

Bringing the Science of Cybersecurity out of the Dark Ages

Jiska Classen, April 4th 2024

The Dark Ages

Ignorance and Error



H		
Li	Be	
Na	Mg	
K	Ca	Sc

Age of Enlightenment

Knowledge and Understanding

Where are we in
Cybersecurity?



The Philosopher's Stone



The Philosopher's Stone



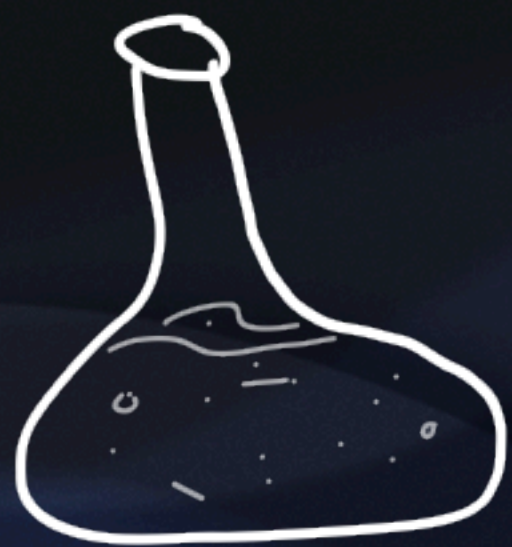
Unhackable Systems



Court Alchemists



Vendor Appliances &
Solutions



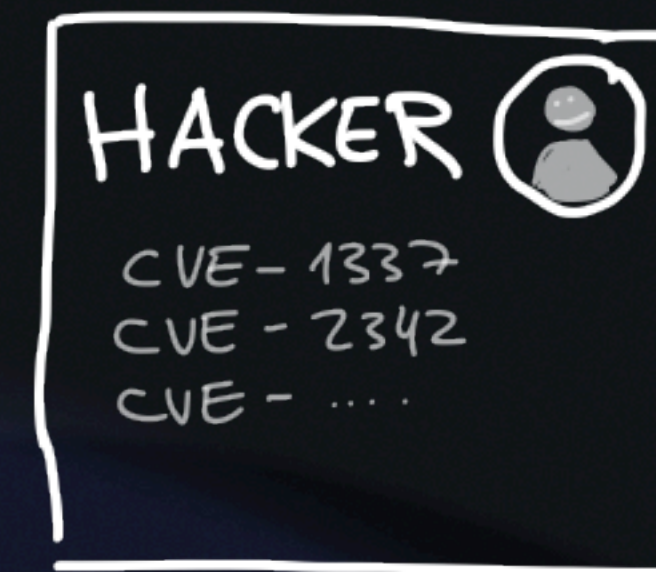
Cooking Recipes



Pentesting Guides



Metals → Gold



Software → CVEs

Current State in Cybersecurity

Cyber attacks happen on
a regular basis.

Skyrocketing numbers: product sales,
job market, academic papers, ...

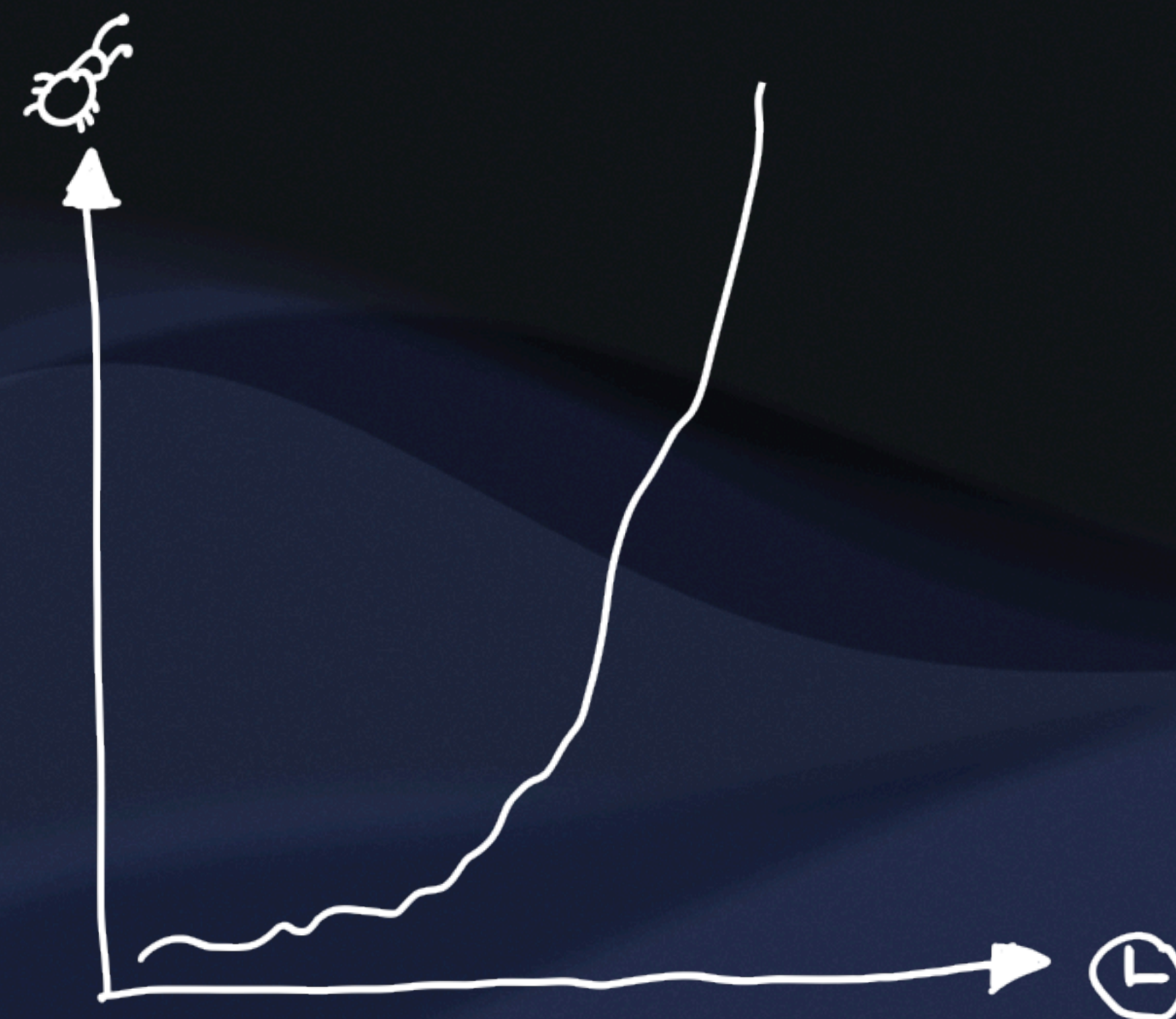
Security researchers report
many bugs.

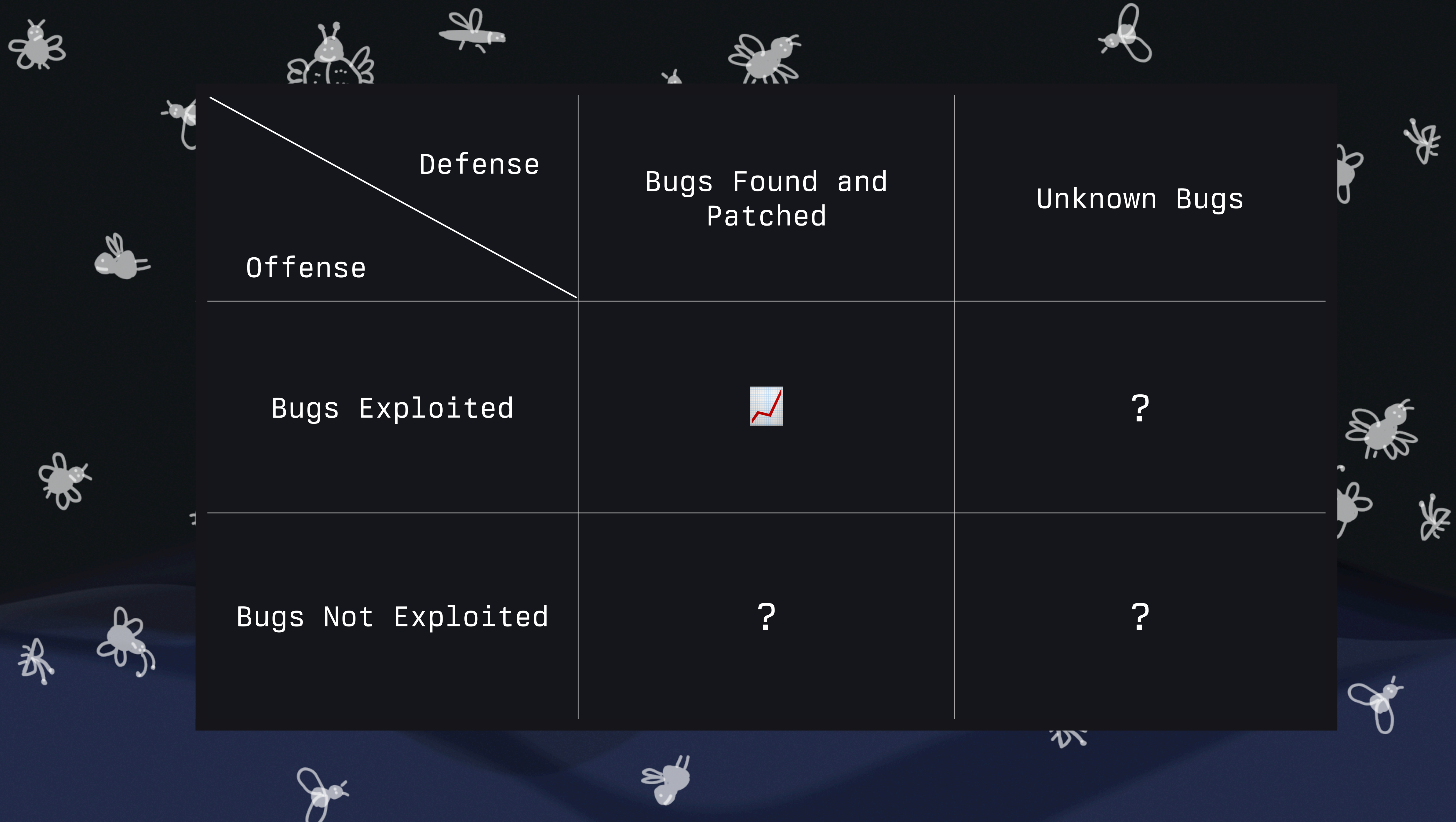


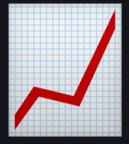
The industry got faster with
applying patches.

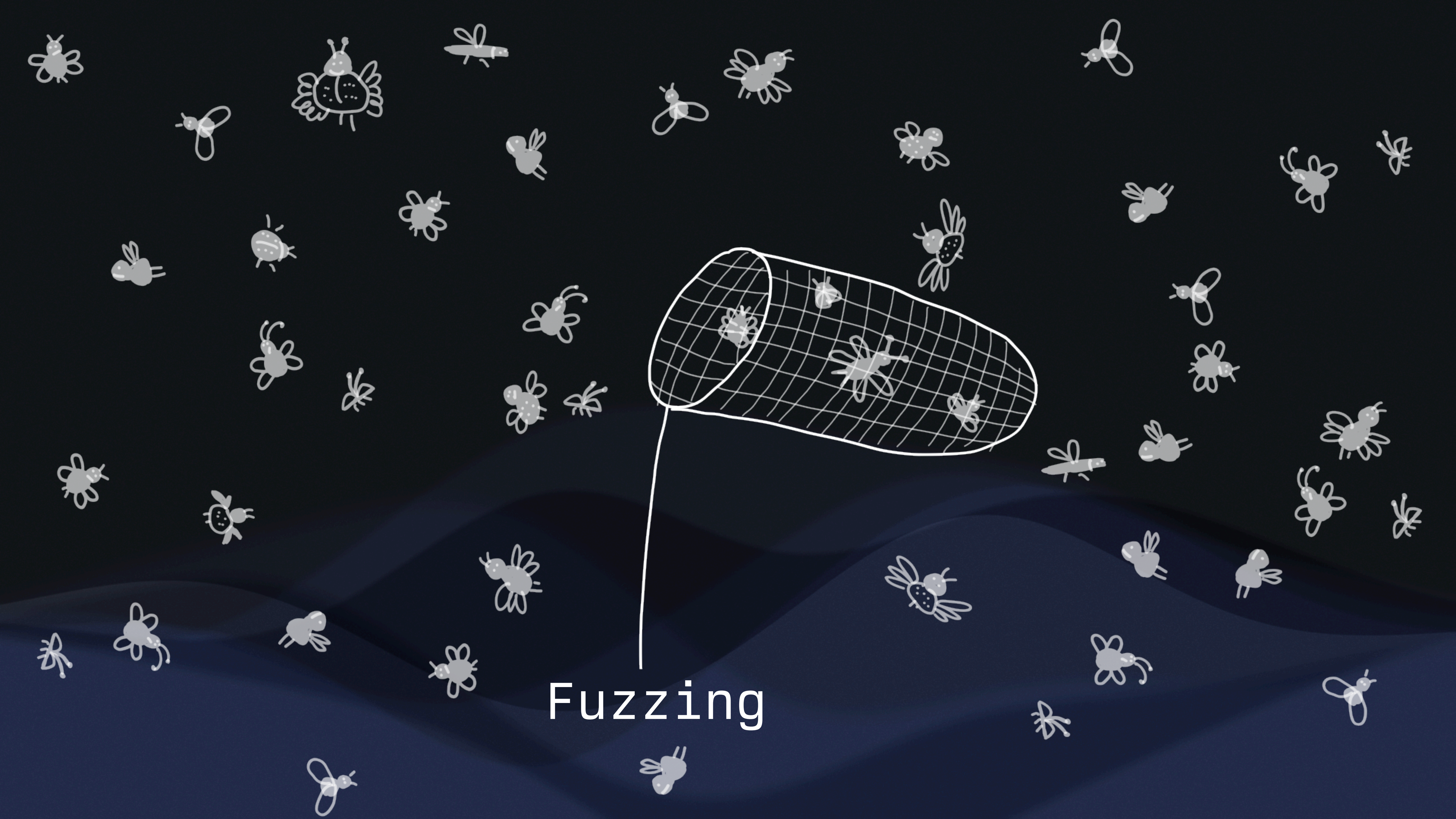


Uncovering bugs became a de facto quality measure.





<p>Defense</p> <p>Offense</p>	<p>Bugs Found and Patched</p>	<p>Unknown Bugs</p>
<p>Bugs Exploited</p>	<p></p>	<p>?</p>
<p>Bugs Not Exploited</p>	<p>?</p>	<p>?</p>



Fuzzing

Cyber attacks keep happening!

We find more bugs, faster.

Does this improve security?

Build & Break

- Repeating pattern of building new security mechanisms and then breaking them.
- We will never accidentally make gold or fix cybersecurity this way!



How can we make a science
out of cybersecurity?

Science is Built on Understanding

- We understand things by grouping them together and finding patterns.
- With understanding, science can make verifiable statements and predictions.
- We are not there yet with cybersecurity!



Finding Useful Abstractions

- Abstractions can help getting away from the pattern of finding and fixing single bugs.
- Some levels of abstraction are more useful than others.
- What is the understanding that we can get from a specific level of abstraction?

Generalizing Mitigations

- An abstraction is useful if it allows us to reason about a mitigation.
- Design systems to be more resistant.



Exploit Chain Complexity

- Exploit chains become more complex in practice.
- Trend towards teams working on this, rather than single persons.
- This shows some success in creating more generalizable mitigations!



Outlook

- Research has to find more generalizations and better mitigations.
- How scientific does cybersecurity need to be, as long as we're still making some progress?
- On the offensive side, finding single bugs still scales. Any exploit is gold!

 @naehrdine

 @jiska@chaos.social

 youtube.com/jiskac