Демо. Микросервисная архитектура

Самосадный Кирилл
https://t.me/kirsamosad
samosad@seclab.cs.msu.su

МГУ 2018

Session fixation

Как атаковать жертву?

- Cookie с флагами secure и httponly могут быть перезаписаны методом переполнения cookie jar
- Нельзя надежно разделить приложения различного уровня критичности, например:
  - payments.site.com от blogs.site.com
- Пусть на blogs.site.com есть XSS
- Пусть на payments.site.com cookie выставлены как secure, httponly и без domain

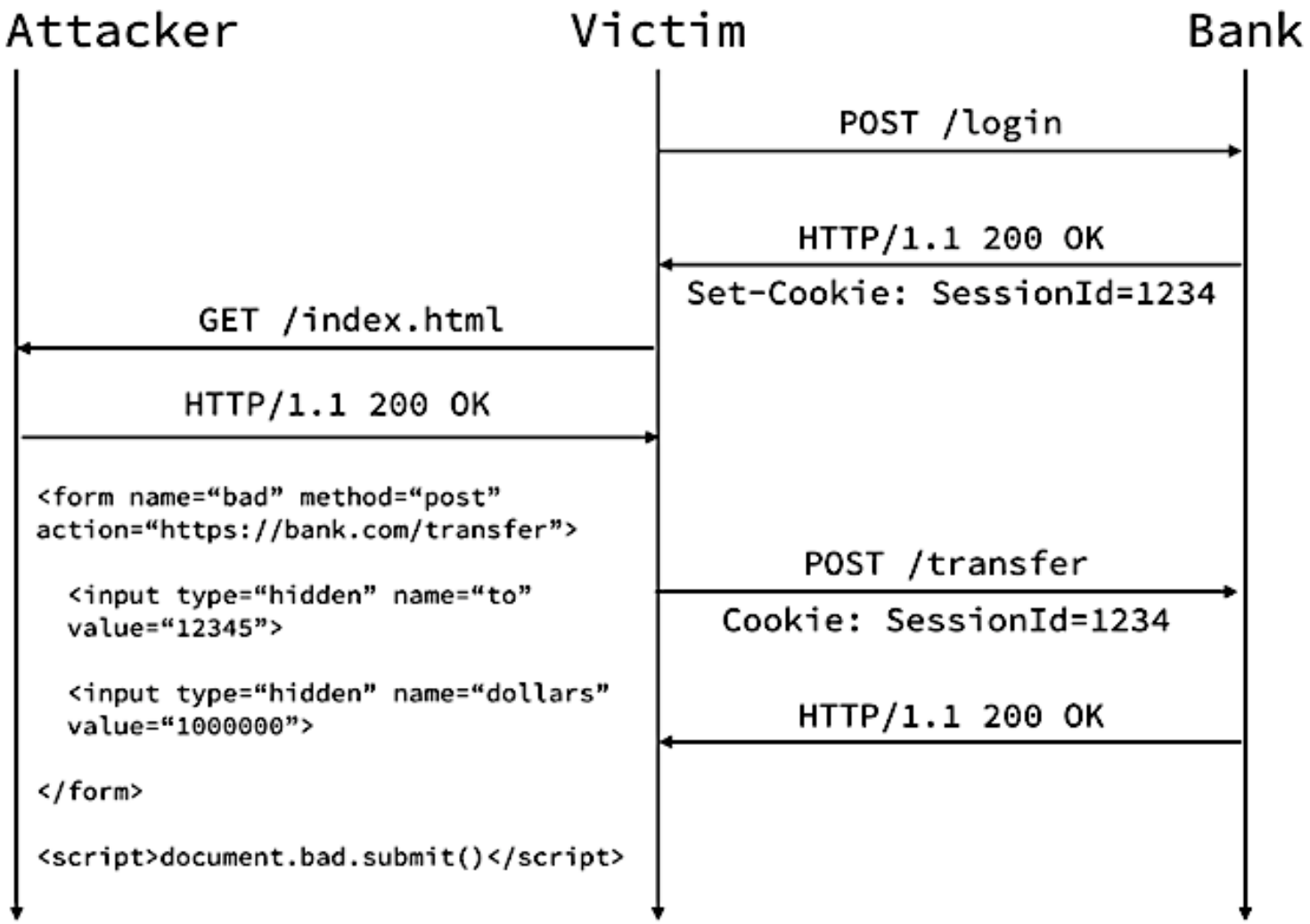
Ответ

- Как атаковать жертву?
  - выставляем через XSS cookie с domain = site.com
  - cookie jar для blogs.site.com переполняется и вытесняет cookies пользователя
  - выставляем свои cookies
  - порядок и кол-во посылаемых cookies зависит от браузера

DEMO: Session fixation

CSRF

Cross Site Request Forgery



DEMO: CSRF

CORS

DEMO: CORS

Аутентификация и авторизация в микросервисной архитектуре

Есть проблемы?

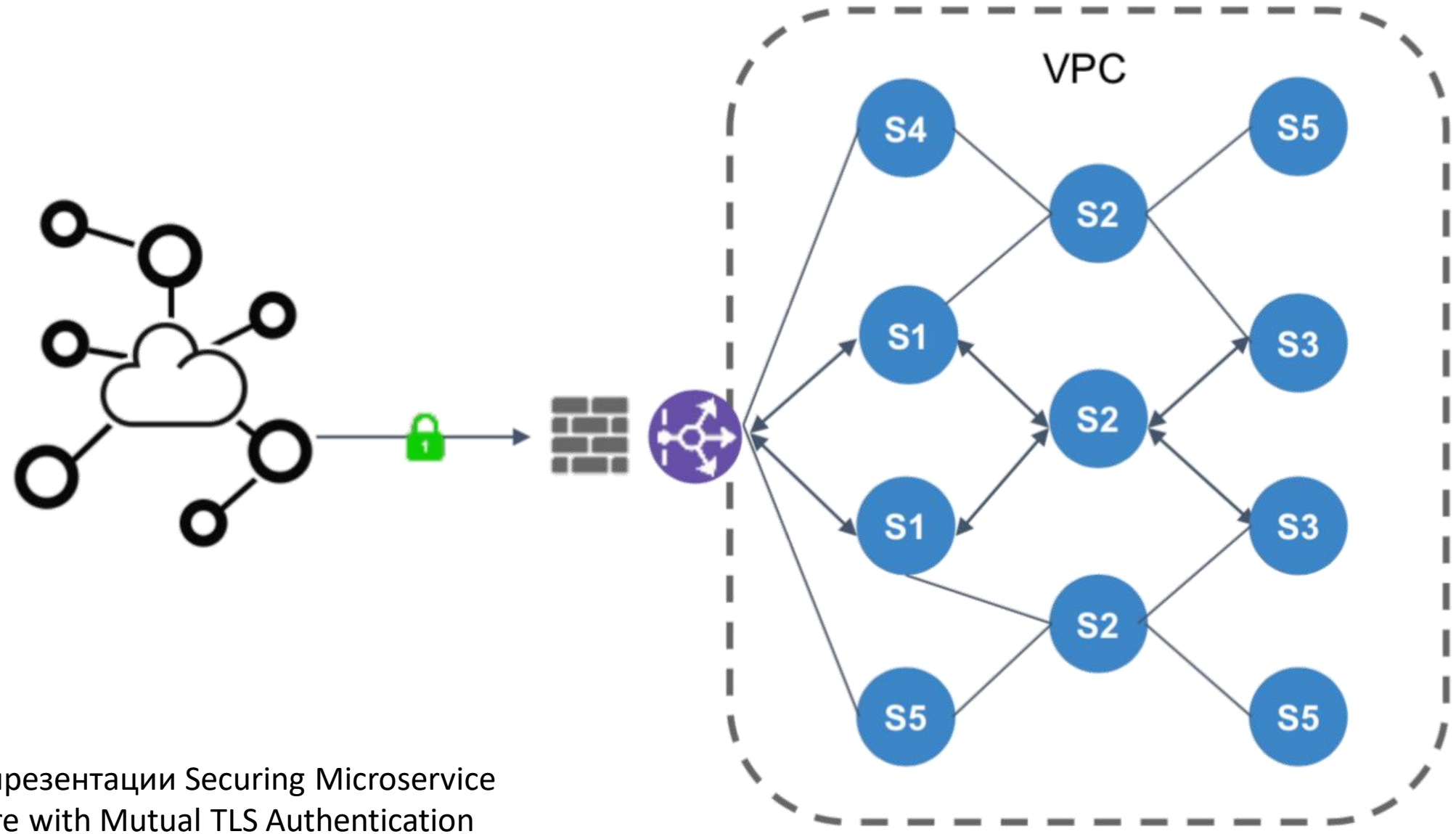


Схема из презентации Securing Microservice Architecture with Mutual TLS Authentication

Что хочется

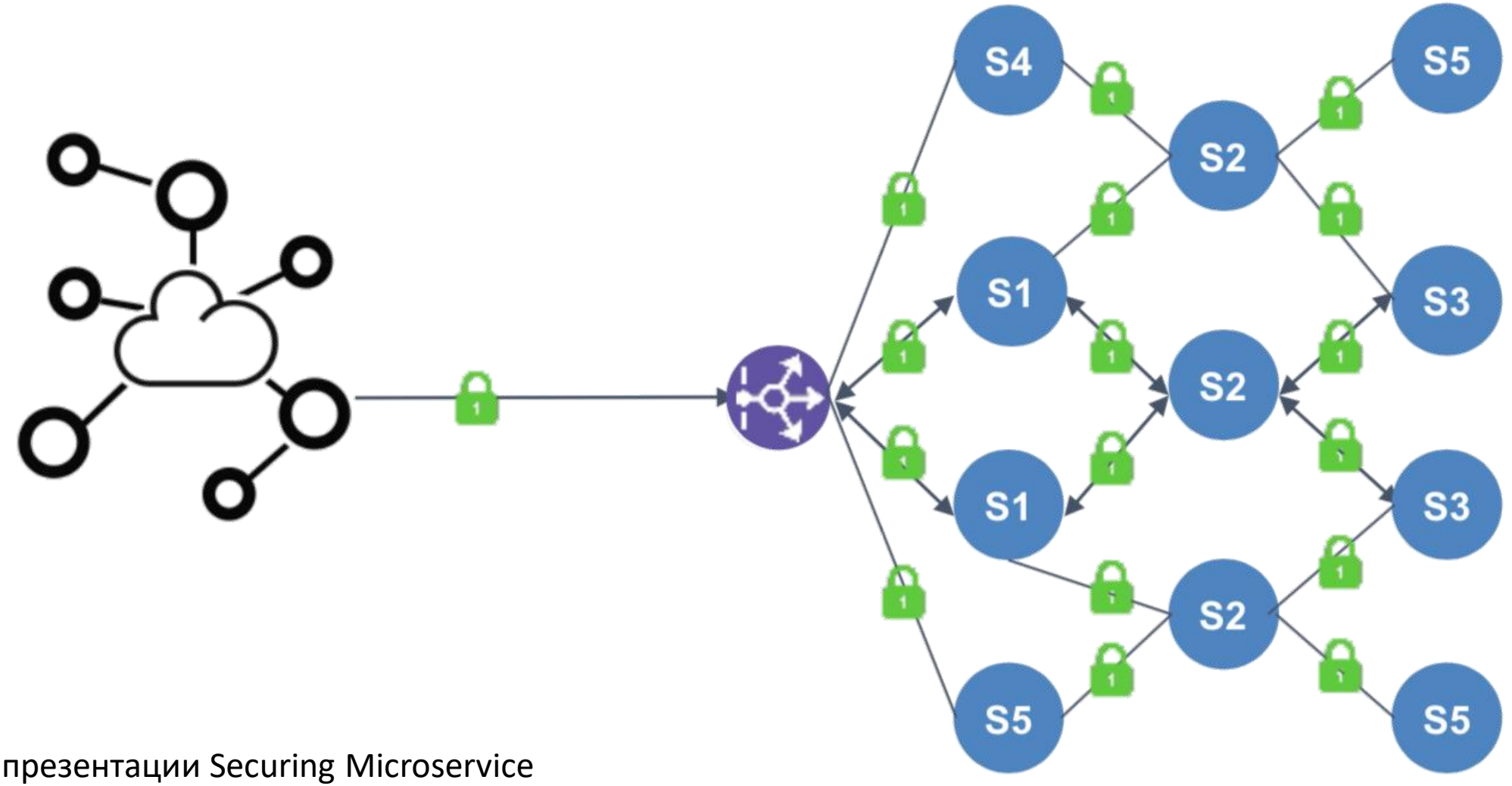
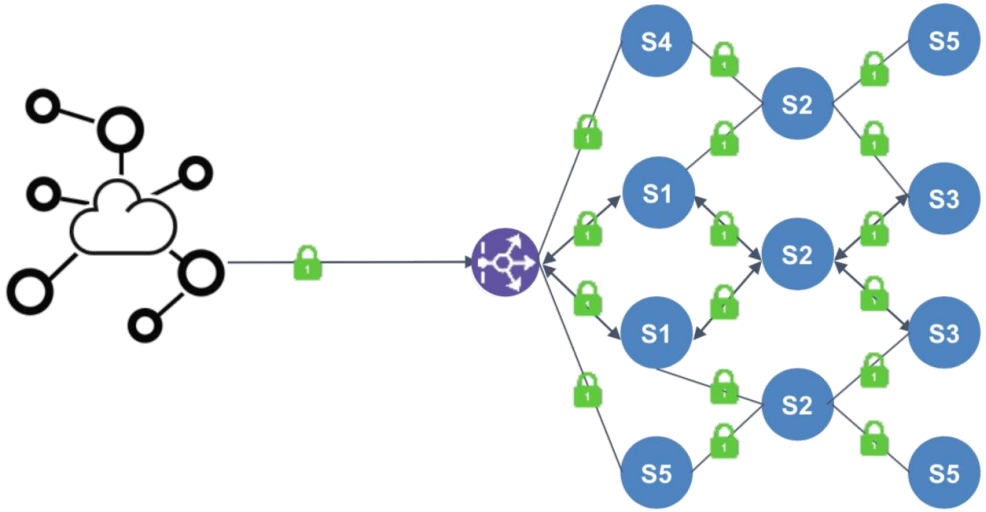


Схема из презентации Securing Microservice Architecture with Mutual TLS Authentication

Задачи



- Взаимная аутентификация микросервисов
- Защищенный транспорт
- Авторизация запросов к микросервисам

Схема из презентации Securing Microservice Architecture with Mutual TLS Authentication

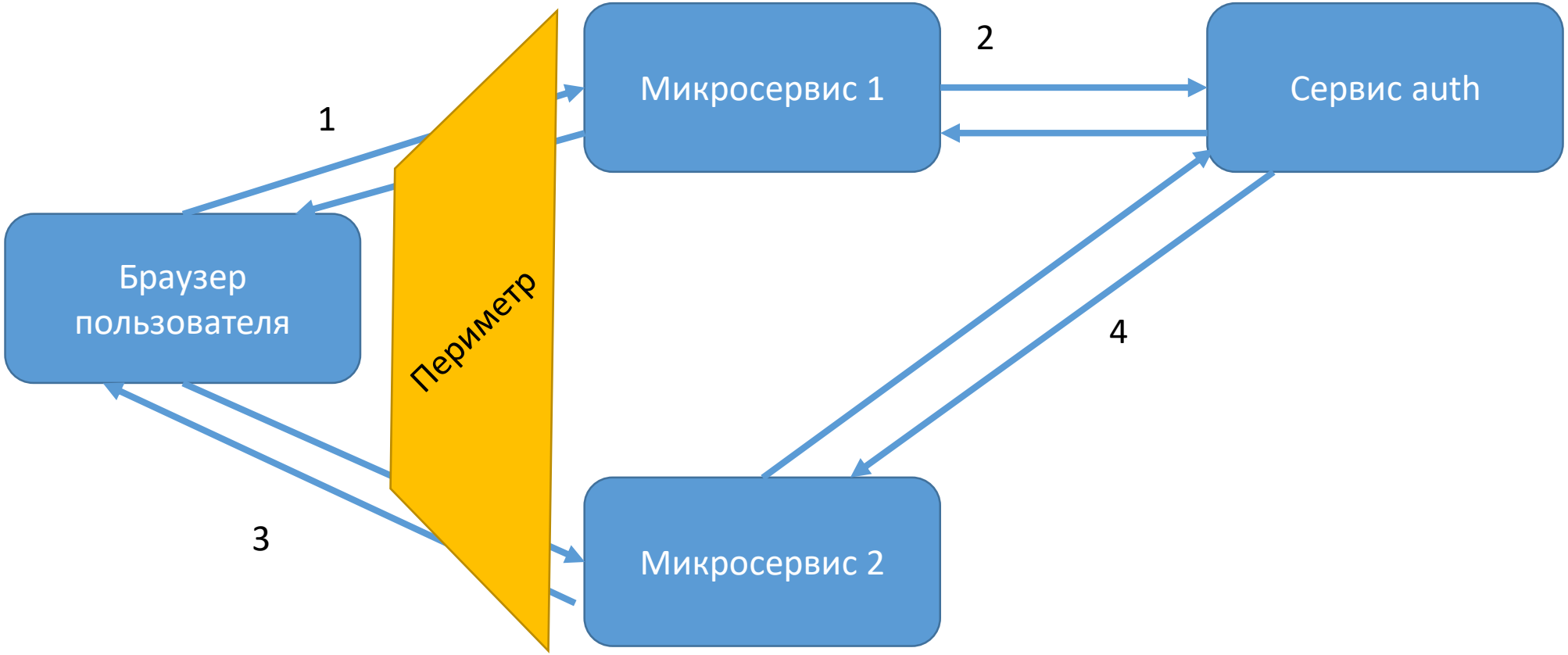
Взаимная аутентификация микросервисов

- Не нужна – мы в ~~домике~~ периметре
- На уровне инфраструктуры (ACL)
- С использованием общего секрета
  - токен в заголовке, параметре (cookie и http auth как частный случай)
  - нужно управление общими секретами (bootstraping/provisioning)
- С использованием ассиметричной криптографии (SSL-сертификаты)
  - нужен свой PKI (bootstraping/provisioning)
  - защищенный транспорт в виде бонуса
- Identity провайдер (внешний или внутренний)

Авторизация запросов к микросервисам

- Оставляем cookie во всех запросах, микросервис должен пойти к Security Manager и спросить, можно ли пользователю его вызвать
- Claims-based authorization
  - JWT
- Комбинированная схема
  - на клиент отдается session id
  - между микросервисами ходит токен с правами
  - gateway выполняет конвертацию

Вариант auth* 1



JSON Web Token

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ
```

Decoded EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

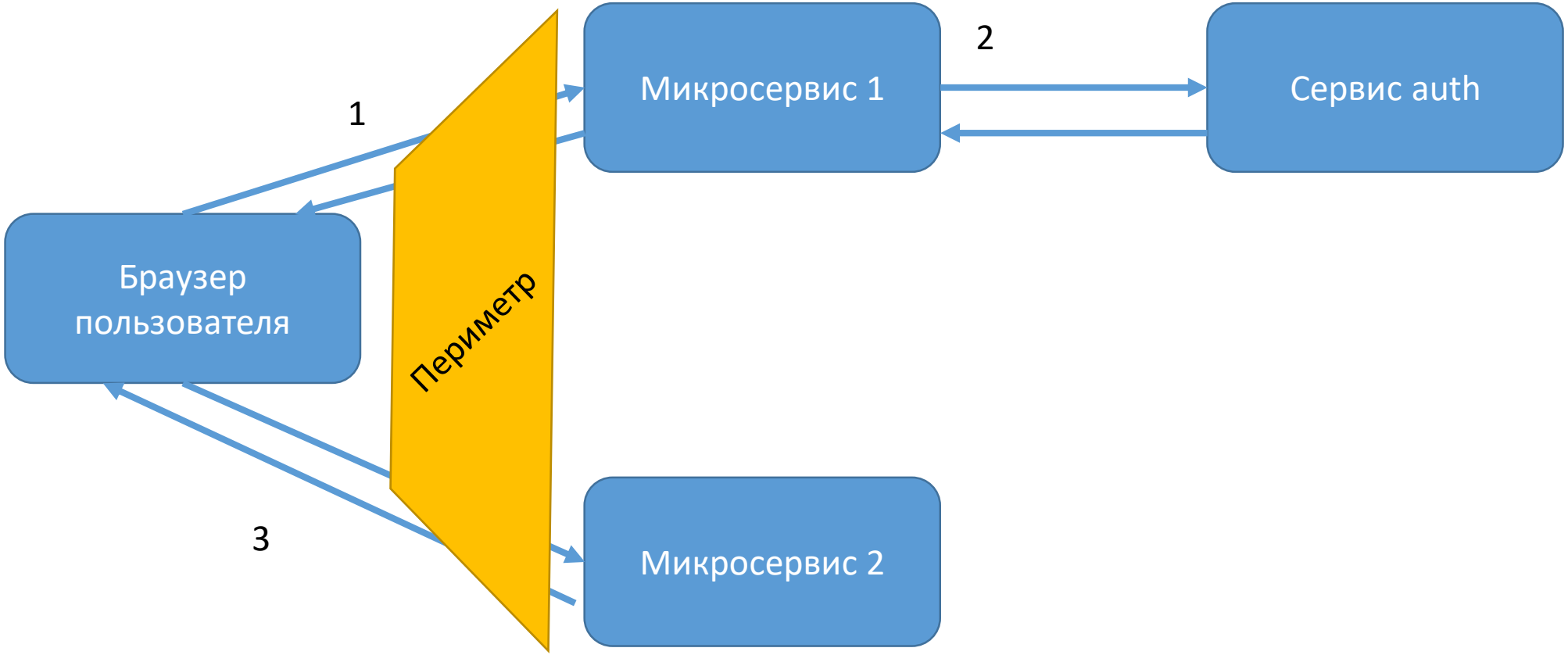
PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
) secret base64 encoded
```

Вариант auth* 2



DEMO: JWT

Задача на понимание

- У нас есть микросервис генерации PDF-отчетов по операциям.
- Какие угрозы связаны с его использованием?
- Как с ними бороться?

Задача на понимание

- У нас есть микросервис генерации PDF-отчетов по операциям.
  - Генерация происходит с помощью создания html-страниц по шаблонам и последующей печати pdf в headless браузере (QtWebKit), запущенном в микросервисе.
- Какие угрозы связаны с его использованием?
- Как с ними бороться?

Литература

- CSRF и cookie
  - https://habr.com/post/272187/
- CORS
  - https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS
  - https://portswigger.net/blog/exploiting-cors-misconfigurations-for-bitcoins-and-bounties
- Authc & Authz в микросервисах
  - https://jwt.io/
  - https://medium.com/tech-tajawal/microservice-authentication-and-authorization-solutions-e0e5e74b248a
  - https://www.slideshare.net/lmeirosu/mtls-securing-microservice-architecture-with-mutual-tls-authentication