"8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016"

“ Hackers stole £2.5m from 9,000 Tesco Bank customers"

Are your APIS secure?
Top 10 threats
and How to Prevent Them

"Hackers apparently accessed the app's database through an unprotected API"

“One OAuth 2.0 hack, 1 Billion Android App Accounts potentially exposed"

How do they work?

#1

API SSL Vulnerabilities

SSL and TLS communication requires handshakes between the client and server in order to negotiate the security and establish the secure protocol tunnel. The threat vectors for SSL vulnerabilities include compromising the client, compromising the SSL server, compromising the algorithms used to secure the SSL, or compromising the C-based toolkit implementations to create buffer exploits.

What APIs are Most Vulnerable?

- APIs that are exposed using products with C-based security libraries such as OpenSSL
- APIs that are enabled with SSLv3, or TLSv1.0/1.1

- APIs that are enabled with SSL2.0, or TLS1.0, 1.1
- APIs that use insecure cipher suites to negotiate the TLS tunnels
- APIs that use weak key sizes
- APIs that do not enforce client authentication

#2

010101
010101
010101
010101

API URL Parameter

Manipulation of hidden fields in HTML form inputs can be performed in order to manipulate information such as product costs that may be inherently used by the application in billing. Similarly, the URI itself may be modified to alter values in the attempt to access information not pertaining to the original request such as account numbers, profiles, session identifiers, etc. Man-in-the middle proxy applications can also inject this information.

What APIs are Most Vulnerable?

- APIs that use REST paradigms with URI query string parameter values
- APIs that pass data via HTML web forms
- APIs that pass information as URL encoded data
- APIs that do no validate form values or URL parameter values
- APIs that do not check and restrict HTTP headers

#3

API HTTP Method Attacks

The HTTP Header is the first part of the HTTP conversation when a consumer connects to an API.   By altering methods in the HTTP header, an attacker can attempt to compromise information via update and delete methods, or compromise the application logic by passing HTTP headers that are not known by the API and therefore allowed through to the application which can result in data compromise.

What APIs are Most Vulnerable?

- APIs that use HTTP or HTTPs
- APIs that are defined with CRUD REST paradigms
- APIs that do not inspect HTTP headers for RFC conformance
- APIs that do not limit HTTP headers
- APIs that can not perform dynamic access control based on the HTTP method

#4

PASSWORD

API HTTP Signature

Hashing and signature digest algorithms vary in strength and risk profile. Depending on the model of hashing and digest calculation, the methods of security based on the resulting hash or digest calculation can be reverse engineered, or spoofed to gain access to the application behind the API

What APIs are Most Vulnerable?

- APIs that use weak hashing algorithms for HTTP security
- APIs that use weak digest algorithms for content signatures
- APIs that use weak symmetric keys
- APIs that do not provide cryptographic acceleration
- APIs that do not limit payload sizes

#5

API Identity Attacks

Weakness in identity comes in many forms. First the usage of solely password based credentials is a common vector for stolen credentials, or brute force attacks that guess the credentials. Once an authentication is achieved, an attacker can access anything that the impersonated user could get access to.These attacks are designed to achieve a data breach or loss of privacy information based on weak identity enforcement.

What APIs are Most Vulnerable?

- API frameworks that do not have a secure OS
- APIs that enable privileged access based on credentials alone
- APIs that use passwords or other single-factor authentication schemes
- APIs that do not enforce role-based access control based on the authenticated user
- APIs that do not perform data inspection

#6

API XML Attacks

Weakness in XML security processing is inherent in applications not explicitly designed to securely process XML data. Attacks designed to break the parser are crafted such as XML Entity Expansion and Recursion Attacks . Attacks targeting the Application behind the API are XML document size attacks, well-formedness, XQuery injection, SQL Injection, and other data injection mutations

What APIs are Most Vulnerable?

- APIs that send or receive XML data
- APIs that do not detect XML attacks
- APIs that do not have a secure XML parser
- APIs that do not limit size of request or response data
- APIs that do not provide schema validation conformance

#7

API JSON Attacks

Weakness in JSON security processing is inherent in applications not explicitly designed to securely process JSON data.   Attacks designed to break the JSON parsing engine and the value mapping deserialization. Attacks targeting the application behind the API are JSON document size attacks, well-formedness, JSON command injection, SQL Injection, and other data injection mutations.

What APIs are Most Vulnerable?

- APIs that send or receive JSON data
- APIs that do not inspect data contents
- APIs that do not have a secure JSON parser to detect JSON vulnerabilities
- APIs that do not limit size of request or response data
- APIs that do not provide schema validation conformance

#8

API Denial of Service

APIs are transactional in that they are designed to accept requests and provide responses. Each API transaction is meant to have an expected duration of time it takes to complete, and an expected amount of impact to the applications serving the business logic behind the API.
API DDOS can be achieved in several ways, the most common is data size, data complexity, invalid data, concurrency, and slow transaction reading/writing.

What APIs are Most Vulnerable?

- APIs that have SLA expectations
- APIs that do not inspect data for application format or size conformance
- APIs that do not limit read/write speeds
- APIs that do not limit size of request data
- APIs that do not limit based on concurrency of Users, IPs, or Groups

#9

API Embedded Malware Attacks

APIs provide the conduit for message exchanges, but lack the ability to inspect and parse data at the business context level of the request and response flows.   Embedded BASE64 malware is encoded within the XML and JSON payloads, and often encrypted as well. This allows the malware threat vectors to pass through any other cybersecurity architecture undetected because the raw malware is never isolated for detection

detection.

What APIs are Most Vulnerable?

- APIs that send or receive XML data
- APIs that send or receive JSON data
- APIs that allow SOAP with Attachments
- APIs that provide HTTP upload capabilities
- APIs that provide other types of encoded file transfers

#10

API Encryption Attacks

Encryption attacks hide the threat vectors such as malware and injection attacks from inspection because the encrypted content does not match the signature profile of the threat. If the encrypted data is only decrypted by the back-end application, the API does not have visibility into the raw data, and thus is similar to passing along a black box of data of which the contents are unknown.

What APIs are Most Vulnerable?

- APIs that send or receive XML data
- APIs that send or receive encrypted data
- APIs that are unable to decrypt and encrypt request and response messages
- APIs that do not perform data inspection
- APIs that do not provide asymmetric and symmetric cryptography capabilities

Are you Sentry Secured?

☑ API Transport Security

- Protocol-break (no direct path to endpoint)
- Accelerated TLS with no OpenSSL
- RFC protocol compliance
- Secure protocol mixing

☑ API Threat Mitigation

- Content-based threat vector mitigation
- Embedded on-board AV engine
- BASE64 content inspection
- Top 10 API and OWASP threat protection
- RegEx pattern engine
- Rate and size throttling

☑ API Message Security

- Bi-directional request/response content anallysis
- Context-aware Layer 7 processing
- Message format conversion

☑ API Data Integrity Assurance

- Request and response data validation
- URI and protocol header validation
- PKI Sign and Verify
- Symmetric and Asymmetric PKI

☑ API Identity and Access Control

- Multi-factor and multi-context authentication
- Identity repository protection
- RBAC, CBAC, ABAC
- Identity token conversion
- SAML, OAuth and OpenId Connect SSO and Federation

☑ API Data Privacy Assurance

- PKI Encrypt and Decrypt
- Encoding and Decoding
- URI, Header, and Data obfuscation