# Software System Architectures (NSWI130)

## Security

Martin Nečaský
Faculty of Mathematics and Physics
Charles University in Prague

# Security Quality Attribute

- measure of ability to protect data and information from unauthorized access
  - unauthorized access to read or modify data
  - denial-of-service
- unauthorized access attempt is called *attack*

# Security Goals

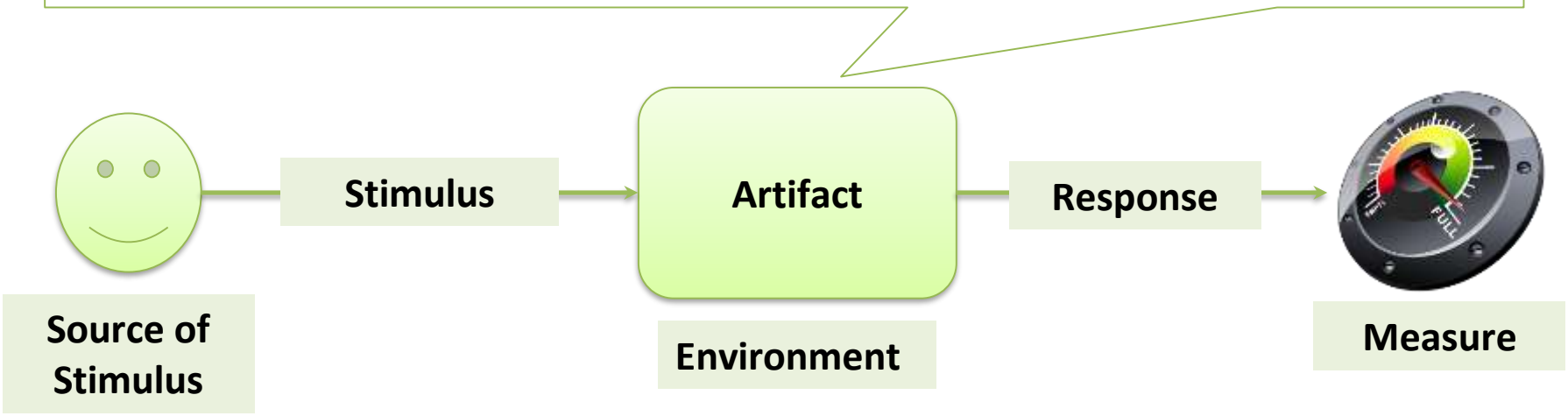
- confidentiality
  - data or services not subject to unauthorized access
- integrity
  - data or services not subject to unauthorized manipulation
  - persisted + transferred data
- availability
  - data or services available for legitimate use

# Security Goals

- authentication, authorization
- nonrepudiation
  - sender cannot deny having sent a message
  - receiver cannot deny having received a message

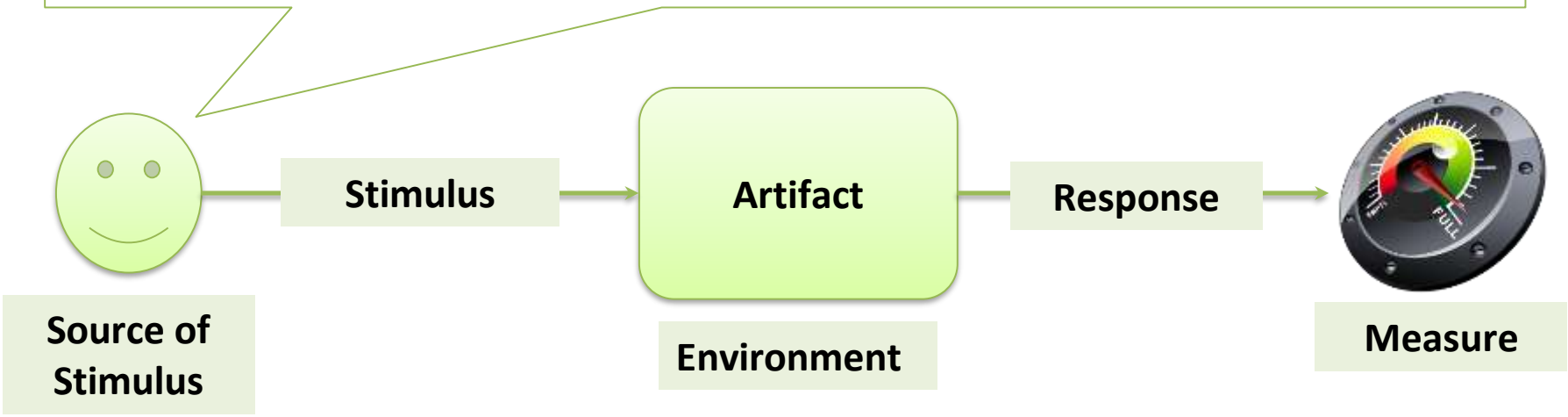
# Security Requirement Scenario

- system's service or data



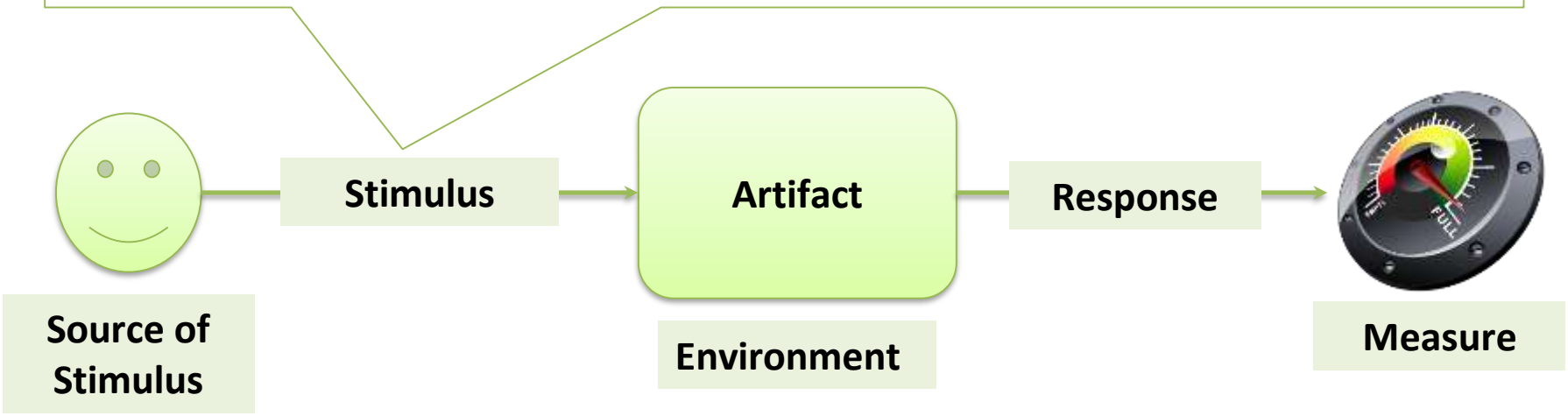
# Security Requirement Scenario

- attacker
  - human or system
  - known or unknown
  - internal or external



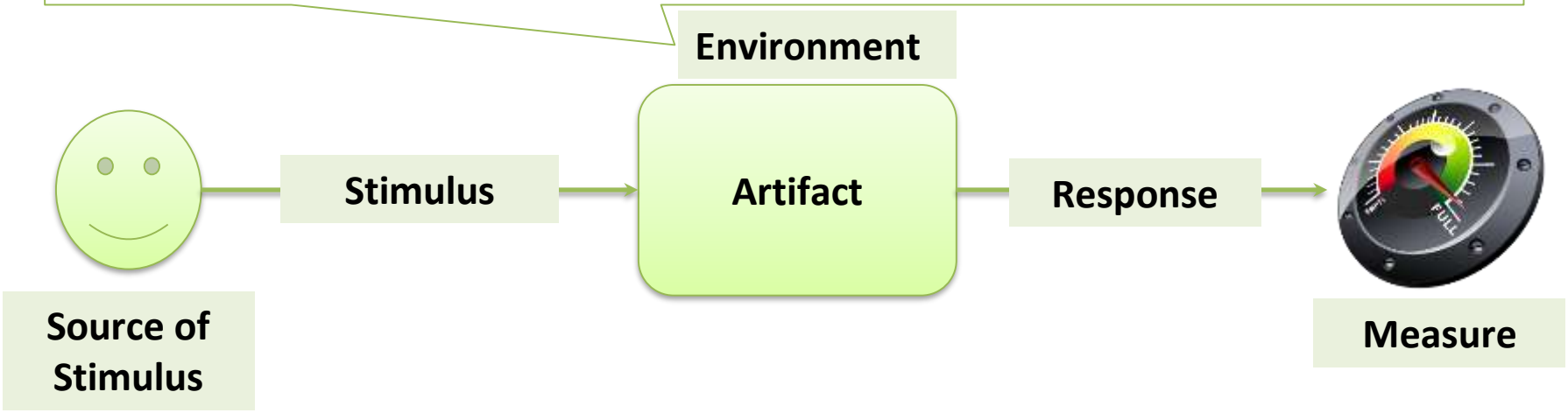
# Security Requirement Scenario

- attack = unauthorized attempt to
  - display, change or delete data
  - access or change behavior
  - reduce availability



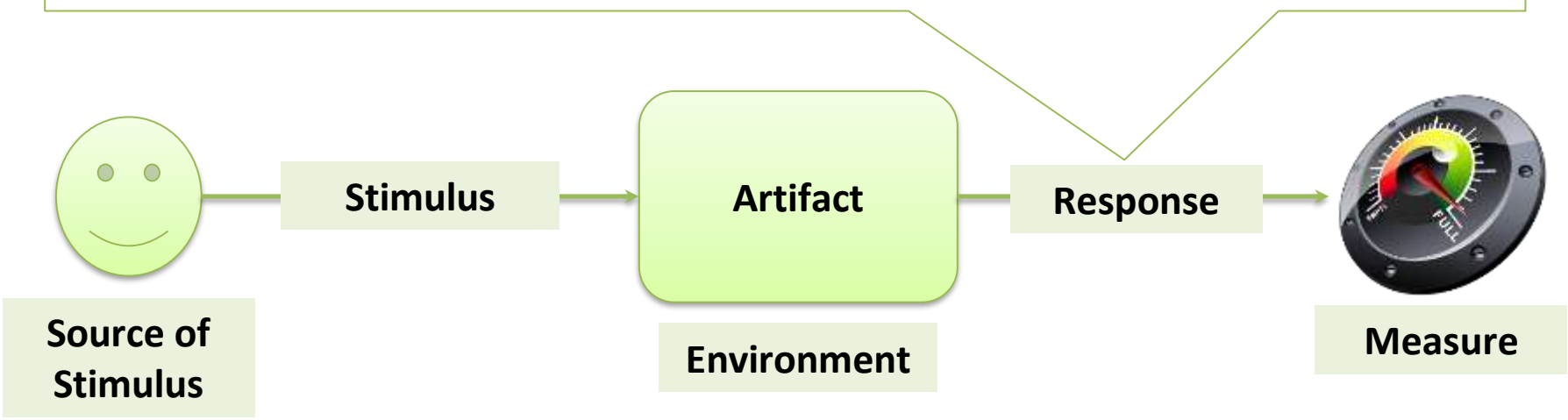
# Security Requirement Scenario

- online or offline
- in internal network or demilitarized zone or open to the internet



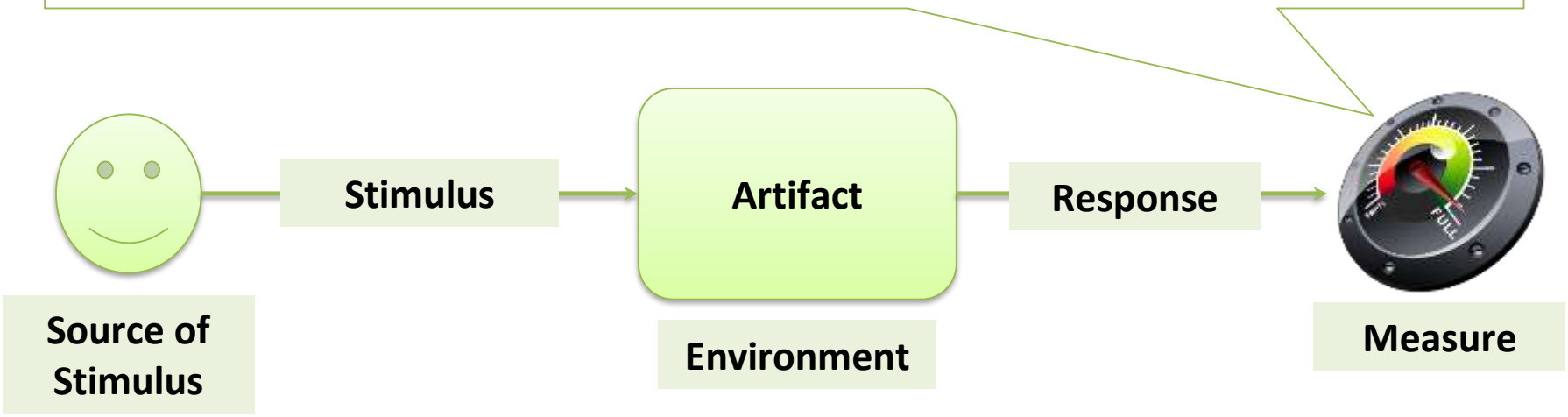
# Security Requirement Scenario

- confidentiality, integrity and availability preserved
  - data or services protected from unauthorized access and manipulation
  - response parties identified
  - supporting actions - audit trail, notifications
- nonrepudiation
- attackers identified or deterred



# Security Requirement Scenario

- compromised part of the system
- time passed before attack detection
- number of attacks resisted
- time to recover from successful attack



# Sample Security Scenario

**Source:**
Known human - employee

**Stimulus:**
Change data – Modify pay rate table

**Artifact:**
Pay rate table

**Environment:**
open to network

**Response:**
Pay rate table modification is identified, the attacker cannot repudiate the modification, data is restored


**Measure:**
Identification and data restoration in 1h

# Sample Security Scenario

**Source:**
Unknown human

**Stimulus:**
Change data –email with ransomware which encrypts all files on network disks

**Artifact:**
Hospital system

**Environment:**
internal network

**Response:**
Ransomware detected, email deleted


**Measure:**
Detected immediately for 90 % of attacks. When attack successful ransomware detected and data restored from backups in 48 hours

# Sample Security Scenario

**Source:**
Known external catalog

**Stimulus:**
Request to catalog high number of odd datasets to make harvesting service unavailable

**Artifact:**
Harvesting service

**Environment:**
open to internet

**Response:**
Harvesting other external catalogs not affected

**Measure:**
DoS detected during the attacked harvesting task, external catalog recorded in the audit trail,
national open data catalog and local catalog administrators notified

# Security Tactics

- detecting attacks (motion sensors in your house)
- resisting attacks (lock on your doors)
- recovering from attacks (insurance)

# Detecting Attacks

- detect intrusion
  - pattern analysis
- detect service denial
  - pattern analysis in network traffic
- verify incoming message integrity
  - cheaper alternative to detection

# Resisting Attacks

- actor authentication
- actor authorization
- limit access
  - Demilitarized zone between two firewalls – one facing the public internet, the other facing the intranet
- limit exposure
  - limit services available on a single host
  - conceal facts about where services and hosts are located
- data encryption
- separate data entities

# Recovering from Attacks

- restoring state
  - See Availability Tactics
- attacker identification
  - audit trail must be maintained