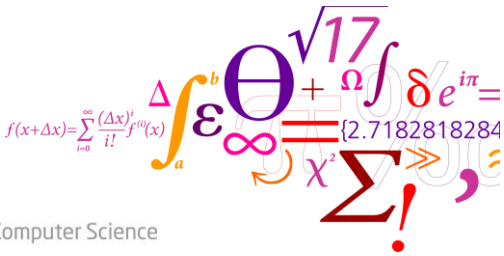
How to Build and Manage Trust Online

Christian Damsgaard Jensen

DTU Compute
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

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"

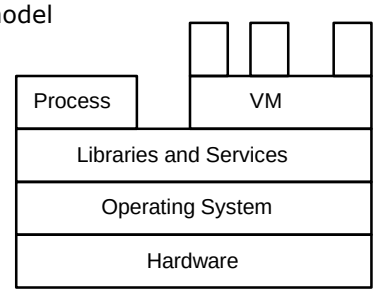
Customer Trust in Service Provider

- 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*

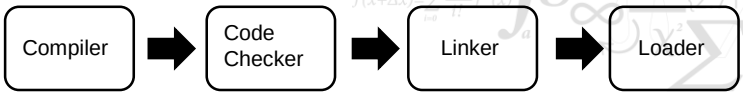
- Honesty and Competence
  - Basically not considered by the security model
  - Impossible to enforce through logical security mechanisms

Trust in Common Infrastructure Security of the Computing Platform

- Classic system model



- Tool chain is also important



Trust in Common Infrastructure
Security of Network Infrastructure

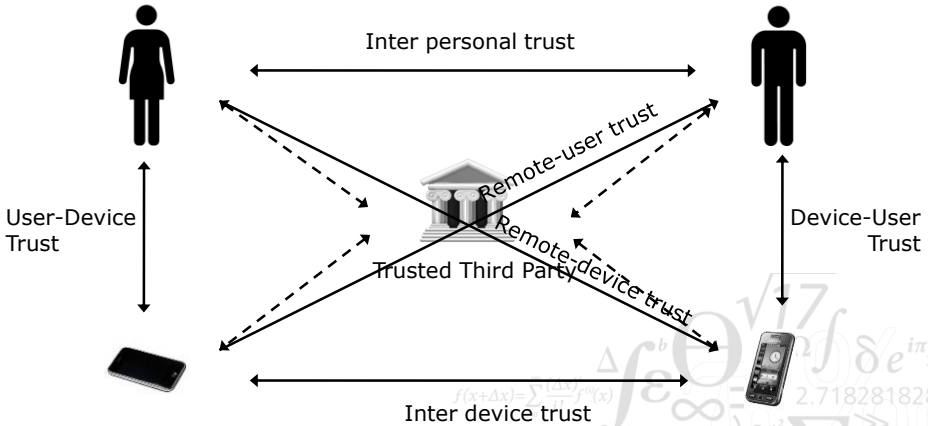
- Lookup services
  - Lookup Protocol (DNS, ARP, …)
  - Lookup service platform (Name Servers)
    - *Same issues as other computing platforms*
- Routing Fabric
  - Routing Information Protocol
  - Routing fabric platform (Routers)
    - *Same issues as other computing platforms*
- Message Confidentiality & 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

Trust in Context

- The need for trust depends on context and risk
  - Risk involved in interaction (cost of misplaced trust)
  - Environment (contributes to probability of trust being misplaced)
    - *Infrastructure trust*
    - *System trust*

- Environmental factors
  - Location
  - Presence of other parties (friends or strangers)
  - Presence of specific infrastructure
    - *Secure communication*
    - *Trusted third parties*
  - Enforcement of stated policies
    - *Sanctions against misbehaving entities*

Trust Relationships



Inter Personal Trust

- Trust between two persons (humans, legal persons, …)
  - Trying to predict the behaviour of the other person
- Based on Previous Experience
  - Outcome of previous interactions
    - *Problem to assess whether outcome was positive or negative*
- Based on Recommendations
  - "Signed" statement about the recommended entity
  - Proactive system
- Based on Reputation
  - Reputation service, majority voting, …
  - Reactive system

User-Device Trust

- Confidence that the user has in device
- Based on user's own experience
- Based on opinions of friends (Recommendations)
  - Friend-of-a-friend (FOAF) systems
- Based on reputation of manufacturer
  - Collaborative filtering
- Based on certification (recommendations)
  - Common Criteria

Device-User Trust

- Confidence that the device has in user
- First step is user authentication
  - Knowledge-based (something you know)
  - Token-based (something you have)
  - Biometrics (something you are)
  - Strength of authentication (single vs. multi-factor authentication)
  - Is authentication still valid
- Is user behaviour consistent?
  - With previous behavioural patterns (behavioural biometrics)
    - *Yes ⇒ device comfort (in comfort zones)*
    - *No ⇒ anomaly detection*

Inter-Device Trust

- Cryptology and Network security
- Device authentication (Sybil Attack)
  - Shared secret
  - Trusted third parties (KDC, trusted introducers)
  - PKI
- TCG Remote Attestation
- Automated Trust Negotiation
  - Policy based exchange of certificates
- QoS assessment
  - Proposed for peer-to-peer (P2P), Mobile Ad-hoc NETworks (MANETs), sensor networks, routing protocols,

Remote-User Trust

- Distributed access control
- Based on decentralised policies (policy based)
  - Trust Management Systems like KeyNote
    - *Assertions about entities*
    - *Inference engine decides if policy is met*
  - Appropriate for Autonomic Computing
- Based on computational trust (experience based)
  - Assess risk of interaction in context
  - Decide if sufficient level of trust is present
    - *Direct comparison of risk/trust*
    - *Indirect, e.g., trust above threshold that allows a certain role*

Remote-Device Trust

- User's trust in a remote device (or service)
- Standard means of assessment
  - Experience, recommendations, reputation systems
- Based on device ownership
  - Transitive interpersonal trust relationship
- Anomaly/outlier detection (e.g., sensor networks)
- Representation of result of inter-device trust establishment
  - Certification and remote attestation
  - Automated trust negotiation
  - Confidence in device authentication and key establishment

Implementing Trust Management Systems

- Example: System to facilitate opportunistic collaboration
  - Ad hoc collaboration between users in a ubiquitous computing system
- User has to trust her own device
  - Certification of device
  - Secure boot (TPM)
- Both users' devices have to establish secure channel
  - Device Authentication
    - *Automated Trust Negotiation*
    - *Certificate authorities*
  - Setting up cryptographic keys (symmetric-/asymmetric cryptography)
- Remote user's device has to trust remote user
  - User authentication
  - Persistence of authentication

Summary

- Examined the problem of 1-1 trust between users and devices
- Presented a classification of 6 trust relationships
  - Inter personal trust
  - User device trust
  - Device user trust
  - Inter device trust
  - Remote user trust
  - Remote device trust
- Trusted third parties are useful mediators of trust in many cases
  - Personal through recommendations
  - Institutional through reputation systems
- Important progress is made in most areas, but much remains to be done

Summary II
From computer models to reality

IFIP Working Group 11.11 on Trust Management

- International working group focusing on Trust and security
- Scope
  - semantics and models for security and trust;
  - trust management architectures, mechanisms and policies;
  - trust in e-commerce, e-service, e-government;
  - trust and privacy; (link with wg 9.6 / 11.7)
  - identity and trust management; (link with wg 11.6)
  - trust securing digital as well as physical assets;
  - social and legal aspects of trust (link with wg 9.6 / 11.7)
- IFIPTM is the annual conference
  - Next year in Darmstadt during the "Security Week" (July 2016)

http://www.ifiptm.org