Question	Response	Response By
what is difference between oauth and hmac message	HMAC is for computing digests of messages, for example with Amazon AWS usage of two API Keys (Secret Key ID which is used for computing the digest, and the Access Key ID which is used for identification). OAuth is used for delegated authorization.	Mark O'Neill
Where does OpenConnect Id fit into this picture	OpenID Connect (OIDC) provides a very userful "UserInfo" API endpoint to look up user attributes based on an OAUth Access Token. So it builds upon OAuth in a very useful way. At Axway we see it being used in this way, and is a useful part of ABAC (to obtain the attibutes used in ABAC)	Mark O'Neill
Any guidance on protecting legacy APIs that are not inherently designed for security? Without complete rewrite / re-engineering?	the API Gateway pattern allows you to place security in front of the legacy (e.g. Plain Old XML / POX) APIs. You can also use the API Gateway pattern to create a virtualized REST API in front of the legacy XML API.	Mark O'Neill
What's the difference between using SAML vs. OAuth from a security perspective?	SAML arguably has a stronger security profile due to digital signatures, however OAuth has wide adoption because developers find it easier to use (and they do not have to deal with XML). Important - BOTH need TLS	gunnar peterson
are the vulnerabilities OS based and tracked by the major sources of vulns? Or are they specific to API/s?	usually API vulnerabilities are at the application layer, but there are some that are specific to particular stacks which often relate to underling OS's (e.g. a full stack Microsoft environment)	Mark O'Neill
Recommendations for migrating from a username/password for an API to SAML or OAuth?	I think either can work, see previous answer, if you need more specifics let me know	gunnar peterson
Building a private REST API that will be used only by web apps and mobile apps developed within our org. Evaluating both SAML and OAUTH, what would you recomend?	Either can work. As a security person I feel like I am in a defensible position with either. I would recommend looking at sample code and building out a reference implementation to see which works with your dev team. Salesforce.com has some sample code to look at for example	gunnar peterson
Q1. Why is the statement - Oauth better than TLS? I was under the impression that both are needed in order to secure	Both are needed. OAuth is at the app level, TLS is at the network level. TLS protects the channel through which OAuth passes	gunnar peterson
How can we take care of DDOS?	DDOS is still taken care of at the network layer - e.g. using Akamai or AWS CloudFront. API Security doesn't replace protection for large scale DDOS	Mark O'Neill
are there different certifications for people doing API security assessments? What should the customer look for as a validation of their capabillities?	currently there isn't a certification, but it is a good question. security certifications such as ISC2 or CISSP are a good indicator, though those of course are not dedicated to API security	Mark O'Neill

How can we leverage API gateways for context based authentication? Can we dynamically challenge for a second factor if detected that the context may have been compromised. In other words is there and authn/authz authorities that the API gateway can levera	Super cool topic, risk based auth is usually a mix of fingerprinting - transactions, usage, patterns. Very powerful, but requires some back end data stores and analytics as well.	gunnar peterson
What would be some security best practices for Hackathons?	Great questions. I have seen the anti-pattern of hackathon organizers removing authentication from their APIs in order to "make it easier for them to be used in a hackathon". I don't recommend that. It is better to make use of an API Portal for the hackathon, where developers can authenticate and see sample API calls, including (for example) OAuth Access Tokens. At Axway our API Portal provides this generation of tokens, to help developers understand the security model of the APIs. A dedicated API Developer Portal for the hackathon also provides a simple "menu" of the APIs which can be used in the hackathon, with documentation, samples, etc	Mark O'Neill
What about HMAC that can be used without TLS?	HMAC provides digests over messages, usually as part of authentication and ensuring message integrity (detecting if it has been tampered it). it doesn't provide encryption of the data itself. So you need TLS for the encryption part. In general it is recommended TLS 1.2 is used, as a given, even when using HMAC for digest of the message itself.	Mark O'Neill
What about JWT? How does that fit in?	JWT (JSON Web Tokens) are often used as a way to package attributes as JSON, and associate them with an OAuth Access Token. In this way, they provide a great way to pass attributes about the user to the API itself, so that fine-grained Authorization can be performed right at the API (or, the API usage can be personalized for the end-user based on the attributes in the JWT token)	Mark O'Neill
Is it assumed that the API Gateway and the APIs themselves are local to each other -- IOW, a private connection between the API Gateway and the API servers?	In my view, its best if they are physically and logically separate, but logical separation alone is way better than nothing	gunnar peterson

What is the best way to go about helping developers learn how to prevent SQL injections?	OWASP has some great information, including example mod_security rulesets which protect against attacks like SQL Injection at www.owasp.org [at Axway we embed mod_security in our API Gateway to enforce these rules]	Mark O'Neill
If there are older proprietory or domain specific communication protocols that lack security how to add security to these communications? E.g. medical software protocols.	First step is usually to ensure you do NOT do lowest common denominator - work toward highest level for each hop. For true legacy, sometimes out of band can work. Try to initiate or validate out of band if possible	gunnar peterson
What authentication mehcanism would you recommend for api that are consumed by only internal applications? Should it still use api manager?	In my view yes. For one thing its an admin convenience. For another its an API for security services that you would otherwise have to write yourself	gunnar peterson
As an API provider, how can I ensure credentials/tokens are not compromised by the client? For e.g., I can force them to use a client secret, but they might have the secret hardcoded/insecure place that will allow malacious user access to it & compromise	good question - e.g. with many API providers they make it clear that the client must ensure that the client API keys are not compromised. So, it the responsibility is on the client. Often, an API Gateway is used at the client side to protect the keys. Many organizations use an API Gateway like the Axway API Gateway at the client side for this reason (security of API keys in the outbound direction)	Mark O'Neill
Which version oauth 1.0 or 2.0?	For use cases that need end to end protection, I prefer signed security tokens which is older version of OAuth	gunnar peterson
How does this interact with other Axwway products like sentinel?	Axway Sentinel is integrated with the API Gateway, and can be used for monitoring. Axway Passport is also integrated, for customers who are using both. In addition, many Axway products have APIs of their own (e.g. Secure Transport) and the API Gateway, and Axway API Management in general, can be used to manage these APIs.	Mark O'Neill
what is the best industry practice - Is it to terminate the TLS in DMZ or terminate at the application layer inside the network?	usually it is already been terminated in the DMZ using Application Delivery Controllers from Citrix, Cisco, etc. When this is already being done, it makes sense to still do this, but use the X-Forwarded header to propagate info about the client (E.g. IP address) from the client through to the API itself. TLS can then be used from the DMZ to an internal layer of APIs or API Gateways (i.e. security is not stripped off)	Mark O'Neill
How does Axway deal with Availability, Scalability, Reliability, Supportability,…?	these are covered in our best practices and deployment guides, which we can provide if you contact Axway	Mark O'Neill

For the order of operations vulnerability, are you stating we should assume that calls can come in in any order and therefore we should carry out ALL expensive security checks in all calls?	in the Axway API Gateway, the order can be managed in a "flowchart" type UI, so you are doing AuthN first, then AuthZ, then content validation. so this narrows down the attack surface so that the security processing is being done in a smart and efficient way	Mark O'Neill
How do you see the relation between an api gateway and an Security Token Service (fe adfs)?	Here at Axway our API Gateway embeds a Security Token service to "mint" OAuth Access Tokens and SAML Attributes. So, two can be linked. But we also have customers who connect to external STS's like PingFederate or Microsoft (ADFS)	Mark O'Neill
Is there a best practice for scope definition? Tied to operations allowed per user per API, do you map to Verbs in a RESTful scenario?	Verbs is a good idea, per user is less common in the field, but can work too. Have to be conscious of you will manage and scale the policy	gunnar peterson
When do you choose SAML over Outh Vice Versa for API authentication? What are pros and cons of each?	Great question - SAML arguably has stronger security properties (w digital signatures). But developers have tended to prefer OAuth, simpler to implement, no XML overhead. There are some security challenges here, for example read the OAuth Threat MOdel in IETF spec which is ~60 pages long	gunnar peterson
Would you consider ABAC being mature to bring is as a method for access modeling and seure auhorization. Other methds suggested for externalized access management o do you suggest to rely on the underlying application	Roles by themselves are necessary but not sufficient, so Roles need attributes (ABAC) to answer the question - not just are you in the Role Doctor, but do your attributes prove you should have access to this operation, this patient, this hospital	gunnar peterson
does axway provide policy's that implement owasp mod_security basic rules, because I supose everybody should implemnt them on there api gateway	yes - and, of course, you can also use third-party (or your own) mod_security rules	Mark O'Neill
where can the owasp basic ruleset policy's be downloaded or found?	OWASP provides this, or there are third-party providers (some with subscriptions) who also provide rulesets covering the OWASP Top 10 https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project	Mark O'Neill
How do you see the link between an api gateway and an STS?	related and sometimes they can be bundled, gtwy can call sts. Mark says: At Axway our API Gateway embeds an STS do you can issue tokens right in the Gateway (for performance reasons), or else call our to PingFederate, ADFS, or other dedicated STS products	Mark O'Neill