

---

# OMOS: A Framework for Secure Communication in Mashup Applications

Saman Zarandioon

Danfeng (Daphne) Yao

Vinod Ganapathy

Department of Computer Science

Rutgers University

Piscataway, NJ 08854

{samanz,danfeng,vinodg}@cs.rutgers.edu

December 2008

[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

[Experiments](#)

▷ What is a **Mashup** application?

## ▷ What is a **Mashup** application?

- Seamlessly combine contents from multiple heterogeneous data sources.
- Overall goal: more integrated and convenient end-user experience.
- Becoming very popular - Web 2.0

[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

[Experiments](#)

- ▷ What is a **Mashup** application?
- ▷ My favorite mashup website *Zillow!*

- Introduction
- Mashups**
- Architecture
- Security in client-side services
- OMOS
- Experiments



Find homes:

[NJ](#) » [Somerset county](#) » [Franklin Township](#) » [08873](#) » Showing Homes

Street  Aerial  Hybrid  List [E-mail Alerts](#)

Microsoft Virtual Earth™

Zillow.com

Zestimate® Values & Accuracy

Introduction

Mashups

Architecture

Security in client-side services

OMOS

Experiments



**199 Buckingham Way** Somerset NJ 08873  
2 beds, 2.5 baths, 1,336 sq ft

🏠 **Recently Sold: \$264,000**

My Estimate: [CREATE](#)

Monthly Payment: \$ **1,613** [EDIT](#) [ING DIRECT Mortgages with Low Rates](#)

💡 Need to refi? Get loan quotes, anonymously. [Zillow Mortgage Marketplace](#)

---

**Street View** [ADD PHOTO](#)

▶ [See a larger Street View](#)

---

**Home Info** [EDIT](#)

199 Buckingham Way, Somerset, NJ

<b>Owner Facts:</b>	<b>Nearby Schools: ?</b>
<ul style="list-style-type: none"><li>• Townhouse</li><li>• 2 beds</li><li>• 2.5 bath</li></ul>	District: <a href="#">Franklin Twp</a> Primary: <a href="#">Conerly Road</a> Middle: <a href="#">Sampson G. Smith ...</a> High: <a href="#">Franklin Twp High</a> <a href="#">See more Somerset schools</a>

Introduction

Mashups

Architecture  
Security in  
client-side services

OMOS

Experiments



[See more Somerset schools](#)

See all home info

### Charts & Data

ZESTIMATE®: **\$266,000** [?](#)  
 Value Range: **\$247,380 - \$281,960**  
 30-day change: **\$2,000**  
 Zestimate updated: 11/26/2008

**Last sale and tax info**  
 Sold 10/06/2008: **\$264,000**  
 2008 Property Tax: **\$5,376**

1YR 5YR 10YR

See all charts & data

### Home Ownership

This home has been claimed by owner.

Flag listing

### Home Q&A

Ask questions, share information [?](#) [See Q&A for other homes in the area](#)

Subject\*

### Comparable Homes

**How this home stacks up**  
 This home \$ per sq ft: **\$199**  
 Comps avg \$ per sq ft: **\$150**  
[How to use these comps](#)

#### Recent comparable sales

- Sold 08/20/2008: **\$280,000**  
[206 Chatsworth Dr](#)
- Sold 09/18/2008: **\$258,000**  
[118 Winchester Way](#)
- Sold 08/13/2008: **\$283,000**  
[162 Picadilly Pl](#)
- Sold 10/23/2008: **\$305,000**  
[392 Glastonbury Ln](#)

See all comparable homes  
Refine Comparables

### Mortgage Calculator

Loan Amount:   
 Interest Rate:   
 Repayment Period:   
**Monthly Payment: \$1,613** [Recalculate](#)  
Payment includes estimated taxes and insurance.

[Get custom quotes - anonymously](#)

Introduction

**Mashups**

Architecture  
Security in  
client-side services

OMOS

Experiments





[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

[Experiments](#)

- ▷ What is a **Mashup** application?
- ▷ My favorite mashup website *Zillow!*
- ▷ **Web desktop** (webtop) (e.g. eyeOS, DesktopTwo, G.ho.st, Netvibes, and Online OS).

Introduction

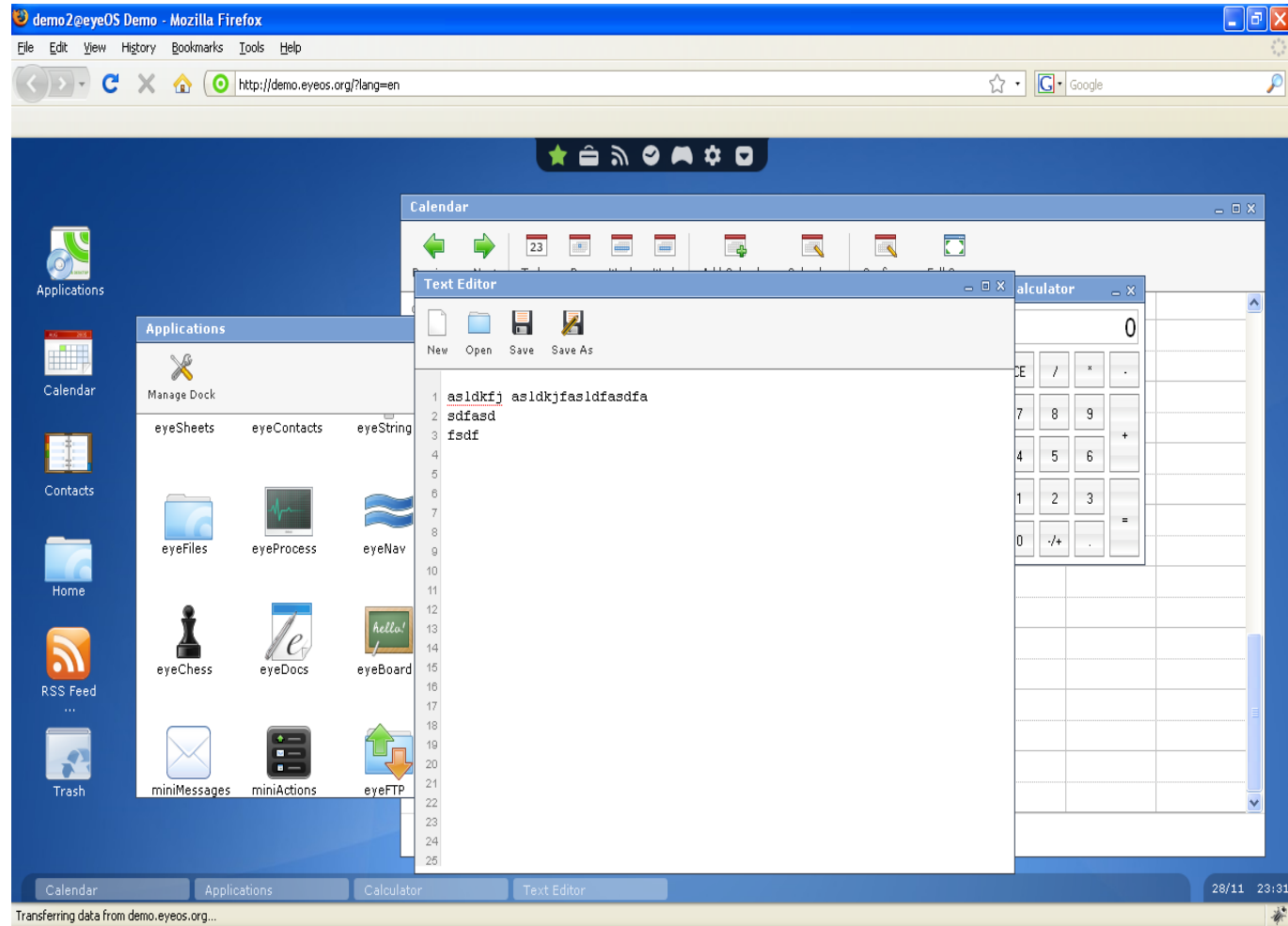
**Mashups**

Architecture

Security in client-side services

OMOS

Experiments



[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

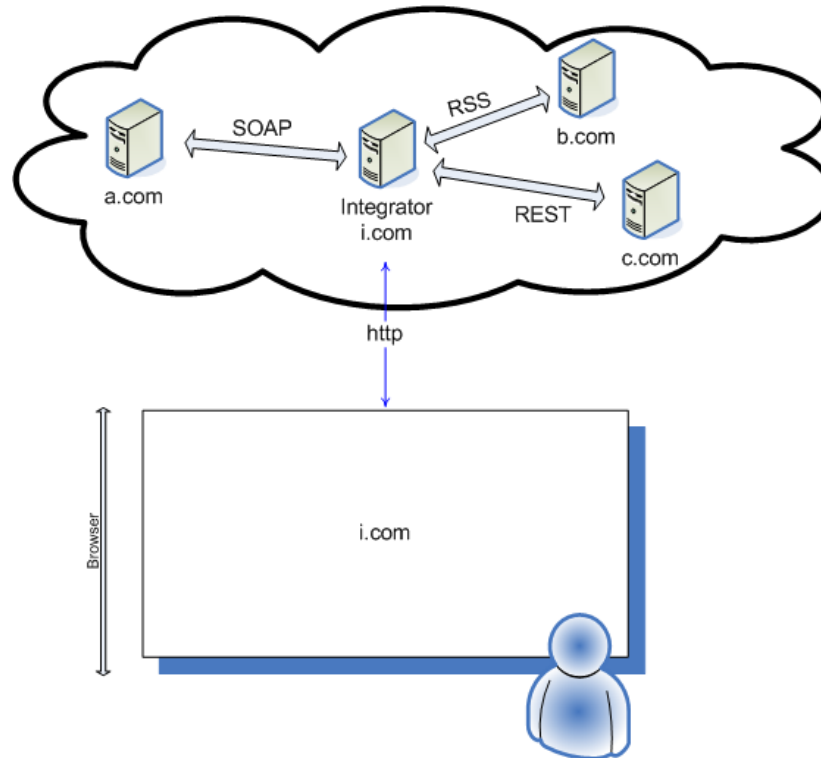
[Experiments](#)

Ways that service providers can expose their services:

▷ **Server-side services**

Ways that service providers can expose their services:

▷ **Server-side services**



[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

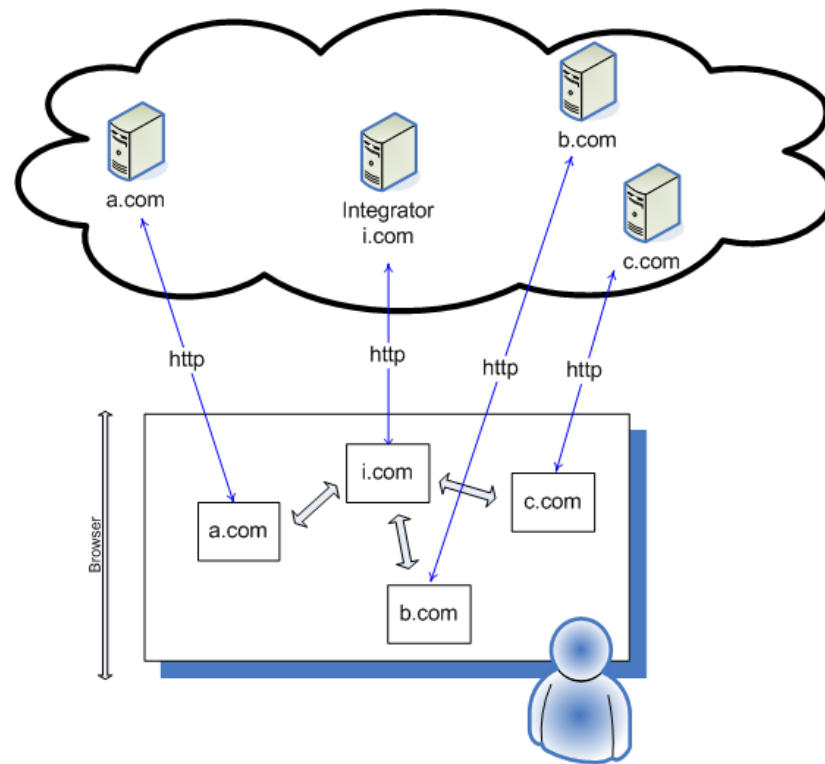
[Experiments](#)

Ways that service providers can expose their services:

- ▷ **Server-side services**
- ▷ **Client-side services**

Ways that service providers can expose their services:

- ▷ **Server-side services**
- ▷ **Client-side services**



User is involved; AJAX-oriented; More responsive/efficient

[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

[Experiments](#)

- Service providers use **ad-hoc non-secure** methods.

[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

[Experiments](#)

- Service providers use **ad-hoc non-secure** methods.
- Consumers need to *trust* service providers: Not suitable when dealing with sensitive personal data.



[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

[Experiments](#)

- Service providers use **ad-hoc non-secure** methods.
- Consumers need to *trust* service providers: Not suitable when dealing with sensitive personal data.
- HTML, JavaScript and browsers are not designed to support client-side communication.

[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

[Experiments](#)

- Service providers use **ad-hoc non-secure** methods.
- Consumers need to *trust* service providers: Not suitable when dealing with sensitive personal data.
- HTML, JavaScript and browsers are not designed to support client-side communication.
- Trade-Off Between Usability and Security: All or Nothing, Complete isolation vs. complete exposure.

[Introduction](#)

[Mashups](#)

[Architecture](#)

[Security in  
client-side services](#)

[OMOS](#)

[Experiments](#)

- Service providers use **ad-hoc non-secure** methods.
- Consumers need to *trust* service providers: Not suitable when dealing with sensitive personal data.
- HTML, JavaScript and browsers are not designed to support client-side communication.
- Trade-Off Between Usability and Security: All or Nothing, Complete isolation vs. complete exposure.

[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

[Stack](#)

[MDP Layer](#)

[MHTTP Layer](#)

[Experiments](#)

- **OpenMashupOS (OMOS)** is a mashup framework that is designed to support secure client-side services.

[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

[Stack](#)

[MDP Layer](#)

[MHTTP Layer](#)

[Experiments](#)

- **OpenMashupOS (OMOS)** is a mashup framework that is designed to support secure client-side services.
- **Design Goals:**

Introduction

OMOS

**Overview**

Mashlet

Secure

Frame-to-frame

Communication

Communication

Stack

MDP Layer

MHTTP Layer

Experiments

- **OpenMashupOS (OMOS)** is a mashup framework that is designed to support secure client-side services.
  
- **Design Goals:**
  - ◆ To be compatible with all major browsers without *any* change or extension to the browsers.

Introduction

OMOS

**Overview**

Mashlet

Secure

Frame-to-frame

Communication

Communication

Stack

MDP Layer

MHTTP Layer

Experiments

- **OpenMashupOS (OMOS)** is a mashup framework that is designed to support secure client-side services.
  
- **Design Goals:**
  - ◆ To be compatible with all major browsers without *any* change or extension to the browsers.
  
  - ◆ To provide a *powerful* abstraction that is *flexible* and *easy* to **understand** and **use** by mashup developers.

Introduction

OMOS

**Overview**

Mashlet

Secure

Frame-to-frame

Communication

Communication

Stack

MDP Layer

MHTTP Layer

Experiments

- **OpenMashupOS (OMOS)** is a mashup framework that is designed to support secure client-side services.
  
- **Design Goals:**
  - ◆ To be compatible with all major browsers without *any* change or extension to the browsers.
  
  - ◆ To provide a *powerful* abstraction that is *flexible* and *easy* to **understand** and **use** by mashup developers.
  
  - ◆ To guarantee *mutual authentication*, *data confidentiality*, and *message integrity* for communication between service provider and consumer.



Introduction

OMOS

**Overview**

Mashlet

Secure

Frame-to-frame

Communication

Communication

Stack

MDP Layer

MHTTP Layer

Experiments

- **OpenMashupOS (OMOS)** is a mashup framework that is designed to support secure client-side services.
  
- **Design Goals:**
  - ◆ To be compatible with all major browsers without *any* change or extension to the browsers.
  
  - ◆ To provide a *powerful* abstraction that is *flexible* and *easy* to **understand** and **use** by mashup developers.
  
  - ◆ To guarantee *mutual authentication*, *data confidentiality*, and *message integrity* for communication between service provider and consumer.

[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

[Stack](#)

[MDP Layer](#)

[MHTTP Layer](#)

[Experiments](#)

- **Mashlet** is a client side component that runs in the browser under the privilege of the principal that is defined by the domain name of the server that hosts the mashlet.

[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

[Stack](#)

[MDP Layer](#)

[MHTTP Layer](#)

[Experiments](#)

- **Mashlet** is a client side component that runs in the browser under the privilege of the principal that is defined by the domain name of the server that hosts the mashlet.
- Mashlets should be able to communicate securely on the client side, meaning that the communication protocol guarantees:

[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

[Stack](#)

[MDP Layer](#)

[MHTTP Layer](#)

[Experiments](#)

- **Mashlet** is a client side component that runs in the browser under the privilege of the principal that is defined by the domain name of the server that hosts the mashlet.
- Mashlets should be able to communicate securely on the client side, meaning that the communication protocol guarantees:
  - ◆ **Mutual Authentication**
  - ◆ **Confidentiality**
  - ◆ **Message Integrity**

[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

[Stack](#)

[MDP Layer](#)

[MHTTP Layer](#)

[Experiments](#)

- **Mashlet** is a client side component that runs in the browser under the privilege of the principal that is defined by the domain name of the server that hosts the mashlet.
- Mashlets should be able to communicate securely on the client side, meaning that the communication protocol guarantees:
  - ◆ **Mutual Authentication**
  - ◆ **Confidentiality**
  - ◆ **Message Integrity**

[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

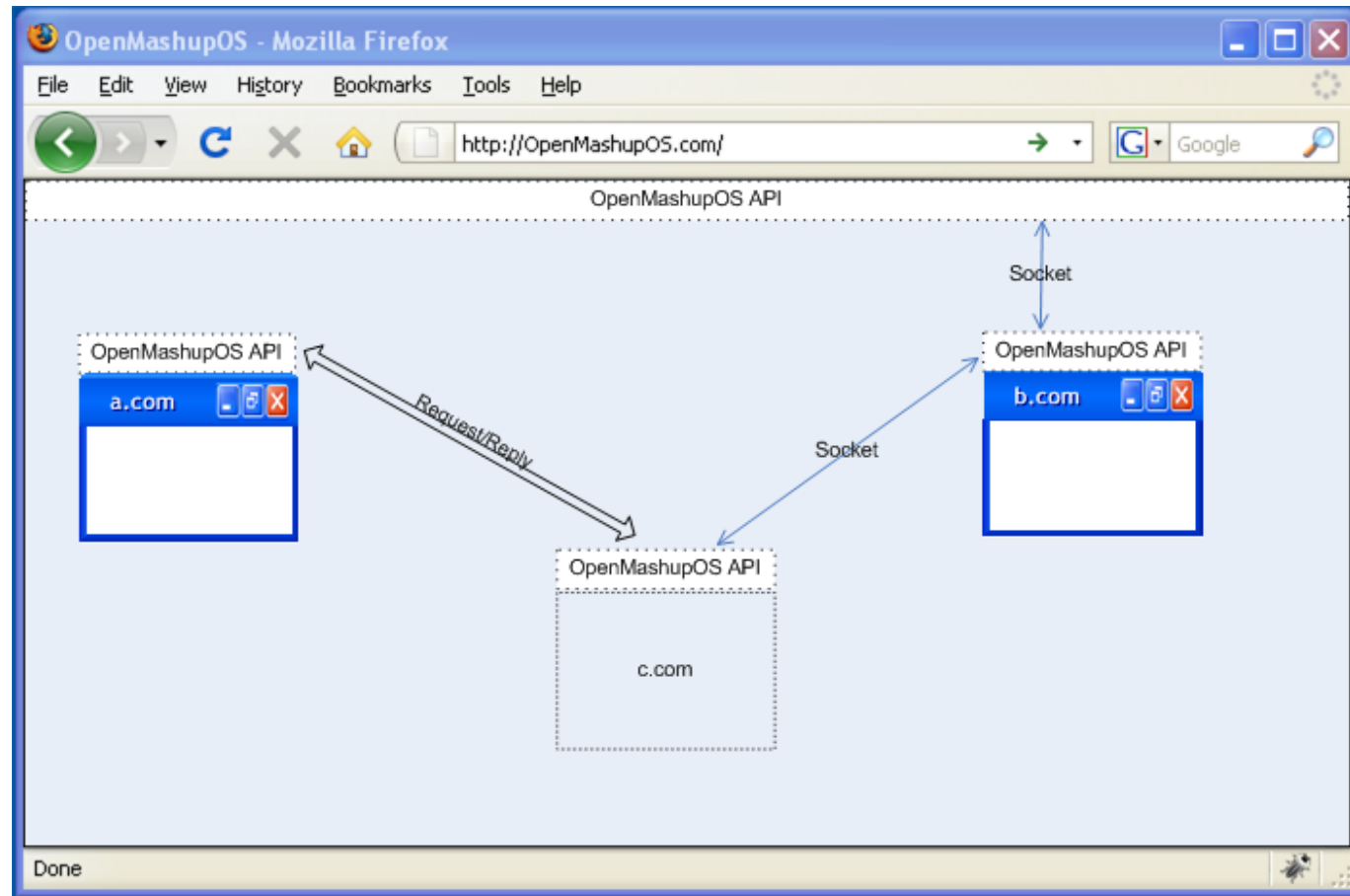
[Stack](#)

[MDP Layer](#)

[MHTTP Layer](#)

[Experiments](#)

- **Mashlet** is a client side component that runs in the browser under the privilege of the principal that is defined by the domain name of the server that hosts the mashlet.
- Mashlets should be able to communicate securely on the client side, meaning that the communication protocol guarantees:
  - ◆ **Mutual Authentication**
  - ◆ **Confidentiality**
  - ◆ **Message Integrity**



Using OMOS API, mashlets can communicate with their siblings and parents.

[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure  
Frame-to-frame  
Communication](#)

[Communication](#)

[Stack](#)

[MDP Layer](#)

[MHTTP Layer](#)

[Experiments](#)

Security of OMOS communication protocol relies on *Same Origin Policy (SOP)*:

- Protects confidentiality of domains against each other. (DOM elements, events, cookies, ...)
- URL property of an iframe is write-only.
- Partial change of URL is not allowed.



Introduction

OMOS

Overview

Mashlet

Secure

Frame-to-frame  
Communication

Communication

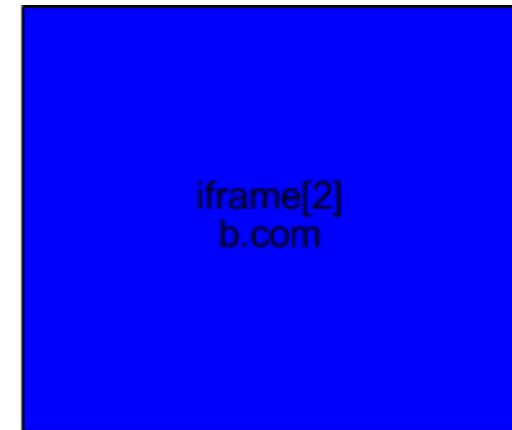
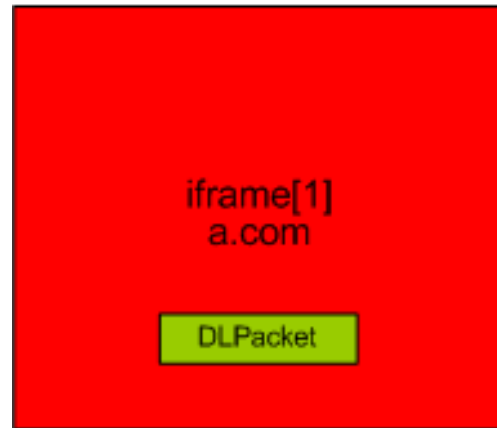
Stack

MDP Layer

MHTTP Layer

Experiments

Destination Frame Address	Source Frame Address	End point ID	Secret Key	Sequence Number	List of data fragments
---------------------------	----------------------	--------------	------------	-----------------	------------------------



Introduction

OMOS

Overview

Mashlet

Secure

**Frame-to-frame  
Communication**

Communication

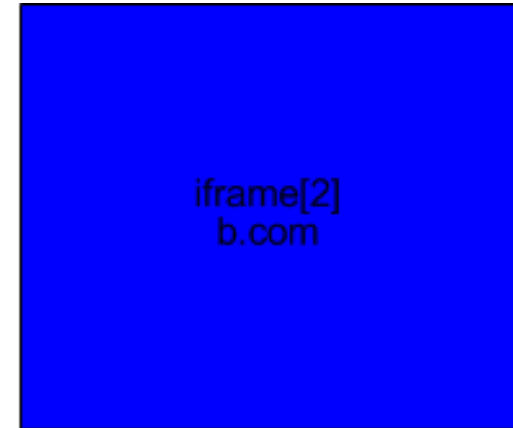
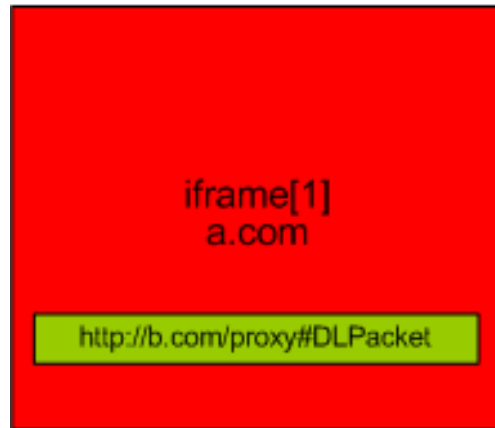
Stack

MDP Layer

MHTTP Layer

Experiments

Destination Frame Address	Source Frame Address	End point ID	Secret Key	Sequence Number	List of data fragments
---------------------------	----------------------	--------------	------------	-----------------	------------------------



Introduction

OMOS

Overview

Mashlet

Secure

Frame-to-frame  
Communication

Communication

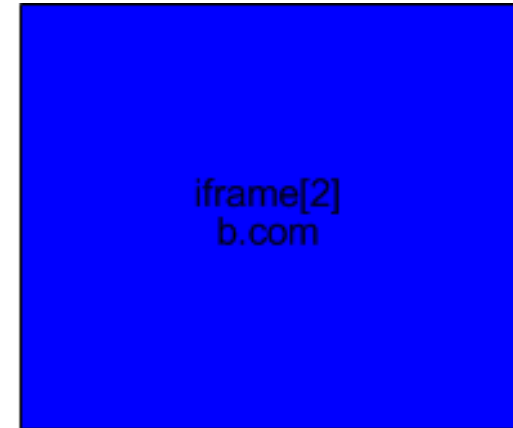
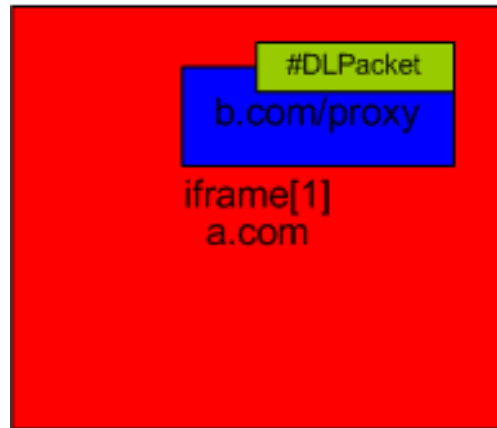
Stack

MDP Layer

MHTTP Layer

Experiments

Destination Frame Address	Source Frame Address	End point ID	Secret Key	Sequence Number	List of data fragments
---------------------------	----------------------	--------------	------------	-----------------	------------------------



Introduction

OMOS

Overview

Mashlet

Secure

Frame-to-frame  
Communication

Communication

Stack

MDP Layer

MHTTP Layer

Experiments

Destination Frame Address	Source Frame Address	End point ID	Secret Key	Sequence Number	List of data fragments
---------------------------	----------------------	--------------	------------	-----------------	------------------------



Introduction

OMOS

Overview

Mashlet

Secure

Frame-to-frame  
Communication

Communication

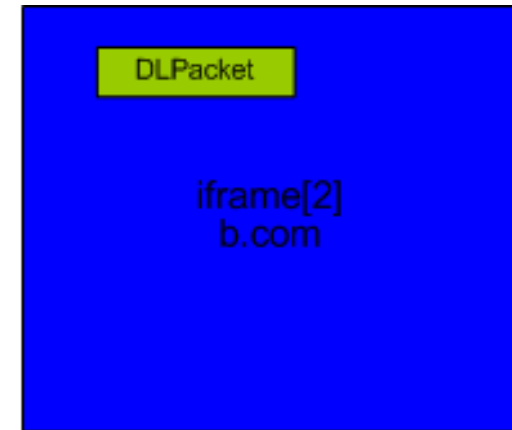
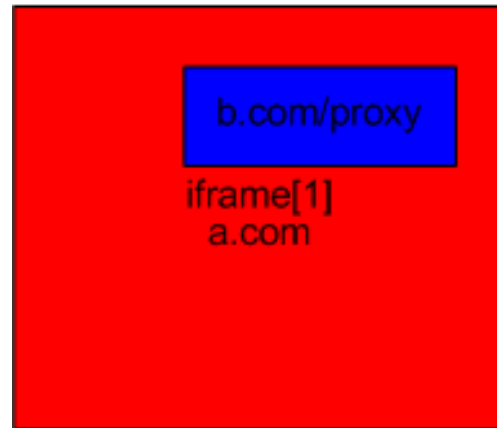
Stack

MDP Layer

MHTTP Layer

Experiments

Destination Frame Address	Source Frame Address	End point ID	Secret Key	Sequence Number	List of data fragments
---------------------------	----------------------	--------------	------------	-----------------	------------------------



[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame  
Communication](#)

[Communication](#)

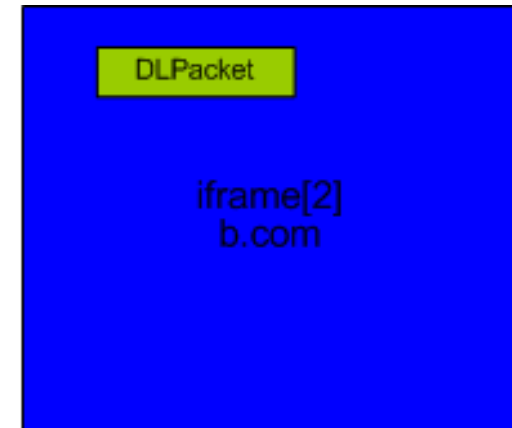
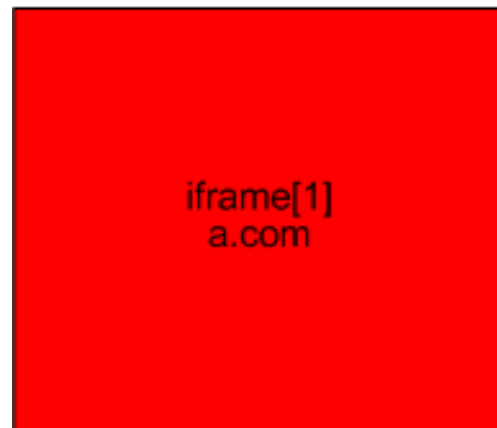
[Stack](#)

[MDP Layer](#)

[MHTTP Layer](#)

[Experiments](#)

Destination Frame Address	Source Frame Address	End point ID	Secret Key	Sequence Number	List of data fragments
---------------------------	----------------------	--------------	------------	-----------------	------------------------



Introduction

OMOS

Overview

Mashlet

Secure

Frame-to-frame  
Communication

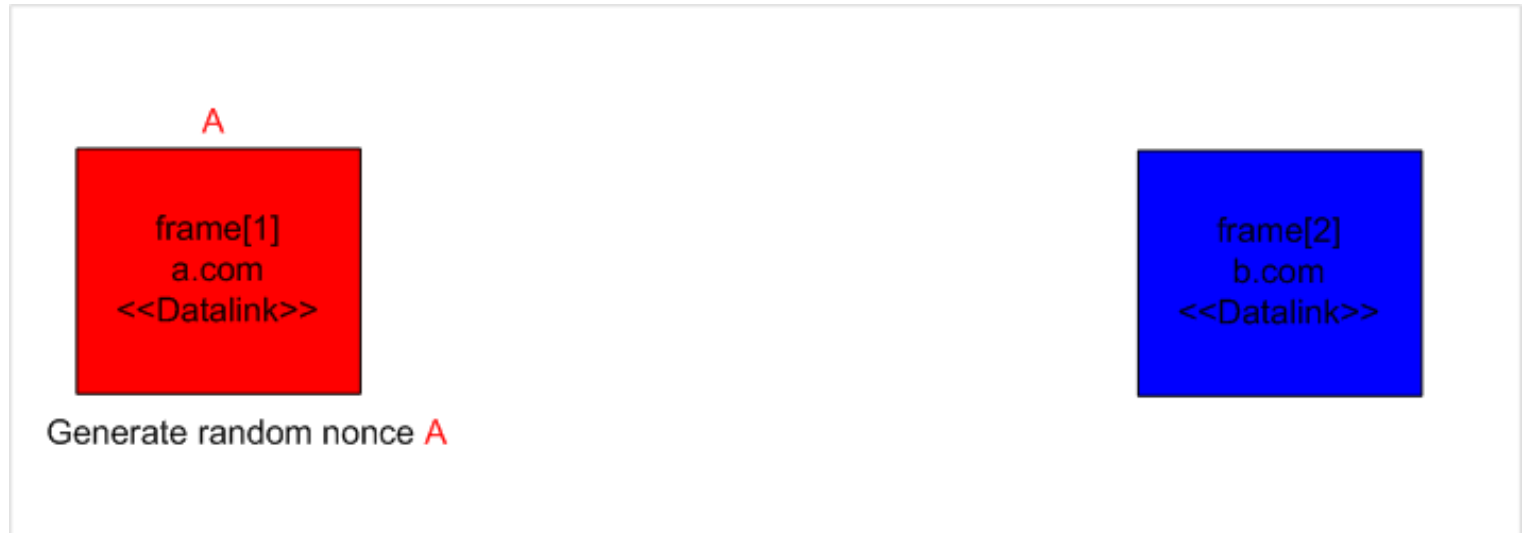
Communication  
Stack

MDP Layer

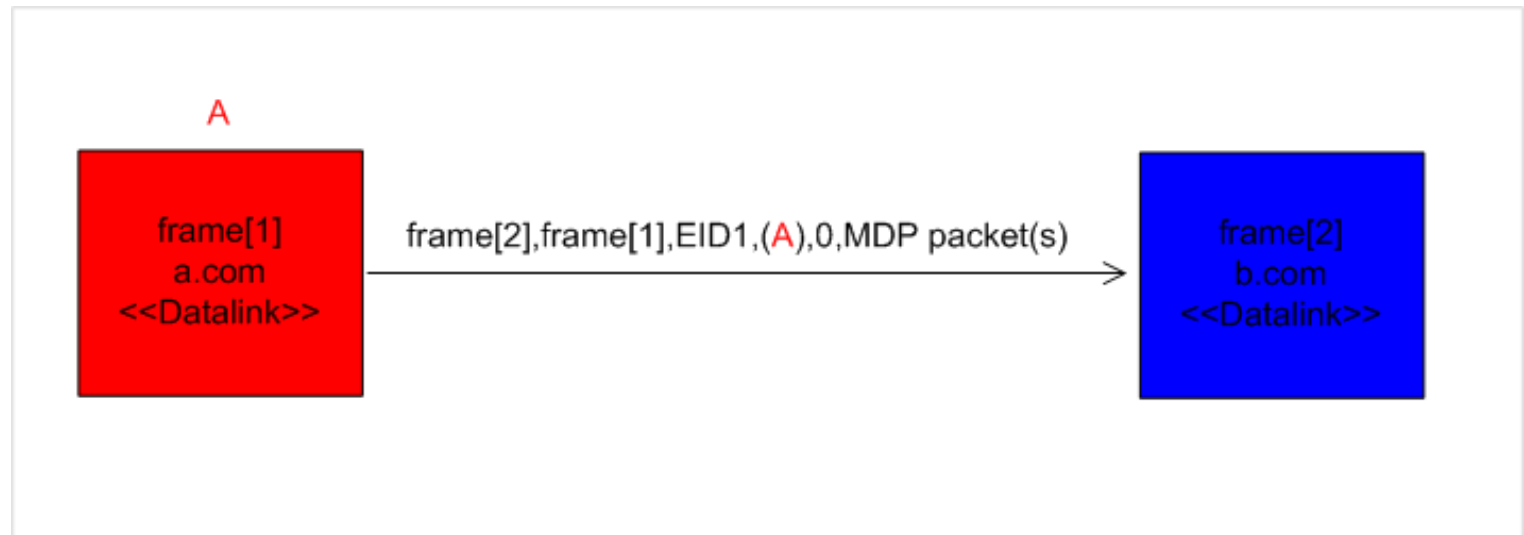
MHTTP Layer

Experiments

## Key exchange protocol:



## Key exchange protocol:





Introduction

OMOS

Overview

Mashlet

Secure

Frame-to-frame  
Communication

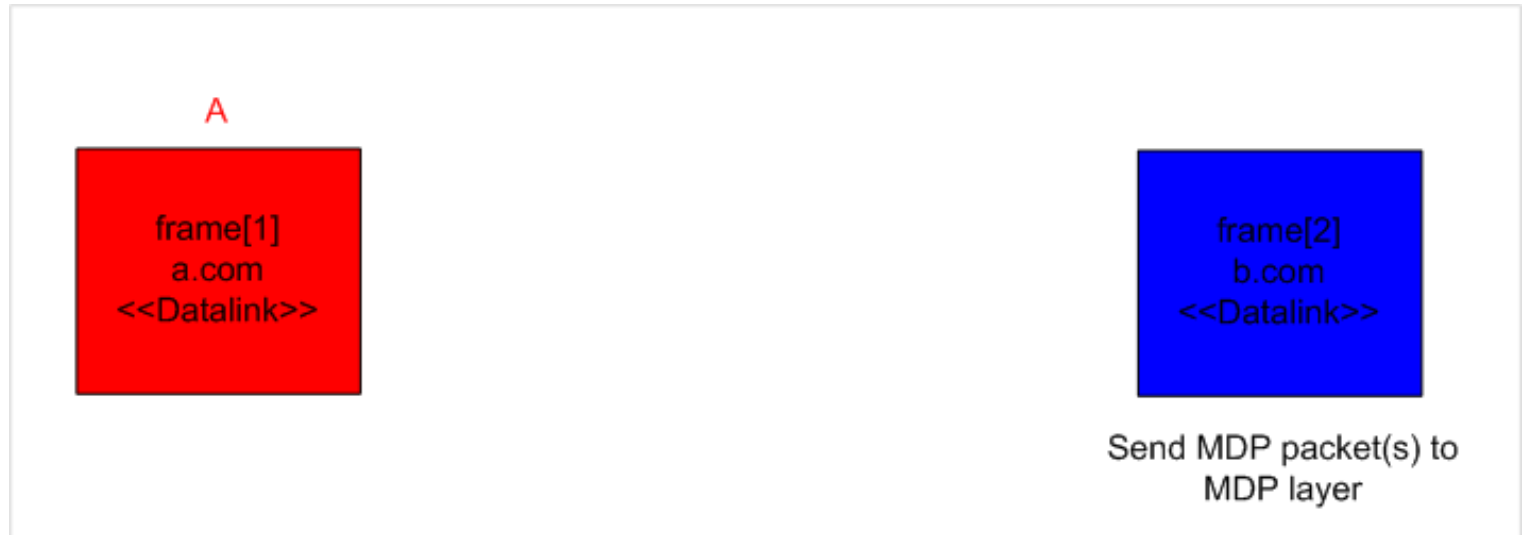
Communication  
Stack

MDP Layer

MHTTP Layer

Experiments

## Key exchange protocol:



Introduction

OMOS

Overview

Mashlet

Secure

Frame-to-frame  
Communication

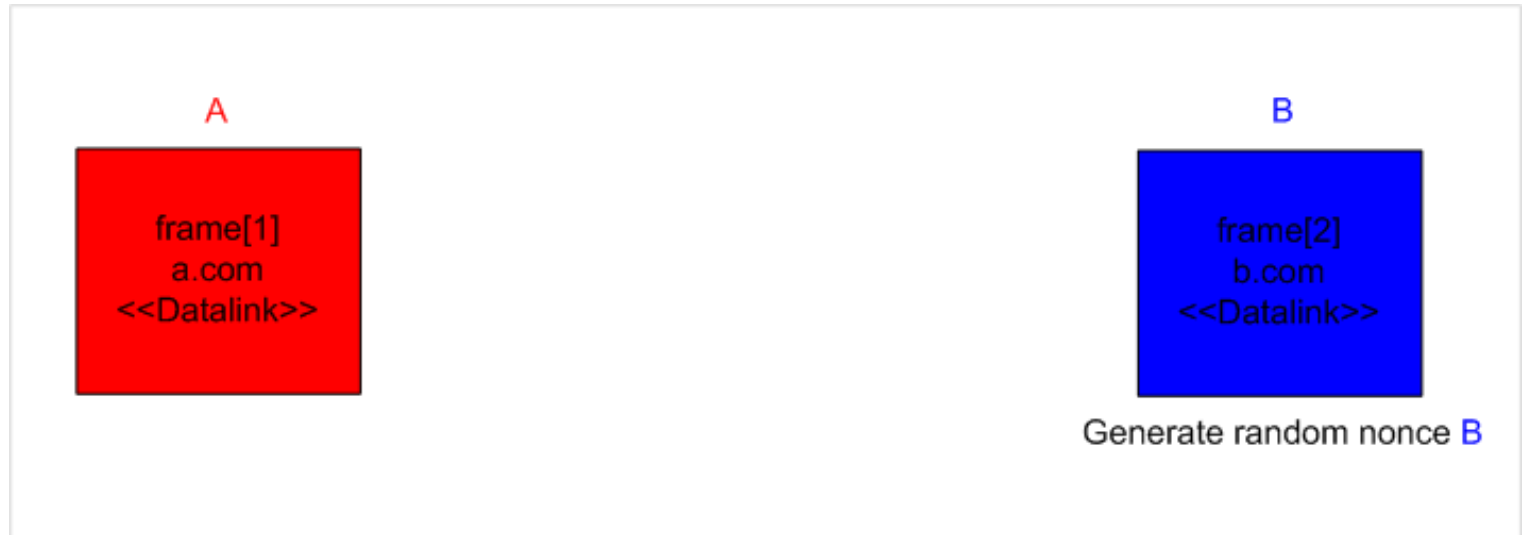
Communication  
Stack

MDP Layer

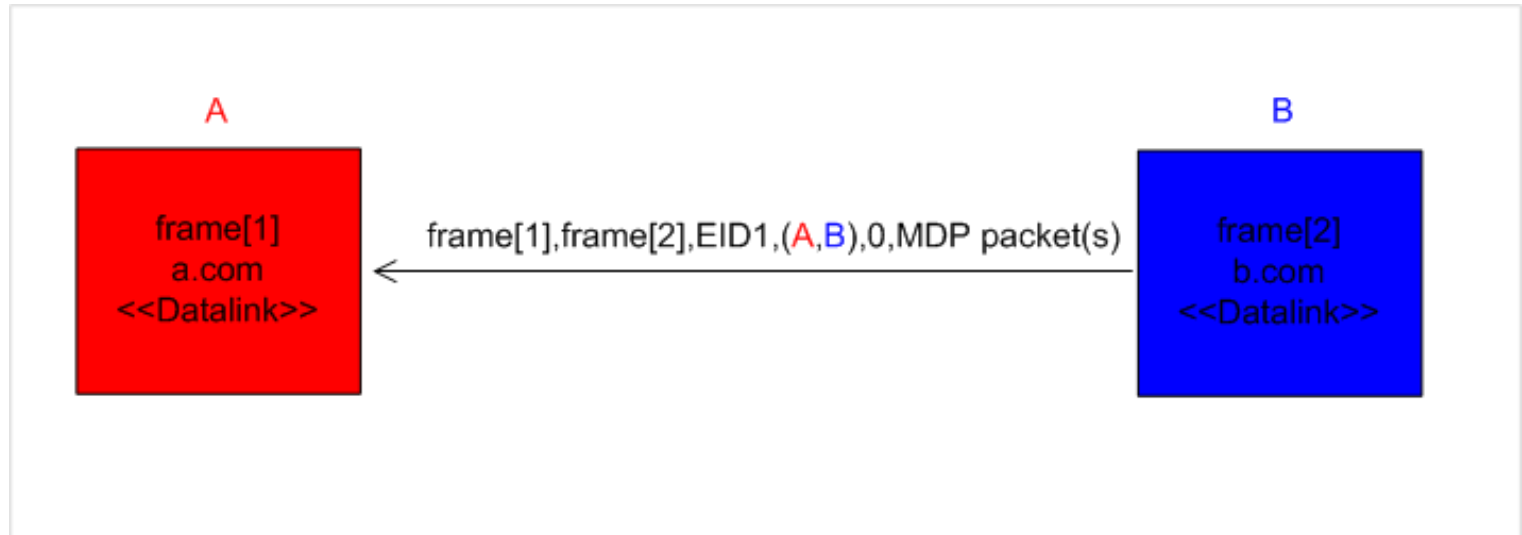
MHTTP Layer

Experiments

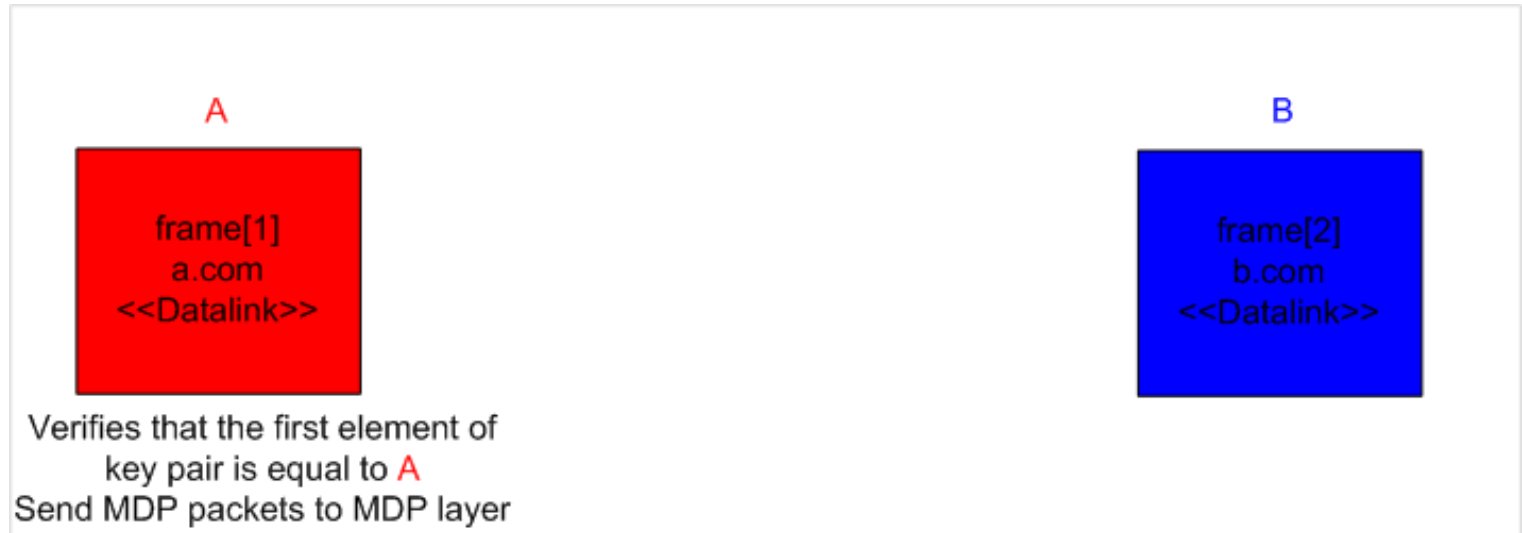
## Key exchange protocol:



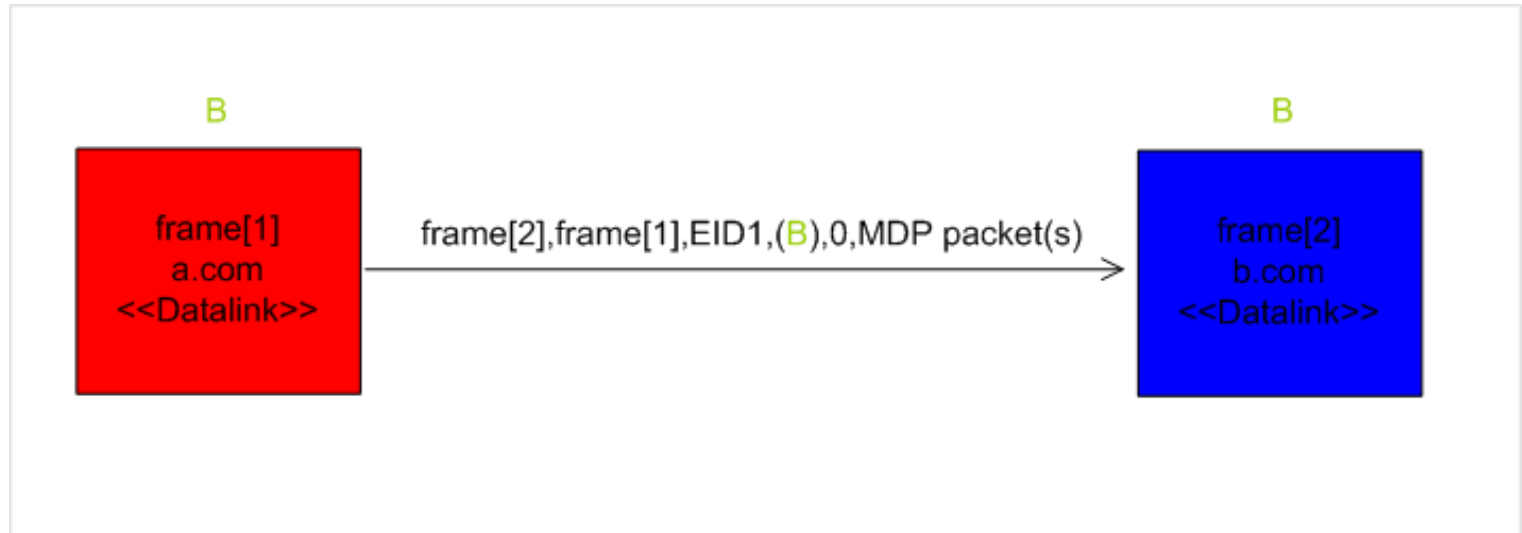
## Key exchange protocol:

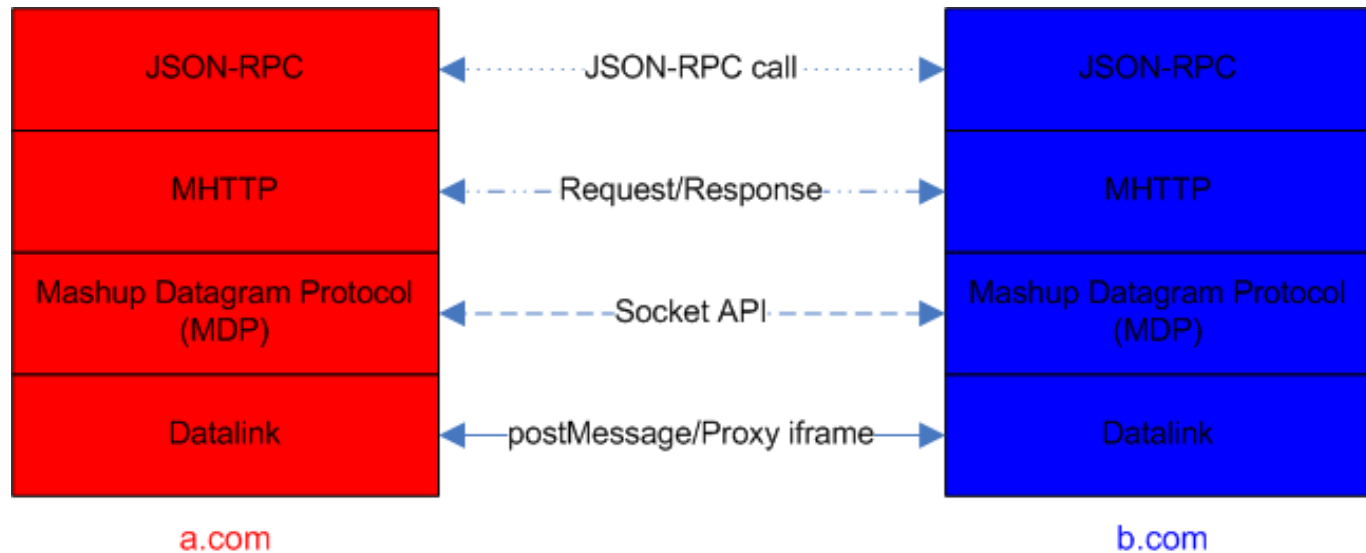


## Key exchange protocol:



## Key exchange protocol:





Each layer hides complex implementation details of communication in lower layers.

[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

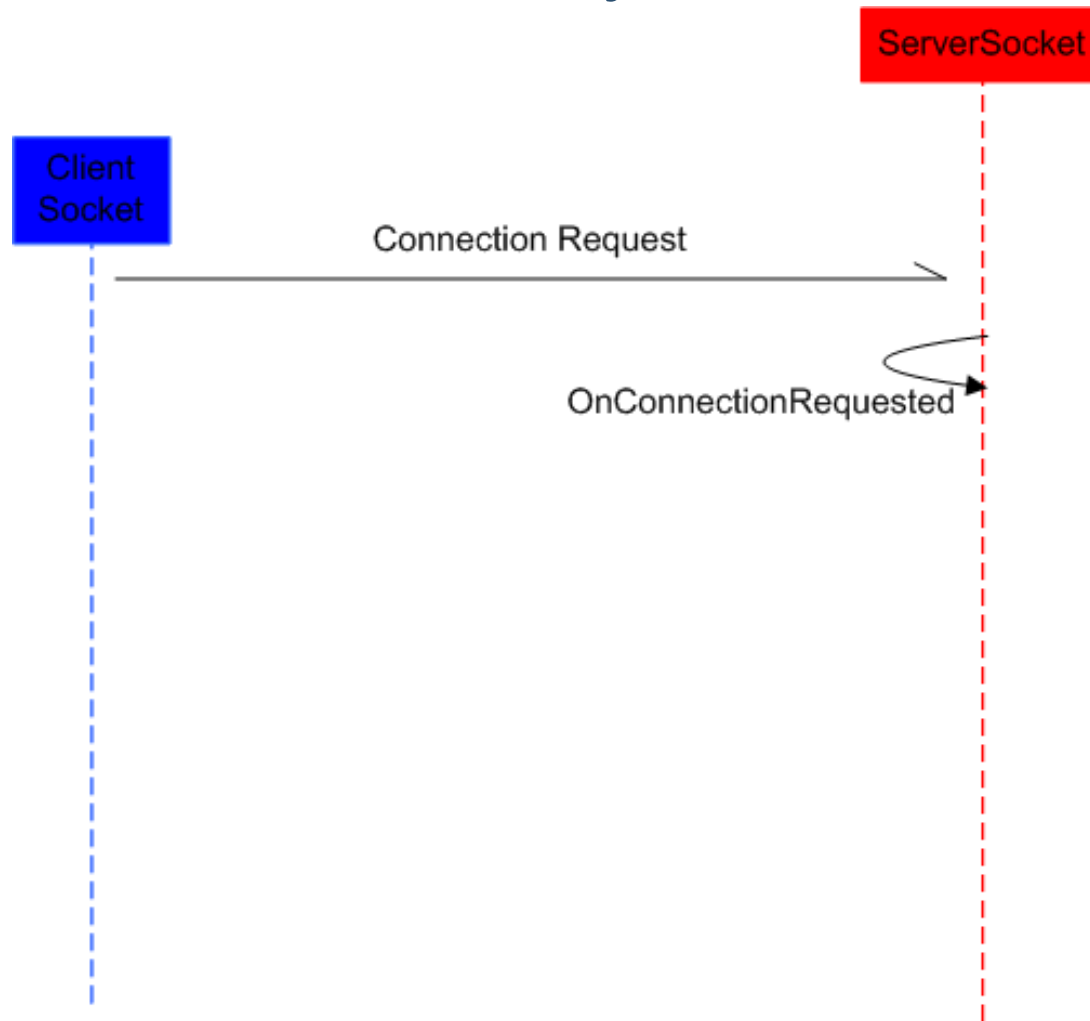
[Stack](#)

**[MDP Layer](#)**

[MHTTP Layer](#)

[Experiments](#)

## 3-way Handshake



[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

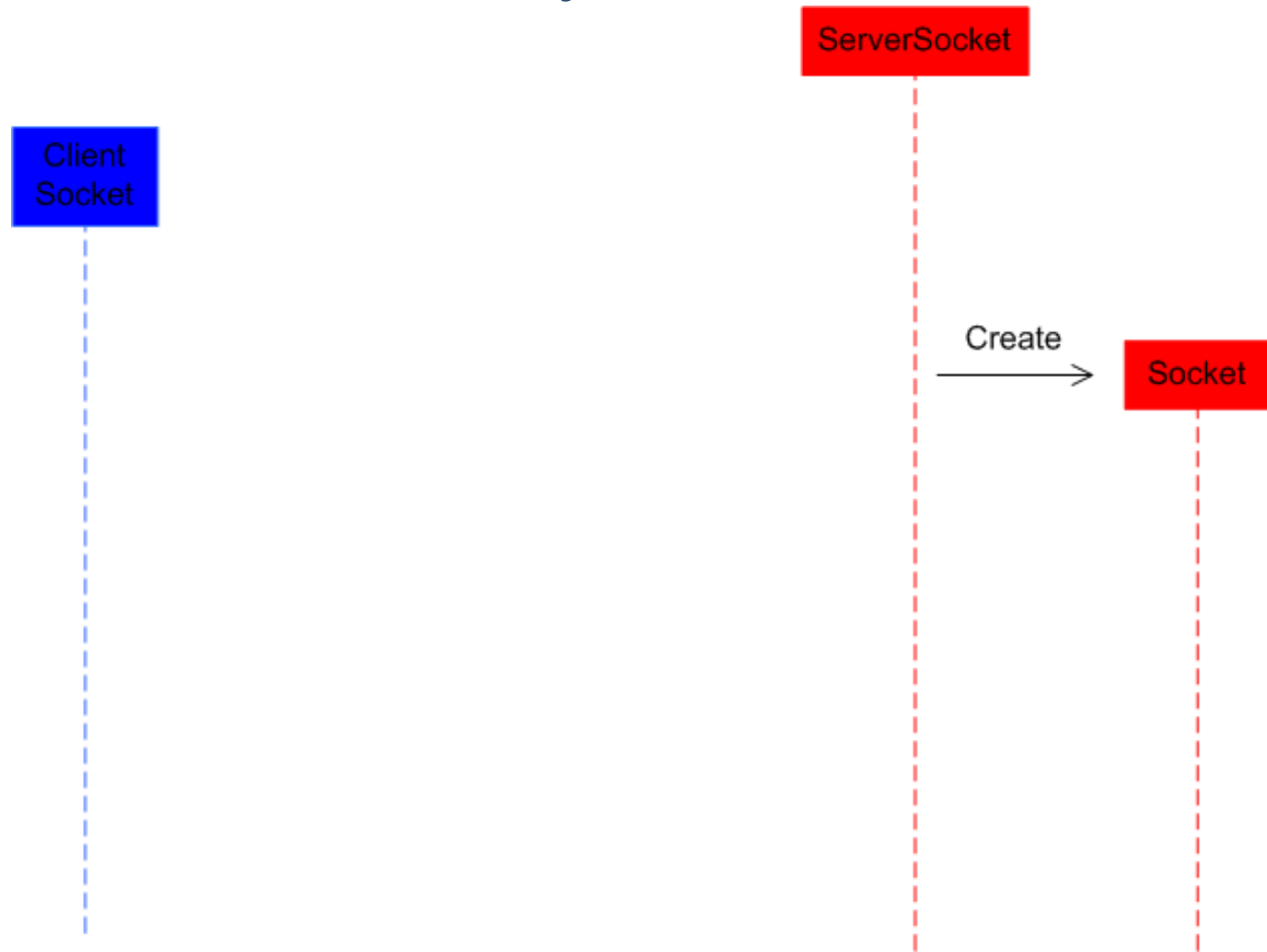
[Stack](#)

**[MDP Layer](#)**

[MHTTP Layer](#)

[Experiments](#)

## 3-way Handshake





[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

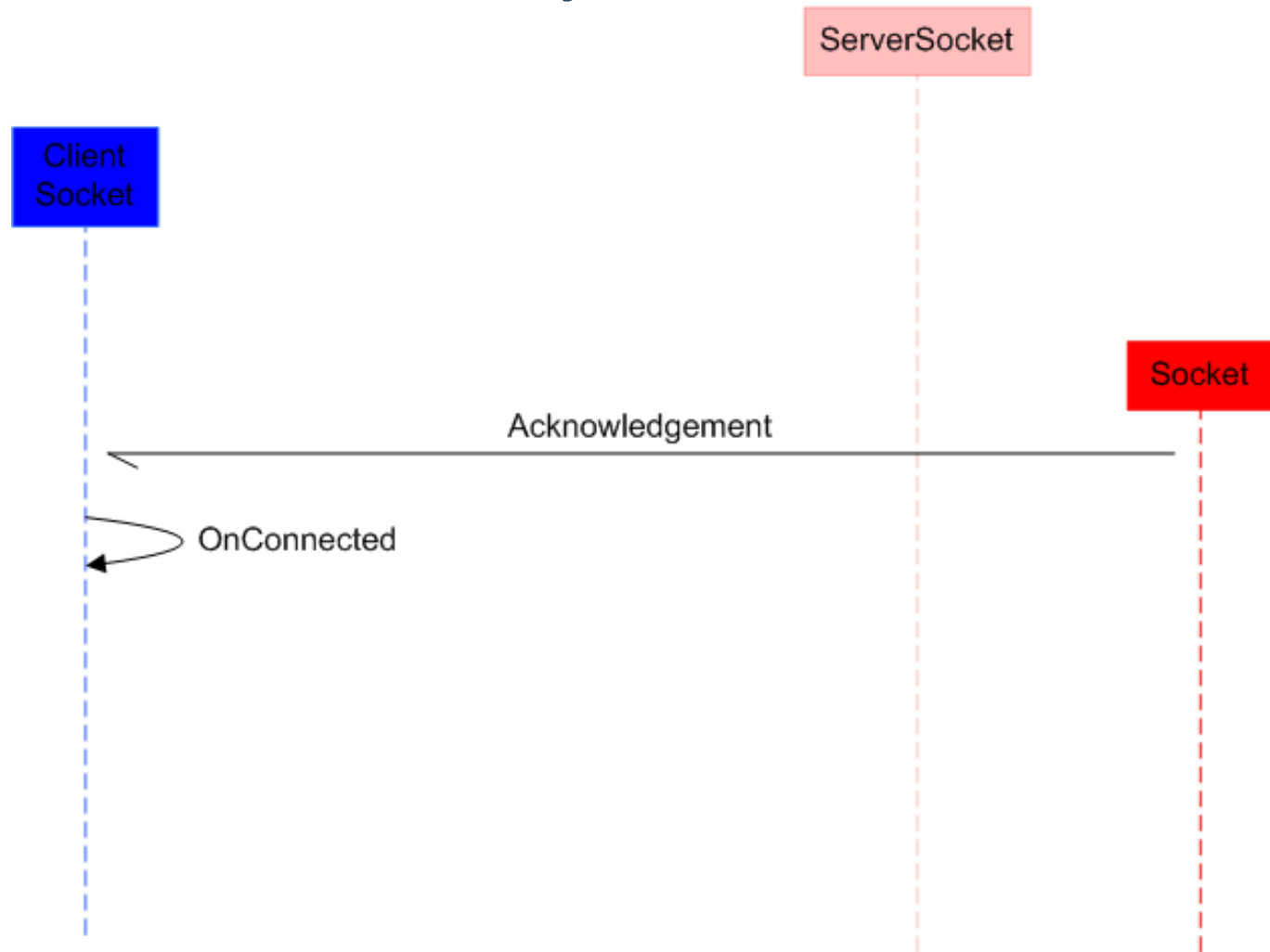
[Stack](#)

**[MDP Layer](#)**

[MHTTP Layer](#)

[Experiments](#)

## 3-way Handshake



[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

[Communication](#)

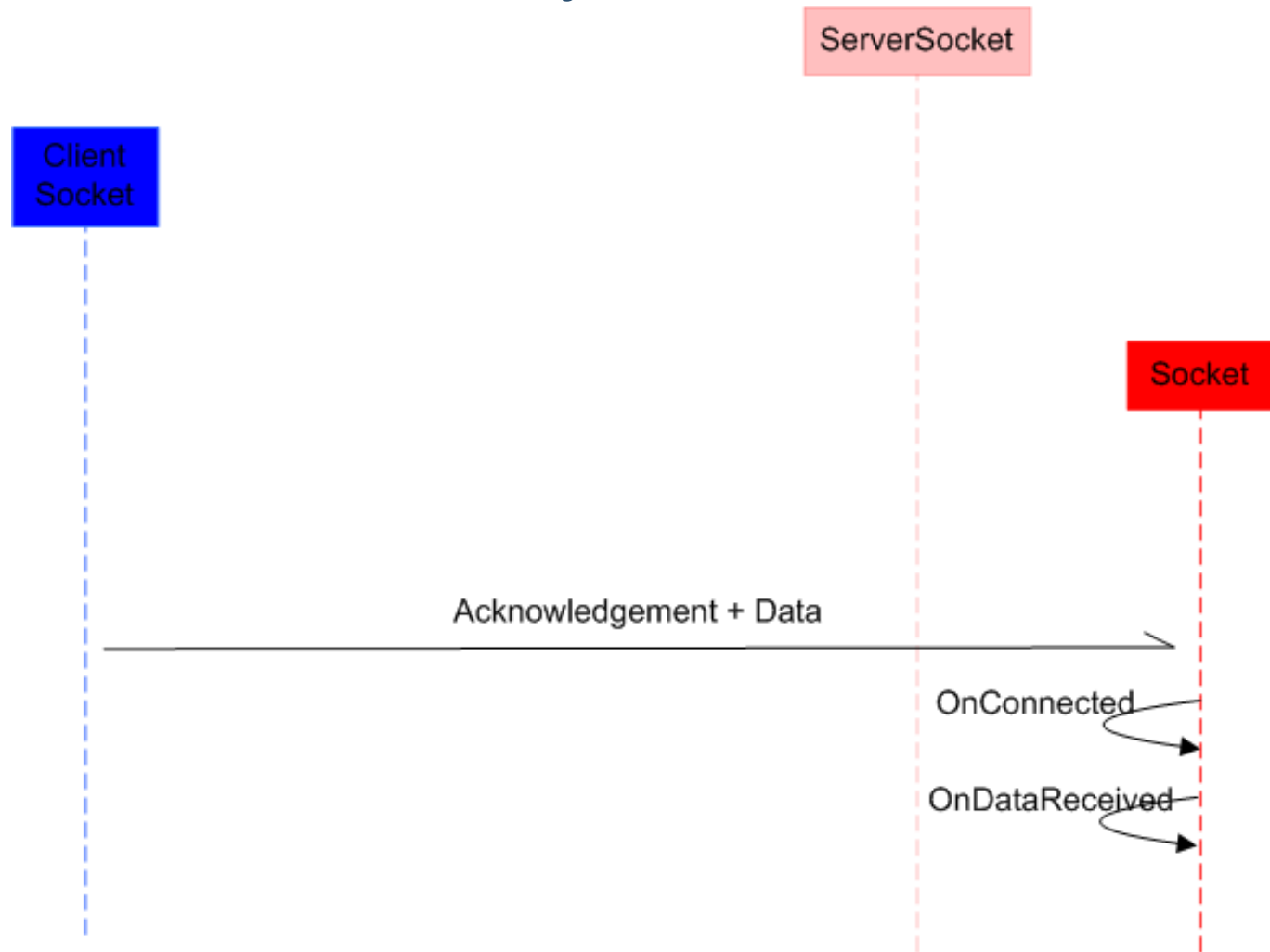
[Stack](#)

**[MDP Layer](#)**

[MHTTP Layer](#)

[Experiments](#)

## 3-way Handshake



[Introduction](#)

[OMOS](#)

[Overview](#)

[Mashlet](#)

[Secure](#)

[Frame-to-frame](#)

[Communication](#)

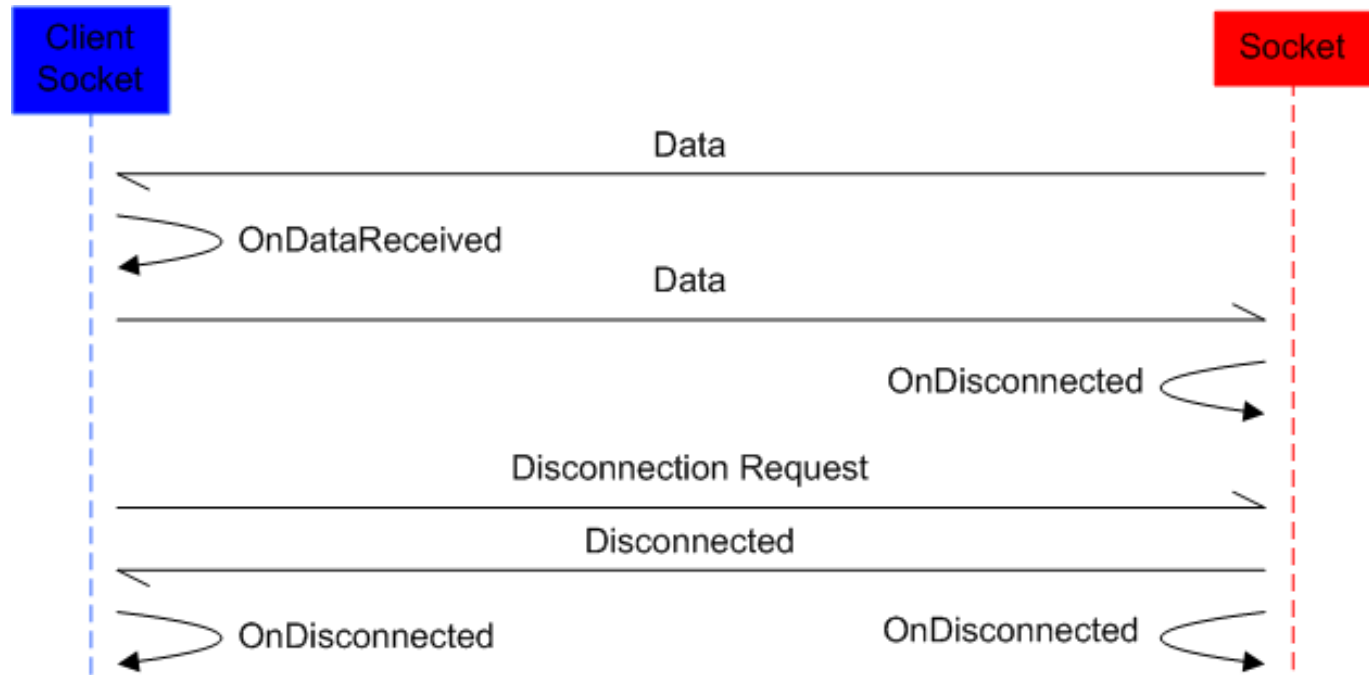
[Communication](#)

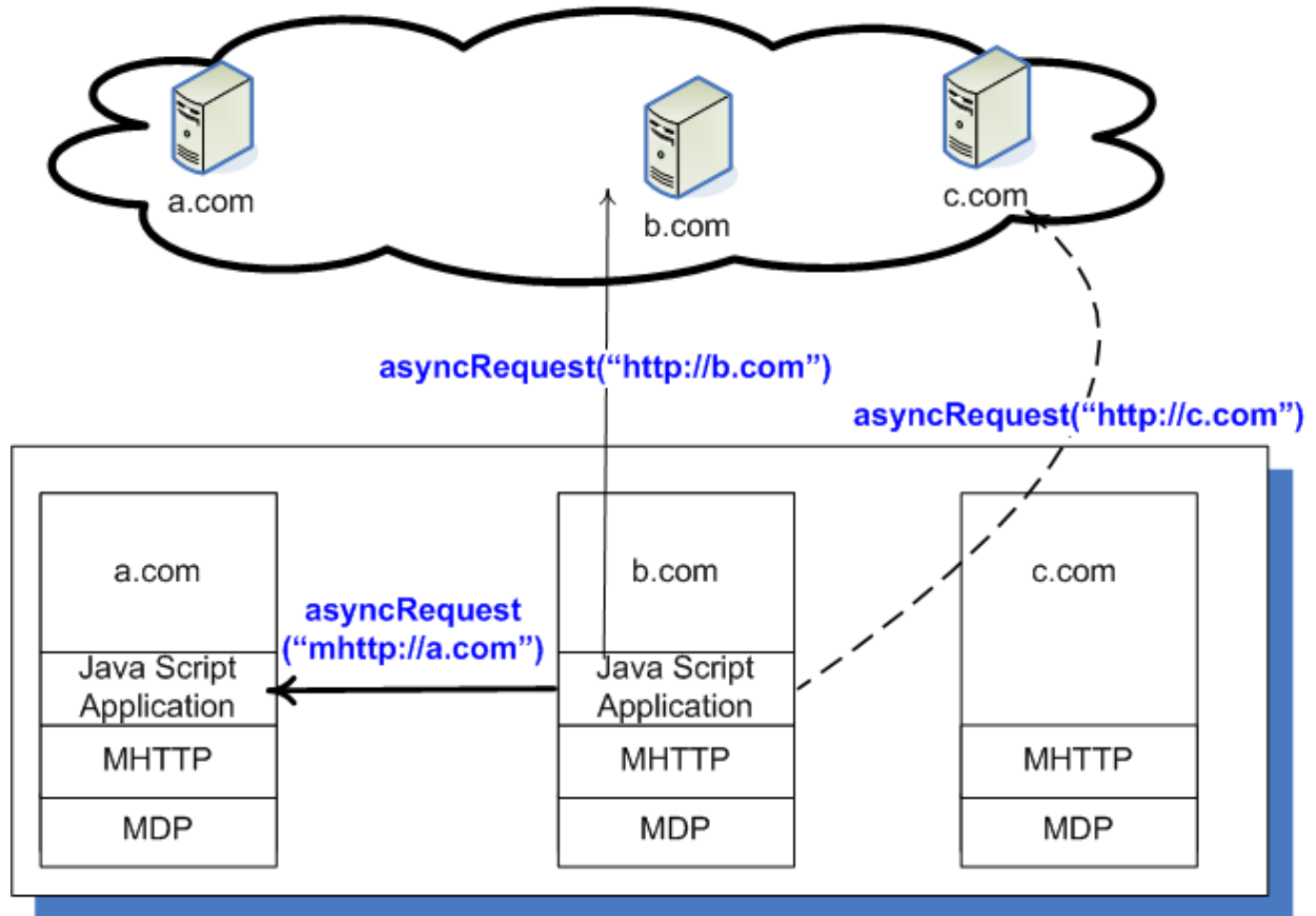
[Stack](#)

**[MDP Layer](#)**

[MHTTP Layer](#)

[Experiments](#)





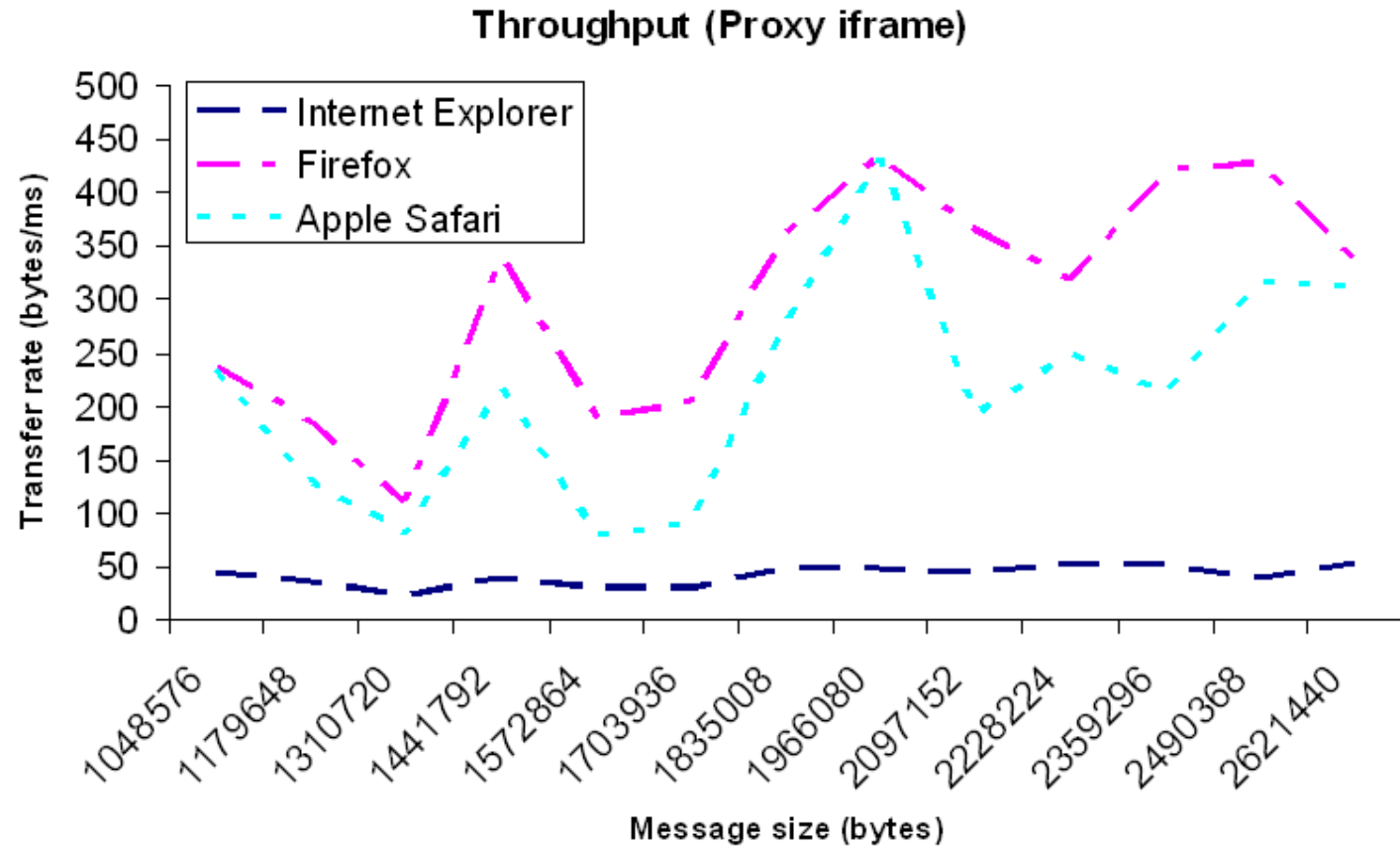
Versatile `asyncRequest`: mashlet-to-mashlet, same-domain & cross-domain mashlet-to-server communication.

[Introduction](#)

[OMOS](#)

[Experiments](#)

[Results](#)



[Introduction](#)

[OMOS](#)

[Experiments](#)

[Results](#)

### Throughput (postMessage/Opera)

