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

- **Spoofing** of user identity.
- **Tampering**.
- **Repudiation**.
- **Information disclosure**.
- **Denial of service**.
- **Elevation of Privilege**.
STRIDE: Security Threat Modeling

- Spoofing of user identity.
- Tampering.
- Repudiation.
- Information disclosure.
- Denial of service.
- Elevation 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

- Linkability.
- Identifiability.
- Non-repudiation.
- Detectability.
- Information Disclosure.
- Content Unawareness.
- Non-compliance.
LINDDUN: Privacy Threat Modeling

- Linkability: linking items of interest.
- Identifiability.
- Non-repudiation.
- Detectability.
- Information Disclosure.
- Content Unawareness.
- Non-compliance.
LINDDUN: Privacy Threat Modeling

- **Linkability.**
- **Identifiability:** can identify subject from item.
- **Non-repudiation.**
- **Detectability.**
- **Information Disclosure.**
- **Content Unawareness.**
- **Non-compliance.**
LINDDUN: Privacy Threat Modeling

- Linkability.
- Identifiability.
- Non-repudiation: attacker can counter claims.
- Detectability.
- Information Disclosure.
- Content Unawareness.
- Non-compliance.
LINDDUN: Privacy Threat Modeling

- **Linkability.**
- **Identifiability.**
- **Non-repudiation.**
- **Detectability:** determines if an item exists.
- **Information Disclosure.**
- **Content Unawareness.**
- **Non-compliance.**
LINDDUN: Privacy Threat Modeling

- **Linkability.**
- **Identifiability.**
- **Non-repudiation.**
- **Detectability.**
- **Information Disclosure:** to those w/o access.
- **Content Unawareness.**
- **Non-compliance.**
LINDDUN: Privacy Threat Modeling

- **Linkability.**
- **Identifiability.**
- **Non-repudiation.**
- **Detectability.**
- **Information Disclosure.**
- **Content Unawareness:** user unaware.
- **Non-compliance.**
LINDDUN: Privacy Threat Modeling

• Linkability.
• Identifiability.
• Non-repudiation.
• Detectability.
• Information Disclosure.
• Content Unawareness.
• Non-compliance: system may not comply.
LINDDUN: Privacy Threat Modeling

- Linkability.
- Identifiability.
- Non-repudiation.
- Detectability.
- Information Disclosure.
- Content Unawareness.
- Non-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.
- Threat prioritization (risk analysis).
- Extract privacy requirements.
- Select appropriate PETs.

Problem space.
Solution space.
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.

Can integrate STRIDE and LINDDUN into SDL.
Data Flow Diagram

- Social network application:
Map privacy threats to DFD

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>I</th>
<th>N</th>
<th>D</th>
<th>D</th>
<th>U</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Data store</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data flow</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Process</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Map privacy threats to DFD

- Entity Linkability:
- Entity Identifiability:
- Entity Unawareness.
Map privacy threats to DFD

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

- 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

- **Linkability of entity**
  - **Linkable login using untrusted communication**
    - **L_e1**
      - **Linkable login**
        - **L_e2**
          - "fixed" login re-used
          - Certificates used that are too specific
            - **L_e4**
            - **L_e5**
      - **Untrusted communication**
        - **L_e3**
          - Untrustworthy receiver
            - **L_e6**
    - **AND**
  - **Information Disclosure at data flow (between user and service)**
    - **L_e7**
  - **Linkability at data store (where identifiable account info is stored)**
  - **Linkability based on metadata of entity communication (linkability of contextual data at L_DF)**

Identify Threat Tree Patterns

Non-repudiation of a data store

- No or weak deniable encryption
  - Prove data is encrypted

- Weak access control to data(base)
  - Prove data can be decrypted to the plaintext

- Person wanting deniability cannot edit database
  - Person wanting deniability not able to remove/alter own data
  - Person wanting deniability cannot remove/alter someone else’s data concerning himself

Information Disclosure at data store
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**

<table>
<thead>
<tr>
<th>Privacy Threat Target</th>
<th>L</th>
<th>I</th>
<th>N</th>
<th>D</th>
<th>D</th>
<th>U</th>
<th>N</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>origIPAddr</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>callingPartyNumber</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>origMediaTransport Addr. IP+Port</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>destIpAddr</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>originalCalledPartyNumber</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>finalCalledParty_Number</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>destMediaTransport Addr. IP+Port</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>dateTimeOrigination</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>dateTimeConnect</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>dateTimeDisconnect</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>duration</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>stakeholder caller</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>stakeholder callee</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>M</td>
<td></td>
</tr>
</tbody>
</table>

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.