FFI Forsvarets forskningsinstitutt

Employing Web services between domains with restricted information flows

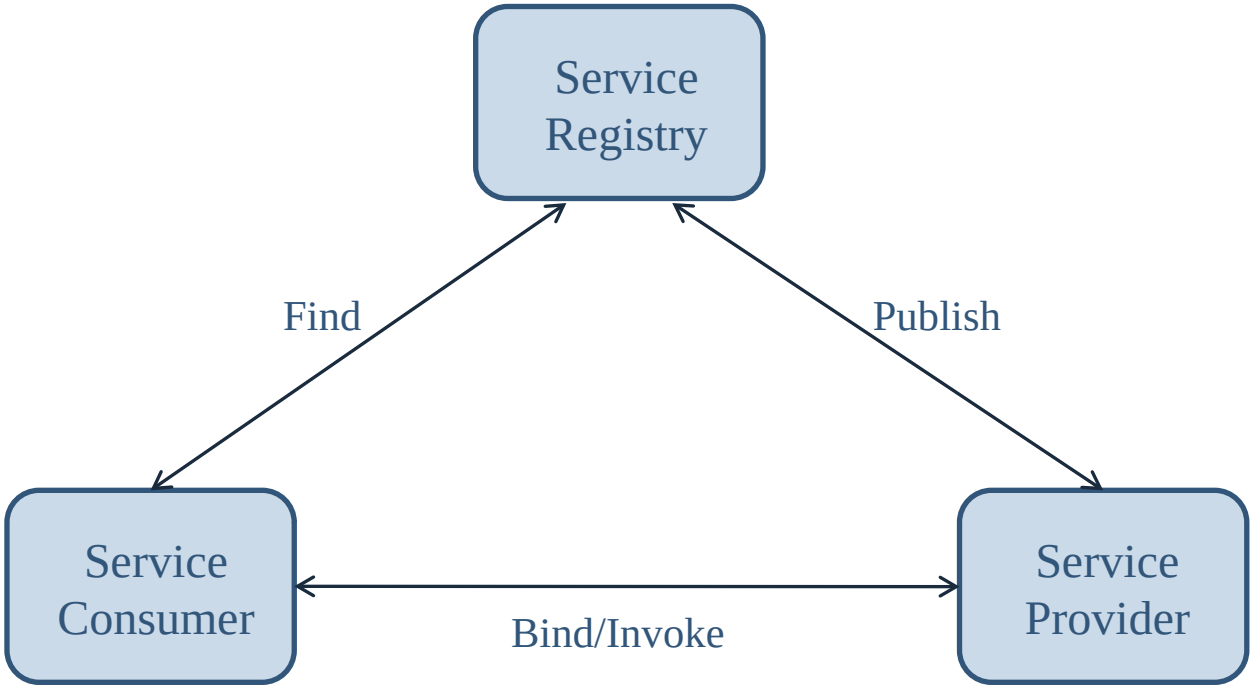
16th ICCRTS
Paper 080
June 23rd, 2011

Trude Hafsøe
trude.hafsoe@ffi.no

Background

- Web service are being introduced into military systems
  - Security solutions are being developed
- Web services will (at least for now) have to co-exist with information diodes
- Web services communication is based on two-way communication patterns
  - Which patterns can be adapted to work in a one-way scenario?
  - Which modifications are required on the Web service level?

SOA Elements



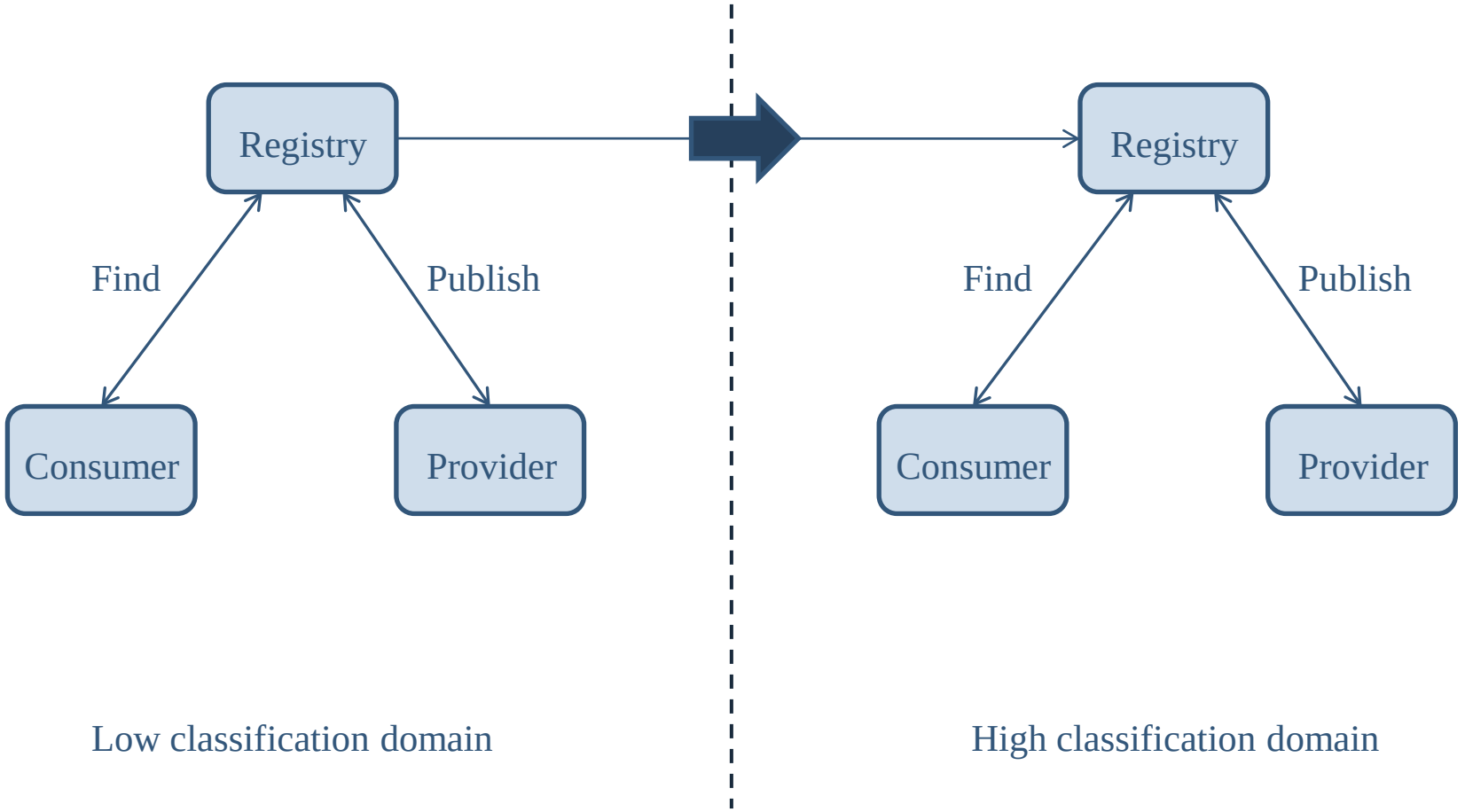
Protocol considerations

- Web services use SOAP messages, expressed in XML
- Transport agnostic, but standard bindings exist
  - The most common transport binding is HTTP over TCP, which is connection oriented
  - A standardized alternative is SOAP over UDP

Service Discovery

- Stand-alone registries
  - Publish and search
- Federated registries
  - Publish and search
  - Replication and/or federated search
- Distributed service discovery
  - Service advertisements
  - Probes

Service Discovery - Registries



Service Discovery - Distributed

- Consumers and providers communicate directly
  - Providers send service advertisements, which consumers can cache
  - Consumers can send probes to query for services, and providers respond to these directly

- Distributed service discovery is mostly used for run-time discovery
  - Knowledge of services that can’t be invoked directly is of limited value

Service Invocation

- Request/Response
  - The consumer initiates the communication by sending a request
  - The information content is supplied by the provider, which sends this information back in the response
  - Since the communication must be initiated by the client, while the main content is in the reply, doing request/response across a diode has limited usefulness

Service Invocation

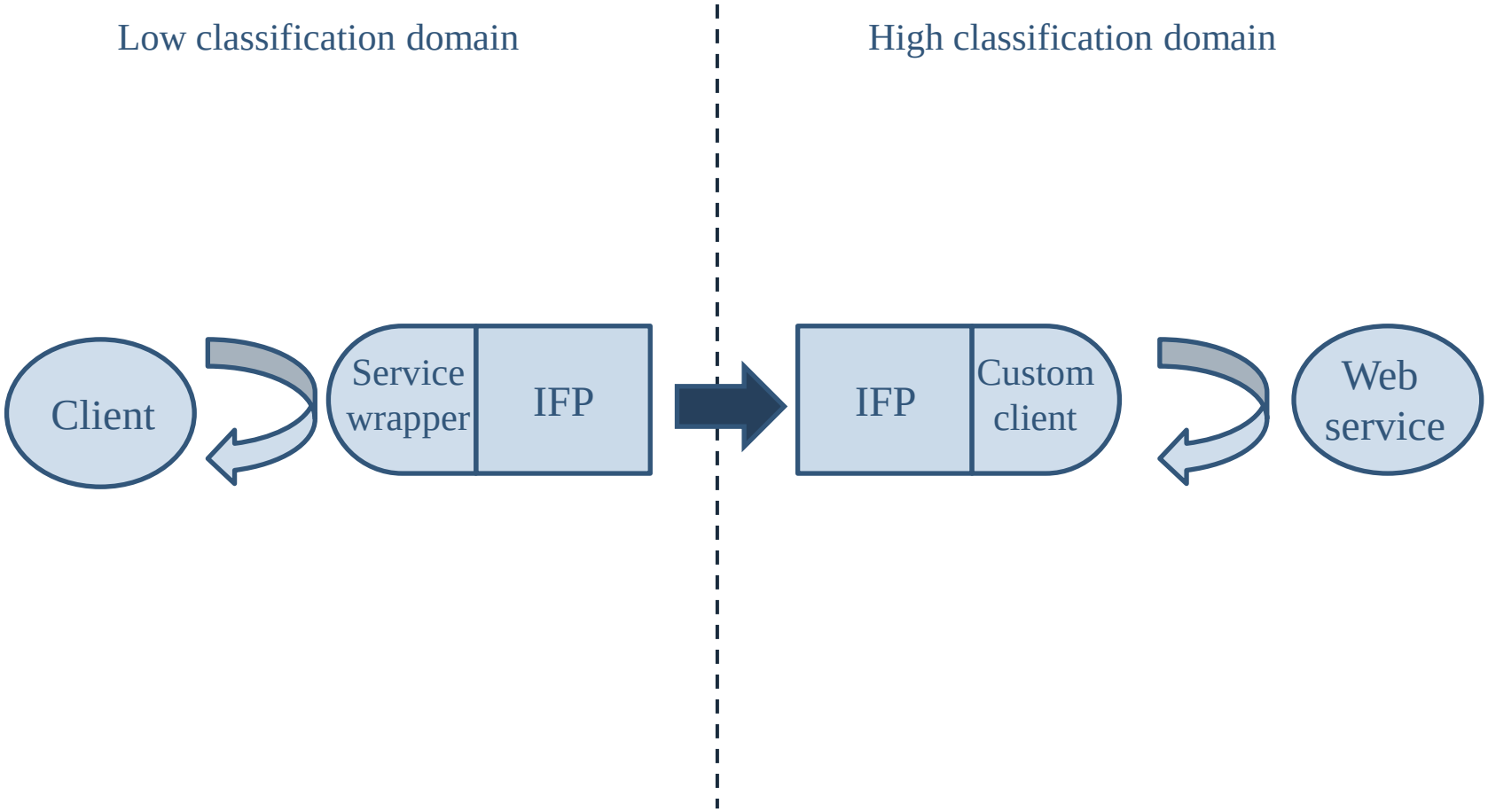
- Publish/Subscribe
  - First a subscription request is sent from the consumer to the provider
  - The provider then sends notifications to the consumer
- Both subscriptions and notifications can be sent either directly between consumer and provider, or via a broker
- The WS-Notification standard allows for third parties to initiate subscriptions on behalf of others

Proof-of-concept test

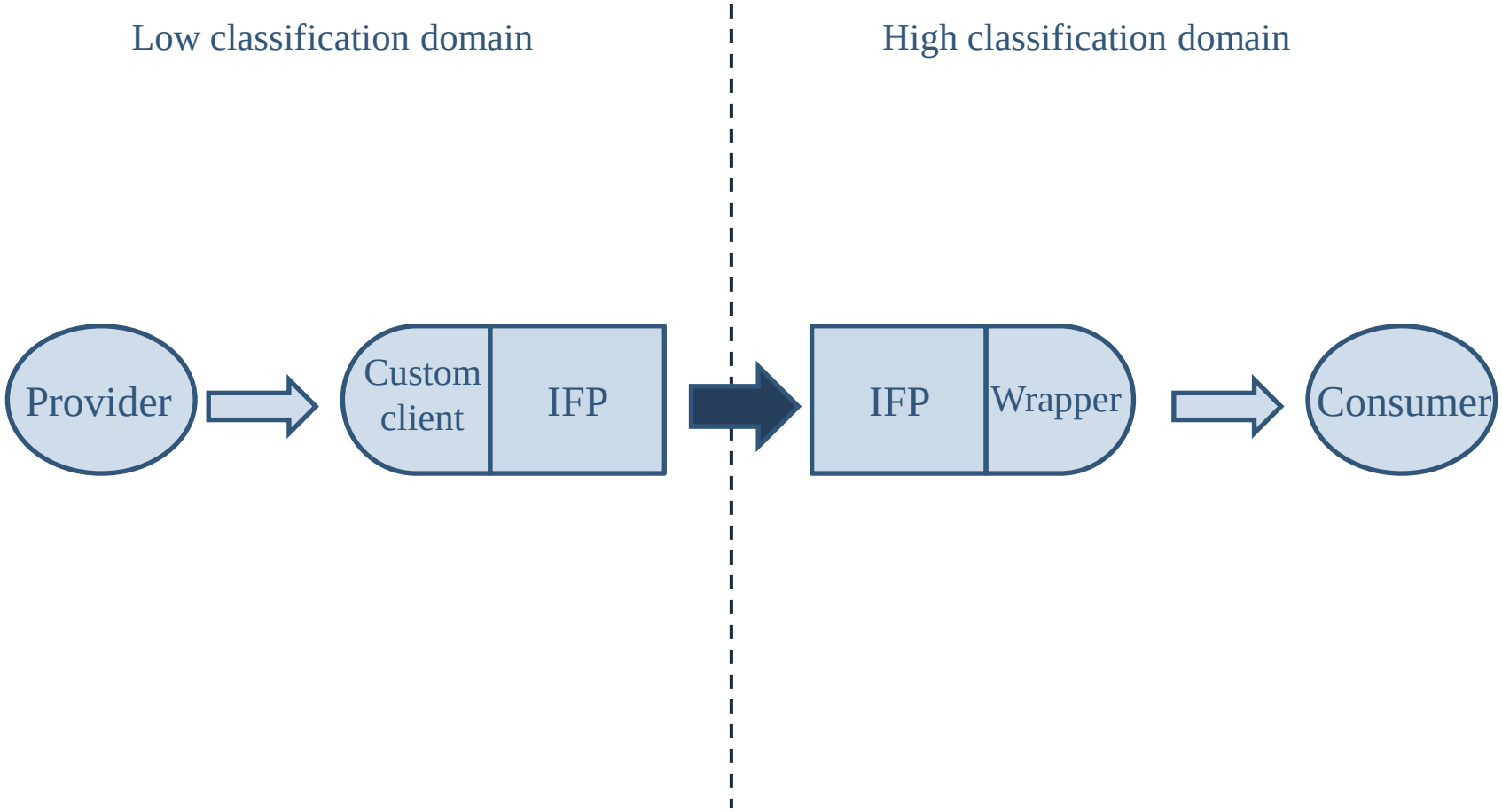
- Uses an Information Flow Proxy (IFP)
  - Proprietary information diode and software
  - Simple configuration (file-based)

- Aims to allow the use of unmodified Web services and Web service clients

Implementation



Publish/Subscribe



Summary

- Web service technology is based on two-way communication
  - Simple modifications allow some communications patterns to function one-way as well
- The notification part of publish/subscribe is the most useful candidate
  - Requires subscriptions to be initiated using other means
- Replication between registries, and service advertisements can be supported
  - Limited value unless the service information is intended for planning/development use