

Security, Privacy & Trust in Ubiquitous Computing

Dr. Jaydip Sen

Innovation Lab

Tata Consultancy Services, Kolkata

Email: Jaydip.Sen@tcs.com

Outline

- The Vision of UbiComp -- According to Mark Weiser
- Trust, Security and Privacy
- Principle of Building Trust and Reputation Systems
- Commercial and Online Systems
- Problems and Proposed Solutions
- Conclusion

Ubiquitous Computing

Mark Weiser, Xerox PARC 1988

“Ubiquitous computing enhances computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user”



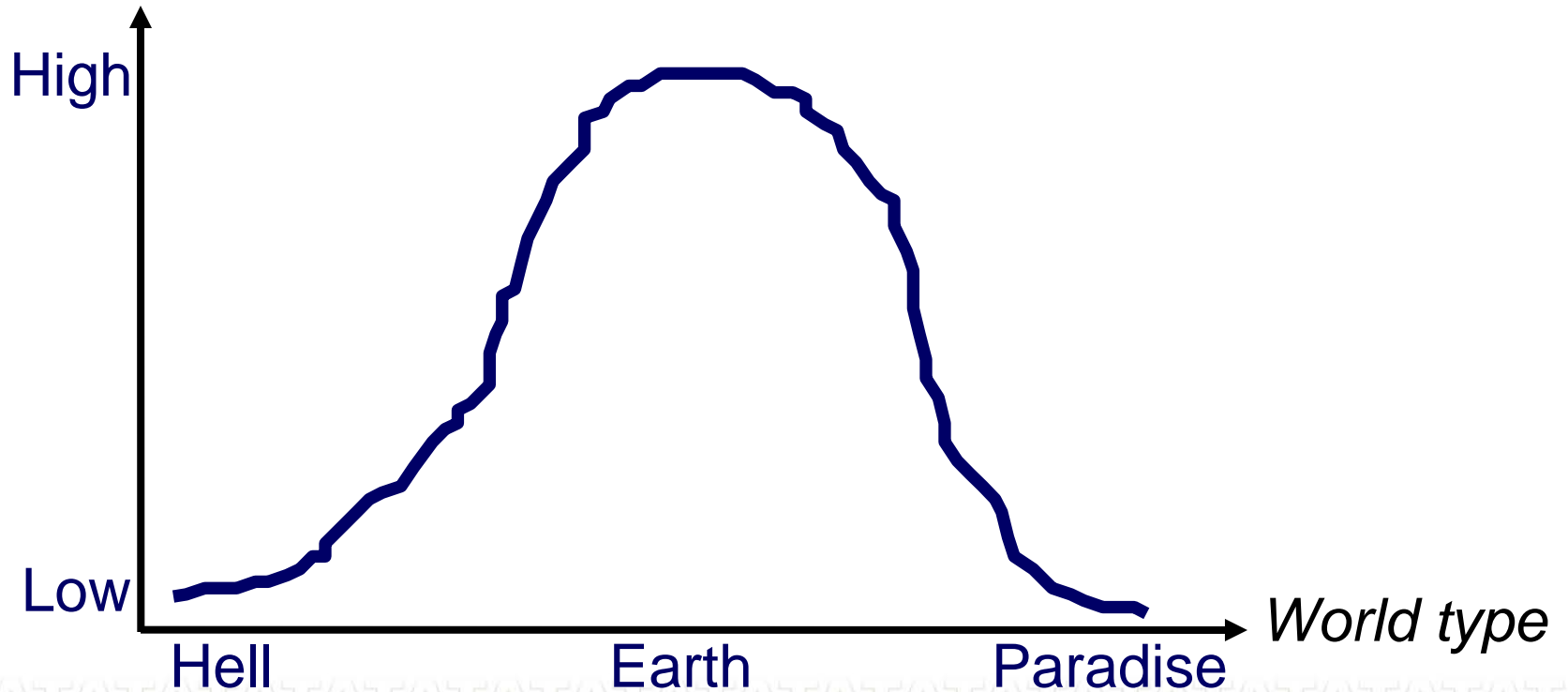
Security and Trust

- Interactions cross multiple organisational boundaries
- Lessons from history: **everything worth hacking gets hacked**
- Need for secure 'out of the box' set up
- Context aware adaptive security
- Identify friend or foe → level of trust
- Small communicators, with confidential data, are easily lost or stolen – biometric authentication?
- Trust based on experience + recommendations
- Credential validation with intermittent network connectivity



When is Trust Important ?

Trust importance



Two Definitions of Trust

- **Reliability trust**

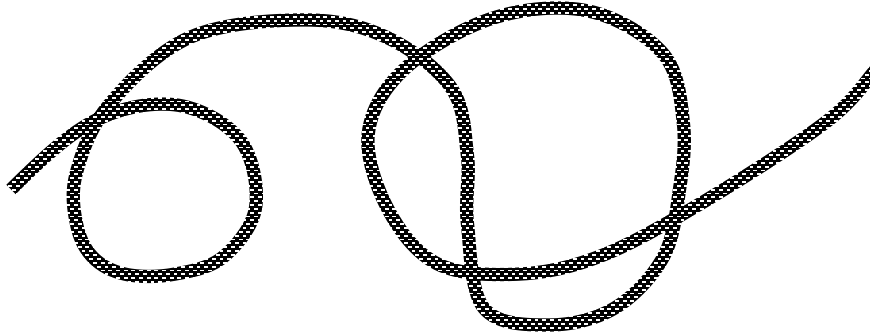
- The **subjective probability** by which an individual, *A*, expects that another individual, *B*, performs a given action on which its welfare depends. (Gambetta 1988)

- **Decision trust**

- The **willingness to depend** on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible. (McKnight & Chervany 1996)



Would You Trust This Rope ?



For what?

To climb down from the 3rd floor window of a house

The rope looks very old

Fire drill:

No!

Real fire:

Yes!

To Describe Complex Things in a Simple Way

- IT people like anthropomorphic expressions like:
 - Firewall, honeypot, virus, Trojan horse, digital signature, ..., ***trusted computing, circle of trust, ...***
- Anthropomorphic security expressions serve as
 - Simple descriptions of complex security concepts
 - Marketing slogans
- Trust expressions are often difficult to precisely understand



Trust Expressions

Trusted code

Trust context

Trust management

Trustworthy computing

Direct trust

Trusted Computing Base

Trusted system

Trusted computing

Indirect trust

Trust transitivity

Trust scope

Trust bar

Trust negotiation

Trust system

Trust provider

Circle of trust

Trusted Third Party

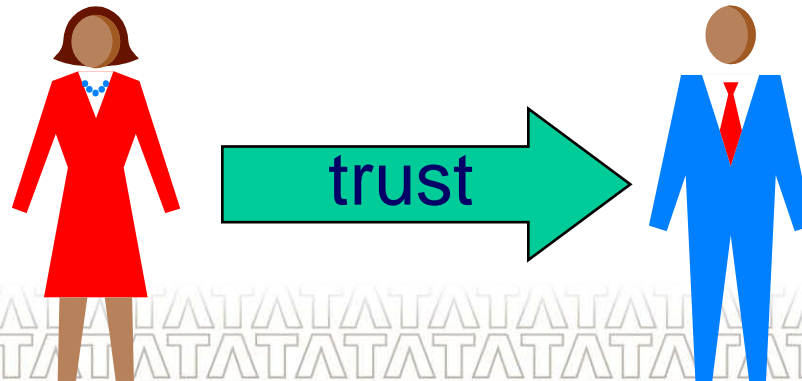
Two Sides of Trust Management

Trusting party

Wants to **assess** and make **decisions** w.r.t. the dependability of the trusted party for a given transaction and context

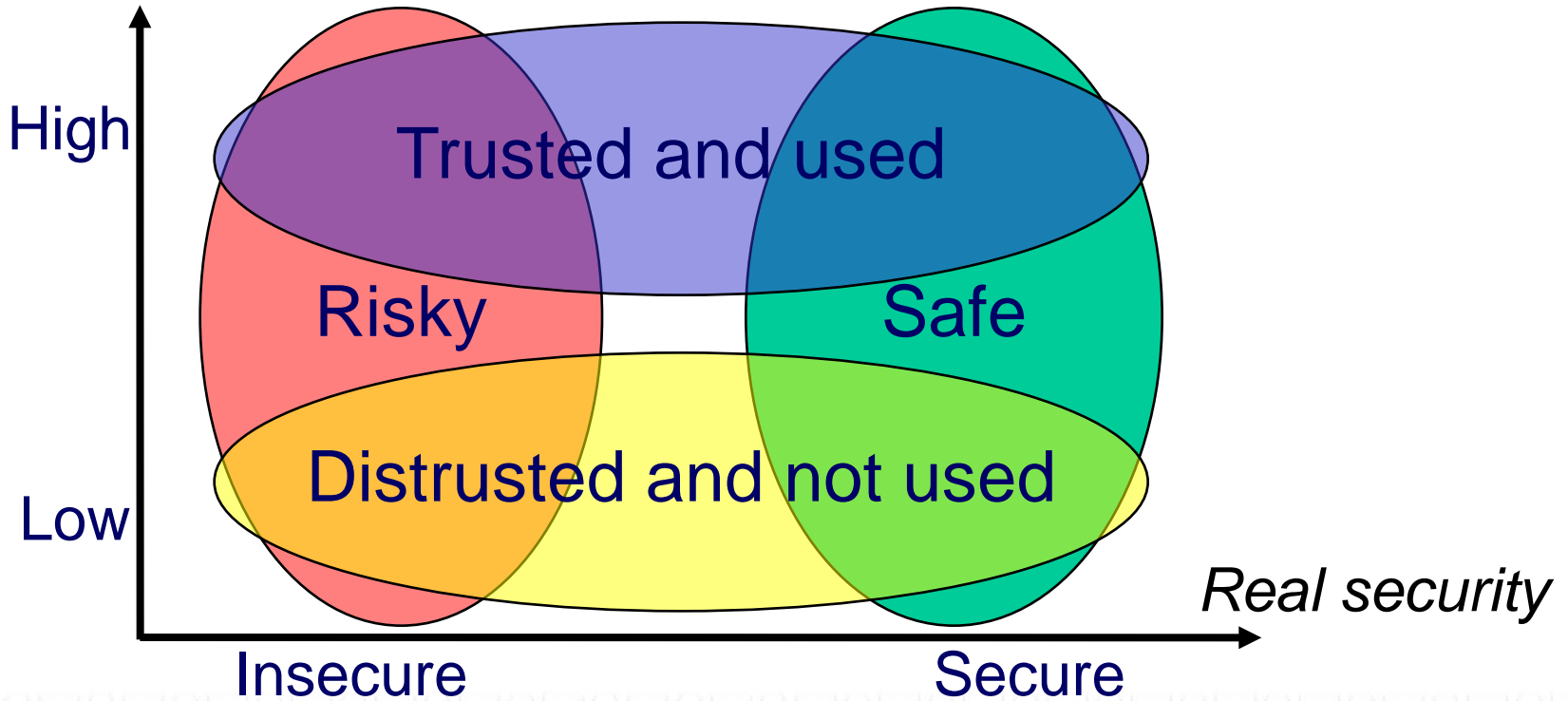
Trusted party

Wants to **represent** and put in a **positive light** own competence, honesty, reliability and quality of service.

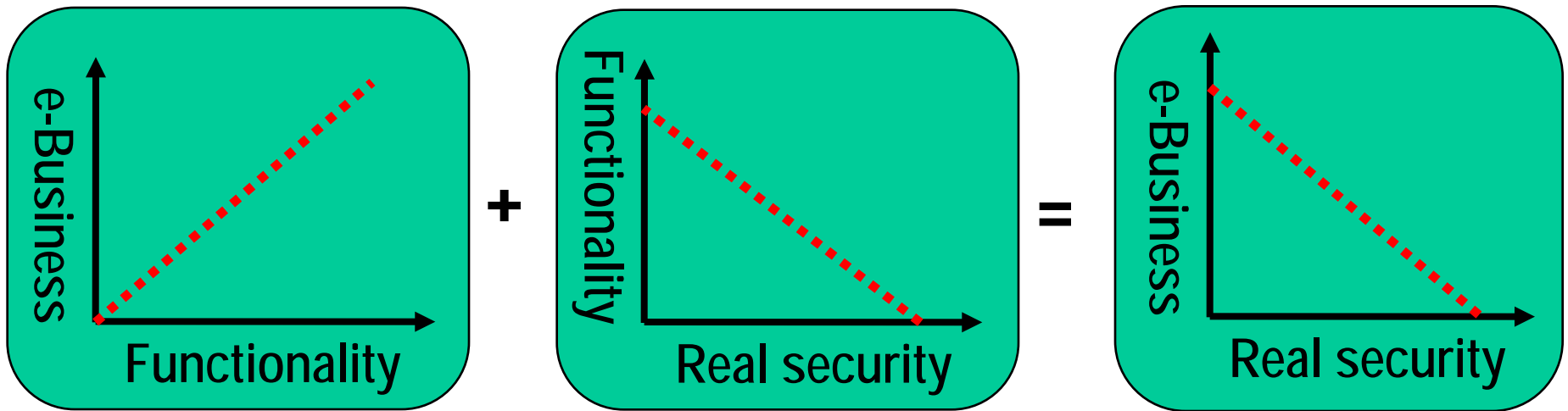


Perception and Reality

Perceived security

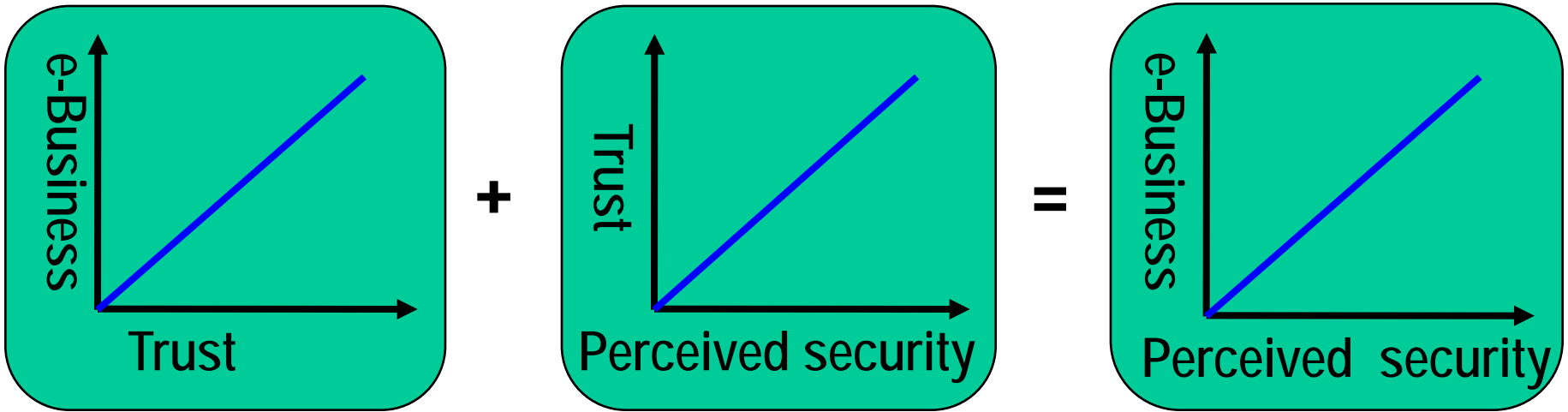


Real Security is Bad for E-Business



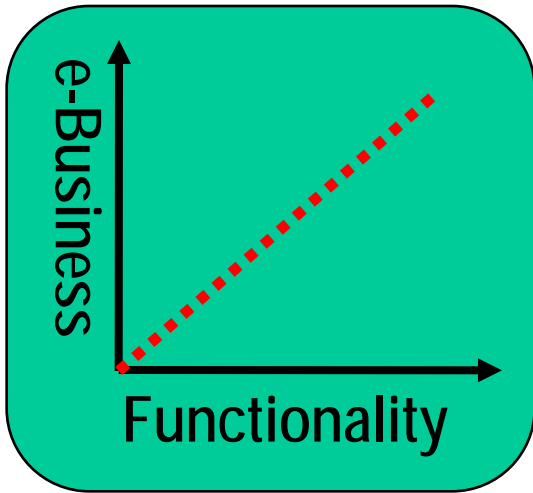
- E-business revolution not possible with real security
- Thank God the Internet isn't secure

Perceived Security is Good for E-business

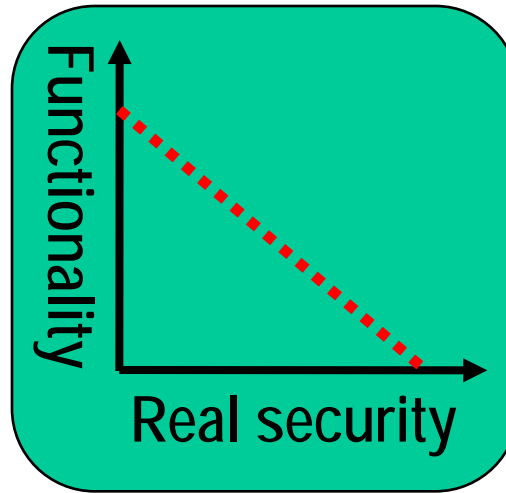


- E-business growth needs perceived security

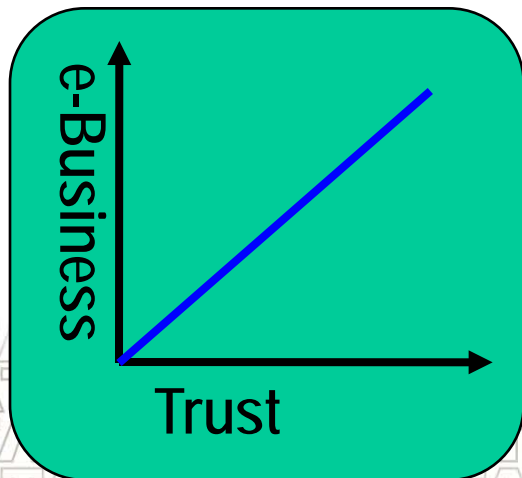
The Security Dilemma



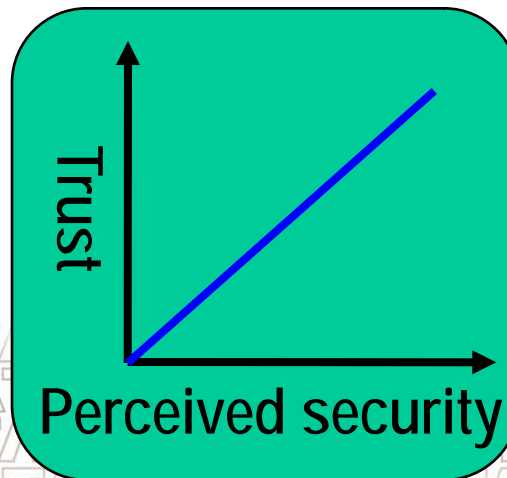
+



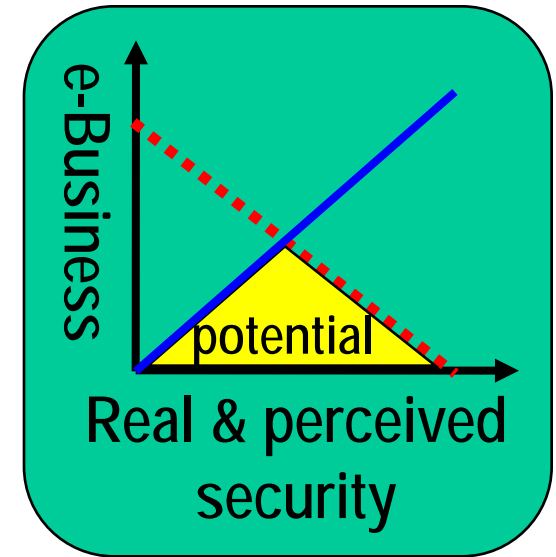
+



+



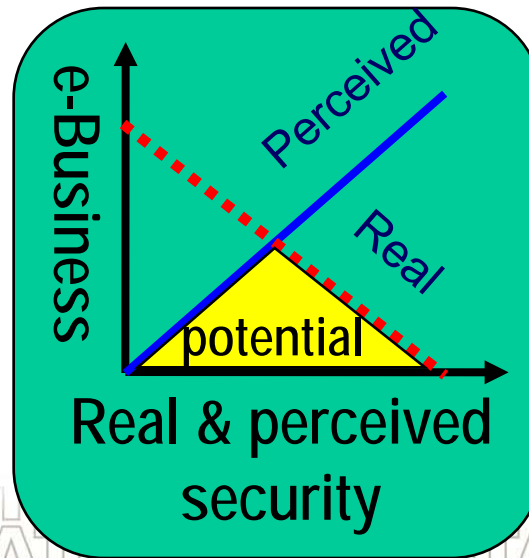
=



Jøsang's Law of Security and E-business

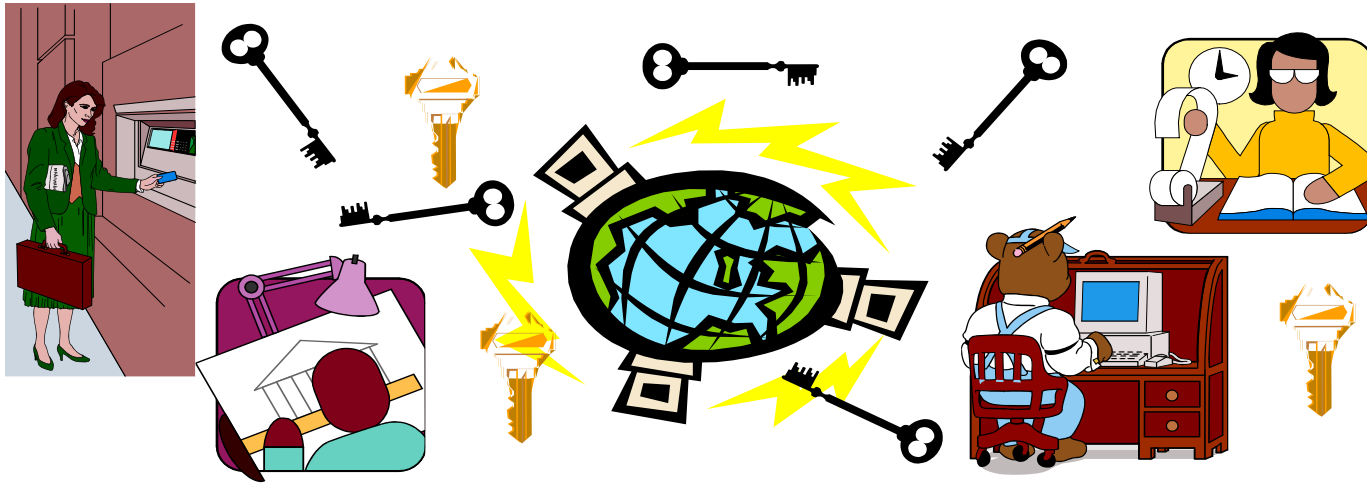
The potential of e-business is bounded by:

- The lack of functionality caused by real security
- The lack of trust caused by perceived insecurity



Trust and PKI

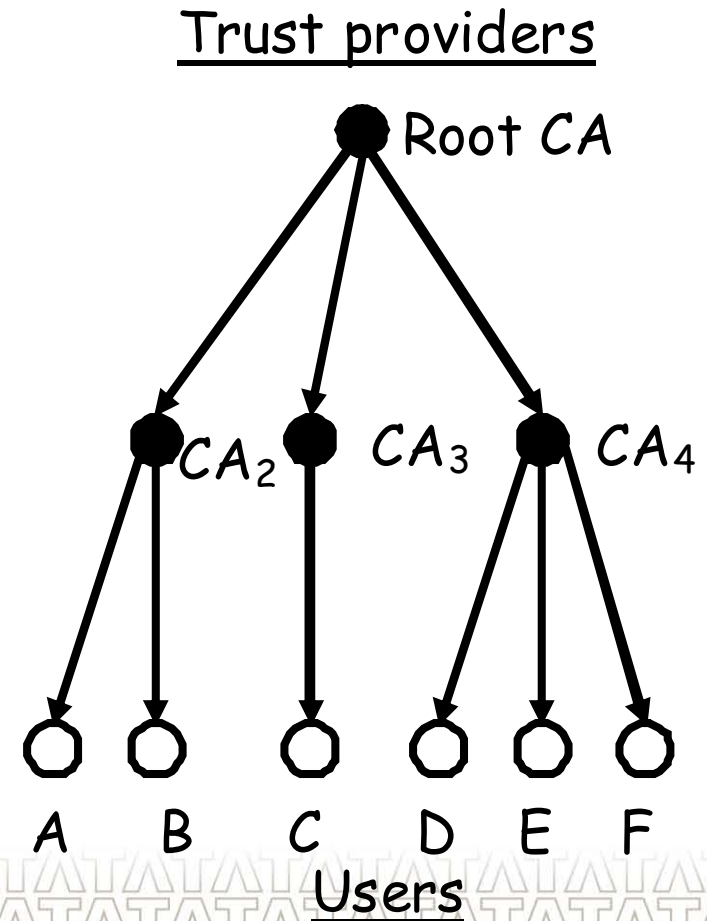
- Cryptography solves security problems, but creates key management complexity



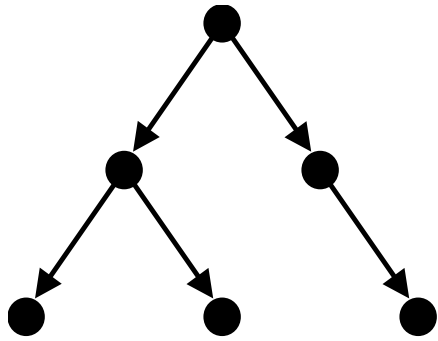
- PKI simplifies the key management, but creates trust management problems

Public Key Infrastructures

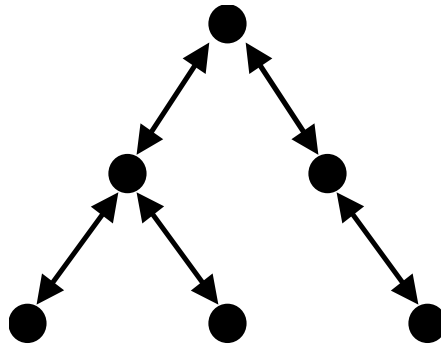
- Key distribution mechanism
- User keys are certified by CAs
- Chain of certificates
- Ultimately certified by root CA
- Keys are distributed online
- Root key must go out-of-band (keys are distributed in a different channel)
- Only guarantees authenticity
 - Not reliability



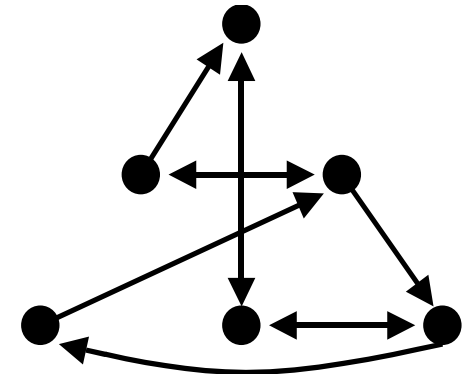
PKI Trust Structures



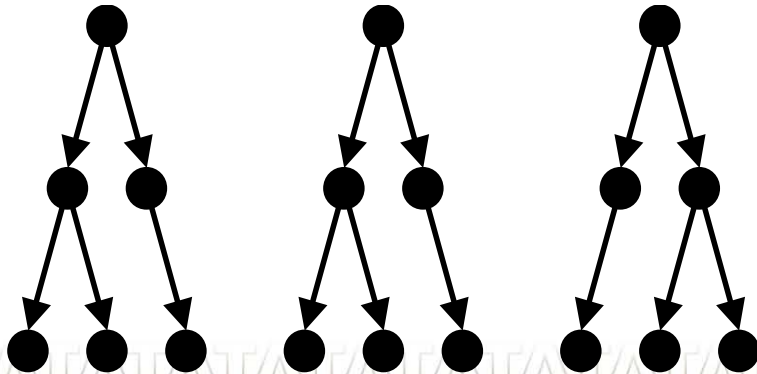
Strict hierarchy



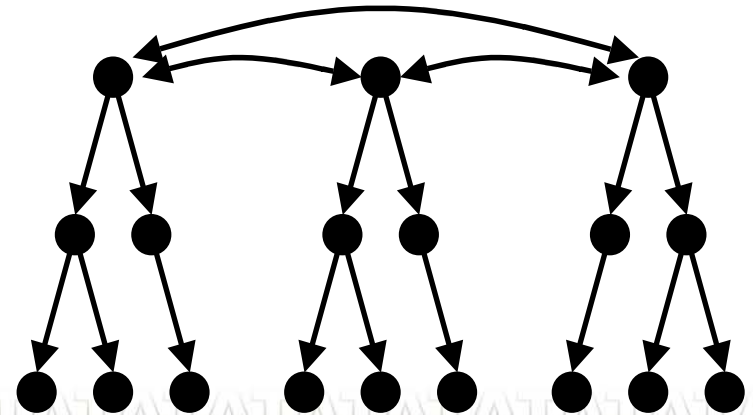
General hierarchy



Anarchic structure
"The PGP PKI"



Isolated strict hierarchies
"The Web PKI"



Cross certified strict hierarchies

PKI Trust Issues

- CAs could issue certificates without checking owner identity
- CAs could deliberately issue false certificates
- Private keys could be disclosed by accident or on purpose
- False certificates could be inserted into browsers
- It is not possible to check whether a revocation request is genuine or not (a denial of service attack is possible)
- Checking revoked certificates requires another secure channel
- Liability issues for false or misused keys



The Web PKI

- Weak out-of-band channel
- No assurance of server security
- No assurance of service provider reliability
- Poor usability
- No real authentication (re: phishing attacks)

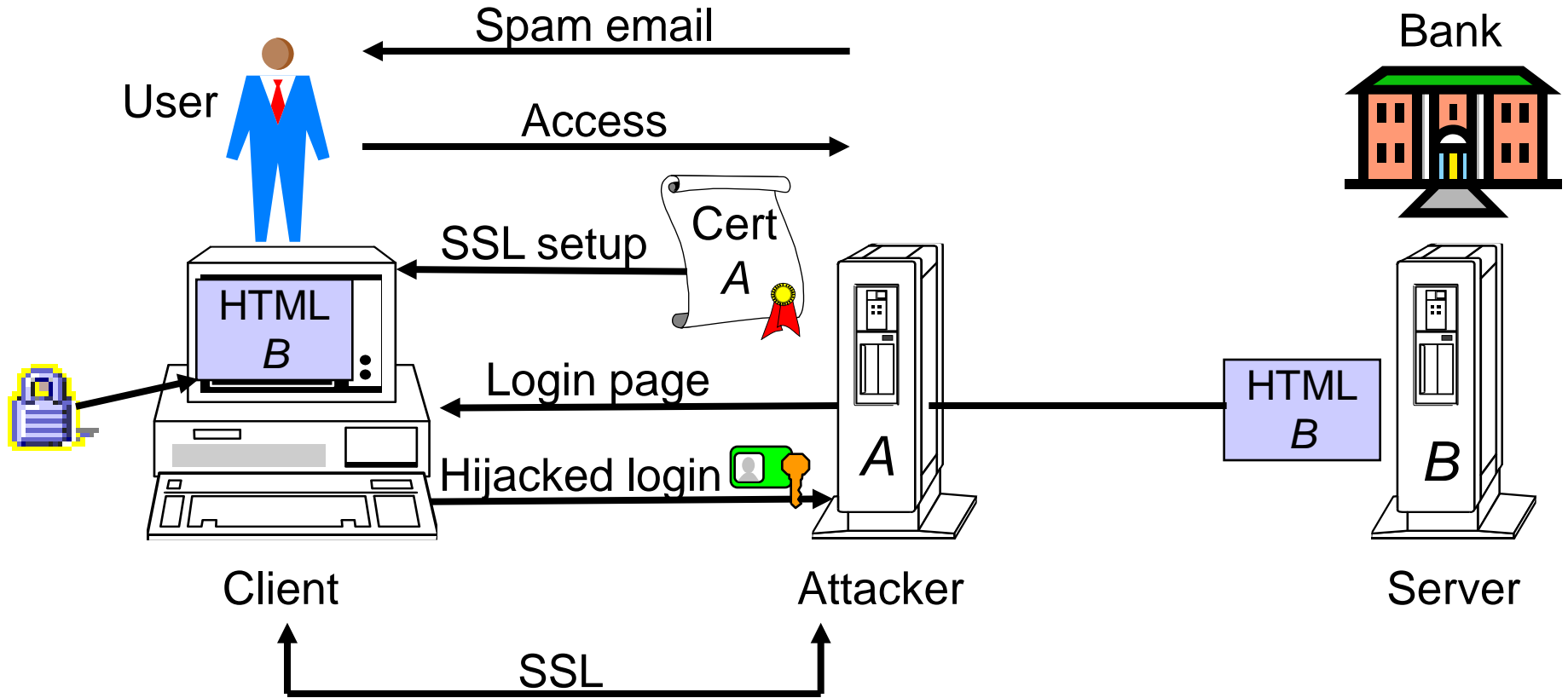
a misnomer:



The Web PKI only provides perceived authentication, not real authentication



Phishing and Spoofing



Illustrates poor Web server authentication

The Purpose of SSL on the Web

- SSL can theoretically provide authentication and confidentiality
- SSL confidentiality eliminates password sniffing
 - SSL in Anonymous Diffie-Hellmann mode (ADH) provides confidentiality
 - ADH mode does not require certificates
- SSL actually provides no practical authentication
 - Can not prevent phishing attacks
- PKI and certificates currently have no real practical purpose for Web security

What Experts Say about Web Certificates

Digital certificates provide no actual security for electronic commerce; it's a complete sham.

Bruce Schneier: Secrets & Lies

SSL gives no security guarantees that are relevant for e-commerce. Still, users feel more secure.

Dr Richard Walton, former Director of CESG

(Communications- Electronics Security Group)

The Web PKI serves to increase perceived security



Trust and Access Control

- Access control paradigm:
 - The resource owner grants access authorisation
 - The system verifies authorisation before access
- Trusted user = authorised user
- Trusted code = code running as system
- Untrusted code = code running in a sandbox
- Semi-trusted code = some more access rights
- Access credentials can be exchanged and evaluated mechanically
⇒ trust negotiation
- Access authorisation can be delegated in a transitive fashion
⇒ transitive trust

Trust Management Systems

- Idea: “Who can I trust to access my resources?”
- Meaning: Access authorisation and control
 - Not (necessarily) based on identity
 - Attribute certificates/credentials
 - Delegation chains
- Better name: Access credentials management

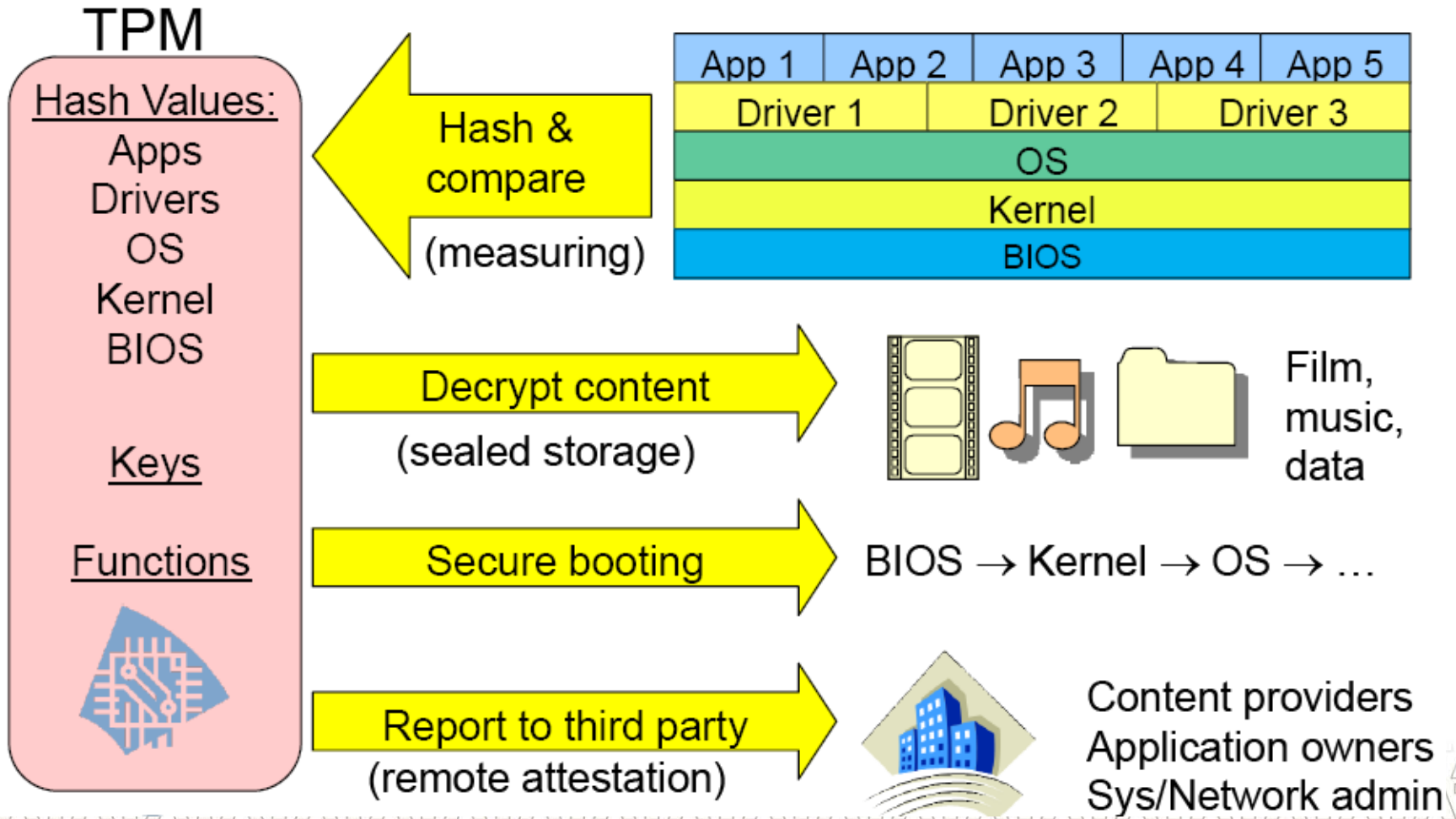
Trust management is supposed to be an incredibly vague and provocative term invented by Matt Blaze. I don't know whether he intended it that way, but it comes natural to him

Joan Feigenbaum, AT&T Bell Labs

Trusted Computing

- Idea: It shall be impossible to install and execute software that is not certified and authorised
 - Current paradigm: Software-open systems
 - Trusted computing paradigm: Software closed systems
 - Controlled by hardware
- 1999: Trusted Computing Group (TCG)
 - Trusted Platform Module (TPM) specification
- 2001: Production of TPM chip
- 2002: Microsoft announces Palladium TPM chip
- 2005: Next Generation Secure Computing Base (NGSCB)
- 2006: Limited trusted computing in Vista
 - Disk encryption based on TPM (Trusted Platform Module)
- 2009: TPM in almost all PCs, not yet in mobiles

Trusted Computing Module (TPM)



What Trusted Computing Can Do ?

- Can prevent
 - Installation and execution of unauthorised software
 - Tampering with installed software
 - Usage of stolen computers
- Can be used for Digital Rights Management (DRM)
 - Prevents playing unlicensed digital content

If you want to do DRM on a PC, you need to treat the user as the enemy.

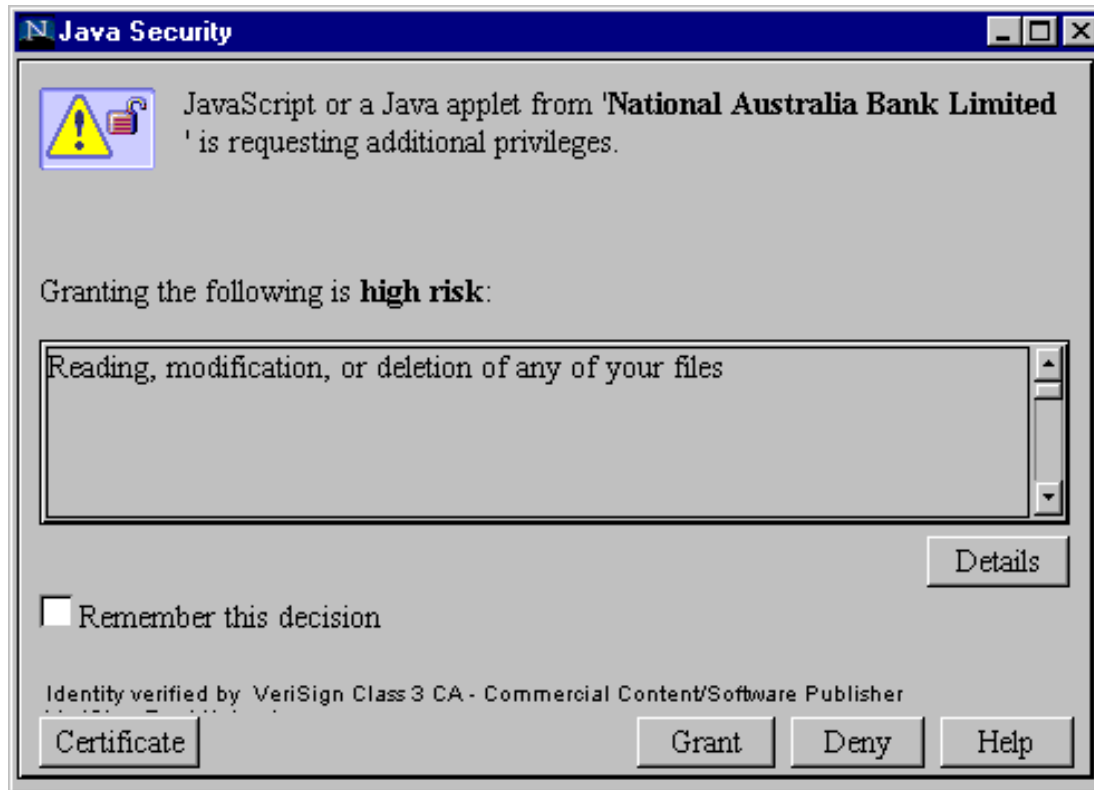
Roger Needham

Former director of Microsoft Research Europe

Problems with Trusted Computing

- No protection against
 - Malicious authorised software
 - Security vulnerabilities due to software bugs
- Bugs in security hardware can be disastrous
- Bureaucracy of software authorisation
 - How to authorise software?
 - Everything or just selected software?
- Control over client machines can be abused under the pretext of DRM
- Introduces liability issues
 - The party in control should also be liable

Trust Pressure on Users



- Users are conditioned to always accept
- Will make wrong decision in case of malware

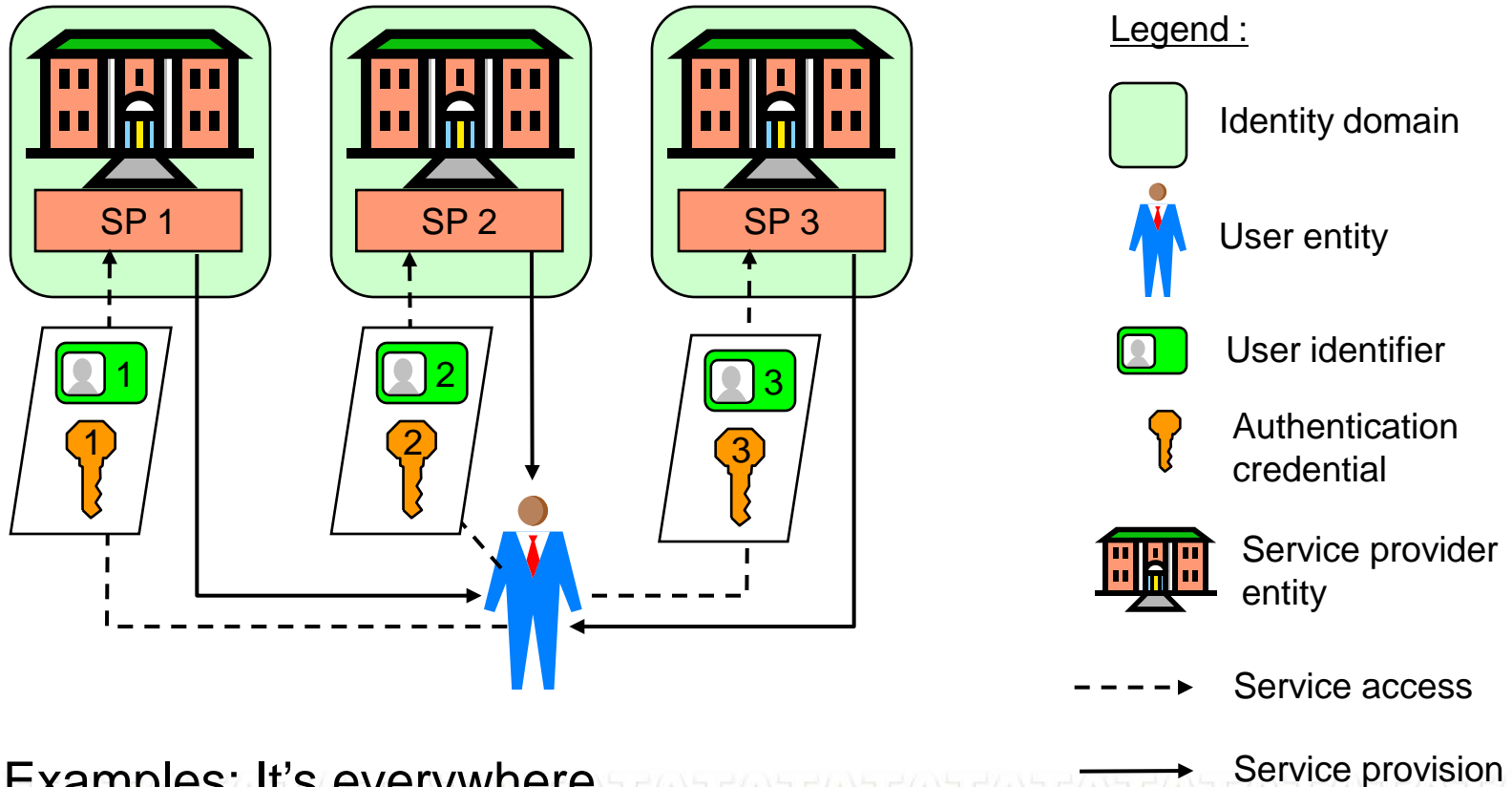
Trusted Computing Base: TCB

- A full combination of security mechanisms (hardware and software) within a system
- Security evaluation gives security assurance
 - US TCSEC (Trusted Computer Security Evaluation Criteria, aka. Orange Book)
 - European ITSEC (Information Technology Security Evaluation Criteria)
 - ISO Common Criteria
 - Represents a public measure of security
 - Additional factors can override security assurance at any time, e.g. security flaws

Trust and Identity Management

- Important issues
 - Privacy violation
 - Identity theft
 - Poor usability leads to policy violation
 - Trust relationship requirements
- Establishing trust relationships has a cost
 - Simple models have simple trust requirements and vice versa
 - Simple models don't scale well

Isolated User Identity Model



Examples: It's everywhere









Trust Requirements for Isolated Identity Mgmt

- T1** Client trusts that service provider protects the client's privacy;
- T2** Client trusts that service provider has satisfactory user registration and authentication mechanisms;
- T3** Service provider trusts that client handles their credentials with adequate care.

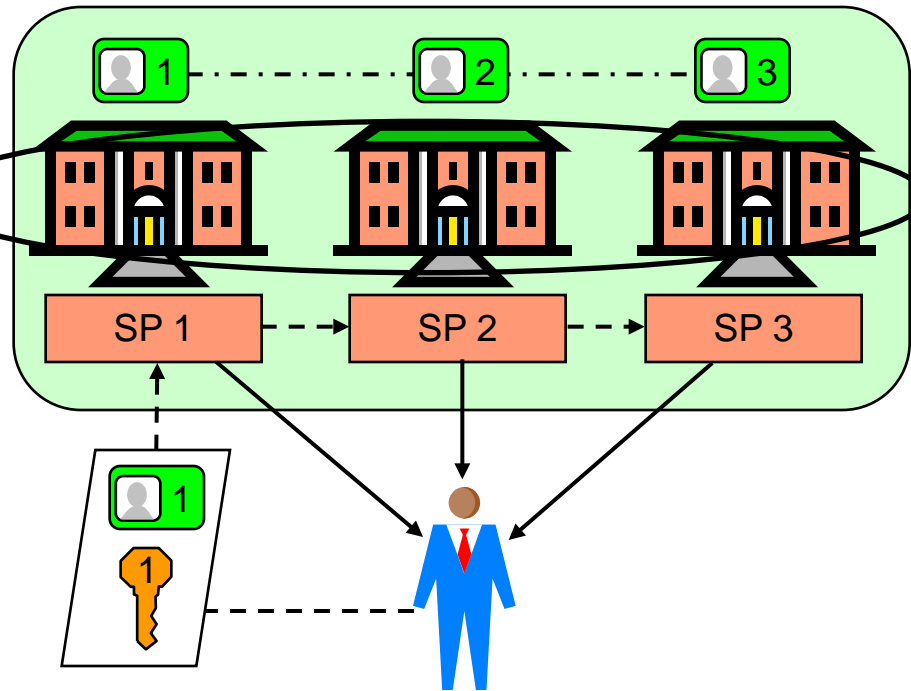


Federated User Identity Model

Legend :

-  Identity domain
-  User entity
-  User identifier
-  Authentication credential
-  Service provider entity
-  Service access
-  Service provision
-  Identifier mapping

Circle of trust
(Liberty Alliance)

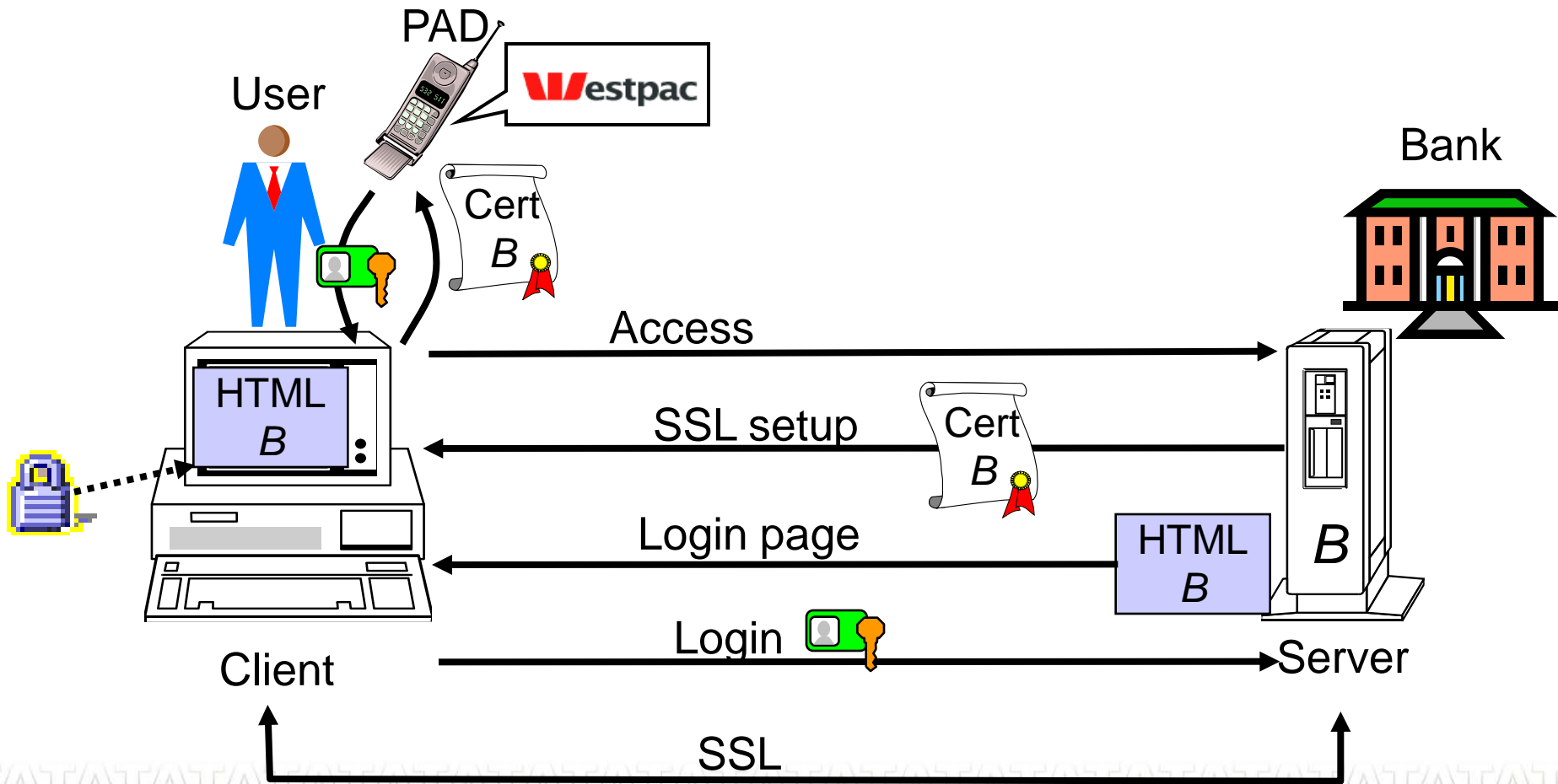


Examples: Liberty Alliance, SAML2.0, WS-Federation, Shibboleth

Trust Requirement for Federated Identity Mgmt

- T1** Client trusts that service provider protects the client's privacy;
- T2** Client trusts that service provider has satisfactory user registration and authentication mechanisms;
- T3** Service provider trusts that client handles their credentials with adequate care;
- T4** Service providers and clients both trust that service access by assertions between service providers will only take place when legitimately requested by the client;
- T5** Service providers and clients both trust that the identifier mapping between service providers is correct;
- T6** Client trusts that all service providers adhere to the accepted policy for correlating personal data about the same client from other service providers.

User Centric Identity Management



Hard vs. Soft Security

- Traditional security systems: Hard security
 - Authentication
 - Access control
 - Encryption
 - ...
- What about deceit and poor quality services?
 - Traditional security provides no protection
 - Trust and reputation systems can provide protection
 - Soft security

Reputation and Trust

REPUTATION

- Based on public info
- Common/average opinion
- Not necessarily objective

■ *“I trust you because of your good reputation”*

■ *“I trust you despite your bad reputation”*

TRUST

- Based on both private and public info
- Personal
- Private info weighs more than public

Trust and Reputation Systems

Trust systems

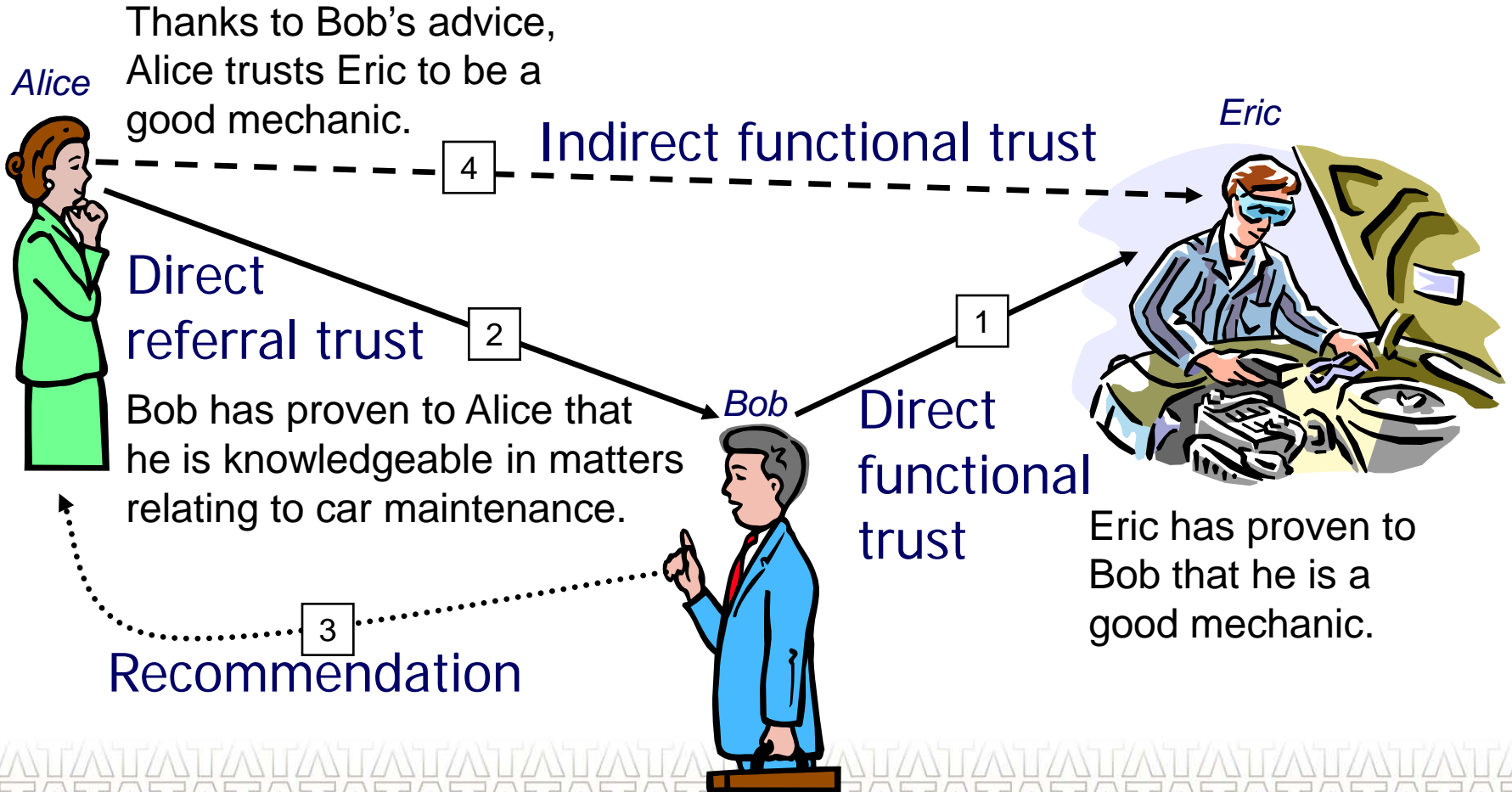
- Private and public ratings as input
- Computes score for target entity only
- Private scores
- Explicit transitivity

Reputation systems

- Public ratings/info as input
- Computes scores for all entities
- Public scores
- Implicit transitivity



Trust Transitivity




Computational Trust with Subjective Logic

Trust Inference Demo - Microsoft Internet Explorer

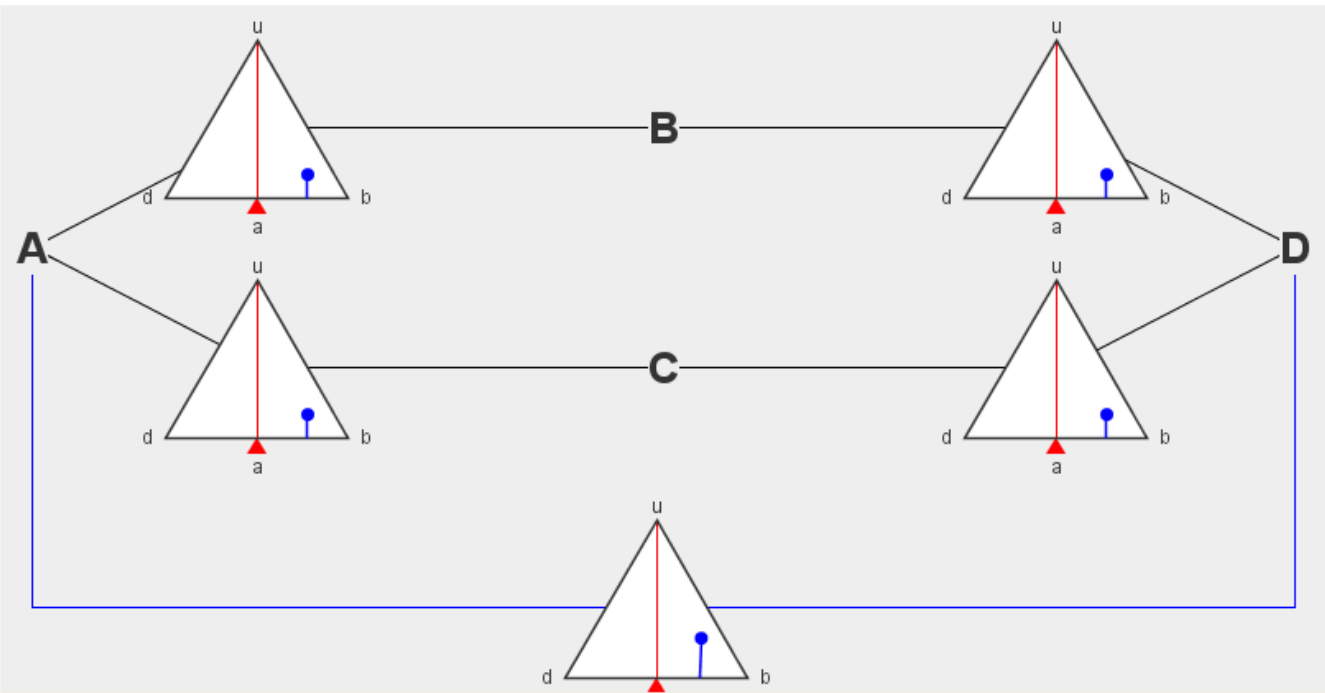
Address <http://security.dstc.edu.au/spectrum/trustengine/demo2.html>

Simple Trust Network Demo

Four entities, labelled A, B, C and D have opinions about each other represented as points in triangles. Entity A is trying to form an opinion about D, and receives opinions from B and C as to the trustworthiness of D. Furthermore, A has his own opinions about the trustworthiness of B and C.



Left-click and drag opinion points to set opinion values. Entity A combines these opinions using the [Subjective Logic Operators](#) to derive his own opinion about D, as shown by the bottom opinion triangle. In detail, entity A *discounts* B's opinion about D by his opinion about B, and does similarly for C. Finally, he combines the two discounted opinions using the *consensus* operator in order to determine his opinion about D. Right-click on the opinion triangles to see the exact values of each opinion. Opinion values can also be visualised using [three-coloured rectangles](#).



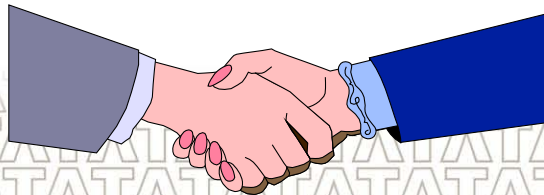
Trust in Online Communities

- Privacy and security mechanisms provide trust in the infrastructure
- Trust and reputation systems provide trust in people and service providers
 - Enhances the quality of online markets and communities
 - P2P networks, eBay, Slashdot, Amazon, Epinion
- Hard and soft security are complementary



Conclusion

- There is no shortcut to trust
 - Provide real security, and it will be trusted
 - Perceived security is no long term solution
- Challenge the security-functionality trade-off
 - Stronger focus needed on usability of security
- Online trust requires more than just security
 - Trust and reputation systems promising technology to make the Internet a safer place to be



Thank You!

