LINDDUN: Privacy Threat Modeling

Presented by a ringer

(Susan Landau)

LINDDUN: Privacy Threat Modeling

- Work out of KU Leuven; researchers are Kim Wuyts, Riccardo Scandariato, Mina Deng, Wouter Joosen, and Bart Preneel.
- See 2010 paper by Deng et al., 2015 PhD thesis by Wuyts, and LINDDUN website.

LINDDUN: Privacy Threat Modeling

- Work out of KU Leuven; researchers are Kim Wuyts, Riccardo Scandariato, Mina Deng, Wouter, Joosen, and Bart Preneel.
- See 2010 paper by Deng et al., 2015 PhD thesis by Wuyts, and LINDDUN website.
- Material here is largely from Wuyts's thesis.

STRIDE: Security Threat Modeling

- **S**poofing of user identity.
- **T**ampering.
- **R**epudiation.
- **I**nformation disclosure.
- **D**enial of service.
- **E**levation of Privilege.

STRIDE: Security Threat Modeling

- **S**poofing of user identity.
- **T**ampering.
- **R**epudiation.
- **I**nformation disclosure.
- **D**enial of service.
- **E**levation of Privilege.

Now part of the Microsoft SDL.

STRIDE Threat Modeling Process

- Define use scenarios.
- Determine external dependencies.
- Define security assumptions.
- Determine external security assumptions (dependencies on outside sources).
- Figure out DFDs.
- Determine types of threats.
- Identify threats to systems.
- Determine risk.
- Plan mitigation.

LINDDUN: Privacy Threat Modeling

- **L**inkability.
- **I**dentifiability.
- **N**on-repudiation.
- **D**etectability.
- Information **D**isclosure.
- Content **U**nawareness.
- **N**on-compliance.

LINDDUN: Privacy Threat Modeling

- **L**inkability: linking items of interest.
- **I**dentifiability.
- **N**on-repudiation.
- **D**etectability.
- Information **D**isclosure.
- Content **U**nawareness.
- **N**on-compliance.

LINDDUN: Privacy Threat Modeling

- **L**inkability.
- **I**dentifiability: can identify subject from item.
- **N**on-repudiation.
- **D**etectability.
- Information **D**isclosure.
- Content **U**nawareness.
- **N**on-compliance.

LINDDUN: Privacy Threat Modeling

- **L**inkability.
- **I**dentifiability.
- **N**on-repudiation: attacker can counter claims.
- **D**etectability.
- Information **D**isclosure.
- Content **U**nawareness.
- **N**on-compliance.

LINDDUN: Privacy Threat Modeling

- **L**inkability.
- **I**dentifiability.
- **N**on-repudiation.
- **D**etectability: determines if an item exists.
- Information **D**isclosure.
- Content **U**nawareness.
- **N**on-compliance.

LINDDUN: Privacy Threat Modeling

- **L**inkability.
- **I**dentifiability.
- **N**on-repudiation.
- **D**etectability.
- Information **D**isclosure: to those w/o access.
- Content **U**nawareness.
- **N**on-compliance.

LINDDUN: Privacy Threat Modeling

- **L**inkability.
- **I**dentifiability.
- **N**on-repudiation.
- **D**etectability.
- Information **D**isclosure.
- Content **U**nawareness: user unaware.
- **N**on-compliance.

LINDDUN: Privacy Threat Modeling

- **L**inkability.
- **I**dentifiability.
- **N**on-repudiation.
- **D**etectability.
- Information **D**isclosure.
- Content **U**nawareness.
- **N**on-compliance: system may not comply.

LINDDUN: Privacy Threat Modeling

- **L**inkability.
- **I**dentifiability.
- **N**on-repudiation.
- **D**etectability.
- Information **D**isclosure.
- Content **U**nawareness.
- **N**on-compliance.

Value of LINDDUN: Systemization.

LINDDUN Steps

- Create a Data Flow Diagram (DFD).
- Map privacy threats to DFD.
- Identify threat scenarios.
- Threat prioritization (risk analysis).
- Extract privacy requirements.
- Select appropriate PETs.

LINDDUN Steps

- Create a Data Flow Diagram (DFD).
- Map privacy threats to DFD.
- Identify threat scenarios.

Problem space.

- Threat prioritization (risk analysis).
- Extract privacy requirements.
- Select appropriate PETs.

Solution space.

LINDDUN Steps

- Create a Data Flow Diagram (DFD).
- Map privacy threats to DFD.
- Identify threat scenarios.

Problem space.

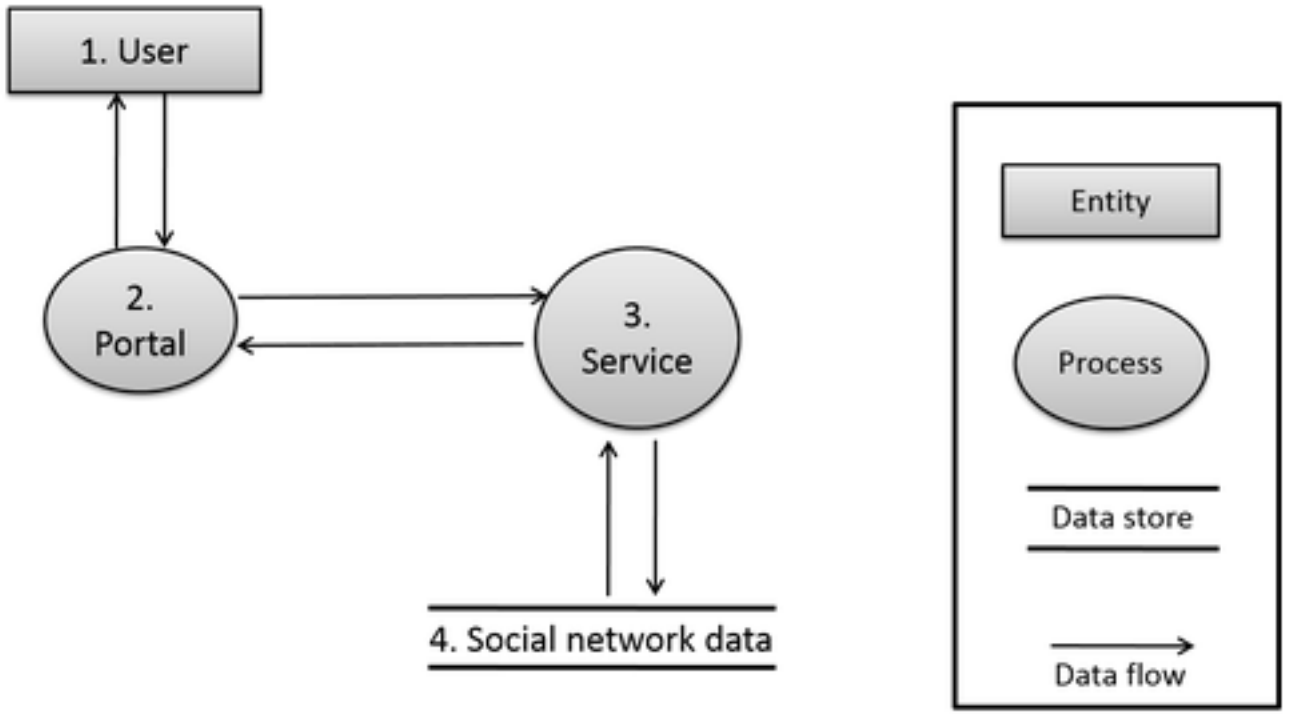
- Threat prioritization (risk analysis).
- Extract privacy requirements.
- Select appropriate PETs.

Solution space.

Can integrate STRIDE and LINDDUN into SDL.

Data Flow Diagram

- Social network application:



Map privacy threats to DFD

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

Map privacy threats to DFD

	L	I	N	D	D	U	N
Entity	X	X				X	

- Entity Linkability:
- Entity Identifiability:
- Entity Unawareness.

Map privacy threats to DFD

	L	I	N	D	D	U	N
Entity	X	X				X	

- Entity Linkability: only applies if require system to be used anonymously.
- Entity Identifiability:

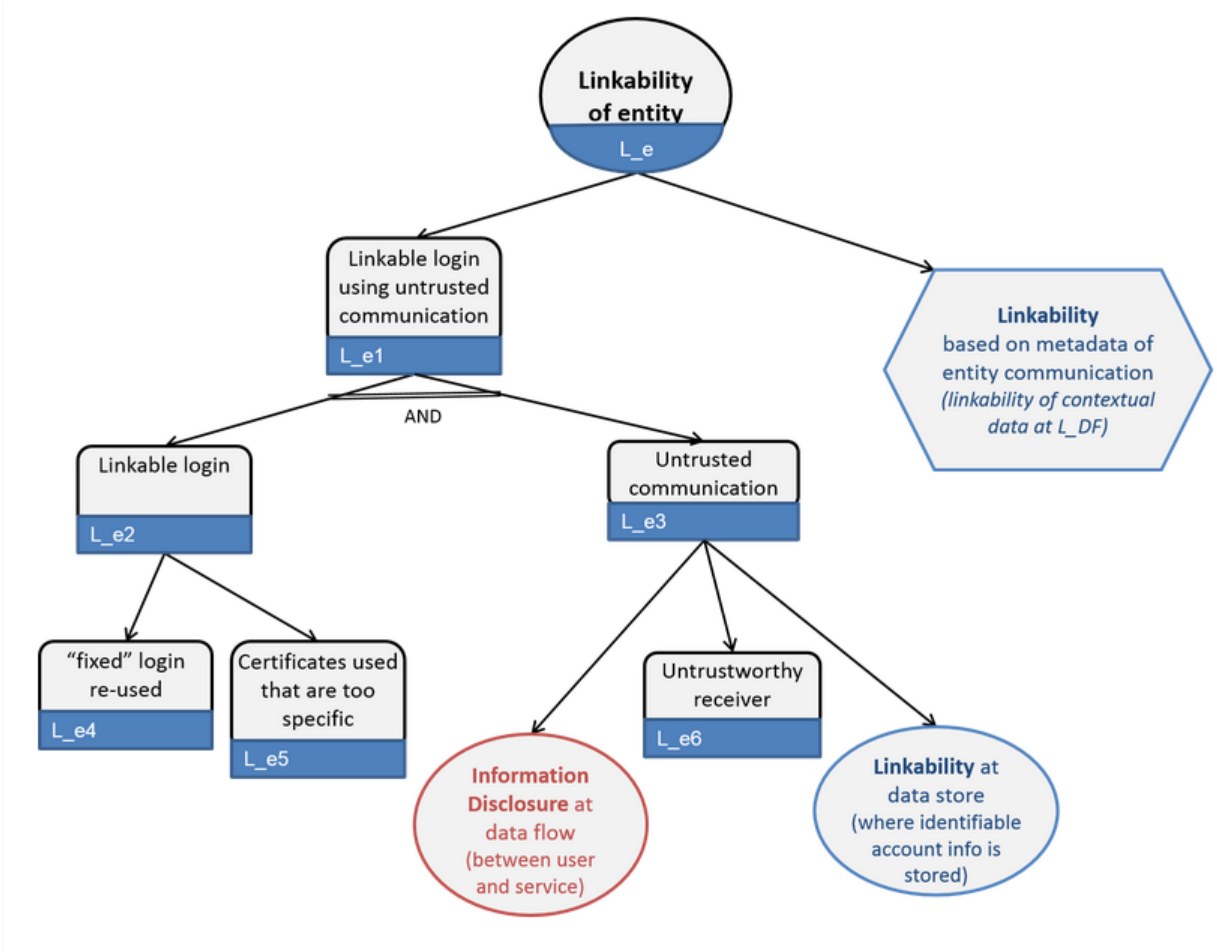
- Entity Unawareness.

Map privacy threats to DFD

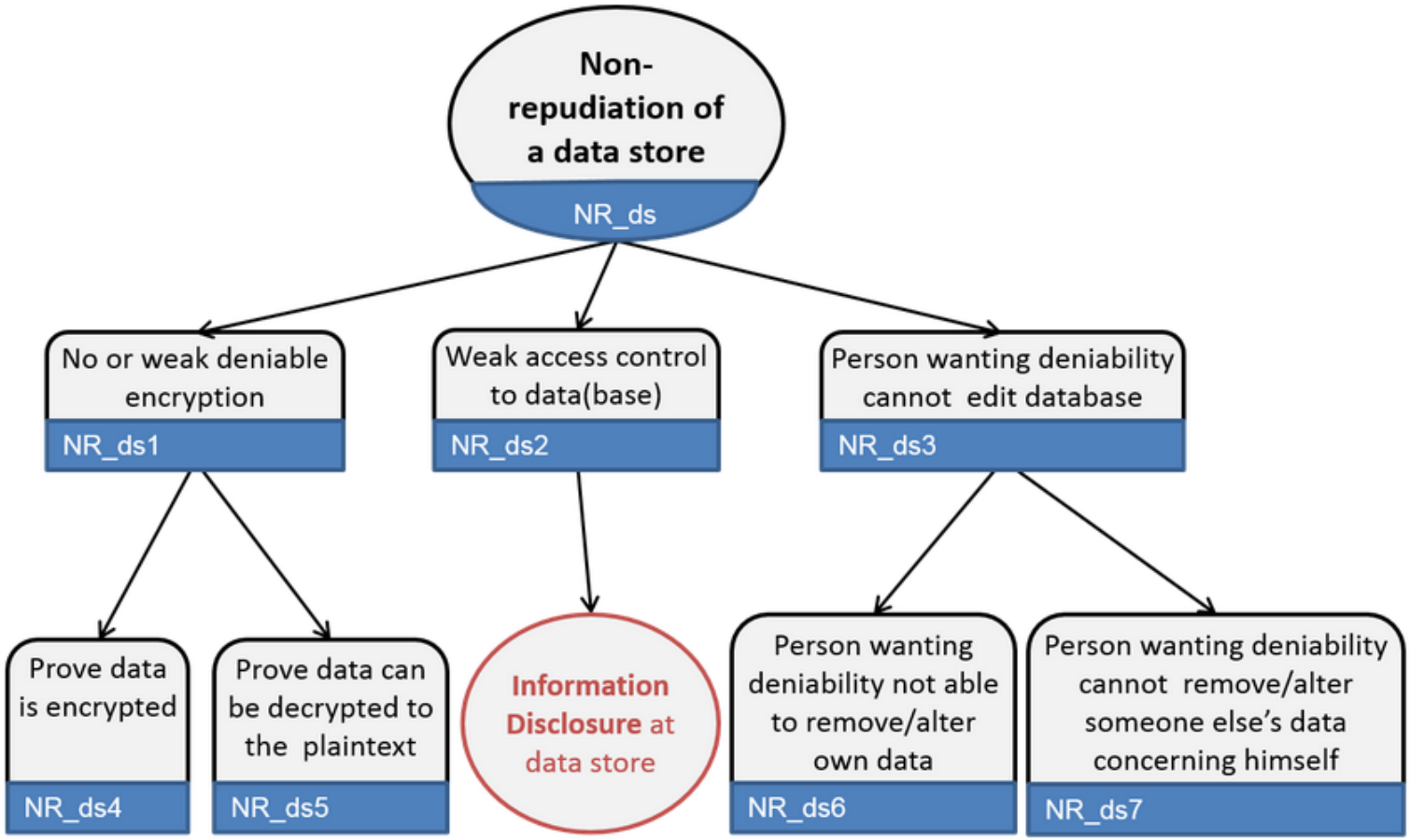
	L	I	N	D	D	U	N
Entity	X	X				X	

- Entity Linkability: only applies if require system to be used anonymously.
- Entity Identifiability: only applies if require system to be used anonymously.
- Entity Unawareness.

Identify Threat Tree Patterns



Identify Threat Tree Patterns



Catalog of Privacy Threat Trees

- **Linkability**
  - Linkability of entity
  - Linkability of data flow
  - Linkability of data store
  - Linkability of process
- **Identifiability**
  - identifiability of entity
  - identifiability of data flow
  - identifiability of data store
  - identifiability of process
- **Non-repudiation**
  - non-repudiation of data flow
  - non-repudiation of data store
  - non-repudiation of process
- **Detectability**
  - detectability of data flow
  - detectability of data store
  - detectability of process
- **Disclosure of information**
- **Unawareness**
  - Unawareness of entity
- **Non-compliance**
  - policy and consent non-compliance

CDR Example

Privacy Threat Target	L	I	N	D	D	U	N	T
origIPAddr	+	+	+	+	+		+	N
callingPartyNumber	+	+	+	+	+		+	S
origMediaTransport Addr. IP+Port	+	+	+	+	+		+	N
destIpAddr	+	+	+	+	+		+	M
originalCalledPartyNumber	+	+	+	+	+		+	N
finalCalledParty Number	+	+	+	+	+		+	S
destMediaTransport Addr. IP+Port	+	+	+	+	+		+	M
dateTimeOrigination	+	+	+	+	+		+	N
dateTimeConnect	+	+	+	+	+		+	N
dateTimeDisconnect	+	+	+	+	+		+	N
duration	+	+	+	+	+		+	S
stakeholder caller	+	+				+		N
stakeholder callee	+	+				+		M

Threat Levels: S = Serious, N = Normal, M Merely.

From “Conducting a Privacy Impact Analysis of an Analysis of Call Detail Records,” by Hofbauer, Beckers, Quirchmayer.

What's Available

- LINDDUN Summary (web page).
- Examples of where LINDDUN has been used (web page on testimonials): social network risk analysis,smart cities IoT, analysis of comms records.
- Mitigation strategies.

What's Available

- LINDDUN Summary (web page).
- Examples of where LINDDUN has been used (web page on testimonials): social network risk analysis,smart cities IoT, analysis of comms records.
- Mitigation strategies.

LINDDUN does PbD by doing rigorous analysis.