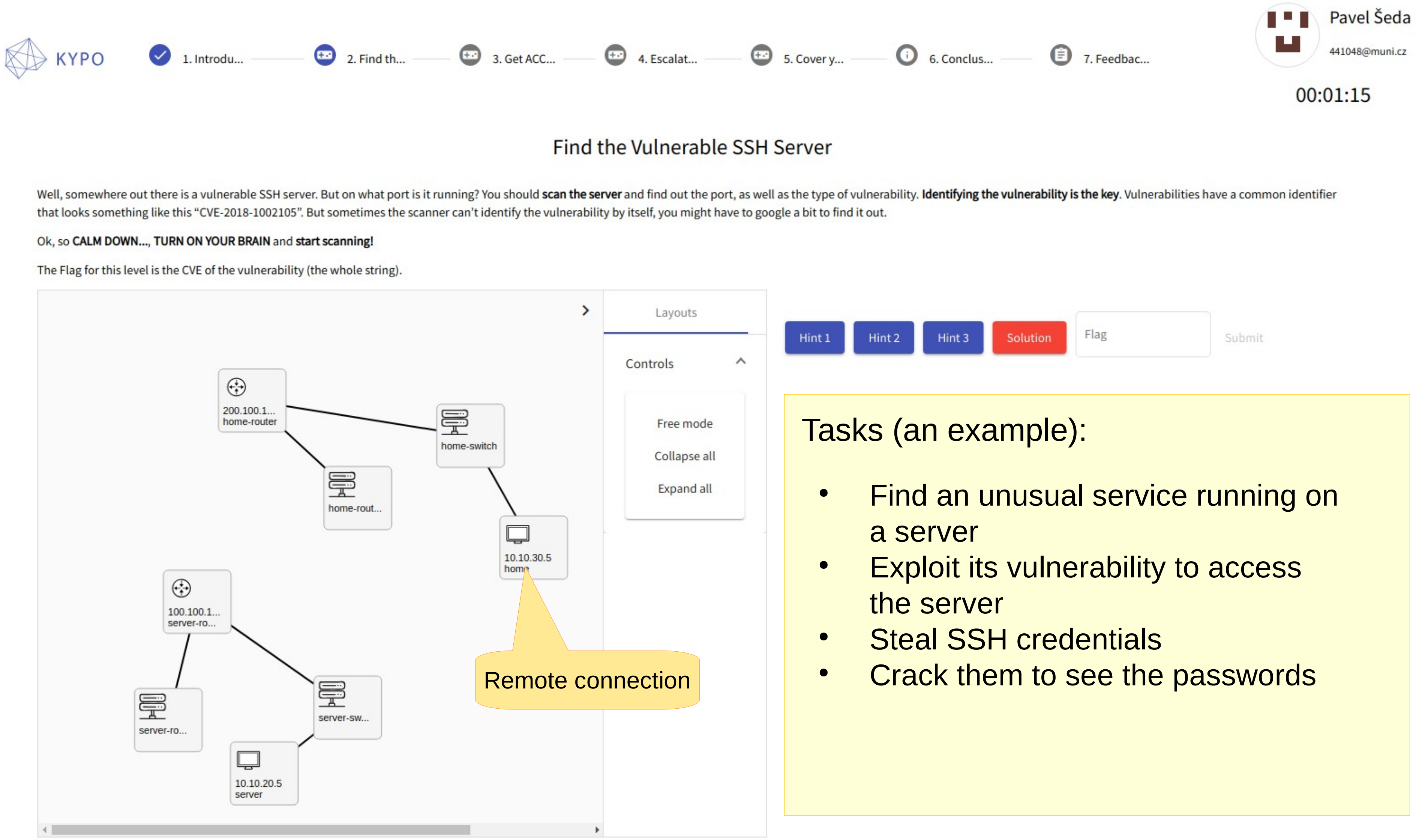
FACULTY
OF INFORMATICS
Masaryk University

Visual Analytics in the KYPO Cyber Range – Principles and Challenges

Radek Ošlejšek

KYPO Cyber Range Platform



Find the Vulnerable SSH Server

Well, somewhere out there is a vulnerable SSH server. But on what port is it running? You should **scan the server** and find out the port, as well as the type of vulnerability. **Identifying the vulnerability is the key**. Vulnerabilities have a common identifier that looks something like this "CVE-2018-1002105". But sometimes the scanner can't identify the vulnerability by itself, you might have to google a bit to find it out.

Ok, so **CALM DOWN..., TURN ON YOUR BRAIN** and **start scanning!**

The Flag for this level is the CVE of the vulnerability (the whole string).

Remote connection

Tasks (an example):

- Find an unusual service running on a server
- Exploit its vulnerability to access the server
- Steal SSH credentials
- Crack them to see the passwords

Problem statement

No tangible output (like a code in programming courses)

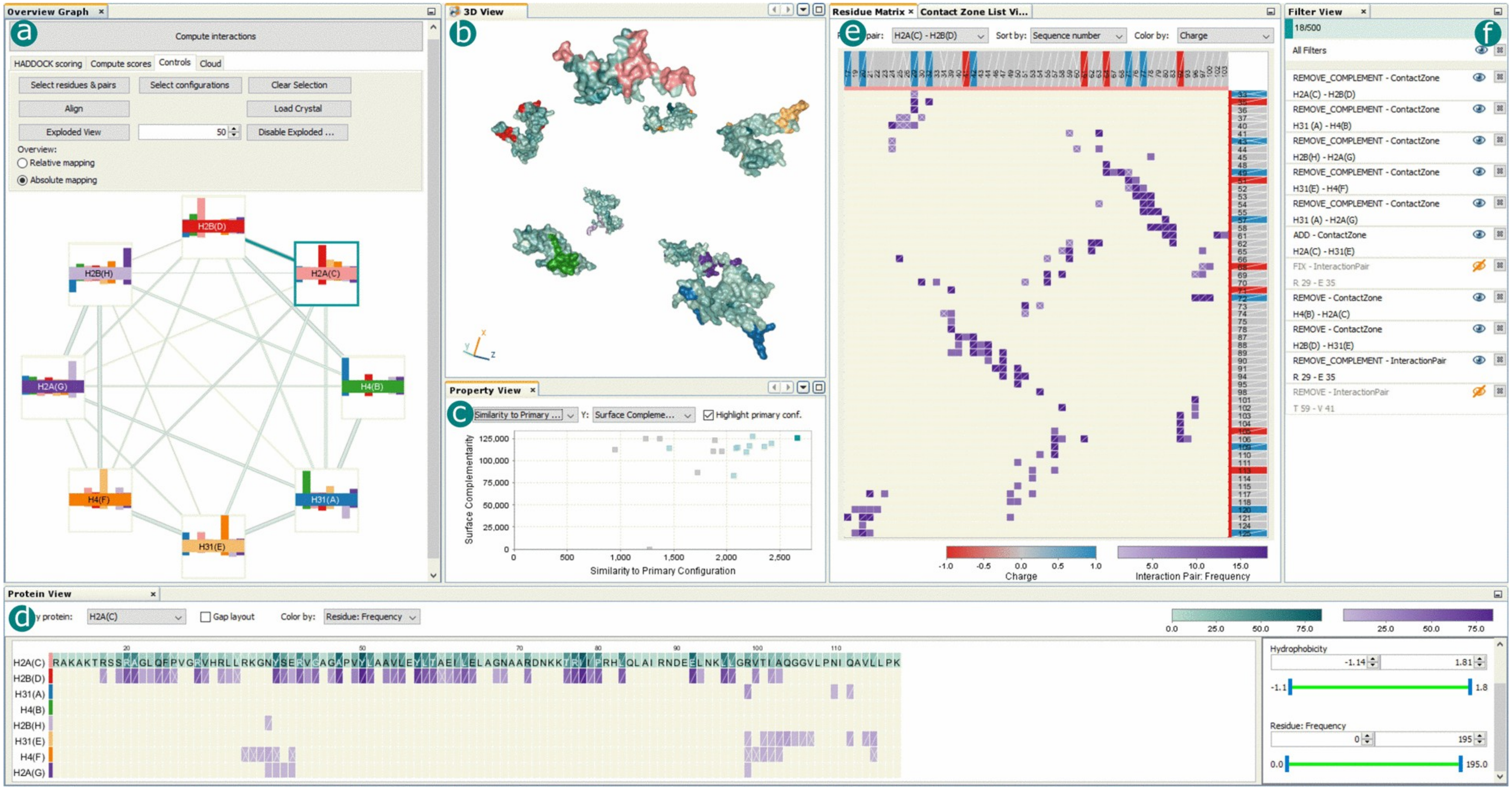
- ***Tutors*** have no idea, what trainees do, whether they are stacked in some task, etc.
- ***Trainees*** don't know whether what they did wrong, or whether there was a faster solution to the tasks.
- ***Training designers*** don't know whether the game was too easy or difficult.

- **Research Goal:** To research and develop data analysis tools providing insight into educational aspects of cybersecurity training and enable comparison, assessment, and continuous improvement.

Avoiding confusion… What is [not] visual analysis

IT IS NOT about the design of GUI, e.g., where to place info window, what color to choose (although these UX aspects are part of any good graphical tool).

IT IS about finding ways to provide insight into complex data and their hidden relationships by means of “smart” interactive visualizations.



50

Overview:
○ Relative mapping
● Absolute mapping

X: Similarity to Primary ... Y: Surface Compleme... ☑ Highlight primary conf.

pair: H2A(C) - H2B(D) Sort by: Sequence number Color by: Charge

18/500

All Filters

REMOVE_COMPLEMENT - ContactZone
H2A(C) - H2B(D)

REMOVE_COMPLEMENT - ContactZone
H31 (A) - H4(B)

REMOVE_COMPLEMENT - ContactZone
H2B(H) - H2A(G)

REMOVE_COMPLEMENT - ContactZone
H31(E) - H4(F)

REMOVE_COMPLEMENT - ContactZone
H31 (A) - H2A(G)

ADD - ContactZone
H2A(C) - H31(E)

FIX - InteractionPair
R 29 - E 35

REMOVE - ContactZone
H4(B) - H2A(C)

REMOVE - ContactZone
H2B(D) - H31(E)

REMOVE_COMPLEMENT - InteractionPair
R 29 - E 35

REMOVE - InteractionPair
T 59 - V 41

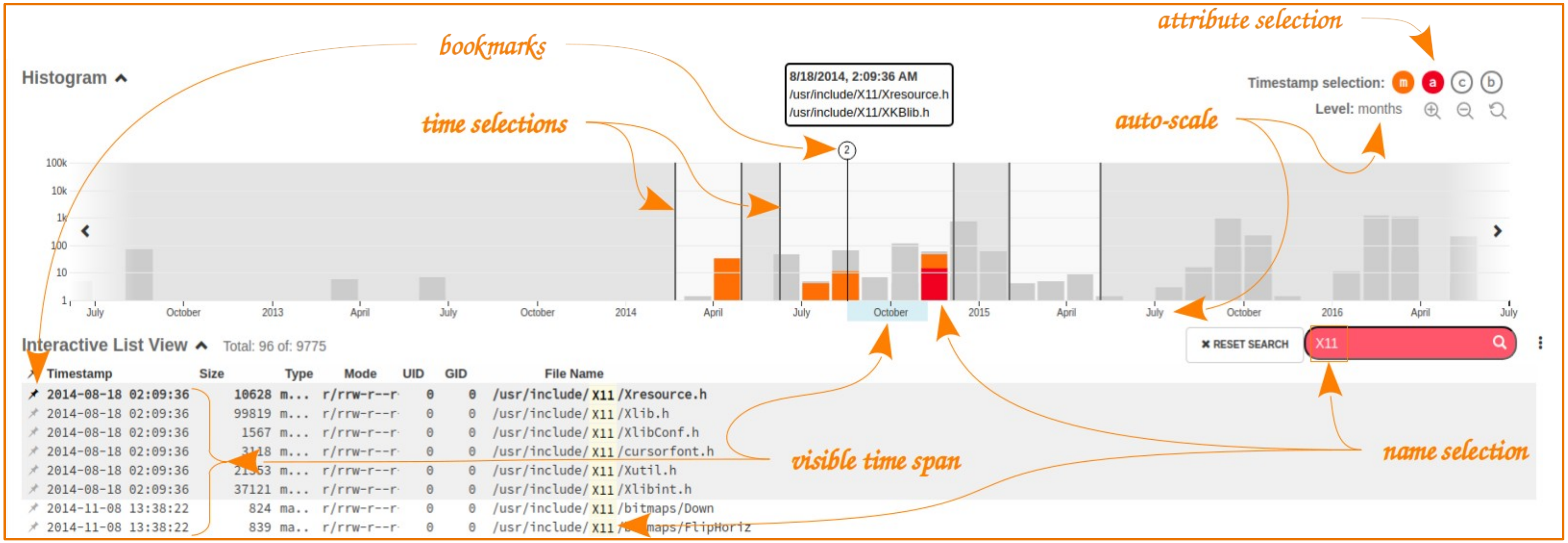
y protein: H2A(C) □ Gap layout Color by: Residue: Frequency

Hydrophobicity -1.14 1.81

Residue: Frequency 0 195

[Furmanová, K., et al. "Multiscale Visual Drilldown for the Analysis of Large Ensembles of Multi-Body Protein Complexes.", TVCG, 2019]

VA examples: Forensic investigation



Interactive List View ^ Total: 96 of: 9775

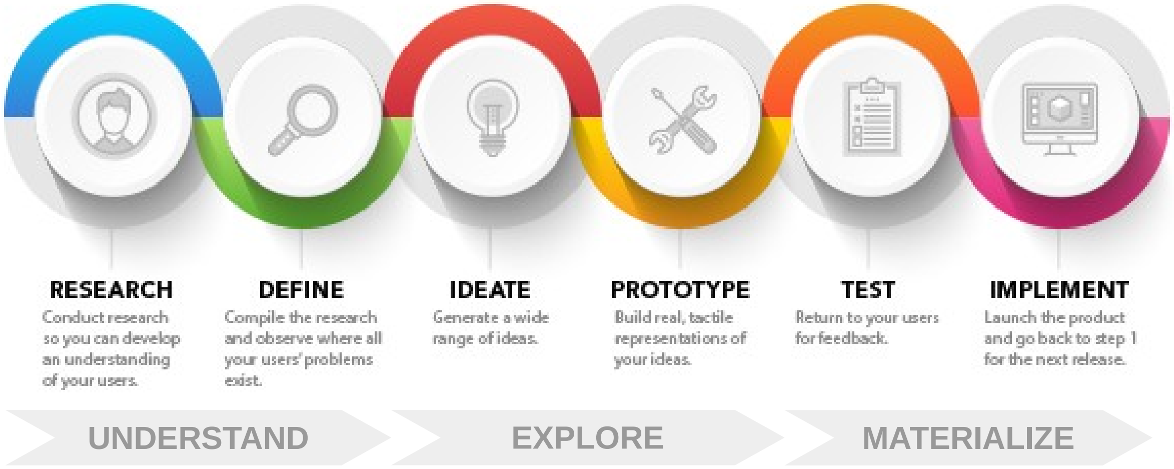
	Timestamp	Size	Type	Mode	UID	GID	File Name
2014-08-18 02:09:36	**10628**	**m...**	**r/rrw-r--r**	**0**	**0**	**/usr/include/X11/Xresource.h**
2014-08-18 02:09:36	99819	m...	r/rrw-r--r	0	0	/usr/include/X11/Xlib.h
2014-08-18 02:09:36	1567	m...	r/rrw-r--r	0	0	/usr/include/X11/XlibConf.h
2014-08-18 02:09:36	3118	m...	r/rrw-r--r	0	0	/usr/include/X11/cursorfont.h
2014-08-18 02:09:36	21553	m...	r/rrw-r--r	0	0	/usr/include/X11/Xutil.h
2014-08-18 02:09:36	37121	m...	r/rrw-r--r	0	0	/usr/include/X11/Xlibint.h
2014-11-08 13:38:22	824	ma..	r/rrw-r--r	0	0	/usr/include/X11/bitmaps/Down
2014-11-08 13:38:22	839	ma..	r/rrw-r--r	0	0	/usr/include/X11/bitmaps/FlipHoriz

FIMETIS – A tool for forensic investigation of disk images

BERAN, Martin, František HRDINA, Dan KOUŘIL, Radek OŠLEJŠEK, Kristína ZÁKOPČANOVÁ. **Exploratory Analysis of File System Metadata for Rapid Investigation of Security Incidents.** In *IEEE Symposium on Visualization for Cyber Security (VizSec'20).*

VA methodology

- The development of a really useful VA tool is challenging. It is necessary to follow many rules and best practices to achieve good results and to prove usability
  - Tight cooperation with *domain experts* for both requirements analysis and usability evaluation
  - Using iterative design methodologies, e.g., *user-centered design* (it isn’t an ad-hoc process)
  - Formal *evaluation* of results, e.g., quantitative and qualitative methods of measuring user experience
- The development process can be considered a special discipline of software engineering



RESEARCH
Conduct research so you can develop an understanding of your users.

DEFINE
Compile the research and observe where all your users' problems exist.

IDEATE
Generate a wide range of ideas.

PROTOTYPE
Build real, tactile representations of your ideas.

TEST
Return to your users for feedback.

IMPLEMENT
Launch the product and go back to step 1 for the next release.

UNDERSTAND
EXPLORE
MATERIALIZE

VA high-level concepts

- Regardless of the methodology and application domain, it is always necessary to
  - clarify *users roles*, actors, personas in given application domain;
  - identify their *analytical goals* and *data processes*;
  - propose *visualization techniques* that *reflect available data* and address analytical goals of user roles.

VA for Hands-on Cybersecurity Training

visual situational awareness

insight of trainees V_1

- trainee — awareness of the state of network environment V_{1A}
- trainee — awareness of cybersecurity posture V_{1B}

insight of organizing participants V_2

- sparring partner — training progression V_{2A}
- supervisor — training management V_{2B}
- operator — infrastructure management V_{2C}

visual data analytics

personal feedback V_3

- trainee — personal reflections on trainees V_{3A}
- supervisor — impact of supervision V_{3B}

quality of training exercise V_4

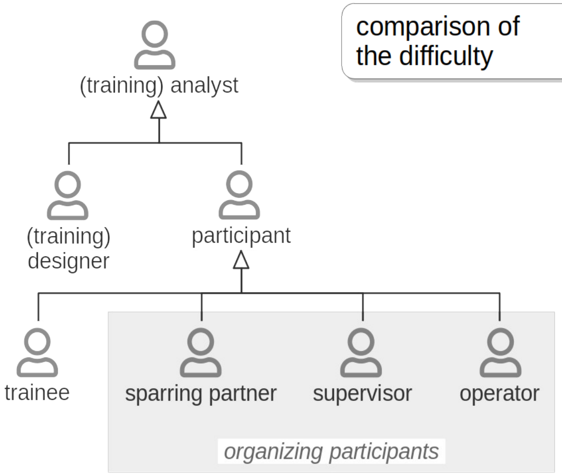
- designer — correctness of a training definition V_{4A}
- designer — difficulty of a training definition V_{4B}
- designer — comparison of the difficulty V_{4C}

behavior analysis V_5

- analyst — successful strategies V_{5A}
- analyst — cooperation patterns V_{5B}

infrastructure analysis V_6

- operator & designer — performance analysis V_{6A}
- operator & designer — reliability analysis V_{6B}



OŠLEJŠEK, Radek, Vít RUSŇÁK, Karolína DOČKALOVÁ BURSKÁ, Valdemar ŠVÁBENSKÝ, Jan VYKOPAL and Jakub ČEGAN. **Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training.** In *IEEE Transactions on Visualization and Computer Graphics*, 2021.

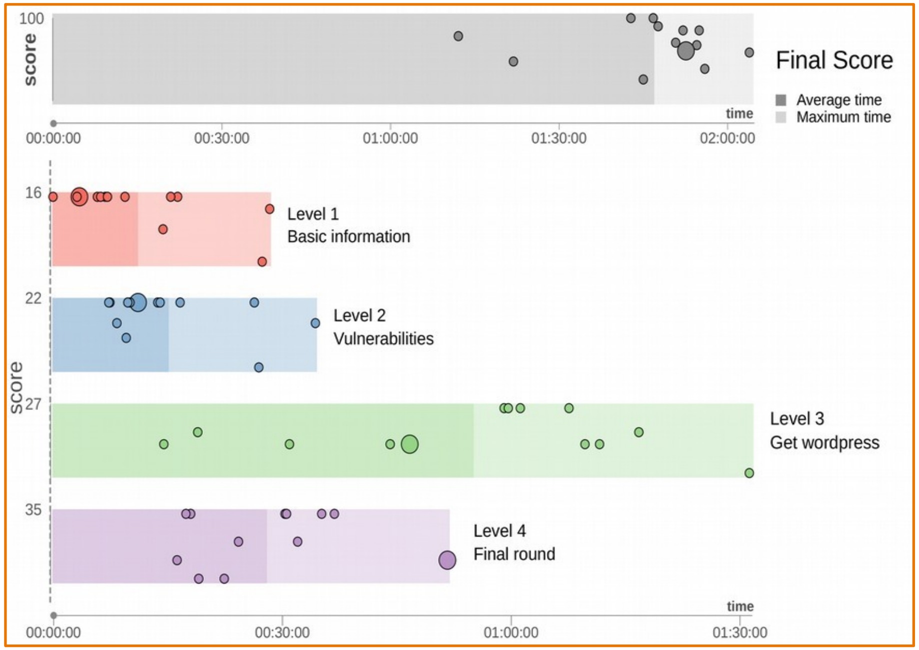
FACULTY OF INFORMATICS
Masaryk University

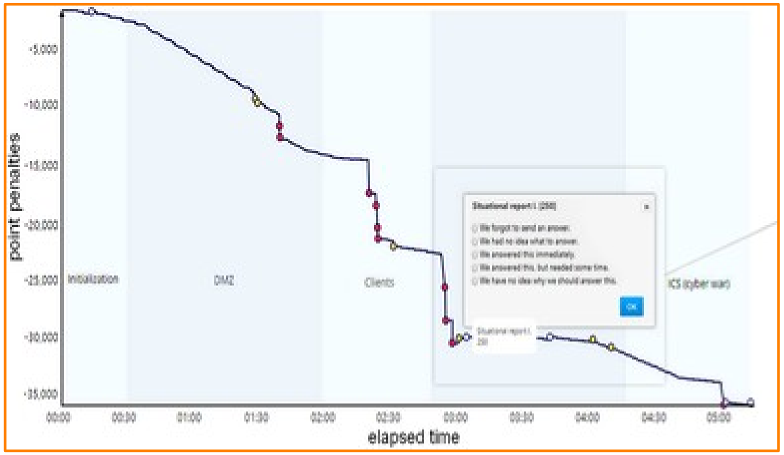
Personalized feedback to trainees

Goal: Learning from own mistakes

- What did I do wrong in selected tasks?
- Where I lost most points and why?
- ...

OŠLEJŠEK, Radek, Vít RUSŇÁK, Karolína BURSKÁ, Valdemar ŠVÁBENSKÝ a Jan VYKOPAL. **Visual Feedback for Players of Multi-Level Capture the Flag Games: Field Usability Study.** In *IEEE Symposium on Visualization for Cyber Security (VizSec'19)*





Situational report I (250)

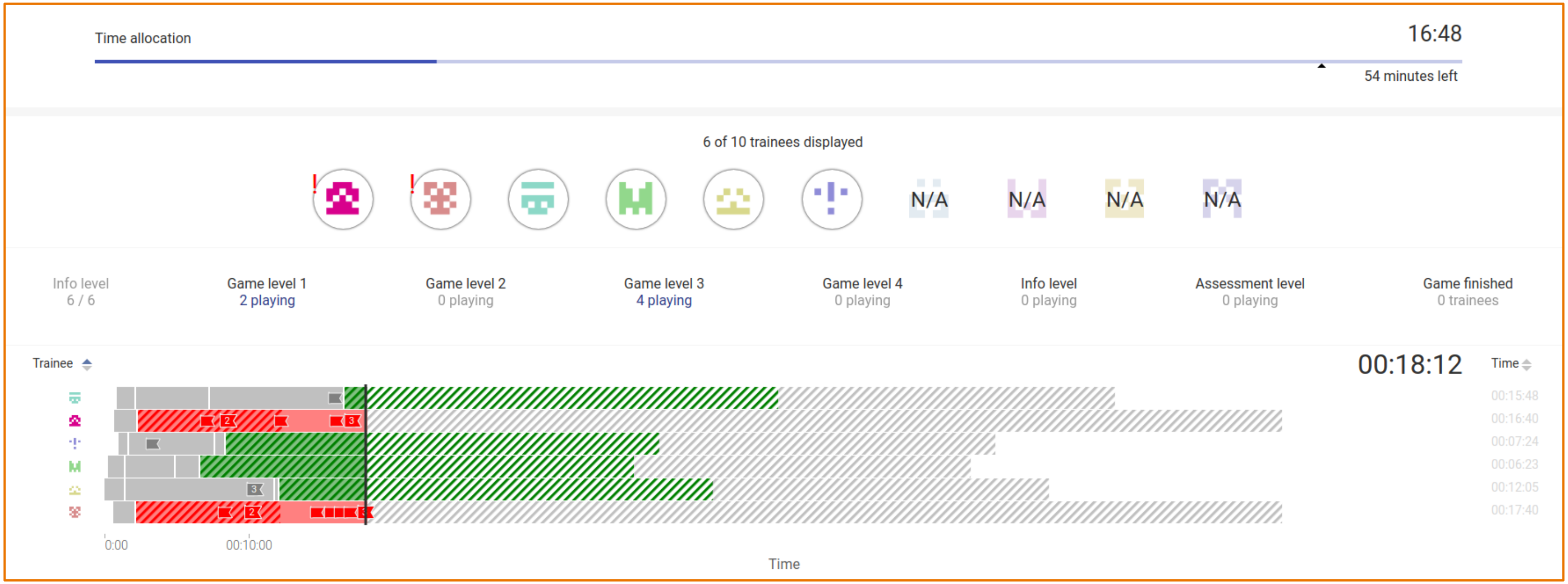
○ We forgot to send an answer.
○ We had no idea what to answer.
○ We answered this immediately.
○ We answered this, but needed some time.
○ We have no idea why we should answer this.

VYKOPAL, Jan, Radek OŠLEJŠEK, Karolína BURSKÁ and Kristína ZÁKOPČANOVÁ. **Timely Feedback in Unstructured Cybersecurity Exercises.** In *ACM Technical Symposium on Computer Science Education (SIGCSE'18)*

Insight for organizing participants

Goal: Situational awareness and timely intervention

- Which trainees are in trouble? Why?
- Is the training session on schedule, or is there some delay?
- ...

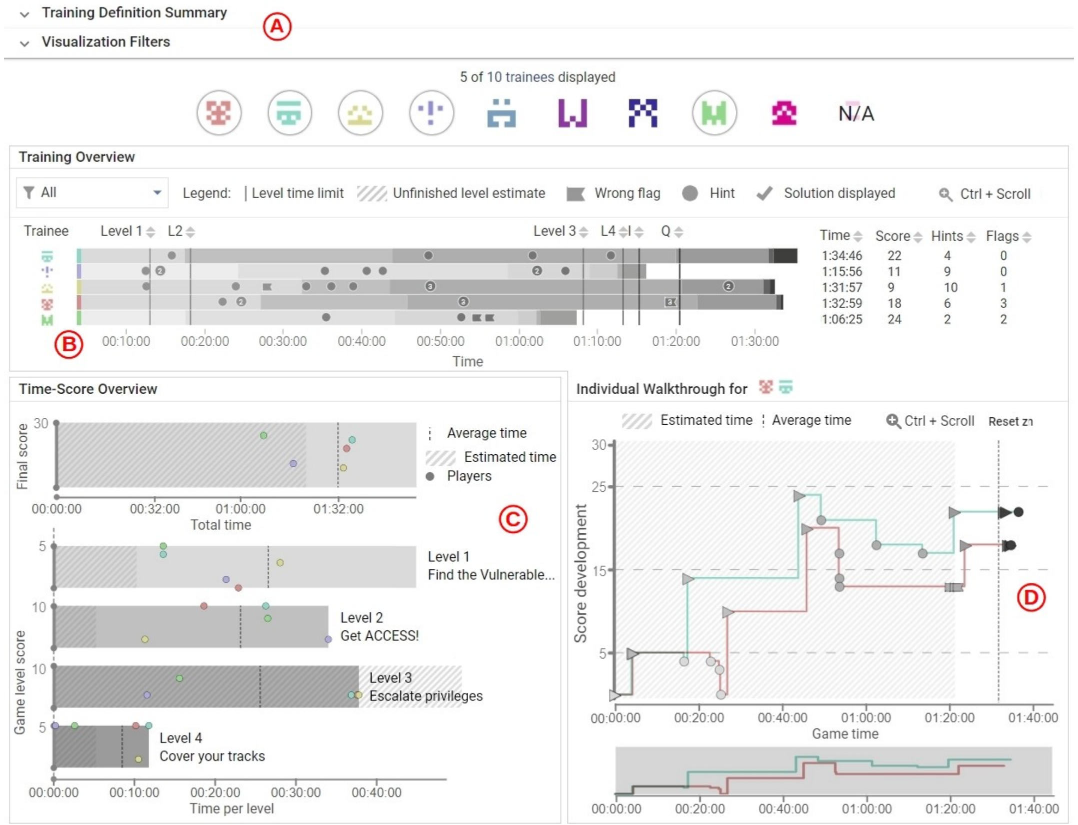


DOČKALOVÁ BURSKÁ Karolína, Vít RUSŇÁK and Radek OŠLEJŠEK.
Enhancing Situational Awareness for Tutors of Cybersecurity Capture the Flag Games.
In *International Conference Information Visualization (iV'21)*.

Post-training analysis

Goal: Improve the impact of learning

- Was training too easy or difficult?
- What are the sources of losing motivation and giving up the training?
- Are there some flows in the scenario, requirements, etc.?
- ...

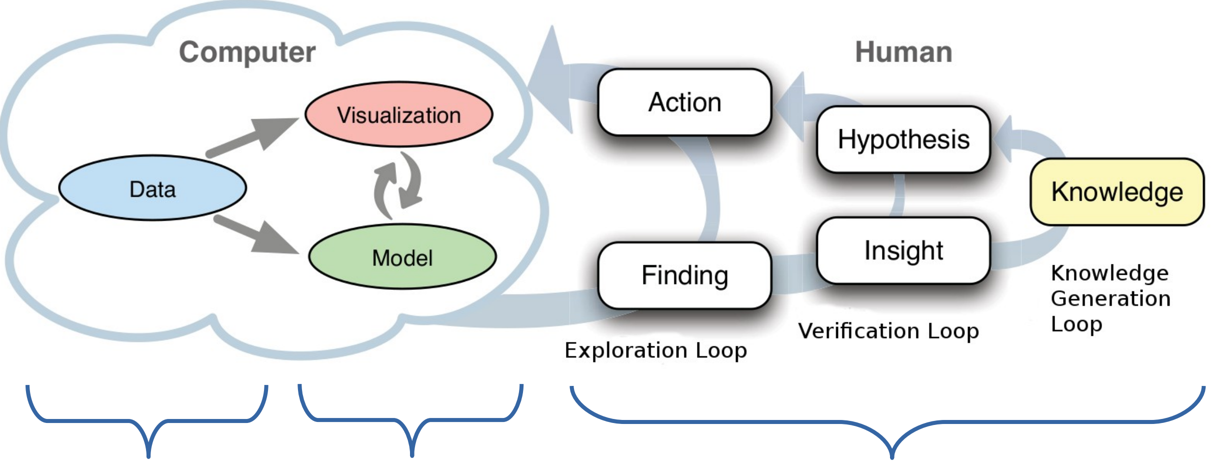


Time	Score	Hints	Flags
1:34:46	22	4	0
1:15:56	11	9	0
1:31:57	9	10	1
1:32:59	18	6	3
1:06:25	24	2	2

DOČKALOVÁ BURSKÁ Karolína, Vít RUSŇÁK and Radek OŠLEJŠEK.
Data-driven insight into the puzzle-based cybersecurity training.
In *Computers & Graphics*, 2021.

Bottom-up approach to VA

- Our recent approach to VA reflects a standard domain-specific paradigm
- Game data and events
  - Estimated time of tasks
  - Start/end of the exercise
  - Submission of a correct flag, i.e., successful solution of a task
  - Submission of an incorrect flag, i.e., wrong attempts to solve the task
  - Taking a hint
- Assessment data
- Bash history



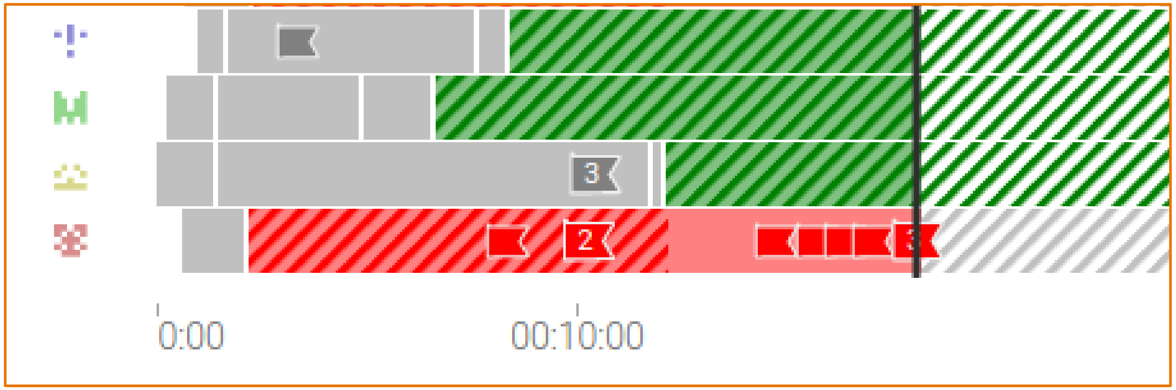
domain-specific data

visualizations

analytical goals

Tailored domain-specific approach

- Precise support of users and their analytical requirements
- The introduction of new data types usually requires adaptation or extension of existing visualizations
- Application to other learning domains that follow puzzle-based gamification principles is also limited
  - Puzzles are used as a metaphor for getting students to think about how to frame and solve unstructured problems.
  - Division of learning tasks into smaller connected parts (puzzles)

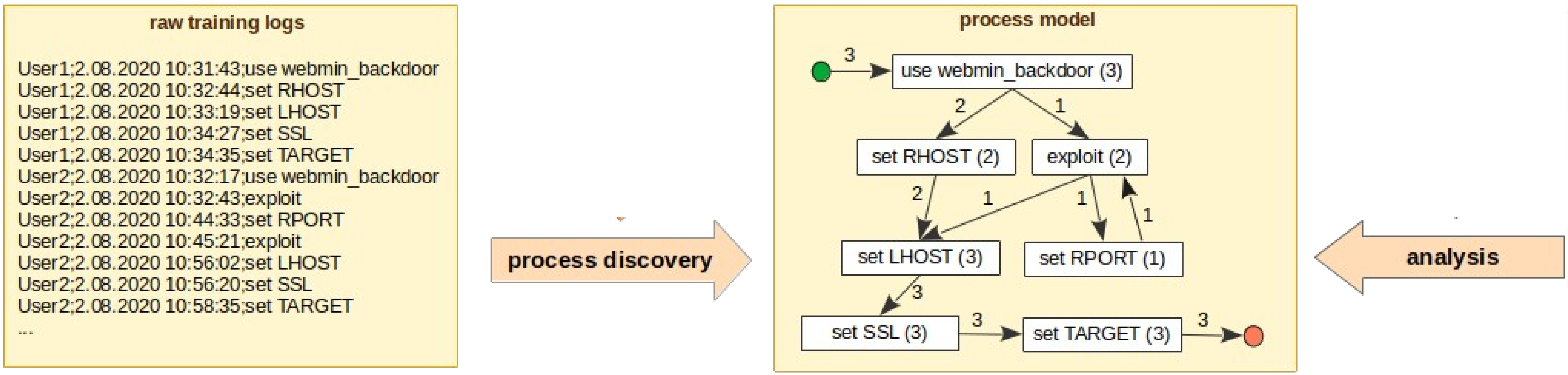


Tailored vs. unified approach to design VA

Is there some more general conceptual approach
to design exploratory visualizations
for cybersecurity exercises?

Process mining

- Cybersecurity learning is **process-oriented**
- There exist a **process mining** research area
  - A bridge between traditional data analysis techniques, like data mining, and business process management analysis
  - Provides algorithms that take event logs as input and produces process graphs reconstructed from the logs (it is called process discovery)
  - Process graphs provide better cognitive features than row event logs and then simplify comprehension

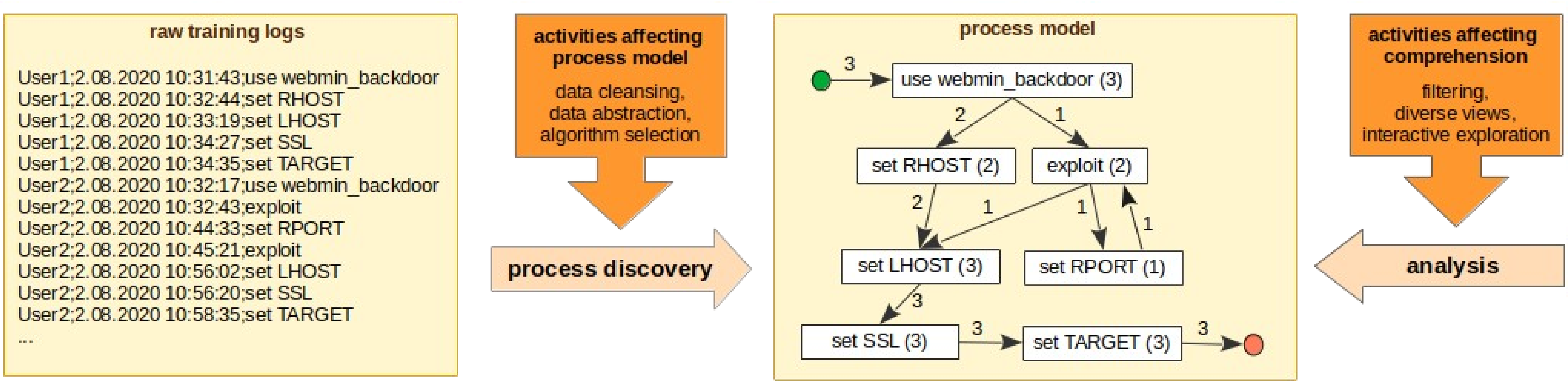


raw training logs

```
User1;2.08.2020 10:31:43;use webmin_backdoor
User1;2.08.2020 10:32:44;set RHOST
User1;2.08.2020 10:33:19;set LHOST
User1;2.08.2020 10:34:27;set SSL
User1;2.08.2020 10:34:35;set TARGET
User2;2.08.2020 10:32:17;use webmin_backdoor
User2;2.08.2020 10:32:43;exploit
User2;2.08.2020 10:44:33;set RPORT
User2;2.08.2020 10:45:21;exploit
User2;2.08.2020 10:56:02;set LHOST
User2;2.08.2020 10:56:20;set SSL
User2;2.08.2020 10:58:35;set TARGET
...
```

Process mining for cybersecurity training

- The idea of using process graphs is not new, even in the subdomain of cybersecurity training
  - Weiss, R. et al.: A reflective approach to assessing student performance in cybersecurity exercises. ACM SIGCSE’16
  - Mirkovic, J. et al.: Using terminal histories to monitor student progress on hands-on exercises. ACM SIGCSE’20
- But they utilize tailored process graphs (i.e., domain-specific approach) while omitting generic process mining approaches
- Using process mining approaches brings many open problems
  - Data pre-processing and mapping affect obtained graphs
  - The selection of process discovery algorithm affects obtained graphs
  - Problem with the scalability of obtained graphs



raw training logs

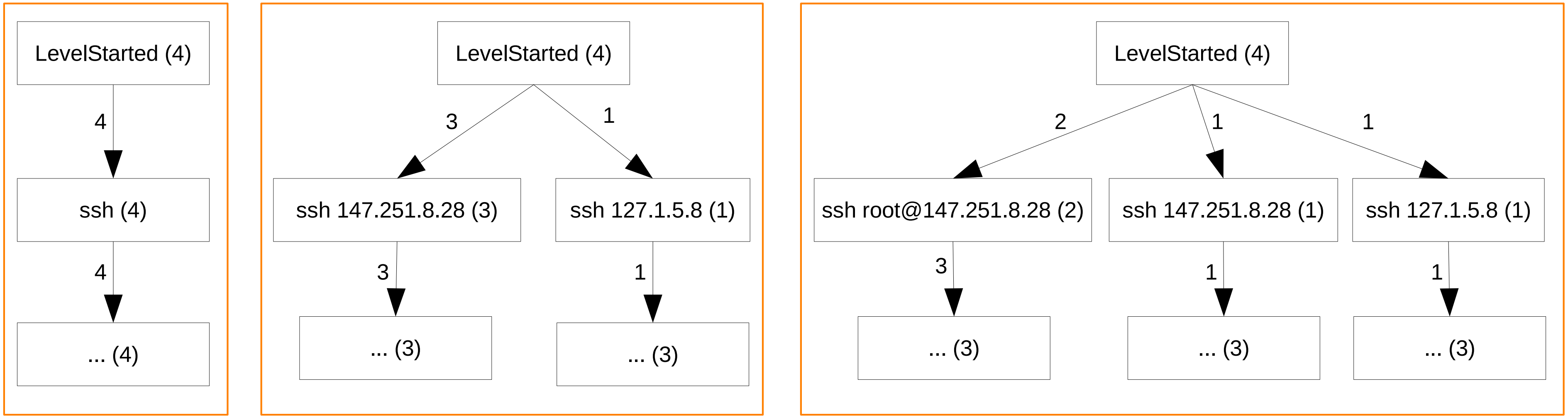
```
User1;2.08.2020 10:31:43;use webmin_backdoor
User1;2.08.2020 10:32:44;set RHOST
User1;2.08.2020 10:33:19;set LHOST
User1;2.08.2020 10:34:27;set SSL
User1;2.08.2020 10:34:35;set TARGET
User2;2.08.2020 10:32:17;use webmin_backdoor
User2;2.08.2020 10:32:43;exploit
User2;2.08.2020 10:44:33;set RPORT
User2;2.08.2020 10:45:21;exploit
User2;2.08.2020 10:56:02;set LHOST
User2;2.08.2020 10:56:20;set SSL
User2;2.08.2020 10:58:35;set TARGET
...
```

Open problems – current research

- Tackling comprehensibility:
  - We defined necessary pre-processing tasks and formulated data abstraction that enables us to get reasonable process graphs from cybersecurity exercises
  - We conducted initial experiments that proved its usability for learning analytics. However, a more robust evaluation with more participants is necessary.
- Tackling scalability:
  - Data aggregation and filtering at the input side of the process mining algorithms
  - Structural properties of puzzle-based games
  - Providing complementary views to process graphs

Data aggregation and filtering

- What is the same or sufficiently similar commands?
  - User 1: `ssh root@147.251.8.28`
  - User 2: `ssh 147.251.8.28`
  - User 3: `ssh -4 root@147.251.8.28`
  - User 4: `ssh 127.1.5.8`

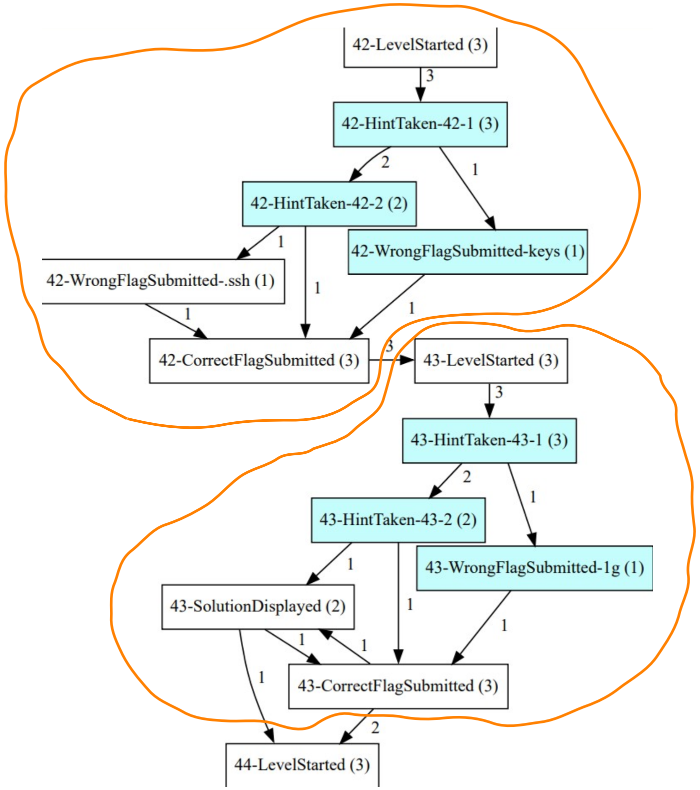


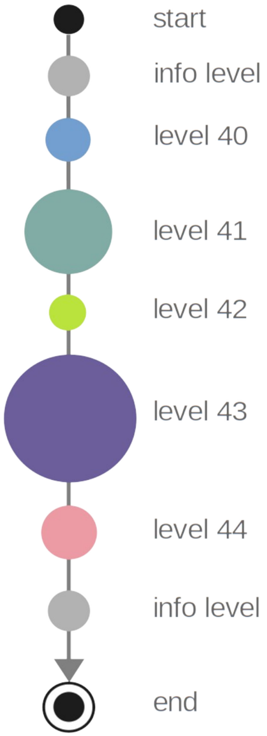
Structural properties of puzzle-based games

- High cohesion inside puzzles (tasks)
- Low decoupling between puzzles (tasks)

"Weakly connected islands of complexity"

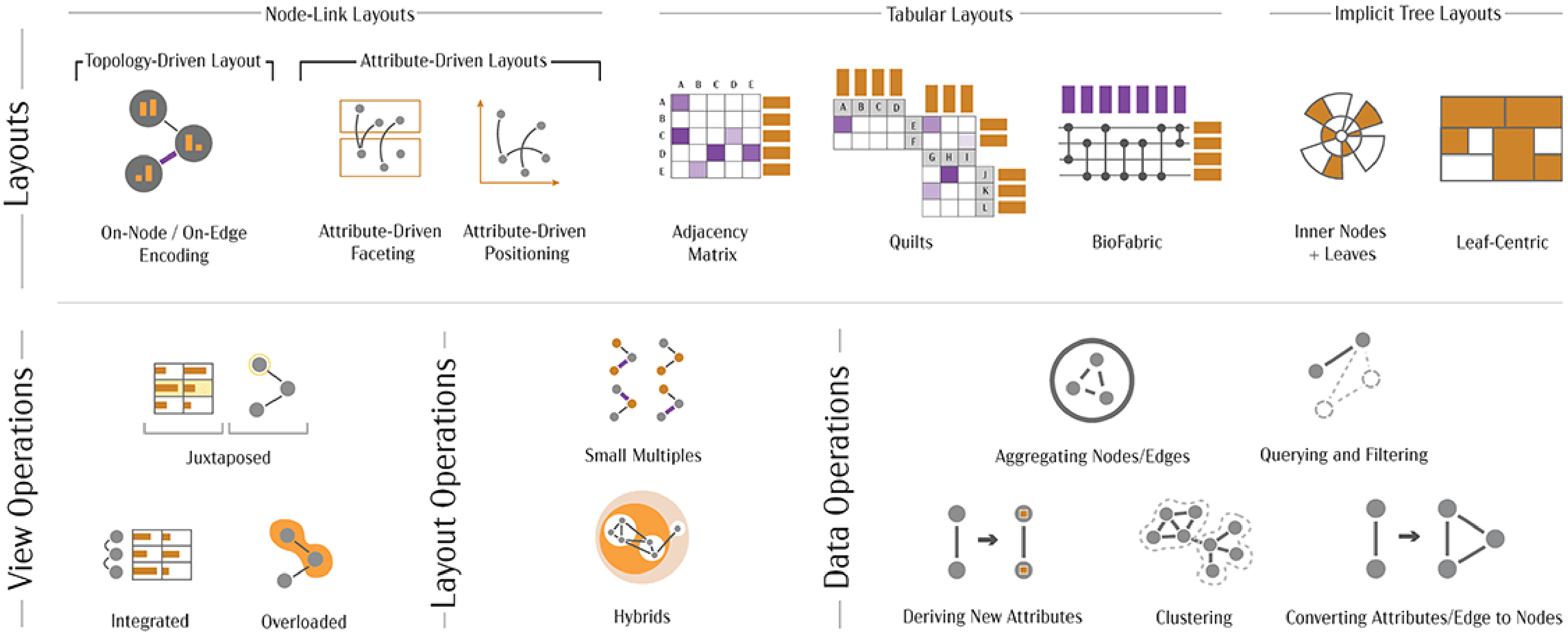
- Schneiderman's visual information-seeking mantra: Overview first, zoom and filter, then details-on-demand



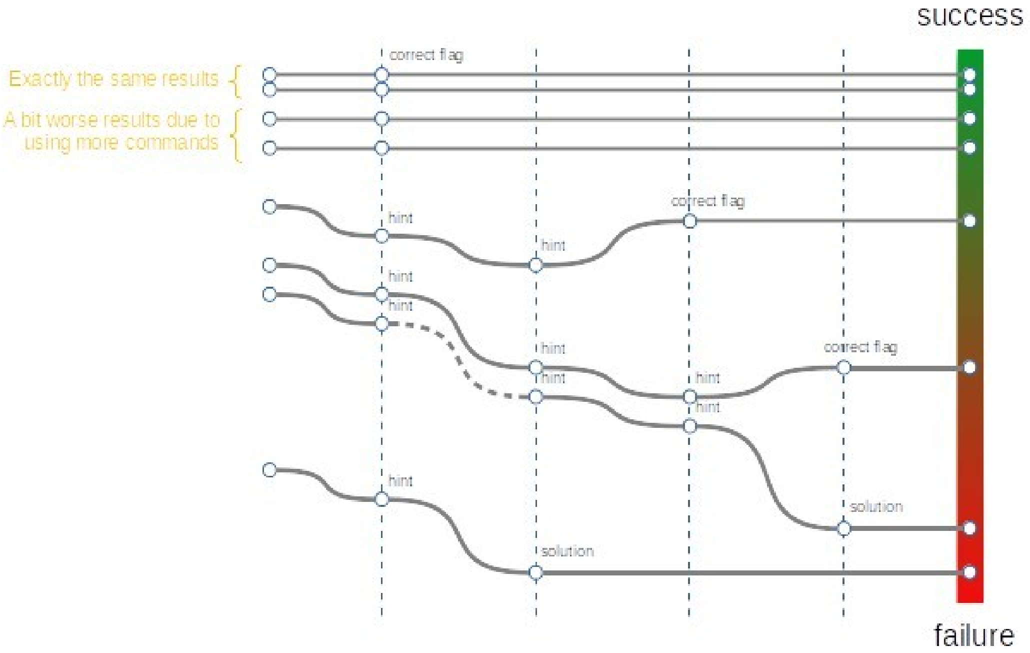


Complementary views to process graphs

- Idea: Provide alternate view to a traditional graph representation
- From the VA perspective, process graphs are so-called multivariate networks
  - Nobre, C. et al. The state of the art in visualizing multivariate networks. In Computer Graphics Forum, Vol. 38, No. 3. 2019
- But still, the design of a concrete tool is challenging



Infrastructure analysis



Highlight possible flows:

- □ Unclear task description
  - *Taking hint immediately (without trying any command)*
- □ The loss of motivation to finish the task or the lack of time
  - *Taking hints or solution without trying any command*
- □ Useful hints, but possibly too much instructive
  - *Taking a hint is followed by the correct flag*
- □ Useless hints
  - *Taking a hint is followed by taking another hint, solution, or incorrect flag*

Thank you for your attention!