EMAILS AND THE DRIVE TO A SUCCESSFUL IoT SECURITY

Yaknan J. Gambo, Charles I. Saidu, John A. Odey, Joel H. Yohanna

Abstract— Emails are a vital part of our lives in today's digital world. It is the hub through which all our digital activities rely on. The email has seen a steady growth in users and accounts created over the years. This research projects the relevance emails will have in the future Internet- The Internet of things (IoT) a vast network of connected devices. The research points out that if the user confidence is to be boosted, the security of users in the IoT must be addressed squarely and as emails are used today, they may well be far more relevant in the future.

Index Terms— Email, Email Security, Future Internet, Internet of Things, IoT Security, Security

1 INTRODUCTION

Emails have been one of the most stable and consistent of all Internet services over the years. Since its invention there have been modifications aimed at increasing its security and ease of use. The most prominent improvements have been in its application layer which has become more user friendly and attractive compared to the initial Command Line Interface it had[1].

Currently, social media networks like Facebook, twitter, WhatsApp, snapchat, Instagram, medium, slack, LinkedIn etc rely on user email accounts in creating accounts and for password retrievals. Banks and eCommerce sites also depend on emails for transactions, correspondence and notifications. All these only affirms the place of emails in today's digital world. This serves as a pointer to the role emails will play in the future Internet- The Internet of Things (IoT) especially in the IoT security.

This research points out the critical role emails will play in the not too distant future where almost everything will be connected in the Internet.

- *Yaknan John Gambo is currently lecturing at the Department of Computer Science, Federal University Wukari, Wukari, Taraba State, Nigeria. E-mail: yaknanjohn@gmail.com*
- *Charles I. Saidu is currently lecturing Department of Computer Science, Baze University, Abuja, Nigeria.*
- *John A. Odey and Joel Yohanna are both currently lecturing at the Department of Computer Science, Federal University Wukari, Wukari, Taraba State, Nigeria.*

2 EMAILS

Since the invention of the email as an application by Shiva Ayyadurai in 1978[2], it has seen considerable increase in usage over the years. The initial purpose of emails was to foster correspondences in a fast and convenient manner via electronic devices[3]. This saw business and organizations scrambling to be part of this new form of communication that will bring efficiency, save time that was otherwise spent on the old mailing system and bring possible profits to them. Reliance on emails increased and the number of users steadily increased. A compilation of email statistics and forecast by Radicati Group[4], [5] showed that worldwide, the number of email users have consistently increased by a factor of 3% as shown in Fig 1.

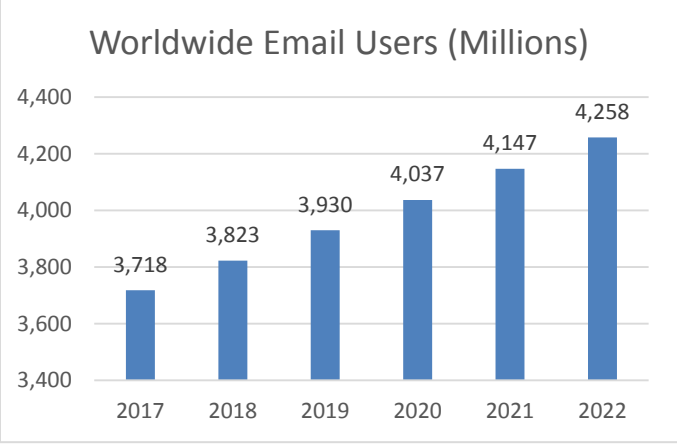

Fig 1: Worldwide Consumer and Business Email Users(Source Radicati Group Inc)

This increase can be attributed to the opening of multiple accounts by single users and also the influx of new users that have not used emails before especially in Africa and other developing parts of the world. Perhaps a point will be reached where the growth rate might slow down when developing nations advance but all together the relevance of emails will still exist.

The Radicati Group in the same email statistic report also forecasted on email accounts that are opened by businesses and consumers. The forecast can be seen in Fig 2 and it showed again a steady growth in the number of email accounts opened by a factor of 6% to 7% annually. This growth had direct bearing on email market profits that accrue due to the following:

a. Cloud business emails from providers such as Google, Intermedia and Microsoft;
b. Messaging platforms for service providers such as Oracle, Open-Xchange, Synchronoss Messaging, Zimbra.
c. Enterprise messaging platforms from vendors like Microsoft and IBM

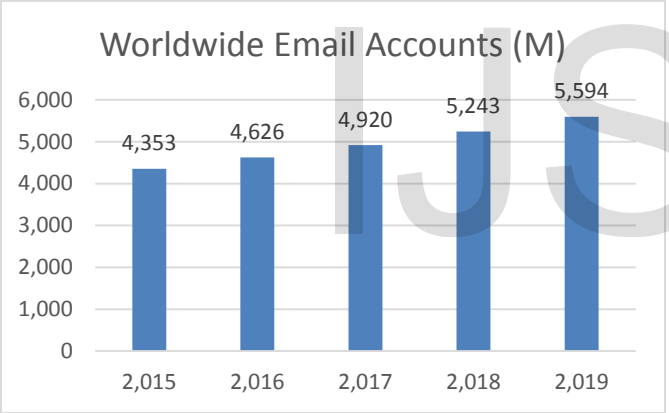

Fig 2: Worldwide Consumer and Business Email Accounts (Source Radicati Group Inc)

All these statistics point to the unavoidable reality that emails will continually find relevance in the future. The question should be how best to modify emails so that it can best meet the Internet needs of the future. Email is here to stay because it is the backbone of the internal as well as external communication structure of organizations[6].

- *Yaknan John Gambo is currently lecturing at the Department of Computer Science, Federal University Wukari, Wukari, Taraba State, Nigeria. E-mail: yaknanjohn@gmail.com*
- *Charles I. Saidu is currently lecturing Department of Computer Science, Baze University, Abuja, Nigeria.*
- *John A. Odey and Joel Yohanna are both currently lecturing at the Department of Computer Science, Federal University Wukari, Wukari, Taraba State, Nigeria.*

3 THE INTERNET OF THINGS

It is no longer news that the next big thing after the Internet as we know it today is the Internet of Things where billions of devices are connected to the Internet. It is also predicted that in the year 2020 there will be at least four(4) Internet connected devices for every person on earth [7]. Although there are arguments that suggest that the predictions are a little exaggerated[8] but what everybody agrees on is that there is going to be an increase in both Internet connectedness and dependence on it.

As these devices continue to increase, dashboards whether graphical or natural[9] will have to be created to manage and control them. It follows that every individual will eventually possess a dashboard to help manage personalized and commercialized services that these devices help to provide. This brings issues of security and access control to the fore. As it stands the confidence levels needed for a complete acceptance of the Internet of things is still behind[10]. We belief that the security challenge of the IoT will be gradually allayed. Taking a cue from the current use of emails as a password recovery tool, one can say that emails will possibly be still used to safeguard the Internet of things.

4 THE USE OF EMAILS AND SECURITY

A research survey carried out by Mimecast [11] showed that emails are the most likely source of data breaches with network servers the least source of data breaches. Fig 3 clearly shows the result of the survey. Emails have become a critical tool in our everyday life, uses include correspondences, access to other web services and social networks etc.

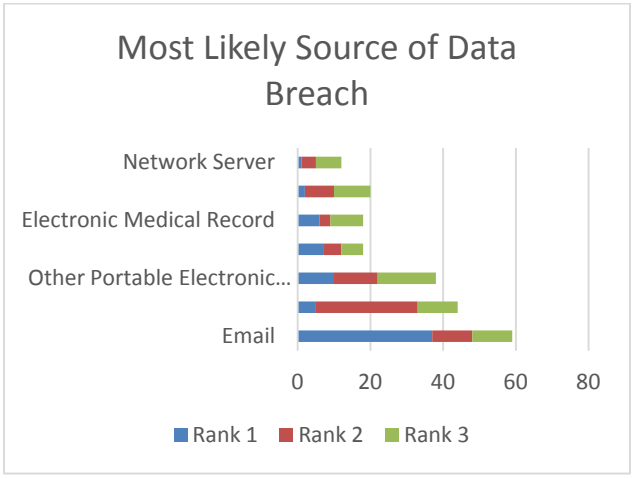

Fig 3: Most Likely Source of Data Breach (Source David Hood, Mimecast)

Because of the vital part emails play in our modern life, it is no wonder that it has become the most likely source of data breaches. Hackers know that if they can gain access to a user's email, they can invariable gain access to almost every other account the user has on other platforms[12]. Jason Murdock sees emails as the post-box of the digital era and everything one does on the web flows through it[13].

5 THE INTERNET OF THINGS AND THE ROLE OF EMAILS

From the foregoing, we see a relationship between the Internet of Things and the Email. However, for emails to be more relevant in the IoT, it must first be secured in ways that breaches will be almost impossible. Email security has seen much advances over the years especially in the area of multi-factor authentication and biometric access[14]. These advances and drive towards a better security has to continue if consumer confidence is to be boosted for the full commercialization of the Internet of things.

6 CONCLUSION

The research has shown that emails will play a vital role in the future Internet especially in the area of security. It is clear that currently emails are depended upon in opening social media accounts, business and bank transactions. Once an email has been compromised, access to every other account would be an easy thing. Therefore, email service providers and users should pay close attention to the security of their email services and accounts respectively. It can be said conclusively that the current trends in IoT suggest that there would be an unavoidable reliance on emails to gain access to IoT Control dashboards in the not too far future. This is another reason that calls for a more proactive and deliberate action by both email service providers and users to secure access to emails by third parties to help safeguard their future in the next generation technologies.

REFERENCES

[1] [www.wikipedia.com], "History of E-mail." 2018.
[2] "The Inventor of Email," International Center for Integrative Systems, 2017. [Online]. Available: http://www.inventorofemail.com/index.asp. [Accessed: 20-Jul-2018].
[3] B. O'KANE, "The Future of EMAIL," The Austrialian Business Review, 2015. [Online]. Available: https://www.theaustralian.com.au/business/business-spectator/the-future-of-email-/news-story/7a2842c80cc4ba75b79f33c1d2f48f85. [Accessed: 12-Jul-2018].
[4] I. The Radicati Group, "Email Statistics Report, 2015-2019," Email Stat. Rep., vol. 44, no. 0, p. 4, 2015.
[5] The Radicati Group, "Email Statistics Report , 2016-2020," Email Stat. Rep. 2016-2020, vol. 44, no. 1, pp. 0–3, 2016.
[6] B. Roussey, "Advances in Email Technology That Deliver Tangible Businesses Benefits," TechGenix, 2018. [Online]. Available: http://techgenix.com/advances-in-email-technology/. [Accessed: 20-Jul-2018].
[7] K. Lant, "By 2020, There Will Be 4 Devices for Every Human on Earth." 2017.
[8] A. Nordrum, "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated," IEEE Spectrum. pp. 0–2, 2016.
[9] Dorothy Shamonsky, "Internet of Things_ Will GUIs Still Exist__ ICS - Integrated Computer Solutions," 2015. [Online]. Available: https://www.ics.com/blog/internet-things-will-guis-still-exist. [Accessed: 20-Jul-2018].
[10] M. A. Iqbal, O. G. Olaleye, and M. A. Bayoumi, "A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches," Glob. J. Comput. Sci. Technol. E Network, Web Secur., vol. 16, no. 7, 2016.
[11] DAVID HOOD, "Healthcare Provider Survey Finds Email Most Likely Source of Data Breach | Mimecast Blog." 2017.
[12] R. Lawton, "3 REASONS WHY HACKERS WANT YOUR EMAIL ADDRESS AND 6 WAYS TO PROTECT YOURSELF," 2016. [Online]. Available: https://www.linkedin.com/pulse/3-reasons-why-hackers-want-your-email-address-6-ways-rachael. [Accessed: 20-Jul-2018].
[13] J. Murdock, "What hackers do with the private data in your email account," International Business Times, 2016. [Online]. Available: https://www.ibtimes.co.uk/what-can-hackers-do-private-data-your-email-account-1596694. [Accessed: 20-Jul-2018].
[14] J. Farnsworth, "5 Technology Advances Creating a More Secure Work-at-Home Business Model _ SYKES," Sykes Enterprises, Incorporated, 2017. [Online]. Available: https://www.sykes.com/thought-leadership/5-technology-advances-creating-secure-work-home-business-model/. [Accessed: 20-Jul-2018].

- *Yaknan John Gambo is currently lecturing at the Department of Computer Science, Federal University Wukari, Wukari, Taraba State, Nigeria. E-mail: yaknanjohn@gmail.com*
- *Charles I. Saidu is currently lecturing Department of Computer Science, Baze University, Abuja, Nigeria.*
- *John A. Odey and Joel Yohanna are both currently lecturing at the Department of Computer Science, Federal University Wukari, Wukari, Taraba State, Nigeria.*