

Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana

15.566
Information Technology
as an Integrating Force in
Manufacturing

Security

Despite all that...
security breaches are on the rise

**Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana**

.. and require far less technical expertise

What is computer security?

- Securing access to resources
 - Two steps:
 - Authenticate = establish identity of the requestor
 - Authorize = grant or deny access
- Securing communications
 - Three steps:
 - Secrecy = prevent understanding of intercepted communication
 - Authentication = establish identity of sender
 - Integrity = establish that communication has not been tampered with

**Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana**

General Access Control Techniques

- Something you have
- Something you know
- Something you are

Smart Cards "Something you have"

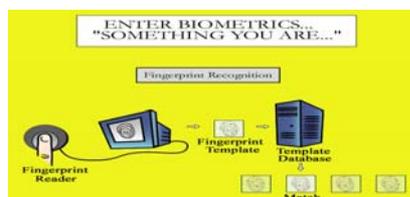
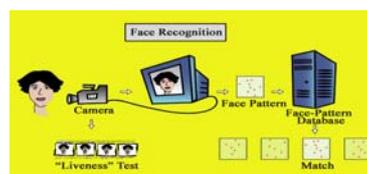
- Several subcategories
- One of interest here are cryptographic smart cards:
 - Store user's digital certificate and/or private key
 - Used to prevent private keys from being "hacked" from user's computer
 - What happens if a smart card is stolen?

**Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana**

System Access Controls "Something you know..."

- Login procedures
 - Usually something you know
- Password leaks
 - Commonly used password
 - Explicitly told
 - Voluntarily
 - Trojan horse
 - Trial and error
 - Intercepted communication
 - paper, camera, wiretap, file on disk, emanations
 - password sniffing on networks
- Passwords are inconvenient
 - In client/server environment, user doesn't want to enter password for every service she connects to

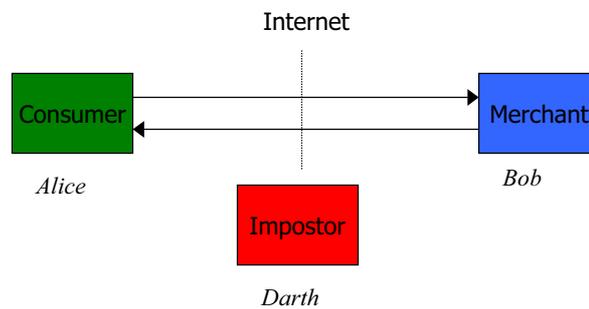
Enter Biometrics... "Something you are..."



Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana

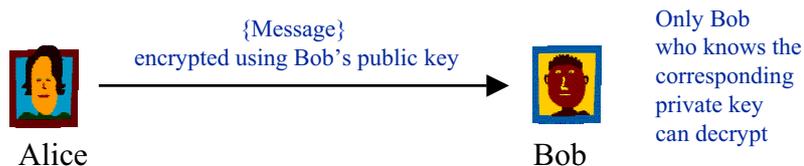
Communication security issues

- Encryption
 - how do I ensure the secrecy of my transactions?
- Authentication
 - how do I verify the true identity of my counterparts?



Public key cryptography

- Secret key cryptography: Based on a secret key
 - Same secret key used for encryption and decryption
 - Problem: How to transmit key securely on the Internet???
- Public key cryptography: Two keys used
 - Public key known to everybody. Used for encryption.
 - Private key known only to owner. Used for decryption.



**Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana**

Public key cryptography works if...

- Private key remains secret
 - Never leaves the owner's computer
 - Typically encrypted and password-protected
- Difficult to guess private key from knowledge of public key
 - Boils down to trying all different key combinations
 - Difficulty of "breaking" the code rises exponentially with the bit length of the key
 - 1024-bit keys require more time than the life of the universe in order to be "broken"
- Reliable public key distributed
 - This is the most difficult problem!

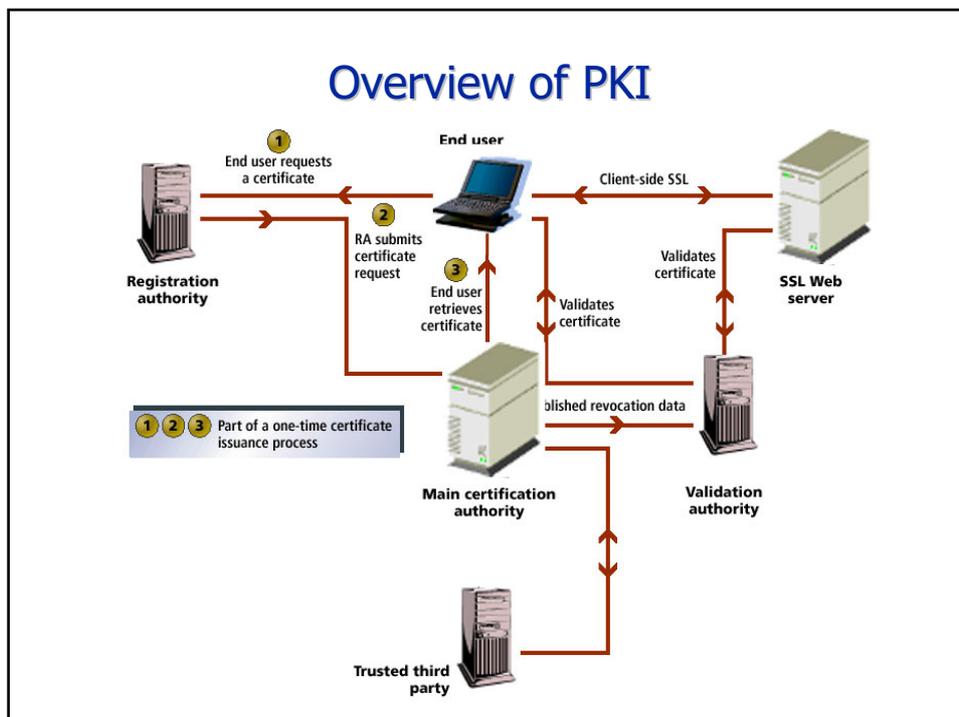
Encryption is not enough: Spoofs

- Pretending to be someone else
- Hard to login without someone's password
- But can send out communications with someone else's name on it
 - email
 - 1993: Dartmouth sent a message saying midterm exam was cancelled
 - Message appeared to come from the Professor!
 - netnews
 - world wide web

Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana

Digital Signatures

- Key property: Public and private keys can be applied in either order
- Alice has message M
 - She applies her **private key** to it
 - She sends encrypted message to Bob
- Bob decrypts it with Alice's **public key**
 - gets back original message
 - infers that Alice is indeed the sender (since only Alice has the private key that corresponds to her public key)
- In that way, encrypting a message with one's private key acts as a digital signature!



© Copyright 2003, This presentation based on material originally developed by Chrysanthos Dellarocas and Thomas W. Malone. All rights reserved.

**Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana**

PKI Industry

- Main players: trusted third party CAs
 - Verisign
 - Entrust
 - Cybertrust
 - RSA
- Revenue from
 - products (PKI servers for intranets and extranets)
 - services (certificate services for individuals and organizations)
- Revenue predictions (Datamonitor)
 - \$330 million for products \$347 million for services
 - Figures will grow to \$1.2b and \$1.4b resp. in 2006
- Mobile devices a big boost

SSL Certificates

- Used to certify a user's identity to another user
 - The certificate issuer's name
 - Who the certificate is being issued for (a.k.a the subject)
 - The public key of the subject
 - Some time stamps
- Digitally signed by issuer
- Issuer must be a trusted entity
- All users must have a reliable public key of the issuer
 - in order to verify signed certificate

Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana

Needed: Message Authentication

- Make sure Bob gets the message unaltered
- Don't let Alice deny sending the message



- Don't care about eavesdropper Darth, unless Darth changes the message
- How can cryptography help?

Public Key Management

- Public key cryptography works as long as
 - ✓ d is really kept secret
 - ✓ Hard to compute d from e
 - Get the correct e from some trusted source
- Bob can send public key over insecure communication channel
- But how do you know Darth didn't send you his key instead?

**Lecture notes for 15.566: Information Systems as
an Integrating Force in Manufacturing:
Prof. Brian Subirana**

A central key distributor

- Alice asks the distributor for Bob's public key
- The distributor sends it to Alice and "digitally signs" it
- Alice knows the key came from the distributor
 - Now just have to be sure that the distributor is honest and got Bob's key from Bob, not Darth
- Requires one secure communication per user
 - Bob sends public key to distributor when he joins the system
- Secret keys require secure communication between every pair of users

Public Key Infrastructure (PKI)

- Certificate Authorities are Trusted Third Parties charged with the responsibility to generate trusted certificates for requesting individuals organizations
 - Certificates contain the requestors public key and are digitally signed by the CA
 - Before a certificate is issued, CA must verify the identity of the requestor
- These certificates can then facilitate automatic authentication of two parties without the need for out-of-band communication