Development of a Formal IT-Security Model for Remote Electronic Voting Systems

Authors: Rüdiger Grimm and Melanie Volkamer

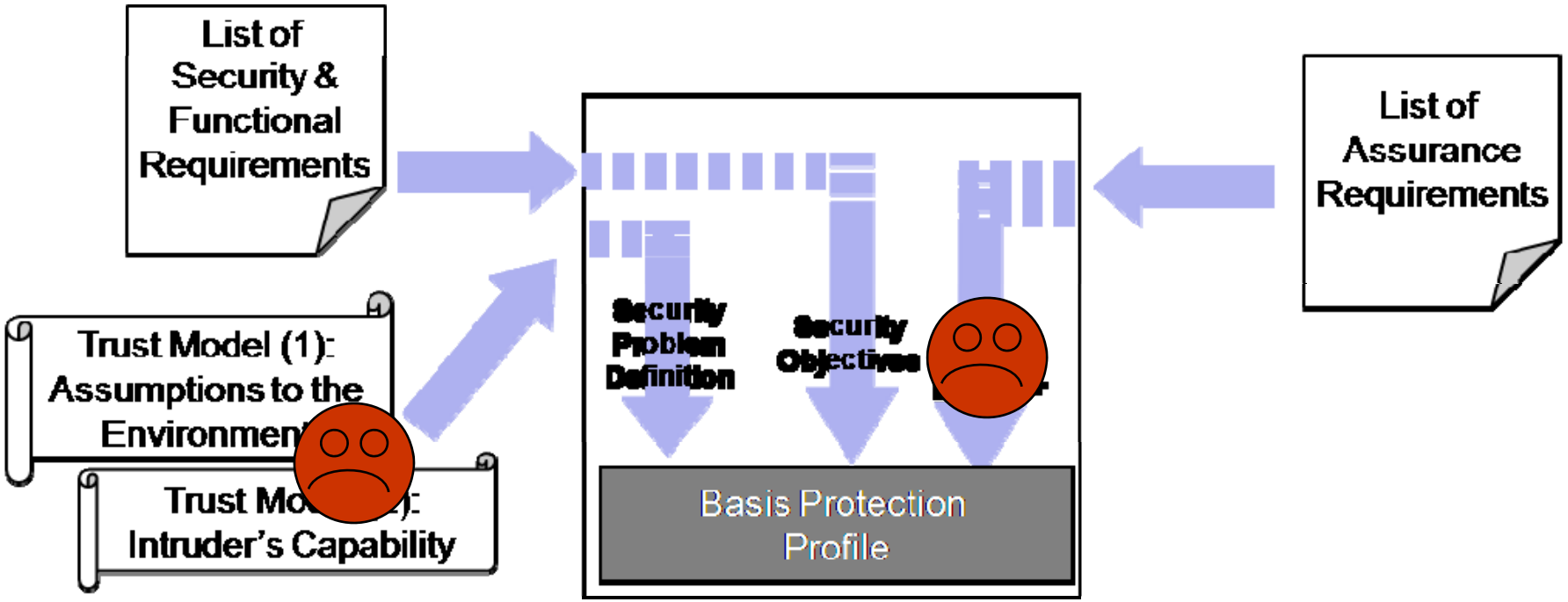
Outline

- Background and motivation
- Common Criteria evaluation assurance levels
- IT-security modeling
- Formal IT-security model for remote electronic voting
- Conclusion

Background and Motivation

- Remote electronic voting is widely used
  - Mostly for low level elections (e.g. in the GI)
  - In some cases for parliamentary elections (e.g. Estonia)
- To gain trust: use only evaluated & certified systems
  - List of requirements
  - Trust model under which the requirements must hold
  - Evaluation procedures/methods & certification procedures
- Solution: Common Criteria Evaluation Methodology
- GI/BSI/DFKI Project (2006-2008)
  - Development of a **Basis** Protection Profile
  - http://www.bsi.de/cc/pplist/pplist.htm#PP0037

GI/BSI/DFKI PP



Evaluation Assurance Levels (EAL)

- Common Criteria Levels: EAL1-EAL7+ (augmented)
- With arising EAL number
  - More trustworthiness into a certified system
  - More effort for developers & evaluators → more expensive
- Most CC evaluations today are below EAL4+
- EAL5 – semi-formal / EAL6&7 – formal methods
  - Redevelopment necessary
  - Developers with knowledge about formal methods

Evaluation Assurance Levels *(Ctd.)*

- Advantages of formal methods:
  - Unambiguous interpretation → easier to implement
  - Identification of inconclusive, inconsistent and contradictory requirements
  - Unambiguous evaluation results

- Parliamentary elections = important for democracy
  →EAL7 should be applied
- ADV_SPM.1 demands a formal IT-security model
  - Already published & established model as a whole or in parts
  - Develop new/ partially new model

New Model Required

- For remote electronic voting: partially new model
- Already existing models possibly usable like
  - BIBA for integrity of data
  - Clark-Wilson for separation of duty
- But no model for anonymity or voter authentication

IT- Security Model (General Intro)

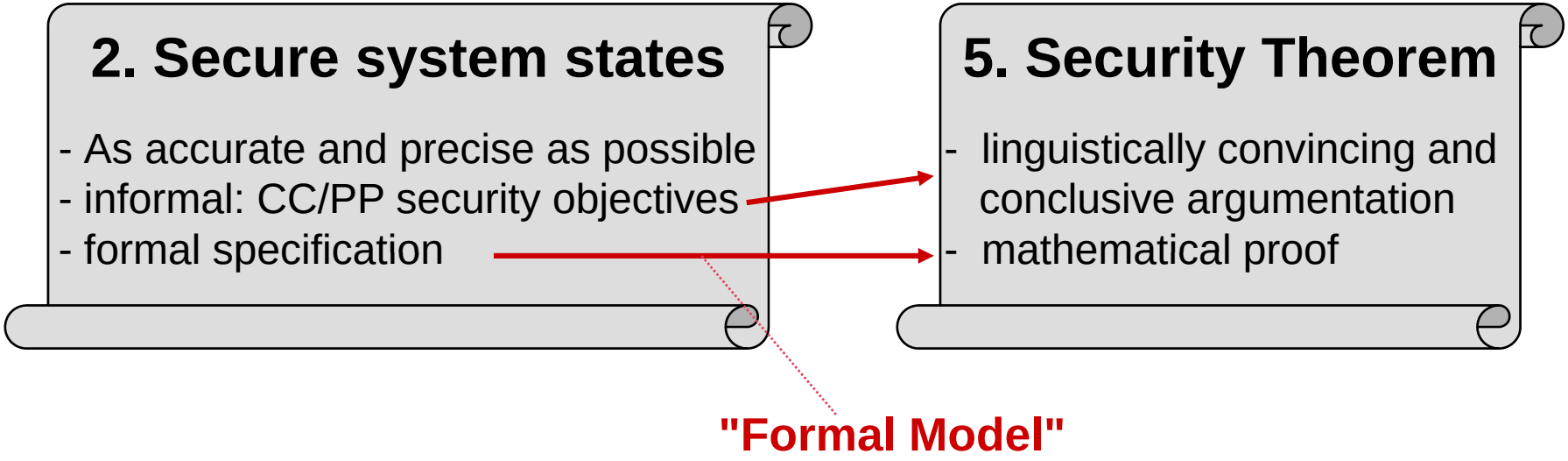
UNIVERSITÄT PASSAU

UNIVERSITÄT KOBLENZ · LANDAU

1. Definition of a *superior security objective*
2. Specification of *secure system states*, which represent together the superior security objective
3. *Trust model* defining a set of assumption under which the set of secure system states is equivalent to the superior security objective
4. Set of *permitted state transitions*
5. *Security theorem* claiming that any permitted state transition transfers any secure state into a secure state again

IT Security Model Elements

1. Superior security objective
2. Secure system states
3. Trust model
4. Permitted state transitions
5. Security theorem



Formal IT-Security Model

- Explanation for 3. (trust model) remains informal

- Third gap may exist between:
  - Linguistically formulated security objectives from the CC/PP
  - Formal specification of the secure states
- Cannot be formalized: subject of argumentative discourse

Formal IT-Security Model for Remote Electronic Voting

1. Superior security objective :

   „Execution of a secure, equal, universal and free remote electronic election."

2. Specification of secure states

   a) Definition of a system state: $< W, S, voter >$

   W – set of eligible voters, S – set of votes in the e-ballot box,
   voter – function S → M (=all persons)

   b) Initial state: $< W_{total}, S_0=\{\}, voter_0=\{\} >$

O.UnauthVoter: $\forall\ s \in S:\ voter(s) \in W_{total}$

O.OneVoterOneVote: (A) $\forall\ s, s' \in S: voter(s)=voter(s') \Rightarrow s=s'$

(B) $\forall\ x \in W_{total} \backslash W:\ \exists\ s \in S: voter(s)=x$

Formal IT-Security Model for Remote Electronic Voting *(ctd.)*

UNIVERSITÄT PASSAU

UNIVERSITÄT KOBLENZ · LANDAU

3. Trust model

   "*The set of assumptions and the corresponding reasoning are part of the CC/PP from the GI/BSI/DFKI project.*"

4. Permitted State Transactions $<S_i,W_i,voter_i>$ to $<S_{i+1},W_{i+1},voter_{i+1}>$

   a) [rule 1] $W_i = W_{i+1} \wedge S_i = S_{i+1} \wedge voter_i = voter_{i+1}$ (no vote is cast)

   b) [rule 2] $\exists\, s \in S_{i+1}\!:\ (\ voter_{i+1}(s) \in W_i \wedge W_{i+1} = W_i \backslash \{voter_{i+1}(s)\} \wedge S_i = S_{i+1} \backslash \{s\}\ )$

5. Theorem

   "*For all permitted state transitions starting with the initial state* $Z_0 = <W_{total}, \{\}, \{\}>$ *holds that any reachable state is a secure state"*

Proof of Theorem

- Formal proof by mathematical induction over state i
- Initial state < W_{total}, S_0={}, $voter_0$={} > obviously secure
  - Reason: Secure states by “universal quantifier ∀"
- Step from states i to i+1 with the help of 3 lemmas (simple propositions)
- For example, "lemma 3":
  - **L3:** $\forall s \in Si : \exists j < i : voter(s) \in W_j \setminus W_i$
  - **Interpretation:** For each vote stored in the e-ballot box, there exists a voting right discarded earlier.

Conclusion

- CC/PP from the GI/BSI/DFKI project proposes EAL2+
- For some type of elections enough trustworthiness
- For other elections, responsible election authority might demand EAL6 or 7
- Formal IT-security model necessary to develope
- First step for two identified security objectives
- **BUT: a lot of open research questions**
  - e.g., how to converge models addressing different security objectives?
  - e.g., how to marry models with technical design

Thank your for your attention

?Questions?

volkamer@uni-passau.de
grimm@uni-koblenz.de