A Typing System for Privacy

Dimitrios Kouzapas* and Anna Philippou*

*Department of Computing, Imperial College London

**Department of Computer Science, University of Cyprus

Τι είναι ιδιωτικότητα;

- Δεν υπάρχει κάποιος γενικός ορισμός:
  - Ορίζεται διαφορετικά σε διαφορετικές επιστήμες (φιλοσοφία, νομική, κοινωνικές επιστήμες)
  - Ορίζεται διαφορετικά σε διαφορετικές χώρες
  - Από διαφορετικούς ανθρώπους

- Νομοθεσία:
  - Ιδιωτικότητα = ένα σύνολο από δικαιώματα του ατόμου

Ιδιωτικότητα και Τεχνολογία

- Νέες τεχνολογίες εγείρουν καινούριες προσκλήσεις σε θέματα ιδιωτικότητας
  - Φωτογραφία, τηλεφωνία, κάμερες
- Το ίδιο ισχύει για εξελίξεις στην Επιστήμη της Πληροφορικής:
  - Συλλογή πληροφοριών σε βάσεις δεδομένων
  - Δίκτυα και εφαρμογές σε αυτά:
    - Ηλεκτρονικό Εμπόριο
    - Υπολογιστικό Νέφος
    - Κοινωνικά Δίκτυα
- Ταυτόχρονα, η Επιστήμη της Πληροφορικής
  - μπορεί να προσφέρει λύσεις για διασφάλιση δικαιωμάτων που σχετίζονται με την ιδιωτικότητα

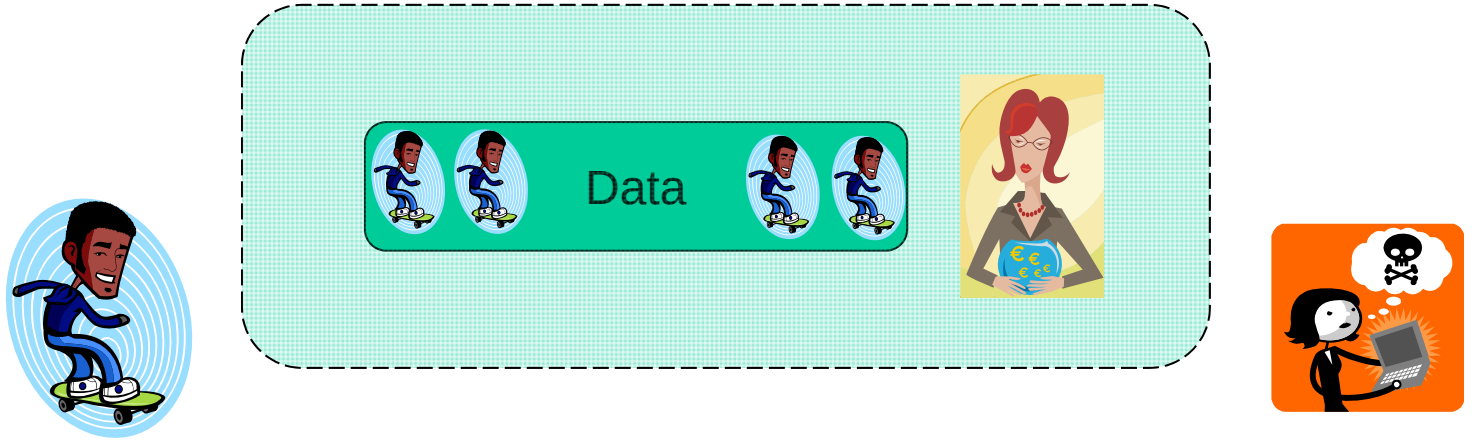
Η σημερινή παρουσίαση

- M. C. Tschantz and J. M. Wing. *Formal methods for privacy*. In Proceedings of FM'09, LNCS 5850, pages 115. Springer, 2009.
  - Ανάγκη μελέτης θεμελιώσεων της ιδιωτικότητας
  - Προτρέπει τη δημιουργία προτύπων και εργαλείων για καλύτερη κατανόηση της έννοιας της ιδιωτικότητας, την ανάλυσή της και των εγγενών δυνατοτήτων/περιορισμών που τη συνοδεύουν
  - Βασίζεται στην ταξινόμηση του νομικού D. Solove

- D. Kouzapas and A. Philippou. *A Typing System for Privacy*. In Proceedings of BEAT'13. LNCS 8368, pages 56-68. Springer 2013.
  - Διατύπωση ενός τυπικού πλαισίου στο οποίο είναι δυνατόν να εγγυηθούμε απαιτήσεις ιδιωτικότητας μέσω στατικής ανάλυσης ενός συστήματος όπου η ανάλυση αυτή διεκπεραιώνεται με επαλήθευση τύπων.

Η Ταξινόμηση του Solove

- Μοντέλο: 3 συνιστώσες
  - Άτομο με το οποίο σχετίζεται η πληροφορία (data subject)
  - Χειριστής Πληροφορίας (date holder)
  - Αντίπαλος (adversary)



- Ο Χειριστής της Πληροφορίας πρέπει να διασφαλίσει την ιδιωτικότητα των δεδομένων του Ατόμου με το οποίο σχετίζεται η πληροφορία έναντι οποιουδήποτε ανεξουσιοδότητου Αντιπάλου.

Η Ταξινόμηση του Solove (1)

- Δυνατές Παραβιάσεις
  - Εισβολή
    - Εισχώρηση στον προσωπικό χώρο ή παρέμβαση σε προσωπικές αποφάσεις
  - Συλλογή Δεδομένων
    - Μέθοδος συλλογής: Παρακολούθηση, Ανάκριση
  - Επεξεργασία Δεδομένων
    - Συσσωμάτωση (aggregation)
    - Συνταύτιση (identification)
    - Παραβίαση ασφάλειας
    - Δευτερεύουσα χρήση (secondary use)
    - Αποκλεισμός (exclusion)

Η Ταξινόμηση του Solove (2)

- Δυνατές Παραβιάσεις (συν.)
  - Διάδοση Δεδομένων
    - Παραβίαση εμπιστευτικότητας
    - Αποκάλυψη
    - Έκθεση (exposure)
    - Παραποίηση (distortion)
    - Οικειοποίηση (appropriation)
    - Αυξημένη προσβασιμότητα

Στόχος Εργασίας

- Διατύπωση τυπικού μοντέλου για μελέτη της ιδιωτικότητας
  - Μελέτη θεμελιωδών αρχών που τη διέπουν
  - Αυστηρή μοντελοποίηση και ανάλυση συστημάτων που συνοδεύονται από απαιτήσεις ιδιωτικότητας
- Επικέντρωση στις διαδικασίες
  - συλλογής, επεξεργασίας και διάδοσης δεδομένων και στη διατύπωση μεθόδων για διασφάλιση ιδιοτήτων ιδιωτικότητας
- Μεθοδολογία
  - Τυπικό μοντέλο βασισμένο σε άλγεβρες διεργασιών για μοντελοποίηση συστημάτων
  - Χρήση συστήματος τύπων για ανάλυση απαιτήσεων ιδιωτικότητας

Τυπικό πρότυπο

- π-calculus: τυπικό πρότυπο μοντελοποίησης και ανάλυσης παράλληλων και κινητών συστημάτων
  - R. Milner, J. Parrow, and D. Walker. *A calculus of mobile processes, parts I and II*. Information and Computation,100(1):1–77, 1992.

- π-calculus with groups: επέκταση του π-calculus με την έννοια της ομάδας (group)
  - L. Cardelli, G. Ghelli, and A. D. Gordon. Secrecy and group creation. Information and Computation, 196(2):127–155, 2005.

π-calculus with groups

- Χαρακτηριστικά
  - Βασικά δομικά στοιχεία: κανάλια, ομάδες (groups), διεργασίες
  - Επιτρεπτές δραστηριότητες: επικοινωνία με κανάλια
  - Μικρός αριθμός τελεστών για δημιουργία συστημάτων
- Σύνταξη

$P ::= x(y).P$	Είσοδος στο κανάλι x
$\mid \bar{x}(y).P$	Έξοδος στο κανάλι x
$\mid P_1 \mid P_2$	Παράλληλη σύνθεση
$\mid !\,\mathrm{P}$	Επανάληψη/Αναδρομή
$\mid 0$	Τερματισμός
$\mid (\nu\ \mathrm{G})P$	Δήλωση συμμετοχής σε ομάδα

- Σημασιολογία: Κανόνες οι οποίοι επεξηγούν τη λειτουργία οποιασδήποτε διεργασίας

Σύστημα Τύπων – Βασική Ιδέα (1)

- Κάθε κανάλι συσχετίζεται με κάποιο τύπο, ο οποίος περιορίζει την επιτρεπτή χρήση του καναλιού, ως προς:
  - Το πεδίο στο οποίο μπορεί να κινηθεί το κανάλι
  - Κατά πόσο μπορεί να χρησιμοποιηθεί για ανάγνωση ή εγγραφή
  - Κατά πόσο μπορεί να διαδοθεί σε τρίτα άτομα

Σημείωση: Κανάλι = Πληροφορία!

- Έστω
  - Γ ένας συσχετισμός καναλιών με τύπους και
  - Sys ένα σύστημα διατυπωμένο στο π-calculus.

  Γράφουμε $\Gamma \vdash Sys$ για να δηλώσουμε ότι το σύστημα Sys χρησιμοποιεί τα κανάλια του σύμφωνα με τις δηλώσεις του Γ.

Σύστημα Τύπων – Βασική Ιδέα (2)

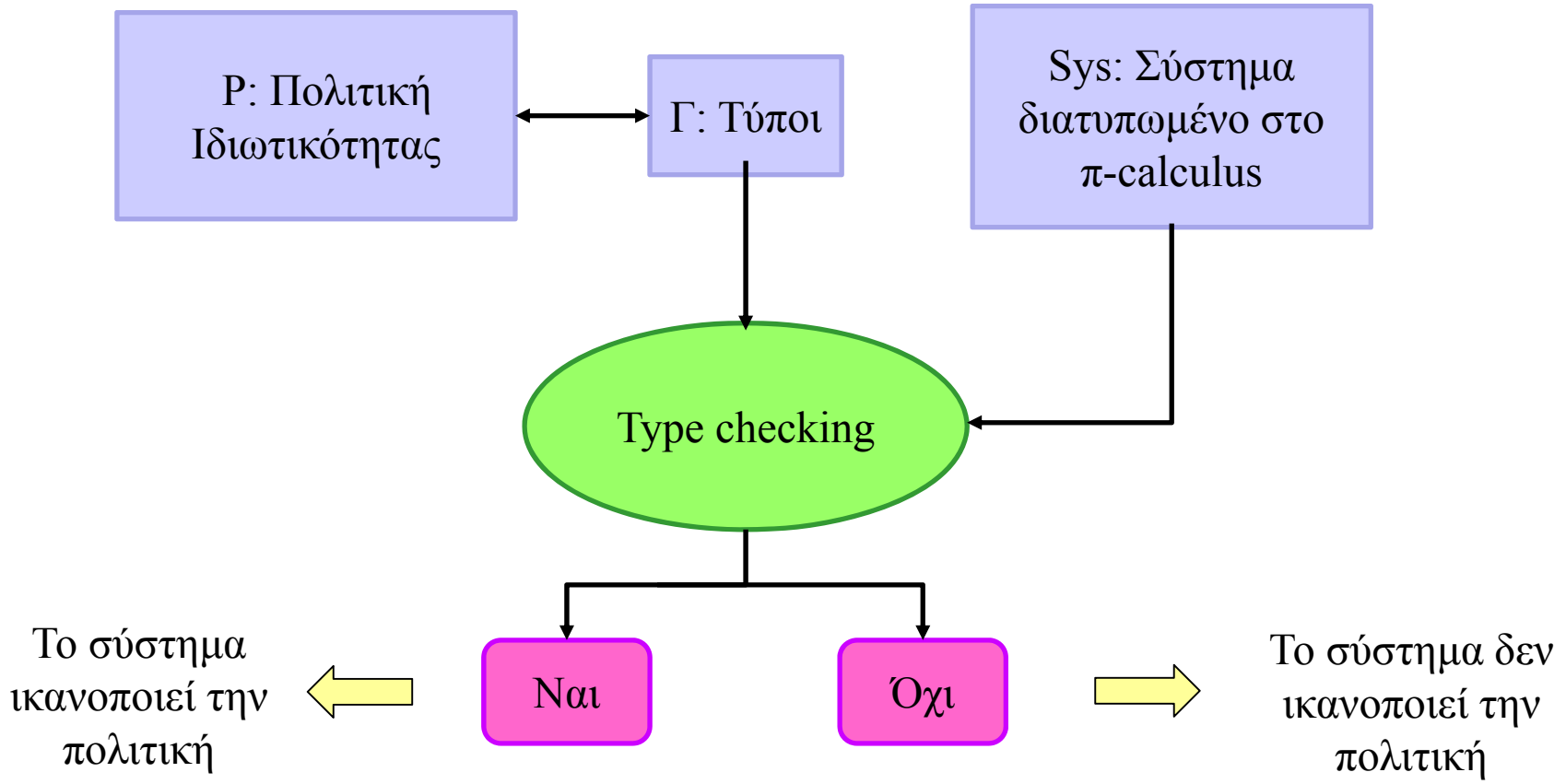
- Έστω
  - Π μια πολιτική ιδιωτικότητας και
  - Γ ένας συσχετισμός καναλιών με τύπους

  Γράφουμε $\Pi \asymp \Gamma$ αν οι περιορισμοί που επιβάλλουν οι τύποι του Γ είναι συμβατοί με την πολιτική Π.

- Κύριο Αποτέλεσμα

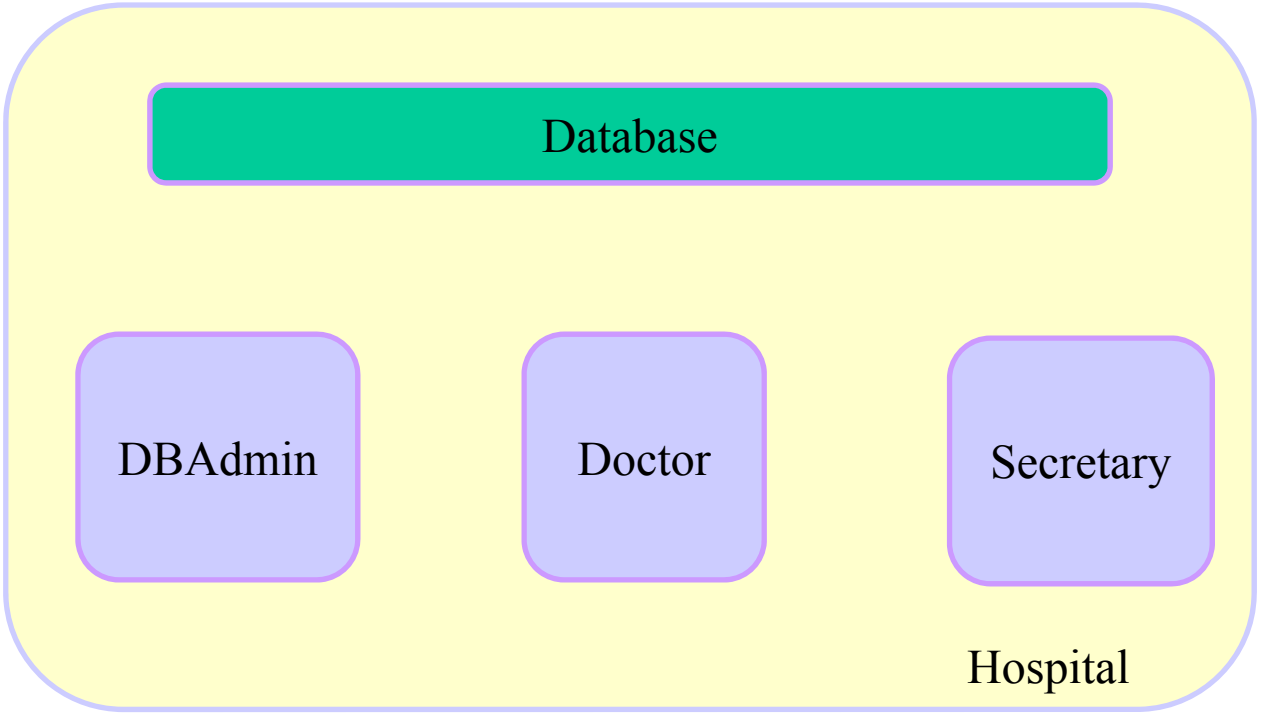
  Αν $\Gamma \vdash \mathrm{Sys}$ και $\Pi \asymp \Gamma$ τότε το σύστημα Sys ικανοποιεί την πολιτική ιδιωτικότητας Π.

Type checking



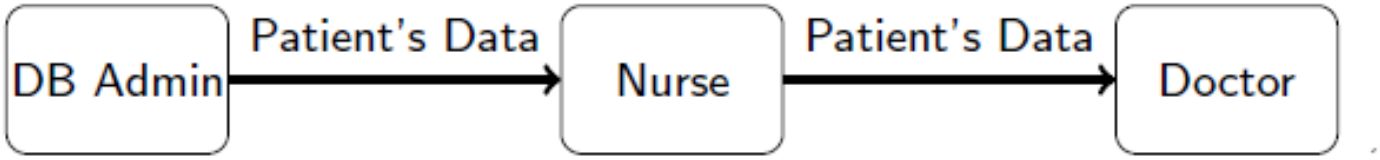
Παρουσίαση μέσω παραδείγματος

- Νοσοκομείο
  - Ο Διαχειριστής Δεδομένων πρέπει να διασφαλίσει ότι τα δεδομένα των ασθενών θα τύχουν ορθού χειρισμού ικανοποιώντας απαιτήσεις ιδιωτικότητας.



Παράδειγμα: Το σύστημα

- Ο διαχειριστής της βάσης δεδομένων (data holder) στέλνει τα στοιχεία ενός ασθενή (data subject) στον γιατρό (authorised adversary) μέσω της γραμματέας (unauthorized adversary).



Παράδειγμα: Η Πολιτική

- Μια πολιτική συλλαμβάνει
  1. Την ιεραρχία ανάμεσα στις διάφορες ομάδες/groups
  2. Αντιστοίχηση ενός συνόλου δικαιωμάτων σε κάθε ομάδα

- Παράδειγμα:

Patient Data {

Hospital: non-extrusion

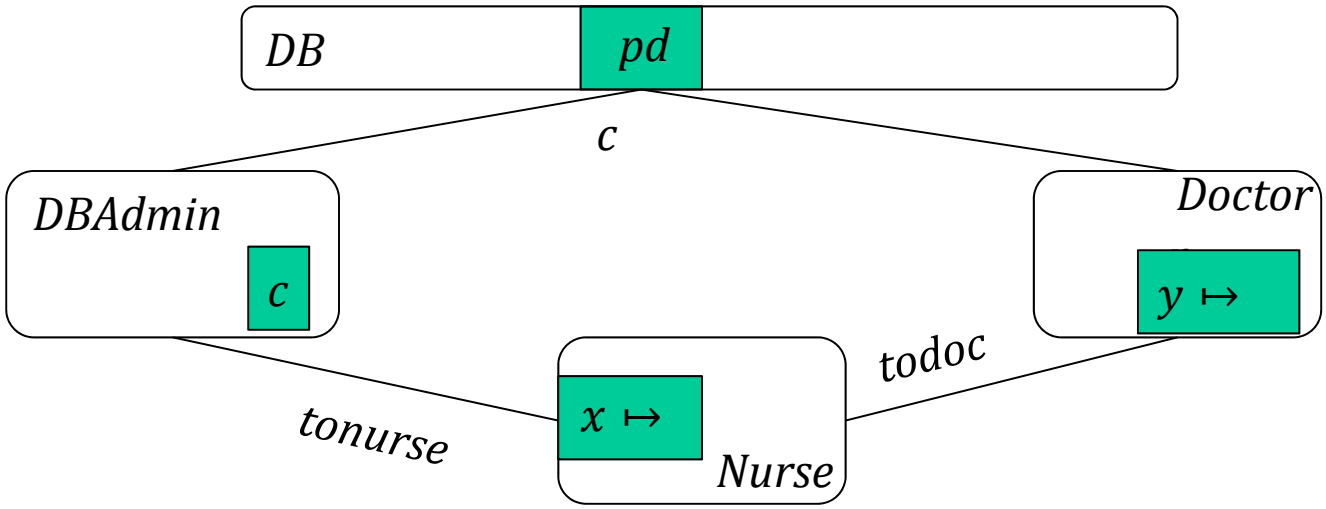
Secretary: forward

Doctor: read, write

Janitor: exclude

}

Μοντελοποίηση στο π-calculus (1)



$$System = DBAdmin \mid Nurse \mid Doctor$$

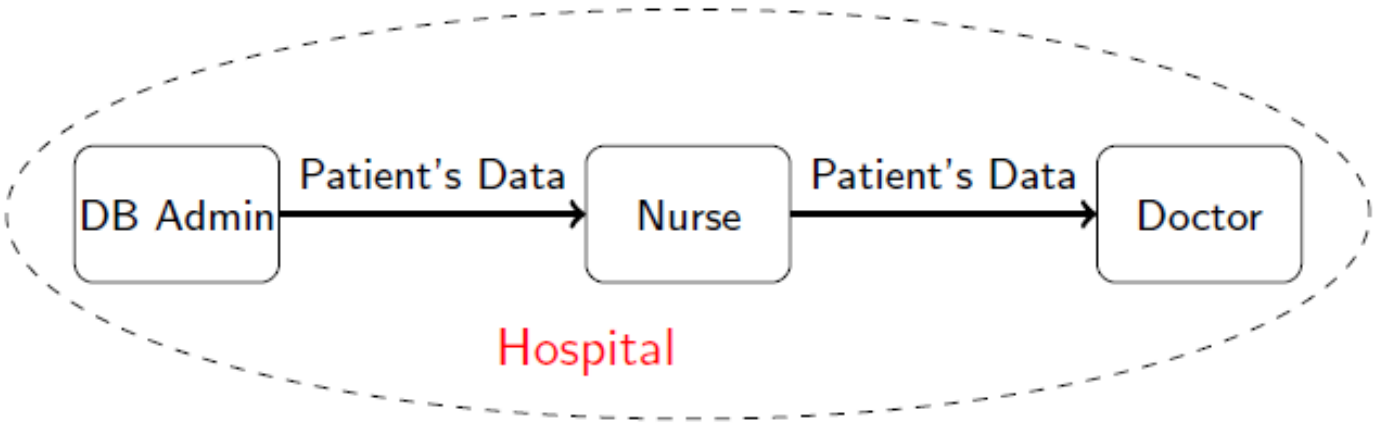
$$DBAdmin = \overline{tonurse}(c).0$$

$$Nurse = tonurse(x).\overline{todoc}(x).0$$

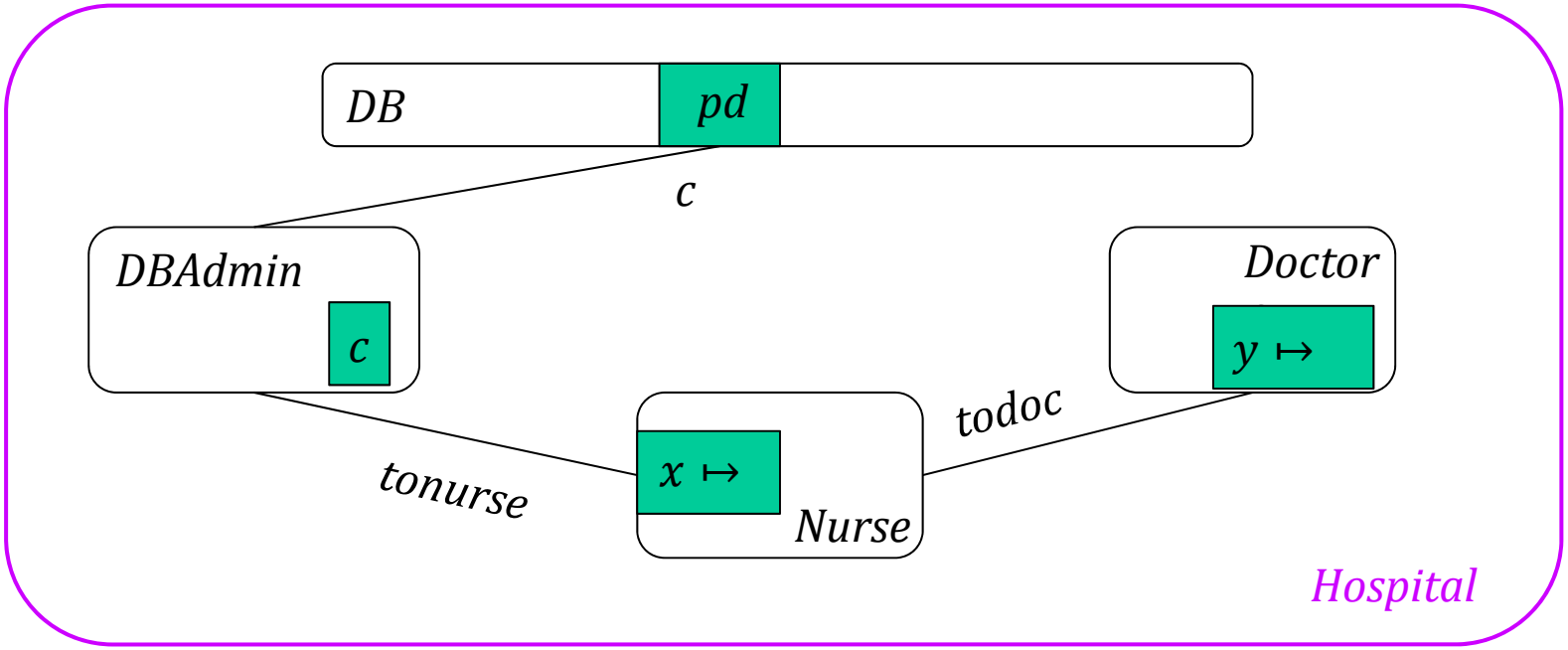
$$Doctor = todoc(y).y(z).\bar{y}(data).0$$

Συλλογή Πληροφοριών

- Χρήση των ομάδων του π-calculus with groups: αποτρέπει τη διαρροή πληροφοριών έξω από την ομάδα



Μοντελοποίηση στο π-calculus (2)



$$System = (\nu\ Hospital)(DBAdmin \mid Nurse \mid Doctor)$$

$$DBAdmin = \overline{tonurse}(c).0$$

$$Nurse = tonurse(x).\overline{todoc}(x).0$$

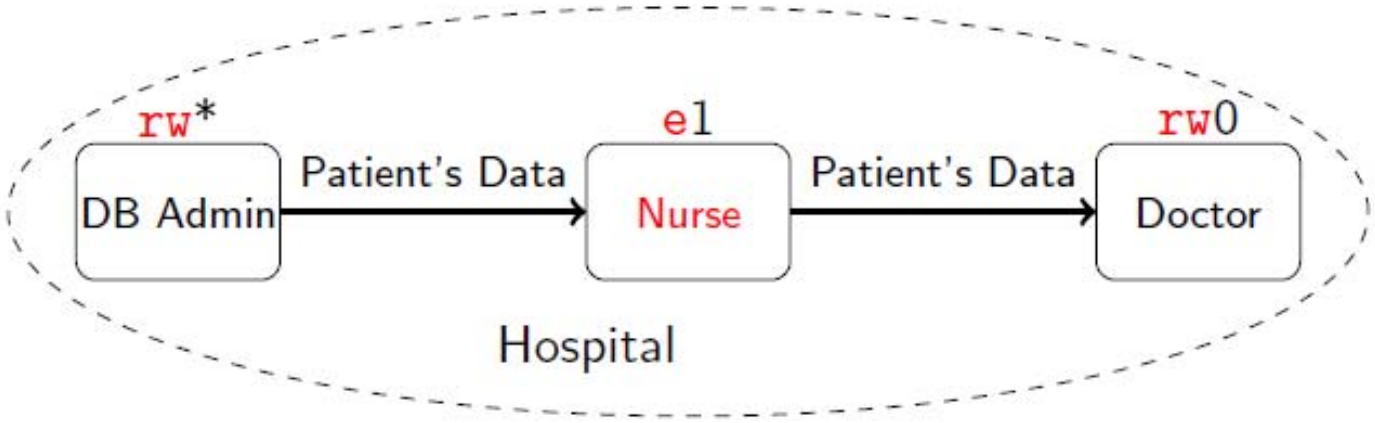
$$Doctor = todoc(y).y(z).\bar{y}(data).0$$

Επεξεργασία Πληροφοριών

- Χρήση τύπων i/o (input/output). Γράφουμε
  - r για να δείξουμε ότι ένα κανάλι μπορεί να χρησιμοποιηθεί για είσοδο/ανάγνωση
  - w για να δείξουμε ότι ένα κανάλι μπορεί να χρησιμοποιηθεί για έξοδο/εγγραφή
  - e: κενή άδεια
- Χρήση πολλαπλότητας
  - int, *: επιτρεπτός αριθμός προώθησης δεδομένων
- Παραδείγματα
  - r*: δικαίωμα ανάγνωσης και προώθησης για απεριόριστο αριθμό φορών
  - rw2: δικαίωμα ανάγνωσης, εγγραφής και προώθησης μέχρι δύο φορές
  - e1: δικαίωμα για μία προώθηση

Επεξεργασία Πληροφοριών

- Χρήση i/o τύπων και πολλαπλότητας για περιορισμό της επεξεργασίας δεδομένων.



Τύποι

- Αυστηρά:

$$T \ ::= \ G[T]^{p\lambda}$$

$$p \ ::= \ \text{e} \mid \text{r} \mid \text{w} \mid \text{rw}$$

$$\lambda \ ::= \ * \mid i$$

- Γράφουμε
  - x : $G[T]^{p\lambda}$ για να δηλώσουμε ότι το κανάλι x μπορεί να χρησιμοποιηθεί εντός της ομάδας G για ανάγνωση/εγγραφή αντικειμένων τύπου T σύμφωνα με τα δικαιώματα p και να προωθηθεί μέχρι λ φορές.

Έλεγχος Τύπων (1)

- $System = (\nu\ Hospital)(DBAdmin \mid Nurse \mid Doctor)$
- $DBAdmin = \overline{tonurse}(c).0$
  - $c: Hospital[PData]$
  - $tonurse: Hospital[Hospital[PData]]^w$

  $\Rightarrow$ Ο διαχειριστής μπορεί να στείλει μέσω του καναλιού *tonurse* τη διεύθυνση του αρχείου με τα δεδομένα του ασθενή
- Πολιτική: $PData\{$

  $DBAdmin: rw\ *,$

  $\ldots\}$
- Συμπέρασμα: Ο κώδικας του διαχειριστή είναι συμβατός προς την πολιτική.

Έλεγχος Τύπων (2)

- $Nurse = tonurse(x).\ \overline{todoc}(x).\ 0$
  - $tonurse: Hospital[Hospital[PData]]^r$
  - $x: Hospital[PData]$
  - $todoc: Hospital[Hospital[PData]]^w$

  $\Rightarrow$ η νοσοκόμα μπορεί να προωθήσει τη διεύθυνση του αρχείου με τα δεδομένα του ασθενή μία φορά στο κανάλι *todoc*

- Πολιτική:$PData\{$ ...

  $Nurse: e1,$

  $\ldots\}$

- Συμπέρασμα: Ο κώδικας της νοσοκόμας είναι συμβατός προς την πολιτική.

Έλεγχος Τύπων (3)

- $Doctor = todoc(y).\, y(z).\, \bar{y}(data).\, 0$
  - $todoc: Hospital[Hospital[PData]]^{r}$
  - $y: Hospital[PData]^{rw}$

  $\Rightarrow$ ο γιατρός μπορεί να χρησιμοποιήσει τη διεύθυνση του αρχείου με τα δεδομένα του ασθενή για εγγραφή και ανάγνωση

- Πολιτική: $PData\{$ ...
  Doctor: $rw0$,
  … }

- Συμπέρασμα: Ο κώδικας του γιατρού είναι συμβατός προς την πολιτική.

Αντιπαράδειγμα

- Έστω

$$Nurse = tonurse(x).\,\bar{x}(data).\,\overline{todoc}(x).\,0$$

$$Doctor = todoc(y).\,y(z).\,\bar{y}(data).\,\overline{todoc}(y).\,0$$

- Τύποι νοσοκόμας
  - $tonurse: Hospital[Hospital[PData]]^{r}$
  - $todoc: Hospital[Hospital[PData]]^{w}$
  - $x: Hospital[PData]^{w1}$
- Τύποι γιατρού
  - $todoc: Hospital[Hospital[PData]]^{r}$
  - $y: Hospital[PData]^{rw1}$

Type Error!

Τεχνικά σημεία από το άρθρο

- Ορισμός της σχέσης $\Gamma \vdash Sys$
  - Σύνολο από κανόνες, π.χ.

$$(\mathsf{In}) \qquad \frac{\Pi, \Gamma \cdot y : T \vdash P \triangleright \Gamma' \quad \Pi, \Gamma \vdash x \triangleright G[T]^{\mathrm{r0}}}{\Pi, \Gamma \cdot y : T \vdash x(y : T).P \triangleright (\Gamma' \uplus \{x : G[T]^{\mathrm{r0}}\})}$$

- Ορισμός της σχέσης $\Pi \asymp \Gamma$

- Θεώρημα 1 (Type Soundness): Αν $\Gamma \vdash Sys$ και Sys → Sys' τότε $\Gamma \vdash Sys'$.

  Γράφουμε: Sys → Sys' αν το Sys μπορεί να εξελιχθεί σε Sys'.

- Θεώρημα 2 (Type Safety): Αν $\Gamma \vdash Sys$ και $\Pi \asymp \Gamma$ τότε το σύστημα Sys ικανοποιεί την πολιτική ιδιωτικότητας Π.

Συμπεράσματα

- Τύποι συμπεριφοράς (behavioral types) μπορούν να αξιοποιηθούν για ανάλυση ιδιοτήτων ιδιωτικότητας.
  - Αποφυγή συλλογής δεδομένων μέσω παρακολούθησης (groups)
  - Αποφυγή παραβίασης εμπιστευτικότητας, αποκάλυψης, αυξημένης προσβασιμότητας (i/o και πολλαπλότητα)

- Στατική μέθοδος
  - Εκτελείται μια φορά. Αν το σύστημα περάσει τον έλεγχο τύπων γνωρίζουμε με βεβαιότητα ότι η πολιτική ιδιωτικότητας δεν πρόκειται να τύχει παραβίασης από το σύστημα

Μελλοντικές Εργασίες

- Δυναμική αλλαγή του συνόλου ομάδων στα οποία ανήκει ένας συμμετέχοντας
- Επέκταση του μοντέλου (τύποι και γλώσσες πολιτικές) για αποτροπή άλλων κατηγοριών παραβιάσεων:
  - Identification
  - Aggregation
  - Appropriation
  - Insecurity
- Ενσωμάτωση θεωρίας σε γλώσσα προγραμματισμού.