Trust No One
The New Security Model for Web APIs

Greg Kliewer
Principal Consultant, Solutions Architect
Layer 7, a CA Technologies company
October 8, 2013
What are Web APIs?
Old School APIs: Application Programming Interfaces

APIs are for connecting “software machines”

- Modules within a program
- Programs on a server
- Programs over local networks
Web APIs are for connecting “web machines”

- Over the World Wide Web
- Exploiting a globally-connected network
How Web APIs Evolved
Before there were Web APIs, there were **Web Apps**

- APIs protected by network separation
- No programmatic access from the Public Internet
- Safety through total isolation and control
Then came **Web Services**

**SOA / SOAP services**

- Used web technologies like HTTP, SSL/TLS, and language-independent, text-based grammar
- Applied mostly for internal application integration, like old school APIs
- BUT there was some limited uptake of SOAP web services for allowing programmatic access to core services by business partners and corporate customers
Security for Web Services
The model most of us are familiar with

- Establish TRUST with public key infrastructure
  - Private key / public certificate pairs
  - Have certificates signed by recognized CA / RA
  - Exchange that certificate with similarly-assured certificate from partners

- Apply asymmetric crypto at runtime to validate digital signatures / decrypt encrypted content
  - SSL/TLS Mutual Authentication
  - XML-DSIG/XML-ENC applied to SOAP documents

- TRUST partner / corporate customer to treat crypto material with care and caution
But now the disrupters are here
Mobile, Social, Cloud, and Embedded Applications

Require **programmatic access**

Do not support **PKI / Asymmetric Crypto**
*to prove their identity*
How can we safely expose Web APIs?
The new security model for Web APIs
In the new world there are exponentially more Apps to be served

Enterprise Apps, Portals, and Web Apps are being decomposed into Apps...
In the new world there are exponentially more Apps to be served

...and released into the wild
So if we are going to publish APIs to these new Apps...
...we had better require more regular and active scrutiny of the Apps’ access privileges...

- First of all, DO NOT issue long-lasting certificates to the Apps (e.g. x.509 expires in 1 yr)
- Instead, issue short-lived access tokens that can be revoked at any time

How long should the Apps have access without re-authenticating?

- Security Architect
- CISO

1 hour for info services
5 mins for financial txns
...we had better require more regular and active scrutiny of the Apps’ access privileges...

- Next, include the end user in authenticating / authorizing the App
- Explicitly *grant* access
- To a limited *scope*
Introducing **OAuth**

The new security model for **Web APIs**

- Open standard **specification** by IETF WG

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.
OAuth adoption
The big guys...
OAuth adoption...and YOU

86.5% of organizations will have an API program in place within 5 years.

- 43.2% currently have an API program
- 27% implementing one in the next year
- 12% implementing one in the next 2-3 years
- 4.3% implementing one in the next 4-5 years
- 13.5% no plans to implement an API strategy

A broad range of key business aims are driving the requirement for API programs:

- Mobility programs are driving 71.9%
- Partner connectivity is driving 69.1%
- Cloud integration is driving 67.6%
- Enabling internal developers is driving 66.9%
- Fostering external developer ecosystems is driving 55.4%
How to learn more
Where to learn more

- **Come talk to us!**
  - Booth #505
  - We’re here today and tomorrow

- **API Academy**
  - Online resources
  - Workshops

- **OAuth Online**
  - [http://oauth.net/](http://oauth.net/)
  - [https://www.ietf.org/mailman/listinfo/oauth](https://www.ietf.org/mailman/listinfo/oauth)

- **Primers**
  - By Aaron Parecki
  - By Jakob Jenkov

- **Publications**
  - The 5 OAuth essentials

- **Blogs**
  - By Francois Lascelles