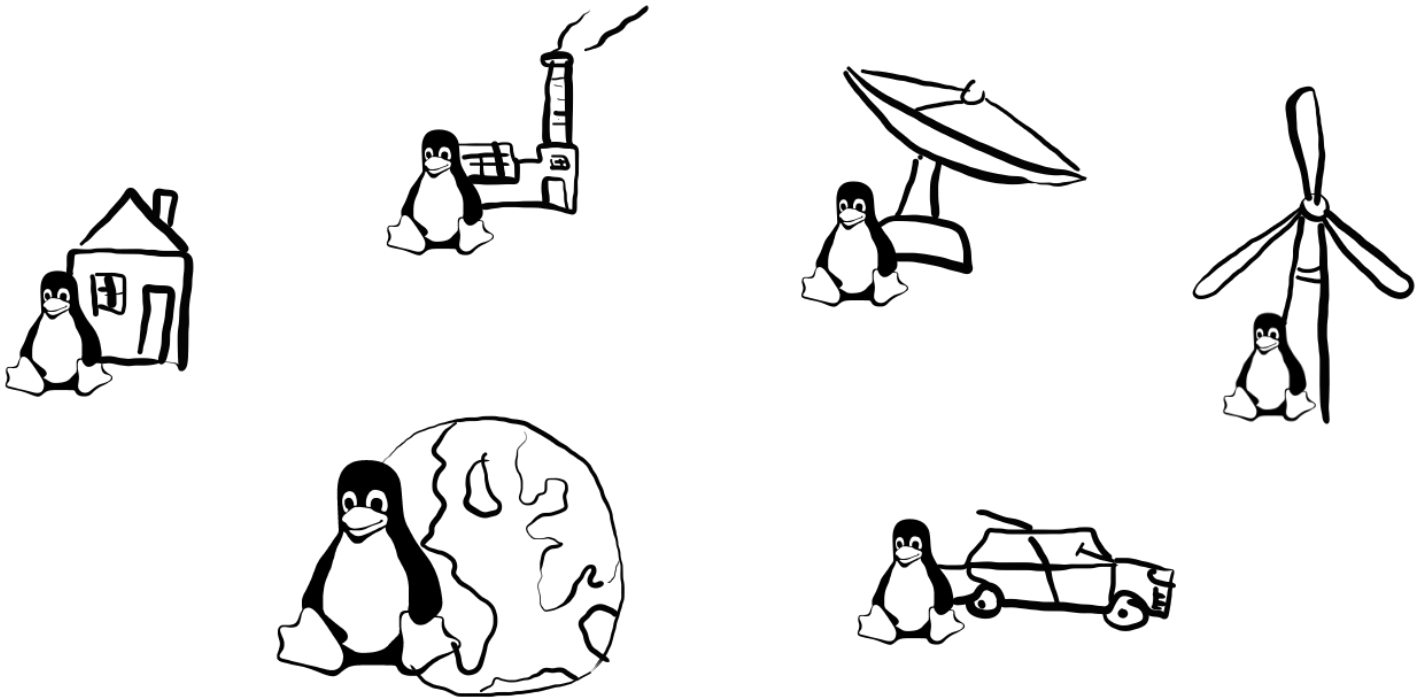
Invading the Penguin:
Breaking operating system kernel IPv6 protocol stack

Bernhards Blumbergs, GXPN, GICSP

Penguins around us



Attacking the core

The User/Kernel land

Invading the kernel

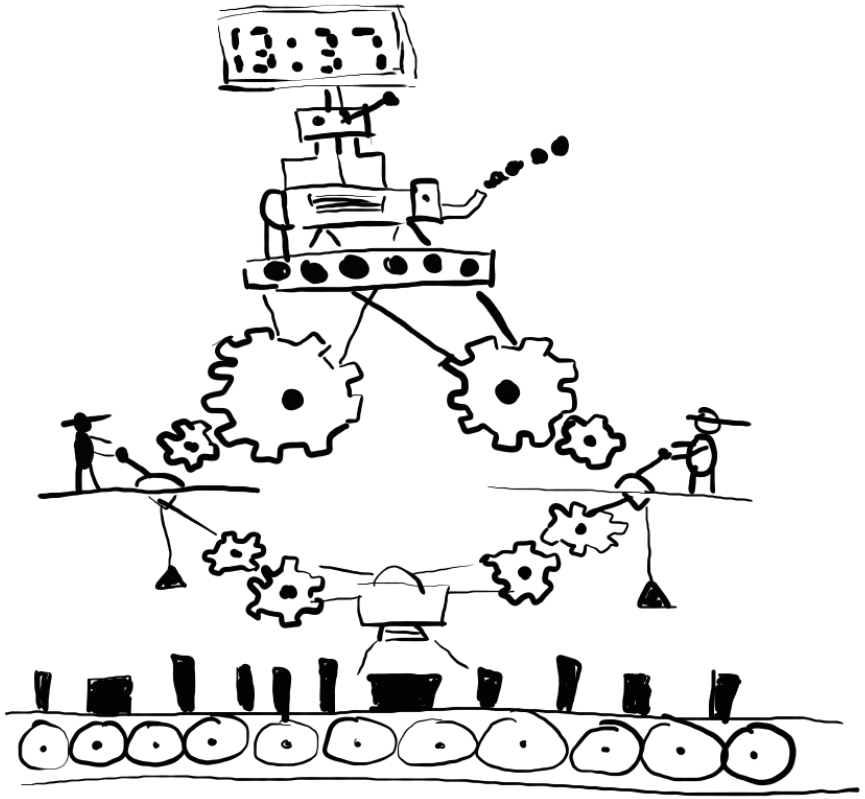
Denial of Service

Information disclosure

Code execution

Kernel development

Dual-stack host



Layer – 7
Layer – 6

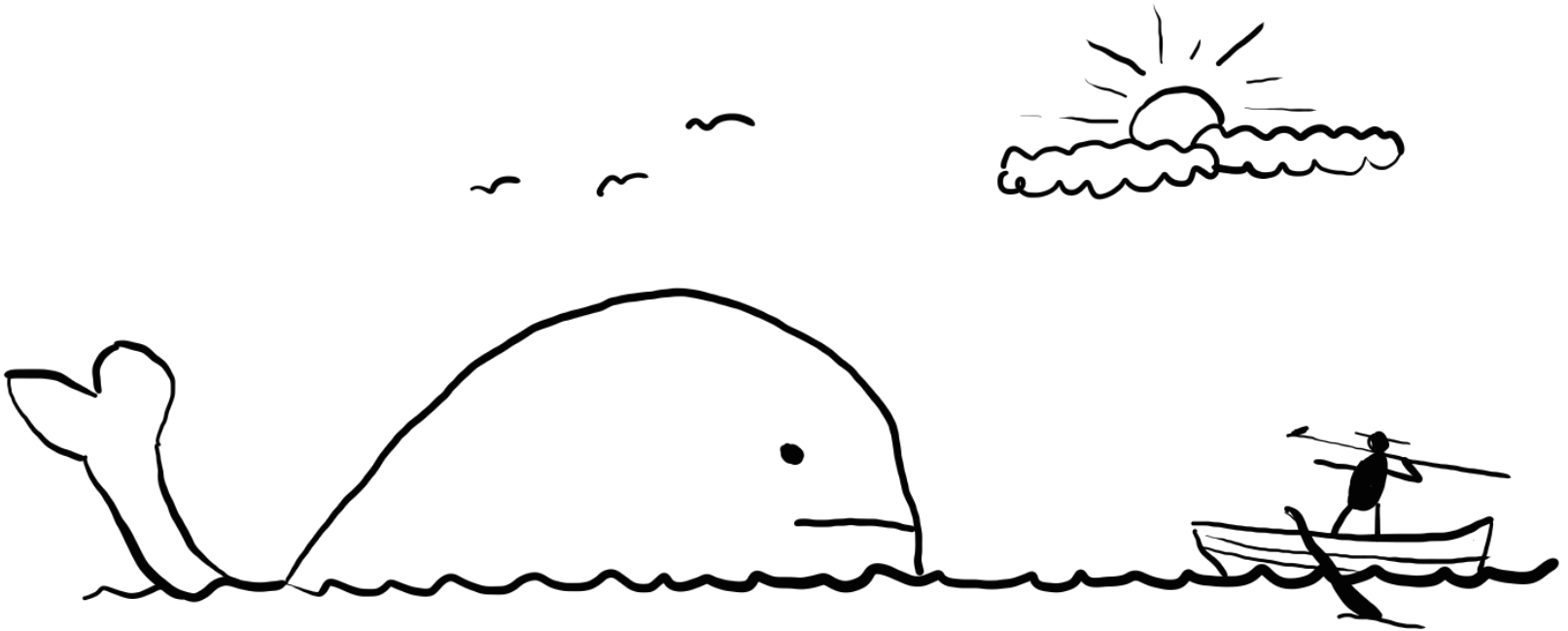
Layer – 5
Layer – 4

Layer – 3

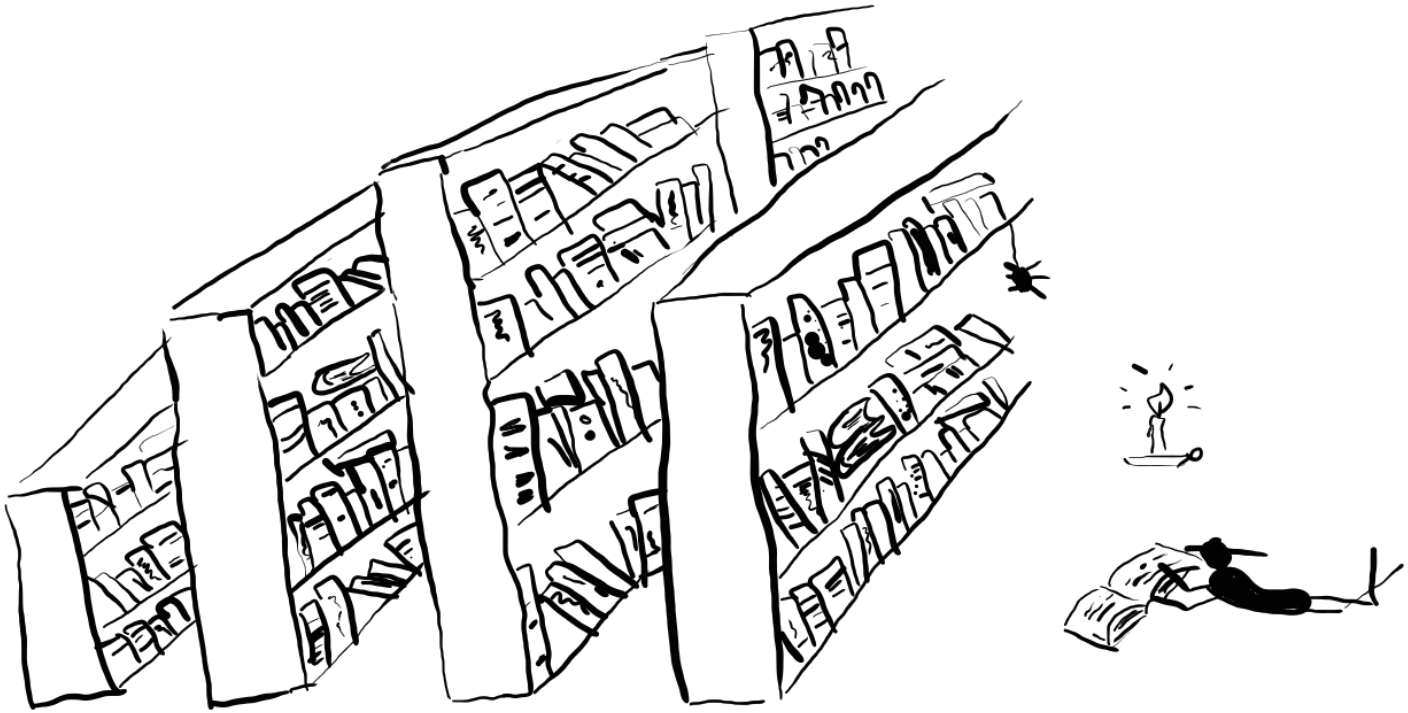
Layer – 2

Layer – 1

Known attacks



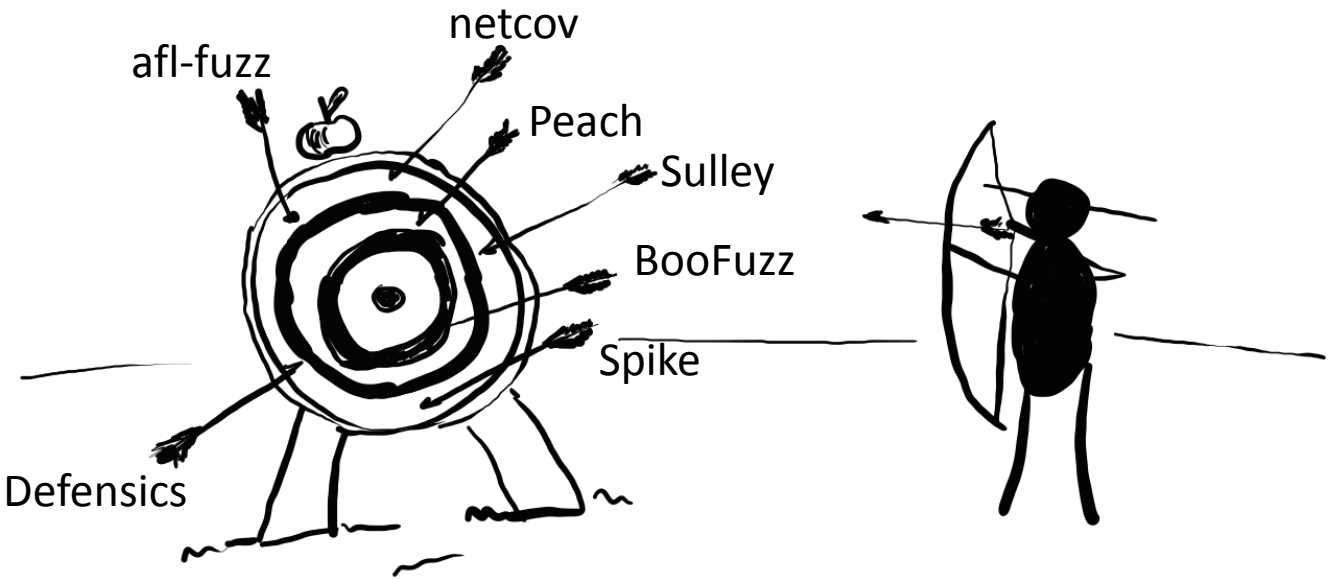
Source code analysis



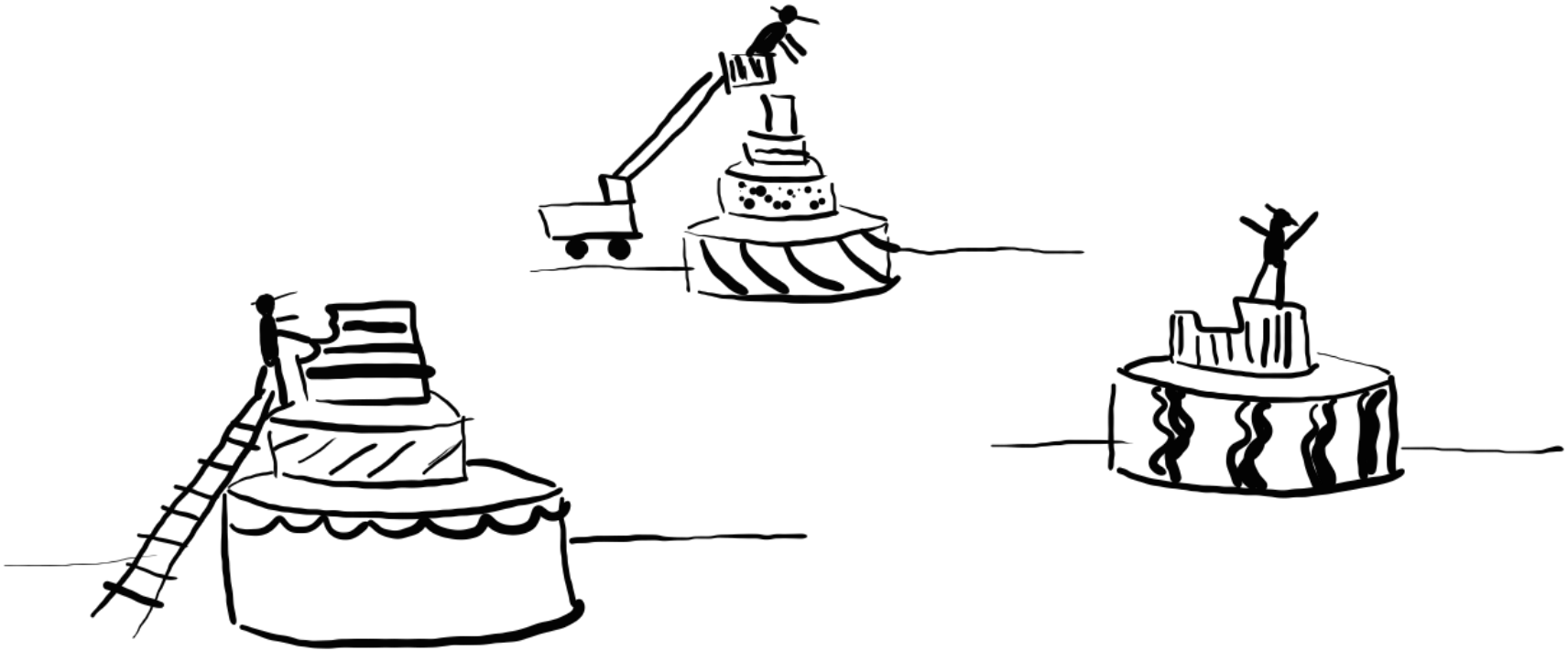
linux/net/ipv6/ip6_input.c

```
/*
 *      IPv6 input
 *      Linux INET6 implementation
 *
 *      Authors:
 *      Pedro Roque             <roque@di.fc.ul.pt>
 *      Ian P. Morris           <I.P.Morris@soton.ac.uk>
 *
 *      Based in linux/net/ipv4/ip_input.c
 *
 *      This program is free software; you can redistribute it and/or
 *    modify it under the terms of the GNU General Public License
 *    as published by the Free Software Foundation; either version
 *    2 of the License, or (at your option) any later version.
 */
```

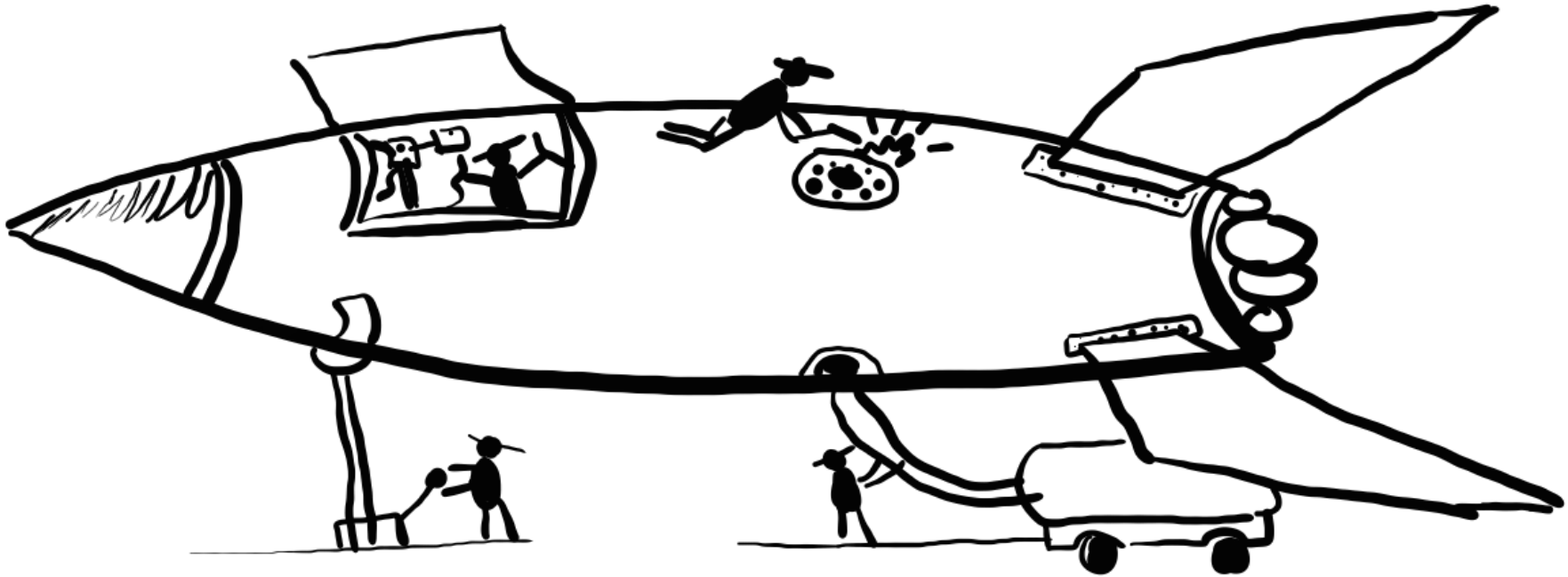
Fuzzing the target



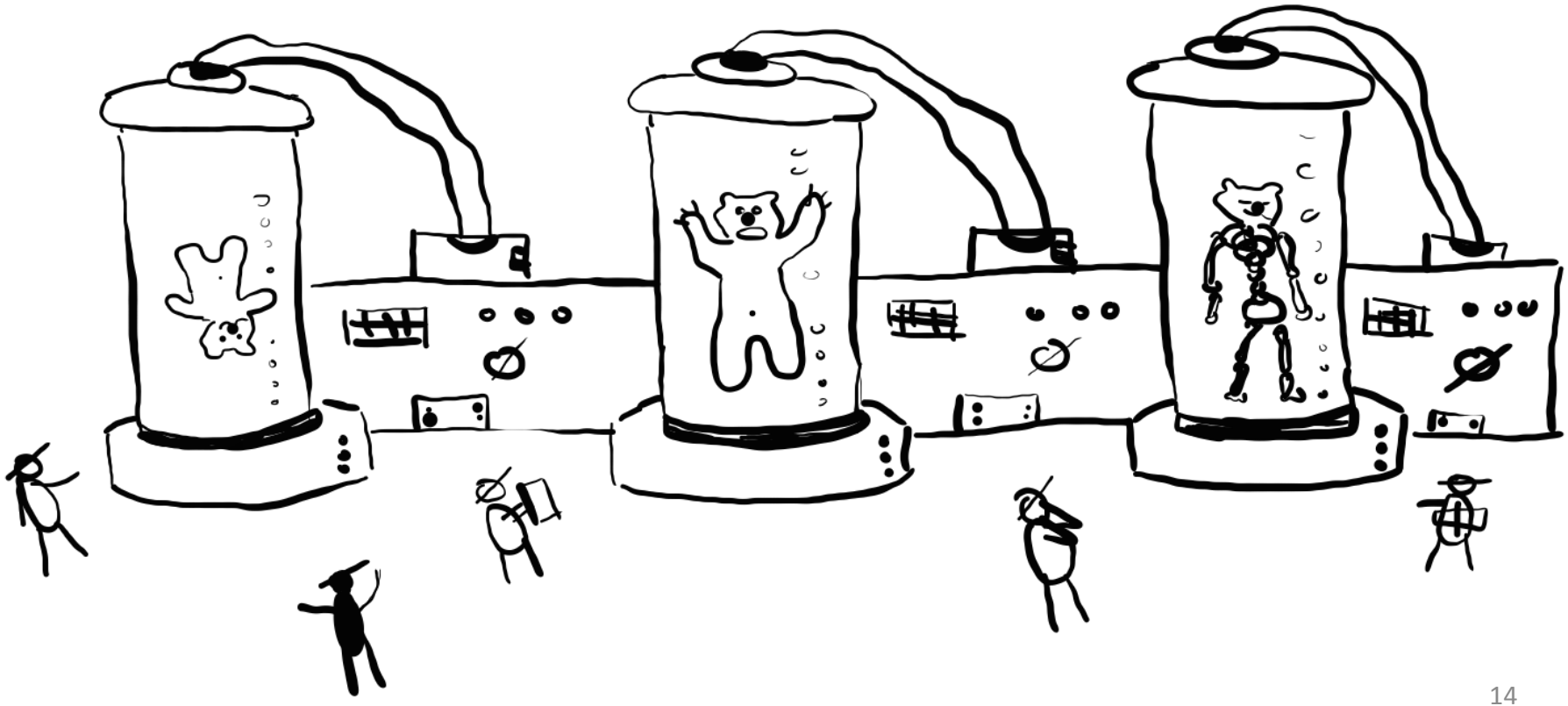
Selecting the layer



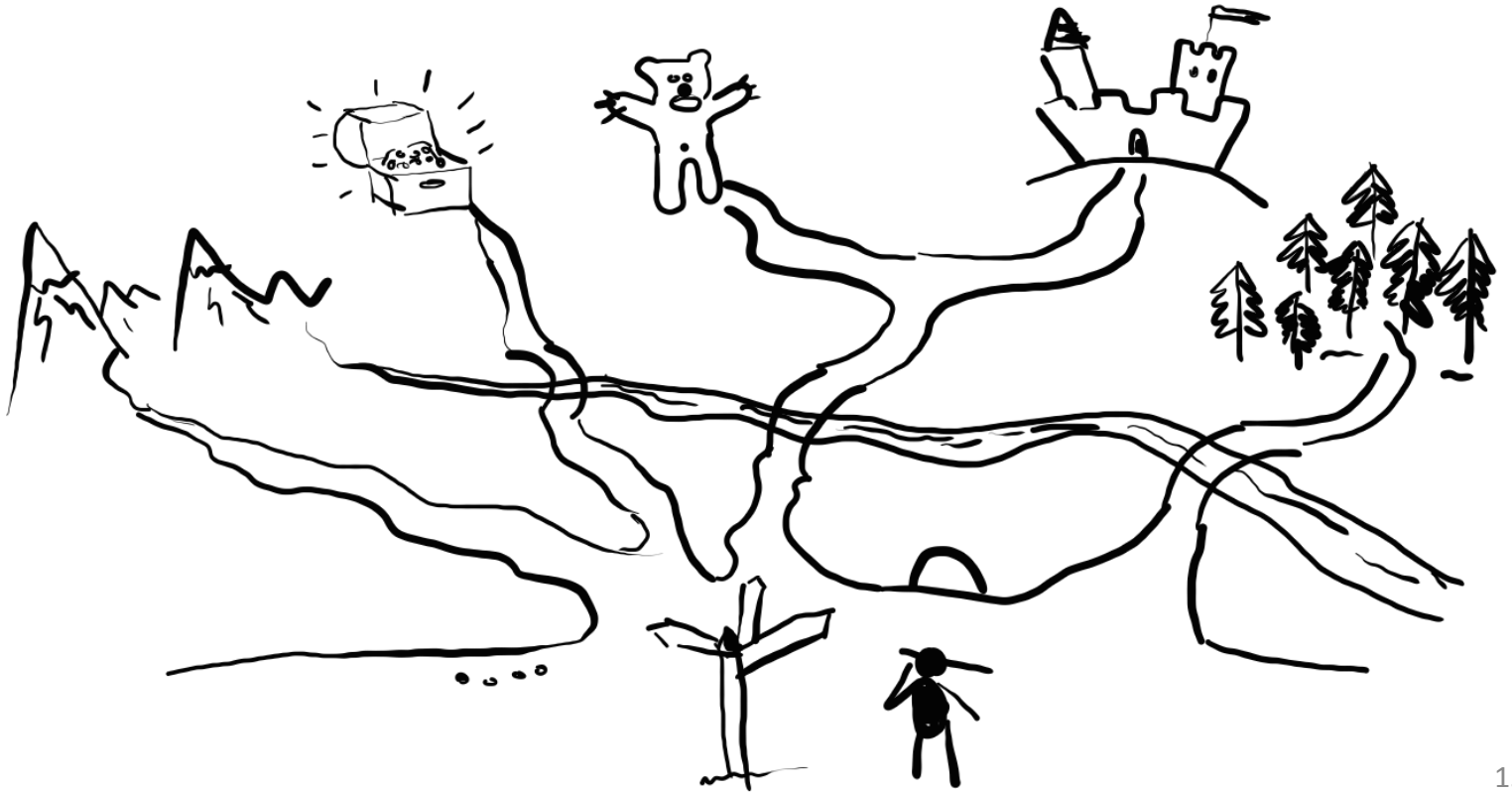
Assembling the payload



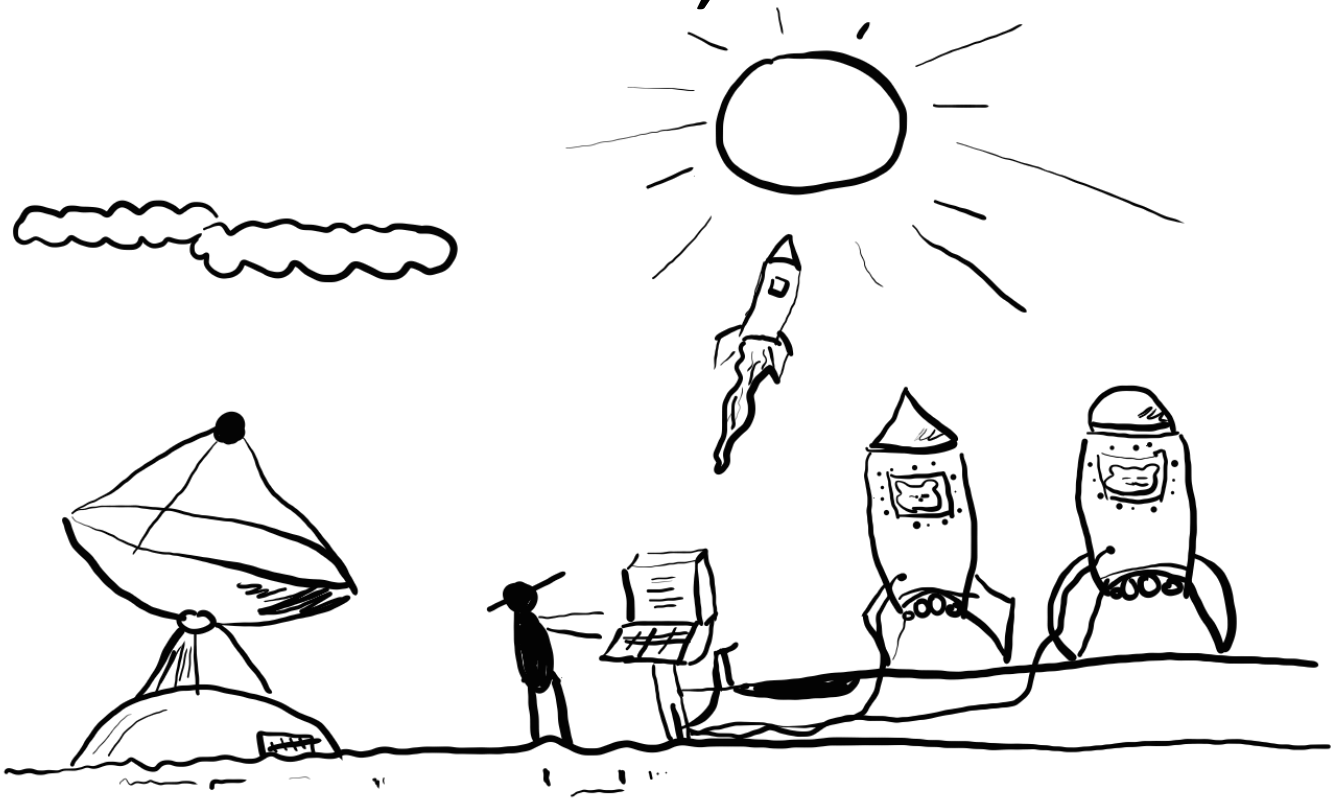
Mutation engine



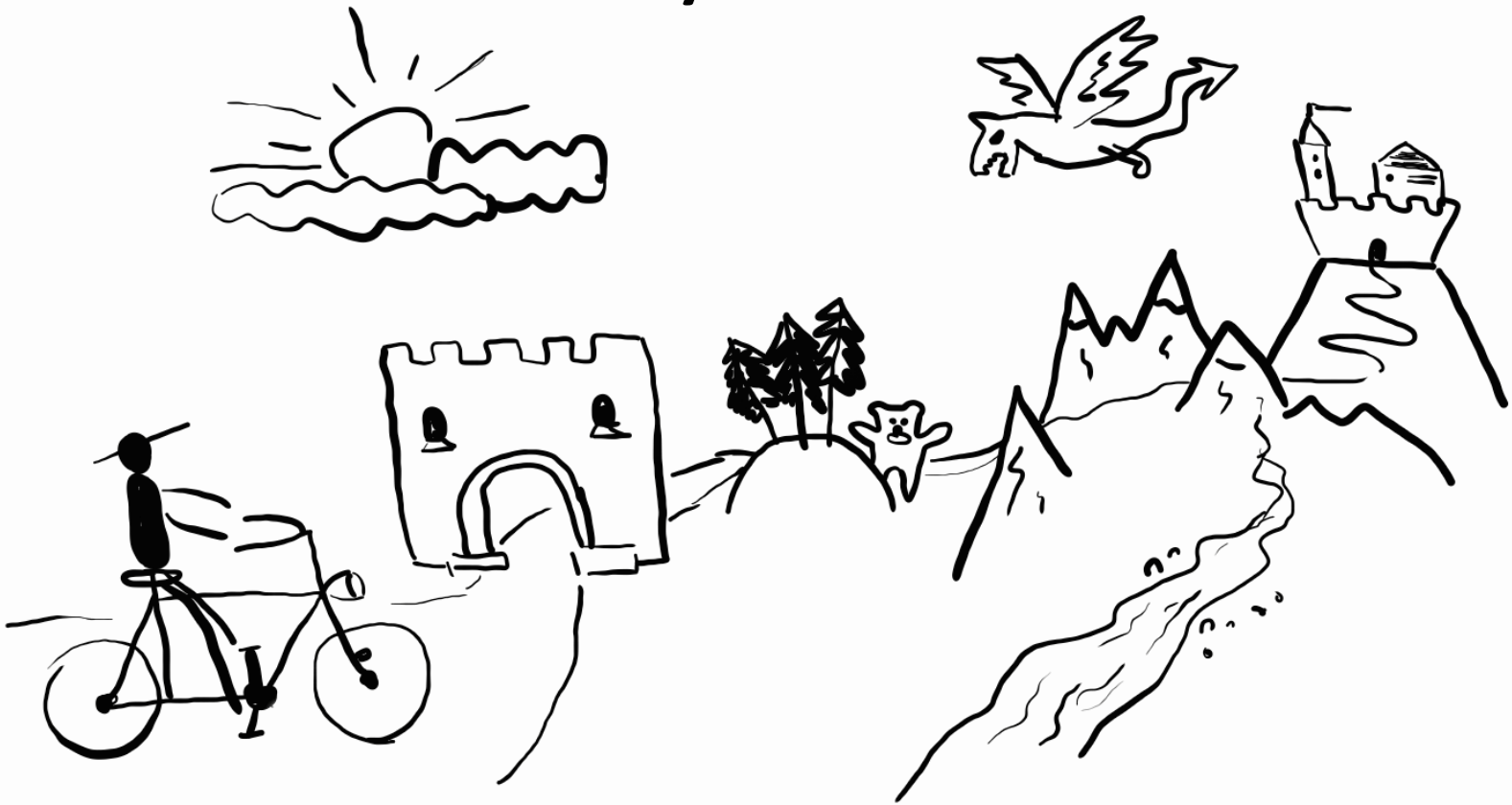
Code coverage



Fuzz Forest, Fuzz!



Way ahead



The truth is out there… in kernel