Threat Models

Dimitris Mitropoulos
dimitro@di.uoa.gr

Security

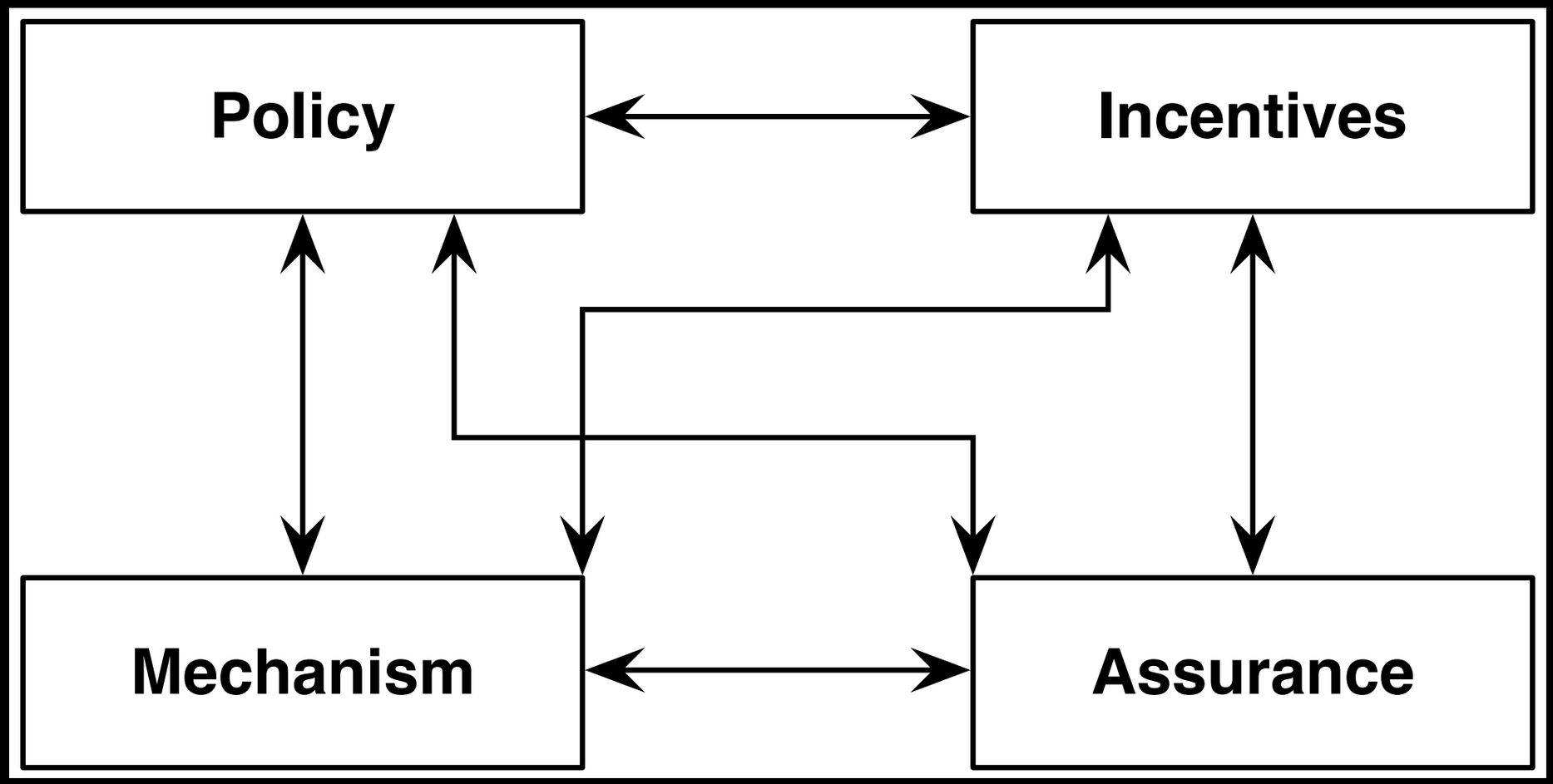
Goal VS Adversary: Θέλουμε να πετύχουμε ένα συγκεκριμένο στόχο όσο ένας αντίπαλος είναι παρών.

Threat Model

Ένα μοντέλο που περιγράφει / περιλαμβάνει όλες τις υποθέσεις που σχετίζονται με το τι μπορεί να κάνει ο αντίπαλος.

Θυμηθείτε

Analysis Framework



Παρατηρήσεις

- Σε ένα δεδομένο threat model, θέλουμε να εγγυηθούμε πως ένα policy δεν μπορεί να παραβιαστεί.
- Είναι όμως ιδιαίτερα δύσκολο να σκεφθούμε όλους τους τρόπους που μπορεί να χρησιμοποιήσει ο αντίπαλος για να παραβιάσει το policy.
- Ένα ρεαλιστικό threat model πρέπει να είναι “αρνητικό” (negative model). Είναι εύκολο να ελένξουμε εαν **όντως** η Alice έχει πρόσβαση σε ένα αρχείο (positive goal).

Πολιτική Ανάκτησης ενός Κωδικού Email

Πηγή εικόνας: https://en.wikipedia.org/wiki/Sarah_Palin_email_hack

Open-ended Threat Model

Προβλήματα στα **Threat Models**

- Δεν λαμβάνουμε υπόψη τον ανθρώπινο παράγοντα (π.χ. phishing, πόσο σύνθετο θα είναι το συνθηματικό που θα επιλέξει ένας χρήστης).
- Οι υποθέσεις που κάνουμε σε σχέση με τα εργαλεία που θα χρησιμοποιήσουμε μπορεί να επηρεάσουν την ασφάλεια του συστήματος στο μέλλον (χρήση παροχημένων συναρτήσεων κατακερματισμού - MD5).
- Ευπάθειες των συστημάτων (λ.χ. security bugs)

Threat Model

Ερωτήματα που Χρειάζονται Απάντηση

- Τι προστατεύουμε;
- Από ποιές επιθέσεις;
- Ποιούς εμπιστευόμαστε;

“I caught my cat running out of my office with my yubikey in his mouth--a threat model I hadn't considered.”

M. Burnet, Twitter:
https://twitter.com/m8urnett/status/964002875994128384

Προβλήματα στους **Μηχανισμούς**

https://github.com/hackappcom/ibrute

Βιβλιογραφία

R. J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. *John Wiley & Sons, Inc.*, New York, NY, USA, 2001. ISBN 0471389226.

Palin E-Mail Hacker Says It Was Easy. Kim Zetter. *Wired*, 18/09/2008, Available. Online: https://www.wired.com/2008/09/palin-e-mail-ha/

How Apple and Amazon Security Flaws Led to My Epic Hacking. Mat Honan. *Wired*, 08/06/2012, Available. Online: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/