International Journal of Engineering &Technology, 7 (3.12) (2018) 81-83

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Changing Mechanisms of Enterprise Security (Comparing Beyond Corp with Prevalent Network Security Mechanisms)

B.Amutha[1], SwastiSaxena[2], Abhinaba Das[3]

[1]HOD CSE, [2,3]B.Tech , CSE(4th Year),
[1,2,3]SRM IST, Kattankulathur
**Corresponding Author Email: [1]bamutha62@gmail.com, [2]saxenaswasti0@gmail.com, [3]abhi.das94@gmail.com*

Abstract

War driving, camp out etc. are common methodologies of gaining access of a company's network and resources illegally. Packet capturing, out of thin air, brute force etc. are common mechanisms to gain key or password access to any company's applications. In the times where hacking and cyber-attacks have become prevalent, companies are deploying various network security mechanisms to counter these attacks and to safe guard company's applications and data. Beyond Corp is a new technology that is being used by Google these days to safe guard its applications. In this paper we will compare some of the network security mechanisms that many companies use to avoid cyber-attacks with Beyond Corp technology which is being used by Google to avoid security breach in the company's network and applications.

Index Terms: *Security, beyond corp , changing trends in security.*

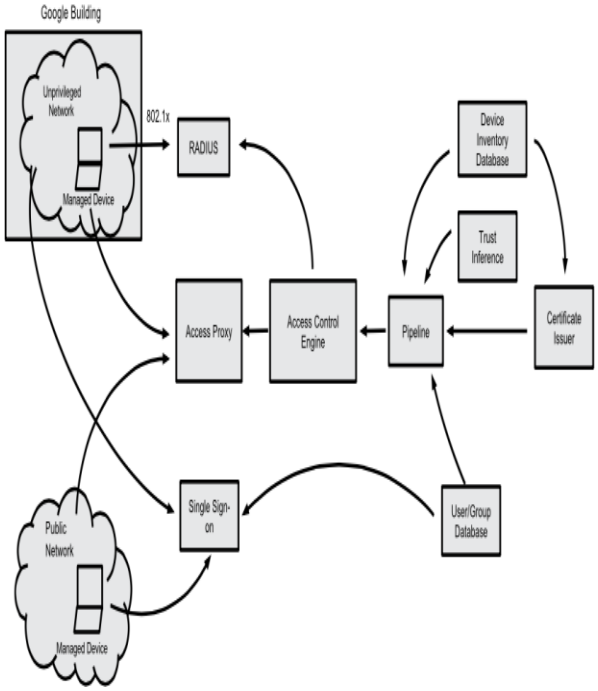
1. beyond Corp: Nascent Approach for Security of Firms and Enterprises, Currently Being Deployed By Google

Today the use of firewalls for network security is very common. Many big firms prefer to use firewalls for protecting their data from security breach. In today's era, using just firewall to protect company's privileged network may not solve the purpose. Companies are moving to cloud database and adopting mobile technology which may lead to more chances of data being vulnerable to cyber-attack as just by breaching the firewall all the company's data is at the attacker's disposal.

To avoid such security breaching of company's data, Google is moving its corporate applications to Internet. Today people may not be working just on one device or may even not be confined to working in an exclusive office environment by just using office intranet. Instead, today people work together from different geographic locations and may use different Wi-Fi connections eg. Of Airport, coffee shop or a personal mobile hotspot etc.

Thus to give more flexibility to workers of working space and network along with making data more secure to security breach Google is now deploying Beyond Corp Technology.

2. Components of Beyond Corp



Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. Device Inventory Database (Securely identifying the device)
Device identification is done based on the concept of **'managed device'**. Google maintains and updates regularly the meta-inventory database. This database keeps track of all the changes that are done in the managed devices. It also has the record of all the managed devices that have the access of Beyond Corp technology.
Device identity is possible only with the help of a certificate that is provided to each managed device after its complete information is updated in Device inventory database. This certificate acts as a key to identify the device as it contains complete device information.

2. Single-Sign-On System (User Identification)
This system validates primary and secondary factor credentials for a device which may require to access company's resources. This centralized authentication system validates and provides a short-lived token which is required for authentication process of the device.

3. Unprivileged Network
All client devices are assigned to unprivileged network that connects only to Internet. It is controlled by ACL (Access Control List). This is present between Google network and the network being used by the client.
Dynamic VLAN assignment is used which deploys RADIUS server that provides devices with appropriate network based on 802.1x authentication. Managed devices provide their certificate as part of 802.1x handshake.

4. Access Proxy
Access proxy between application and client, who may be on an internal or external network. All Google's applications are registered in public DNS with a CNAME.

5. Trust Interface
The amount of access given to a particular user's device is based on the level of trust that is assigned to a user's device. It is dynamically inferred using multiple data sources. There is a different level of trust provided for a device using updated OS than a device which does not have an updated OS.

6. Access Control Engine
This provides service-level authorization to company's applications on per-user basis. It can also enforce location based access control.

7. Pipeline
It dynamically extracts information that is necessary for making access decisions and provides it constantly to Access Control Engine.

Functioning of Beyond Corp Technology

Suppose a user is on an un-identified network and is demanding access to enterprise's applications then the following check is done before granting access to the applications:
1) The request is sent to Access Proxy and the user needs to provide its device certificate.
If the Access Proxy fails to identify the user then it is directed to Single-Sign-On system where the user needs to provide primary
2) factor and secondary factor authentication. A short-lived token is provided and the user is redirected to Access proxy.
3) The Access Proxy now has access to device's certificate and the Single-Sign-On token identifies the user.
4) A mandatory test is performed of every user by codereview.corp.google.com. This authorization check ensures that the user belongs to either of the engineering groups, user and device has sufficient trust level and the device is a managed device.
5) If any of the above mentioned tests fail, then the user is not granted access to the company's applications.

Comparative Analysis of Beyond Corp and Other Major Network Security Mechanisms

1) Explicit Client Restriction v/s Beyond Corp
The MAC address or Ethernet card of users NIC can be stored in Access Point. This may allow access only to authorized NICs. This method works well only for relatively smaller installations or group of people using the same network. Address of these NICs need to be programmed in Access Points where access is required and they also need to tracked. This may increase the workload of the company. This may even not be effective as security breach can happen by reprogramming the NIC with an allowed network address. This may, lead to illegal access. Beyond Corp on the other had does not require NIC programming and can serve the purpose of a large organization rather than a small installation.

2) Firewalls/ VPN v/s Beyond Corp
VPN technologies may be used to access company's applications. Firewall may act as a gateway as it is there for internet access which may provide access only to VPN connections. No specific authentication method is employed for security of company's applications. Beyond Corp on the other hand has a device certificate, Single-Sign-On short-lived token , primary and secondary factor authentication as well as managed device status to validate and authorize the device and user access to company's applications

3) Wired Equivalent Privacy(WEP) v/s Beyond Corp
WEP can be used for data hiding via the usage of forty bit encryption. It can also be done by using an algorithm of more number of bits e.g. 128 bits. It deploys the mechanism in which key sharing is required. In this password is creation is done for all wireless devices. After that password is installed in each device and Wireless Access point. This key cannot be obtained through packet capturing. Encryption and decryption mechanism is employed using the shared key to gain access to the company's applications. WEP is can be attacked by using brute force or reverse encryption. This may require changing of shared key and again installation of new key in all the devices and wireless access points. Beyond Corp does not function on shared key mechanism and thus is much more secure. It does not require the installation of Wireless Access points with any passwords.

4) User Authentication v/s Beyond Corp
In this user authentication is done on the basis of providing a valid (registered) username and password on the access point to gain access to company's applications. This type of user authentication can be easily breached as many times users may tend to use the same password on other networks as well. This may lead to password being easily hacked. It can also be easily done by capturing / out of thin air/ brute force mechanism. Beyond Corp requires device certificate, Single-Sign-On short-lived token , primary and secondary factor authentication as well as managed device status to validate and authorize the device and user access to company's applications

5) PATE v/s Beyond Corp
In this method, Machine learning approach is used for data hiding and decryption. Data as an entity is trained. Thus results are not presented based on any particular data which may be used during training purpose. This modular collection of data protects against black-box threats. The major problem here is that if the training data entities are made vulnerable to security breach then the whole information may get compromised. In Beyond Corp Technology, data training is not required thus time is saved and thus there is no vulnerable data breach of security.

6) Adversarial Neural Cryptography v/s Beyond Corp
In this method neural networks are used. Neural networks are get trained by using adversarial mechanism to use secret key. It is applicable for multi –user environment. In Beyond Corp there is a concept of providing primary and secondary factor authentication which is far more secure than just having one secure key which may be illegally obtained by a non-authorized person.

7) Route control mechanism v/s Beyond Corp

In this method data is sent through a pre-assigned route which may be done either dynamically or it may be static in nature. The whole purpose of Beyond Corp is to eliminate the requirement of any particular network or route and thus allow application access from any network. This is not restricted to any particular route or network.

8) Encipherment Technology v/s Beyond Corp

In this method public key and private keys are required by the sender and the receiver of the data. Without valid public and private keys none can decode the conversation as it comes in encrypted form to the receiver which can only be decrypted using a private key. Beyond Corp does not require keys to identify the user. It checks device certificate for device identification and single-sign-on token for user identification.

In case of Encipherment technology, the public or private keys can get compromised over unsecure network and may lead to data breach.

3. Conclusion

Beyond Corp is the most reliable technology that is being used now a days by Google as its chances of leading to security breach in company's network is really faint. Many network security mechanisms that are being used these days may have some short coming which may lead to the company's applications being vulnerable to cyber-attacks and losses. Though Beyond Corp is better than most of the existing network security technologies being used these days but it also has some short comings which need to be looked upon. They include:

1) Meta- inventory database needs to be kept and managed.
2) It is requied to update and track all the changes in the managed device and then send the information to other interconnected databases in order to provide access to managed device from any location.
3) Special registration is required to get a 'managed device' label. Any new device cannot access company applications until its complete information is not updated in Beyondcorp database.
4) More manpower, time and database management space on cloud is required for this purpose.

For a new device to migrate to Beyondcorp technology, it is required to activate simulator in enforcement mode and has to maintain greater than 99.99% of eligible traffic. After 30 days of monitoring the device, then the device is provided with device
5) certificate. Thus the process to avail device certificate in order to migrate to Beyond Corp technology is a lengthy process for a new device or a device which is not yet using Beyond Corp Technology.

References

[1] Keromytis, "A Look at VoIP Vulnerabilities" in USENIX, 2010
[2] Gentry, "Fully Homomorphic Encryption Using Ideal Lattices" in ACM ,Stanford University and IBM Watson, 2009
[3] Osborn, Betsy beyer, Justin Mcwilliams and max saltonstall, " Beyond Corp : Design to Deployment at Google" in ;login: , SPRING 2016 VOL. 41, NO. 1
[4] Luca Cittadini ,Batz Spear, Betsy Beyer and Max Saltonstall, " Beyond Corp Part III: The Access Proxy", in ;login: ,WINTER 2016 VOL. 41, NO. 4
[5] Jeff Peck, Betsy Beyer, Colin Beske and Max Saltonstall, "Beyond Corp: Maintaining Productivity while maintaining Security" , in ;login:, SUMMER 2017 VOL. 42, NO. 2
[6] Victor Escobedo, Betsy Beyer, Max Saltonstall and FilipZyzniewski, "Beyond Corp 5: The User Experience" in ;login:, FALL 2017 VOL. 42, NO. 3
[7] RADIUS Server, wikipedia
[8] Martín Abadi and David G. Andersen, "Learning to Protect Communications with Adversarial Neural Cryptography" in arXiv:1610.06918v1 [cs.CR] 21 Oct 2016
[9] Sophia, James Nobel and Mark S. Miller, "Permission and Authority Revisited towards a formalization" in Workshop on Formal Techniques for Java-like Programs, ACM (2016).
[10] S.V.Manikanthan and T.Padmapriya "Recent Trends In M2m Communications In 4g Networks And Evolution Towards 5g", International Journal of Pure and Applied Mathematics, ISSN NO:1314-3395, Vol-115, Issue -8, Sep 2017.
[11] S.V. Manikanthan , T. Padmapriya "An enhanced distributed evolved node-b architecture in 5G tele-communications network" International Journal of Engineering & Technology (UAE), Vol 7 Issues No (2.8) (2018) 248-254.March2018.
[12] S.V. Manikanthan, T. Padmapriya, Relay Based Architecture For Energy Perceptive For Mobile Adhoc Networks, Advances and Applications in Mathematical Sciences, Volume 17, Issue 1, November 2017, Pages 165-179