CS 5430

Goals and Requirements

Prof. Clarkson
Spring 2016

(see CMS for files; do at home; we'll discuss it at beginning of next class)

EXERCISE: CHROMIUM BROWSER

SECURITY REQUIREMENTS

Methodology

- Functional requirements
- Threat analysis
- Harm analysis
- Security goals
- Feasibility analysis
- Security requirements

Functional requirements

- Security = **does what it should** + nothing more
- Should be **testable**: a 3rd party could determine whether requirement is met
- User stories:
  - brief description of single kind of interaction user can have with system
  - "As a *user* I can *action* so that *purpose*"
  - Examples from CMS:
    - As a professor, I can create a new assignment by specifying its name, number of possible points, and due date.
    - As a student, I can submit a file as a solution to an assignment.
- These stories reveal system assets

Threat analysis

- Identify threats of concern to system
  - Especially malicious, human threats
  - What kinds of attackers will system resist?
  - What are their motivations, resources, and capabilities?
- Best if analysis is specific to system and its functionality
- Non threats?
  - Trusted hardware
  - Trusted environment
  - e.g., physically secured machine room reachable only by trustworthy system operators

Harm analysis

- Harm: action adversely affects value of asset
- Harm to...
  - confidentiality: disclosure
  - integrity: modification
  - availability: deprivation
- "Performing *action* on/to/with *asset* could cause *harm*"
  - e.g., "stealing money could cause loss of revenue"
  - e.g., "erasing account balances could cause loss of customers"

Harm triples

- (action, asset, harm)
  - e.g., (theft, money, loss of revenue)
  - e.g., (erasure, account balance, loss of customer)
- Useful methodology:
  - start with asset
  - brainstorm actions that could harm asset
  - let brainstorming be guided by CIA triad

(Just the Harm Analysis)

EXERCISE: GRADE MANAGEMENT

Security goals

- "The system shall prevent/detect *action* on/to/with *asset*."
  - e.g., "The system shall prevent theft of money"
  - e.g., "The system shall prevent erasure of account balances"
- Specify **what** not **how**
- Poor goals:
  - "the system shall use encryption to prevent reading of messages"
  - "the system shall use authentication to verify user identities"
  - "the system shall resist attacks"

Feasibility analysis

- Not all goals are feasible to achieve
- Relax goals:
  - "prevent theft of items from a vault"
  - to "resist penetration for 30 minutes"
  - or to "detect theft of items from a vault"

From goals to requirements

- Goals: what should never happen in any situation
  - not testable
- Requirements: what should happen in specific situations
  - testable

Security requirements

- Constraints on functional requirements, in service of security goals
- Example:
  - **Functional requirement:** allow people to cash checks
  - **Security goal:** prevent loss of revenue through bad checks
  - **Security requirement:** check must be drawn on bank where it's being cashed (so funds can be verified), or customer must be account holder at bank and depositing funds in account (so funds could be reversed)

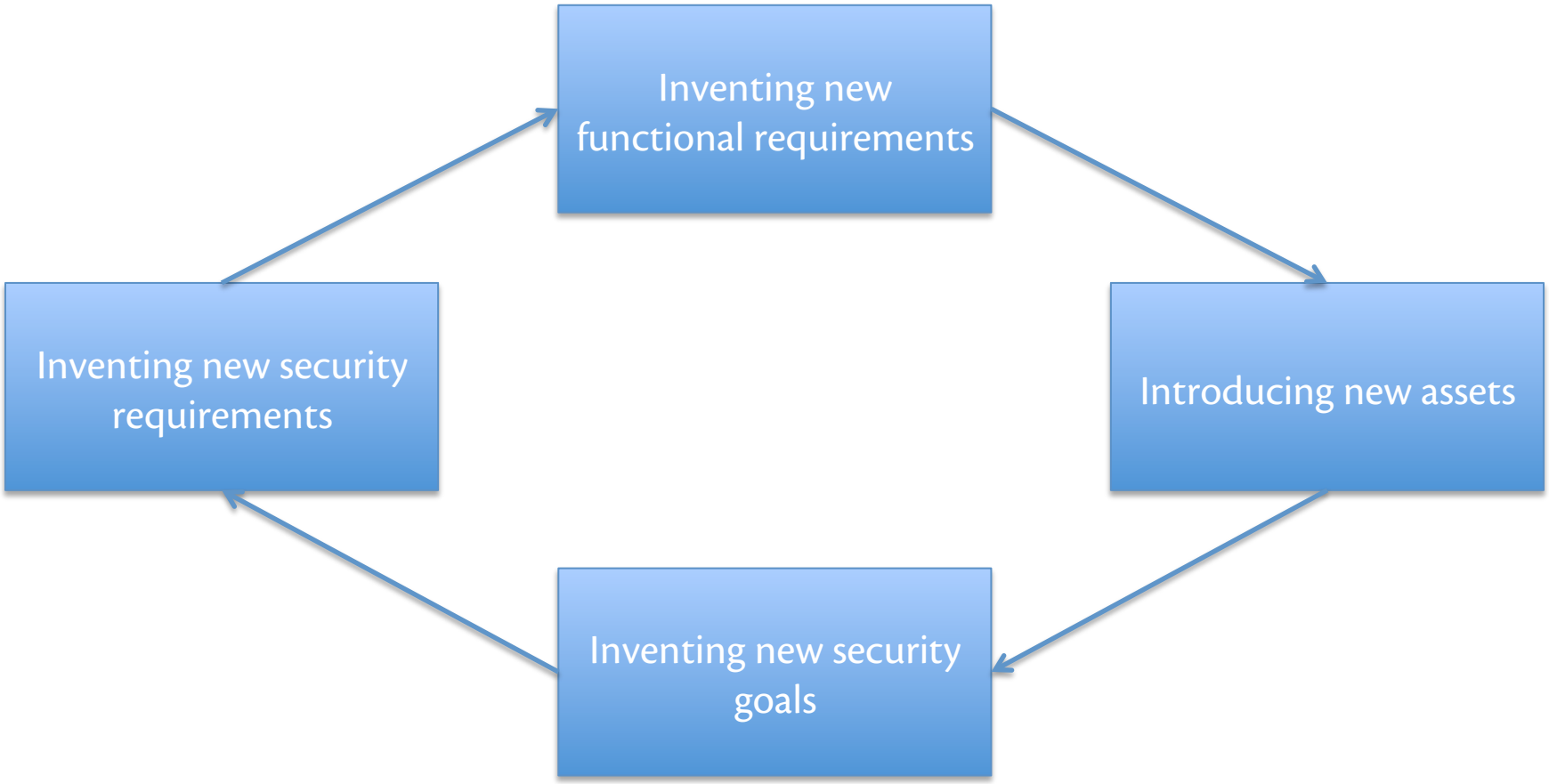
Security requirements

- Constraints on functional requirements, in service of security goals
- Another example:
  - **Functional requirement:** allow two users to chat using IM
  - **Security goal:** prevent disclosure of message contents to other users
  - **(Poor) security requirement:** contents of message cannot be read by anyone other than the two users
  - **(Improved) security requirement:** message is encrypted by key shared with the two users
    - doesn't over-commit to encryption algorithm, key size, etc.

Goals vs. requirements

Goals	Requirements
Broad scope	Narrow scope
Apply to system	Apply to individual functional requirements
State desires	State constraints
Not testable	Testable
Not about design/implementation details	Provide some details

Iteration


Inventing new functional requirements
Introducing new assets
Inventing new security goals
Inventing new security requirements

(Goals and Requirements)

EXERCISE: GRADE MANAGEMENT

Upcoming events

- [today] A1 due

"A desire presupposes the possibility of action to achieve it; action presupposes a goal that is worth achieving." – Ayn Rand