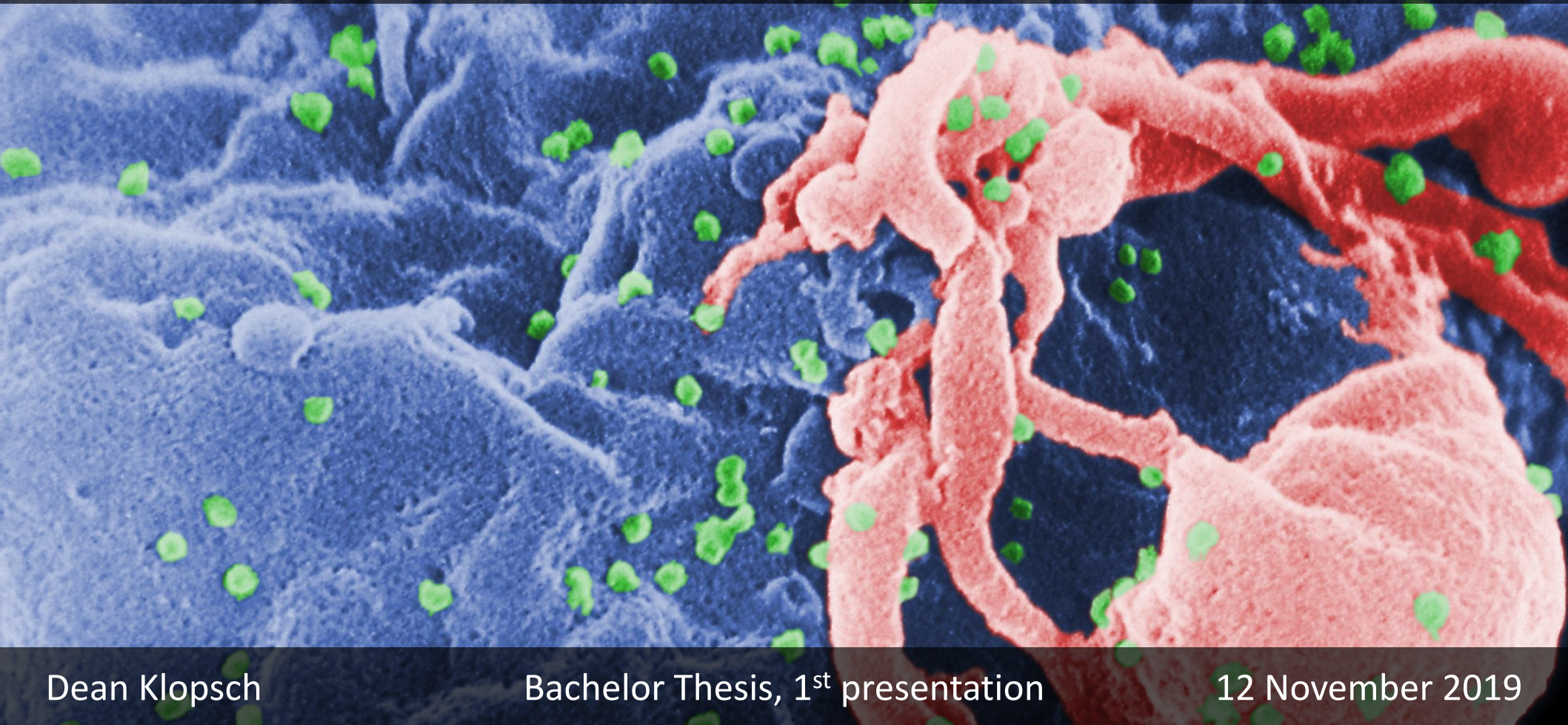
Learning from Nature:
How Nature Resolves Security Issues

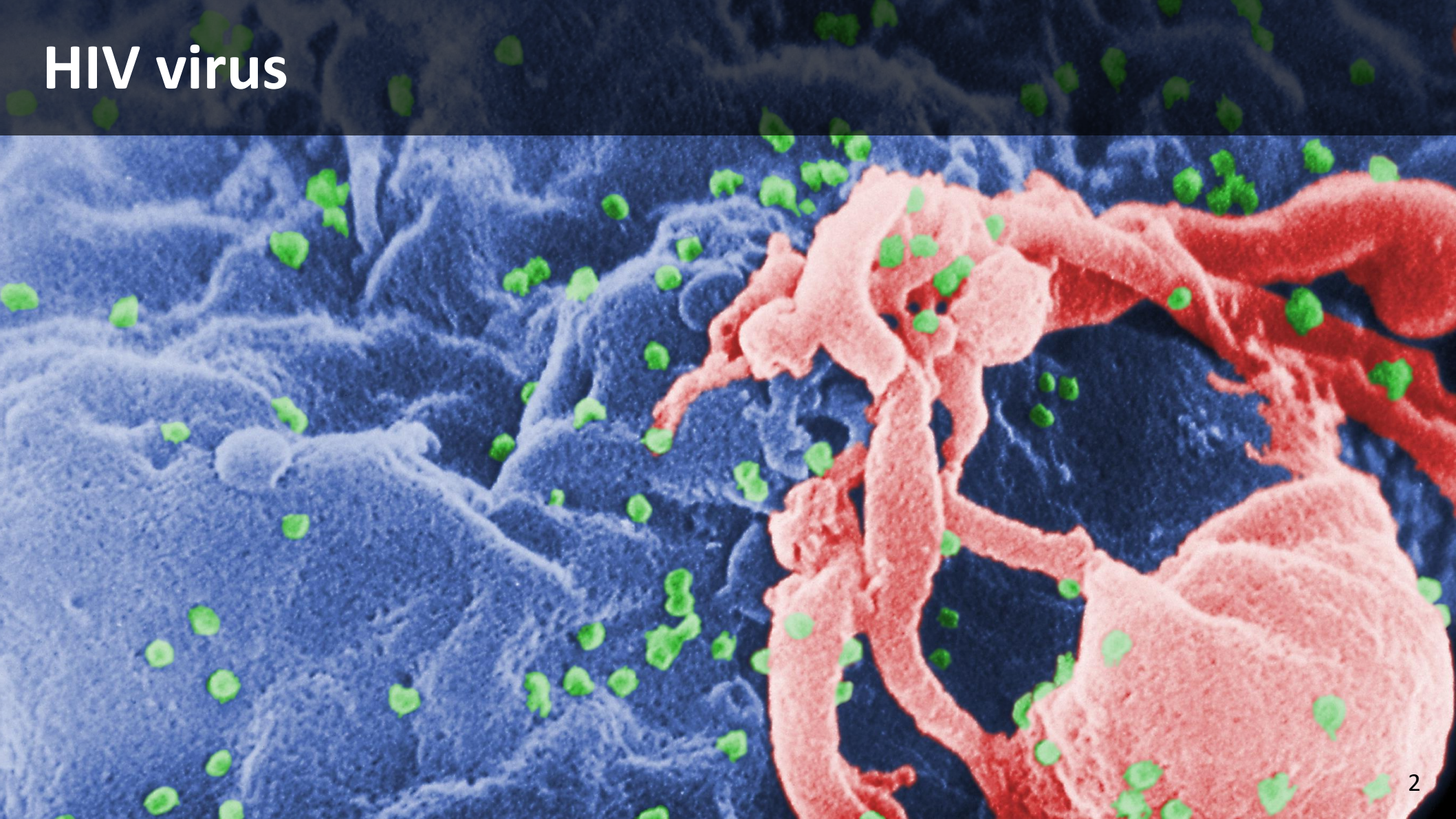


Dean Klopsch

Bachelor Thesis, 1st presentation

12 November 2019

HIV virus



A problem in nature ...

Problem
HIV virus spread leads to weakened immune system (AIDS)

Solution
currently unavailable

Difficulties in finding a vaccine
- HIV is highly mutable
- HIV isolates are highly variable
- (almost) no recovered AIDS patients
- traditional vaccines protect against disease, not against infection
- killed HIV-1 does not retain antigenicity
- live retrovirus vaccine raises safety issues

... revisited for software

Problem
a computer virus causes harm

Solution
(ultimate) solution currently unavailable

Difficulties in finding countermeasures
- virus code is highly mutable (polymorphism)
- virus code is highly variable
- (almost) no virus samples from targeted attacks
- virus scanners often detect symptoms, but not the infection

Is nature *that* different?

nature
difficulties in finding a vaccine:

- HIV is ***highly mutable***
- HIV isolates are ***highly variable***
- (almost)
  no recovered AIDS patients
- traditional vaccines
  protect against disease,
  not against infection
- killed HIV-1 does not retain antigenicity
- live retrovirus vaccine raises safety issues

software
difficulties in finding countermeasures:

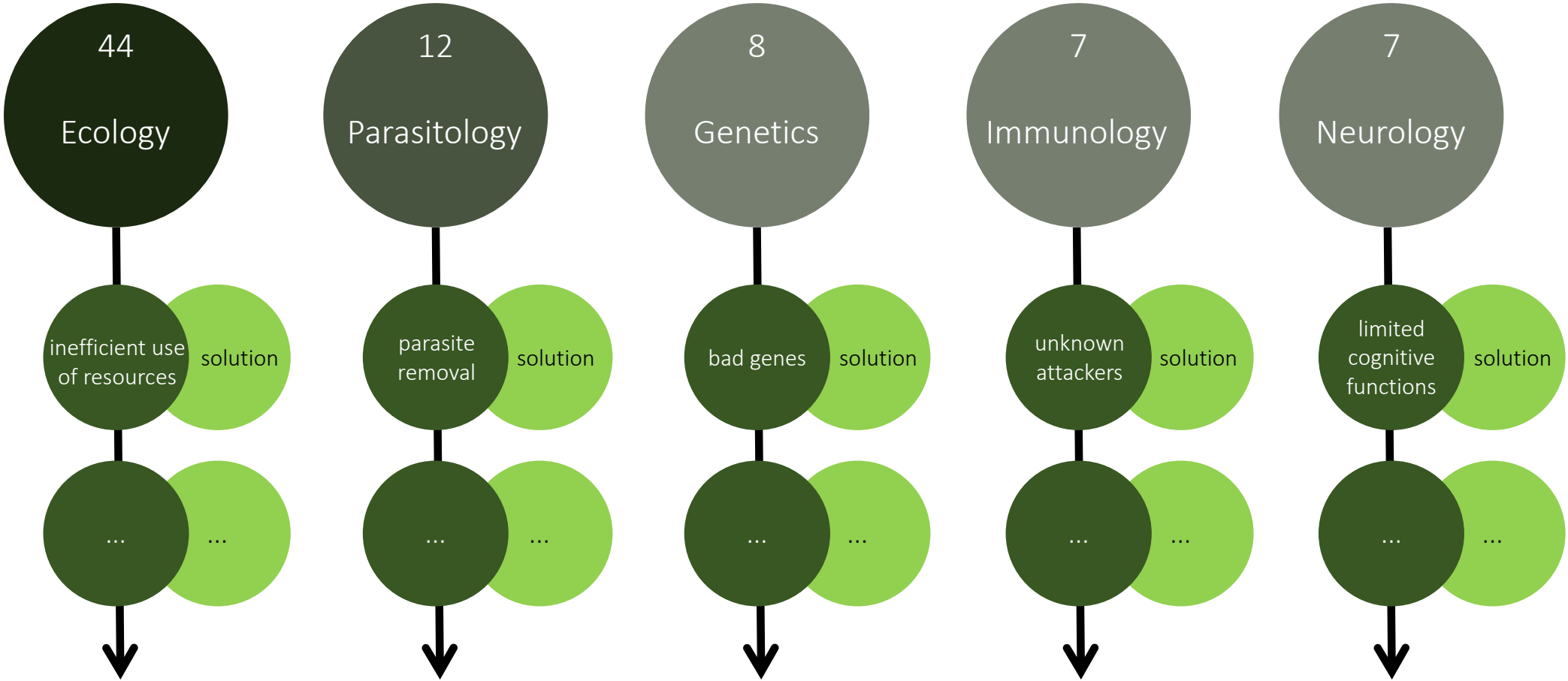
- virus code is ***highly mutable***
- virus code is ***highly variable***
- (almost)
  no virus samples from targeted attacks
- virus scanners often
  detect symptoms,
  but not the infection

We asked ourselves two questions:

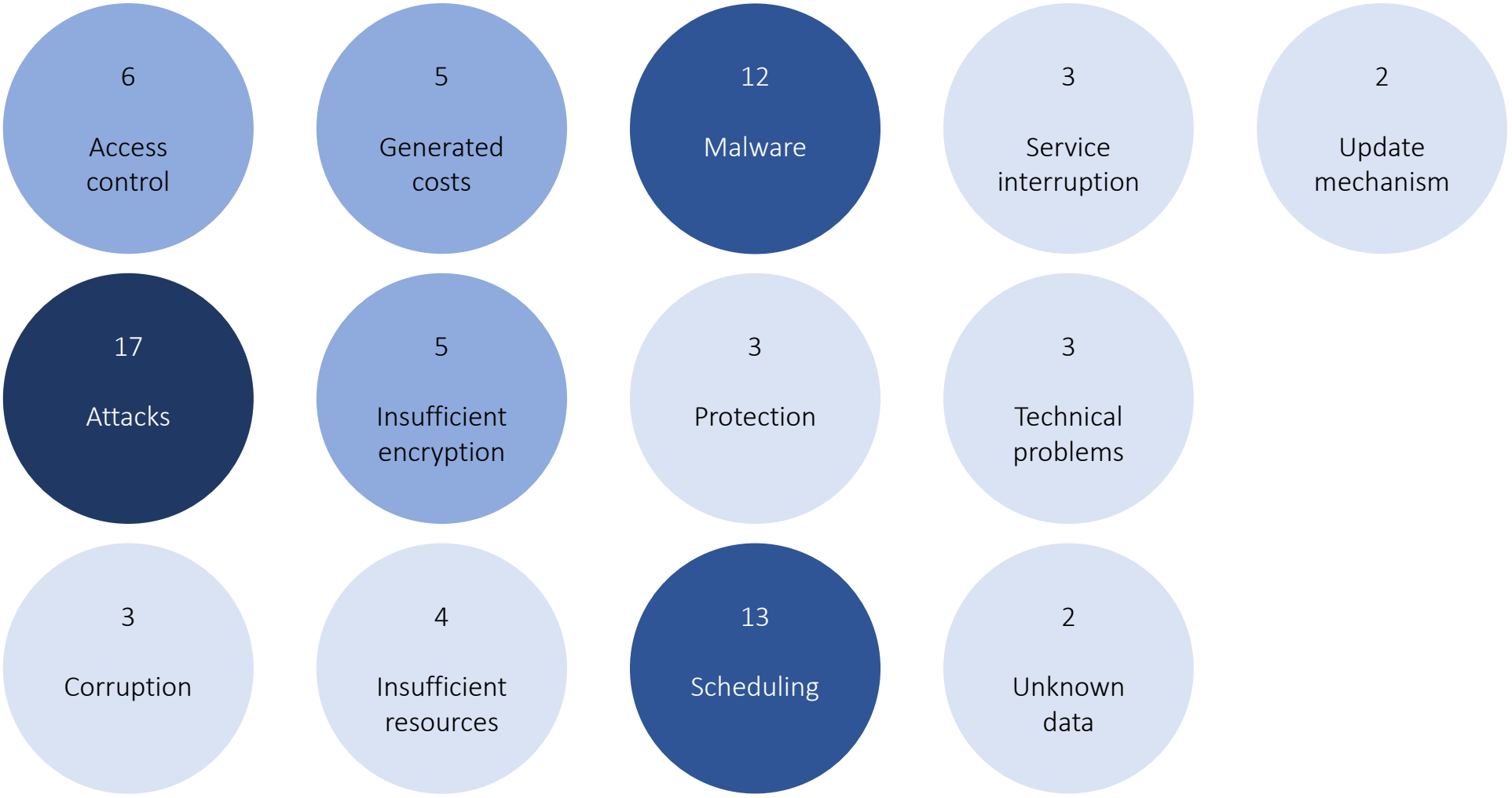
Which problems, threats, and solutions exist in living nature?

Which problems, threats, and solutions exist in software?

Problems and solutions in nature ...



… mapped to problems in software



Proposal #01: Oxpecker bird

Symbiosis between Oxpecker bird and mammals

nature		adaptation
Problem mammal suffers from parasites		**Problem** software suffers from irregularities (code injections, exploits, ...)
Threat wounds, infections		**Threat** unexpected results, outages
Solution bird eats the parasites		**Solution** proactive monitoring service

Proposal #02: Locust

A solitarious male Desert locust (left) facing a gregarious male (right) of the same species.

Mutation of a locust

nature

Problem
too many individuals together (scarce food)

Threat
starvation

Solution
locust transforms into travel form

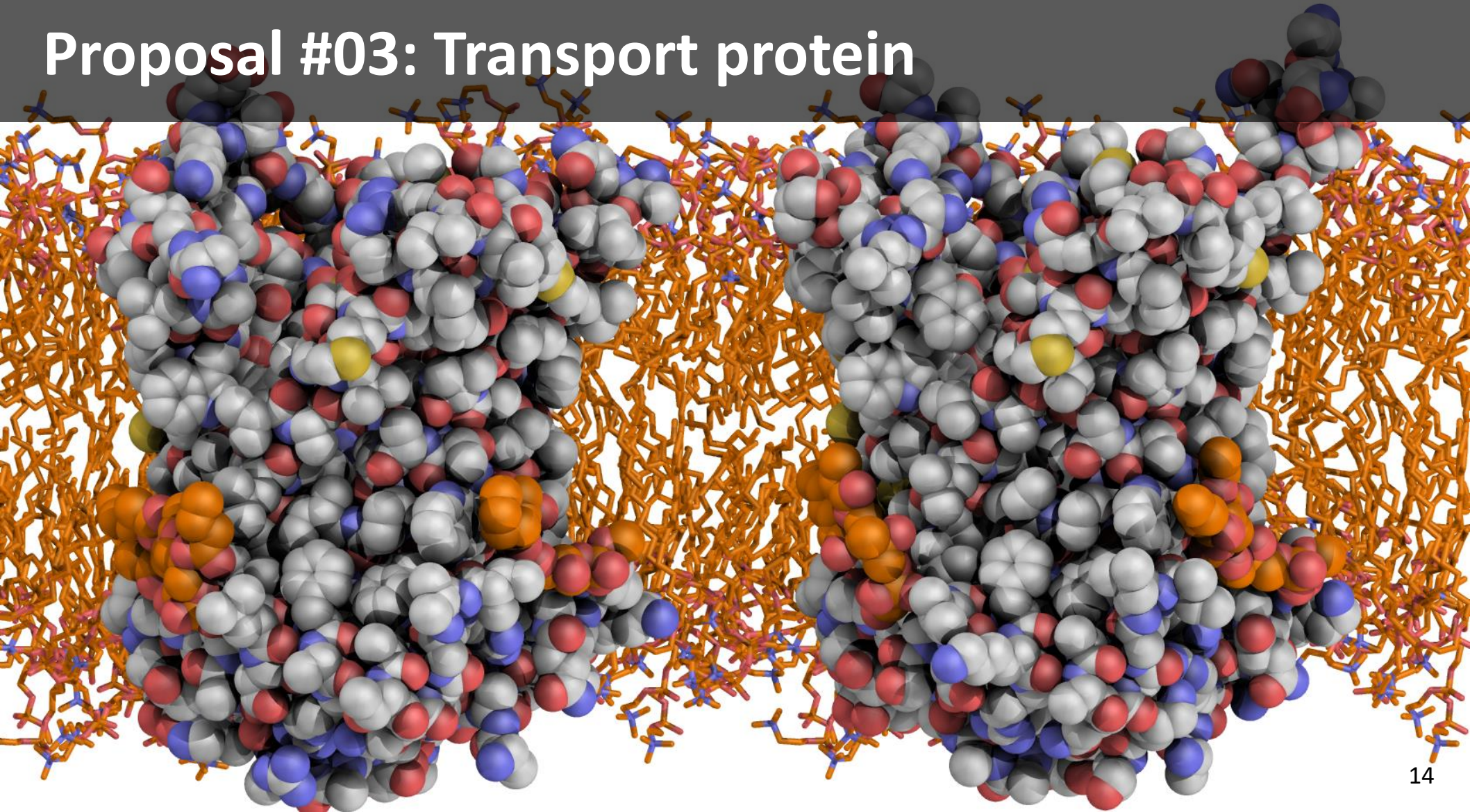
adaptation

Problem
sensitive information is centralized

Threat
data leaks

Solution
spread of sensitive information (less risk at each location)

Proposal #03: Transport protein



Transport protein supports carrier-mediated transport

nature

Problem
reliable delivery of resources

Threat
lack of ions and (macro) molecules

Solution
carrier-mediated transport ensures integrity

adaptation

Problem
resource repositories lack support for security-related meta data

Threat
vulnerabilities in software

Solution
bidirectional meta data communication

Proposal #04: Golden poison frog

Lethal venom protects against attackers

nature		adaptation
Problem hungry carnivores		**Problem** software is under attack
Threat being eaten		**Threat** data leak, service outage
Solution lethal venom on skin		**Solution** serve (unexpected) outputs to crash attacker

Proposal #05: Sea urchin

Protein triggers immune system reaction

nature		adaptation
Problem hungry carnivores		**Problem** software is under attack
Threat being eaten		**Threat** data leak, service outage
Solution “cheap” but powerful proteins in spikes		**Solution** misuse of anti-malware software to resolve the threat

Potential empirical studies

Proposal #06: Precocial species

What are secure default configurations, and where are they used?

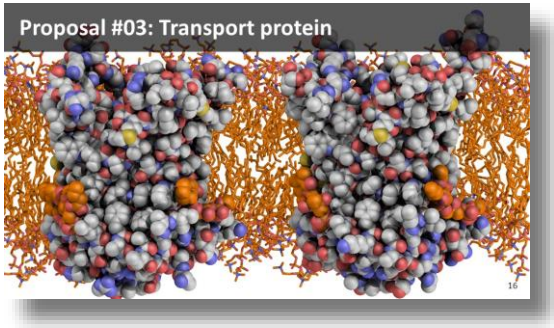
Proposal #07: Altricial species

How are resource repositories secured?

Discussion

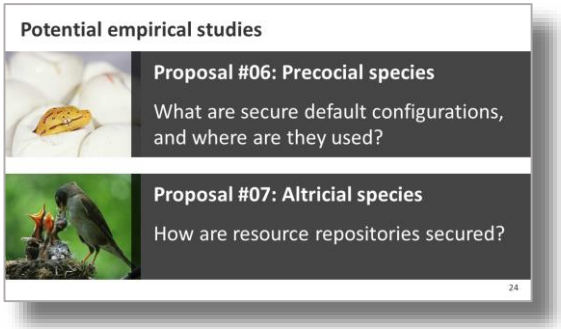

Proposal #01: Oxpecker bird


Proposal #02: Locust


Proposal #03: Transport protein


Proposal #04: Golden poison frog


Proposal #05: Sea urchin


Potential empirical studies
Proposal #06: Precocial species
What are secure default configurations, and where are they used?
Proposal #07: Altricial species
How are resource repositories secured?