Comparison of Security Layers for Store and Forward Scenarios

William R. Soley

SunSoft

Problem

Various security protocols exist at different layers in the OSI framework.

- **may be confusing**
- **implementing at the wrong layer may be:**
  - **weak**
  - **inefficient**
  - **difficult to administer**

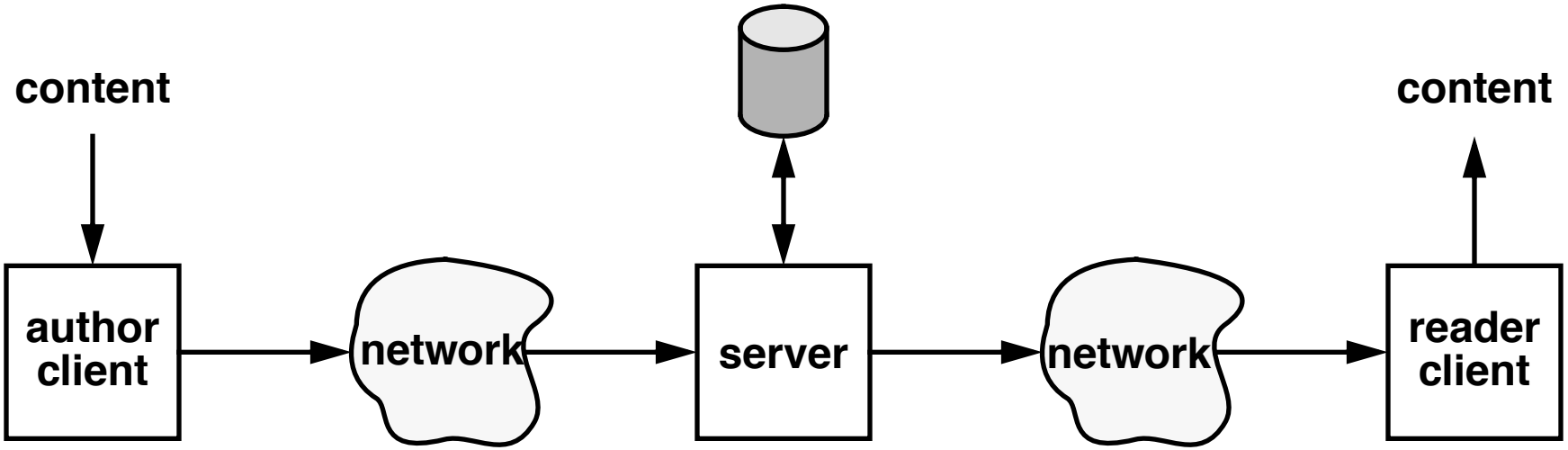
Solution

Select a protocol which operates at the layer which best meets the policy requirements of the application being protected.

- **the best solution for application *A* may not be the best for application *B***
- **in some cases, the best solution may combine more than one security protocol** (*e.g.* application-layer signature on content with transport-layer encryption for privacy)

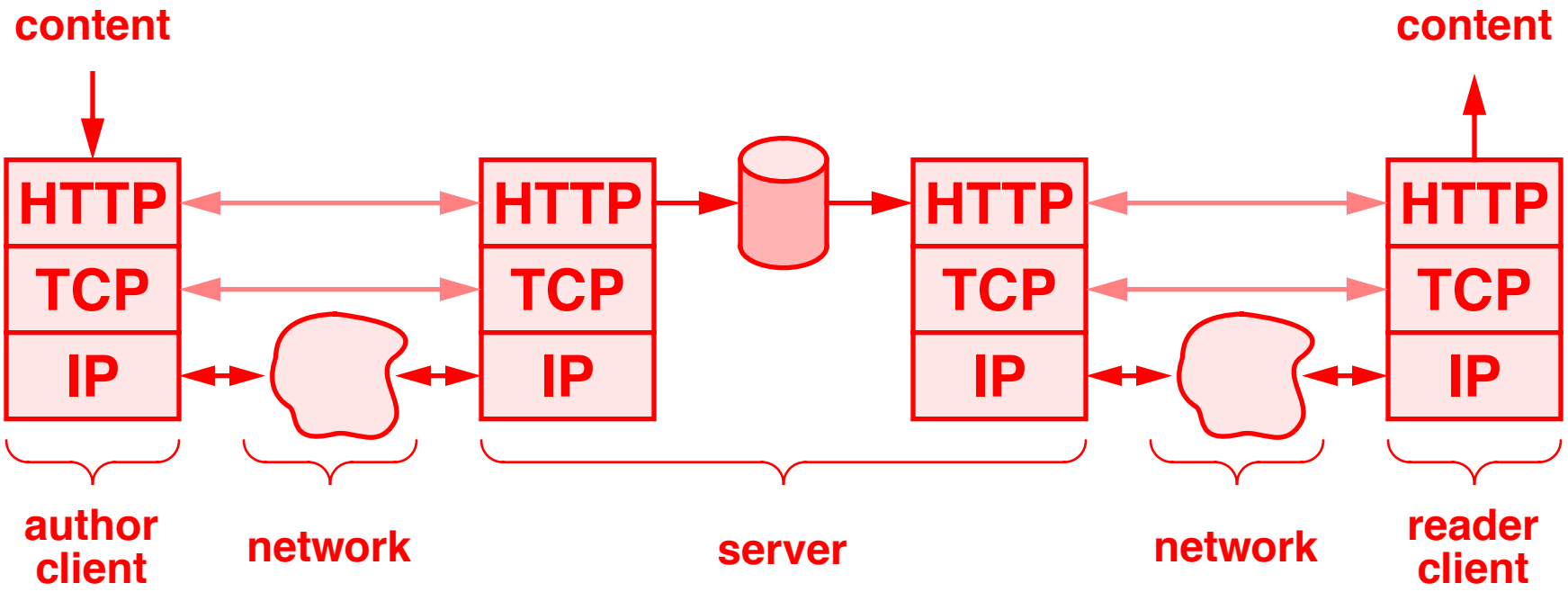
Sample Scenario

Store and Forward Server



sun microsystems

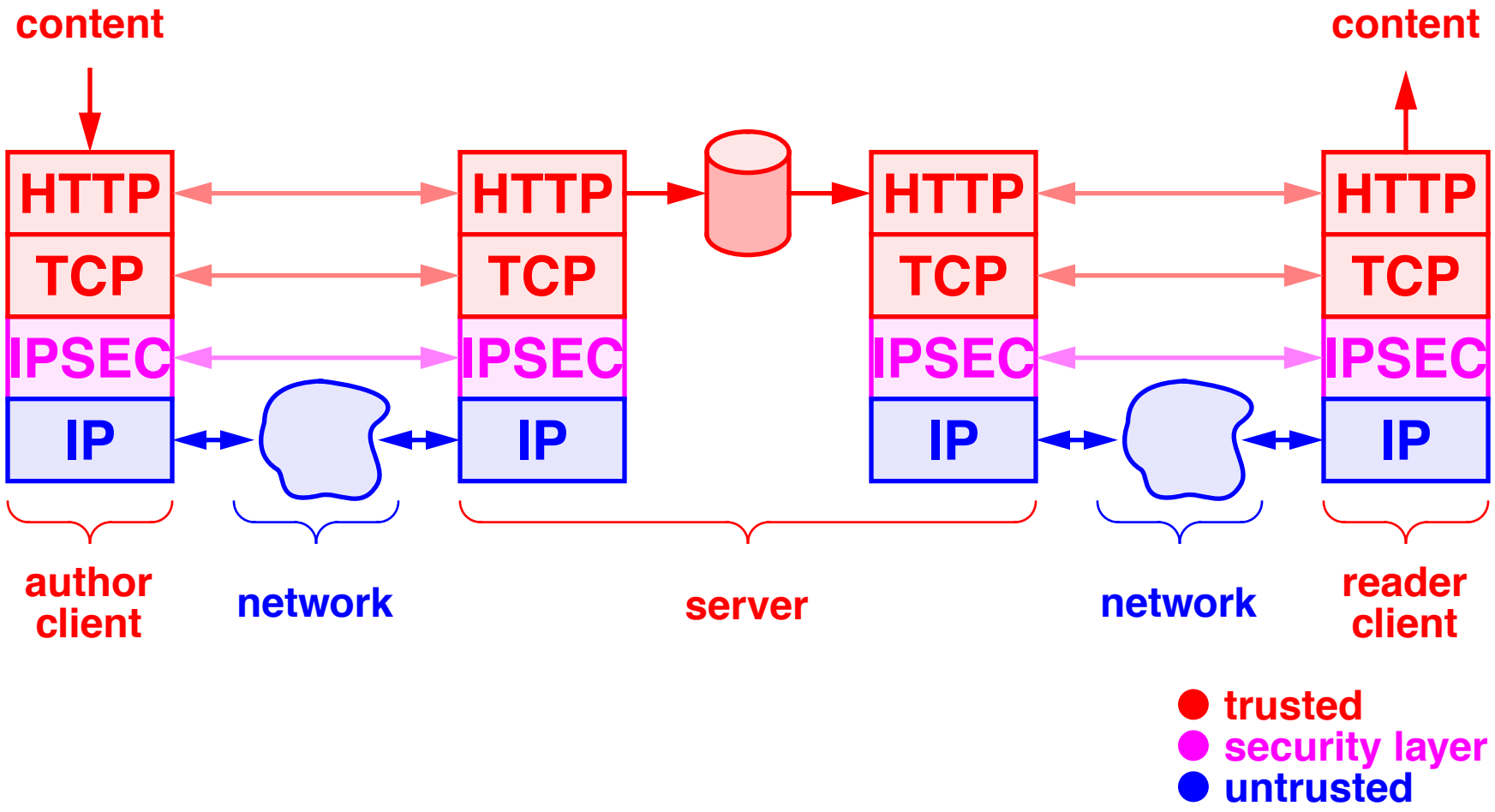
No Security



- trusted
- security layer
- untrusted

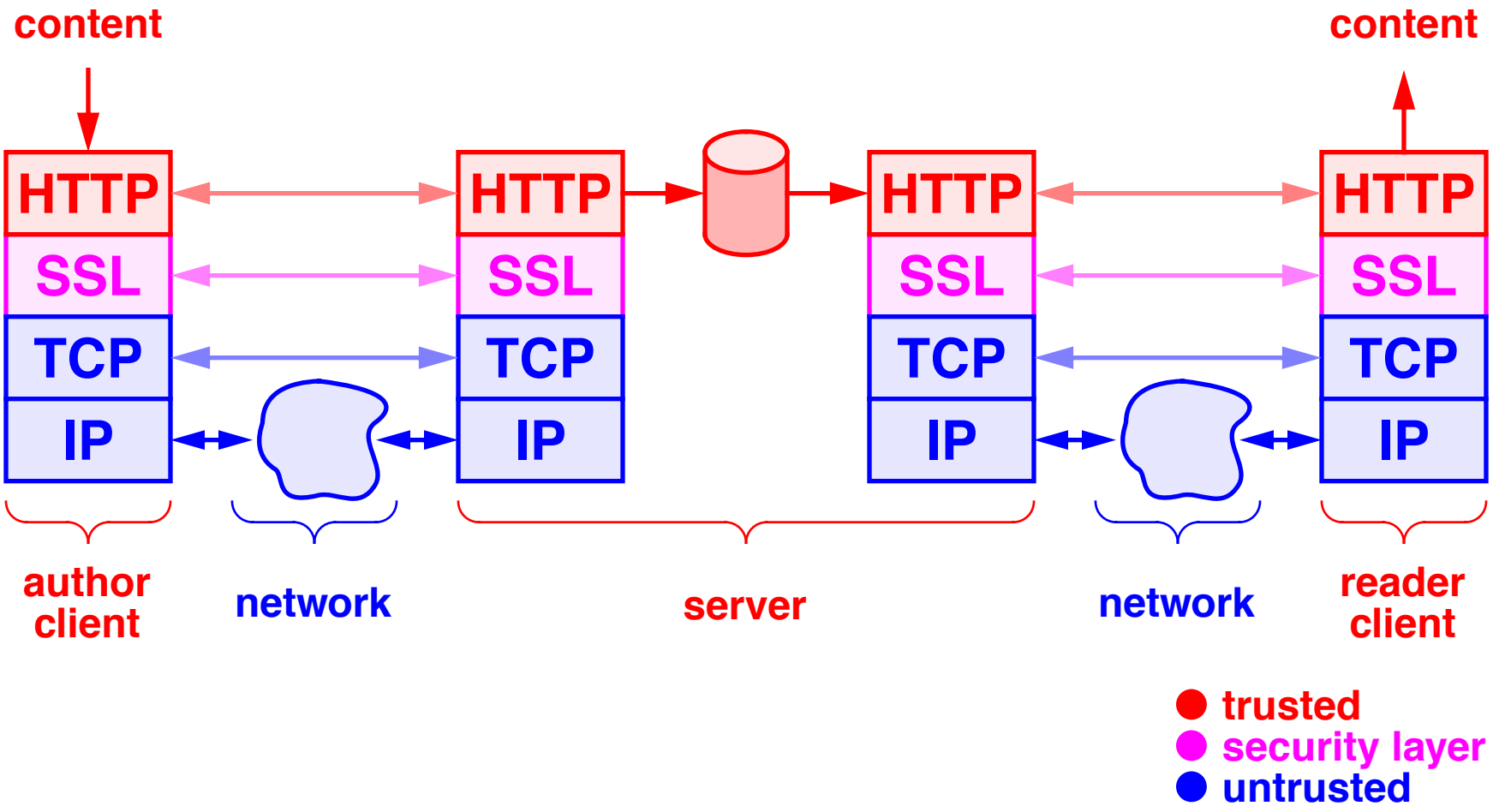
sun microsystems

Network Layer Security



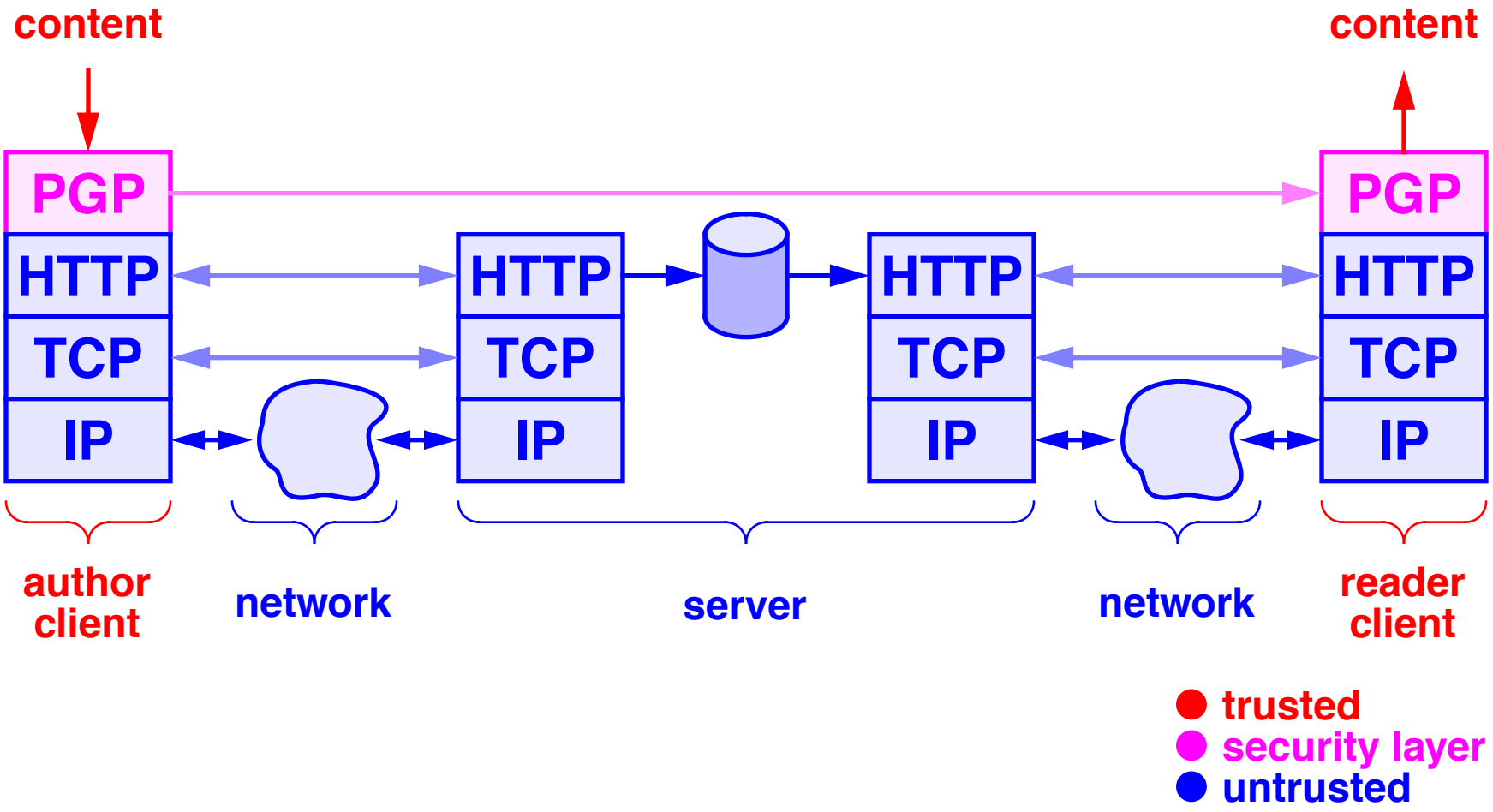
sun microsystems

Transport Layer Security



sun microsystems

Application Layer Security



sun microsystems

Comparison

feature	security layer		
	network	transport	application
author authentication	no*	by server	by reader
reader authentication	no*	by server	by sender
server authentication	by client	by client	n/a
content integrity	each hop	each hop	end to end
nonrepudiation of authorship	no	no	yes
privacy scales to many readers	yes	yes	no
secure through caching proxy	no	no	yes
traffic analysis exposure	IP addr	TCP port	URL
need to modify application	*no	some	yes
need kernel support	yes	no	no
negotiable crypto algorithms	yes	yes	no
server must be trusted	yes	yes	no
server need crypto code	yes	yes	no
server CPU requirement	high	high	low

Conclusion

For store and forward:

- **application-layer is favorable for authentication/integrity/nonrepudiation**
- **application-layer privacy is prohibitively expensive for large number of recipients, but is favorable for just a few recipients**
- **transport and application-layer privacy cooperating together might solve the scaling problem while preserving some of the advantages of application-layer privacy**
- **network-layer security is favorable when application transparency is needed**