Implementing an API in ASP.NET Web API

Module 3: Securing the API

Shawn Wildermuth
Wilder Minds LLC
http://wilderminds.com

pluralsight
hardcore developer training

Agenda

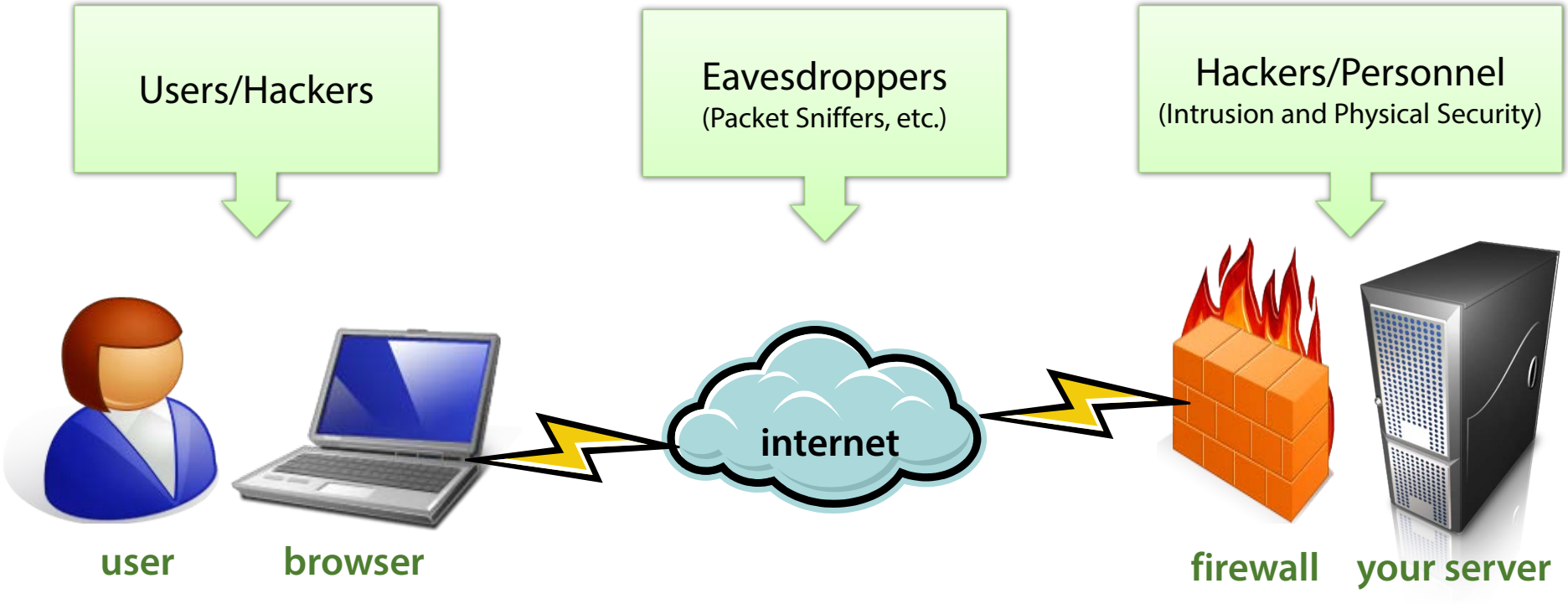
- **Securing the API**
  - APIs and Security
  - Cross-Origin Security
  - Authentication vs. Authorization
  - User Auth vs. App Auth
  - Using ASP.NET Authentication in Web API
  - Basic Authentication
  - Token Authentication
  - OAuth

APIs and Security

- Do you need to secure your API?

Are you…	Secure?
…using private or personalized data?	Yes.
…sending sensitive data across the 'wire'?	Yes.
…using credentials of any kind?	Yes.
…trying to protect against overuse of your servers?	Yes.

Threats to Your API



Security

- **Protect Your API**
  - Secure Your Server Infrastructure is outside scope of API security
  - Secure In-Transit
    - SSL is almost always appropriate
    - Cost of SSL is worth the expense…usually
  - Secure the API itself
    - Cross Origin Security
    - Authorization/Authentication

Supporting SSL

Cross Origin Security

- **To support calling from other domains:**
  - Support JSONP as Format
  - Enable Cross Origin Resource Sharing (e.g. CORS)

Supporting JSONP

Supporting CORS

- **In Web API 2 (not yet released)**
  - Allow CORS support out of the box

```
// WebApiConfig.cs
public static void Register(HttpConfiguration config)
{
  ...
  config.EnableCors(new EnableCorsAttribute());
}
```

Supporting CORS

- **In Web API 2 (not yet released)**
  - Can apply CORS per-controller/method

```
// WebApiConfig.cs
public static void Register(HttpConfiguration config)
{
  ...
  config.EnableCors();
}
```

```
// Your Controller
[EnableCors]
public class FooController : ApiController
{
  [DisableCors]
  public object Get()
  {
  }
}
```

Authentication vs. Authorization

- **Authentication**
  - Using Credentials to determine Identity
- **Authorization**
  - Verifying an Identity has rights to a specific resource

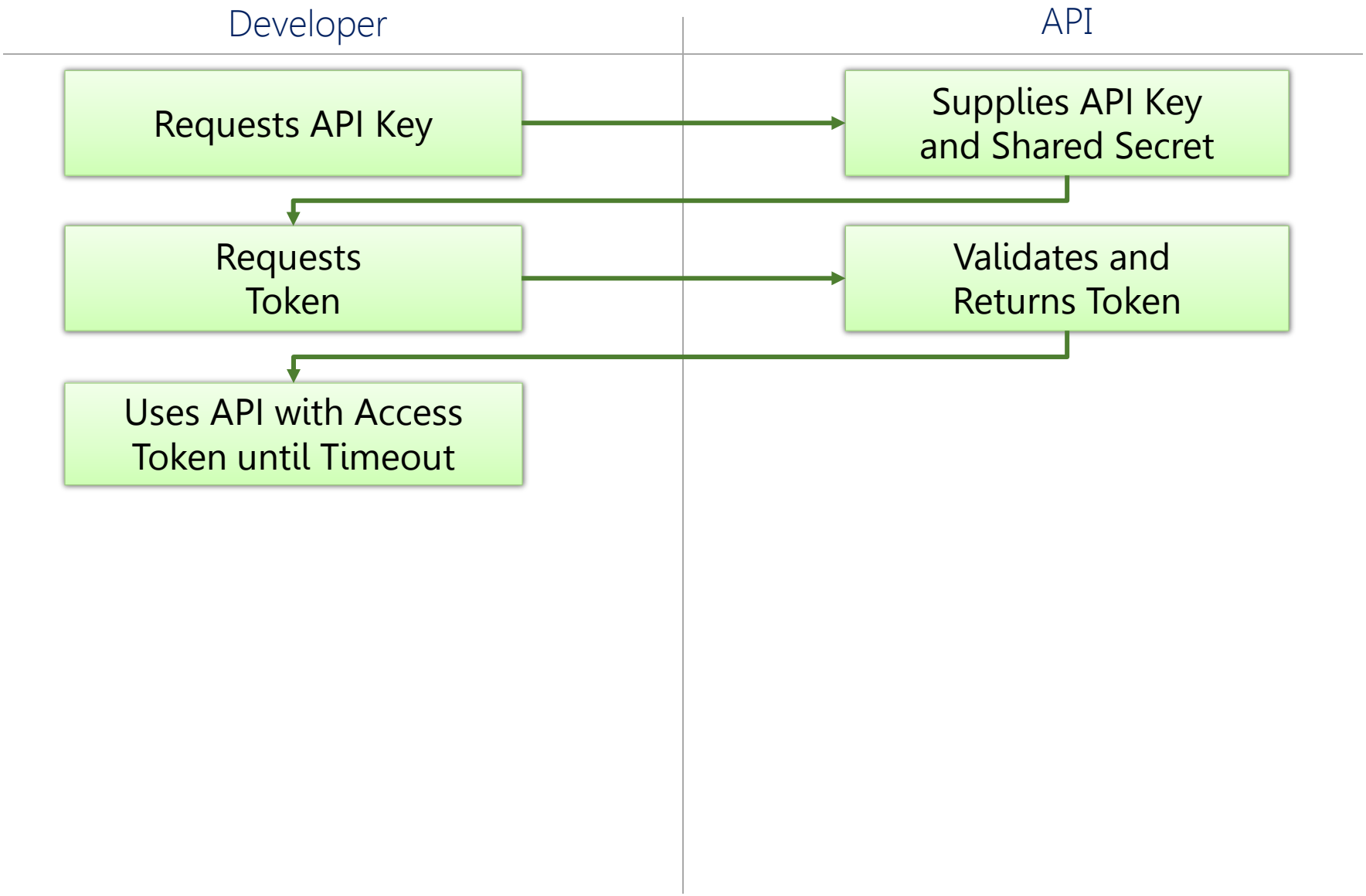
User Auth and App Auth

- **Who Do You Authenticate For?**
  - Allowing developers to use the API means App Authentication
    - Typically AppKey/Secret Pair
  - Authenticating Users is granting access to the API for users
    - Important for accessing user-specific data
    - Typically Basic Auth, OAuth and/or Integrated Auth

Piggybacking on ASP.NET Authentication

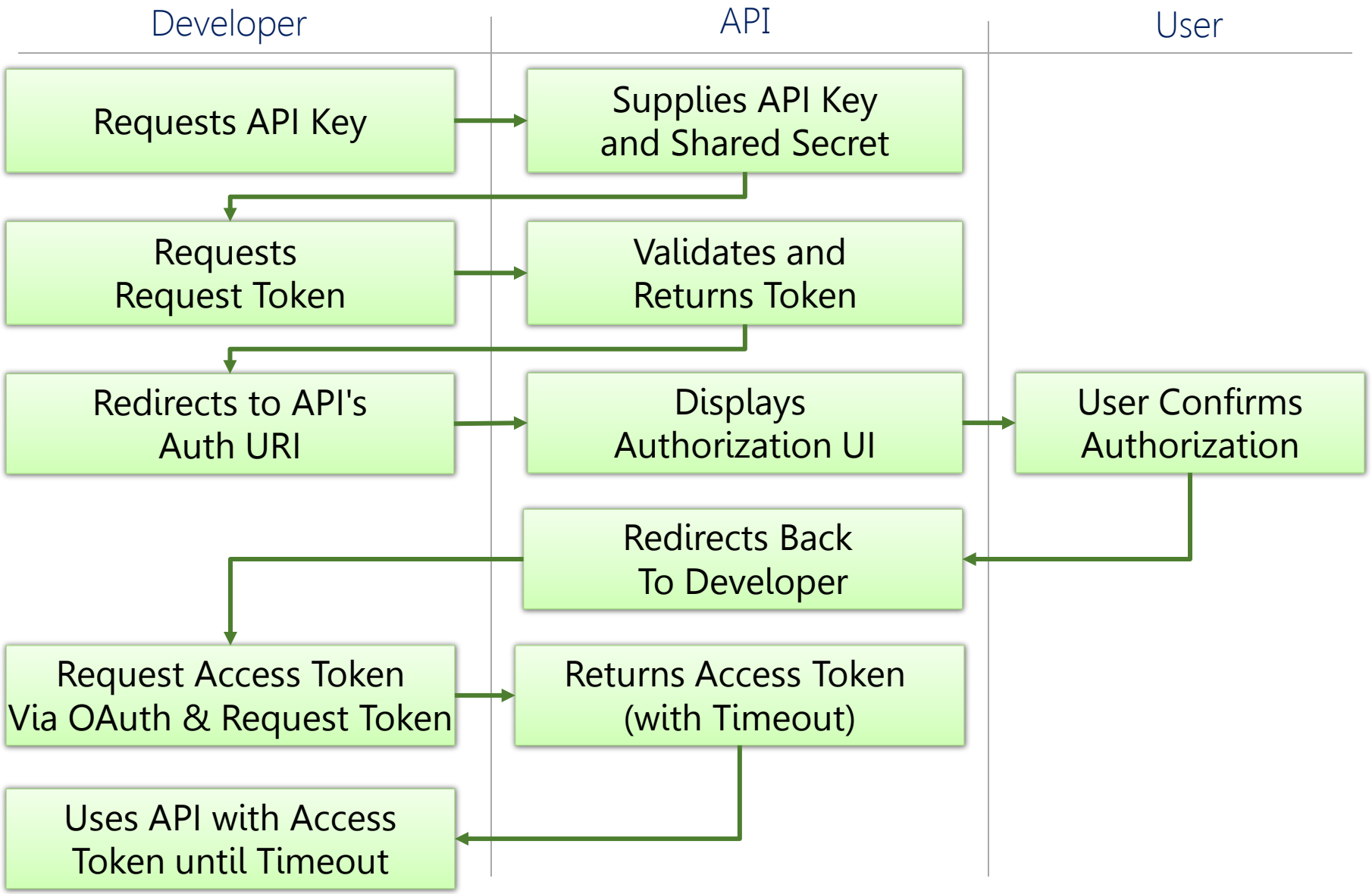
Implementing Basic Authentication

Token Authentication



Implementing Token Authentication

How OAuth Works



Walkthrough of OAuth Implementation

Summary

- **Securing Your API**
  - Requiring HTTPS is basic security requirement that you should implement
  - Using JSONP and/or CORS can allow your API to be used on other websites
  - Piggybacking on ASP.NET Authentication can simplify user Auth
  - Implementing Token-based App Authentication is Straightforward
  - OAuth can provide user-authentication without leaking user secrets