

Cryptography on Non-Trusted Machines

Stefan Dziembowski



Outline

- Introduction
- State-of-the-art
- Research plan

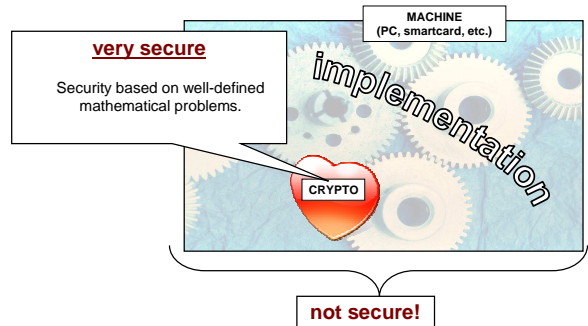
Idea

Design **cryptographic protocols that are secure**

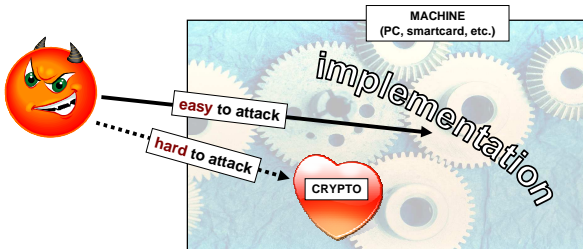
even

on the machines that are not fully trusted.

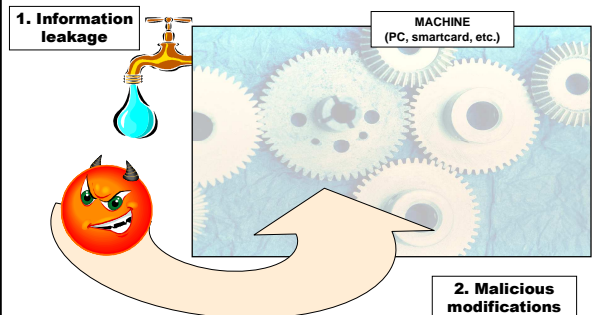
How to construct secure digital systems?

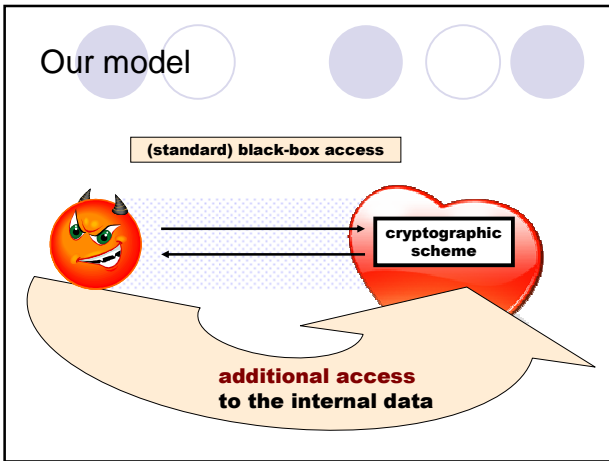
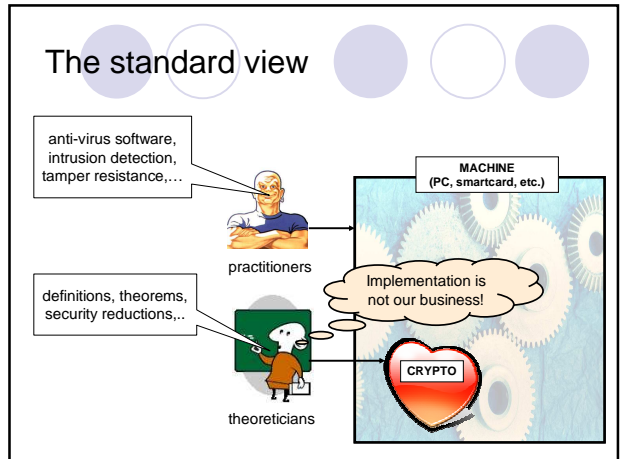
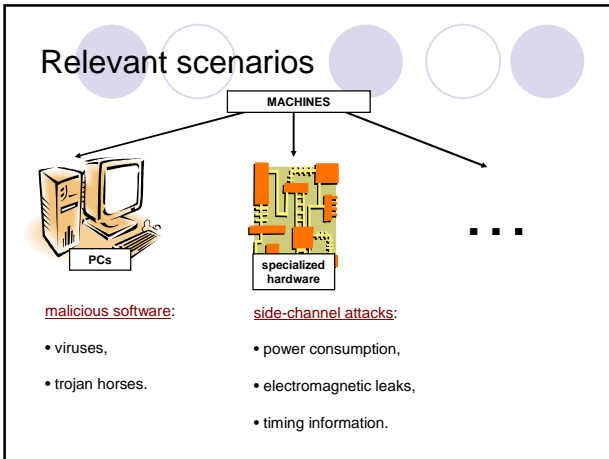


The problem

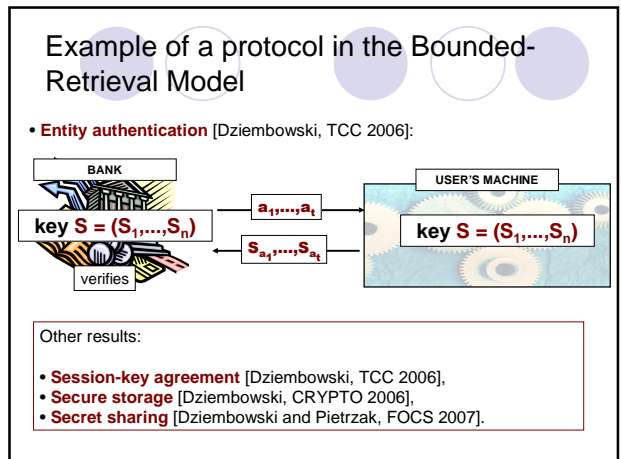
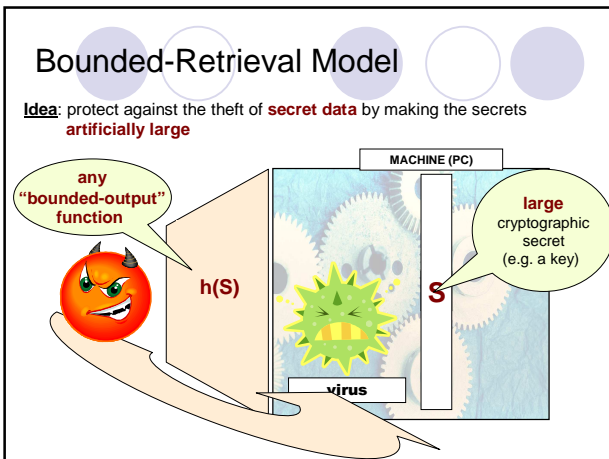


Machines cannot be trusted!

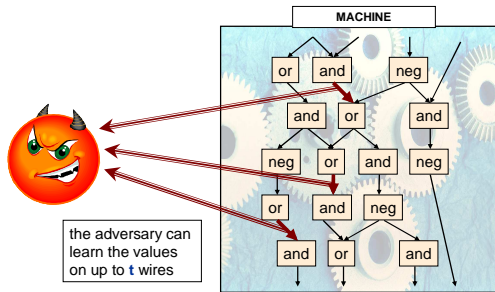




State-of-the-art

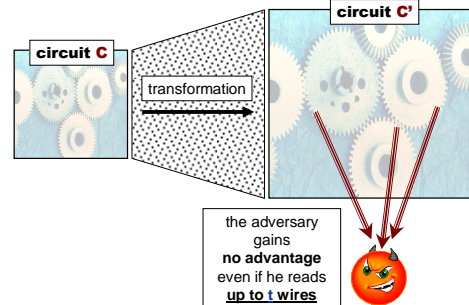


Private circuits – the model:

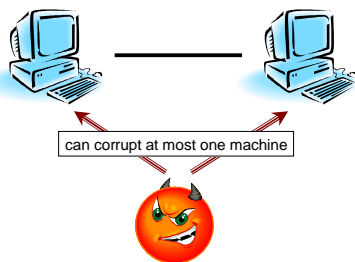


Private circuits – the construction:

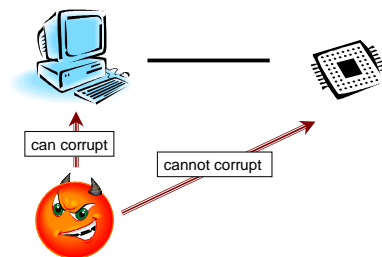
[Ishai, Sahai and Wagner, CRYPTO 2003]



Distributed cryptography



External trusted hardware



Research Plan

The general goal

Contribute to creating a **new discipline**:

“**Cryptography on Non-Trusted Machines**”

with

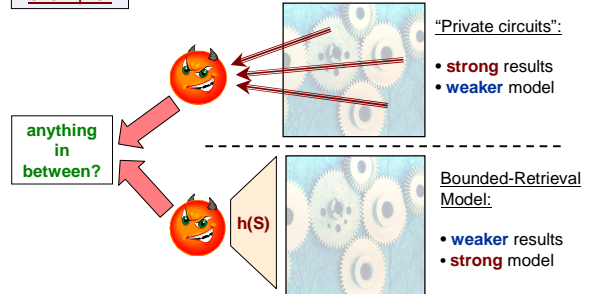
- solid foundations, and
- practical impact.

Objectives

1. Extensions of the models
2. New applications and methods
3. Improvement of the previous results
4. Theoretical foundations

Objective 1: Extend (and unify) the existing models

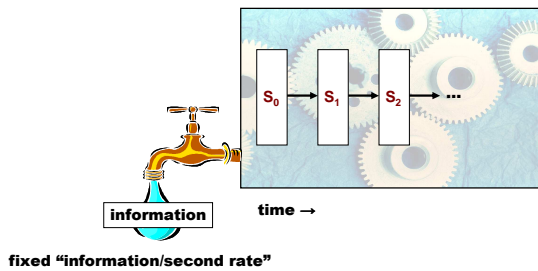
example:



Objective 2: New methods

Example 1:

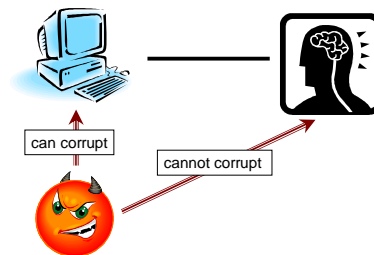
Key evolution:



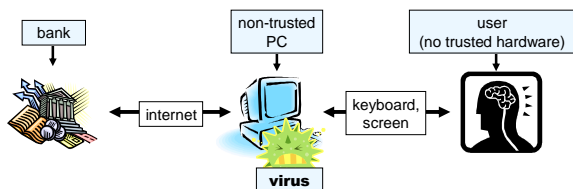
Objective 2: New methods

example:

human-based methods:



Human-based methods – an example



Known method of **user authentication**:

one-time passwords

drawback: authenticates the user not the transaction!

Can we also authenticate the transaction?

Objective 3: Improvement of the previous results

Most of the papers in this area contain just the feasibility results.

Can they be optimized?

Objective 4: Theoretical foundations

- Cryptography has well-known connections to the **complexity theory**.
- "Cryptography on Non-Trusted Machines" provides new connections of these type.

Bounded-Retrieval Model has non-trivial connections to:

1. the theory of **compressibility of NP-instances** [Dziembowski, CRYPTO 2006], and
2. the theory of **round complexity** [Dziembowski and Pietrzak, FOCS 2007].

Can these be extended?

Conclusion

"Cryptography on Non-Trusted Machines" - a new area with a **big potential**.

- Dziembowski and Pietrzak
Intrusion-Resilient Secret Sharing.
FOCS 2007
- Dziembowski
On Forward-Secure Storage.
CRYPTO 2006
- Dziembowski
Intrusion-Resilience Via the Bounded-Storage Model.
TCC 2006