ICS 132: Organizational Information Systems

Security

TOP SECRET

---

what is security?

- the techno-geek answer:
  - cryptosystems, access control, intrusion detection
- the 132 answer:
  - security is about managing risk
    - risks can come from many sources
      - failure as well as malicious damage
    - *managing* risk rather than *eliminating* risk
      - the most secure system is one that can't be used
      - there's an inherent tension between security and practicality

---

why is it important?

- security for internal needs
  - protecting against failure or attacks
  - ensuring robustness and ability to deliver
  - failure recovery is costly!
- security for competitive advantage
  - customers require secure services
  - clients won't trust us with their information
  - everyone else is doing it…

---

security is a *system* feature

- security issues arise at specific points
  - giving out credit card details
  - identifying myself
  - using passwords
- but… think about the *temporal* issues
  - electronic systems make ephemeral information permanent
  - accumulated information yields patterns
    - and patterns provide information that you never thought you'd disclosed

---

sources of risk

- hardware malfunctions
- software bugs
- data errors
- damage to physical facilities
- inadequate system performance

- the overriding question: *liability*

---

threats of computer crime

- theft
- unauthorised use
- entering fraudulent data
- stealing/modifying data
- modifying software
  - back doors
  - trojans
  - viruses

other factors

- increasing complexity
  - systems are growing larger and more complex
  - increasing interdependence between components
  - failure modes interact and multiply
    - example: Three Mile Island
- human limitations
  - memory
  - attention
- business pressures
  - do more and do it faster

security and trust

- we think we understand trust
  - everyday phenomenon
  - based on personal contact and experience
- trust in the electronic domain?
  - what are the cues that engender trust for us?
  - who do you trust?
    - paul@dourish.com?
    - jpd013902@hotmail.com?

security and trust

- security is *manufactured trust*
  - if I trust my infrastructure, everything is fine
  - but if I don't, I need to put something into place
  - security measures allow me to trust the system
    - making guarantees about integrity
    - detecting intrusions and problems
- aspects of security
  - authentication
  - authorisation
  - accounting

manufacturing trust

- authentication
  - "I am who I say I am"
    - password systems
    - challenge/response
    - smart cards
    - biometrics

manufacturing trust

- authorisation
  - "I can do this"
    - capabilities
      - absolute capabilities
      - inference systems
    - delegation
    - revokable rights
    - physical access

manufacturing trust

- accounting
  - maintaining an audit trail
    - the ability to reconstruct what's happened
    - the ability to "roll back time"
  - accurately logging and billing
    - managing scarce resources
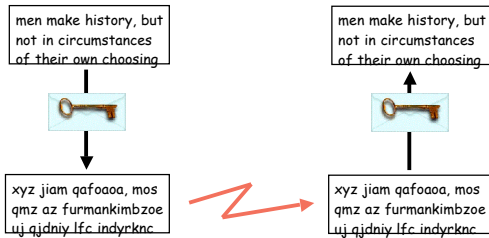
manufacturing trust

- privacy
  - privacy is more than not disclosing information
  - knowing *what* I disclose, *when*, to *whom*, and *why*
    - these are the conditions on which I can make an informed decision
  - what happens when the policy changes?
- two issues in privacy
  - trusting the recipient
  - trusting the channel

security strategies

- "security through obscurity"
- open access, strong firewall
- secure channels
- layered security
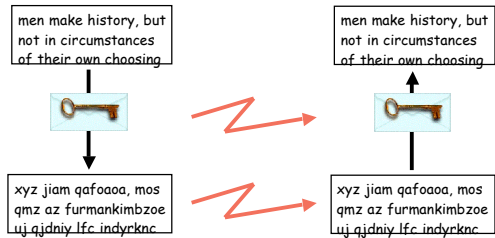- personalising security
  - don't trust technology, trust people

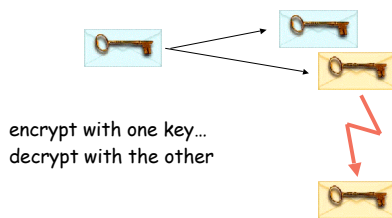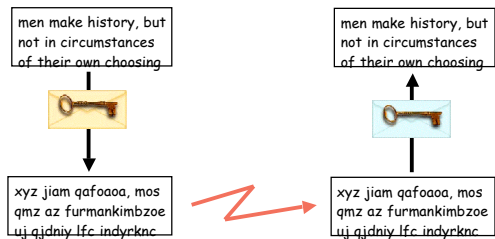## cryptosystems

- private key encryption

men make history, but not in circumstances of their own choosing

men make history, but not in circumstances of their own choosing

xyz jiam qafoaoa, mos qmz az furmankimbzoe uj qjdniy lfc indyrknc

xyz jiam qafoaoa, mos qmz az furmankimbzoe uj qjdniy lfc indyrknc

cryptosystems

- private key encryption

men make history, but not in circumstances of their own choosing

men make history, but not in circumstances of their own choosing

xyz jiam qafoaoa, mos qmz az furmankimbzoe uj qjdniy lfc indyrknc

xyz jiam qafoaoa, mos qmz az furmankimbzoe uj qjdniy lfc indyrknc

cryptosystems

- public key encryption

encrypt with one key…
decrypt with the other

cryptosystems

- public key encryption
  - encrypt with the RECIPIENT's public key

men make history, but not in circumstances of their own choosing

men make history, but not in circumstances of their own choosing

xyz jiam qafoaoa, mos qmz az furmankimbzoe uj qjdniy lfc indyrknc

xyz jiam qafoaoa, mos qmz az furmankimbzoe uj qjdniy lfc indyrknc

cryptosystems

- public key encryption – digital signature
  - encrypt with YOUR OWN private key

this document has been signed by Paul Dourish		this document has been signed by Paul Dourish

| jiam qafytaoa mos dddd nackme ax adiq mahqncx | → | jiam qafytaoa mos dddd nackme ax adiq mahqncx |
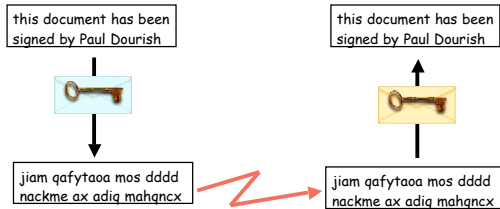
cryptosystems

- technology is only part of the problem
  - it is well understood, but think about *implementation*
- infrastructure obstacles
  - how do I find someone's public key?
  - what and whom do I trust?
- legislative obstacles
  - governments don't approve
    - in turn, this affects the atmosphere in which adoption occurs
  - encryption is an international phenomenon
    - governments have little reason to collaborate
      - encryption is okay for us, but not for you

security and usability

- remember, this is about trust
  - trust isn't a technical phenomenon
  - trust is an outcome of someone's evaluation
    - so, it needs to be comprehensible to the end party
- the inherent tension
  - security involves putting up barriers
  - usability involves tearing them down
- which barriers to use?
  - example: email deletion

the usability of passwords

- an example of the tension
  - the system manager's view
    - passwords should be obscure and hard to guess
  - the user's view
    - passwords should be simple and easy to remember
  - common results…
    - people set the same password everywhere
    - passwords written on post-it notes

visualising system security

- security is an end-to-end phenomenon
  - modern networks are remarkably bad at handling end-to-end issues
    - when I connect to Amazon.COM, who is responsible for security?
    - when I login from home to read my email, where does security reside?
  - example – S/Key and SecurID

the cost of security

- remember cost-benefit analysis
  - what does some level of security cost?
    - adds complexity to implementation
    - imposes restrictions on use
    - limits performance
  - what benefits result?
    - secure *enough*
  - example: Placeless Documents
    - SSL-based security model
    - Java 2 security model
      - the dangers of all or nothing!

summary

- security is an increasingly important issue
  - more work moved online
    - increases risks
  - new domains for interaction with customers
    - increases need for mechanisms of trust
- security is risk management
  - supporting informed decision making
  - making consequences clear

next time

- project
  - due on Thursday (March 6)
- next week's topic:
  - e-commerce
- the week *after* next
  - case studies/review lecture
    - let me know if there are specific topics