LINDDUN

PRIVACY THREAT MODELING

Privacy knowledge *(tables)*

This document contains:

- the **LINDDUN mapping template** (*step 2*)
- the **LINDDUN mitigation strategies taxonomy** and corresponding **mapping table** (*step 5*)
- the **LINDDUN solutions table** (*step 6*)

DistriNet
iMinds
KU LEUVEN

Abstract

This document contains the tables that LINDDUN provides to support the analyst with the required privacy knowledge in each of the LINDDUN steps.

More specifically, this document contains:

- the **LINDDUN mapping template** (used in *step 2*) to map DFD elements to LINDDUN threat categories
- the **LINDDUN mitigation strategies taxonomy** and corresponding **mitigation strategies mapping table** (used in *step 5*) to ease the translation of threats to the solution space
- the **LINDDUN solutions table** (used in *step 6*) to select to most appropriate privacy enhancing technologies (PETs) that correspond to the selected mitigation strategies

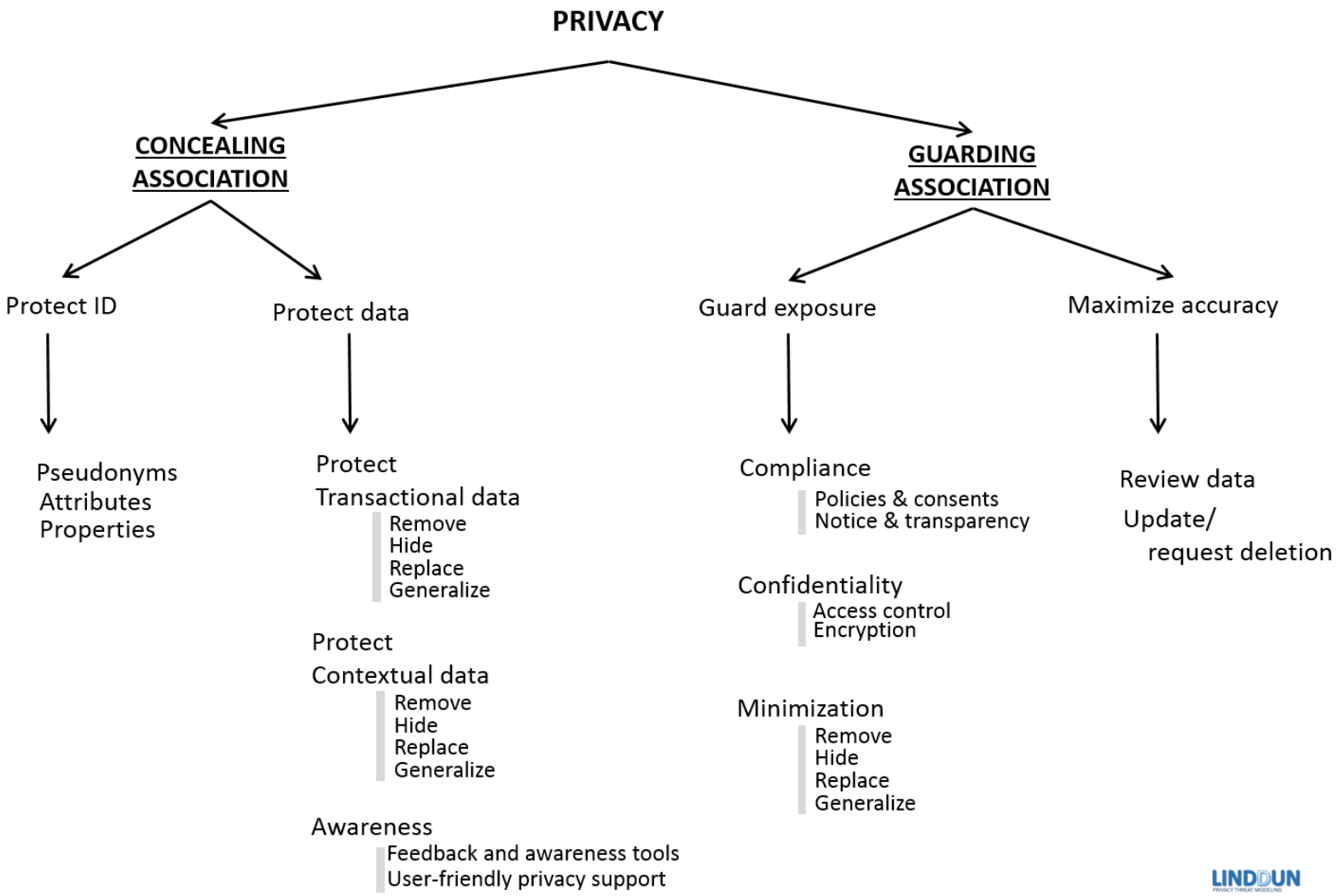
We refer the reader to the LINDDUN website for the most recent LINDDUN threat catalog (as required privacy knowledge in step 3) and other information on the methodology.

LINDDUN - mapping template (step 2)

	L	I	N	D	D	U	N
Data store	X	X	X	X	X		X
Data flow	X	X	X	X	X		X
Process	X	X	X	X	X		X
Entity	X	X				X	

LINDDUN
PRIVACY THREAT MODELING

LINDDUN - mitigation strategies taxonomy (step 5)



LINDDUN - mitigation strategies mapping (step 5)

Mitigation Strategy	LINDDUN Threat Tree
Protect ID	L_e, I_e
Protect data	
Transactional data	L_DF1, I_DF1
Contextual data	L_DF2, I_DF2, D_DF, NR_DF
Awareness	U_1
Guard exposure	
Compliance	NC
confidentiality	ID_DS, NR_DS, *_P
Minimization	L_DS, I_DS, D_DS
Maximize accuracy	
Review data	U_2
Update/request deletion	NR_DS3

LINDDUN
PRIVACY THREAT MODELING

LINDDUN – privacy enhancing solutions (step 6)

Mitigation Strategy					Privacy Enhancing Techniques (PETs)
Concealing association	**Protect ID**	Pseudonyms			Privacy enhancing identity management system [HBC+04], User-controlled identity management system [CPHH02]
		Attributes			Privacy preserving biometrics [STP09], Private authentication [AF04, ABB+04]
		Properties			Anonymous credentials (single show [BC93], multishow [CL04])
	Protect data	Transactional data	Remove		(see awareness to minimize information sharing)
			Hide	Data-flow specific	Multi-party computation (Secure function evaluation) [Yao82, NN01], Anonymous buyerseller watermarking protocol [DBPP09]
				General	see guard exposure - Confidentiality - encryption
			Replace		/
			Generalize		see guard exposure - minimization - generalize
		Contextual data	Remove		Mix-networks (1981) [Cha81], , ISDN-mixes [PPW91], Onion Routing (1996) [GRS96],Tor (2004) [DMS04])
			Hide	General	Crowds (1998) [RR98], Low-latency communication (Freedom Network (1999-2001) [BGS01], Java Anon Proxy (JAP) (2000) [BFK00]
				Undetectability	Steganography [AP98] , Covert communication [MNCM03], Spread spectrum [KM01]
				Non-repudiation	Deniable authentication [Nao02], Off-the-record messaging [BGB04]
			Replace		Mixmaster Type 2 (1994) [Mixa],Mixminion Type 3 (2003) [Mixb]) Single proxy (90s) (Penet pseudonymous remailer (1993-1996), Anonymizer, SafeWeb), anonymous Remailer (Cipherpunk Type 0, Type 1 [Bac],
			Generalize	Undetectability	dummy traffic, DC-networks (1985) [Cha85, Cha88]
		Awareness	Feedback and awareness tools		Feedback tools for user privacy awareness [LHDL04, PK09, LBW08]
			User-friendly privacy support		Data removal tools (spyware removal, browser cleaning tools, activity traces eraser,harddisk data eraser)
Guarding association	**Guard exposure**	Compliance	Policies and Consents		Policy communication (P3P [W3C]), Policy enforcement (XACML [oo], EPAL [IBM])
			Notice and Transparency		/
		Confidentiality	Encryption		Symmetric key & public key encryption [MOV97], Deniable encryption [Nao02],Homomorphic encryption [FG07] , Verifiable encryption [CD98]
			Access control		Context-based access control [GMPT01], Privacy-aware access control [CF08, ACK+09]
		Minimization	Remove		/
			Hide	Receiver privacy	Private information retrieval [CGKS98], Oblivious transfer [Rab81, Cac98])
				Database privacy	Privacy preserving data mining [VBF+04, Pin02], Searchable encryption [ABC+05],Private search [OS05]
				General	see guard exposure - confidentiality - encryption
			Replace		/
			Generalize		K-anonymity model [Swe02b, Swe02a], l-Diversity [MGKV06]
	Maximize accuracy	Review data			/
		Update/ request deletion			/

LINDDUN – privacy enhancing solutions - References (step 6)

[ABB+04] William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Just fast keying: Key agreement in a hostile internet. *ACM Transactions on Information and System Security (TISSEC)*, 7(2):242–273, 2004.

[ABC+05] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In *Advances in Cryptology (CRYPTO'05)*, volume 3621 of *LNCS*, pages 205–222. Springer, 2005.

[ACK+09] Claudio A. Ardagna, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer, and Mario Verdicchio. Exploiting cryptography for privacy-enhanced access control: A result of the PRIME project. *Journal of Computer Security*, 2009.

[AF04] Martín Abadia and Cédric Fournet. Private authentication. *Theoretical Computer Science*, 322(3):427–476, September 2004.

[AP98] Ross Anderson and Fabien Petitcolas. On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, 16:474–481, 1998.

[Bac] André Bacard. Anonymous.to: Cypherpunk tutorial. http://www.andrebacard.com/remail.html.

[BC93] Stefan Brands and David Chaum. Distance-bounding protocols (extended abstract). In *Advances in Cryptology (EUROCRYPT'93)*, volume 765 of *LNCS*, pages 344–359. Springer, 1993.

[BFK00] Oliver Berthold, Hannes Federrath, and Stefan Köpsell. Web MIXes: A system for anonymous and unobservable Internet access. In *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, LNCS, pages 115–129. Springer, 2000.

[BGB04] Nikita Borisov, Ian Goldberg, and Eric Brewer. Off-the-record communication, or, why not to use PGP. In *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society*, pages 77–84. ACM New York, NY, USA, 2004.

[BGS01] A. Back, I. Goldberg, and A. Shostack. Freedom systems 2.1 security issues and analysis. White paper, Zero Knowledge Systems, Inc., May 2001.

[Cac98] Christian Cachin. On the foundations of oblivious transfer. In *Advances in Cryptology (EUROCRYPT'98)*, pages 361–374. Springer, LNCS 1403, 1998.

[CD98] J. Camenisch and I. Damgard. Verifiable encryption and applications to group signatures and signature sharing. In *Technical Report RS-98-32, BRICS, Department of Computer Science, University of Aarhus*, Dec. 1998.

[CF08] Barbara Carminati and Elena Ferrari. Privacy-aware collaborative access control in web-based social networks. In *Proceedings of the 22nd IFIP WG 11.3 Working Conference on Data and Applications Security (DBSEC2008)*, pages 81–96. Springer, 2008.

[CGKS98] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *Journal of the ACM*, pages 41–50, 1998.

[Cha81] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[Cha85] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[Cha88] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *Advances in Cryptology (CRYPTO'04)*, volume 3152 of *LNCS*, pages 56–72. Springer, 2004.

[CPHH02] Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, and Els Van Herreweghen. Privacy-enhancing identity management. The IPTS Report 67, 8-16, September 2002.

[DBPP09] Mina Deng, Tiziano Bianchi, Aalessandro Piva, and Bart Preneel. An efficient buyer-seller watermarking protocol based on composite signal representation. In *Proceedings of 11th ACM workshop on Multimedia and Security*, pages 9–18, 2009.

[DMS04] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.
[FG07] Caroline Fontaine and Fabien Galand. A survey of homomorphic encryption for non-specialists. *EURASIP Journal on Information Security*, pages 41–50, 2007.

[GMPT01] Christos K. Georgiadis, Ioannis Mavridis, George Pangalos, and Roshan K. Thomas. Flexible team-based access control using contexts. In *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies*, SACMAT '01, pages 21–27. ACM, 2001.

[GRS96] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. Hiding Routing Information. In *Proceedings of Information Hiding: First International Workshop*, volume 1174 of *LNCS*, pages 137–150. Springer, May 1996.

[HBC+04] Marit Hansen, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, and Michael Waidner. Privacy-enhancing identity management. *Information Security Technical Report (ISTR)*, 9(1):35–44, 2004.

[IBM] IBM. Enterprise Privacy Authorization Language (EPAL 1.2). W3C Member Submission, 10 November 2003.

[KM01] Darko Kirovski and Henrique Malvar. Robust covert communication over a public audio channel using spread spectrum. In *Information Hiding*, volume 2137 of *LNCS*, pages 354–368. Springer, 2001.

[LBW08] Heather Richter Lipford, Andrew Besmer, and Jason Watson. Understanding privacy settings in facebook with an audience view. In *UPSEC*. USENIX Association, 2008.

[LHDL04] Scott Lederer, Jason I. Hong, Anind K. Dey, and James A. Landay. Personal privacy through understanding and action: Five pitfalls for designers. *Personal and Ubiquitous Computing*, 8:440–454, 2004.

[MGKV06] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, and Muthuramakrishnan Venkitasubramaniam. l-diversity: Privacy beyond k-anonymity. In *Proceedings of the 22nd International Conference on Data Engineering (ICDE'06)*, page 24, 2006.

[Mixa] Mixmaster. Mixmaster homepage. http://mixmaster.sourceforge.net/.

[Mixb] Mixminion. Mixminion official site. http://mixminion.net/.

[MNCM03] Ira Moskowitz, Richard E. Newman, Daniel P. Crepeau, and Allen R. Miller. Covert channels and anonymizing networks. In *In Workshop on Privacy in the Electronic Society*, pages 79–88. ACM, 2003.

[MOV97] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography, 1997. http://www.cacr.math.uwaterloo.ca/hac/.

[Nao02] Moni Naor. Deniable ring authentication. In *Advances in Cryptology (CRYPTO'02)*, volume 2442 of *LNCS*, pages 481–498. Springer, 2002.

[NN01] Moni Naor and Kobbi Nissim. Communication preserving protocols for secure function evaluation. In *Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing (STOC '01)*, pages 590–599. ACM, 2001.

[oo] OASIS (oasis open.org). XACML 3.0 - work in progress, retrieved 09-september-2009. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#CURRENT.

[OS05] Rafail Ostrovsky and William E. Skeith. Private searching on streaming data. In *Advances in Cryptology (CRYPTO'05)*, volume 3621 of *LNCS*, pages 223–240. Springer, 2005.

[Pin02] B. Pinkas. Cryptographic techniques for privacy preserving data mining. *SIGKDD Explorations*, 4(2):12–19, 2002.

[PK09] Sameer Patil and Alfred Kobsa. *Privacy Considerations in Awareness Systems: Designing with Privacy in Mind*, chapter 8, pages 187–206. Human–Computer Interaction Series. Springer, June 2009.

[PPW91] Andreas Pfitzmann, Birgit Pfitzmann, and MichaelWaidner. ISDNmixes: Untraceable communication with very small bandwidth overhead. In *Proceedings of the GI/ITG Conference on Communication in Distributed Systems*, pages 451–463, 1991.

[Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. Technical report TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[RR98] Michael Reiter and Aviel Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1), June 1998.

[STP09] Koen Simoens, Pim Tuyls, and Bart Preneel. Privacy weaknesses in biometric sketches. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, pages 188–203. IEEE Computer Society, 2009.

[Swe02a] Latanya Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):571–588, 2002.

[Swe02b] Latanya Sweeney. k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.

[VBF+04] V.S. Verykios, E. Bertino, I.N. Fovino, L.P. Provenza, Y. Saygin, and Y. Theodoridis. State-of-the-art in privacy preserving data mining. *ACM SIGMOD Record*, 3(1):50–57, Mar. 2004.

[W3C] W3C. Platform for privacy preferences (p3p) project. http://www.w3.org/P3P/.

[Yao82] Andrew Chi-Chih Yao. Protocols for secure computations. In *Proceedings of Twenty-third IEEE Symposium on Foundations ofComputer Science*, pages 160–164, November 1982.