JMSDigger

By

Gursev Singh Kalra – Senior Principal (@igursev)

McAfee, Foundstone Professional Services

gursev.kalra@foundstone.com

BlackHat Las Vegas - July 31, 2013

MESSAGING 101

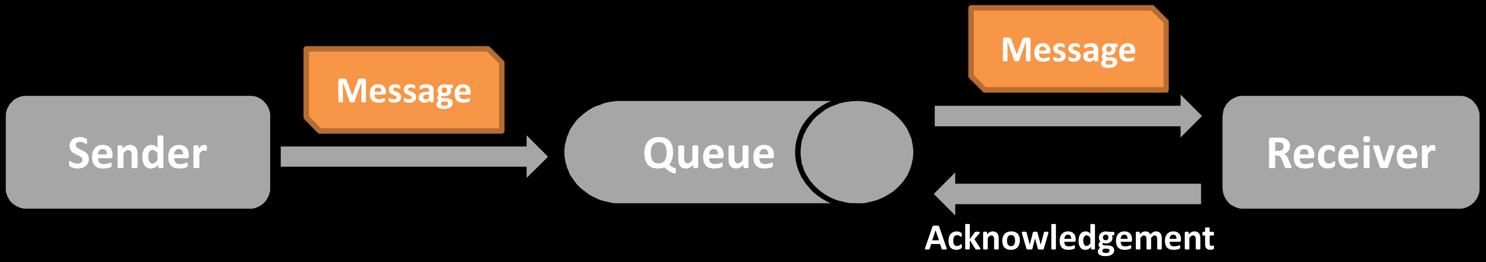
Messaging Infrastructure

- Clients
  - Send and Receive Messages
- Message Brokers
  - Route Messages
  - Provide JNDI interface
  - Administer Objects

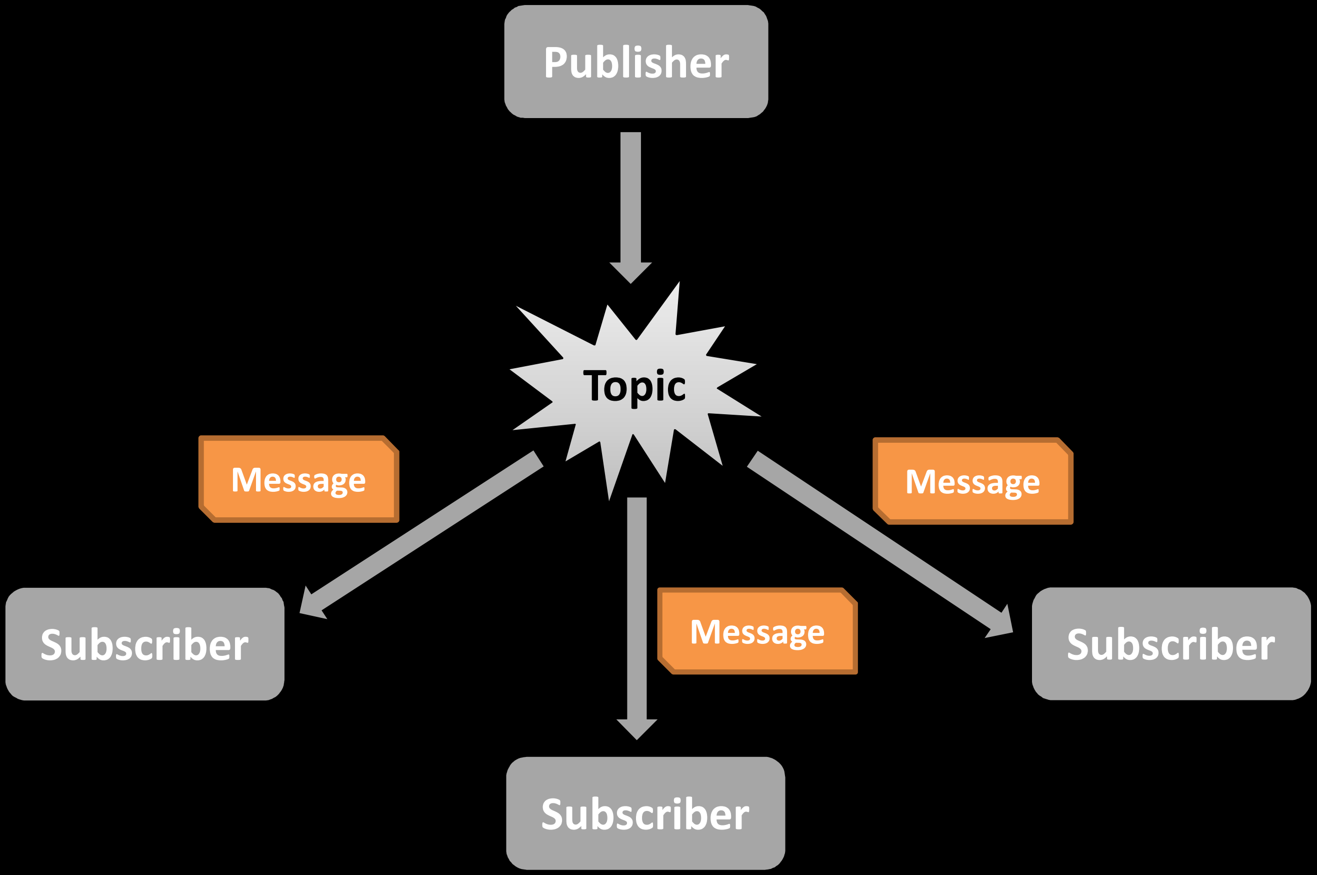
Messaging Topologies

- Point to Point
- Publish and Subscribe

Point to Point Domain



Publish/Subscribe Domain



Java Messaging Service

- An Enterprise Messaging API
- Supported by large number of Messaging Products
- Write once, Run everywhere
- Allows:
  - Heterogeneous Integration
  - High Scalability and Reliability
  - Asynchronous Operation

JMSDIGGER

Allows you to….

Verify a Broker Configuration

- Initial Context Factory Class
- Connection Factory Names
- Provider URL
- Username + Password
- Validate

Test Authentication

- Single Credential Check
- Credential Bruteforce
- Demonstration

Perform ActiveMQ Specific Operations

- Create Destinations
- Query Statistics
- Decrypt ActiveMQ Password
- Demonstration

Extract Data From Destinations

- Queues
  - Every Message can be consumed once
- Dump Queues and Topics
- Extract Contents of Durable Subscribers
- Demonstration

Manipulate Durable Subscribers

- Create
- Erase
- Demonstration

View its source

https://github.com/OpenSecurityResearch/jmsdigger

?

THANK YOU