From Enabling to Enforcing Privacy

Naipeng Dong, **Hugo Jonker**, Jun Pang

Why privacy for eHealth?

- Healthcare data: inherently private.
- Subversion of data processing: dangerous!

Current approaches to privacy in eHealth

patient privacy (1/3): access control

- Anderson [And98]: restrict #users that access a record, restrict #records accessed by a user.
- Louwerse [Lou98]: consent-based access control necessary to implement “need-to-know”.
- Evered et al. [EB04]: minimal disclosure rules: use middle layer.
- Reid et al. [RCHS03]: RBAC + explicit consent + explicit denial for privacy.
- Kalam et al. [KBM$^+$03]: RBAC, TBAC insufficient for context-aware policies. Organisational BAC (OrBAC).
- Cuppens et al. [CCG07]: inconsistent access rules: rule prioritisation.

patient privacy (2/3): architectural design

- Ko et al. [KLS+10]: privacy issues in wireless sensor networks for eHealth.
- Maglogiannis et al. [MKD09]: patient location privacy via proxies.
- Chiu et al. [CHCK07]: privacy-aware cross-institution image sharing: RBAC and watermarks.

patient privacy (3/3): cryptographic approaches

- vd Haak et al. [HWB+03]: digital signatures, PK authentication.
- Ateniese et al. [ACM+03]: patient pseudonyms, method to transform statements on pseudonym a to pseudonym b.
- Layouni et al. [LVS+09]: wallet-based credentials for patient control of sensor info.
- De Decker et al. [DLV08]: Belgian healthcare system compliant system using ZKP, signed proofs of knowledge, bit-commitments.

Doctor privacy

- Matyáš [Mat98]: prescription analysis while preserving doctor privacy.
- Ateniese et al. [ACM+03]: doctor privacy to protect against administrative meddling.
- De Decker et al. [DLV08]: doctor privacy to prevent bribery.

Survey summary

- Access control to ensure patient privacy:
  [And98, Lou98, RCHS03, KBM+03, EB04, CCG07].
- Architectural design for patient privacy:
  [CHCK07, MKD09, KLS+10].
- Using crypto for patient privacy:
  [HWB+03, ACM+03, LVS+09, DLV08]

Survey summary

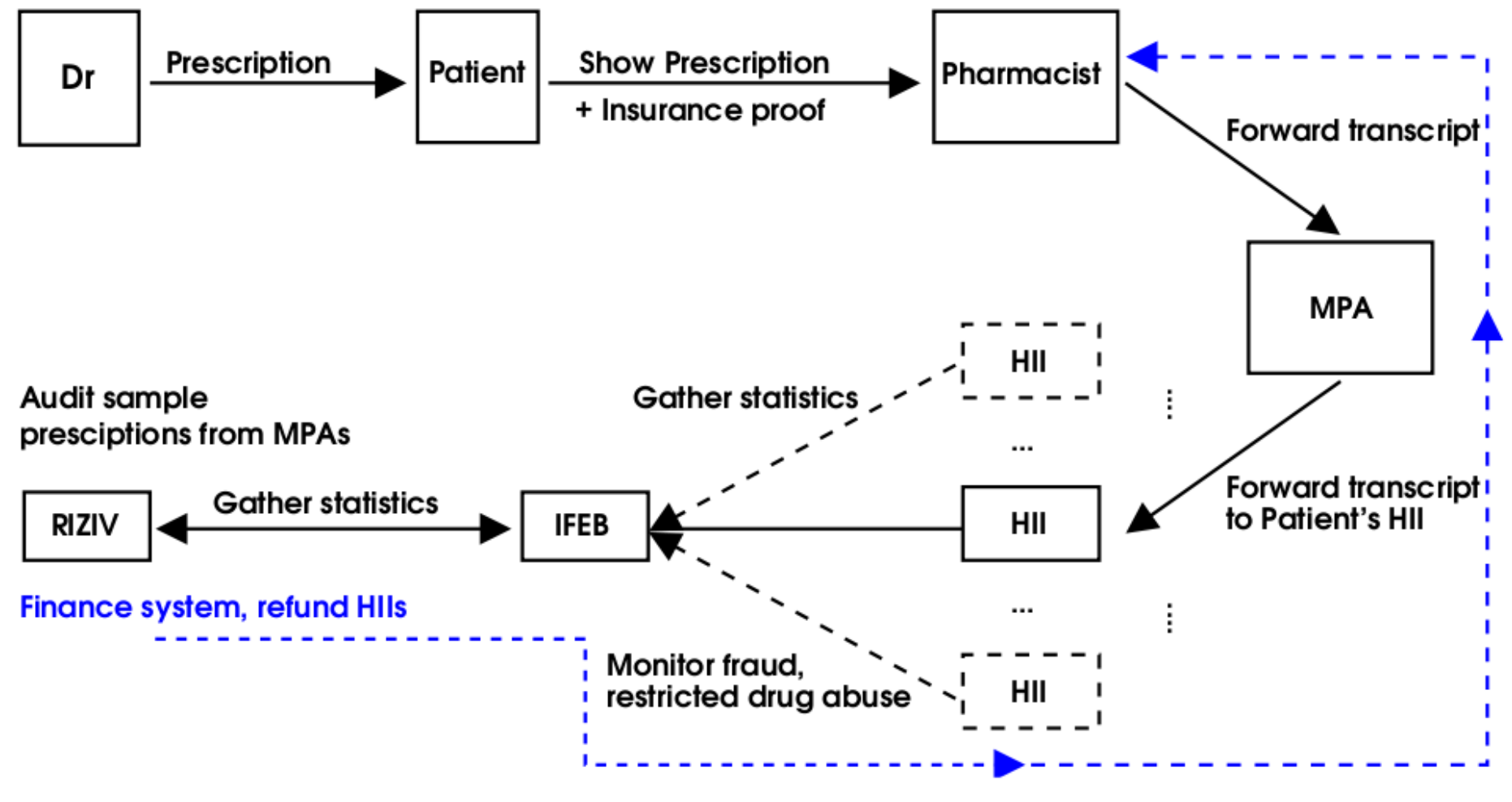
- Access control to ensure patient privacy:
  [And98, Lou98, RCHS03, KBM+03, EB04, CCG07].
- Architectural design for patient privacy:
  [CHCK07, MKD09, KLS+10].
- Using crypto for patient privacy:
  [HWB+03, ACM+03, LVS+09, DLV08]
- Doctor privacy:
  [Mat98, ACM+03, DLV08]

Survey summary

- Access control to ensure patient privacy:
  [And98, Lou98, RCHS03, KBM+03, EB04, CCG07].
- Architectural design for patient privacy:
  [CHCK07, MKD09, KLS+10].
- Using crypto for patient privacy:
  [HWB+03, ACM+03, LVS+09, DLV08]
- Doctor privacy:
  [Mat98, ACM+03, DLV08]
- Much focus on patient privacy, not on doctor privacy.

Sufficient concern for privacy?

- roles:



- enforced privacy

Motivation for doctor privacy

- [ACM+03]: safeguard against administrative meddling.
- [DLV08]: prevent bribery by pharmaceutical industry.

Motivation for doctor privacy

- [ACM+03]: safeguard against administrative meddling.
- [DLV08]: prevent bribery by pharmaceutical industry.

[Jonker, FHIES'11]: Privacy protection needs no motivation. Privacy **invasion** needs motivation.

Motivation for doctor privacy

- [ACM+03]: safeguard against administrative meddling.
- [DLV08]: prevent bribery by pharmaceutical industry.

[Jonker, FHIES'11]: Privacy protection needs no motivation.
Privacy **invasion** needs motivation.

Neither relation with doctors is on equal footing.

Enforced privacy

- Emerged in voting: vote buying (receipt-freeness) [BT94].
  “A voter cannot prove how she voted.”

Enforced privacy

- Emerged in voting: vote buying (receipt-freeness) [BT94].
  "A voter cannot prove how she voted."

- Matured in voting: coercion-resistance [JCJ05].
  RF+resistance against:
  - Forced randomised voting.
  - Forced abstention.
  - Forced to give up voting credentials.

  $\Longrightarrow$ resistance against interactive intruder.
  $\Longrightarrow$ no transferable voter-secrets

Enforced privacy

- Emerged in voting: vote buying (receipt-freeness) [BT94].
  "A voter cannot prove how she voted."

- Matured in voting: coercion-resistance [JCJ05].
  RF+resistance against:
  - Forced randomised voting.
  - Forced abstention.
  - Forced to give up voting credentials.

  $\Longrightarrow$ resistance against interactive intruder.
  $\Longrightarrow$ no transferable voter-secrets

- Considered in online auctions: [AS02, CLK03].

What is enforced privacy?

Privacy

- what can the intruder find out?
- observer
- optional: enabling

Enforced privacy

- what can you prove?
- prover + verifier
- mandatory: enforcing

EPRIV project

"understanding and verifiying enforced privacy"

- application domain: voting, auctions, healthcare, anonymous routing, ...

- approach:
  1. domain-specific case study $\Longrightarrow$ domain-specific verification framework.
  2. specific frameworks $\Longrightarrow$ domain-independent verification framework.
  3. tool support.

Case study: DLV08

- formalise protocol in applied π.
- extract and formalise requirements upon the model.
- use ProVerif to prove[a] security.

DLV08 requirements:

- . . . , doctors cannot prove what they prescribed, . . .

[a] limited models where necessary

DLV08 protocols

- patient-doctor
- patient-pharmacist
- pharmacist-MPA
- MPA-HII
- IFEB-MPA

Doctor not often involved: easy to ensure prescription privacy?

DLV08 protocols

- patient-doctor
- patient-pharmacist
- pharmacist-MPA
- MPA-HII
- IFEB-MPA

Doctor not often involved: easy to ensure prescription privacy?

but a pharmacist also knows things about prescriptions!

Privacy challenges for eHealth

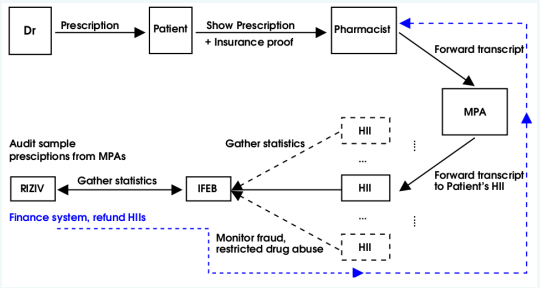
Challenge I: Enforced privacy.

- doctor privacy. . . who else?
- needs privacy-enforcing protocols and techniques.
- also needs independent verification framework.

Privacy challenges for eHealth

Challenge II:
Coalition-enforced privacy.

- one party may help another wrt unveiling privacy.



- helper can help either prover or verifier.

- helping verifier: threshold crypto.
  helping prover: ??.

Enforced privacy in DLV08

Notation:

- $P_{dr}(a, a)$: doctor prescribes a, claims to prescribe a.
- ${P_{dr}}'(a, b)$: doctor prescribes a, claims to prescribe b.

Privacy enforced iff:

$$P_{dr}(a, a)|P_{pt}|P_{ph}|P_{mpa}|P_{hii} \approx {P_{dr}}'(b, a)|P_{pt}|P_{ph}|P_{mpa}|P_{hii}$$

Possible directions

- privacy-strengthening coalitions
- game-theoretic approaches
- improving tool support

Conclusions

- 2 key privacy challenges:
  - Challenge I: enforced privacy
  - Challenge II: coalition-enforced privacy
- formal methods necessary for security
- initial steps made
- still some work left.

References

[And98] Anderson, R.: A security policy model for clinical information systems. In: Proc. 17th IEEE Symposium on Security and Privacy, IEEE CS (1996) 30–43

[Lou98] Louwerse, K.: The electronic patient record; the management of access – case study: Leiden University hospital. International Journal of Medical Informatics **49** (1998) 39–44

[EB04] Evered, M., Bögeholz, S.: A case study in access control requirements for a health information system. In: Proc. 2nd Australian Information Security Workshop. Volume 32 of Conferences in Research and Practice in Information Technology., Australian Computer Society (2004) 53–61

[RCHS03] Reid, J., Cheong, I., Henricksen, M., Smith, J.: A novel use of rBAC to protect privacy in distributed health care information systems. In: Proc. 8th Australian Conference on Information Security and Privacy. LNCS 2727, Springer (2003) 403–415

References (cont.)

[KBM+03] Kalam, A., Benferhat, S., Miège, A., Baida, R., Cuppens, F., Saurel, C., Balbiani, P., Deswarte, Y., Trouessin, G.: Organization based access control. In: Proc. 4th IEEE Workshop on Policies for Distributed Systems and Networks, IEEE CS (2003) 120–131

[CCG07] Cuppens, F., Cuppens-Boulahia, N., Ghorbel, M.B.: High level conflict management strategies in advanced access control models. Electronic Notes in Theoretical Computer Science **186** (2007) 3–26

[KLS+10] Ko, J., Lu, C., Srivastava, M.B., Stankovic, J.A., Terzis, A., Welsh, M.: Wireless sensor networks for healthcare. Proceedings of IEEE **98** (2010) 1947–1960

[MKD09] Maglogiannis, I., Kazatzopoulos, L., Delakouridis, C., Hadjiefthymiades, S.: Enabling location privacy and medical data encryption in patient telemonitoring systems. IEEE Transactions on Information Technology in Biomedicine **13** (2009) 946–954

Refs (cont.)

[CHCK07] Chiu, D.K.W., Hung, P.C.K., Cheng, V.S.Y., Kafeza, E.: Protecting the exchange of medical images in healthcare process integration with web services. In: Proc. 40th Hawaii Conference on Systems Science, IEEE CS (2007) 131–140

[HWB+03] van der Haak, M., Wolff, A.C., Brandner, R., Drings, P., Wannenmacher, M., Wetter, T.: Data security and protection in cross-institutional electronic patient records. International Journal of Medical Informatics **70** (2003) 117–130

[ACM+03] Ateniese, G., Curtmola, R., de Medeiros, B., Davis, D.: Medical information privacy assurance: Cryptographic and system aspects. In: Proc. 3rd Conference on Security in Communication Networks. LNCS 2576, Springer (2003) 199–218

Refs (cont.)

[LVS+09] Layouni, M., Verslype, K., Sandikkaya, M.T., De Decker, B., Vangheluwe, H.: Privacy-preserving telemonitoring for eHealth. In: Proc. 23rd Annual IFIP Working Conference on Data and Applications Security. LNCS 5645, Springer (2009) 95–110

[DLV08] De Decker, B., Layouni, M., Vangheluwe, H., Verslype, K.: A privacy-preserving eHealth protocol compliant with the Belgian healthcare system. In: Proc. 5th European Workshop on Public Key Infrastructures, Services and Application. LNCS 5057, Springer (2008) 118–133

[Mat98] Matyáš, V.: Protecting doctors' identity in drug prescription analysis. Health Informatics Journal (1998) 205–209

Refs (cont.)

[BT94] Benaloh, J., Tuinstra, D.: Receipt-free secret-ballot elections (extended abstract). In: Proc. 26th Symposium on Theory of Computing, ACM Press (1994) 544–553

[JCJ05] Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Proc. 4th ACM Workshop on Privacy in the Electronic Society, ACM Press (2005) 61–70

[AS02] Abe, M., Suzuki, K.: Receipt-free sealed-bid auction. In: Proc. 5th Conference on Information Security. LNCS 2433, Springer (2002) 191–199

[CLK03] Chen, X., Lee, B., Kim, K.: Receipt-free electronic auction schemes using homomorphic encryption. In: Proc. 6th Conference on Information Security and Cryptology. LNCS 2971, Springer (2003) 259–273