Dealing with masquerading traitors in organizations

Martin Macák

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY, BRNO

lasaris

Masquerading traitors

- Traitors that are masquerading as their coworkers in an organization.
- They know the organization.
- They can act inconspicuously.
- They can perform a colluding insider attack by themselves.

State of the art

- Traitor detection
  - Usually uses psychological aspects.
  - For example narcissism, alienation, radical political attitudes, …
  - These techniques might be hard to perform due to available data sources (emails, Facebook, Twitter, YouTube, …)
  - Furthermore, their precision and recall might be low.
- Masquerader detection
  - Usually relies on the fact that the masquerader is an outsider.
  - Their behavior is distinguishable from the usual behavior of employees.
  - These techniques do not work on someone who knows the organization and its processes.

Computer usage – example

- Alice’s work on her PC:
  1. Starts to program in Visual Studio IDE.
  2. Sometimes, while programming, she connects to the database using SQL Server Management Studio.
  3. After some time, she closes Visual Studio and starts to open PDF files using Acrobat Reader and rewrite some info from them to text documents using Microsoft Word.
  4. Afterwards, she opens the Outlook email client and sends the created text documents to a colleague.
  5. After some time, she goes to a coffee break.
  6. When she comes back from a coffee break, she opens Visual Studio and uses it until the end of her work.

Computer usage – example

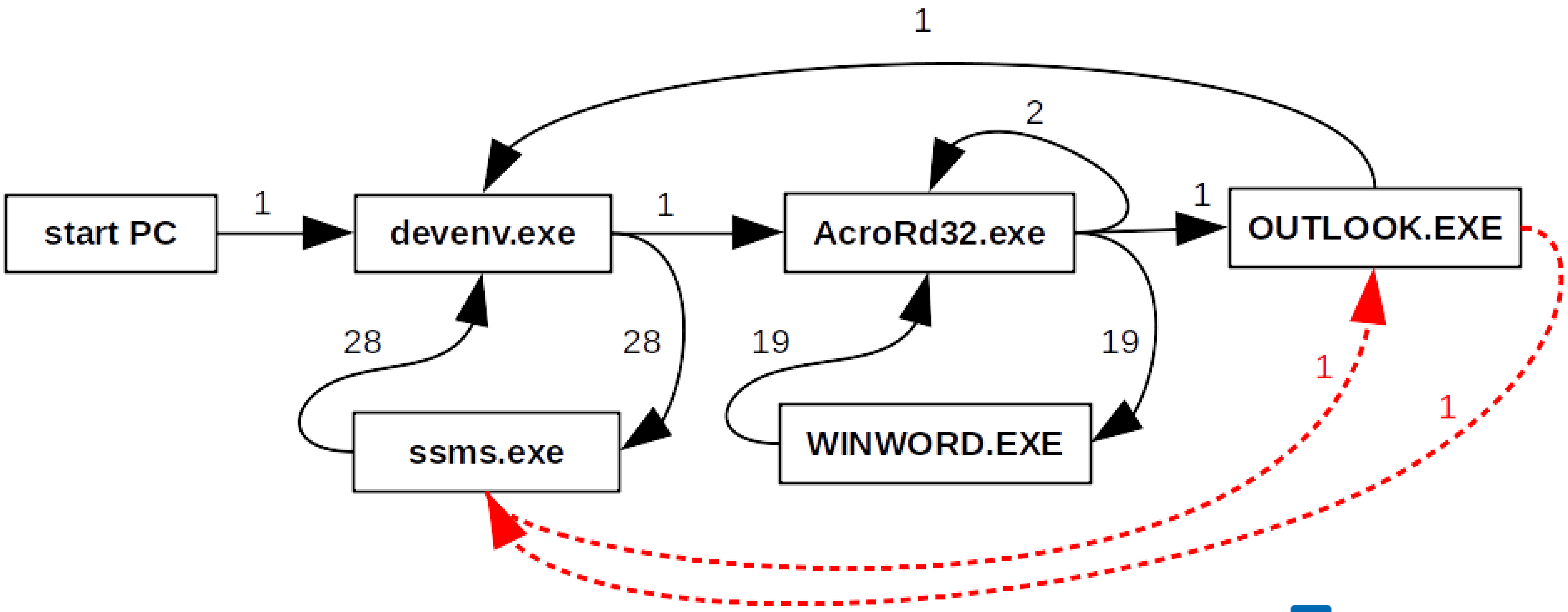
- Chuck’s evil motive:
  - He wants to exfiltrate data about specific customers.
  - He has access to such data but sees just customerIDs.
  - Alice from the other department has access to customer names he needs to get.
  - Therefore, Chuck starts to look for an opportunity…

- Chuck’s evil activity:
  1. During Alice’s coffee break, Chuck notices she left her PC unlocked.
  2. He uses it to connect to the database using SQL Server Management Studio and gets the data he wants.
  3. He sends the desired customerIDs to his email address via Outlook and deletes the email from sent emails.

lasaris

Proposed solution

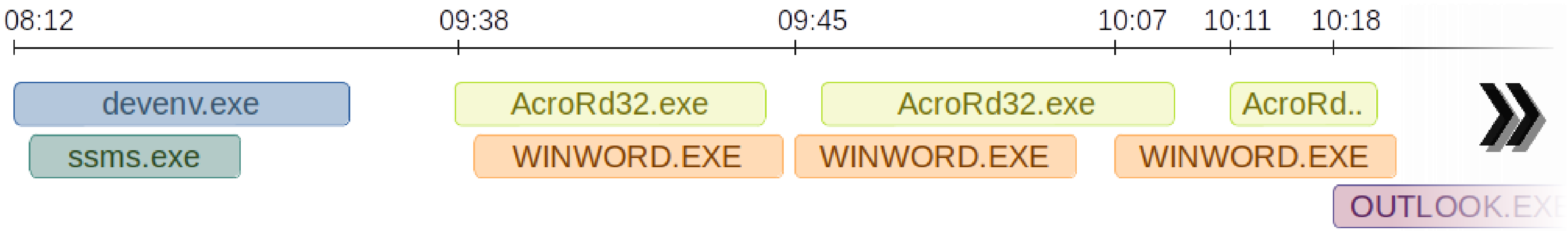
- Let Alice decide at the end of her work time whether her computer’s usage was OK.



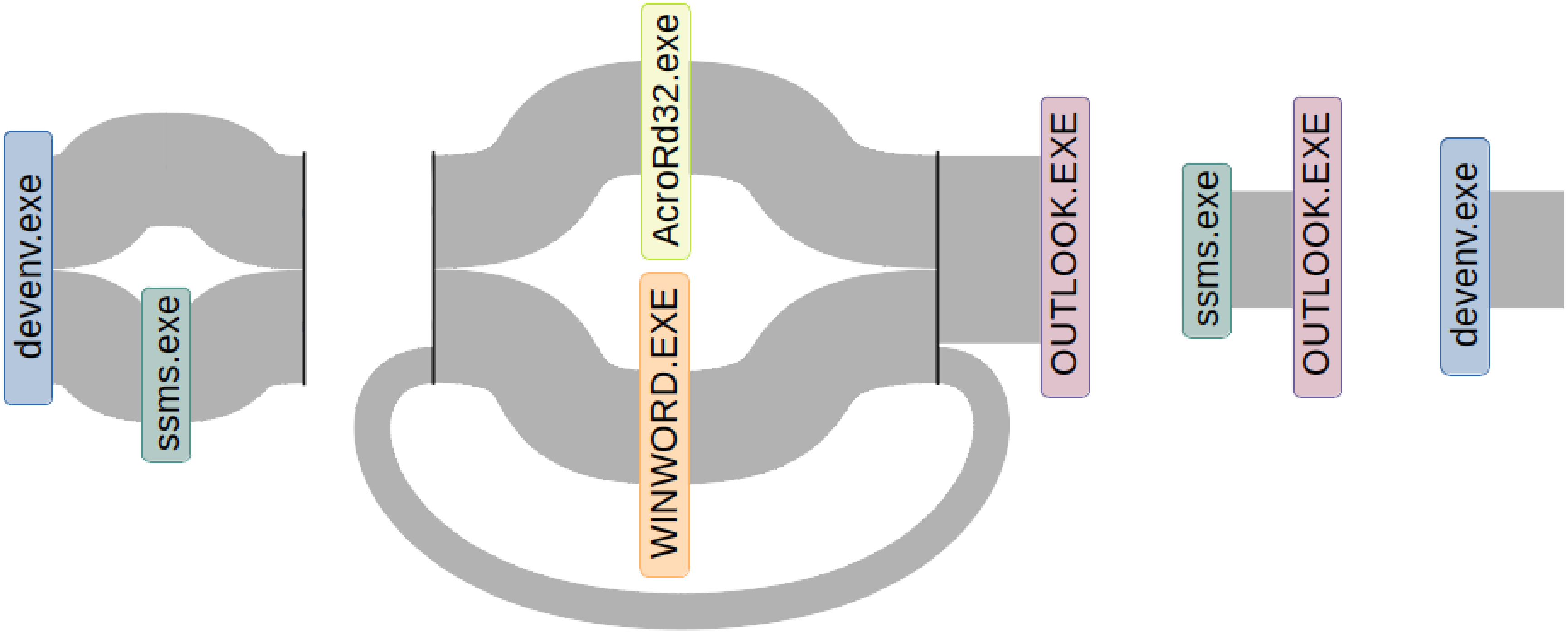
Challenges and issues

1. Automated collection of data that captures the evidence of computer usage.
   - Which data can be useful?
   - How to transform and select the proper data for the model discovery?
2. Automatic creation of aggregated models that usefully capture the behavior on the PC of its user.
   - Which process mining algorithm to use?
   - How to choose the proper process visualization for the user?
3. Automatic generation of interactive data views.
   - How to provide users the interactive option to inspect their activity effectively?

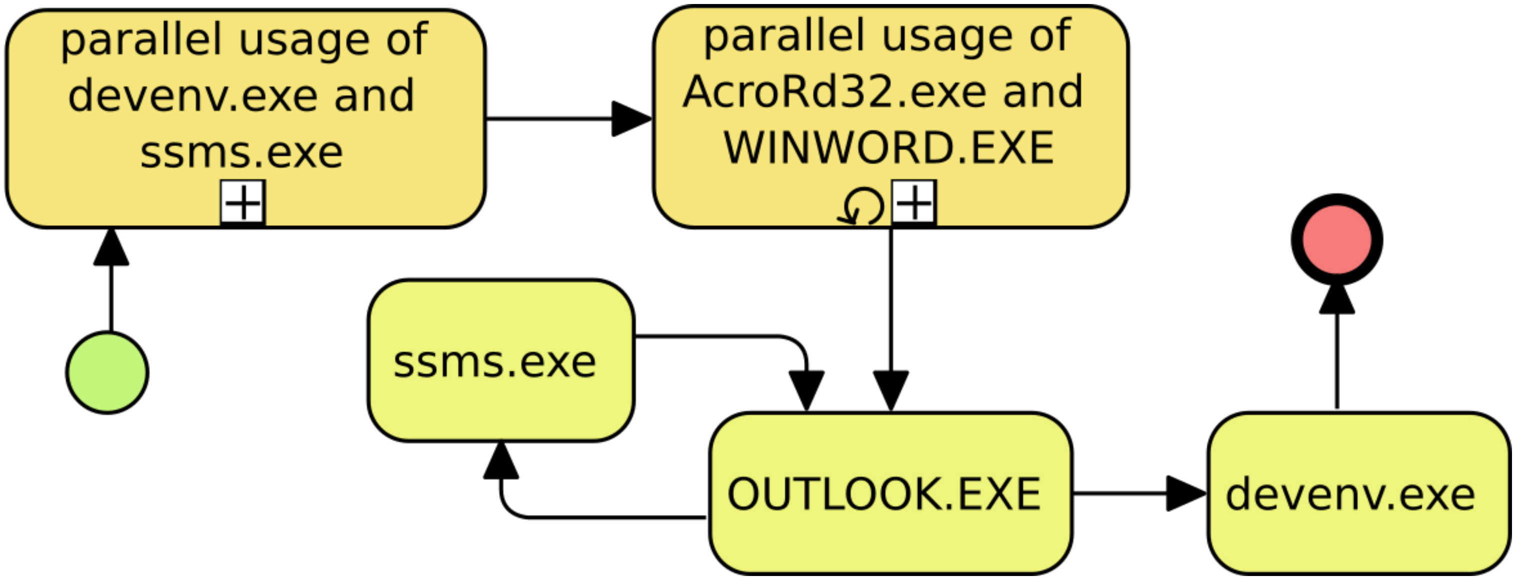
Examples of process models



Examples of process models



Examples of process models


parallel usage of devenv.exe and ssms.exe
parallel usage of AcroRd32.exe and WINWORD.EXE
ssms.exe
OUTLOOK.EXE
devenv.exe

Future work

1. Assessment of data that can be gathered from Windows.
2. Creation of process models from the collected data.
3. Evaluation of participants’ abilities to detect suspicious behavior from the process model.
4. Evaluation of enhanced interactive views on models.
5. Real case study.

If something "fails", we can still use the results in other research directions ☺