Synthesizing Allowlists With RASPunzel

Runtime protection against deserialization vulnerabilities

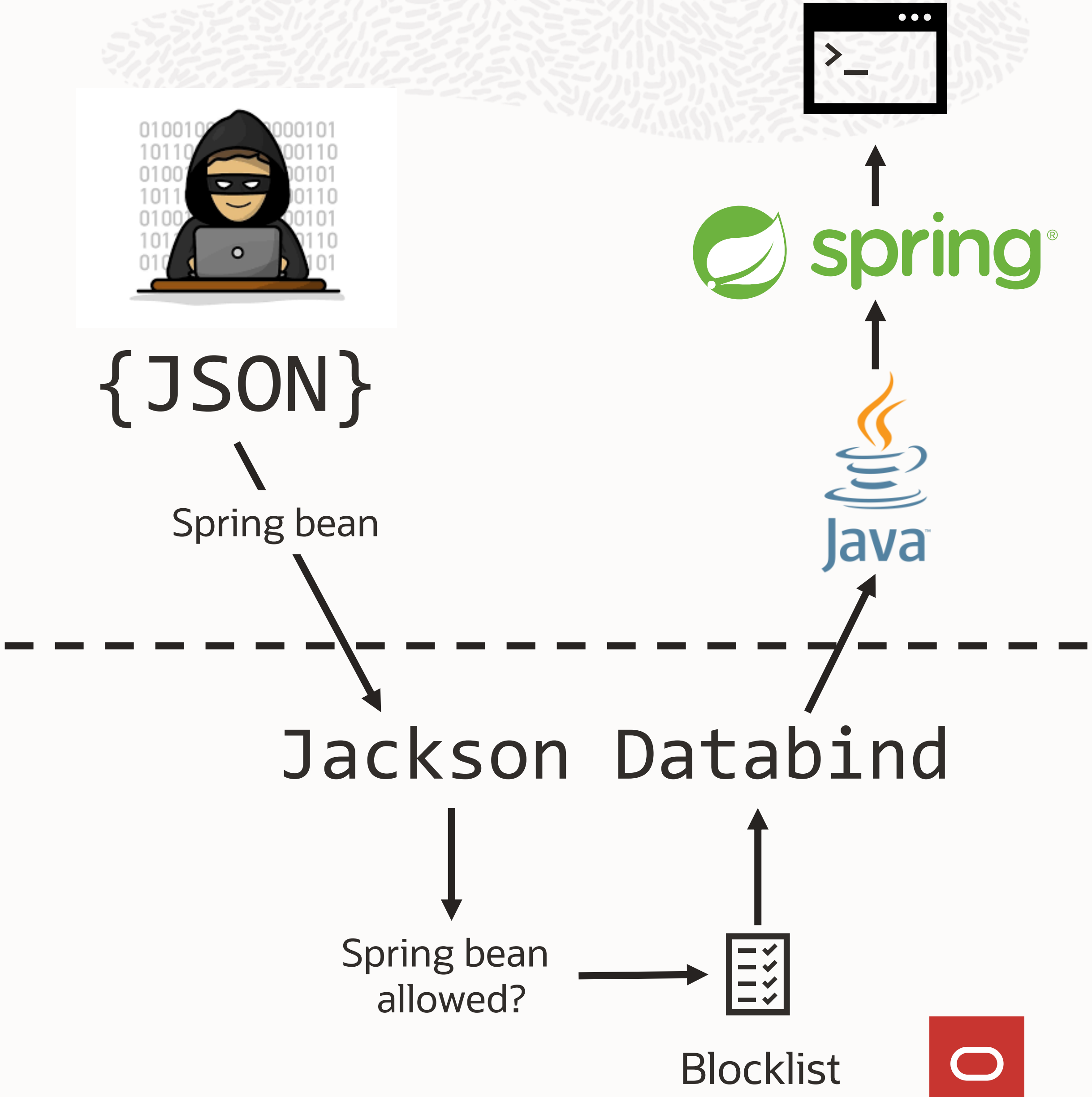
François Gauthier

Principal Researcher, Oracle Labs Australia

Deserialization Vulnerabilities Lead to Remote Code Execution

The Jackson Databind Use Case

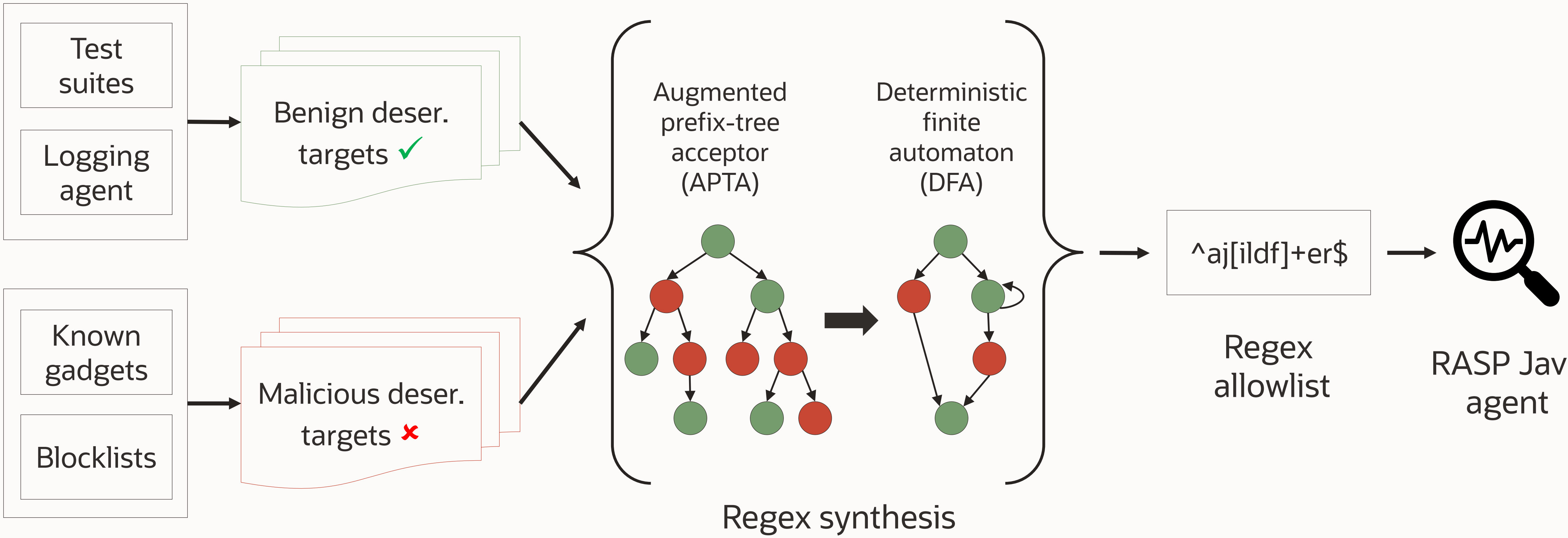
- JSON ↔ Java (de)serialization library.
- Enabling `defaultTyping` allows to specify the target deserialization class in JSON.
- Jackson Databind < 2.10 uses a blocklist to prevent deserialization attacks.
  - Blocklist evasion led to 40+ CVEs.
- **Best practice is to also use allowlists.**



RASPunzel

Synthesizing Allowlists

Data-driven Runtime Application Self-Protection (RASP)



Test suites

Logging agent

Benign deser. targets ✓

Known gadgets

Blocklists

Malicious deser. targets ✗

Augmented prefix-tree acceptor (APTA)

Deterministic finite automaton (DFA)

Regex synthesis

^aj[ildf]+er$

Regex allowlist

RASP Java agent

RASPunzel

RASPunzel demo:

1. Deserialization exploit (jackson-databind)
2. Allowlist synthesis
3. Runtime protection

francois.gauthier@oracle.com

https://labs.oracle.com/