

A Sociotechnical Systems Perspective on the Science of Security and Privacy

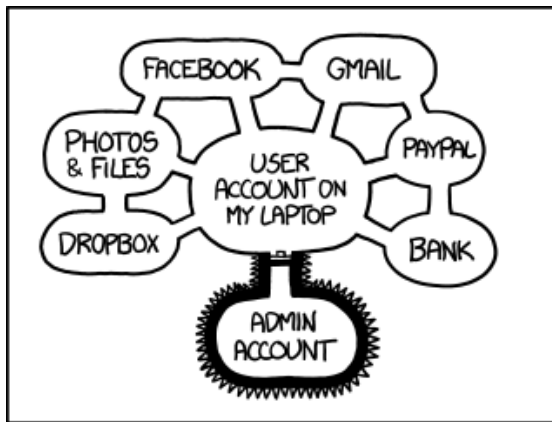
Munindar P. Singh

singh@ncsu.edu

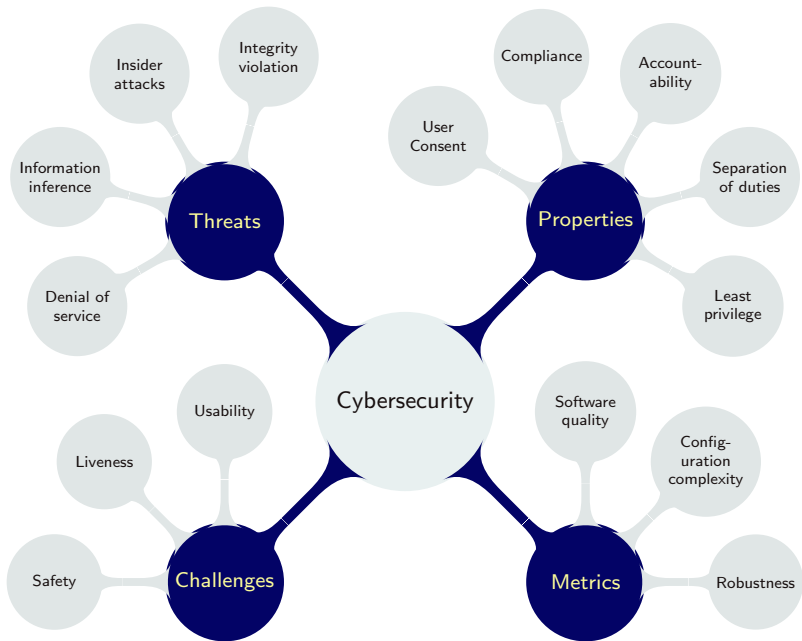
(Joint work with Özgür Kafalı and Nirav Ajmeri)

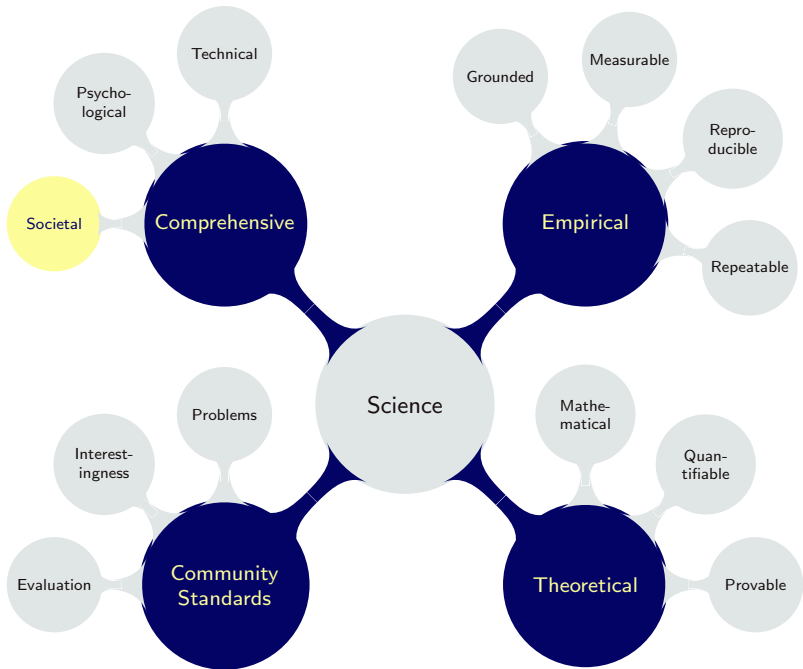
Department of Computer Science
North Carolina State University

XKCD's Assessment of Cybersecurity Today



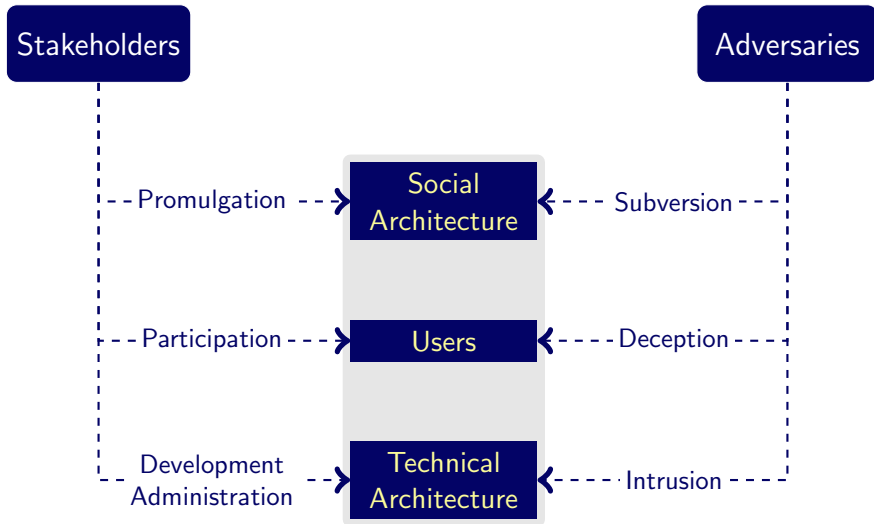
IF SOMEONE STEALS MY LAPTOP WHILE I'M
LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY
MONEY, AND IMPERSONATE ME TO MY FRIENDS,
BUT AT LEAST THEY CAN'T INSTALL
DRIVERS WITHOUT MY PERMISSION.





Participants and Artifacts in Security

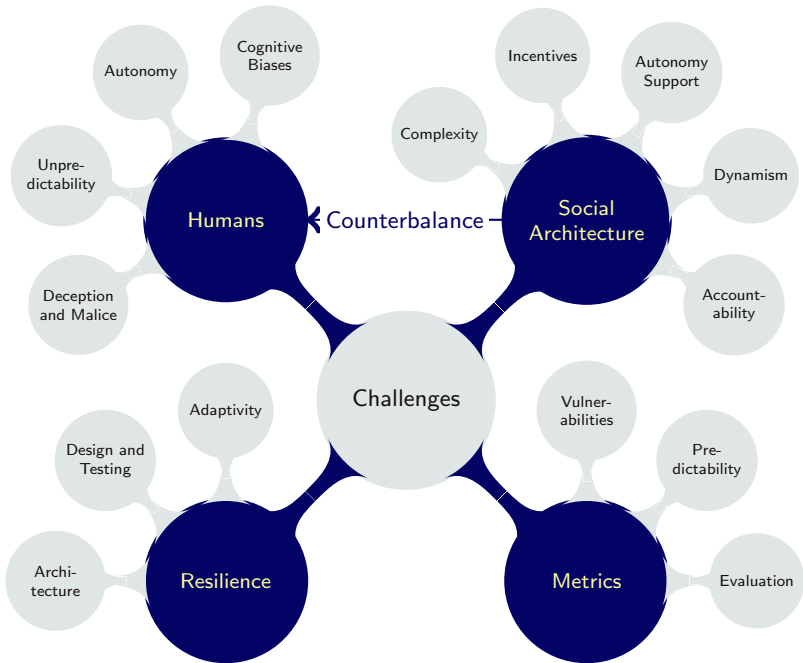
Greatest challenges arise in the upper two; most past effort is on technical architecture

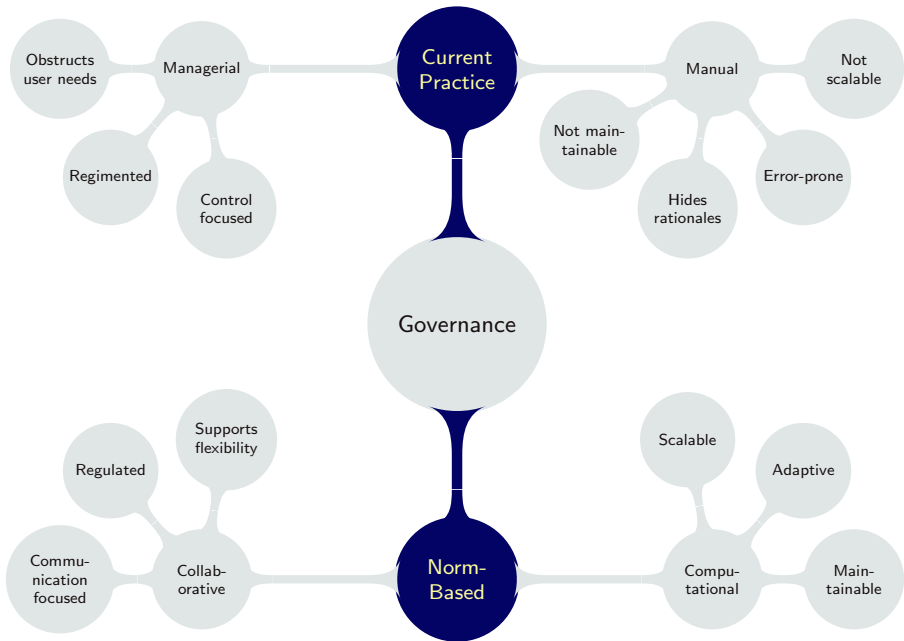


Usability and Strange User Behavior

Can we protect users from themselves?



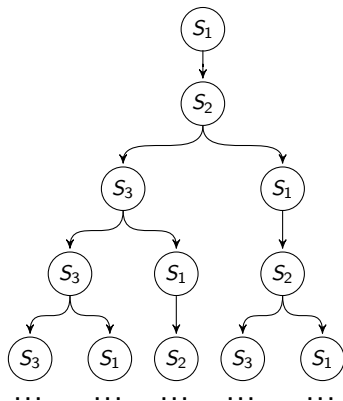
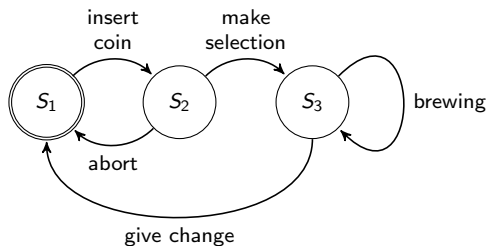






Vending Machine in Vienna

Conventional formal methods assume regimentation, i.e., a technical service



AF[Brew]: On every path, coffee is eventually brewed

A[\neg Brew U Coin]: On every path, no coffee is brewed prior to payment

©Fachhochschule Technikum Wien

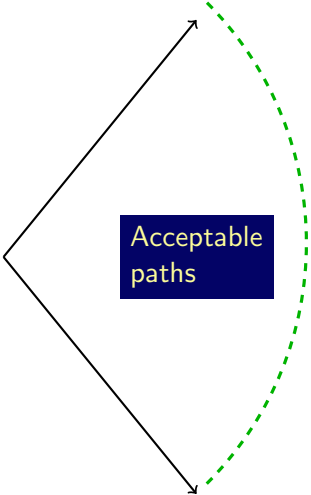
<http://embsys.technikum-wien.at/projects/decs/verification/formalmethods.php>

Regimentation: Violations are Impossible

Viable assumption in a closed system

All paths the machine can generate in its environment

Acceptable paths



Vending Machine in Valencia

A business service

- ▶ Tall structure
- ▶ Hard to reach for short people
- ▶ Is that a bug or a feature?



Vending Machine Close Up: Cigarettes!

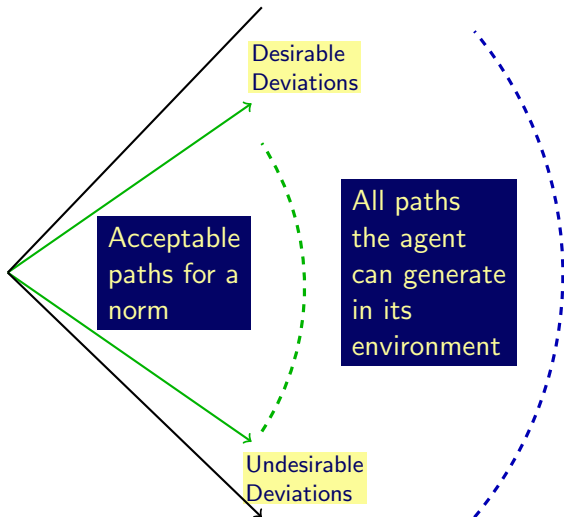


Regulation

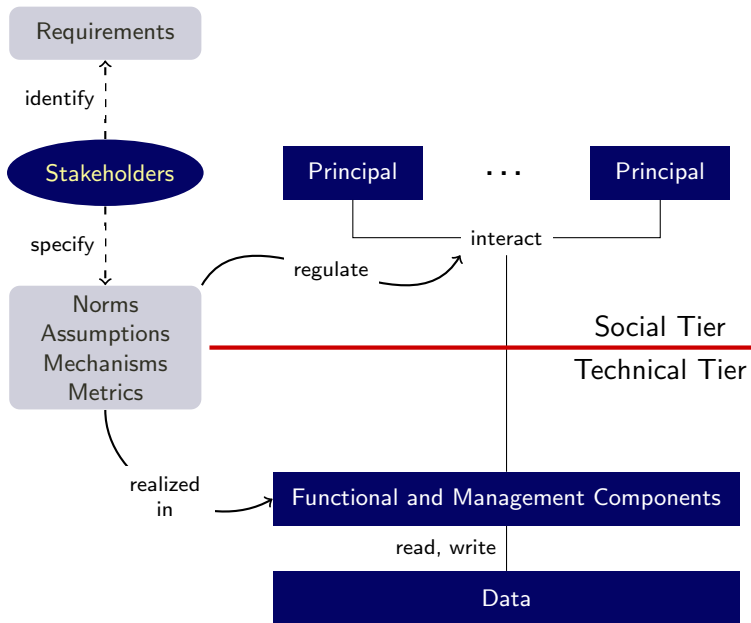


Regulation: Violations are Possible

Appropriate assumption when dealing with autonomous parties



Specifying and Enacting Sociotechnical Systems



Emergency Scenario

- ▶ Hospital authorizes Physician to enter the emergency department
 - ▶ `authorization(physician, hospital, swipe_card, access_PC)`
- ▶ Hospital authorizes Physician to access the patient's health records
 - ▶ `authorization(physician, hospital, consent ∨ logged_in, EHR)`
- ▶ Hospital prohibits Physician from accessing EHRs of other patients
 - ▶ `prohibition(physician, hospital, logged_in, nonpatient_EHR)`
- ▶ Physician commits to Hospital to log off after reviewing EHR
 - ▶ `commitment(physician, hospital, EHR, ¬logged_in)`
- ▶ Hospital prohibits Physician from disclosing patient's protected health information (PHI) online
 - ▶ `prohibition(physician, hospital, EHR, disclose_PHI_online)`

Requirements

- r_1 : Patient's PHI must not be published online
 - ▶ AG (\neg disclose_PHI_online)
- r_2 : Physician must be allowed access to EHR in emergency (with or without consent)
 - ▶ AG (emergency \rightarrow AF (EHR))
- r_3 : Open sessions must be closed after reviewing EHR
 - ▶ AG (EHR \rightarrow AF (\neg logged_in))
- r_4 : In case of a disaster, physician must be able to share the patient's PHI with family members on some path
 - ▶ AG (disaster \rightarrow EF disclose_PHI_family)

Refinement via Design Patterns

R-Disclose: $AG (\neg \text{disclose_PHI})$

R-Access: $AF (\text{EHR})$

R-Logout: $AG (\text{EHR} \rightarrow AF \neg \text{logged_in})$

R-Share: $AG (\text{disaster} \rightarrow EF \text{share_PHI})$

\mathcal{R} : {R-Disclose, ~~R-Access~~, ~~R-Logout~~, ~~R-Share~~}

\mathcal{A} : { $\neg \text{logged_in}$, POWER_FAILURE, ...}

\mathcal{M} : { $m(\text{true}, \{\text{consent}\}, \{\})$, ...}

A(PHY, HOS, consent, EHR)

P(PHY, HOS, true, share_PHI)

P(PHY, HOS, true, disclose_PHI)

Expansion pattern

\mathcal{R} : {R-Disclose, R-Access, ~~R-Logout~~, ~~R-Share~~}

\mathcal{A} : { $\neg \text{logged_in}$, POWER_FAILURE, ...}

\mathcal{M} : { $m(\text{true}, \{\text{consent}\}, \{\})$, ...}

* A(PHY, HOS, consent \vee logged_in, EHR)

P(PHY, HOS, true, share_PHI)

P(PHY, HOS, true, disclose_PHI)

Responsibility pattern

\mathcal{R} : {R-Disclose, R-Access, R-Logout, R-Share}

\mathcal{A} : { $\neg \text{logged_in}$, POWER_FAILURE, ...}

\mathcal{M} : { $m(\text{true}, \{\text{consent}\}, \{\})$, ...}

A(PHY, HOS, consent \vee logged_in, EHR)

C(PHY, HOS, EHR, $\neg \text{logged_in}$)

~~P(PHY, HOS, true, share_PHI)~~

P(PHY, HOS, true, disclose_PHI)

Accessibility pattern

\mathcal{R} : {R-Disclose, R-Access, R-Logout, ~~R-Share~~}

\mathcal{A} : { $\neg \text{logged_in}$, POWER_FAILURE, ...}

\mathcal{M} : { $m(\text{true}, \{\text{consent}\}, \{\})$, ...}

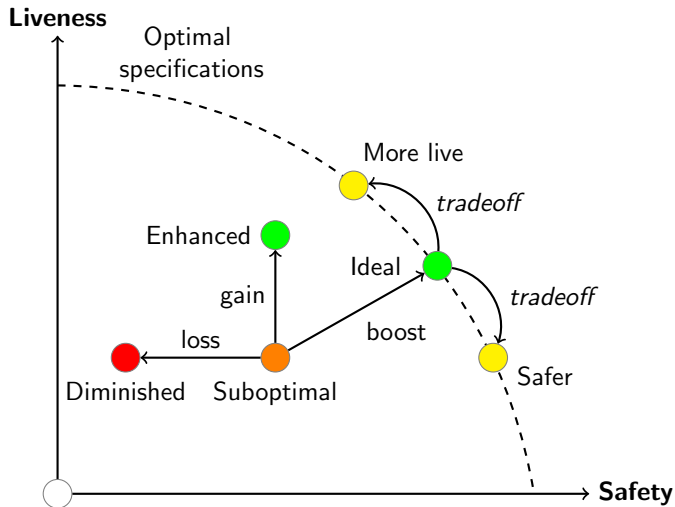
A(PHY, HOS, consent \vee logged_in, EHR)

+ C(PHY, HOS, EHR, $\neg \text{logged_in}$)

P(PHY, HOS, true, share_PHI)

P(PHY, HOS, true, disclose_PHI)

Tradeoffs



Comparing STS Specifications

- ▶ Experiments on surgical procedures using constraint logic programming

$$\text{Liveness score} = \frac{\text{supported procedures}}{\text{all procedures}}$$

$$\text{Safety score} = 1 - \frac{\text{procedures by outside physicians}}{\text{supported procedures}}$$

Mode of operation	Liveness score		Safety score	
	Suboptimal	Enhanced	Suboptimal	Enhanced
Regular practice	0.19	0.19	1.00	1.00
Medical emergency	0.10	0.73	1.00	0.14
Server failure	0.00	0.21	1.00	0.00

Representing Misuse Cases for Software Engineering

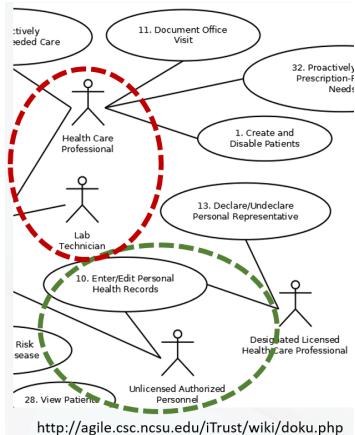
To help build secure sociotechnical systems

Current approaches provide

- ▶ Informal representations to visualize misuse cases
- ▶ Mechanisms needed to protect sensitive resources

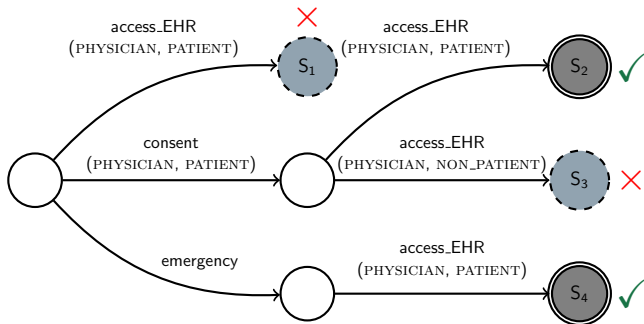
Current approaches cannot capture

- ▶ Social interactions among users
- ▶ Computational models for misuse
- ▶ Sufficiently expressive representations that support digital forensics



Identifying Misuse from Norm Enactments

- ▶ $P(\text{PHYSICIAN, HOSPITAL, } \neg\text{consent}(\text{PHYSICIAN, PATIENT}) \wedge \neg\text{emergency, access_EHR}(\text{PHYSICIAN, PATIENT}))$



Thanks!

- ▶ Department of Defense
- ▶ National Science Foundation
- ▶ Amit Chopra, Lancaster

<http://www.csc.ncsu.edu/faculty/mpsingh/>

