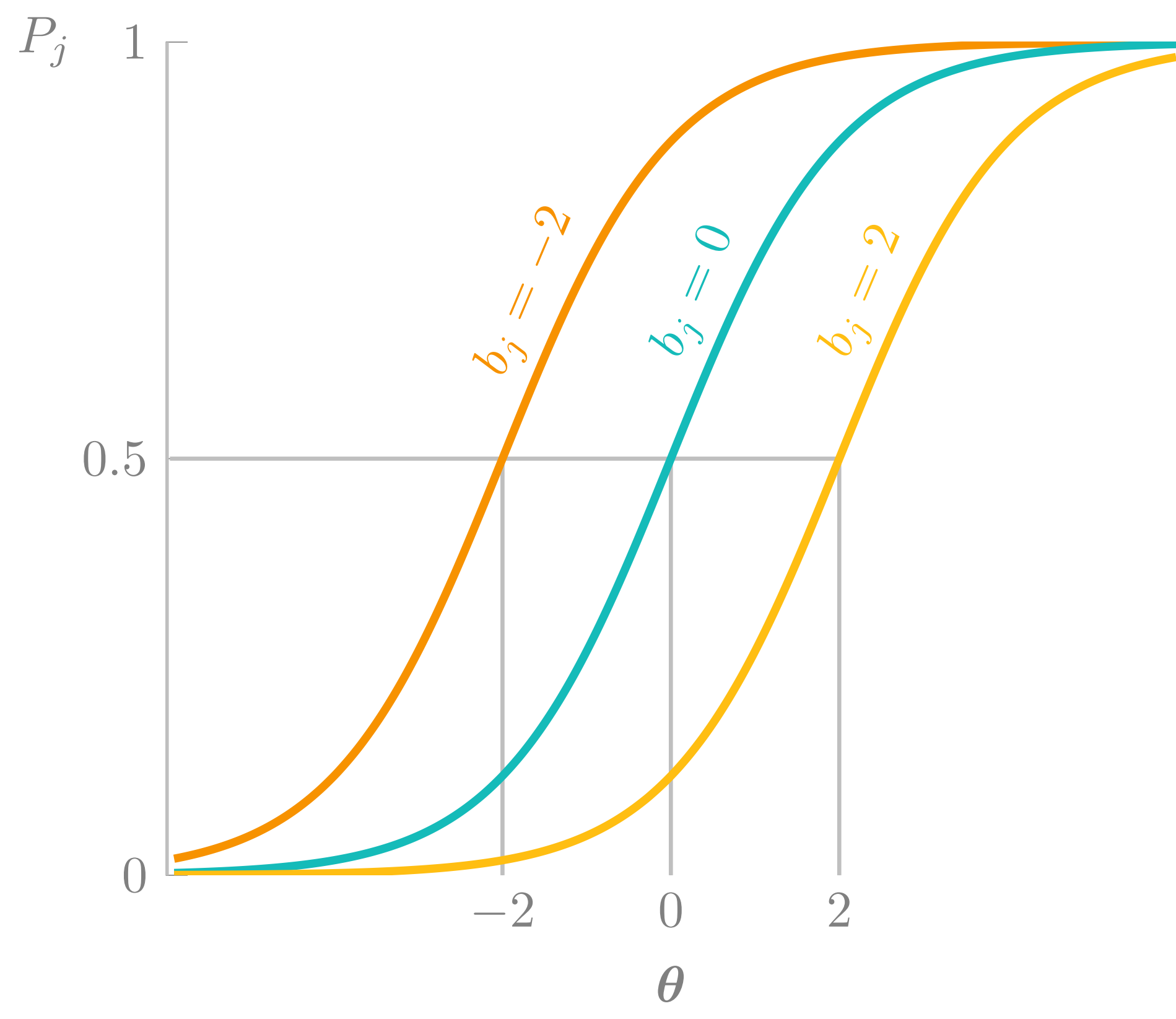
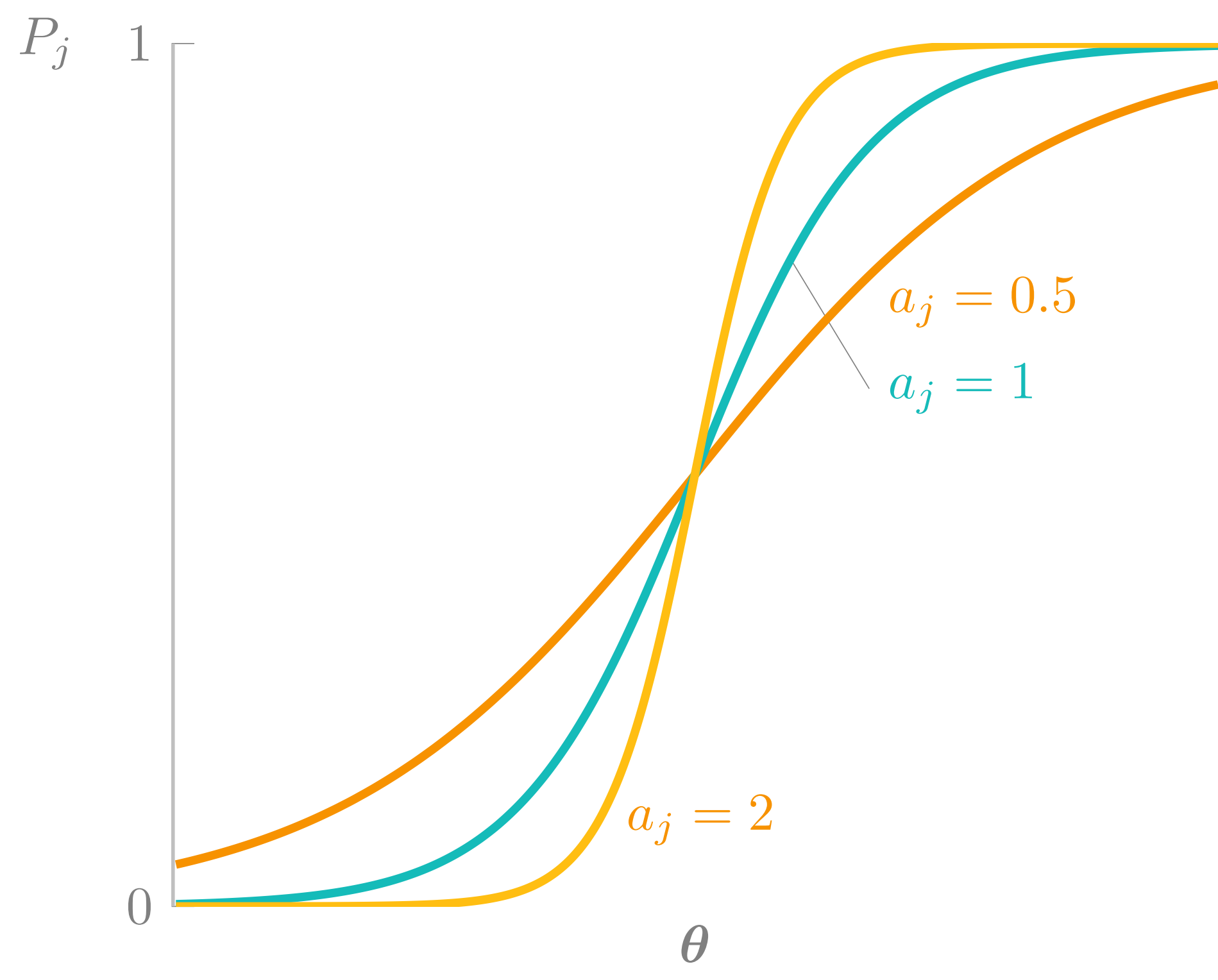
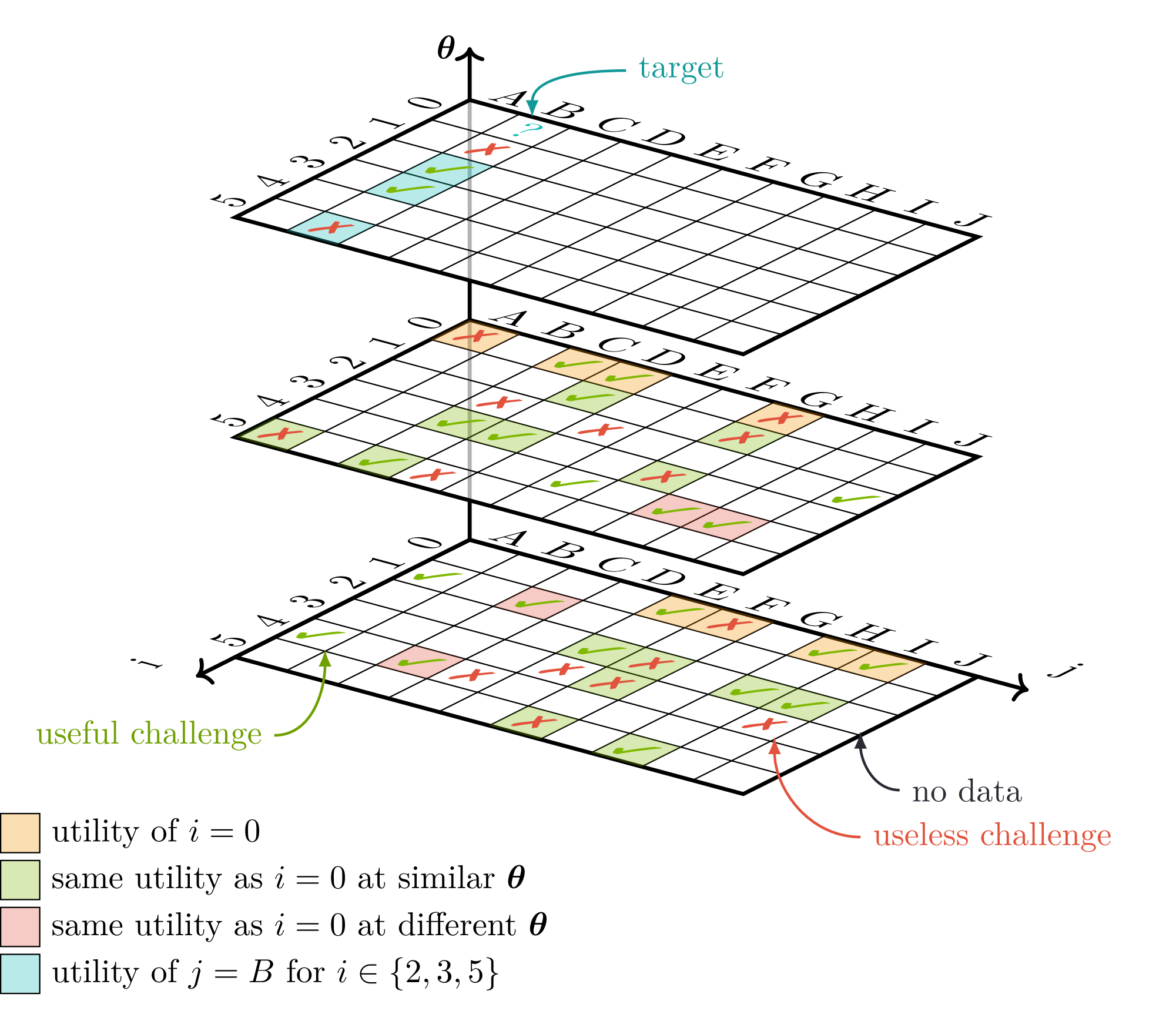
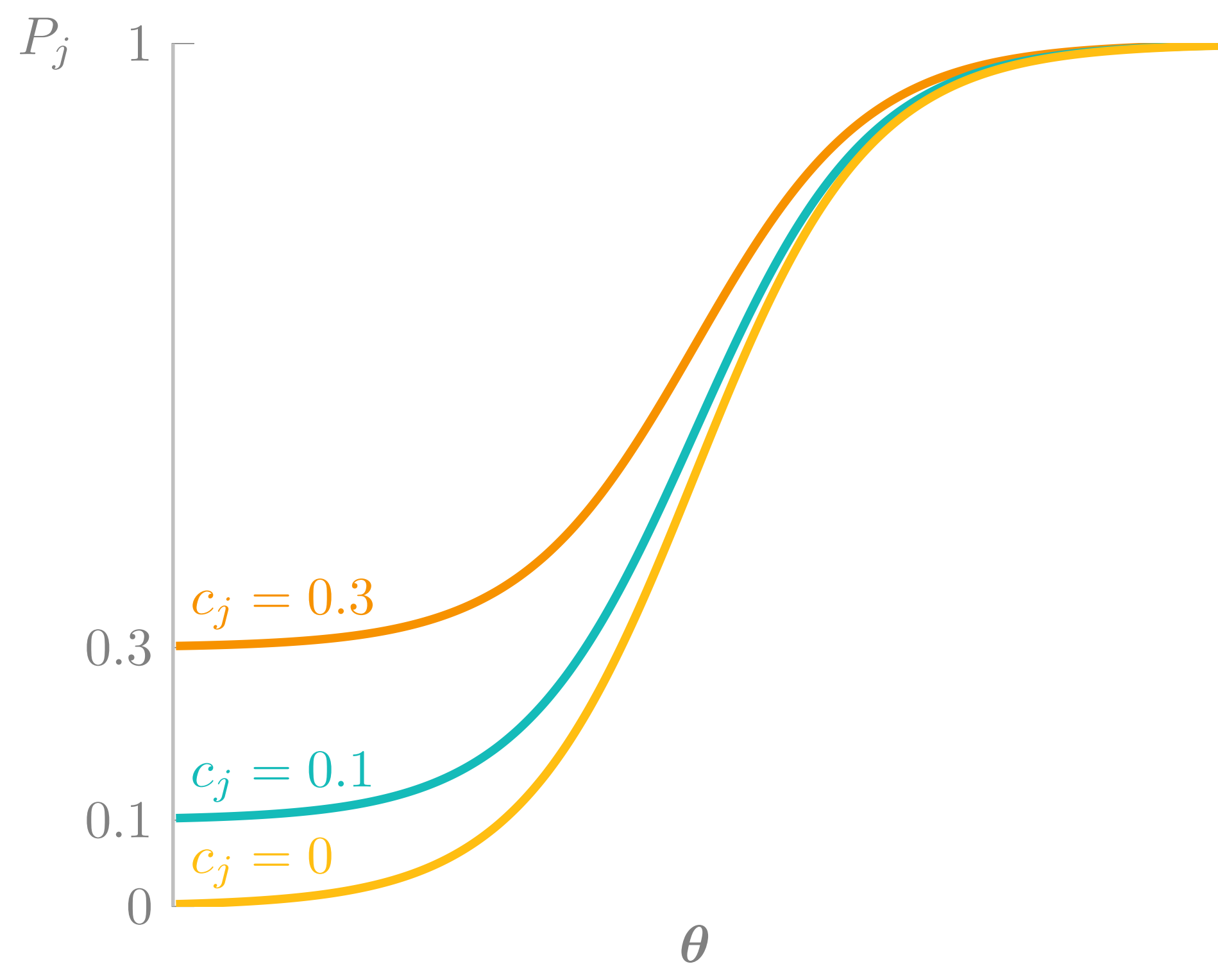
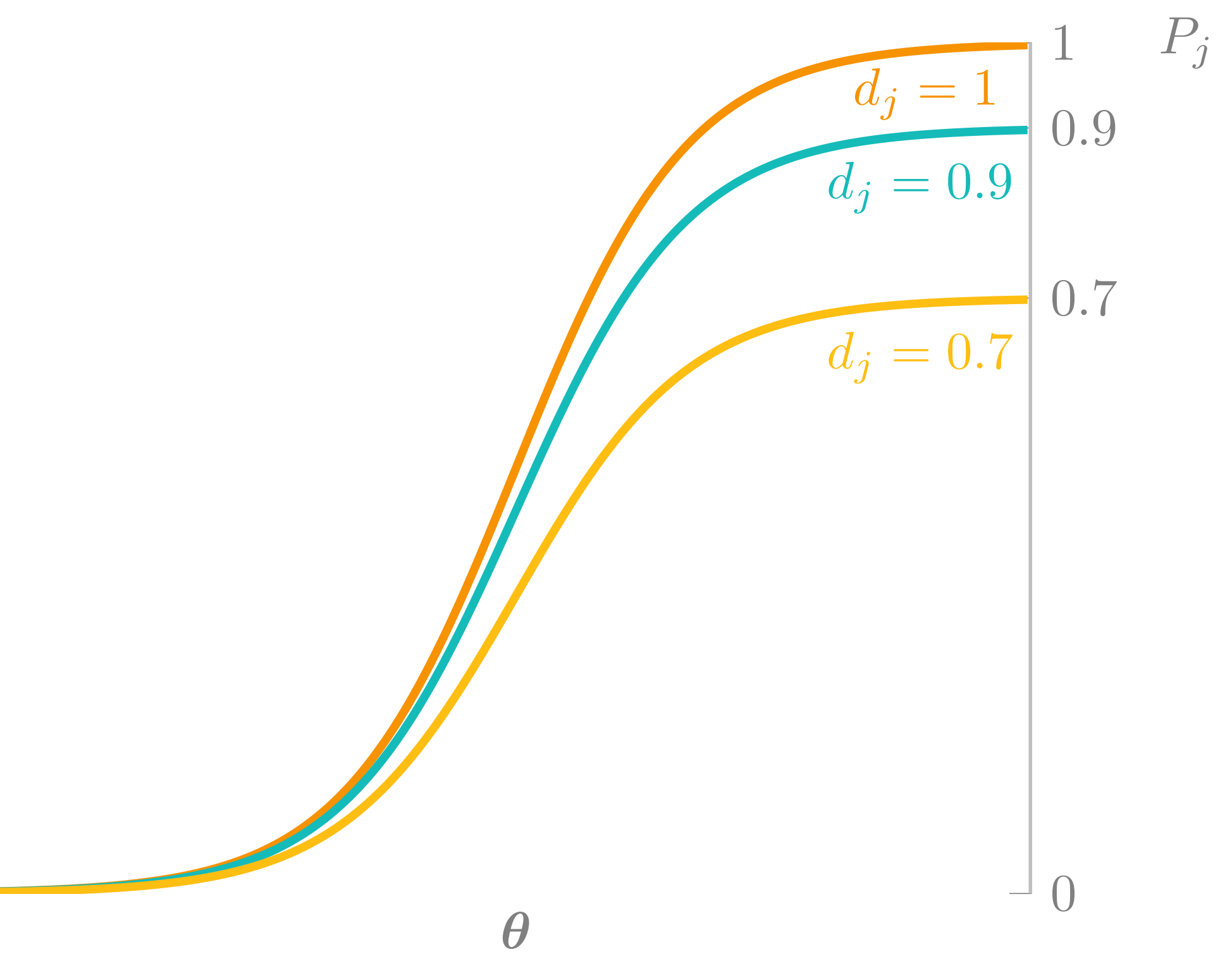
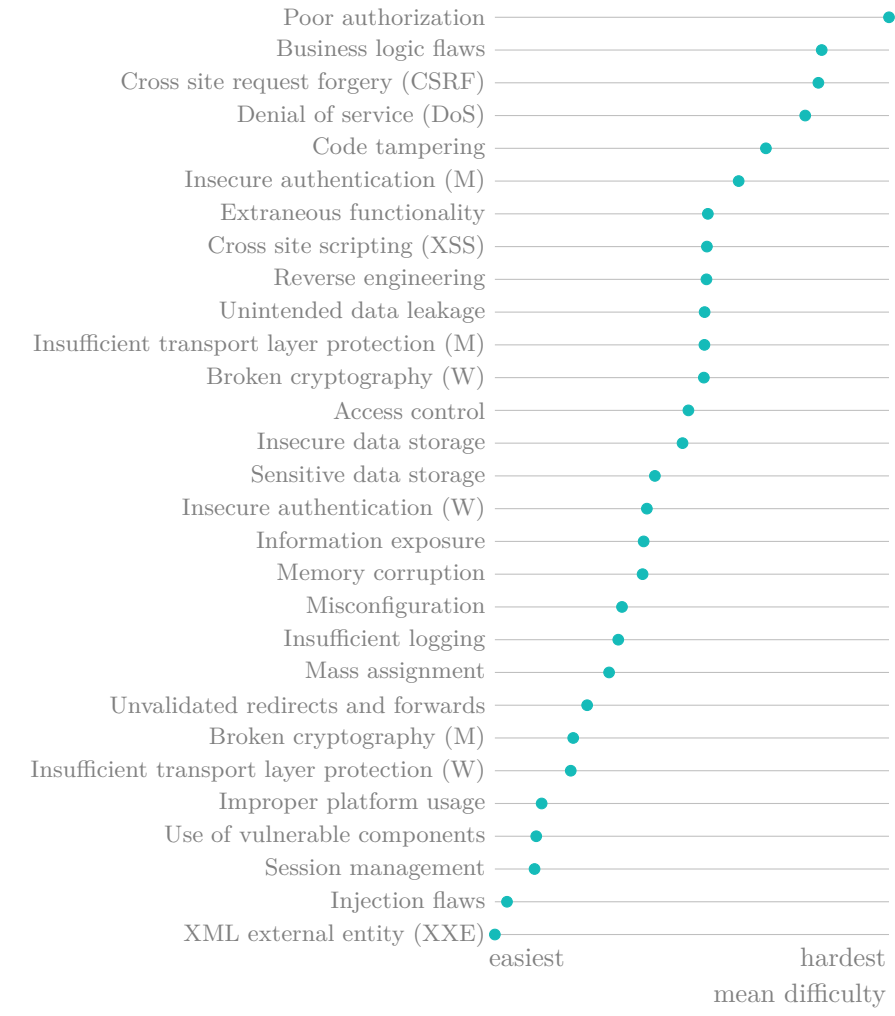

P_j
1
0.5
0
$b_j = -2$
$b_j = 0$
$b_j = 2$
-2
0
2
θ

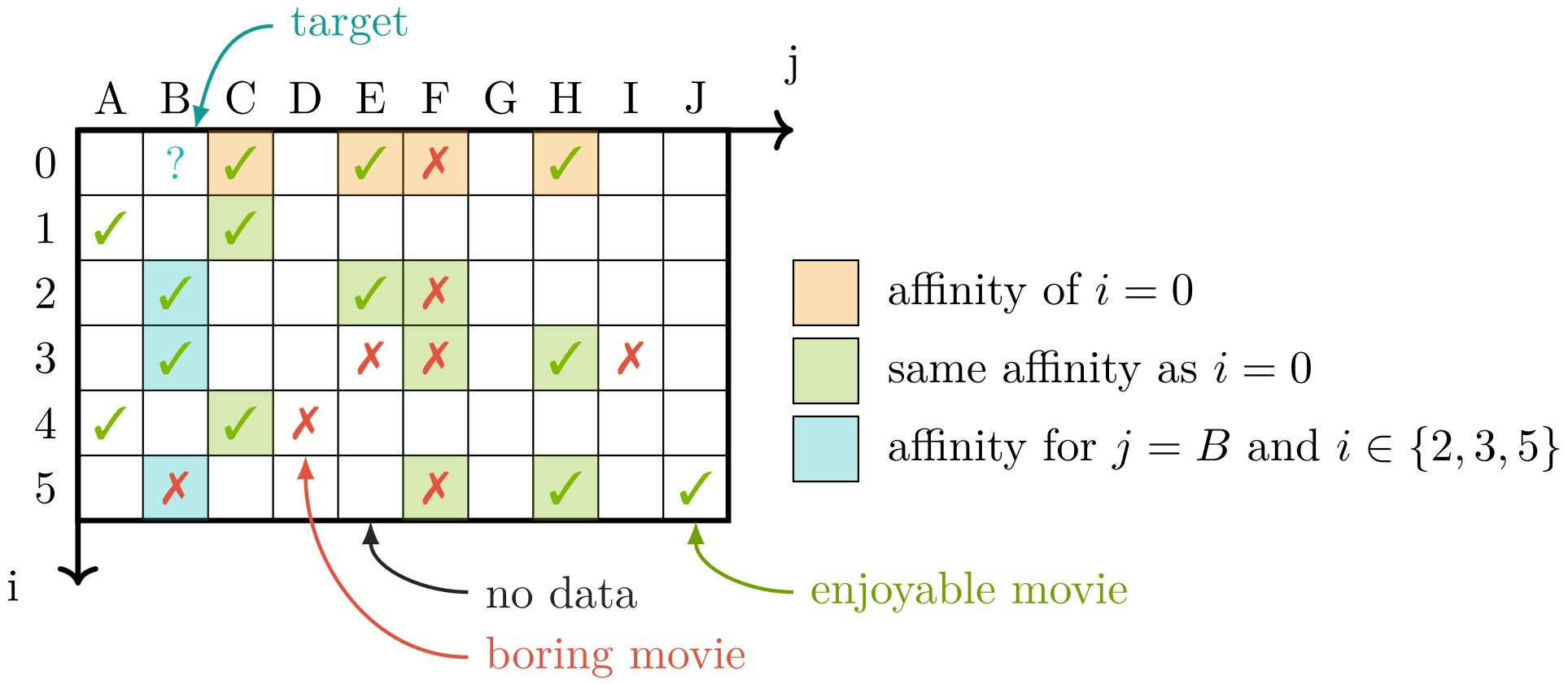

P_j
1
0
θ
$a_j = 0.5$
$a_j = 1$
$a_j = 2$

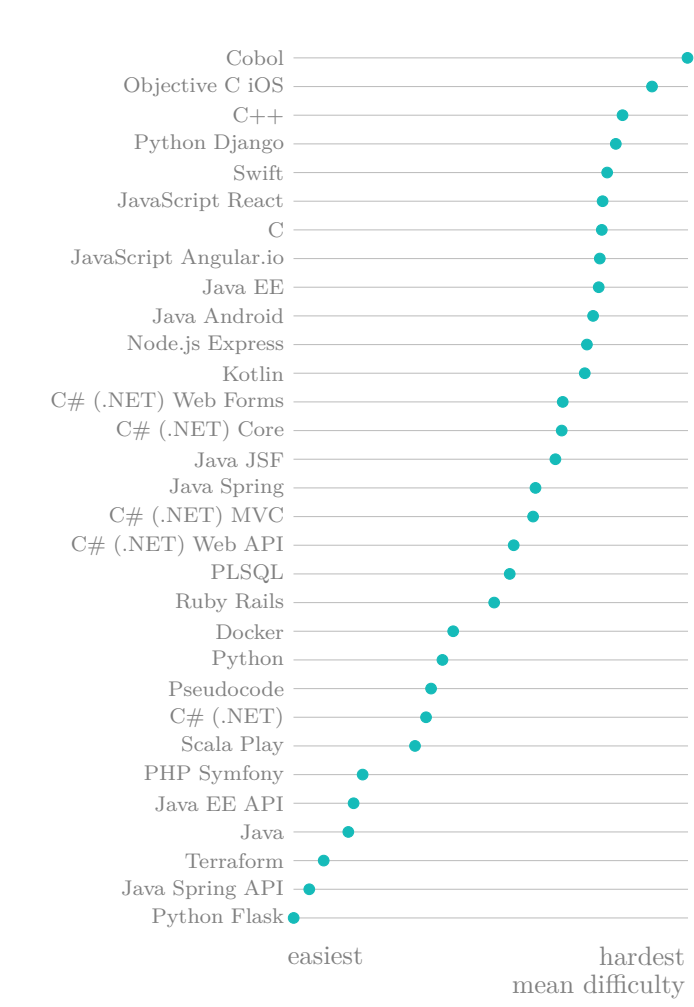

θ
target
?
A B C D E F G H I J
0 1 2 3 4 5
i
j
useful challenge
no data
useless challenge
utility of $i = 0$
same utility as $i = 0$ at similar $\boldsymbol{\theta}$
same utility as $i = 0$ at different $\boldsymbol{\theta}$
utility of $j = B$ for $i \in \{2, 3, 5\}$

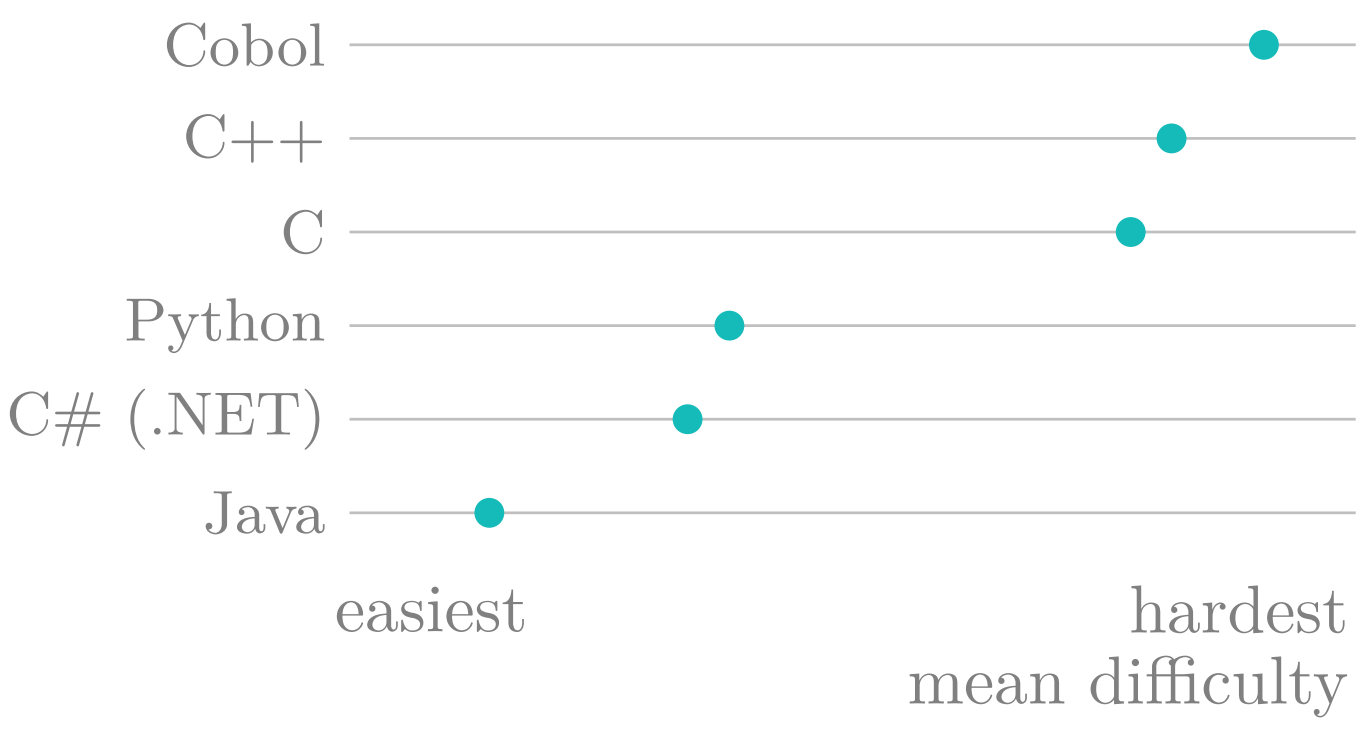

P_j
1
0.3
0.1
0
$c_j = 0.3$
$c_j = 0.1$
$c_j = 0$
θ

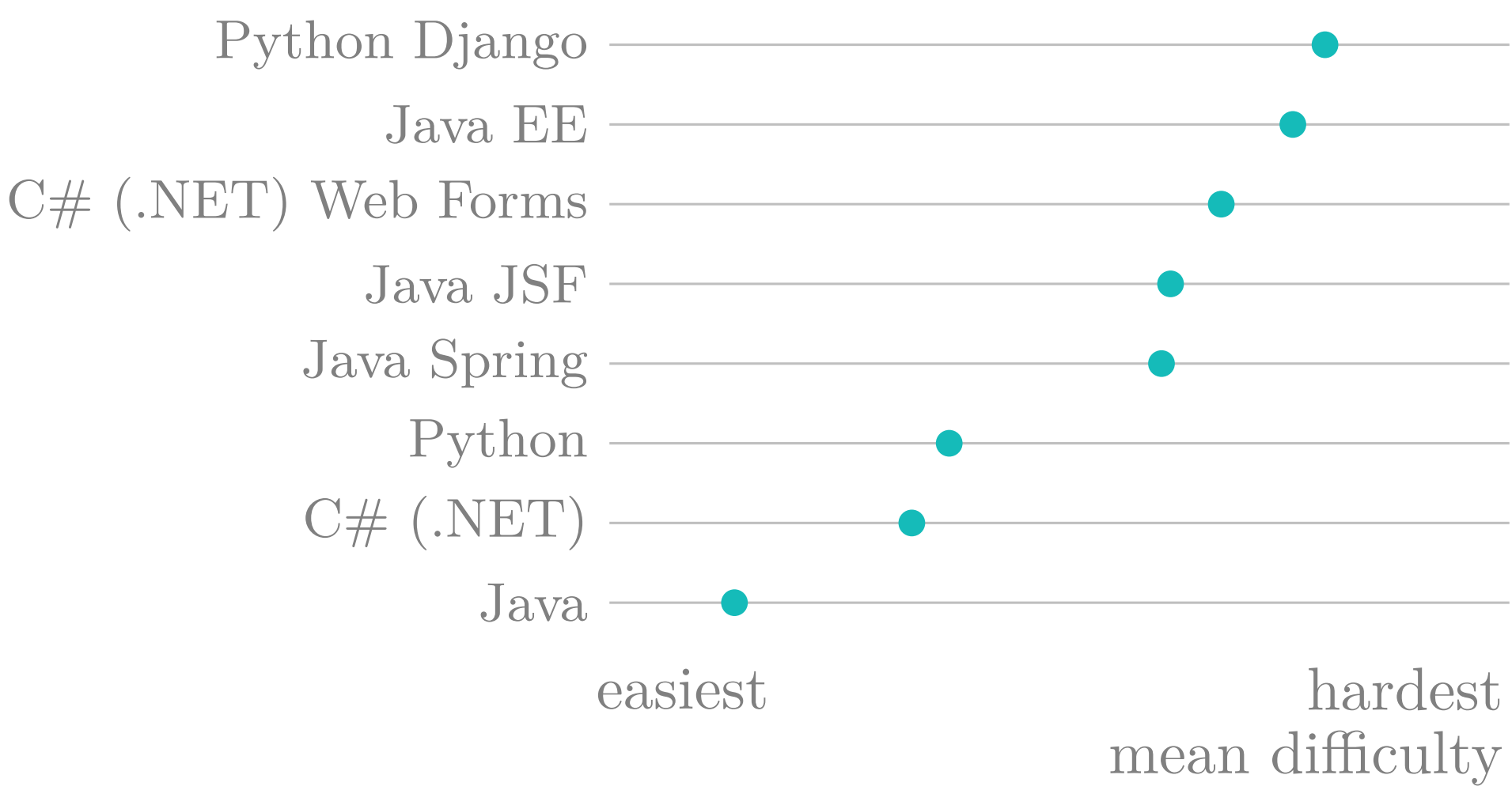

P_j
1
0.9
0.7
0
$d_j = 1$
$d_j = 0.9$
$d_j = 0.7$
θ

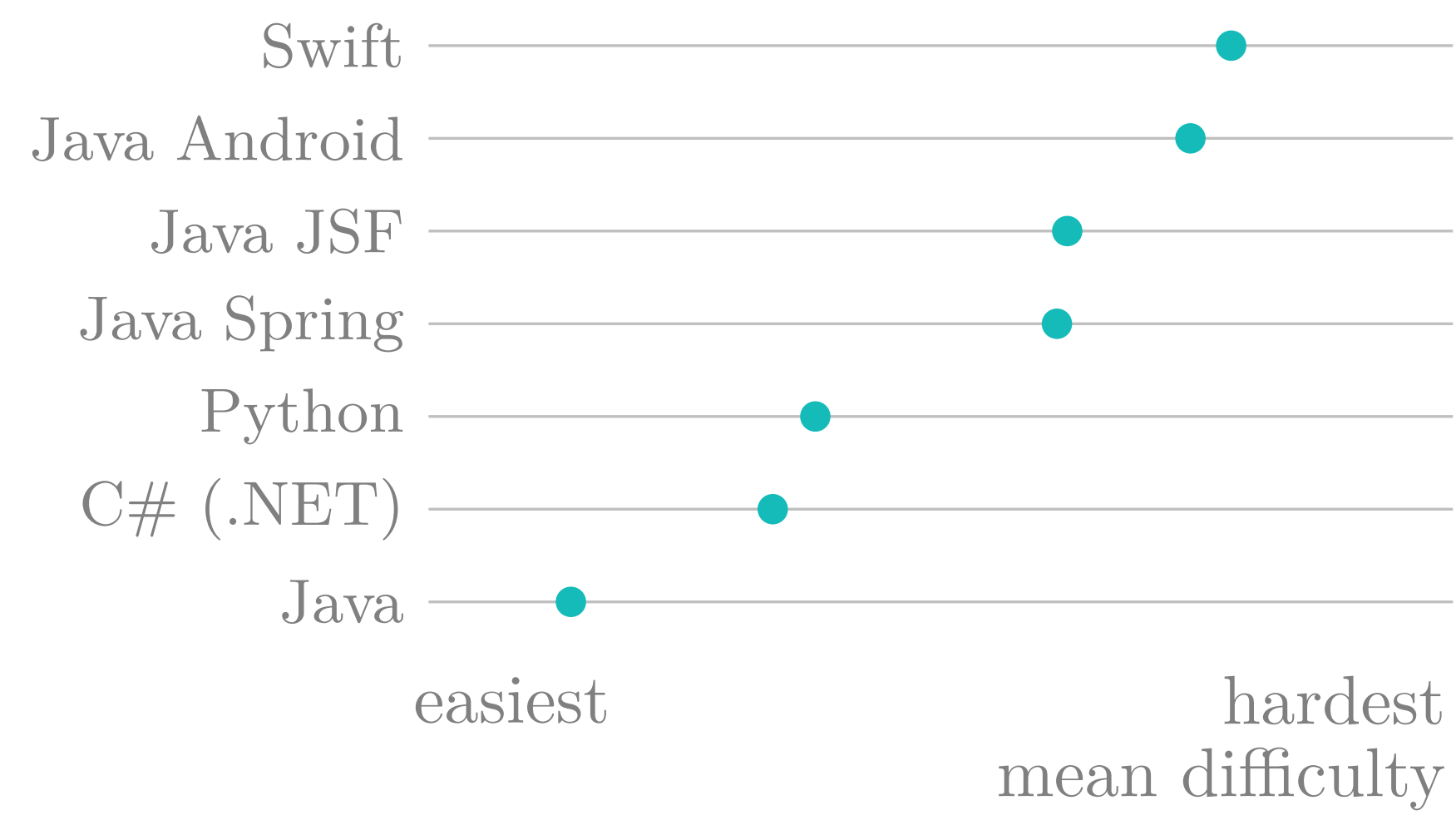

Poor authorization
Business logic flaws
Cross site request forgery (CSRF)
Denial of service (DoS)
Code tampering
Insecure authentication (M)
Extraneous functionality
Cross site scripting (XSS)
Reverse engineering
Unintended data leakage
Insufficient transport layer protection (M)
Broken cryptography (W)
Access control
Insecure data storage
Sensitive data storage
Insecure authentication (W)
Information exposure
Memory corruption
Misconfiguration
Insufficient logging
Mass assignment
Unvalidated redirects and forwards
Broken cryptography (M)
Insufficient transport layer protection (W)
Improper platform usage
Use of vulnerable components
Session management
Injection flaws
XML external entity (XXE)
easiest
hardest
mean difficulty

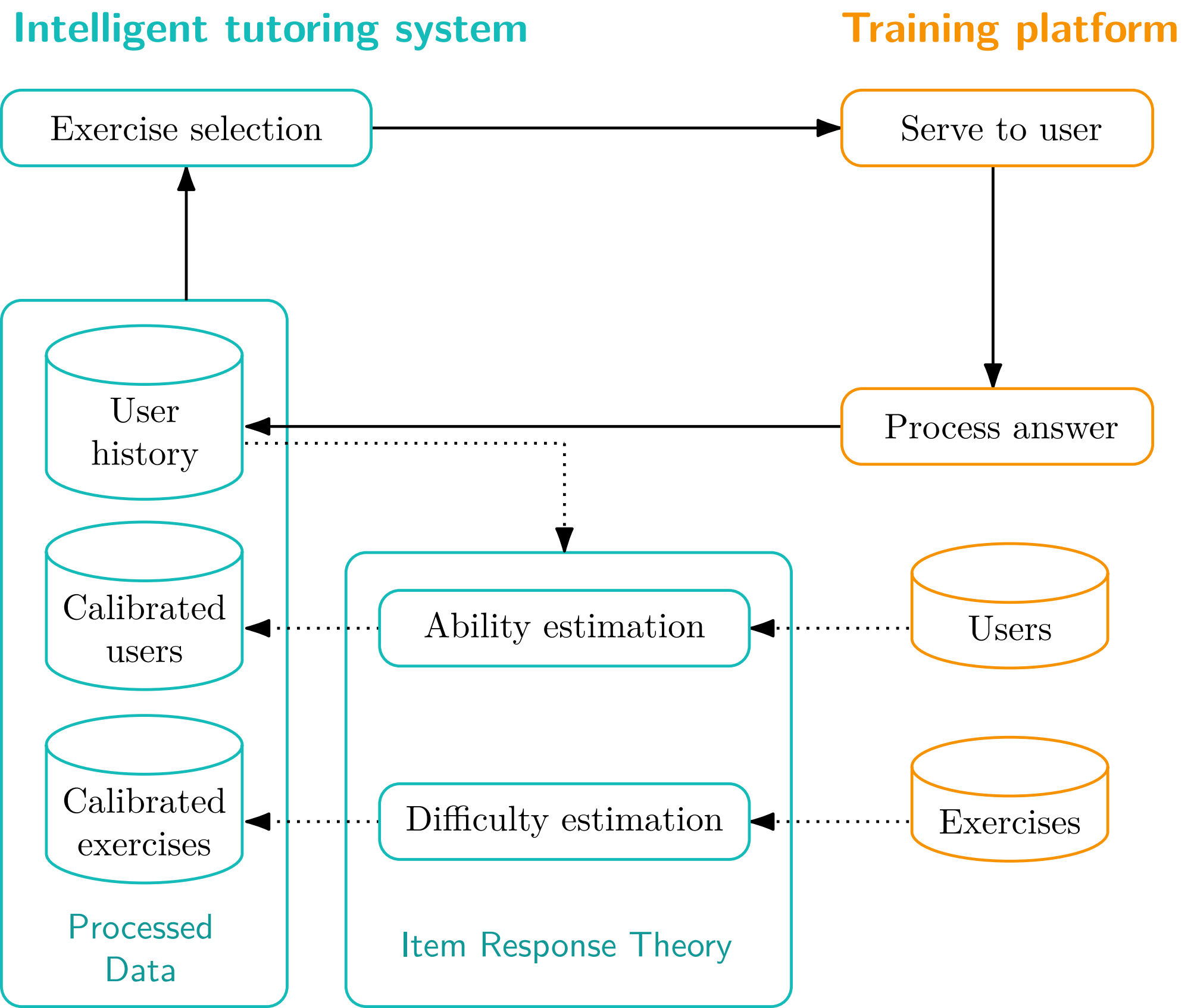

target
A B C D E F G H I J
j
0
1
2
3
4
5
i
affinity of $i = 0$
same affinity as $i = 0$
affinity for $j = B$ and $i \in \{2, 3, 5\}$
no data
enjoyable movie
boring movie

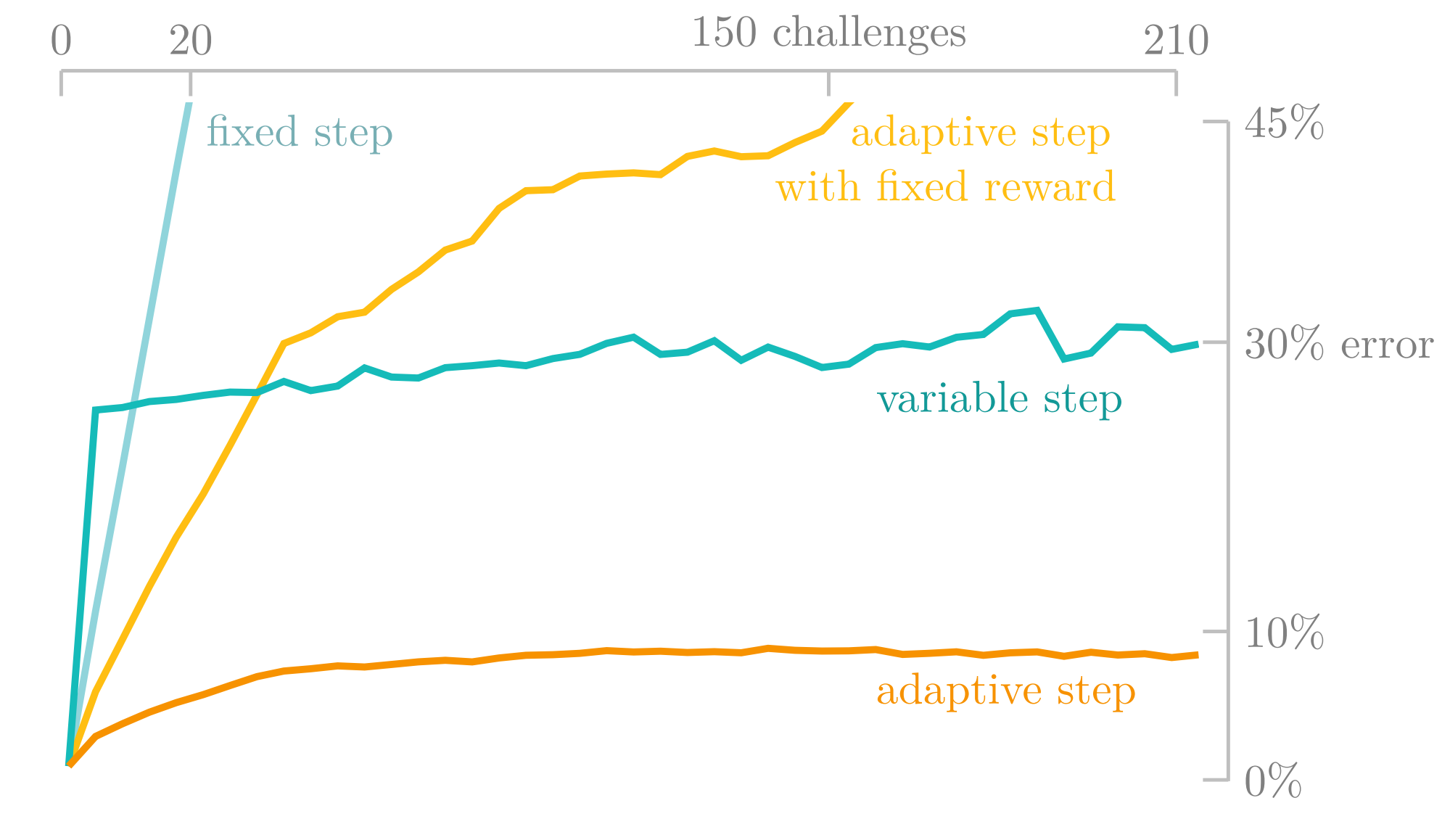

Cobol
Objective C iOS
C++
Python Django
Swift
JavaScript React
C
JavaScript Angular.io
Java EE
Java Android
Node.js Express
Kotlin
C# (.NET) Web Forms
C# (.NET) Core
Java JSF
Java Spring
C# (.NET) MVC
C# (.NET) Web API
PLSQL
Ruby Rails
Docker
Python
Pseudocode
C# (.NET)
Scala Play
PHP Symfony
Java EE API
Java
Terraform
Java Spring API
Python Flask
easiest
hardest
mean difficulty

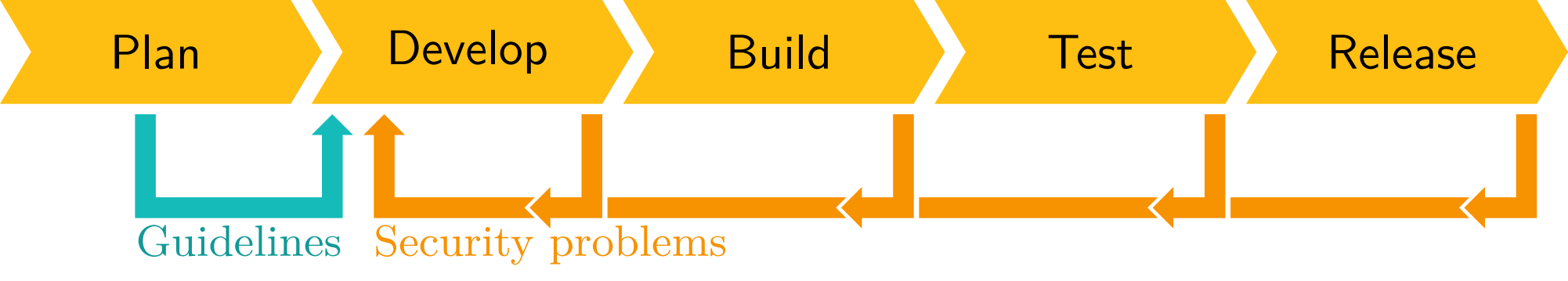

Cobol
C++
C
Python
C# (.NET)
Java
easiest
hardest
mean difficulty

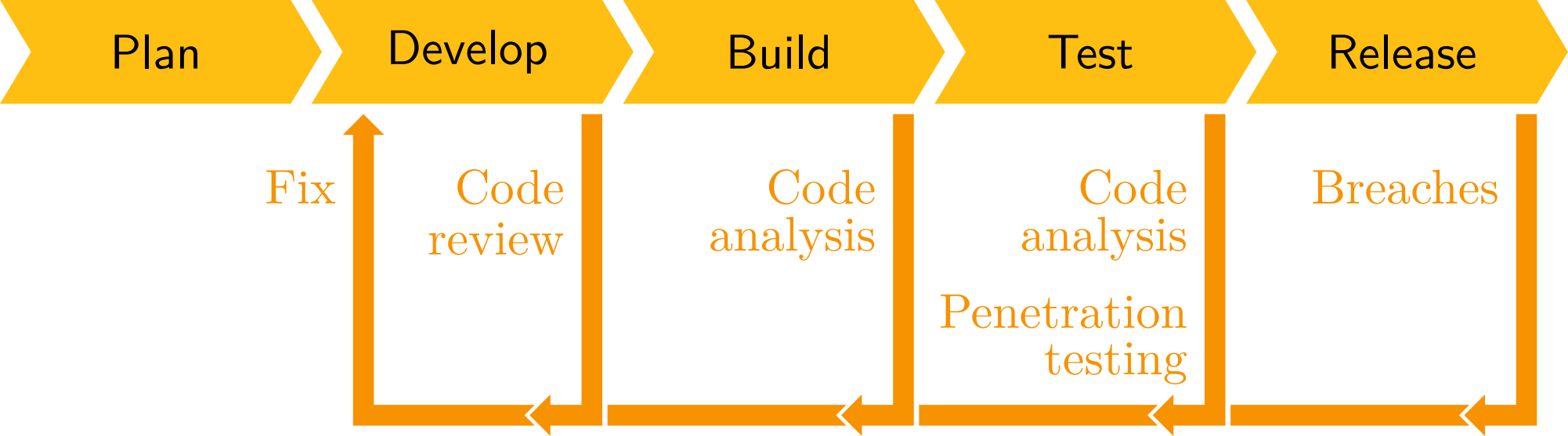

Python Django
Java EE
C# (.NET) Web Forms
Java JSF
Java Spring
Python
C# (.NET)
Java
easiest
hardest
mean difficulty


Swift
Java Android
Java JSF
Java Spring
Python
C# (.NET)
Java
easiest
hardest
mean difficulty

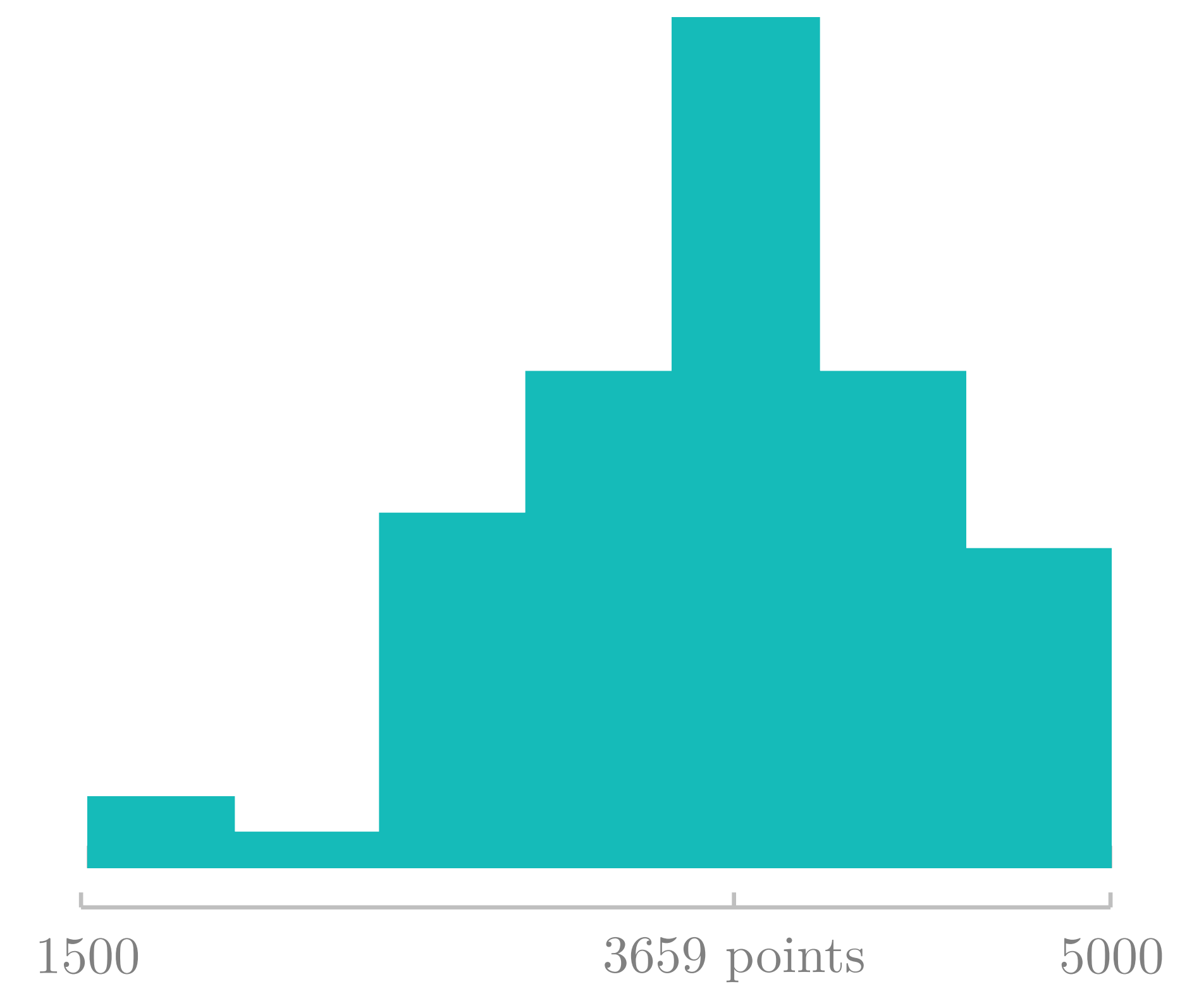

Intelligent tutoring system
Training platform
Exercise selection
Serve to user
User history
Process answer
Calibrated users
Ability estimation
Users
Calibrated exercises
Difficulty estimation
Exercises
Processed Data
Item Response Theory

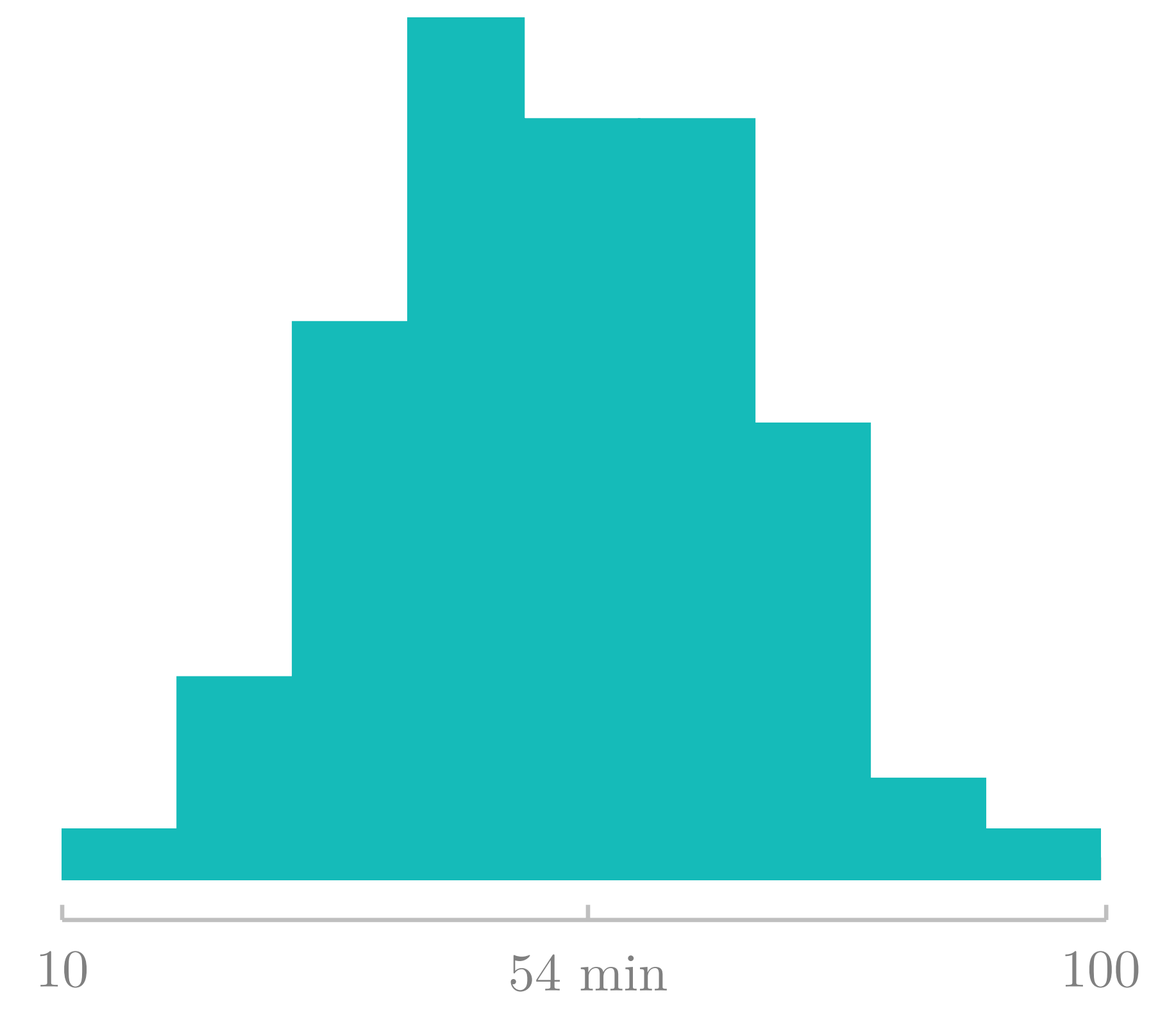

0
20
150 challenges
210
fixed step
adaptive step
with fixed reward
45%
30% error
variable step
10%
adaptive step
0%

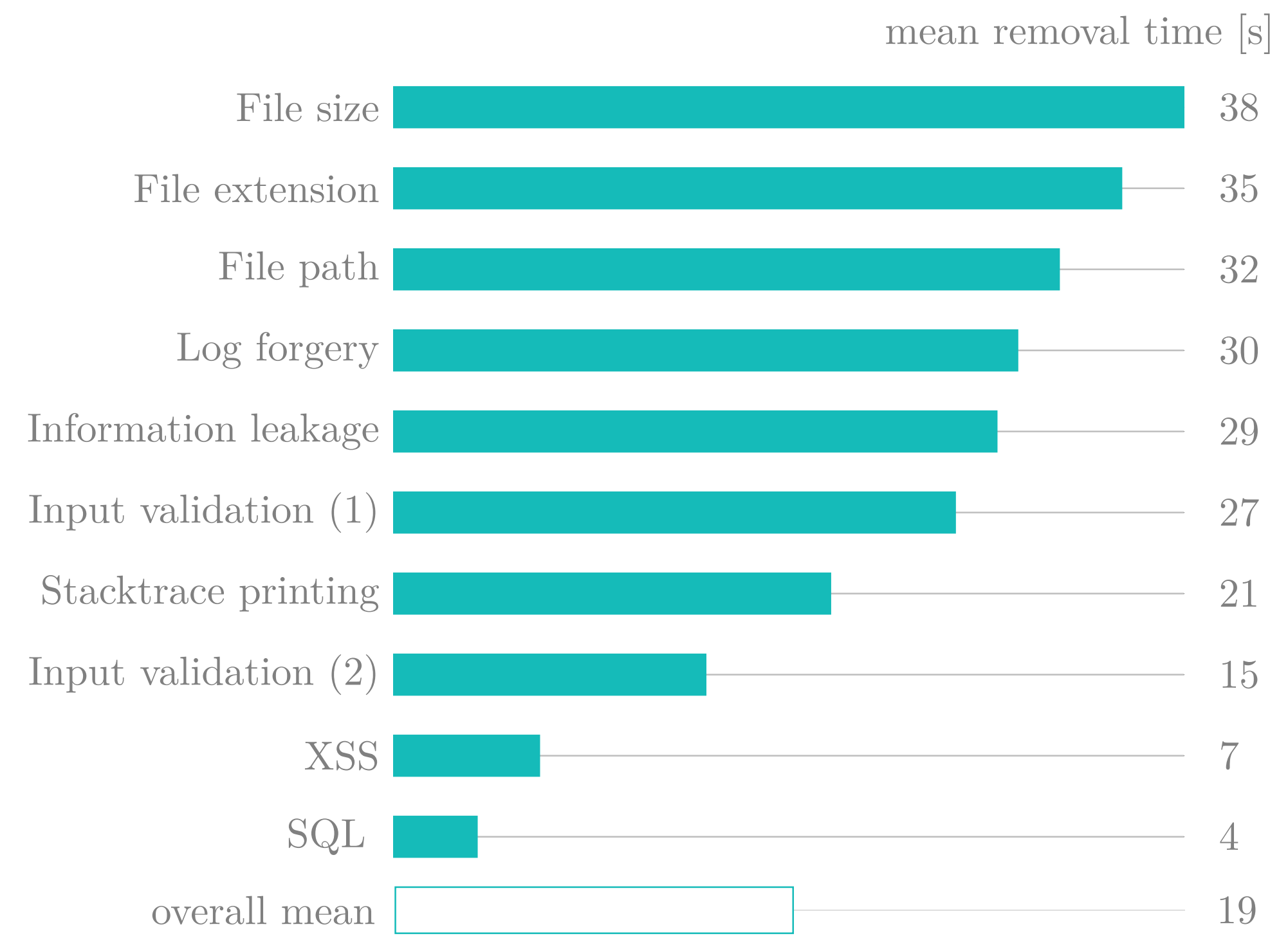

Plan
Develop
Build
Test
Release
Guidelines
Security problems

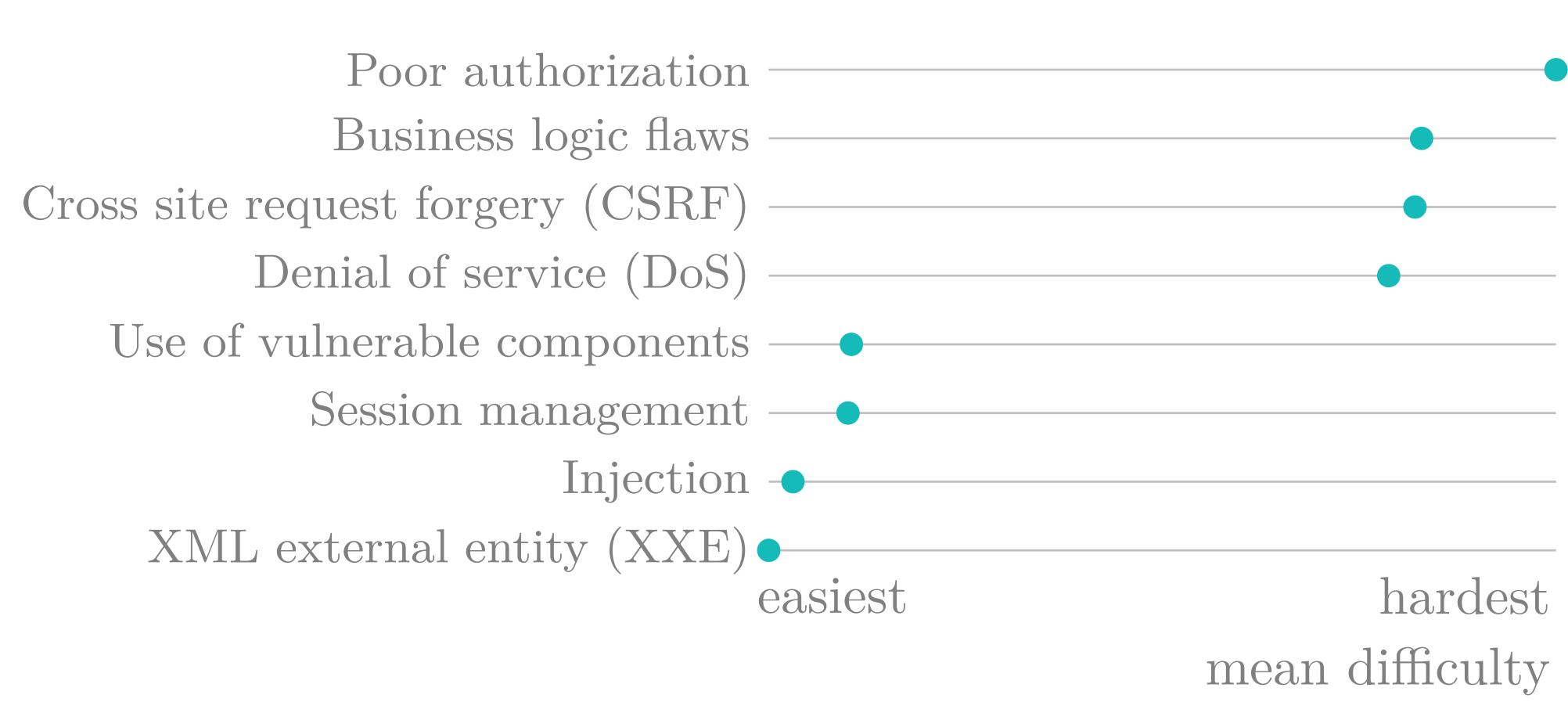

Plan
Develop
Build
Test
Release
Fix
Code review
Code analysis
Code analysis
Penetration testing
Breaches

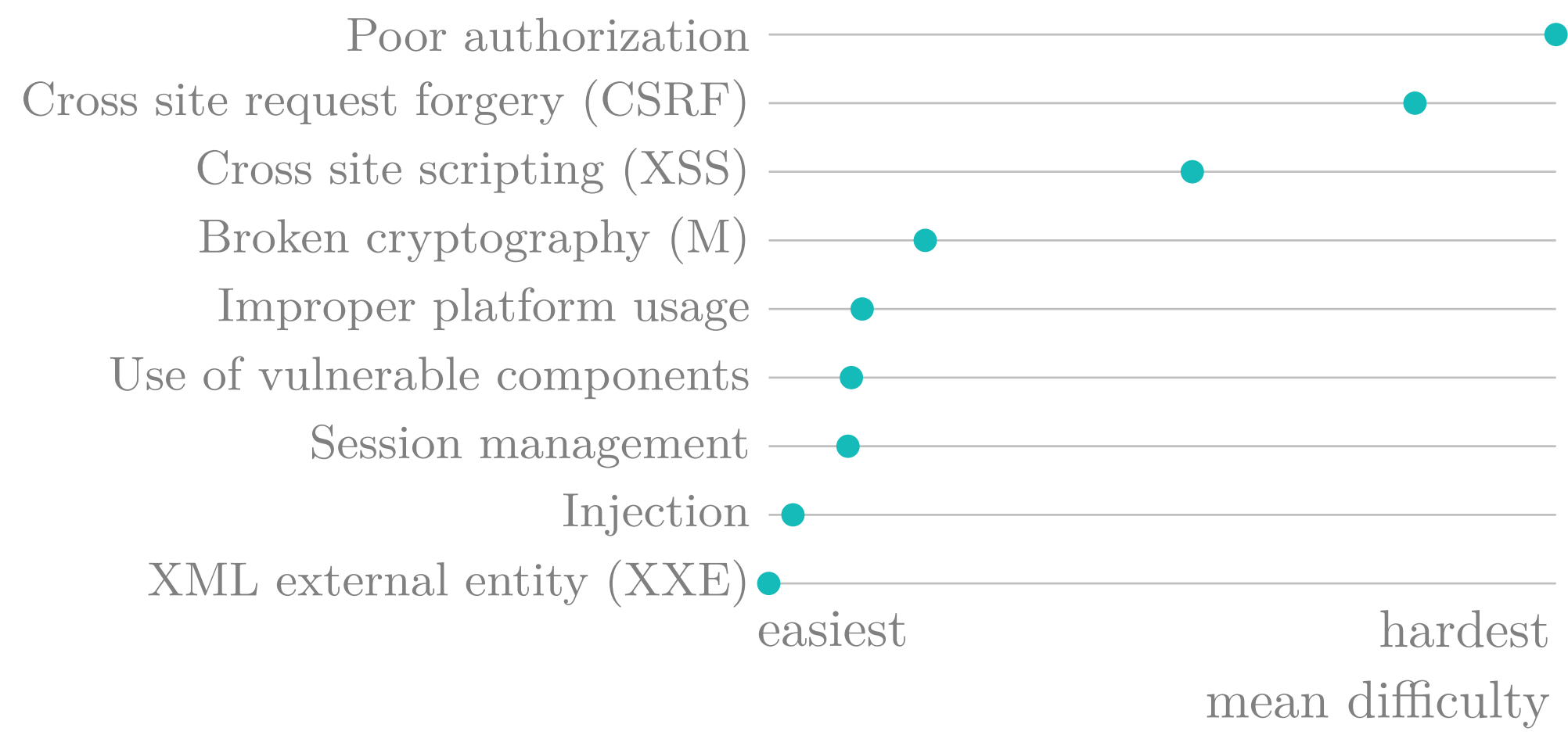
Plan
Develop
Build
Test
Release
Fix
Code analysis
Penetration testing
Breaches

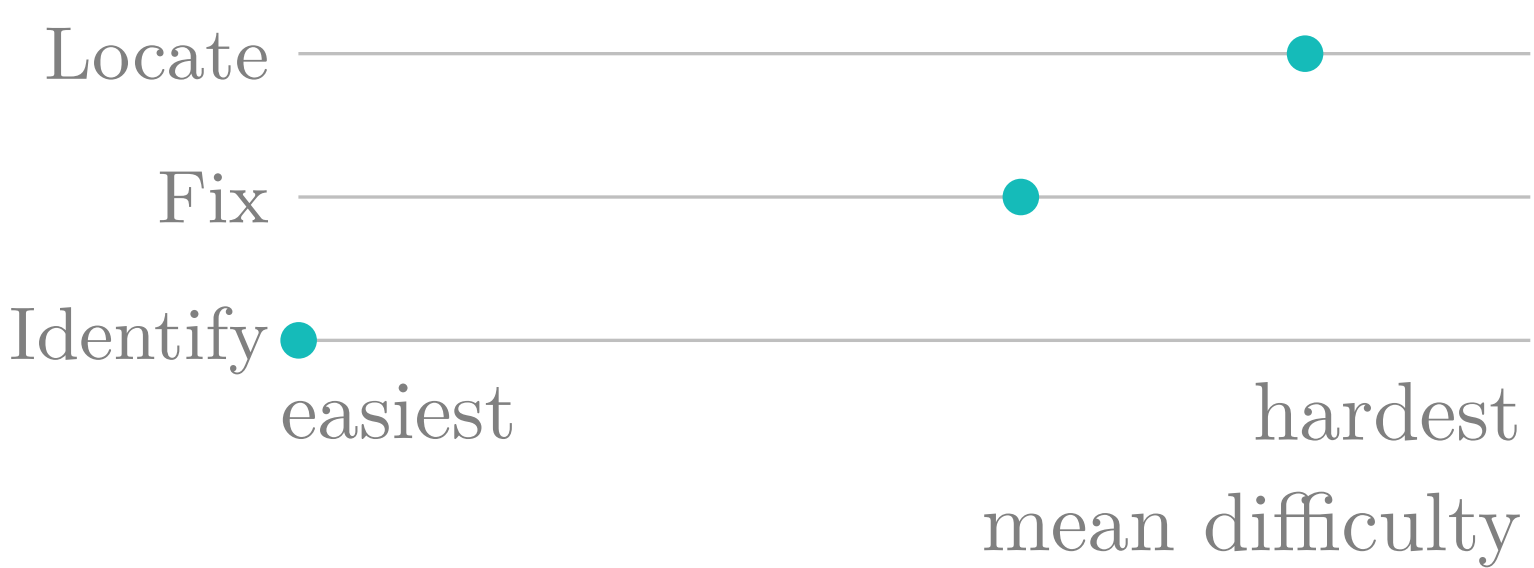

1500
3659 points
5000

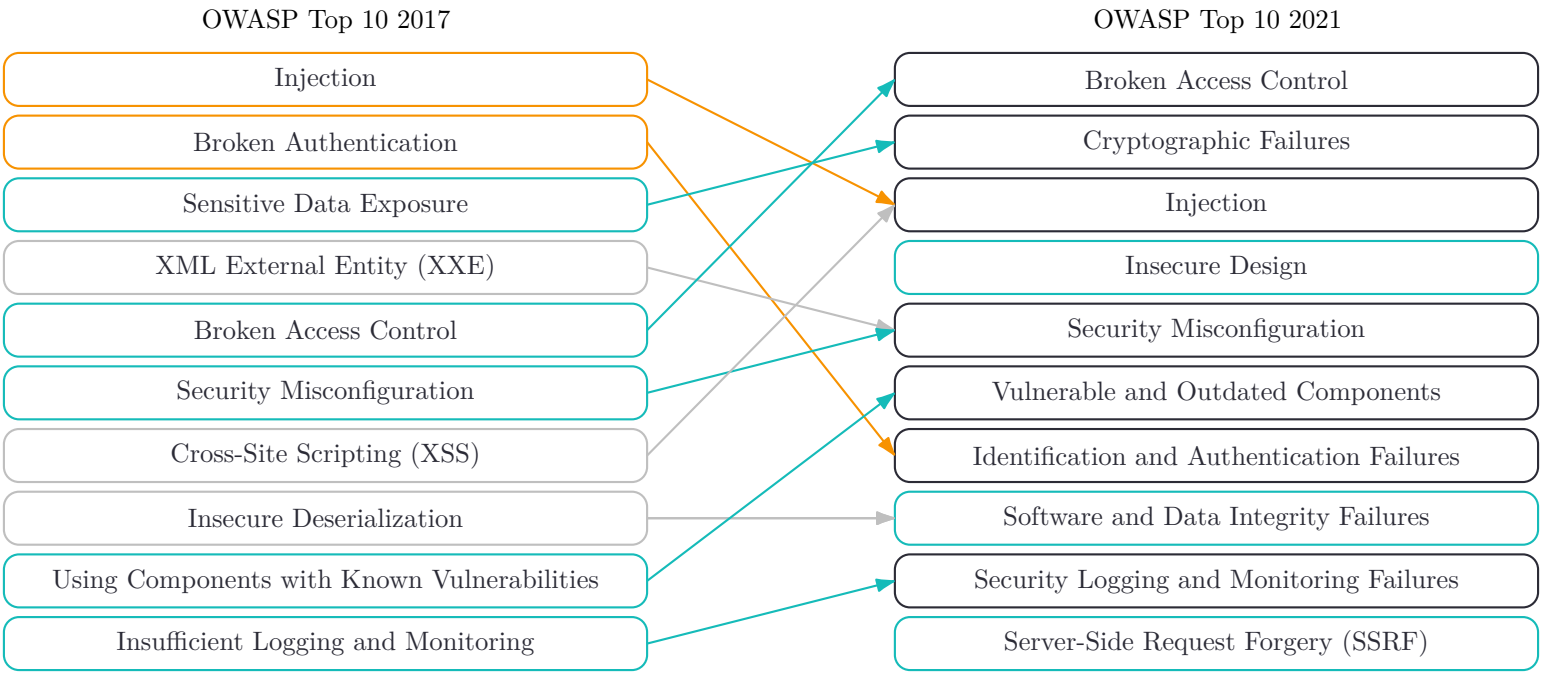

10
54 min
100


mean removal time [s]
File size
38
File extension
35
File path
32
Log forgery
30
Information leakage
29
Input validation (1)
27
Stacktrace printing
21
Input validation (2)
15
XSS
7
SQL
4
overall mean
19

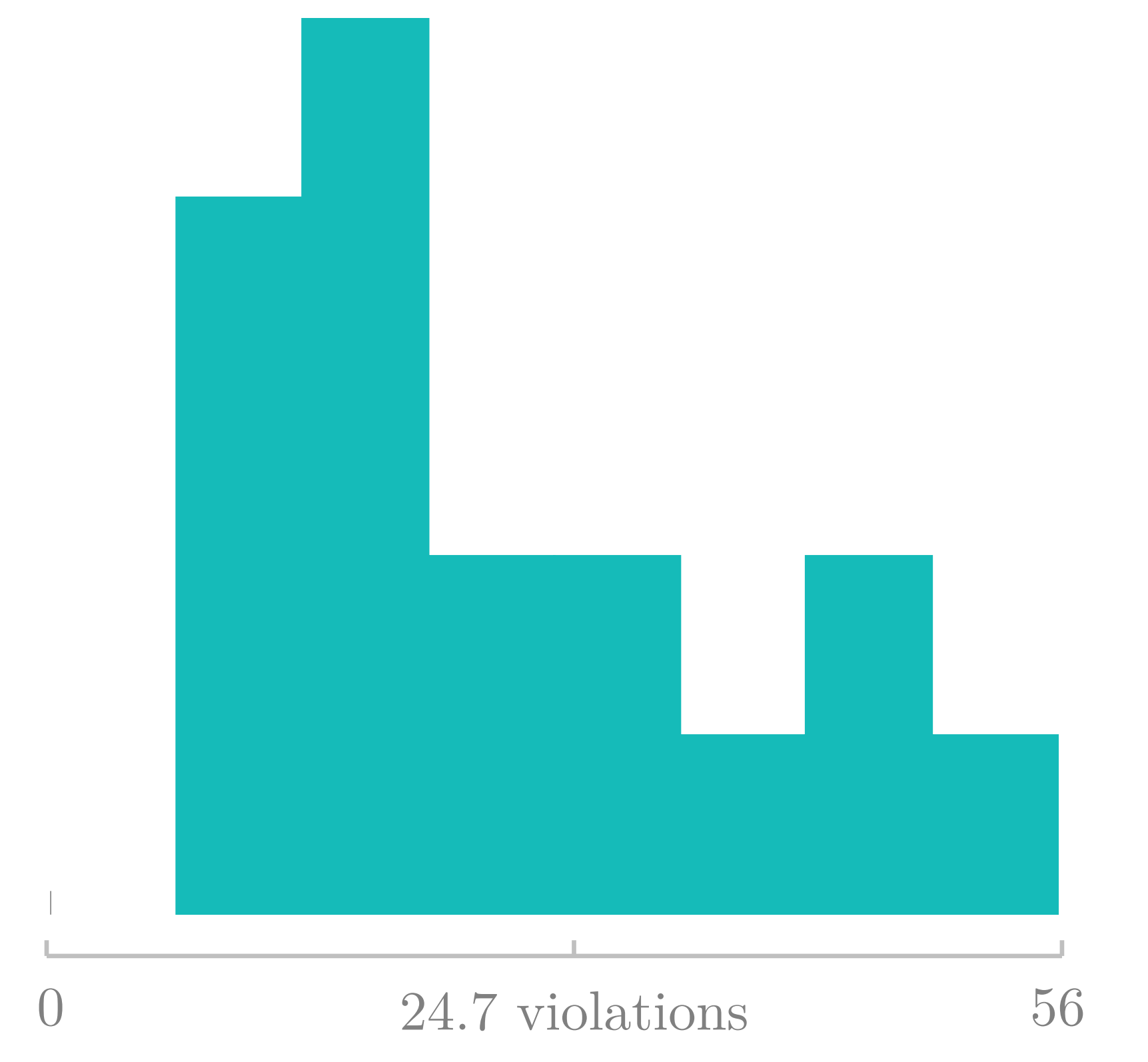

Poor authorization
Business logic flaws
Cross site request forgery (CSRF)
Denial of service (DoS)
Use of vulnerable components
Session management
Injection
XML external entity (XXE)
easiest
hardest
mean difficulty

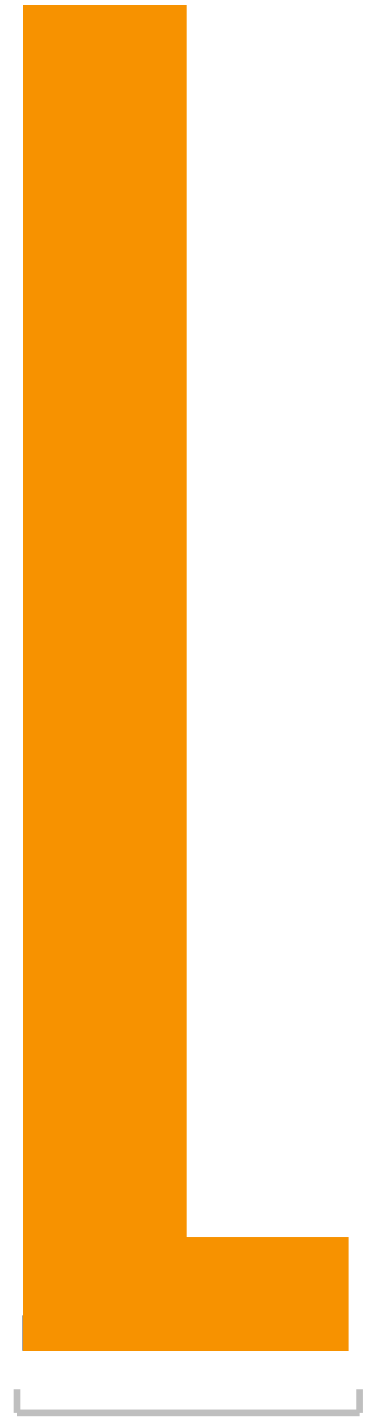

Poor authorization
Cross site request forgery (CSRF)
Cross site scripting (XSS)
Broken cryptography (M)
Improper platform usage
Use of vulnerable components
Session management
Injection
XML external entity (XXE)
easiest
hardest
mean difficulty


Locate
Fix
Identify
easiest
hardest
mean difficulty


OWASP Top 10 2017
Injection
Broken Authentication
Sensitive Data Exposure
XML External Entity (XXE)
Broken Access Control
Security Misconfiguration
Cross-Site Scripting (XSS)
Insecure Deserialization
Using Components with Known Vulnerabilities
Insufficient Logging and Monitoring
OWASP Top 10 2021
Broken Access Control
Cryptographic Failures
Injection
Insecure Design
Security Misconfiguration
Vulnerable and Outdated Components
Identification and Authentication Failures
Software and Data Integrity Failures
Security Logging and Monitoring Failures
Server-Side Request Forgery (SSRF)

0
17.6 violations
42


0
24.7 violations
56


0
6 violations

0
8.8 violations
27