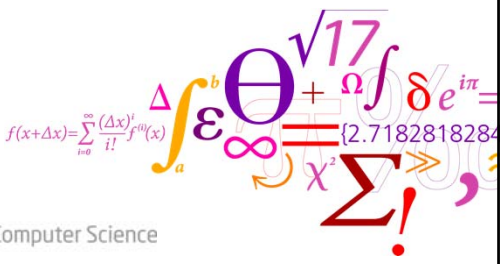
Trust is the Foundations for Computer Security

Christian Damsgaard Jensen

Department of Applied Mathematics and Computer Science
Technical University of Denmark

Christian.Jensen@imm.dtu.dk



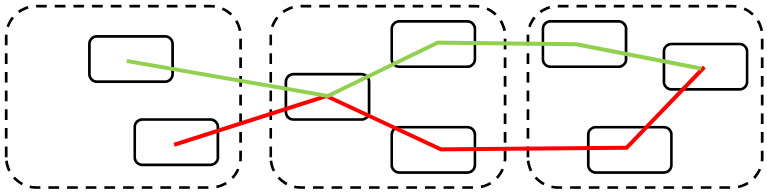
DTU Compute
Department of Applied Mathematics and Computer Science

Security and Trust

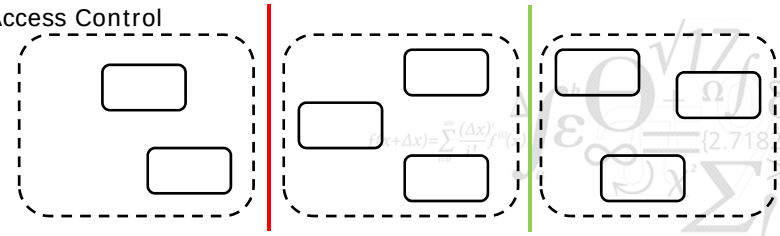
- Computer security is sometimes divided into:
  - Hard security (based on mathematics & formal methods)
    - *Authentication and Biometrics*
    - *information flow and access control*
    - *Formal modelling and analysis of software and systems*
    - *Cryptology*
  - Soft security (based on other scientific disciplines)
    - *Trust-based security mechanisms*
    - *Wiki-style access control*
    - *Security usability*
    - *Security awareness programmes*
    - *Security based on economic theory and games*
- Claim: Ultimately, it is all based on trust

Two Fundamental Models of Security

- Information Flow



- Access Control

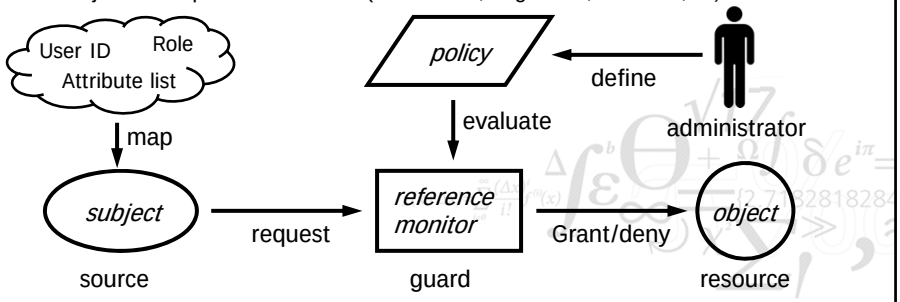


Information Flow Model

- Definition:
  - *The command sequence c causes a flow of information from x to y if, after execution of c, some information about the value of x before c was executed can be deduced from the value of y after c was executed [Matt Bishop]*
- Two types of information flow analysis
  - Program analysis
    - *Analysing information flows in a system where all components are known (and available for analysis)*
  - Protocol analysis
    - *Analysing information flows between components in a system where not all components are known*
- Information flow analysis provides guarantees (assurance) about the enforcement of the security policies
  - Requires that the components are known

Access Control Model

- Security policy is evaluated every time an object is accessed
  - Reference Monitor mediates all access by subjects to objects
    - *Guards access to object*
    - *Interprets access control policy*
  - Subjects are active entities (users, processes)
  - Objects are passive entities (resources, e.g. files, devices, …)



Mapping Subjects in Access Control

- Identity Based Access Control
  - Permissions are granted directly to users
  - Unique system identifier (UID) for every user
  - User identity must be verified before use (authentication)
- Role Based Access Control
  - Permissions are granted to roles
  - Users assigned one or more roles
  - User identity must be verified before role is assumed (authentication)
- Attribute Based Access Control
  - Permissions depend on user's attributes
  - Users must prove possession of attributes
    - *Attributes are often encoded in certificates*
  - Use of certificates often require user's public-key
    - *Use of public-key certificate implies authentication*
- Ultimately, users normally prove identity to exercise access rights

Role of Identity in Computer Security

- The user identity serves three primary purposes:
  - It allows the authentication of subjects
    - *Validation of enrolled users*
    - *Real world identity is difficult/expensive to change*
  - It allows different permissions to be granted to different subjects
    - *Defined in the access control policy*
      - Enforce Principle of Least Privilege
      - Enforce constraints, e.g. Separation of Duty
    - *Ultimately based on the identity mapped to the subject*
  - It allows accountability
    - *Record the identity mapped to the subject performing an action*
    - *Log serves as evidence if something goes wrong*

Semantics of Identity in Computer Security

- Identity defines on which side of the perimeter an agent belongs
  - Only insiders (enrolled in the system) have system identifiers
- Semantics of (real world) identity
  - String of bits that names an entity (person, machine, process …)
  - Distinguish particular entity from similar entities
  - Difficult and time consuming to get another string of bits
- What makes me Christian Damsgaard Jensen?
  - My parents liked the name
  - Name recorded in birth certificate
  - Danish government issues identity certificates to me
- Identity is simply a string that someone is willing to authenticate
  - Nothing more
- Security properties of system cannot be derived from identity alone

Basis for assigning privileges

Employment contract

Social norms

Company policies

What constrains the behaviour of subjects?

Criminal law

- Security depends on ”the system’s” ability to enforce these rules

Human Notion of Trust

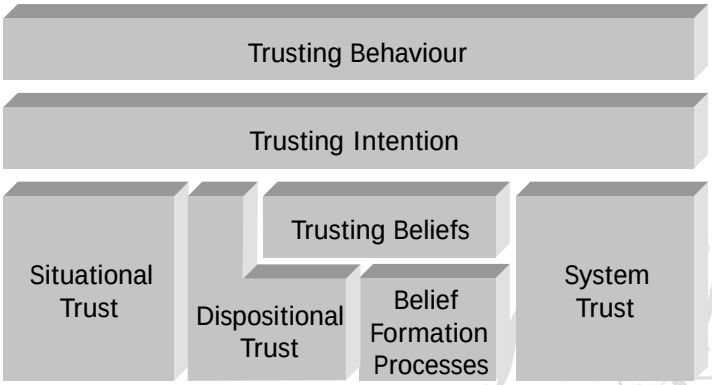
Decision to trust or not

Behaviour of another person

Ambiguous path

- Human notion of trust
  - A person is confronted with an ambiguous path that may lead to something beneficial or something harmful
  - He perceives that the occurrence of the beneficial or harmful event is contingent on the behaviour of another person
  - If he chooses to take an ambiguous path with such properties, he makes a trusting choice but exposes himself to some risk

Elements of Trust



(McKnight & Chervany, 1997)

Security in Online Transactions

- Consider a standard e-commerce scenario
  - Alice wants to buy a new camera

Trust in directory and reputation services

Customer trust in web-shop
- Genuine
- Honest
- Competent

Both parties must trust the common infrastructure

- *computing platform*
  - browser/webserver
  - plugin and libraries
  - operating system
  - hardware
- *network infrastructure*
  - naming
  - routing
  - confidentiality
  - integrity

Web-shop trust in customer
- ability to pay

Trust in Directory and Reputation Services

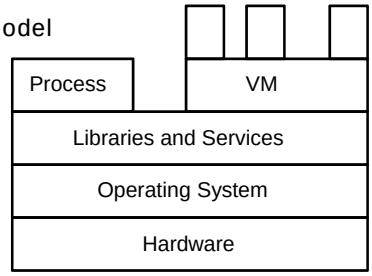
- How do we decide who to interact with?
  - How do we locate service providers
    - *Search engines and web portals*
      - Google, Yahoo, Pricerunner, …
      - Private companies
  - How do we decide which one to interact with?
    - *Reputation systems*
      - eBay, Trustpilot, Epinions, trip-advisor, …
    - *Recommendation systems*
      - Web-shields
      - Testimonials on service providers web-site
- Security models and mechanisms don't really consider these issues
  - " … considered beyond the scope of the model"

Customer Trust in Service Provider

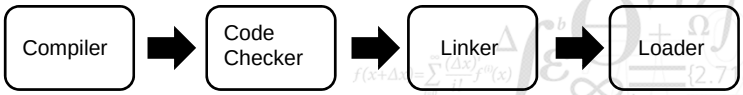
- Genuine
  - Link business to webserver (DNS name registration)
  - Link webserver to IP address (DNS resolution)
  - Authenticity of party at the other end of communication channel
    - *Authentication protocol (https, SSL, TLS, …)*
    - *Typically based on certificates and PKI*
- Honesty and Competence
  - Basically not considered by the security model
  - Impossible to enforce through logical security mechanisms

Trust in Common Infrastructure
Security of the Computing Platform

- Classic system model



- Tool chain is also important



- Read Ken Thompson's "Reflections on Trusting Trust"

Trust in Common Infrastructure
Security of Network Infrastructure

- Lookup services
  - Lookup Protocol (DNS, ARP, …)
  - Lookup service platform (Name Servers)
    - *Same issues as other computing platforms*
- Routing Fabric
  - Routing Information Protocol
  - Routing fabric platform (Routers)
    - *Same issues as other computing platforms*
- Message Confidentiality & Integrity (Cryptology)
  - Cryptographic algorithm developers and reviewers
  - Crypto-library developers (and reviewers)
  - Crypto-system installation and operation
  - Key generation and distribution
  - Key management and hygiene

Summary
From computer models to reality

Conclusions

- Computer and network security define properties that can be enforced by the computer system
  - Information flow analysis
  - Access Control Mechanism
- Most Computer Systems consist of a collection of software executed on hardware and communicating through networks
  - Many of these have never been thoroughly analysed in combination
- Ultimately, security assurances rely on
  - Correct specifications (trust in system architect)
  - Correct implementation (trust in system developers)
  - Correct execution (trust in hardware manufacturers)
  - Correct configuration (trust in system administrators and HR)
  - Correct operation (trust in the computer users)
- In order to achieve security, this trust must be explicitly managed