Technische Hochschule
Brandenburg
University of
Applied Sciences

Virtual Sessions for Forensic Analysis of VCS:
A Novel Methodology

Jaykumar Soni, Tom Neubert, Benjamin Dietrich, Claus Vielhauer

Agenda

I. **Introduction to VCS**

II. The Growing Concern and Research Gap

III. Our Contribution and Visualisation

IV. State-of-the-Art in VCS Analysis

V. Detailed steps of our methodology

VI. Early Results

VII. Future work and Conclusion

Introduction to VCS

- Bridging Geographical Divides
- Essential for Remote work and Collaboration
- Vital in personal communications
- Benefits and associated challenges

Agenda

I. ~~Introduction to VCS~~

II. The Growing Concern and Research Gap

III. Our Contribution and Visualisation

IV. State-of-the-Art in VCS Analysis

V. Detailed steps of our methodology

VI. Early Results

VII. Future work and Conclusion

The Growing Concern and Research Gap

- **Growing Concerns:**

  ➡ Surge in VCS usage globally

  ➡ Increasing reports of security breaches

  ➡ **Privacy issues:** Facial videos, speech audios as biometric data

  ➡ **Behavioural patters:** Absence, movements, chatting behaviour derived from VCS

- **Research Gap:**

  ➡ Current VCS analysis methods are limited

  ➡ Closed-source nature of commercial VCS hinders analysis

  ➡ Need for a method that's reproducible, comparable
  and doesn't compromise privacy

Agenda

I. ~~Introduction to VCS~~

II. ~~The Growing Concern and Research Gap~~

III. Our Contribution and Visualisation

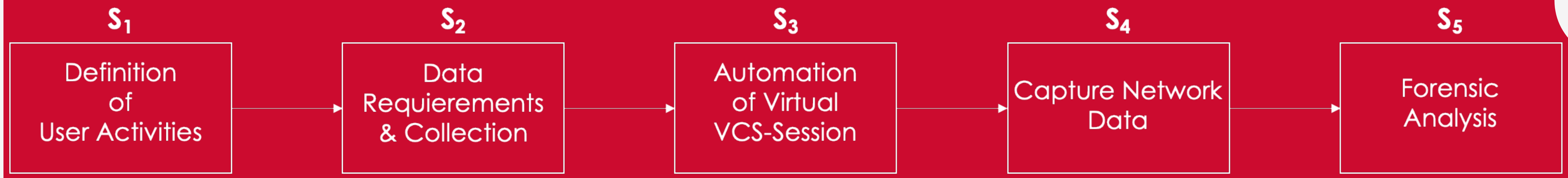
IV. State-of-the-Art in VCS Analysis

V. Detailed steps of our methodology

VI. Early Results

VII. Future work and Conclusion

Our Contribution



S_1 Definition of User Activities

S_2 Data Requierements & Collection

S_3 Automation of Virtual VCS-Session

S_4 Capture Network Data

S_5 Forensic Analysis

- **Contribution:**

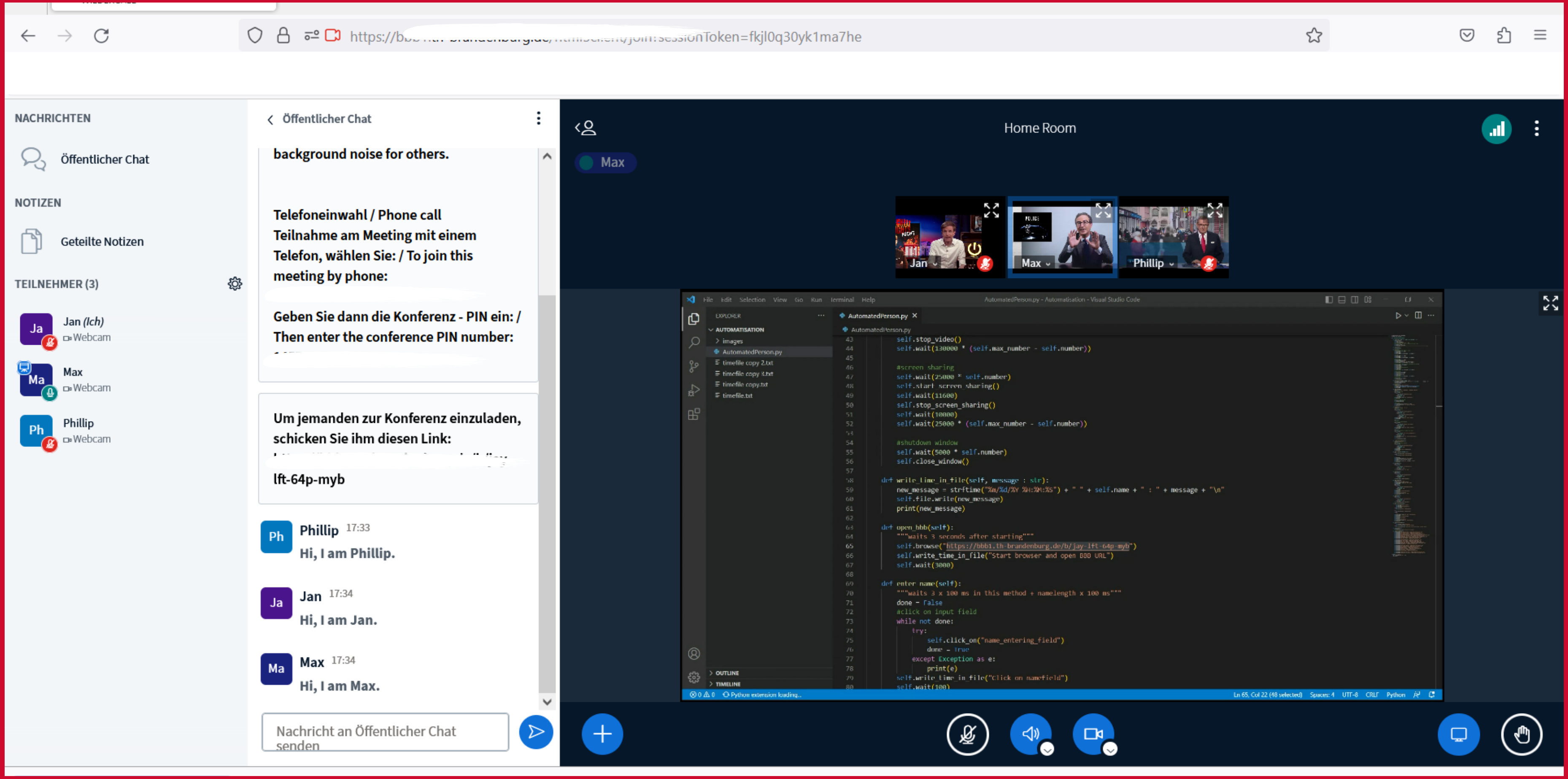
➡ Introduction of a novel, privacy-preserving approach

➡ Use of publicly available videos and scripts for VCS simulation

➡ Ethical testing: No new real biometric data, ensuring user privacy

➡ Five-step process from defining user activities to forensic analysis

Visualisation



https://b[redacted]/join?sessionToken=fkjl0q30yk1ma7he

background noise for others.

Telefoneinwahl / Phone call
Teilnahme am Meeting mit einem Telefon, wählen Sie: / To join this meeting by phone:
[redacted]

Geben Sie dann die Konferenz - PIN ein: / Then enter the conference PIN number:
[redacted]

Um jemanden zur Konferenz einzuladen, schicken Sie ihm diesen Link:
[redacted]
lft-64p-myb

Phillip 17:33
Hi, I am Phillip.

Jan 17:34
Hi, I am Jan.

Max 17:34
Hi, I am Max.

AutomatedPerson.py - Automatisation - Visual Studio Code
AUTOMATISATION
images
AutomatedPerson.py
timefile copy 2.txt
timefile copy 1.txt
timefile copy.txt
timefile.txt
OUTLINE
TIMELINE
Python extension loading...
Ln 65, Col 22 (48 selected) Spaces: 4 UTF-8 CRLF Python

```python
        self.stop_video()
        self.wait(130000 * (self.max_number - self.number))

        #screen sharing
        self.wait(25000 * self.number)
        self.start_screen_sharing()
        self.wait(11600)
        self.stop_screen_sharing()
        self.wait(10000)
        self.wait(25000 * (self.max_number - self.number))

        #shutdown window
        self.wait(5000 * self.number)
        self.close_window()

    def write_time_in_file(self, message : str):
        new_message = strftime("%m/%d/%Y %H:%M:%S") + " " + self.name + " : " + message + "\n"
        self.file.write(new_message)
        print(new_message)

    def open_bbb(self):
        """waits 3 seconds after starting"""
        self.browse("https://bbb1.th-brandenburg.de/b/jay-lft-64p-myb")
        self.write_time_in_file("Start browser and open BBB URL")
        self.wait(3000)

    def enter_name(self):
        """waits 3 x 100 ms in this method + namelength x 100 ms"""
        done = False
        #click on input field
        while not done:
            try:
                self.click_on("name_entering_field")
                done = True
            except Exception as e:
                print(e)
        self.write_time_in_file("Click on namefield")
        self.wait(100)
```

Agenda

I. ~~Introduction to VCS~~

II. ~~The Growing Concern and Research Gap~~

III. ~~Our Contribution and Visualisation~~

IV. State-of-the-Art in VCS Analysis

V. Detailed steps of our methodology

VI. Early Results

VII. Future work and Conclusion

State-of-the-Art in VCS Analysis

- **Historical Focus:**

➡ Predominantly on Skype™: Memory analysis, packet identification, hard drive forensics.

➡**Key Research Areas:**

➡ Memory and traffic analysis

➡ Forensic behaviour on Hard drives

- **Recent Advancements:**

➡ 2021 WebEx & Zoom™ studies: Forensic traceability across devices.

➡ Heuristic analysis of VCS streams, identifying 20 sensitive event [1]

[1] - Altschaffel, R., Hielscher, J., Kiltz, S., & Dittmann, J. (2021, June). Meta and media data stream forensics in the encrypted domain of video conferences. In *Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security* (pp. 23-33).

Agenda

I. ~~Introduction to VCS~~

II. ~~The Growing Concern and Research Gap~~

III. ~~Our Contribution and Visualisation~~

IV. ~~State of the Art in VCS Analysis~~

V. Detailed steps of our methodology

VI. Early Results

VII. Future work and Conclusion

Detailed Steps of our Methodology

- Definition of User Activities
- Data Requirements and Collection of Data
- Automation of Virtual VC-Session
- Capture Network Data from Virtual Session
- Forensic Analysis

Agenda

I. ~~Introduction to VCS~~

II. ~~The Growing Concern and Research Gap~~

III. ~~Our Contribution and Visualisation~~

IV. ~~State of the Art in VCS Analysis~~

V. ~~Detailed steps of our methodology~~

VI. Early Results

VII. Future work and Conclusion

Early Results

- **User Activity Tracking:**

➡ Successfully identified select activities in initial tests.

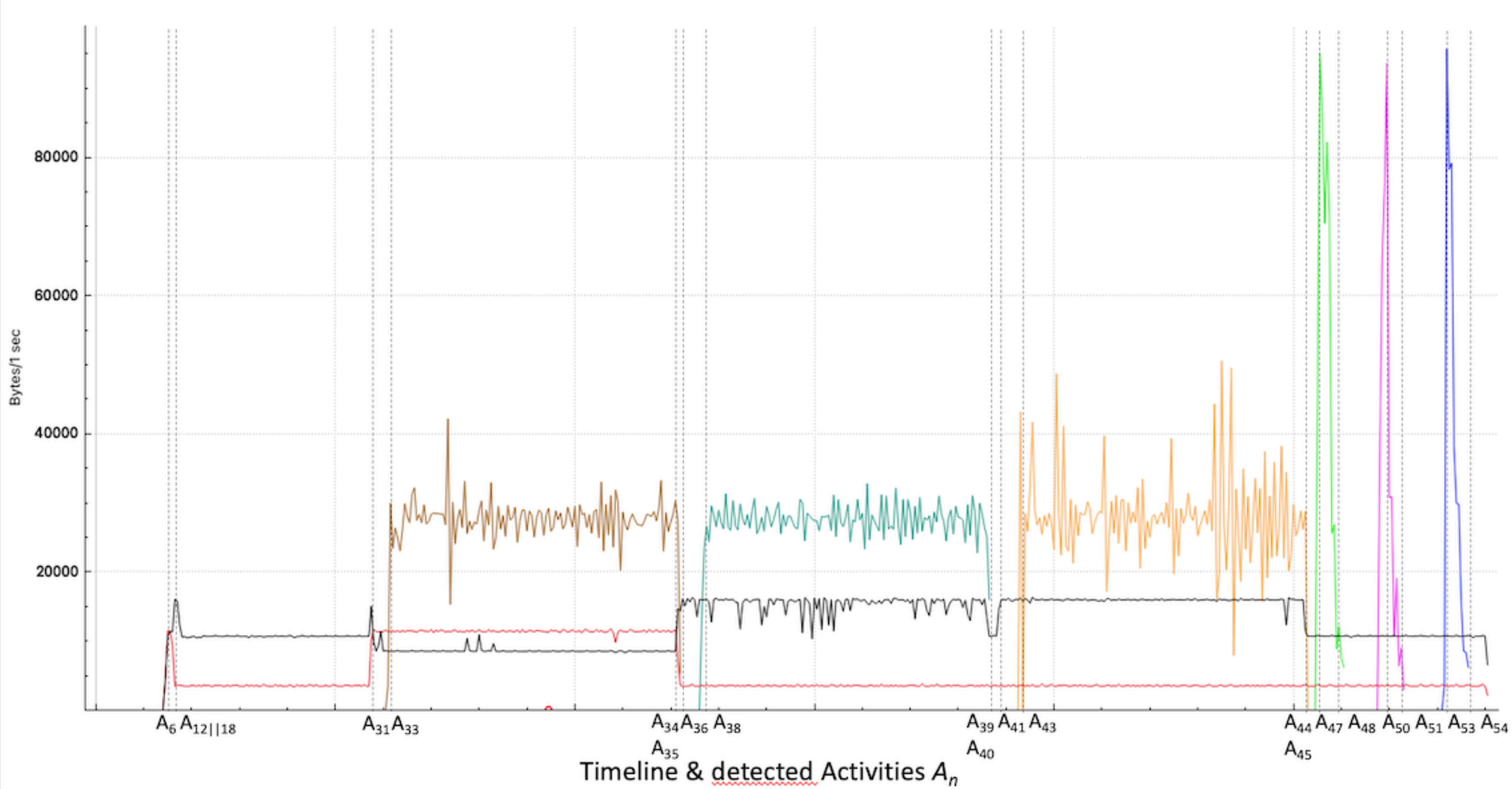
➡ Events captured include webcam on/off, muted/unmuted, and screen sharing

- **Proof-of-Concept Validation:**

➡ Demonstrates potential for reliable and reproducible virtual VC-sessions

➡ Sets the stage for further, in-depth analysis

Early Results



Agenda

I. ~~Introduction to VCS~~

II. ~~The Growing Concern and Research Gap~~

III. ~~Our Contribution and Visualisation~~

IV. ~~State of the Art in VCS Analysis~~

V. ~~Detailed steps of our methodology~~

VI. ~~Summary and Early Results~~

VII. Future work and Conclusion

Future Work and Conclusions

- **Conclusions:**

➡ Introduced privacy-focused VCS analysis methodology.

➡ Validated concept with promising early results.

- **Future Work:**

➡ Integrate machine learning for VCS analysis.

➡ Refine user activity tracking.

➡ Expand virtual VC-session datasets.

THANK YOU!