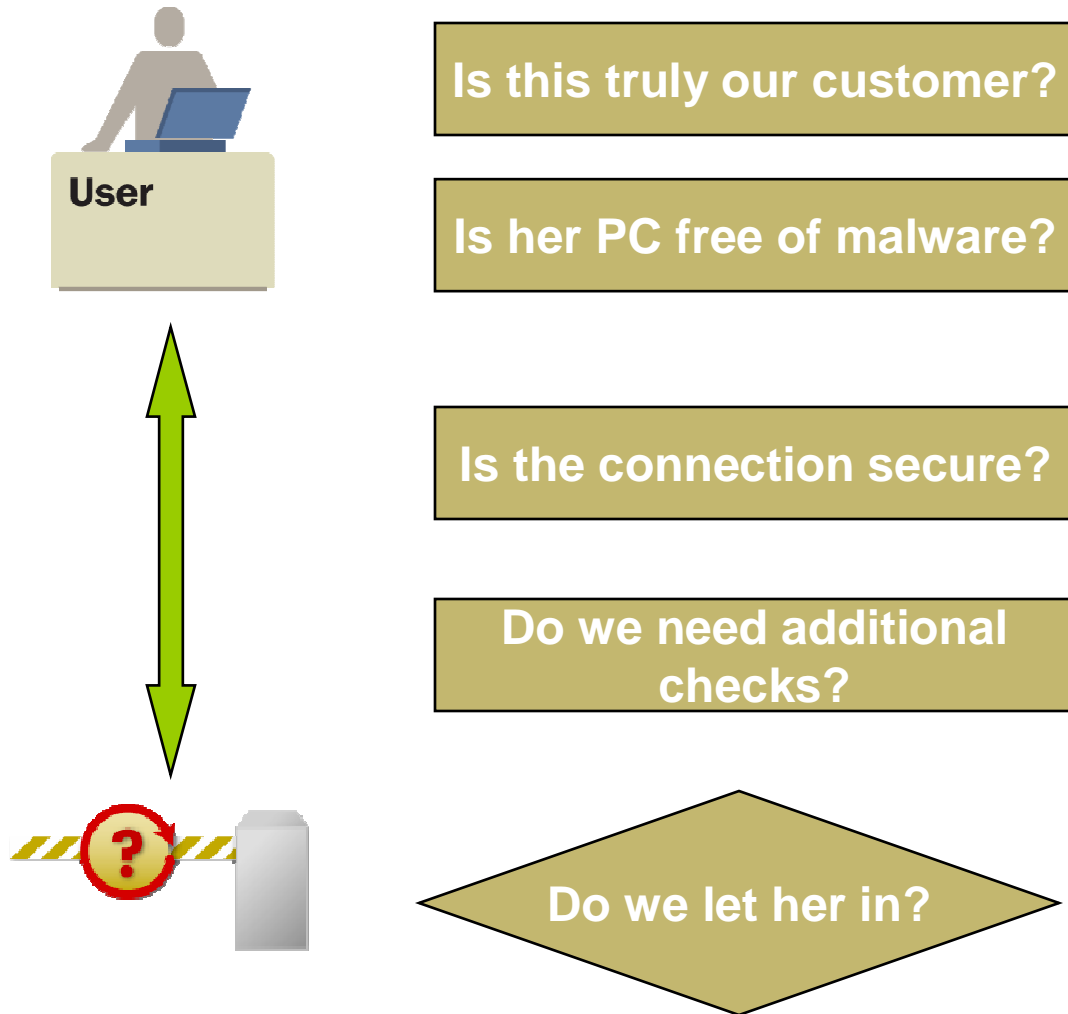
- *Which* of these can we know?
- How *certain* are we?
- How much *should* we care?
- How much can we *afford* to care?

Is the connection secure?

- Can we *prevent* criminals from getting access in the first place?

Do we need additional checks?

Do we let her in?

Post-Access Online Fraud Prevention

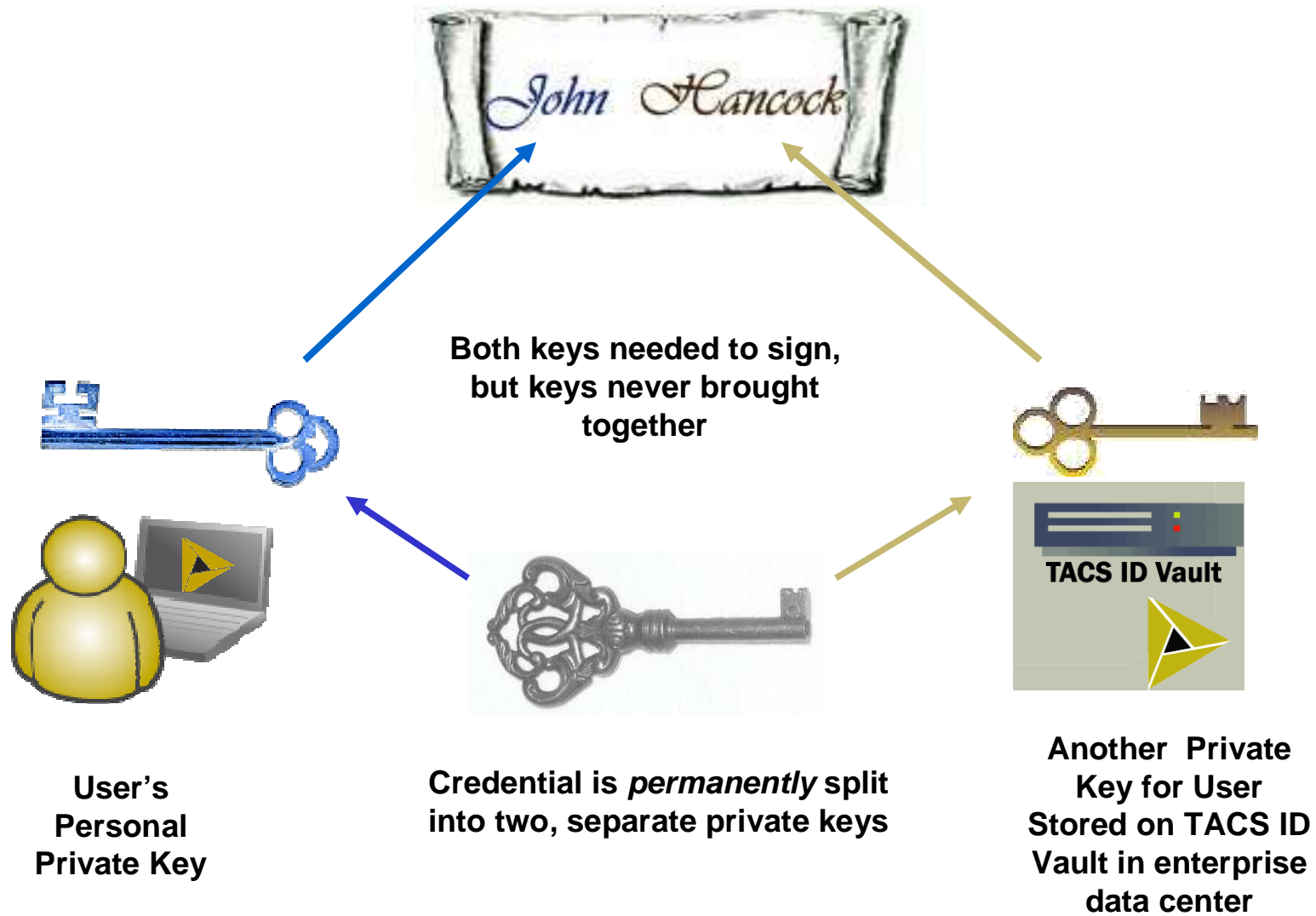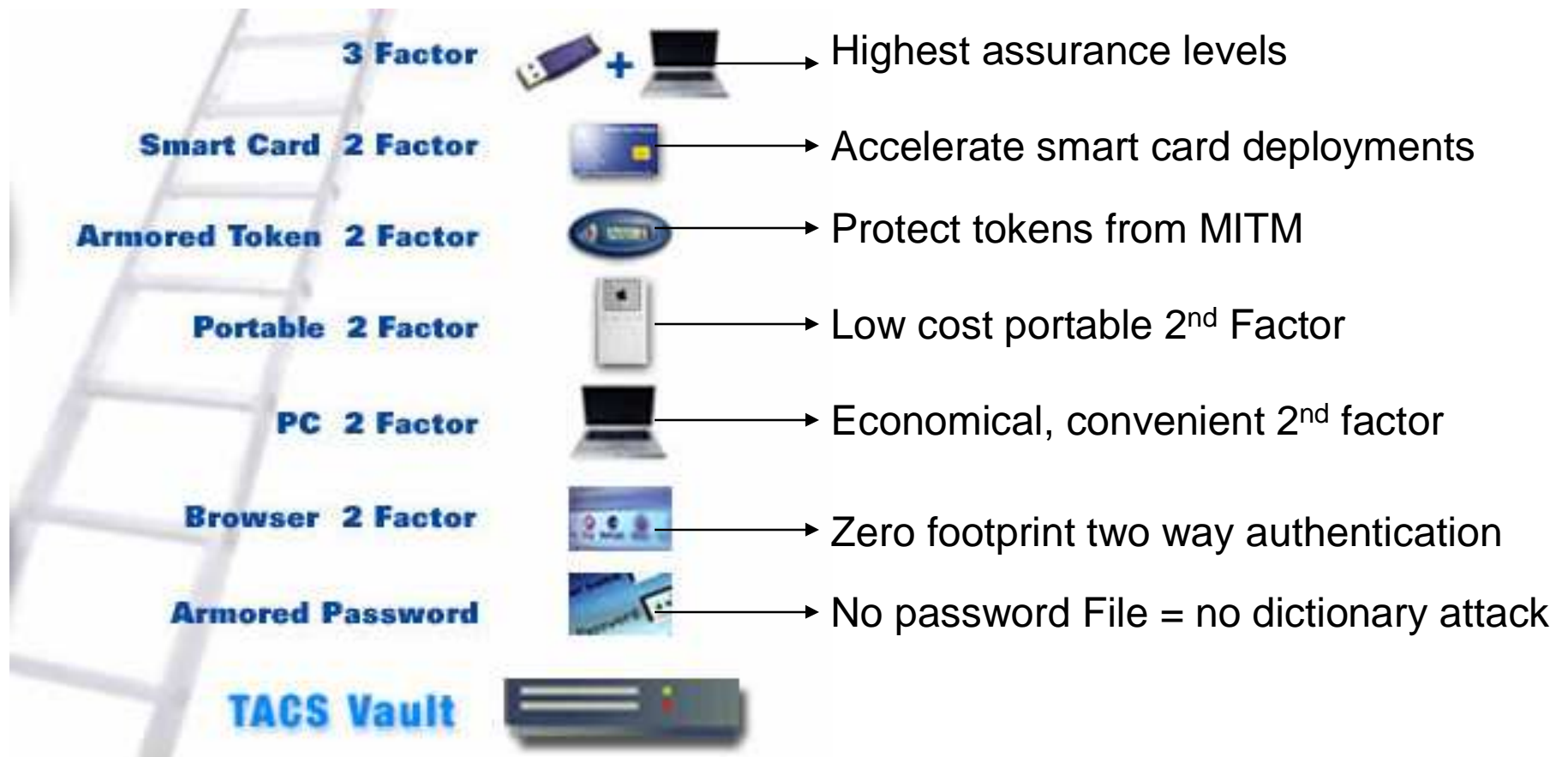| Are 'her' actions suspicious?	• What % do we catch? • What % do we 'catch' in error?
Do we need additional checks?	• How suspicious are we? •What methods can we use to double check the authentication?
Are we adequately protecting the credential in our data center?	•Are her credentials safe with us? • Is her identity data safe with us?

TACS Core Innovation: Multi-part Credentials

John Hancock

Both keys needed to sign, but keys never brought together

TACS ID Vault

User's Personal Private Key

Credential is *permanently* split into two, separate private keys

Another Private Key for User Stored on TACS ID Vault in enterprise data center

TACS Authentication Ladder

|		
3 Factor		Highest assurance levels
Smart Card 2 Factor		Accelerate smart card deployments
Armored Token 2 Factor		Protect tokens from MITM
Portable 2 Factor		Low cost portable 2nd Factor
PC 2 Factor		Economical, convenient 2nd factor
Browser 2 Factor		Zero footprint two way authentication
Armored Password		No password File = no dictionary attack
TACS Vault		

*All supported by a single infrastructure under a
perpetual licensing agreement!*

Protecting credentials/identity data
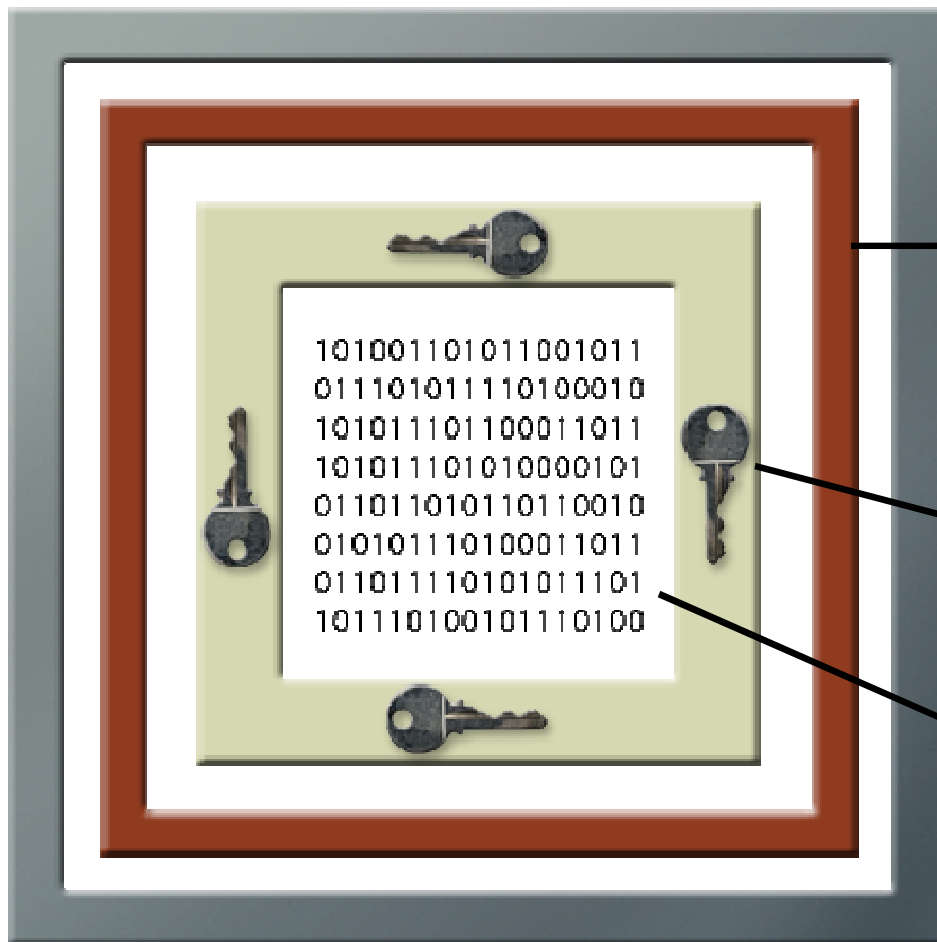
Appliance Architecture

- Locked down, dedicated hardened OS
- US Govt. FIPS 140-1 Level 2 rating

Compartmentalization layer

- All system and user administration strictly compartmentalized on least privilege, need to know, basis
- *Fortressed from insider attacks*

Strong Authentication layer

- Uses Multi-part credential technology
- Flexible authentication options

Result: An ID Data Vault

- Store encryption keys (or ID data)
- Only revealed to authorized party
- After strong authentication
- Support for group encryption, key escrow, etc.

Summary

TRICIPHER

- **Pre- and Post-Access Online Fraud Protection**
    - Prevent access *before* fraud occurs
    - Secondary authentication when back-end fraud detection systems get suspicious

- **Secure storage of identity data to prevent insider or mass theft**

- **Flexible deployment to balance security, cost and usability across a wide range of user needs**

Contact Information

Ravi Sandhu

sandhu@tricipher.com

703 283 3484

www.tricipher.com