Prototypische Erstellung eines Online-Bestellmoduls für Schließanlagen

Tim Krämer

outline

1. general
2. Definition of task
3. Identification
4. Requirements to the software
5. Investigation of possible attacks
6. My solution

general

Tim Krämer (7kraemer@inf...)

please aks your questions directly!

download slides and sources here: https://tim-kraemer.de/BA

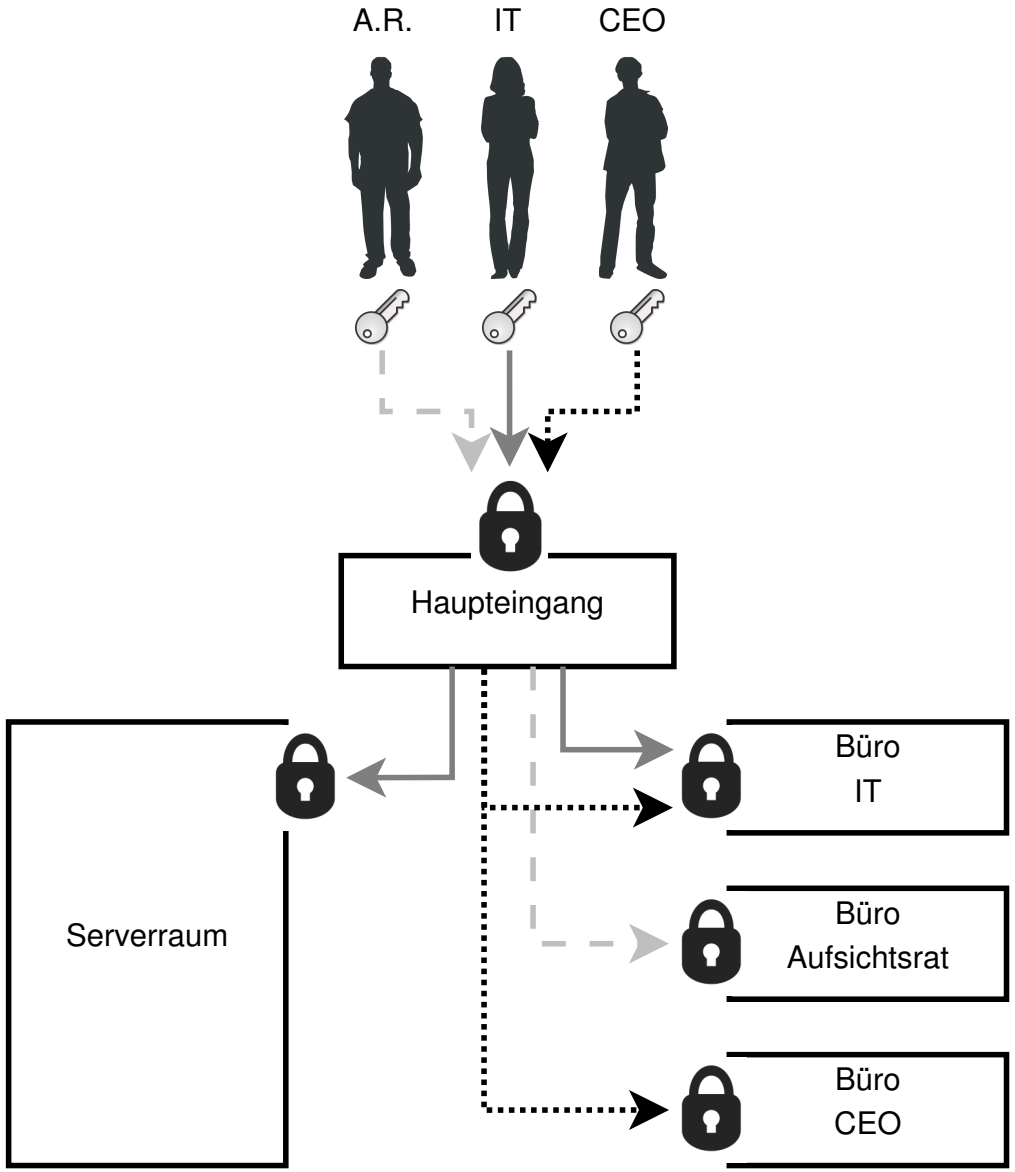
Definition of task

- creating a concept for a software based order in the context of master-key systems

What is a master-key system?

- used in doors and special devices against unauthorised use or openings
- known concept of locks and keys - with a speciality:
  - one lock can be opened by multiple keys
- results in: every person needs just one key for the whole building

What is a master-key system?



Back to the task

- speak to your lock-smith or supplier of master-key systems to get new keys (or locks)
- but: customers want to order keys online

Whats the difference in contrast to typical consumer products?

- keys must not fall into wrong hands
- (low-cost) mechanic keys are easy copyable
- unauthorised access to information about your system could be a security risk:
  - how many cylinders/doors are there? how many keys? in which quality?

Where is this data?

- usually you don’t cut keys, or build cylinders
- lock-smiths or manufacturers of master key systems are in possession of your master-key system data
- they have to match you to your data
- results in: Identification to get a new key or modifications

Identification

- currently: done by your supplier (e.g. he knows you personally or via id-card)
- additional non-digital identification methods

Requirements to the software

- a nice GUI and easy functions to create an order
- an identification progress
- an encrypted communication channel
- an interface to the suppliers/manufactures software-systems

Investigation of possible attacks

- examination of attacks against the current identification methods
- compared to attacks against software-based methods

- current used non-digital identification methods: mostly safe against attackers from outside
- but: not exactly comfortable for the customers
- comfortable orders via internet represent a high security risk:
  - sufficient identification is hard to ensure via e-mail
  - non encrypted data-transfer via internet could easily be eavesdropped

My solution

- encrypted mail is not distributed and easy enough
- web-shop systems does not fulfil the identification requirements

My solution

On the customers side:

1. create your order
2. sign your order with your private key (read from external device, e.g. a crypto-chipcard)
3. send your signed order over an encrypted channel to your supplier

On the suppliers/manufacturers side:

1. receive an order
2. verify the signature with the help of a public-key database of your customers
3. check for errors in the order (possibly fix those errors for your customer)
4. send the ordered items to your customer

Thanks!

Thank you for your time!