Role of Identity in Network and Information Systems

RK Shyamasundar,
Fellow IEEE, Fellow ACM, FNA, FTWAS
Tata Institute of Fundamental Research
Mumbai
shyam@tifr.res.in

Cyber space

The New Yorker
5 July 1993

"On the Internet, nobody knows you're a dog."

Organization

- Identity and Identification
  - General notions and Cyber world notions
  - Biometric Attributes
  - Relevance to Trust
  - (Delivering a secure trusted service)
- Application of Cryptography
- Examples of TPH, AI Techniques ..
- Role of securing embedded devices

Identity and Identification

Human Identity

- the condition of being a specified person (Oxford)

or

- the condition of being oneself ... and not another (Macquarie)
- may adopt different identities at various times and some maintain several concurrently. [CLARKE]

Identification

- establishing the identity of, [or] recognising, or the treating of a thing as identical with another (Oxf)
- act of recognising or establishing as being a particular person & the act of making, representing to be, or regarding or treating as the same or identical (Macquarie)

In the Cyber World

human identification
is
the association of data
with
a particular human being

Security Threats : Taxonomy

- Confidentiality
  - violated when unauthorized users get protected information
- Integrity
  - violated when unauthorized users modify information
- Availability
  - violated when the system is prevented from doing its intended function

Authorized vs Unauthorized

How to you distinguish?

- IDENTIFICATION: User says who (s)he is
- AUTHENTICATION: Proof of of validity of the Identity
- AUTHORIZATION: Controller provides relevant admissible access

Failure of Authentication lead to violations of Confidentiality, integrity and availability

IT Security: Aims

- **Confidentiality**
- **Integrity, Availability, Reliability, Functionality, …**
- **Anonymity-** use resource without disclosing id
- **Pseudonymity**- may use a resource without disclosing its id but still accountable for use
- **Unobservability –** make multiple uses of resources or services without others being able to observe its use
- **Unlinkability**- multiple uses of resources without being able to link the uses together

IT Security (contd)

- **Security Models**: **Chinese wall, Role based,Object oriented, Resource allocation monitor** …
- **Basic Security Functions:** identification & authentication, Access control, Audit, Objcet reuse, Reliability of Service, Anonymization, Pseudonymization, communication security functions
- **Security Mechanisms :**
  - **Internal:** passwords, chipcards, Access control lists, Cryptography (digital signatures- nonrepudiation (co-registry signatures ..)), redundancy etc
  - **External:** Physical, Organizational, personnel controls

Formal Identification: Organisatonal Needs

- one-to-one relationship between persons and identities
- Requirements of client-oriented approaches
- Employees as customers
- When is anonymity unacceptable and Identification necessary
- When do you need to restrict a person to have single identity

Formal Identification Process

- appearance -
- social behaviour -
- names –
- codes - used by an organisation;
- knowledge - or what the person knows;
- tokens - or what the person has;
- bio-dynamics - or what the person does;
- natural physiography - or what the person is;
- and imposed physical characteristics - or what the person is now.

Taxonomy of Biometrics (a)

- **appearance** (passport descriptions of height, weight, colour of skin, hair and eyes, visible physical markings; gender; race; facial hair, wearing of glasses; supported by photographs);
- **social behaviour** (habituated body-signals; general voice characteristics; style of speech; visible handicaps; supported by video-film);

Taxonomy of Biometrics (b)

- **bio-dynamics** (manner of signature is written; statistically-analysed voice characteristics; keystroke dynamics, particularly in relation to login-id and password)
- **Natural physiography** (skull measurements; teeth and skeletal injuries; thumbprint, fingerprint sets and handprints; retinal scans; earlobe capillary patterns; hand geometry; DNA-patterns);
- **imposed physical characteristics** (dog-tags, collars, bracelets and anklets; brands and bar-codes; embedded micro-chips and transponders).

Human Identifier: Characteristics

- Universality:
- Uniqueness:
- Permanence: identifier should not change, nor be changeable
- Indispensability: id should be one or more natural characteristics each person has and retains. If artificial, the identifier should be enforcedly available at all times
- Collectibility: id should be collectible by anyone on any occasion
- Storability: id should be storable in manual/ automated systems
- Exclusivity: no other form of identification should be necessary or used
- Precision: id should be sufficiently different from every other identifier that mistakes are unlikely

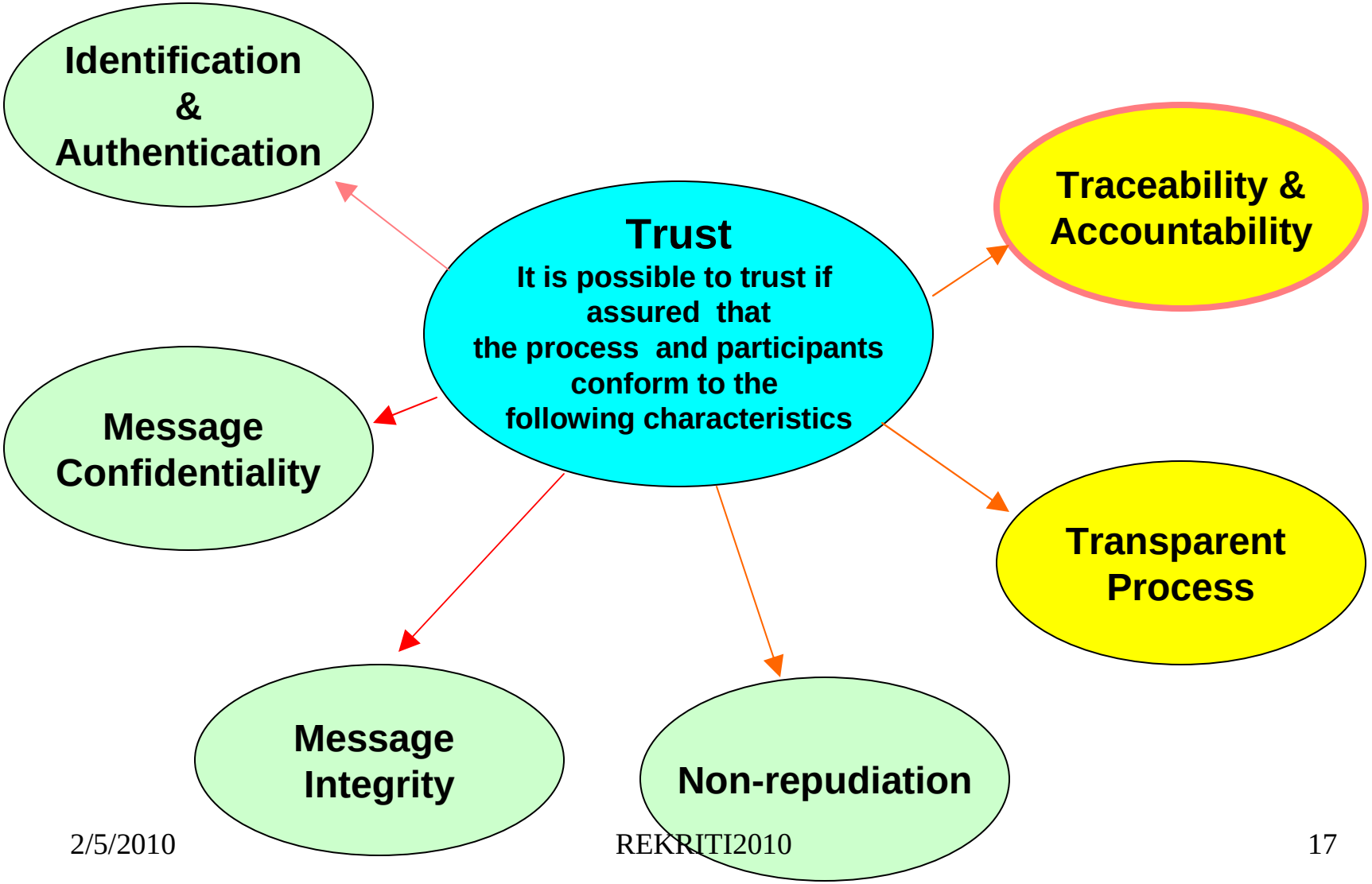
Human Identifier: Characteristics

- simplicity :
  - recording /transmission be easy & not error-prone
- cost
  - measuring /storing id should not be unduly costly
- Convenience:
  - measuring /storing id should not be unduly inconvenient or time-consuming
- Acceptability
  - should conform to contemporary social standards

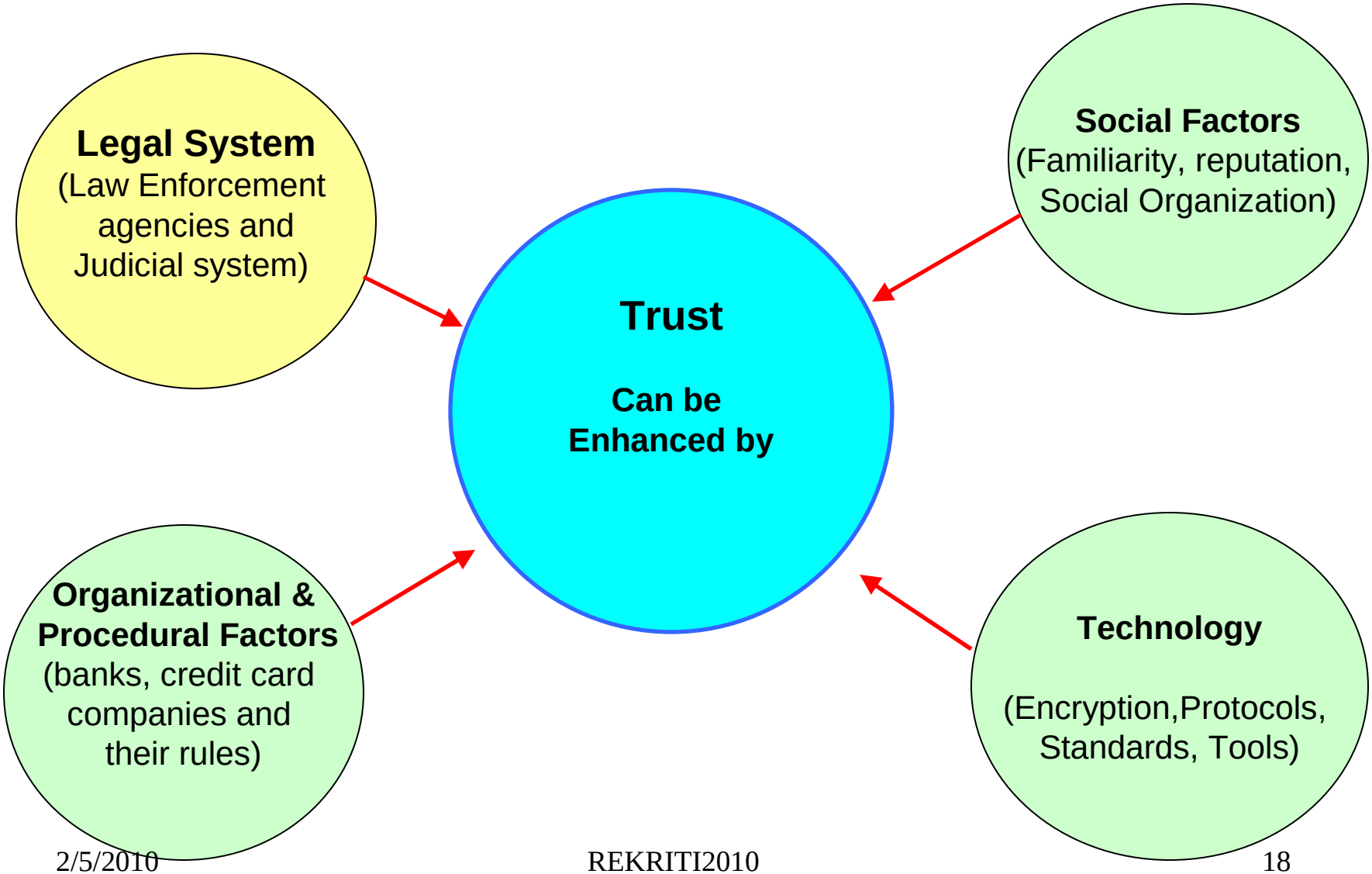
Identification Schemes in Organisational Information Systems

- Documentary Evidence:
  - To establish relationship & on persons' knowledge or a token
- Enable Trust

Constituents of Trust



Creating & Enhancing Trust



Anonymous and Pseudonymous Transactions

- Functional needs of identification:
  - Loans, repayments, market goods, services, class of buyer, taxation, …
- E-Transactions:
  - transaction techniques which protect the identity of one or all participants
  - pseudonymity: parties are aware of an identification code for the other party, and may be able to initiate contact with them using that code, but cannot associate that identity with any particular person

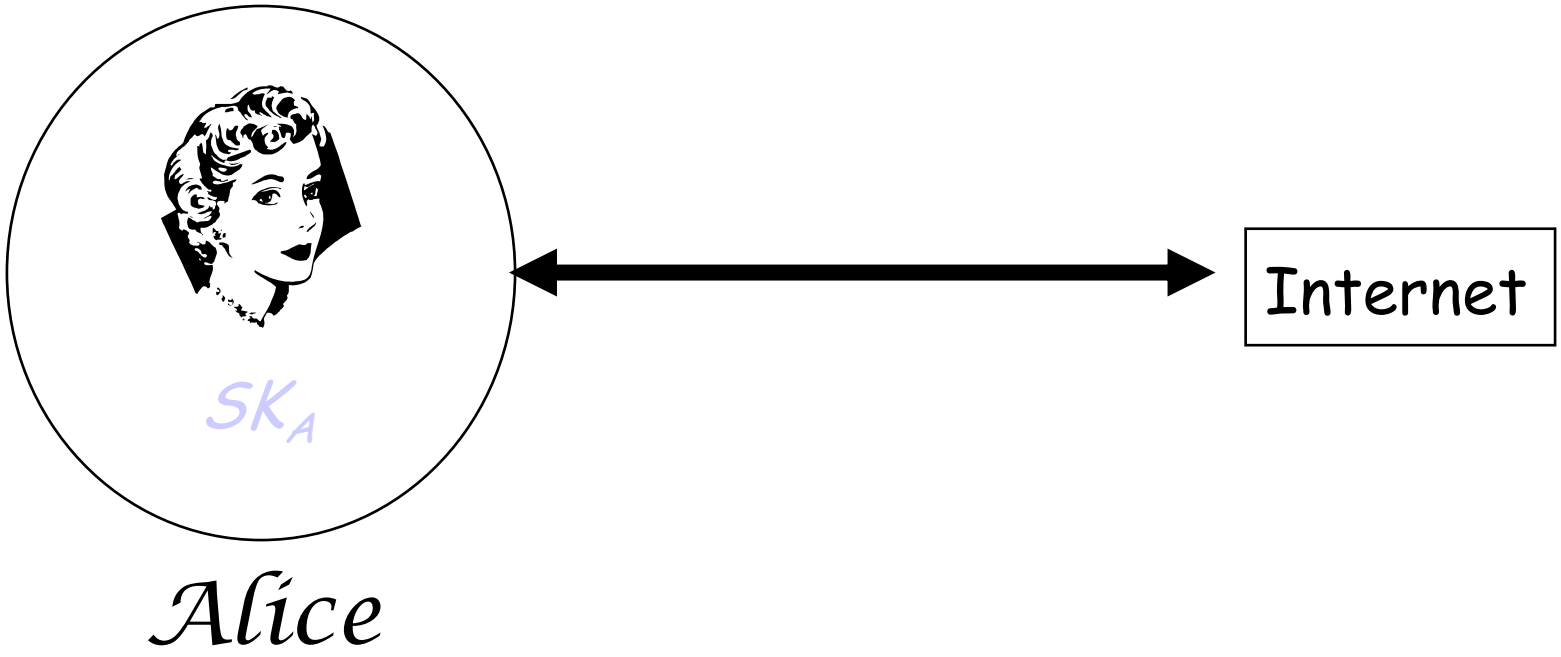
How does Cryptography Help?

The “Alice abstraction”

- Assumes Alice can generate and use her secret key SK_A, while keeping it secret.
- Alice’s secret key SK_A is her “cyber-soul”, her “electronic identity” (or pseudonym), her way of identifying herself. SK_A ***<u>is</u>*** Alice!

- [From RIVEST]

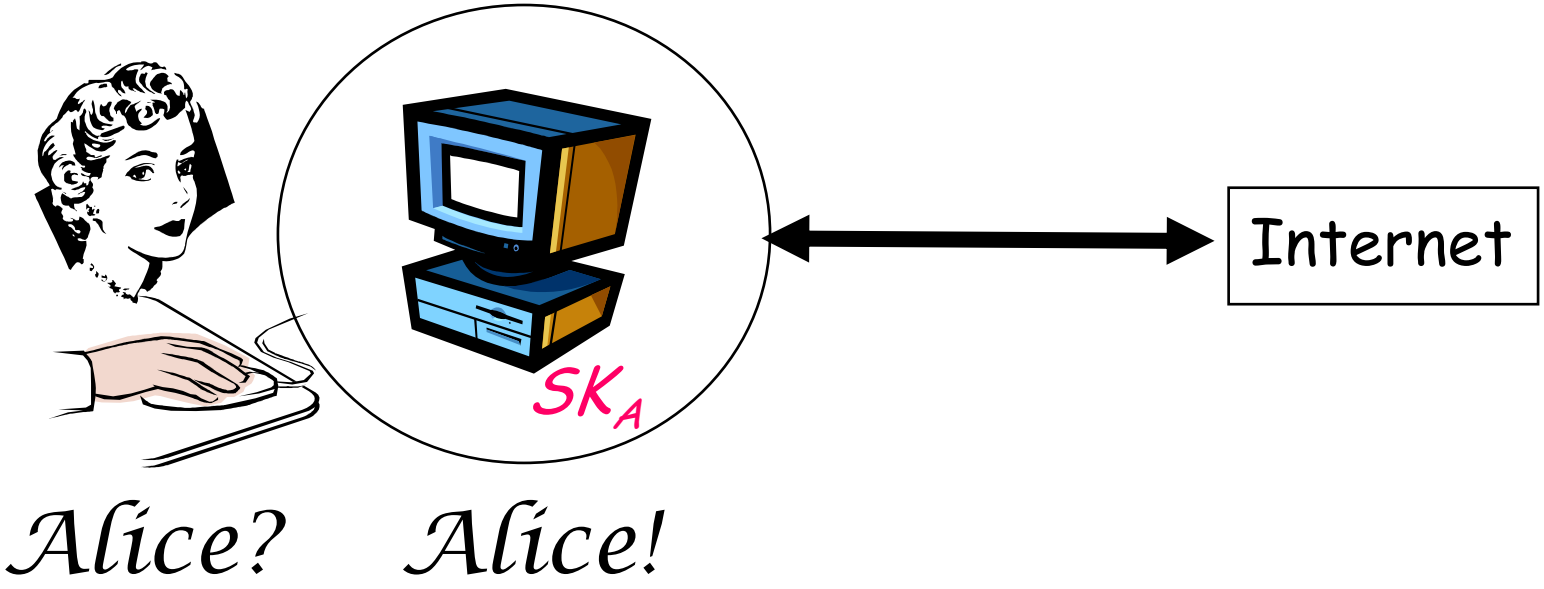
Cryptography in Theory



But Alice is not a computer!

- Alice needs a computer (or at least a processor) to store her secret key SK_A and perform cryptographic computations on her behalf.
- In particular, her processor should produce Alice's digital signature when appropriately authorized…

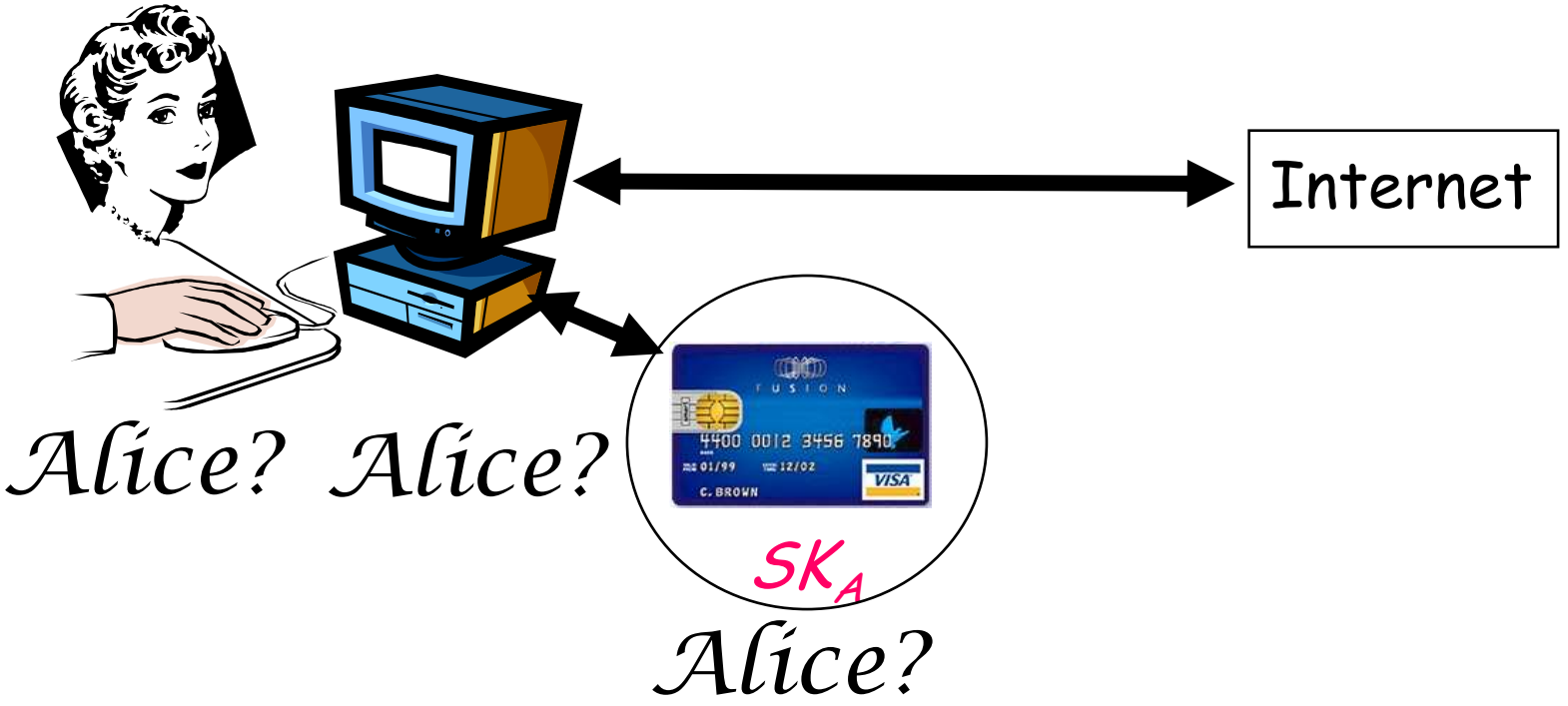
Cryptography in Practice



But her OS is not secure!

- Modern OS's (Windows, Unix) are too complex to be adequately secure for many applications (viruses, Trojan horses).
- Would *you* base the security of an Internet presidential election on the security of Linux?
- Alice's key SK_A may be vulnerable to abuse or theft…

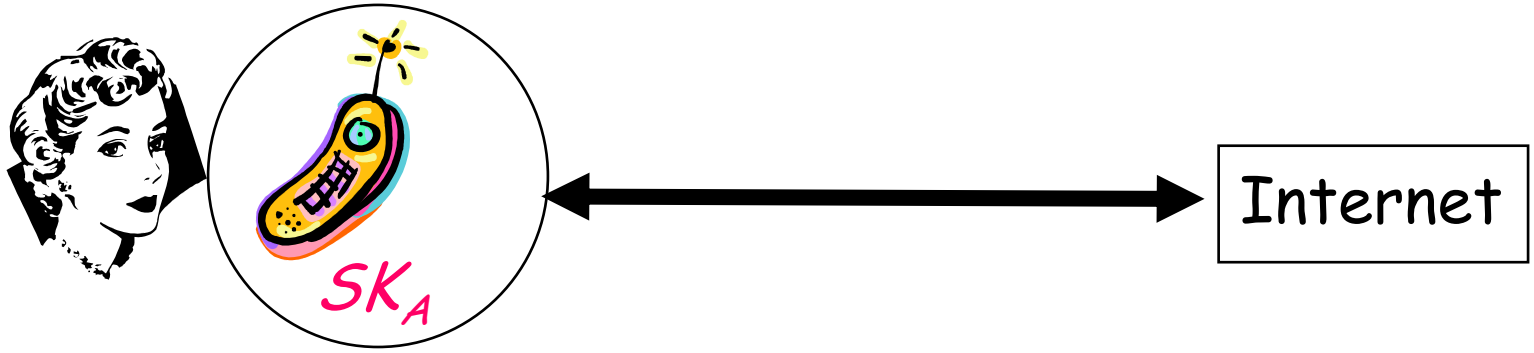
Can SK_A go on a smart card?



But her OS is still not secure!

- Smart card has no direct I/O to Alice.
- When Alice authorizes a digital signature, she must trust OS to present correct message to smart card for signing.

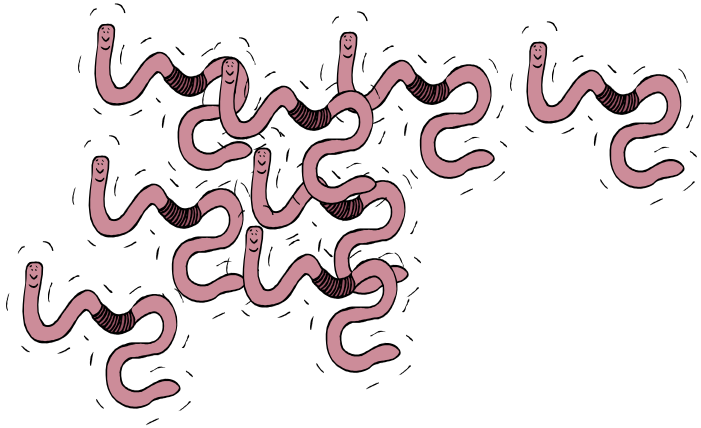
Can SK_A go on a phone or PDA?



Alice? Alice?

But this looks very familiar!

- Same story as for PC, but smaller!
- PC smart card → Phone SIM card.
- Phones now have complicated OS's, downloadable apps, the whole can of worms.
- Little has changed.

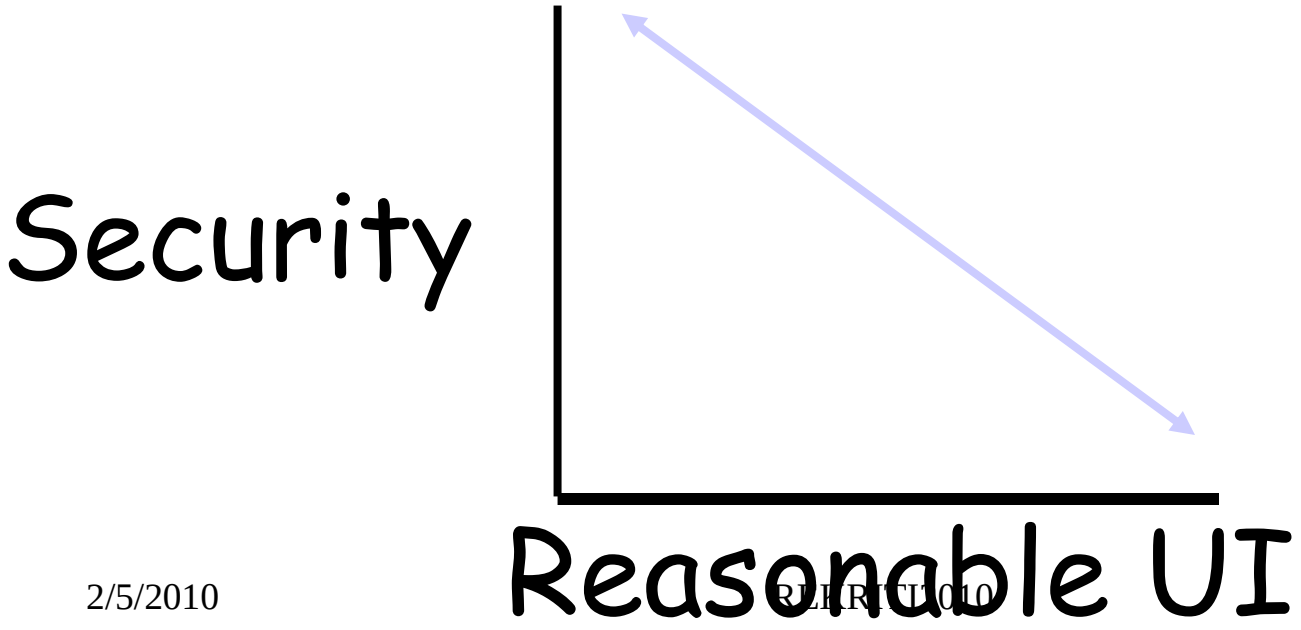


Why can’t we solve problem?

- There is a *fundamental conflict!*
- Downloadable apps and complexity are:
  - *Necessary* for reasonable UI
  - *Incompatible* with security

The Sad Truth?

- *The following are incompatible*:
  - A reasonable UI
  - Security



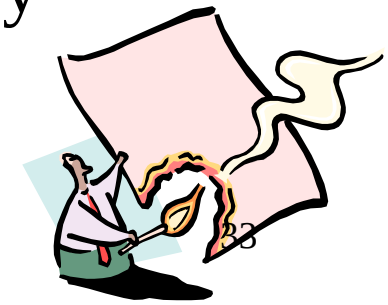
But Digital Sigs Need Both!

- *Security*
  to protect secret key and securely show user what is being signed.
- *Reasonable UI*
  to support complex and variable transactions.

Are Digital Signatures Dead?

- *As usually conceived, perhaps…*
- We should change our mind-set:
  - A digital signature is not
    nonrepudiable proof
    of user's intent, but merely
    plausible evidence.

  - We should build in *repudiation mechanisms* to handle the damage that can be caused by malicious apps.
  - Repudiate *signatures*, not *keys*.



Use a Co-Signing Registry

- Signature not OK until saved and co-signed by user's *co-signing registry* (e.g. at home or bank).
- User can easily review all messages signed with his key.
- Registry can follow user-defined policy on co-signing.
- Registry can notify user whenever his key is used to sign something.

Use One-Time Signing Keys

- Registry can give user a set of *one-time* signing keys, so damage from key compromise is limited. Registry won't co-sign if key was used before.

In this case, registry really holds user's secret signing key, and signs for him when authorized by one-time key.

Repudiation

- May not be so hard to live with, once we accept that it is necessary.
- Consistent with legal status of handwritten signatures (can be repudiated, need witnesses for higher security).

Examples of Technologies

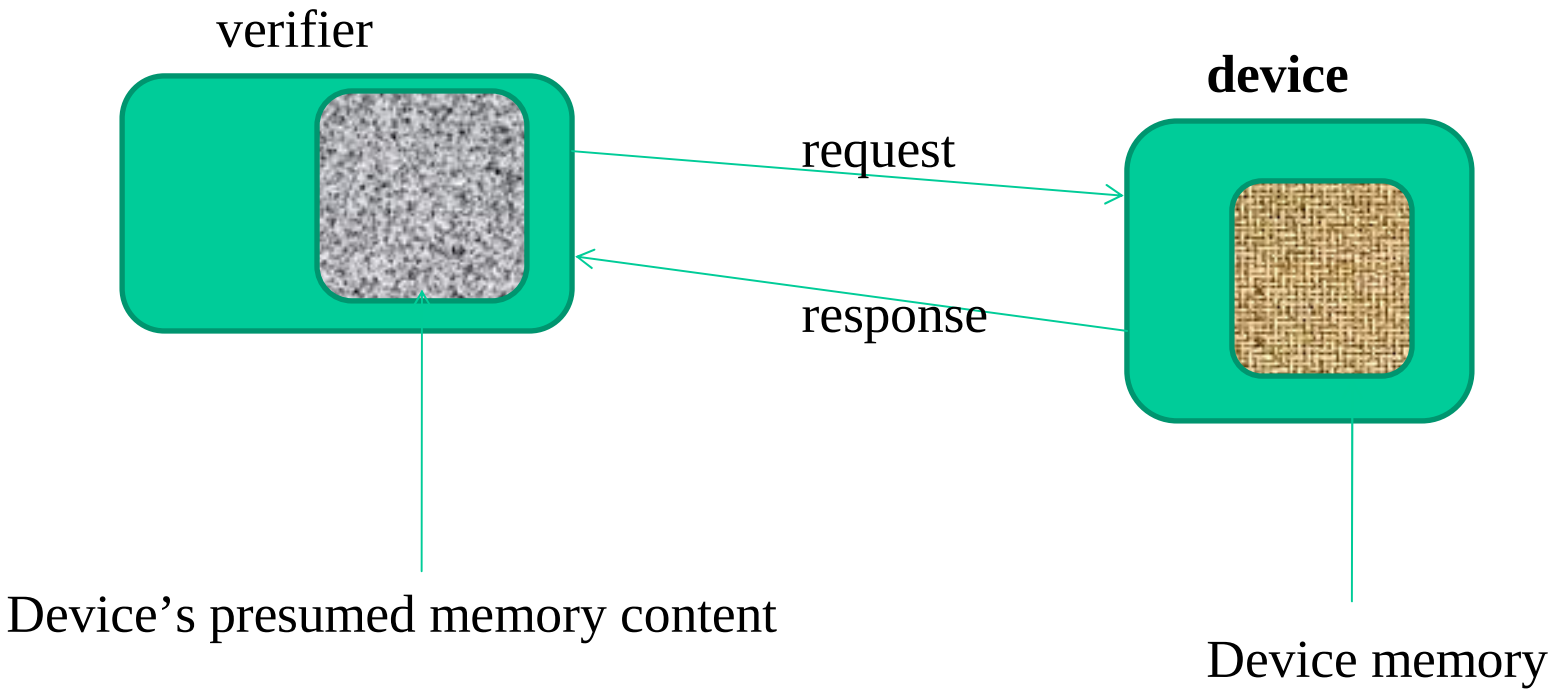
Authenticity of Embedded Devices

- An adversary can compromise our privacy and safety my maliciously modifying the memory content
- Can we establish the absence of malicious changes to the memory contents without physical access to the device's memory?
- [Seshadri,Perrig,van Doorn, Khosla]

Embedded devices: Malicious modifications

- A network printer is vulnerable
- Cell-phone with an email client vulnerable to worms
- Electronic Voting Machines (EVMs) using uncertified voting software
- Smart cards
- Services being provided PDAs by hotels, …

Remote Verification of Embedded devices



Attesting Embedded Devices

Assumptions

- Device contains a memory-content-verification procedure that the verifier can activate remotely
- Exact H/W architecture (clock speed, mem arch, ISA, size) and the expected contents of the device
- Random challenge and check the response (detect compromised device)

Threat Model

- Attacker has full control over the memory device (not modify H/W)
- Verif. Proc. Proeperties
  - Pseudo-random traversal,
  - Resistance to pre-computation & replay attacks
  - High probability of even single byte changes,
  - Small code, efficient implementation and non-parallelizable

Wireless world

- Location, Time
  - Different policies may apply for the same user
  - Time and location restrictions
  - Eg Tax sheets can be opened only while in office
  - Tracking
- Profile of the user

Conclusions

- Social factors (familiarity, reputation, social organization)
- Organizations and Procedures
  - Banks, Credit Card Companies
  - Transparent Rules and Procedures
- Technology
  - Encryption, Protocols, Standards etc
- Legal System (Enforce Trust)
  - Law Enforcement and Judicial system

- Balance between the different security requirements of different stakeholders
  - protecting users in a way privacy regulations demand it
- Identification based on perceived threat model and Identity attributes

Thank you