**Assignment-2**

**Kunal Saini**

**2014053**

**Q1**

US based Companies

**Apple: - George Stathakopoulos (Vice President of Corporate Information Security)**

* Experience

Vice President of Information Security, Amazon (6 years 2 months)

GM of Product Security, Microsoft (8 years 9 months)

Engineer, Microsoft Corporation (5 years 5 months)

* Some of the top skills

Information Security, Cloud Computing, Security; Computer Security, Scalability, Distributed System etc.

* Responsibility

Protecting corporate assets, such as the computers used to design products and develop software, as well as data about customers.

Apple Inc, amid a pitched battle with the U.S. government over law enforcement's desire to crack into iPhones, has hired a new security executive to oversee its corporate digital defenses.

Profile Link: - <https://www.linkedin.com/in/george-stathakopoulos-85173020>

**Microsoft: - Bret Arsenault (Corporate Vice President and Chief Information Security Officer)**

* Experience

Seasoned executive with 25+ years of security experience in multiple technology disciplines. Bret has designed, implemented and led the information security organization for a multinational, Fortune 50 technology company for over a decade.

* Some of the top skills

Security, Information Security, Cloud Computing, Leadership, Risk Management, Leadership, Networking Engineering

* Responsibility

Enterprise-wide information security, compliance and business continuity efforts. Leads a global team of security professionals with a strategic focus on information protection, assessment, awareness, governance and enterprise business continuity.

Profile Link: -<https://www.linkedin.com/in/bret-arsenault-97593b60>

**Amazon: - Stephen Schmidt (Vice President, Security Engineering & Chief Information Security Officer)**

* Experience

##### [Rescue Operations Lieutenant](https://www.linkedin.com/title/rescue-operations-lieutenant?trk=mprofile_title), [Sterling Volunteer Rescue Squad](https://www.linkedin.com/company/1073140?trk=prof-exp-company-name)**(12 years)**

[General Manager, Technical Services](https://www.linkedin.com/title/general-manager%2C-technical-services?trk=mprofile_title), Amazon (2 year 2 month)

##### [Section Chief](https://www.linkedin.com/title/section-chief?trk=mprofile_title), [Federal Bureau of Investigation](https://www.linkedin.com/company/6408?trk=prof-exp-company-name)(10 years)

##### [Vice President](https://www.linkedin.com/title/vice-president?trk=mprofile_title), American Information Systems, Inc (5 years)

##### And do have many patients on his name

* Some of the top skills

Security, Information Security, Computer Security, Program Management, Cloud Computing, Security Clearance

* Responsibility

# Privacy and Data Security of Amazon AWS

# Link: - https://aws.amazon.com/blogs/security/privacy-and-data-security/

Profile Link: - <https://www.linkedin.com/in/stephenschmidt1>

India based Companies

**HCL: - Manoj Sarangi (Chief Information Security Officer)**

* Experience

#### [Group CISO & Head- Technology](https://www.linkedin.com/title/group-ciso-%26-head-technology?trk=mprofile_title), [Aditya Birla Group](https://www.linkedin.com/company/162288?trk=prof-exp-company-name) **(3 years)**

#### [Director, Enterprise Risk Services](https://www.linkedin.com/title/director%2C-enterprise-risk-services?trk=mprofile_title), [Deloitte](https://www.linkedin.com/company/1038?trk=prof-exp-company-name) **(1 year)**

##### [Member, Certification Advisory Board](https://www.linkedin.com/title/member%2C-certification-advisory-board?trk=mprofile_title), [IAPP](https://www.linkedin.com/company/643535?trk=prof-exp-company-name) **(1 year)**

#### [Chief Privacy and Security Officer, India & South Asia](https://www.linkedin.com/title/chief-privacy-and-security-officer%2C-india-%26-south-asia?trk=mprofile_title), [IBM](https://www.linkedin.com/company/1009?trk=prof-exp-company-name) **(4 year)**

##### [Program Lead](https://www.linkedin.com/title/program-lead?trk=mprofile_title), [Hewlett-Packard](https://www.linkedin.com/company/1025?trk=prof-exp-company-name) (4 year)

* Some of the top skills

Information Security, Business Continuity, Security, Risk Management, Security Management

* Responsibility

Information Security, Cyber Security, Data Privacy, Risk Management, Business Continuity,  
IT Service Delivery, Organizational Transformation, Security Metrics and Measurement

Profile Link: - <https://www.linkedin.com/in/manojsarangi?authType=name&authToken=a_vz&trk=prof-sb-browse_map-name>

**Infosys Ltd: - Vishal Salvi (CISO)**

* Experience

Salvi has 15 years of industry experience having worked in Crompton Greaves, Development Credit Bank, Global Trust Bank, Standard Chartered Bank before taking on the role of Chief Information Security Officer & Senior Vice President at HDFC Bank. Prior to joining HDFC Bank, he has worked in Standard Chartered Bank for eleven years and played variety of roles in IT Service Delivery, Governance and Risk Management and Information Security. At HDFC Bank, Vishal heads the Information Security Group and responsible for driving Information Security strategy and its implementation across the Bank & its subsidiaries.

* Some of the top skills

Security Strategy and its implementation, Information Security, Risk Management

* Responsibility

Vishal Salvi, one of the most recognizable names in the information security world, according to two executives familiar with the development.   
  
Salvi will be the company's new chief information security officer (CISO), filling a position that's been lying vacant since company veteran Prabhakar Mallya retired from Infosys in July 2014.

# Flipkart: - Ganapathi Subramaniam (Director - Information Security)

* Experience

#### [Chief Security Officer](https://www.linkedin.com/title/chief-security-officer?trk=mprofile_title), [Microsoft India](https://www.linkedin.com/company/1035?trk=prof-exp-company-name)(1 year 5 months**)**

#### [Global IT Security Lead](https://www.linkedin.com/title/global-it-security-lead?trk=mprofile_title), [Accenture](https://www.linkedin.com/company/1033?trk=prof-exp-company-name) **(**5 years 10 months)

#### [Head of IT Security Group - Global Compliance and Monitoring](https://www.linkedin.com/title/head-of-it-security-group-global-compliance-and-monitoring?trk=mprofile_title), [PricewaterhouseCoopers LLP](https://www.linkedin.com/company/1044?trk=prof-exp-company-name)**(1 year)**

#### [Head of Information Security & Risk](https://www.linkedin.com/title/head-of-information-security-%26-risk?trk=mprofile_title), [HML](https://www.linkedin.com/company/164199?trk=prof-exp-company-name)**(**5 years**)**

#### [Senior IT Audit Consultant](https://www.linkedin.com/title/senior-it-audit-consultant?trk=mprofile_title), [Skipton Building Society](https://www.linkedin.com/company/28603?trk=prof-exp-company-name)**(2 year)**

##### [Senior IT Consultant](https://www.linkedin.com/title/senior-it-consultant?trk=mprofile_title), [Ernst & Young](https://www.linkedin.com/company/1073?trk=prof-exp-company-name) (1 year)

#### [Manager - Information Systems Audit](https://www.linkedin.com/title/manager-information-systems-audit?trk=mprofile_title)****,**** [Thomas Cook](https://www.linkedin.com/company/166434?trk=prof-exp-company-name) (1 year)

#### [Systems Officer](https://www.linkedin.com/title/systems-officer?trk=mprofile_title), [Hindustan Petroleum Corporation Limited](https://www.linkedin.com/company/11668?trk=prof-exp-company-name) (6 years)

* Some of the top skills

Information Security, IT Audits, Security, IT Management

* Responsibility

Ensuring the security of the company in all aspects

**COMPARISON**

The profiles of US based companies seems to have more experience that the Indian profiles and not only the experience, the companies that they have worked for before were also the top companies among the world (top 5 fortune companies).This may be because in India security don’t seems to be the most important issue as compared to US because they have suffered and still suffering from various security attacks. And Indian profiles do lack in skills and popularity too. So conclusion; US wins the race in terms of security.

**Q2**

1. Recently a massive DDOS attack was made on the Dyn servers.Dyn is a major DNS service provider and some of its customers are Twitter,Spotify etc. The attackers this time attack the DNS service provider instead of a particular website ,so this time the data on the companies server were secure but the link that connect user to the website was under attact.The attack was made through bots (malicious programmes),The attackers exploiter the IOT’s vulnerability and over the month implanted these bots into the insecure IOT devices and they made multiple request at the Dyn servers due to which the server got shut and were not able to convert users requests into IP’s; names were not converted into IP’s and vice versa. Because of this half of the internet was down.

1. The blame for this attack has been firmly placed on IoT devices and as a supplier of connectivity to IoT and M2M devices. So securing these IOT’s is the technical mitigation to these attacks. The device should run a number of monitoring functions that look for potentially malicious interactions from unknown IP addresses. This will prevent a bot from trawling the internet and repeatedly trying to guess the username and password. The device needs to be regularly updated and its security analysed. Leaving a device unsupported for any length of time raises the potential of the device being compromised. As a manufacturer or designer of a connected device you cannot rely on the end user securing the device for you. Setting a unique username and password in the factory is the bare minimum, preferably you should insist these are changed when the device is first powered on (whether this is completed by the end user or remotely by the management company). A mistake common in the compromised devices was that the web interface username and password were separate to the command line versions; even the most security conscious end users wouldn’t have been able to secure the devices.

Secondly apart from securing the IOT’s ,when these kind of attack happen user could still access the website using the Tor browser or connect through VPN’s. Because the server near the region are not able to server the request but we if we could redirect the traffic to servers that are place in some other region the user will be able to access the websites as these DNS are relayed all around the world.

1. There should be some laws that these IOT’s manufacturing company should follow and insure some of the basic security to their devices so that they can’t be exploited .The IOT’s manufacturer’s should hire some good penetration testers and should launch their product after complete testing of the product .They should follow secure designing principles while developing to prevent the future sue of them.Gov. should ban the devices that are not secure and penalize the companies that are not following the laws (security principles).

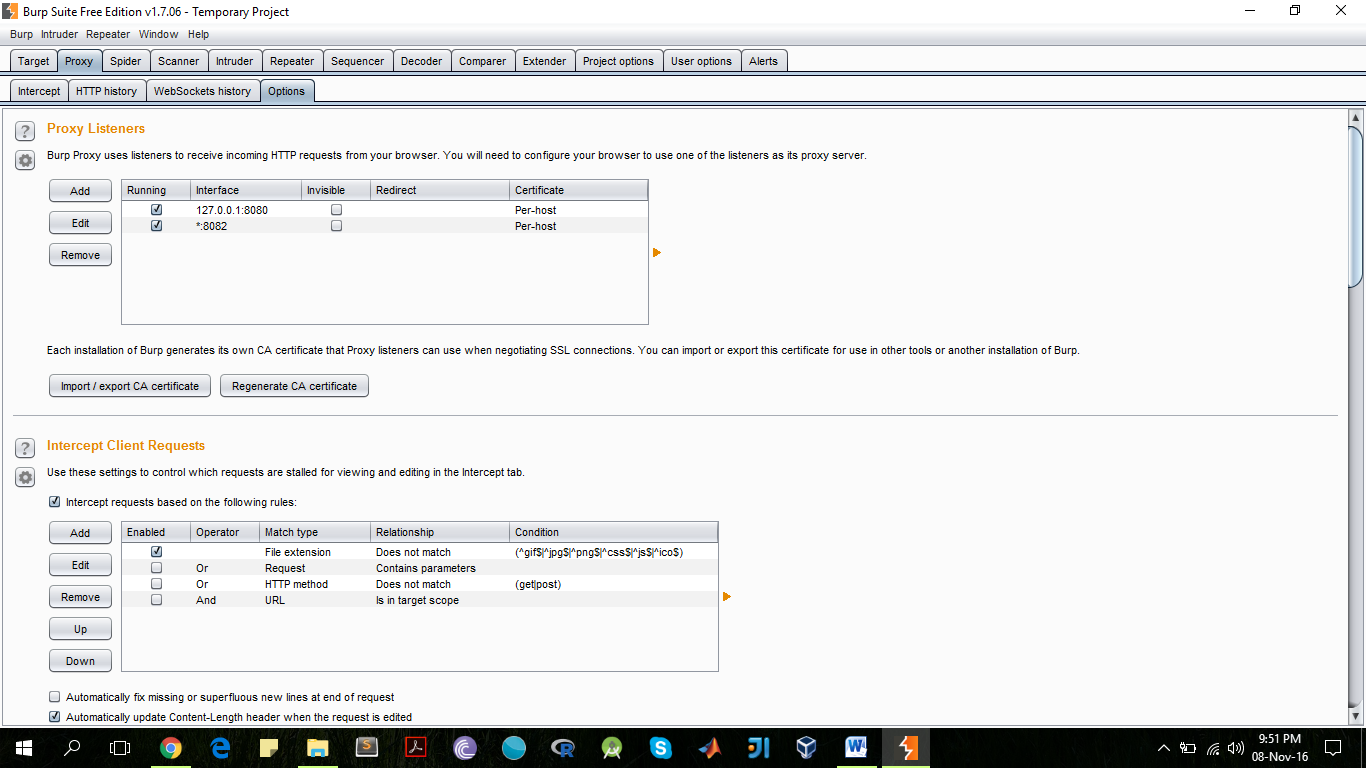
**Q4**

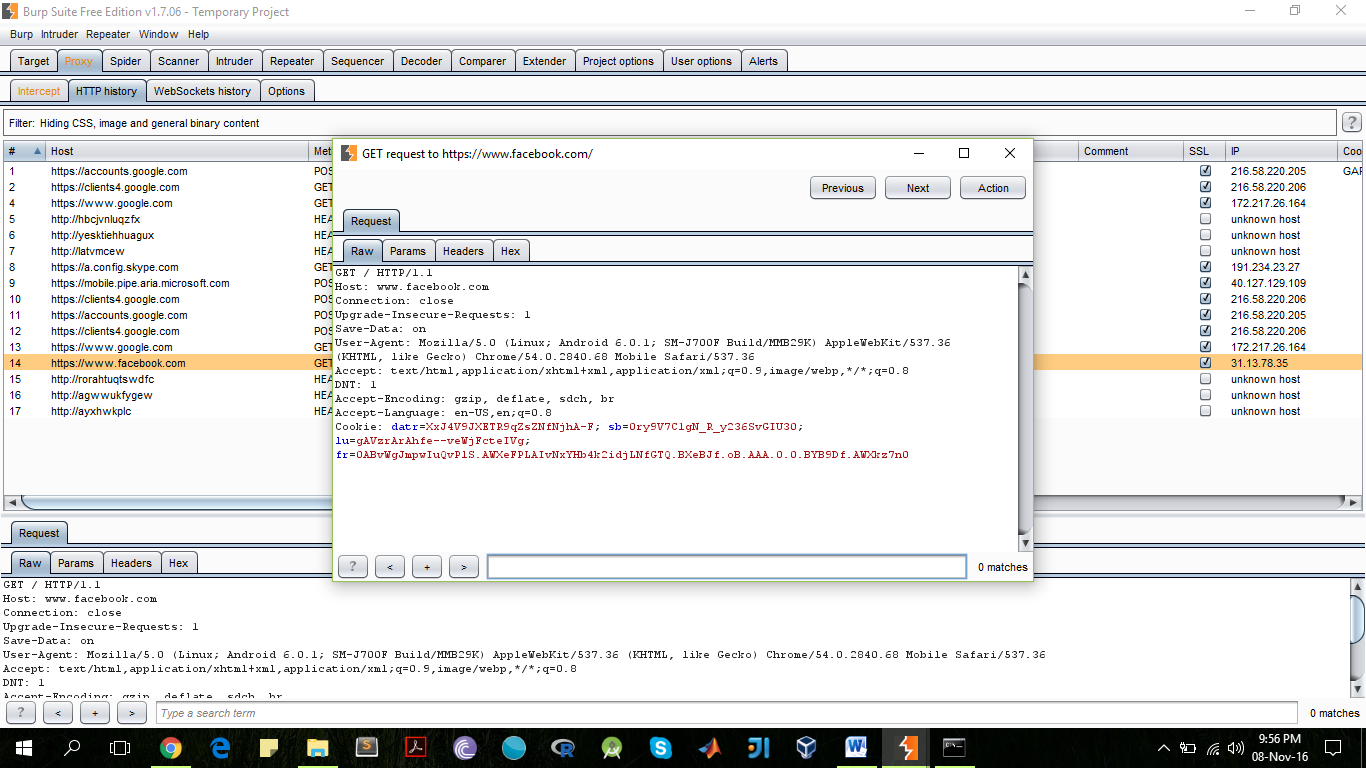
**Security/privacy related vulnerabilities: -**

Through Burp we can see/monitor all the traffic going to [www.facebook.com](http://www.facebook.com) , we can see all the packets, cookie, sessions that are send and receive from Facebooks sometimes we can see the access tokens and Facebooks graph api through which developer use to read and write the user's data, Facebook don’t allow the deletion of pictures but if we use it through mobile we can delete these pictures.

Apart from that we can see how the graph api which is also used by Facebook is communication while we are opening, deleting or scrolling over the page.

And through these request and responses we can sometimes see the access tokens, these access tokes are part of PII’s .If we can someone’s access tokens we can query to get data from Facebook, and what if we get multiple such tokens we can make a DDOS attack over Facebook server’s and make Facebook down without getting caught as these tokes will be registered on various accounts.





**Q5**

**Difference b/w Bell-LaPadula and Biba Model**

**Bell-LaPadula Model**

About Information Confidentiality

The model formally represents the long tradition of attitudes about the flow of information concerning national security.

It has 3 properties: -

* Simple; no read up
* Simple (\*); no write down
* Strong (\*); read and write at same level

Bell-laPadula star property rule means "no write down" -confidentiality

**Biba Model**

About Information Integrity

This model is based on the flow of information where preserving integrity is critical.

Preserves integrity, no limit access

Dual of Bell-LaPaudal model

Only one variant: - no read down, no write up and no execute up.

It uses invocation property.

BIBA start integrity axiom means "no write up" – integrity

**Subjects** **Objects**

**Order; create and validate (Customers)**

**Product; create and validate (Merchants)**

**Company Official Documents /Employee Details**

**Clerk**

**Manager**

**Accounts Keeper**

**Administrator**

**Information/Analysis Regarding Product and Orders**

**Biba:**

**No Read Down**

**No Write Up**

**No Execute Up**

Clear; can write/read the order and read the above but can’t write

Manager; can write/read the products, can’t read the order but can write them and read the above but can’t write.

Similar is the case for Accounts Keeper and Administrator.

**Bell-Lapadula:**

**Strong\* property: Read or write at the same level**

**+**

**Simple Security Property: No read up but can read below**

We will use a modified version which will consist of both the above mentioned property.

We can read and write at the same level with that we can give an extra privilege to read the below records as the Administrator should have write to access to all ;at least read all if now write.

**Which One Is Better?**

**A:** I think the second one that is Bell-Lapadulaversion is better as only the same level have access to write to the object in front of it as in this case if can thing goes wrong we can immediately capture the culprit as object are writing inly to the subjects that are at the same level and since the above one can read they can monitor too and report to the concerned authority regarding the person who is involved in that.