Open vs. Closed Systems for Accountability

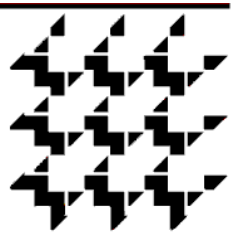
Rebecca Wright
Rutgers University
www.cs.rutgers.edu/~rebecca.wright

Joint work with Joan Feigenbaum (Yale) and Aaron D. Jaggard (US Naval Research Laboratory)

Symposium and Bootcamp on the Science of Security
April 2014

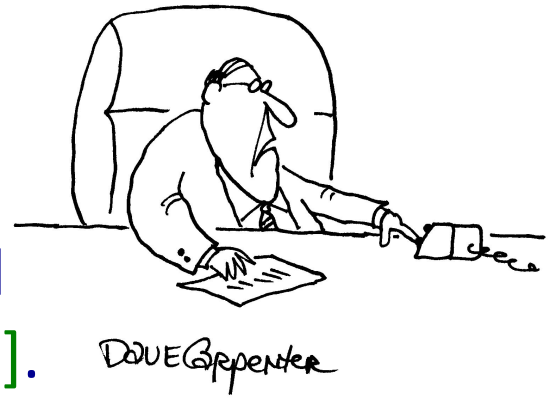
RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

DIMACS
Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center



Accountability

- Both in the real world and in Internet systems, people often express a desire for "accountability".
- Not completely clear what people mean, but often about ensuring consequences for people who break the rules.
- May or may not require identification and tracking of everyone at all times. (Without definitions, we can't tell!)
- We are exploring this as a useful paradigm shift from approaches based only on prevention [FJW11, FHJWW11].



" MISS WILCOX, SEND IN SOMEONE TO BLAME."

Need for Accountability

Weitzner et al., CACM 2008:

> This hide-it-or-lose-it perspective … on privacy, copyright, and surveillance is increasingly inadequate. … As an alternative, accountability must become a primary means through which society addresses appropriate use.

Lampson, CACM 2009:

> Misplaced emphasis on prevention ("security based on locks") rather than accountability ("security based on deterrence") has resulted in unusable security technology that people do not understand and often work around.

Examples of Scenarios in which Prevention is Inadequate

- Surveillance and Copyright
  - an agent might first need to break the policy in order to determine whether or not he can comply
- Emergencies ("break-glass" scenarios)
- Data exchange in (evolving!) online life
  - Search, e-commerce, and social networking
  - P2P photo sharing
  - Location-dependent services
- High-volume transactions
  - robots.txt
  - micropayments

Research Agenda

- Formalize accountability and related concepts
  - Clarify interrelated (and often conflated) notions
  - Provide framework for formal analysis
- Use these ideas to study accountability and identity requirements in systems
  - Tradeoffs and impossibility results
  - To what extent is identity required?

Our Earlier Formulation [FJW11]

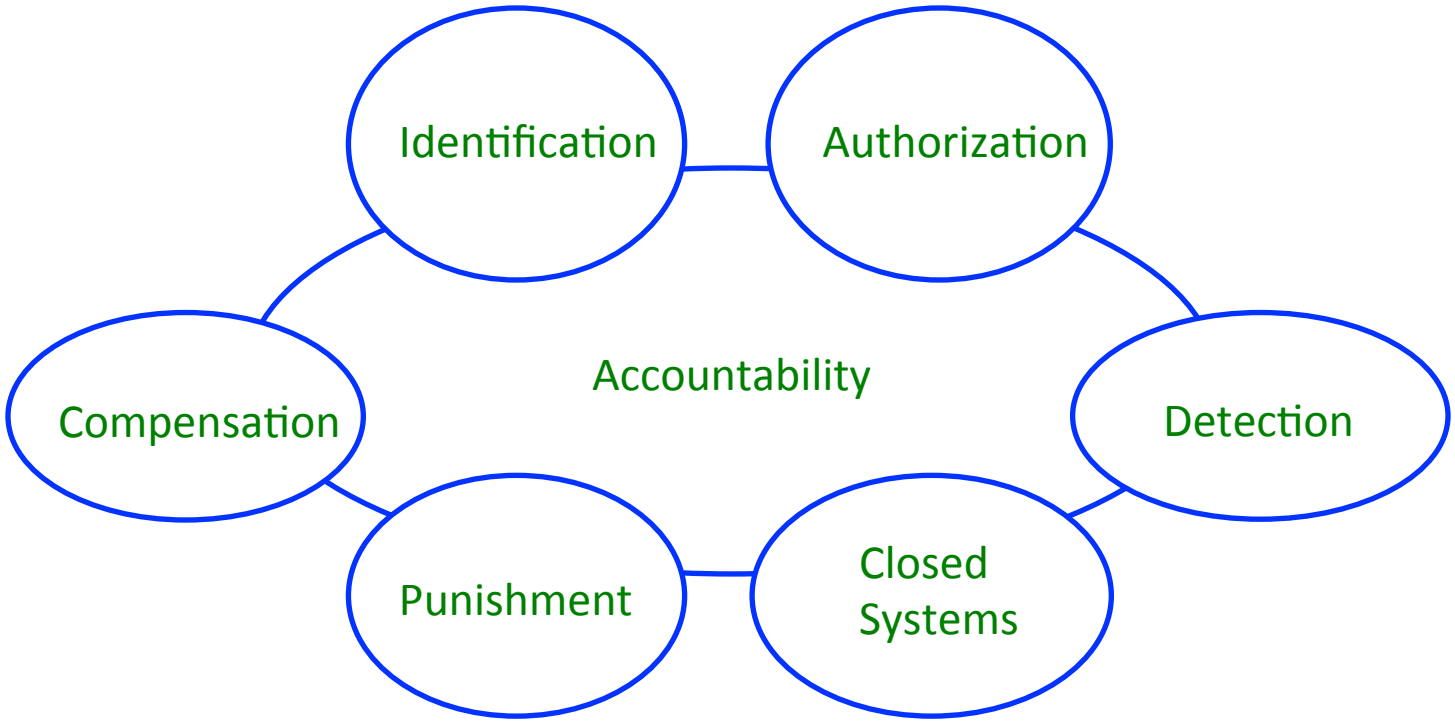
- **Working Definition**: An entity is accountable with respect to policy P if, whenever the entity violates P, then it could be punished (maybe probabilistically).
  - We separate accountability from identifiability.
  - Broadens Lampson's definition (to allow *automatic* punishment).

(Toy) Example: Car Dealership Lot

Policy: people shouldn't be able to drive cars off the lot without paying for them first.

- Mediated, identifiable accountability:
  - a customer can show ID and sign paperwork to drive the car around the lot. If she leaves in the car without payment, a judge can punish her based on the presented evidence.
- Prevention:
  - an electronic shut-off device stops cars from driving through the exit. Can only be disabled by the manager, who does this upon payment.
- Automatic, anonymous accountability:
  - an electronic explosive device blows up cars and their passengers if they drive through the exit. Can only be disabled by the manager, who does this upon payment.

Research Goal: Explicate Relationship Between Accountability and Related Properties

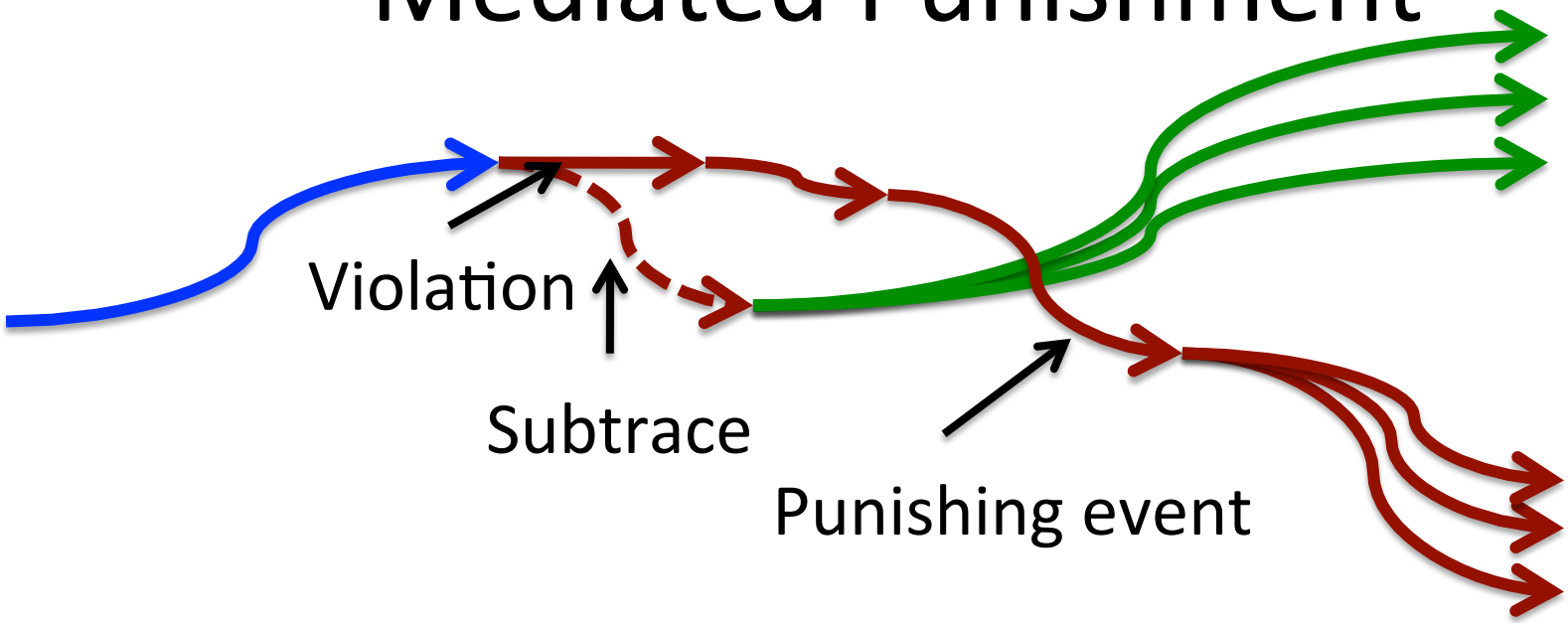


- Example research question: in open systems with mediated punishment, are anonymity and accountability compatible?

Formalizing This Approach

- Traces as finite sequences of events
  - Outcome: a trace that can't be extended
- Violation predicate:
  - Does this trace violate the policy in question?
- An event e is a violation at trace T if the violation predicate holds on Te but not on T.
- Assume each principal has a utility function defined on outcomes of the system.
  - Necessary to know when something is a punishment.
  - We can do this for either the expected utility or the most typical utility.

Mediated Punishment



- Punishing event must be caused by the fact of the violation
- Compare utility of outcomes after punishing event with utility of outcomes extending the subtrace

Open and Closed Systems

- Typical properties of "Open" systems:
  - users can come and go
  - users may be anonymous
  - may still be some requirements of participation (payment, proof of eligibility)
- Typical properties of "Closed" systems:
  - users are more tightly regulated as a condition of participation in the system
  - need to establish identity to join
  - identity may be revealed to other system participants
- Many systems are somewhere in between.

Example: State Fair

- Anyone can buy a ticket without showing identification.
- The fair needs to be able to know who has and hasn't paid to the extent that those who have not paid are not let in, but doesn't necessarily need to know identities beyond this.
- Might also issue wristbands or other tokens for those with additional privileges (e.g., has shown proof of age for alcohol consumption, or purchased the ability to skip lines).
- If someone violates fair rules, the fair authorities might attempt to identify him, or at least ask him to leave.

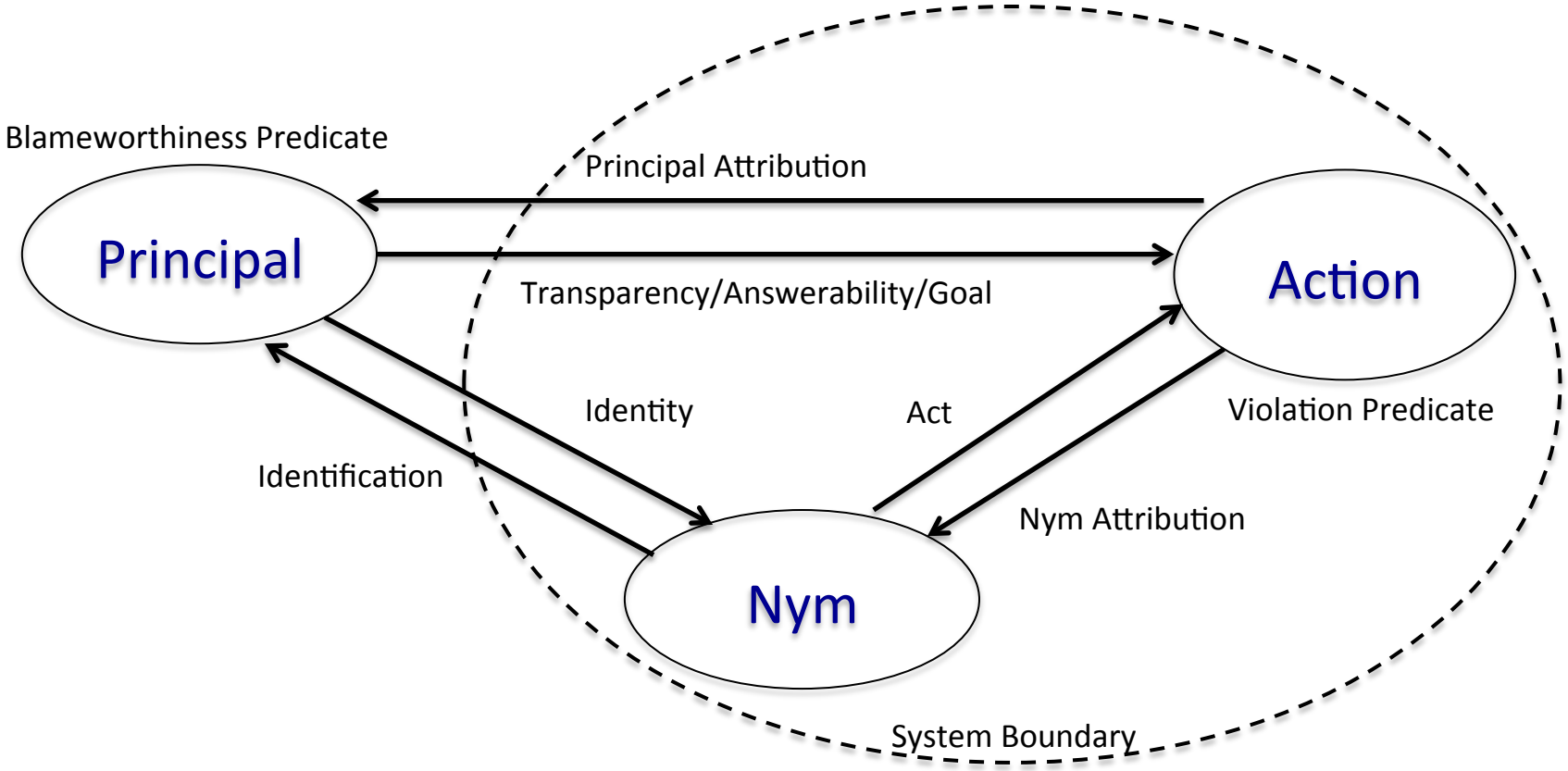
Example: Auction House

- Issues bidding paddles to bidders so that no two bidders have the same paddle number.
- Auctioneer and other bidders do not need to know the bidders' real identities.
- Auction house may require real identities, or sufficient cash deposit.

Principals and Nyms

- We assume a system S, a set P of principals, and a set N of nyms.
- Informally, nyms are the identities that principals use to interact with a system.
- Given a system S, principals P, and nyms N, a participation predicate for S is a predicate on P x N. We say p participates in S using n if P(p, n) holds.
- A violation predicate holds on actions, and a blameworthiness predicate on principals.

Concepts and Relationships



Revisiting the State Fair

- Anyone can buy a ticket without showing identification. Open system.
- The fair needs to be able to know who has and hasn't paid to the extent that those who have not paid are not let in, but doesn't necessarily need to know identities beyond this. Only one nym: "participant".
- Might also issue wristbands or other tokens for those with additional privileges (e.g., has shown proof of age for alcohol consumption, or purchased the ability to skip lines). Two nyms: "wristband" and "no wristband".
- If someone violates fair rules, the fair authorities might attempt to identify him, or at least ask him to leave. Possible identification, punishment in any case.

Working Definitions of Open and Closed Systems

- Closed System
  - For a principal to participate using nym n, S must have the ability to determine the set of principals using n in a "sufficiently reliable" way.
- Weakly Open System
  - For every p, there is some n such that p can participate in S using n and S is unable to reliably determine the set of principals that participated in S as n.
- Strongly Open System
  - For every n, S is unable to reliably determine the set of principals that participated in the system as n.

Utilities

- Punishment is defined in a utility-theoretic way. Goals for principals' utilities include:
  - Utility should depend on the trace.
  - Utility should depend on the connection between principals and nyms.
  - These two parts should be separable in order to facilitate study of the effects on the connection between principals and nyms.

Utilities with Linear Transfer

- Generalizing quasilinear utilities, we consider utilities with linear transfer:
  - $u_p(x_1, \ldots) = w_p(x_1) + \Sigma_y \alpha_p(y, \ldots)\, v(y, x_1)$

- An important special case is:
  - $u_p(T, f) = w_p(T) + \Sigma_n \alpha_p(n, f)\, v(n, T)$

  where T is a trace, f is the mapping between principles and nyms in T, and the sum is over all nyms n.

Example: Software Vulnerabilities

- Suppose Alice, acting as nym n, finds a software vulnerability.
- Consider trace T_P in which she patches it and T_E in which she exploits it.
- If Alice can obtain sufficient payment for exploiting the vulnerability, she may choose that. Her ability to do so without repercussion may depend on the extent to which she can be identified.
- As extremes, this difference is shown by the mappings f_{id} in which principals are mapped to distinct nyms and f_{anon} in which all principals are mapped to the same nym.
- If she can be identified, she may also care about an increased reputation for her action.

Toward Proving Theorems

Research question: In open systems with mediated punishment, are accountability and anonymity compatible?

Lemma: If a system without principal attribution is to be able to punish blameworthy participants in a mediated and targeted way, then for a nym n that may be used to carry out an unattributable action, the system must be able to decrease the value of v(n, T) while not decreasing the value of v(n', T) for n' ≠ n so that for each principal who acts as n, the decrease in $\alpha_p(n, f)$ v(n, T) strictly outweighs any incidental increase to P's utility arising from this punishing action.

Future Directions

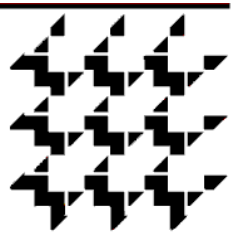
- Refining and applying the model.
- It may be necessary to further enrich utilities to capture factors (like reputation) that accrue directly to the principal rather than to the nym, or that obey nonlinear transfer.
- Continue investigating conceptual relationships among accountability, deterrence, identification, etc.

Open vs. Closed Systems for Accountability

Rebecca Wright
Rutgers University
www.cs.rutgers.edu/~rebecca.wright

Joint work with Joan Feigenbaum (Yale) and Aaron D. Jaggard (US Naval Research Laboratory)

Symposium and Bootcamp on the Science of Security
April 2014

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

DIMACS
Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center