OWASP

Open Web Application Security Project

OWASP
The then, the now, and the future

Henry Hu

Chief Research Officer / OWASP Taiwan Chapter
Chief Technology Officer / VSSecurity, Inc.

CISSP / CISM / CISA / CEH / CHFI / ISO 270001 LA

Seasoned IT professional with over 20 years of security and IT related architecture, planning, implementation and consultation under his belt.

Security Audit	**95%**
Malware	**80%**
Data Analytic	**95%**
Programming	**75%**
Pre-Sales	**95%**

OWASP
Open Web Application Security Project

OWASP – An Introduction

The Open Web Application Security Project

- Web Security
- Application Security
- Vulnerability Assessment

- Founded on 2001
- 8 Employee
- 42,000+ Volunteers

OWASP
Open Web Application Security Project

We are everywhere!! (well… almost!)

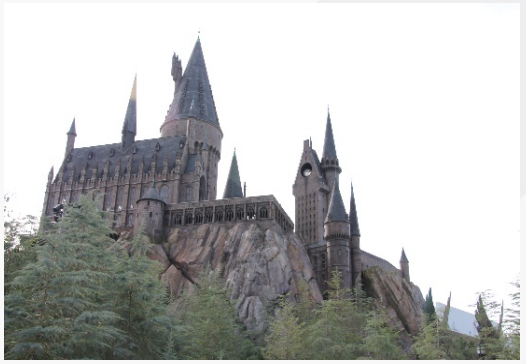
OWASP
Open Web Application Security Project

OWASP is not…

Private forums

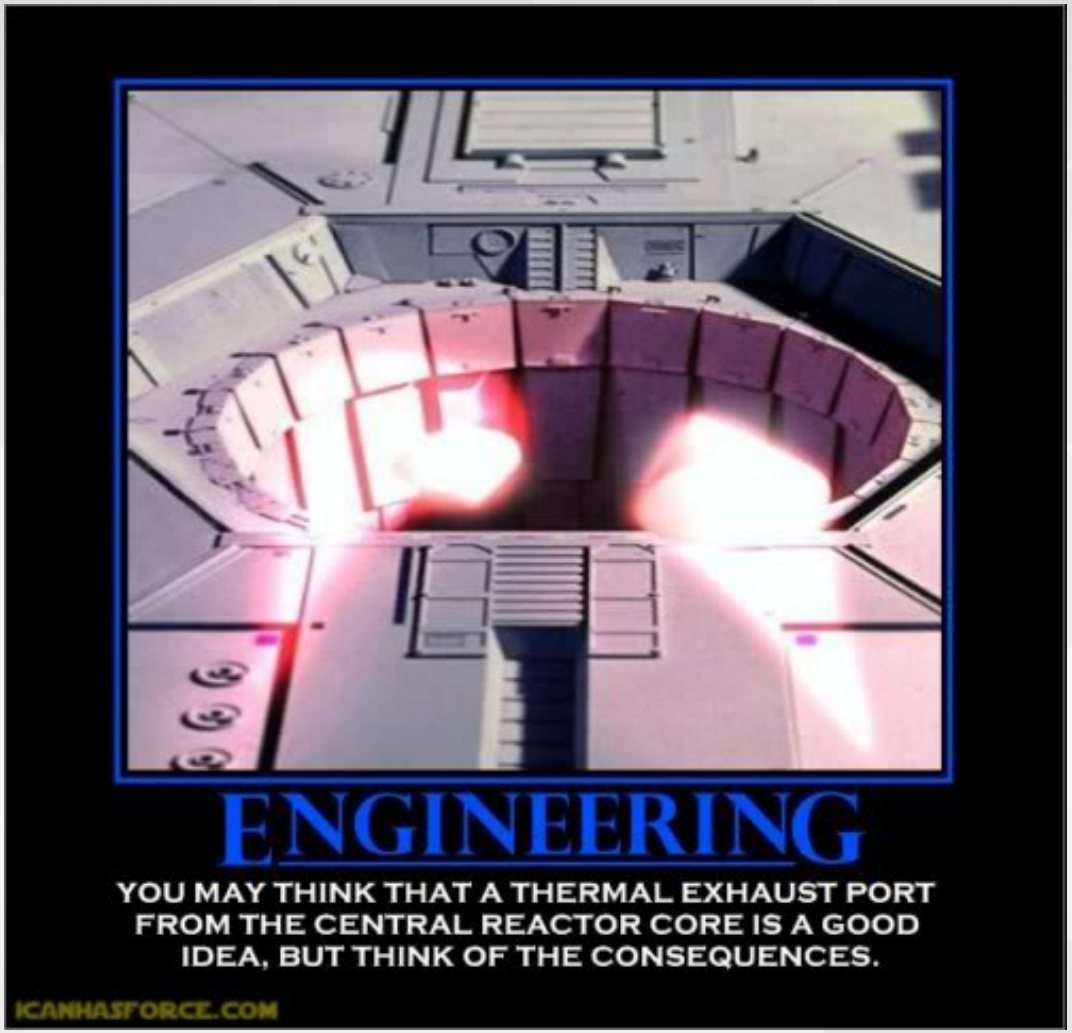
L33t haxorzing

Private 0day

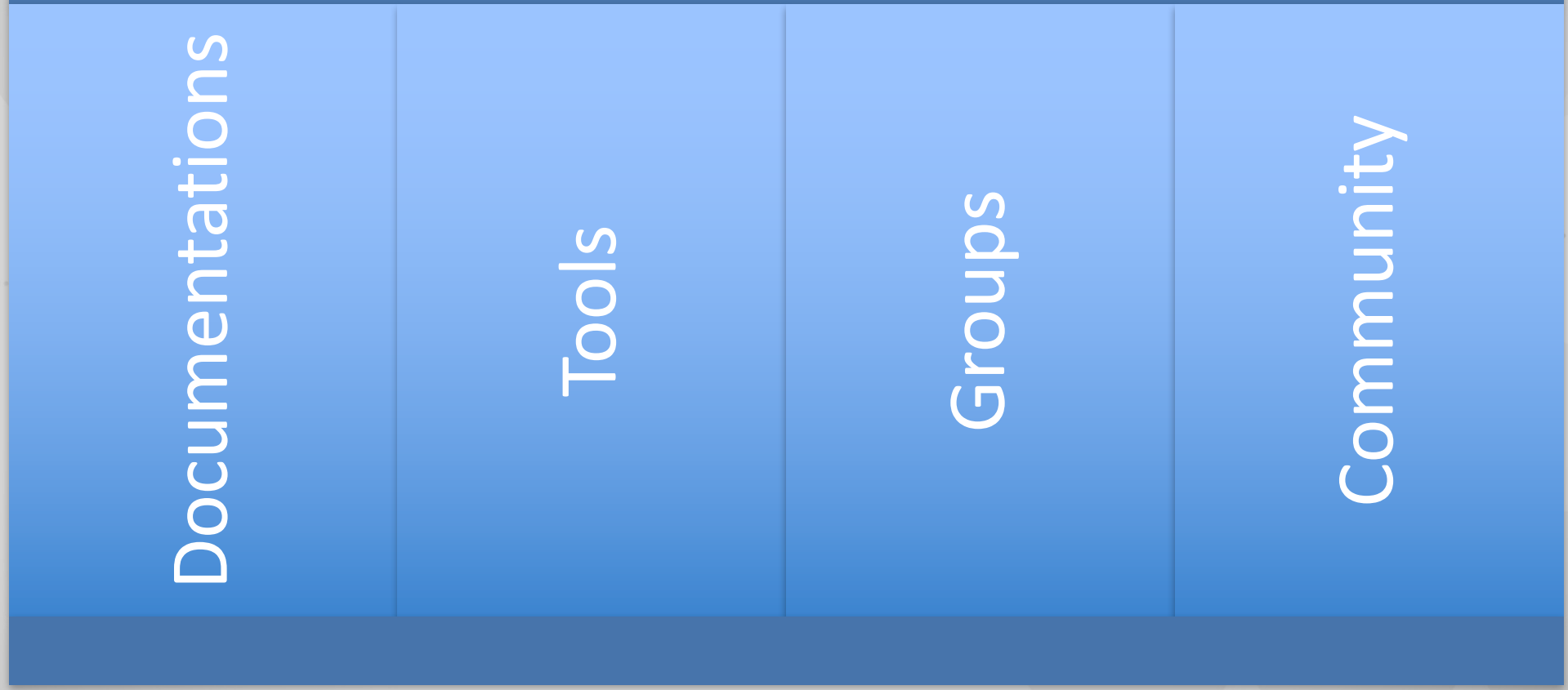


Hogwarts School of Witchcraft and Wizardry

Mad 0wnag3 sk1lz


ENGINEERING
YOU MAY THINK THAT A THERMAL EXHAUST PORT FROM THE CENTRAL REACTOR CORE IS A GOOD IDEA, BUT THINK OF THE CONSEQUENCES.
ICANHASFORCE.COM

OWASP Projects



OWASP Documentations

OWASP Application Security Verification Standard Project	OWASP Software Assurance Maturity Model	OWASP AppSensor Project	OWASP Top Ten Project	OWASP Testing Guide Project

OWASP
Open Web Application Security Project

OWASP Tools

OWASP Zed Attack Proxy	OWASP Web Test Environment Project	OWASP OWTF	OWASP Dependency Check

OWASP
Open Web Application Security Project

OWASP Code

OWASP ModSecurity Core Rule Set Project

OWASP CSRFGuard Project

OWASP AppSensor Project

OWASP Groups

Browser Security	Industry Sectors	Access Control	Education

OWASP
Open Web Application Security Project

OWASP Community

Local Chapters	Conferences	Tutorials	Mailing List

OWASP
Open Web Application Security Project

Other OWASP Projects

OWASP Development Guide

OWASP Code Review Guide

OWASP XML Security Gateway Evaluation Criteria Project

OWASP Risk Rating Management Project

OWASP Top 10 Incident Response Guidance

OWASP WebScarab

OWASP Webgoat

OWASP AppSec Pipeline

OWASP
Open Web Application Security Project

About the OWASP Top 10

OWASP Top 10 is an Awareness Document

- Not a standard…

First developed in 2003

- Was probably 3rd or 4th OWASP project, after
  - Developers Guide
  - WebGoat
  - Maybe WebScarab ??

Released

- 2003, 2004, 2007, 2010, 2013

What Didn't Change

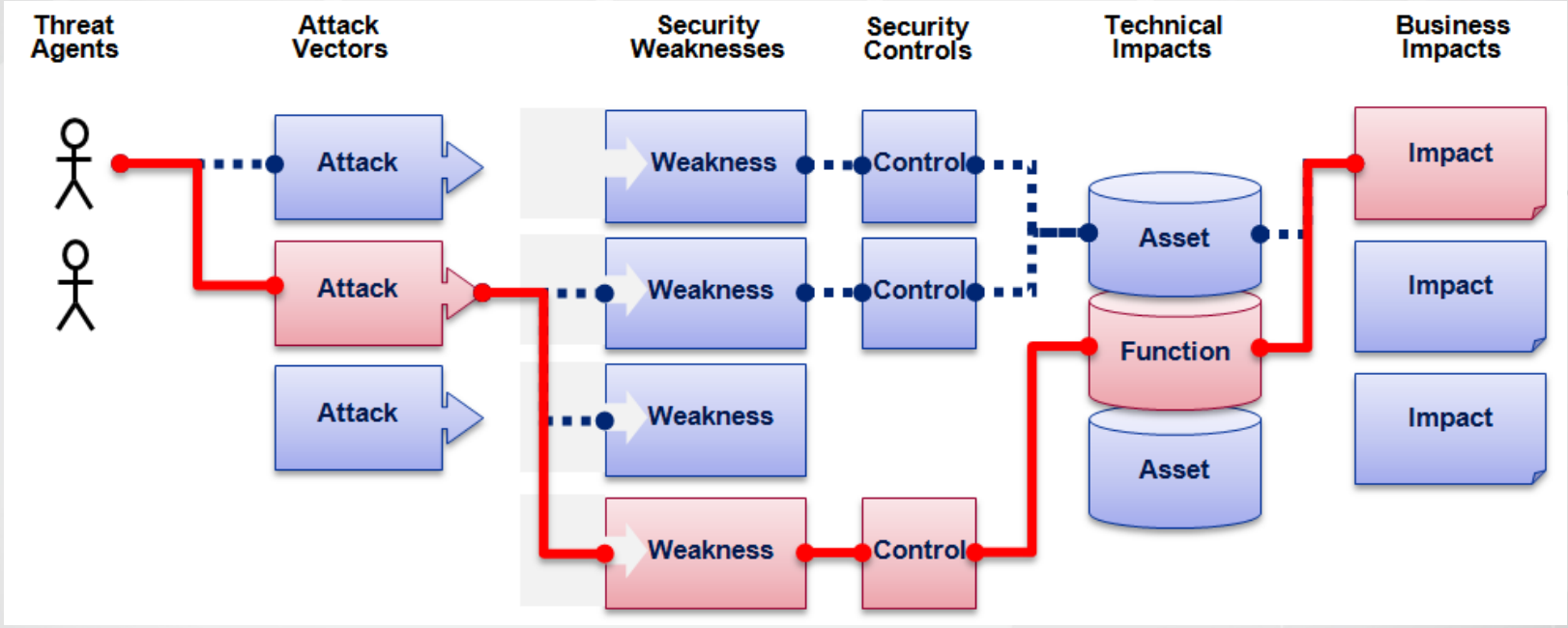
It's About Risks, Not Just Vulnerabilities

- Title is: "The Top 10 Most Critical Web Application Security Risks"

OWASP Top 10 Risk Rating Methodology

- Based on the OWASP Risk Rating Methodology, used to prioritize Top 10

OWASP Top 10 Risk Rating Methodology



OWASP Top 10 Risk Rating Methodology

Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
	1 Easy	Widespread	Easy	Severe	
?	2 Average	Common	Average	Moderate	?
	3 Difficult	Uncommon	Difficult	Minor	
	1	2	2	1	
		1.66	*	1	

Injection Example

1.66 weighted risk rating

CONNECT. LEARN. GROW.

OWASP Top 10 2003

- A1. Unvalidated Parameter
- A2. Broken Access Control
- A3. Broken Authentication and Session Management
- A4. Cross Site Scripting (XSS) Flaws
- A5. Buffer Overflow
- A6. Command Injection Flaws
- A7. Error Handling Problem
- A8. Insecure Use of Cryptography
- A9. Remote Administration Flaws
- A10. Web and Application Server Misconfiguration

OWASP Top 10 2004

- A1. Unvalidated Input
- A2. Broken Access Control
- A3. Broken Authentication and Session Management
- A4. Cross Site Scripting (XSS) Flaws
- A5. Buffer Overflow
- A6. Injection Flaws
- A7. Improper Error Handling
- A8. Insecure Storage
- A9. Denial of Service
- A10. Insecure Configuration Management

OWASP
Open Web Application Security Project

OWASP Top 10 2007

- A1. Cross Site Scripting (XSS) Flaws
- A2. Injection Flaws
- A3. Malicious File Execution
- A4. Insecure Director Object Reference
- A5. Cross Site Request Forgery (CSRF)
- A6. Information Leakage and Improper Error Handling
- A7. Broken Authentication and Session Management
- A8. Insecure Cryptographic Storage
- A9. Insecure Communication
- A10. Failure to Restrict URL Access

OWASP Top 10 2010

- A1. Injection Flaws
- A2. Cross Site Scripting (XSS) Flaws
- A3. Broken Authentication and Session Management
- A4. Insecure Direct Object References
- A5. Cross Site Request Forgery (CSRF)
- A6. Security Misconfiguration
- A7. Insecure Cryptographic Storage
- A8. Failure to Restrict URL Access
- A9. Insufficient Transport Layer Protection
- A10. Unvalidated Redirects and Forwards

OWASP
Open Web Application Security Project

OWASP Top 10 2013

- A1. Injection Flaws
- A2. Broken Authentication and Session Management
- A3. Cross Site Scripting (XSS) Flaws
- A4. Insecure Director Object Reference
- A5. Security Misconfiguration
- A6. Sensitive Data Exposure
- A7. Missing Function Level Access Control
- A8. Cross Site Request Forgery (CSRF)
- A9. Using Components with Known Vulnerabilities
- A10. Unvalidated Redirects and Forwards

OWASP
Open Web Application Security Project

OWASP Top 10 2017

- A1. Injection Flaws
- A2. Broken Authentication and Session Management
- A3. Cross Site Scripting (XSS) Flaws
- A4. Broken Access Control
- A5. Security Misconfiguration
- A6. Sensitive Data Exposure
- A7. Insufficient Attack Protection
- A8. Cross Site Request Forgery (CSRF)
- A9. Using Components with Known Vulnerabilities
- A10. Under Protected APIs

OWASP
Open Web Application Security Project

Who has always been on the list?

	2003	2004	2007	2010	2013	2017
Injection Flaws	6	6	2	1	1	1
Broken Authentication Management	3	3	7	3	2	2
Cross Site Scripting	4	4	1	2	3	3

Who rated second on the Top 10?

Misconfiguration and Mismanagement of Configurations (Web, Applications, Security)

The New Players to Top 10

Using Components with Known Vulnerabilities	Insufficient Attack Protection
Sensitive Data Exposure	Under Protected APIs
Insecure Direct Object References	Using Components with Known Vulnerabilities

Those That Comes and Goes

Unvalidated Parameter	Unvalidated Redirects and Forwards
Insecure Communication (Transport Layer Protection / Encrypted)	Buffer Overflow
Insecure Storage (Encrypted / Unencrypted)	Remote Administration Flaws

The Single Hit Wonders

- Missing Function Level Access Control
- Denial of Service
- Malicious File Execution
- Insecure Use of Cryptography

OWASP Mobile Top 10

- M1. Insecure Data Storage
- M2. Weak Server Side Controls
- M3. Insufficient Transport Layer Protection
- M4. Client Side Injection
- M5. Poor Authorization and Authentication
- M6. Improper Session Handling
- M7. Security Decision Via Untrusted Inputs
- M8. Side Channel Data Leakage
- M9. Broken Cryptography
- M10. Sensitive Information Disclosure

OWASP
Open Web Application Security Project

OWASP IoT Top 10

- I1. Insecure Web Interface
- I2. Insufficient Authentication and Authorization
- I3. Insecure Network Services
- I4. Lack of Transport Encryption
- I5. Privacy Concerns
- I6. Insecure Cloud Interface
- I7. Insecure Mobile Interface
- I8. Insufficient Security Configurability
- I9. Insecure Software / Firmware
- I10. Poor Physical Security

OWASP
Open Web Application Security Project

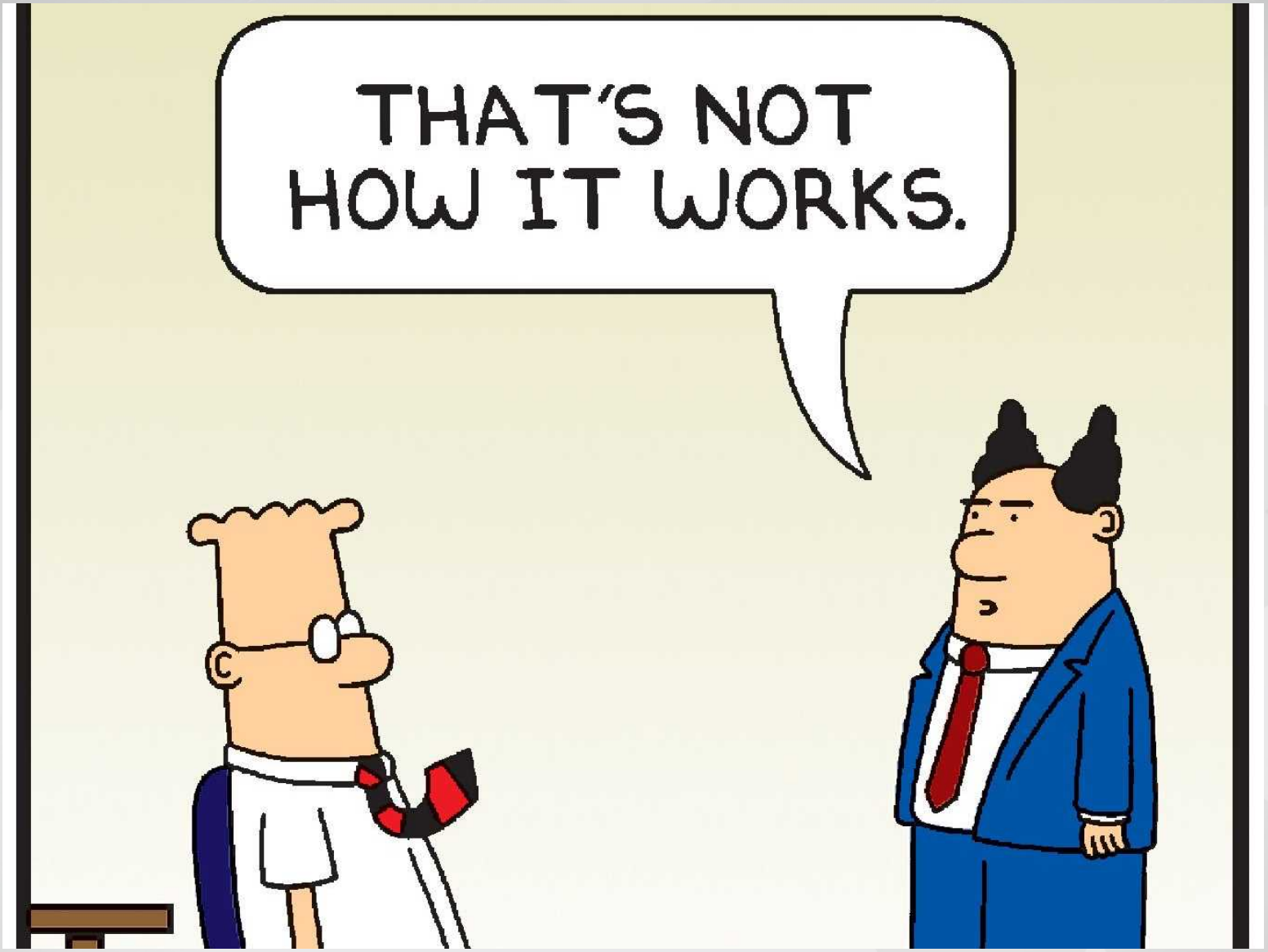
Moving on…

- Top Tens will again re-shuffle and new additions will come in place as the technology becomes more complicated.
- Authentication / Authorization factors will always be an issue.
- As services moves onward to cloud, more concerns will arise from cloud infrastructure

What can we expect in the future?

- API –
  - As API usage becomes more flexible and widely use, how API are form and written is critical
  - More security issues will arise from API usage, as well as how data is exchanged through API
- Web Infrastructure –
  - As more data are exchanged between infrastructures and devices, keeping it secured is yet another critical task (Communication / Encryption / etc.)

We all do our best to try and keep everything secured…
BUT! There will always be….


THAT'S NOT HOW IT WORKS.

OR…

BDU

is short for

Big Dumb User

.....

by allacronyms.com

Questions, Any?