THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY

# ON CLOUD SECURITY AND USABILITY: HOW DO WE MAKE SECURITY USABLE?

WILLIAM AIKEN
FALL 2015

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Security and Risk Analysis
with honors in Information Sciences and Technology

Reviewed and approved* by the following:

Jungwoo Ryoo
Associate Professor of Information Sciences and Technology
Thesis Supervisor

David Barnes
Senior Instructor in Computer Science
Thesis Supervisor

Laura Rotunno
Associate Professor of English
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

# ABSTRACT

The rapid adoption of cloud computing means an unprecedented amount of sharing technological resources. In an architecture that relies on systematic sharing, it is absolutely crucial to design robust cloud systems with measurable security patterns built into them in order to provide adequate audits and reviews of security performance. And yet even now security is frequently reported as the number one concern when enterprises turn to cloud based solutions. This hesitancy applies to global corporations with a large number of employees as well as small businesses and even the average end user. As a result of increasingly rapid adoption, cloud service providers cannot expect all users to fully understand the security patterns and practices or how to take full advantage of them.

This paper reviews the current architecture and its approach to auditable security mechanisms for cloud based platforms, and it also takes an in-depth look at how to achieve understandable and usable security tools for the average, uninterested end users. From there, the research covers several mechanisms for implementing usable security on cloud platforms with a special focus on how to design cloud systems via secure software engineering patterns.

## TABLE OF CONTENTS

## LIST OF FIGURES

# LIST OF TABLES

# ACKNOWLEDGEMENTS

I must give acknowledgements to all those who made this research possible. I owe the Schreyer Honors College for supporting me in my endeavors to write this paper. The Pennsylvania State University Altoona Honors College headed by Dr. Laura Rotunno was invaluable in its constant guidance and support both monetary and personal throughout the entirety of this process.

I thank Doctors Jungwoo Ryoo and Hyoungshick Kim and Professor David Barnes for their expertise and help in the creation of this work. Without them, I could not have even begun undertaking this research.

And finally I thank Dr. Steven Bonta. It is because of him that I had the courage to face any academic obstacle and tackle it with ease.

# Chapter 1

## Introduction

Cloud computing provides numerous advantages to service providers, developers, and customers with respect to flexibility, scalability, and availability at lower cost. Cloud services are offered to customers through three fundamental service models defined as: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Non-IT users most frequently encounter SaaS. For example, Google Docs, a popular file editing and sharing platform, is considered SaaS. With the increasing popularity of cloud computing, even the average cloud user can share a vast collection of files with other users instantly and provide seamless access to them from anywhere in the world. While this provides end users with a large amount of freedom with their data, it also raises an equal amount of potential for harm. Because cloud computing fundamentally relies on the concept of shared resources, a lack of proper security by just one member can result in severe data or privacy loss or for all other parties.

Many businesses and research organizations have spent significant time and money on the development of better security for their cloud systems. Previous research has focused on the collaboration between three large scale entities – a Cloud Service Provider (CSP), a Keying as a Service Provider (KaaSP), and the owning organization – to decrypt cloud data via a highly customizable and auditable role-based access control system [1]. A Keying as a Service Provider would ensure that no information could be decrypted without the cooperation of at least two of the parties. This KaaS model focused on the challenges facing small- and medium-sized enterprises (SMEs). However, individual end users of cloud also face similar security challenges when using cloud systems like Google Docs or Dropbox. But even more so than SMEs, the average end user lacks the time, money, and expertise to implement or understand safe practices regarding their data [2].

At this point, current and future research at PSU Altoona is aimed at taking advantage of these kinds of third-party computing paradigms in processing big data. PSU Altoona and IBM are already collaborating to improve knowledge on the security and usability of the cloud. Emphasis on secure big data processing will only grow, especially as big data becomes more affordable to both SMEs and individuals. For example, the Internet of Things (IoT) may bring an unprecedented amount of information to the business and the home, ranging from health information to utility use [3].

The ultimate goal of this paper is to combine several years worth of research into a tangible and reviewable contribution to security methodologies and secure development of applications. With a properly designed and planned architecture, future cloud computing programs can have security built into the system from the outset rather than added as an afterthought.

# Chapter 2

## The Current Data Sharing Architecture, Usability vs. Security

A public cloud allows for casual end users to store and manipulate data on the fly from essentially any Internet connection in the world. The underlying capabilities (and security issues) from this kind of power are vast. In order to limit the scope, this paper is going to focus solely on the issues related to sharing personal files from one user to another.

Throughout this section, it is important to note three major assumptions about the cloud user who shares the file and the recipients of it:

1) The owner has no knowledge of the quantitative security mechanisms of the recipients (i.e. the password strength, implementation of account recovery options, multi-factor authentication, etc.),

2) The owner has no knowledge of the qualitative security habits of the recipients (i.e. storing passwords in browser, frequently unlocking device by PIN instead of biometrics, etc.), and

3) The owner of the data should not be concerned about this information.

The owner should be able to enforce her own expectations of security without worrying about the security practices of others any more than she worries about the internal mechanisms of the cloud system itself.

The current mechanism of cloud computing requires the owner to blindly accept the security practices of the recipients. For example, if Bob shares an important file or collection of files with Alice via the cloud, Alice's password could easily be "123456". If the file were compromised, a logical question would be to ask who is at fault: Alice with an insecure password or Bob who shared the file in the first place? The implications of lost personal information may vary per person, but to a SME that must meet several accountability standards, they are even less clear.

In short, despite their tremendous potential, cloud computing systems come with their own unique set of security problems. A cloud infrastructure is the result of a constant three-way negotiation among service organizations, cloud service providers (CSPs), and end users to ensure productivity while maintaining a reasonable degree of security. A CSP should keep data safe from security threats and yet maintain constant availability. In addition, the client organization must verify that the cloud computing enterprise contributes to its own business goals, objectives, and future needs. As a result, the issues of transparency; encryption; colocation; and scale, scope, and complexity require specialized system administers in order to properly report the security procedures of the organization [4].

For the average adopter of cloud platforms, this is an obvious problem. With the flood of regulatory problems that may actually impede security [5], how are SMEs supposed to protect themselves? And do the users understand proper security procedures even when they are implementing them?

## Related Work

There is an important relationship between the psychology of end users and usable security. Recent research has shown that end users are able to differentiate security/privacy concerns from general computer concerns [6]. However, from this study, it is impossible to tell whether this ability actually leads to practical steps to achieve secure practices.

Relying on end user knowledge of a system is fraught with challenges as systems designed to rely on end user feedback result in incorrect security decisions. Research has shown that “informational cascades” are likely to occur in these systems. Informational cascades occur when users agree with a community consensus even when they have data that goes against the community decision. The research indicates that this is because users have to not only make objective decisions about security, but make them correctly based on limited expertise [7]. Other research points out that end users prioritize security incorrectly [8] and that internal security messages carry more weight than external ones [9].

## Motivation

Finding a balanced level where an uninformed or apathetic end user can make proper security decisions is a difficult task for two reasons:

1) Some users will inevitably want to adopt secure practices, and it is the job of the software to help them achieve their security preferences, and

2) For those who are reluctant to adopt new security practices, it is the job of software engineers to make security an integral and effortless part of the software.

In other words, the goal is to make adopting security procedures actually improve usability.

In some high profile cases of data breaches, password based authentication systems are not enough, especially when the owner is not immediately able to react to a suspicious login. The benefit of cloud computing allows for instantaneous access, but it also allows for instantaneous exploitation. The value of personal data stored in the cloud might be just as high as “traditionally” sensitive information such as credit card numbers or social security numbers; this may become more true as cloud based platforms like Facebook grow not only in user base but also in content [10]. The value of this information regarding the private lives of high profile individuals like celebrities or politicians is likely even higher.

In order for security to have any value, the recipient of the file must be trusted enough not to deliberately violate the trust relationship with the owner. The owner could put view-only rights on images, not downloading; however, this does not account for analogue weaknesses where the recipient can take a literal photograph of the image, for example. The fuzzy issue of trust between sharer and recipient is a subject for other research.

Much research has already been done and will continue to be done on the threat assessment on cloud computing given the plethora of availability and confidentiality failures of top notch CSPs like Amazon, Sony, and Dropbox that marred the beginning of this decade [11]. Likewise, the threat of powerful adversaries such as governments or other CSPs is a frequent topic of research [1]. The threat of insecure CSP architectures or government brute force techniques is real; nonetheless, it is important to recognize the threat of carelessness or apathy by the owner of the data and those within her circle of trust.

## Proposed Architecture

SMEs need an auditable cloud architecture. Similar to ISO 27001 and other high profile audit standards, a step-by-step security integration checklist should be available for securely sharing files. Instead of forcing another audit on SMEs, the existing and developing cloud standards should encourage proper sharing procedures in the applications themselves.

The CloudAudit Working Group has done some substantial work for “enterprises who are interested in streamlining their audit processes” and for “cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance” of the most popular cloud platforms [12]. The review process shown in Figure 1 stays in accordance with the style of other popular auditing standards. If an aspect of this review is not met, system administrators should be alerted immediately, and the organization may choose to temporarily suspend the availability of the file.

**Table 1 Proposed File Sharing Audit Standard**

| Audit Standard for File Sharing over Public Cloud Based Systems | |
|---|---|
| Sharing and receiving roles | Every employee, contractor, and third party user who shares a file must belong to a group that is governed by the organization’s information security policy – as they would be governed in a traditional infrastructure |
| Security level classification | All users shall be required to meet an objective threshold of security. Their level will be measured by password strength, usage of biometrics, data about network habits, etc. The level is flexible, and it should be updated in real-time on the computer system. |
| Encryption standard | All data shall be encrypted with a key mechanism such that no information can be accessed without the expressed consent of the owning organization |
| Sharing limitations | Any sharing of data must be limited or defined by group as well as time and location. Should the recipient try to access the data outside of these constraints, the file will be inaccessible. |

In keeping with CloudAudit’s desire to achieve a streamlined audit, all of the aspects found in Figure 1 can be evaluated in real-time automatically. Any application (either developed in-house or by a third party) that deals with file sharing over a public cloud system should conform to a similar auditable standard.

# Chapter 3

## Improving Usable Security in the Cloud

Balancing security and usability is an ongoing challenge in information security. Even in traditional IT domains, there is a conflict between the interests of end users and the interests of the security managers. Figure 1 is featured in security expert Michael Kummer's blog entry about data security and usability [13], but a reversal in thinking about this concept can lead to a dramatic increase in security mindedness.

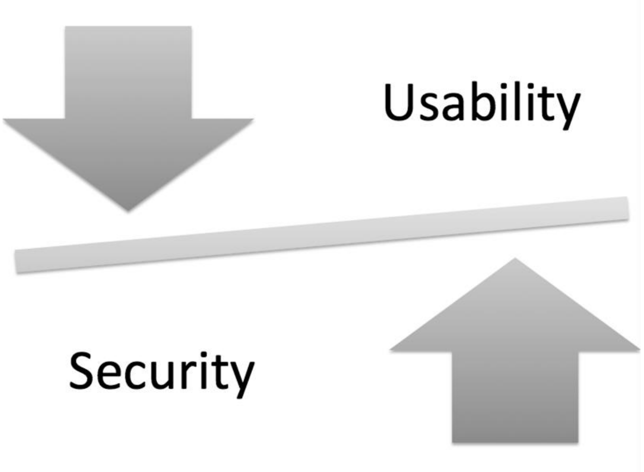

Figure 1 Usability vs. Security

In Malcolm Harkin's book about security practices at IBM, he takes on the motto "Protect to Enable", where security increases usability [14]. However, his commentary leaves out a crucial point: usability should also strengthen security. Figure 2 reflects a more appropriate model of this concept.

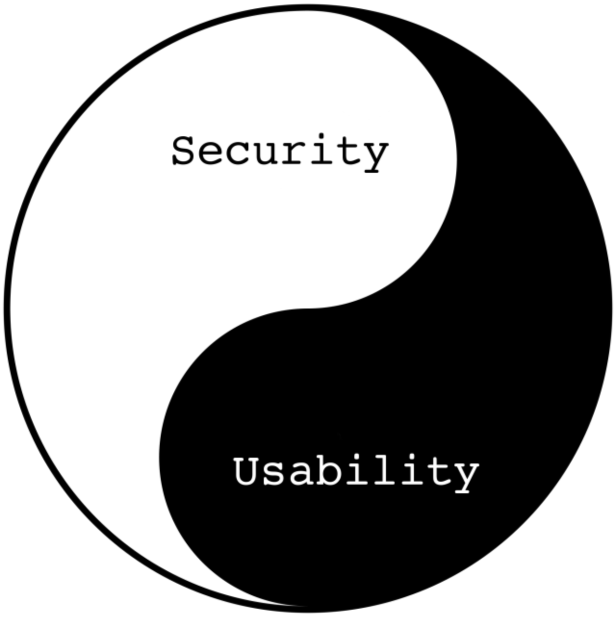

**Figure 2 Appropriate Model on Security and Usability**

The interfaces of cloud systems are becoming more intuitive, especially with the growth of big data applications. This is a remarkable step in the usability of complex and powerful systems. Providing robust security tools at the touch of a button ought to follow suit. CSPs do have many security measures [15] [16], but system administrators of SMEs have little control over their actual implementation. Thus, if a vulnerability is exposed, the end user continues to be at risk until the provider decides to take action. By simply providing a few security tools to the administrator herself, the burden can be more distributed.

## Cloud Breaches, A Security vs. Usability Problem

Research has already proven that giving end users many options may decrease the quality of information security as well as the usability of the system in general [17]. Development must focus on both aspects simultaneously.

Big data technology reaches a whole new level of intimacy with users. It is becoming frighteningly accurate with predictions of human behavior and preferences. In response, security must increase to protect this information, and if humans are always the weakest link in a secure system, this can lead to some very interesting security dynamics. Despite encryption schemes that current technology would need thousands of years to crack via brute force, high profile individuals have their personal information stolen because of usability issues like re-used passwords [18]. Even knowledgeable developers have slipped up by leaving their Amazon Web Service passwords in plaintext on their GitHub pages [19].

As a result, for the application developer, excellent security must be so integral and easy to use that all end users would have to go out of their way to not use it. Some research has already been done on the ways in which the most efficient increase in security can be achieved with the littlest end user effort.

## Related Research

Several universities have already done substantial research into system generated PINs. Their work has shown that increasing the complexity from traditional 4-digit PINs does not statistically differ in memorability when increasing to 6-, 7-, or even 8-digit PINs [20]. Similarly, Sungkyunkwan University research on mobile pattern locks has shed some light on their usability. In particular, they implemented a strength meter for user defined unlock patterns using a score based on the length, the ratio of non-repeated segments, and the number of intersecting points [21]. Their research has shown that “a well-designed pattern lock strength meter is indeed effective in helping users choose more secure pattern locks” with the caveat that it seems to encourage users to default back to the top-left dot as their initial starting point. Their analysis on the entropy of pattern locks also indicates a higher level of security on the user defined pattern locks over the user defined 4-digit PINs.

Assuming their entropy measuring mechanism is correct, their research indicates that mobile security systems are not taking full advantage of the user’s preference of security. In other words, getting a user to adopt security is the difficult part in the process. Increasing the effectiveness of that security is the job of the designer, not the user.

## Proposed Implementations

Overall, more work needs to be done on the usability of security for the average data owner. A repeated password stolen from an insecure website or mobile application will undo even the best efforts on many cloud storage sites. Using a customized authentication (or encryption) system would mitigate this problem, but it is something the average cloud user may find burdensome to use. Likewise, sharing a large collection of data with a close friend can be a poor choice if that friend has no authentication system built into his devices.

One proposed solution is to add a “one-click” multi-factor authentication scheme to any file sharing architecture. For example, most file sharing systems allow for a file to be shared by a link. Anyone who has that link has unfettered read access to that file. This can be especially convenient when sharing a collection of files with end users who may not use that particular cloud service. However, a link to that file may still exist long after the intended share period has expired with no notice to the original owner. When clicking “Share Link” for example, the application could prompt the user to require either a PIN or password to access the file. It could also ask for a termination date for the share link. When someone clicks on this link, they may be shown the owner as well as a file name, but in order to read it, he will be required to input the PIN. In this way, the owner of the data can implement a modest degree of confidentiality even with recipients who have little to no security practices at all.

# Chapter 4

## A Software-Engineering Approach to Implementation

Entire organizations may begin implementing solutions similar to the KaaS model [1], and with so much research being done on improving usability, service providers will build more and better security mechanisms into cloud environments for SMEs. However, developing an architecture for a usable yet secure cloud is no simple task.

### Previous Research

Previous research on stakeholder-orientated assessments of cloud services has focused on assigning metrics to existing frameworks. Many ranking systems are based on evaluation before adopting a cloud based solution. For example, one proposed measurement index relied on the evaluation of “Vendor weights” and their subfactors [24].

This security index includes not only the security specification or preferences provided by the user but also the subfactors deemed important by a system manager or auditor. A security index of this type may become increasingly important because even adding a numeric ranking to something as human as a pattern lock can make a difference in increasing security [21]. Applying both the pattern lock concept as well as a cloud ranking metric to the development of future cloud based applications gives more comprehensive security.

## Implementation

In addition to examinations of several problems and literature surveys, this research has also focused on implementing the proposals given above. While still growing and likely to be taken over by other PSU research students, the project will remain open source. The entirety of the source code is currently available; please contact the author of this paper to receive access to it.

The three major proposals of this paper have already been implemented in the application:

1) Pattern lock restrictions on certain (picture) files are permitted. This lets the user define the security level that recipients must achieve before downloading the file locally,

2) Sungkyunkwan University's pattern lock metrics inform the user about the strength of their PINs as well as their pattern locks,

3) The application can make a connection to both a KaaSP and the CSP to download files via an All-or-Nothing Framework discussed in the KaaSP paper [1] as shown in a UML visualization in Figure 3.

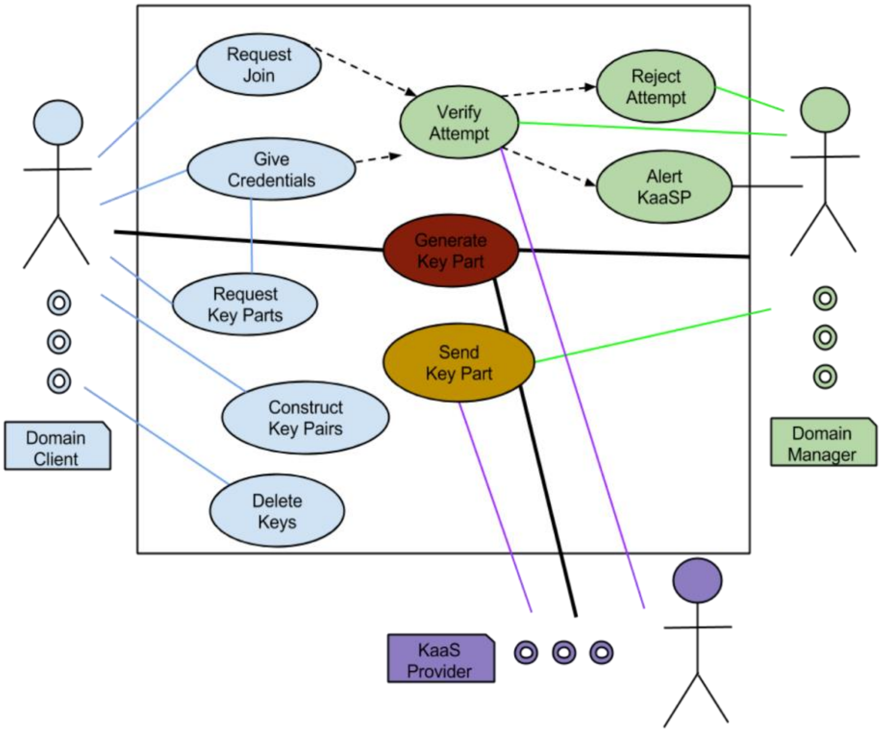

Figure 3 KaaSP UML Visualization

However, the prototype does have some limitations. For example, the API hooks at this stage are only those related to Dropbox, but future work will:

1) Be compatible with all or most major cloud providers (such as Amazon Web Service, Windows Azure and Google Drive), and

2) Allow for easy integration of custom cloud storage systems, based on SFTP file transfers, etc.

# Chapter 5

## Future Research

As stated, the source code is available for evaluation. However, in order to make a long term, meaningful contribution to this project, future work will involve use-case research. It is crucial that the user base is broad and diverse, and analyzing the results of a large test study should not be done lightly. In other words, this research has been designed to focus on the development of the ideas behind the prototype as well as the prototype itself.

The issue of usable security lies at the intersection between robust computation systems and complex human psychology. Future research aims to bridge the gap between these two topics.

Additionally, this research approaches the issue from a software-engineering perspective; follow-up research will review how effectively this work performs in the wild.

# Chapter 6

## Conclusion

Developing a comprehensive framework for cloud computing is not simple. Future computing paradigms must find a balance between the end user and the software developer as well as a productive relationship between wholesome security and simplistic usability.

In order to achieve this goal, this research reviewed the current architecture of a security problem, examined possible solutions from the end user usability perspective, and brought these two seemingly contradictory mindsets together.

Usability and security are not two separate issues. On the surface, they seem to clash, existing in a give-and-take relationship. But instead of treating them as opposing, mutually exclusive problems, software engineers should be answering them in the same question: how do we make security usable?

# BIBLIOGRAPHY

[1] W. Aiken, “KaaSP: Keying as a Service Provider for Small and Medium Enterprises Using Untrusted Cloud Services,” in *AMC IMCOM 2015*, Bali, Indonesia, 2015.

[2] Symantec, “The Myth of Keeping Critical Business Information Out of Clouds,” 2012. [Online]. Available: http://www.symantec.com/content/en/us/about/presskits/b-myth-of-keeping-critical-business-information.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012_worldwide_CloudLaunch. [Accessed: 20- Oct- 2015].

[3] J. Bertolucci, “Big Data In The Home,” 2014. [Online]. Available: http://www.informationweek.com/big-data/software-platforms/big-data-in-the-home/d/d-id/1141608. [Accessed: 20- Oct- 2015].

[4] J. Ryoo et al., “Cloud Security Auditing: Challenges and Emerging Approaches” in *Institute of Electrical Electronics Engineers Computer and Reliability Societies*, 2014.

[5] R. Bowen, “Do More Regulations Equal Less Safety?,” 2013. [Online]. Available: http://mercatus.org/sites/default/files/publication/More-Regulations-Less-Safety.pdf. [Accessed: 15- Sep- 2015].

[6] J. B. Gross and M. B. Rosson, “End User Concern about Security and Privacy Threats”, in *Symposium On Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, 2007.

[7] J. Goecks, et al., “Challenges in Supporting End user Privacy and Security Management with Social Navigation,” in *Symposium On Usable Privacy and Security (SOUPS),* Mountain View, CA, 2009.

[8] H. Du et al., “Effects of Fear appeals and point of reference on the persuasiveness of IT security communications” in *Intelligence and Security Informatics (ISI), 2013 IEEE International Conference*, Seattle, WA, 2013. DOI: 10.1109/ISI.2013.6578791.

[9] D. LeBlanc and R. Biddle, “Risk perception of internet-related activities”, in *Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference,* Paris, France, 2012. DOI: 10.1109/PST.2012.6297924.

[10] C. Marshall. An argument for archiving Facebook as a heterogeneous personal store. In *Digital Libraries (JCDL), 2014 IEEE/ACM Joint Conference*, 11 – 20. London, England, 2014.

[11] C. Cachin and M. Schuner, “A Cloud You Can Trust: How to ensure that cloud computing’s problems – data breaches, leaks, service outages – don’t obscure its virtues,” 2011. [Online]. Available: http://spectrum.ieee.org/computing/networks/a-cloud-you-can-trust. [Accessed: 10- Aug- 2015].

[12] Cloud Security Alliance, “CloudAudit Working Group.” [Online]. Available: https://cloudsecurityalliance.org/group/cloudaudit/. [Accessed: 25- Aug- 2015].

[13] M. Kummer, “Data Security vs. Usability,” 2013. [Online]. Available: http://www.michaelkummer.com/2013/01/18/data-security-vs-usability/. [Accessed: 26- Oct- 2015].

[14] M. Harkins, “Managing Risk and Information Security: Protect to Enable”. 2013.

[15] Dropbox, “Dropbox for Business security: A Dropbox whitepaper”, 2014. [Online]. Available: https://cf.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vfl_b7tp-.pdf. [Accessed: 15- Oct- 2015].

[16] Google, “Security Whitepaper: Google Apps Messaging and Collaboration Products,” 2011. [Online].

[17] S. Korff and R. Böhme, “Too Much Choice: End user Privacy Decisions in the Context of Choice Proliferation,” in *Symposium on Usable Privacy and Security (SOUPS)*, 69 – 87, Menlo Park, CA, 2014.

[18] “Apple Media Advisory: Update to Celebrity Photo Investigation,” 2014. [Online]. Available: http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html. [Accessed: 01- Oct- 2015].

[19] M. Kotadia, “AWS urges developers to scrub GitHub of secret keys”, 2014. [Online]. Available: http://www.itnews.com.au/news/aws-urges-developers-to-scrub-github-of-secret-keys-375785. [Accessed: 15- Jul- 2015].

[20] J. H. Huh, et al., “On the Memorability of System-generated PINs: Can Chucking Help?” 2015. [Online]. Available: http://seclab.skku.edu/wp-content/uploads/2015/07/chunking-pins-soups.pdf. [Accessed: 15- Sept- 2015].

[21] Y. Song, et al., “On the Effectiveness of Pattern Lock Strength Meters – Measuring the Strength of Real World Pattern Locks,” 2015. [Online]. Available: http://seclab.skku.edu/ wp-content/uploads/2015/01/PatternLockMeter.pdf. [Accessed: 15- Sept- 2015].

[22] Y. Song, et al., “A Private Walk in the Clouds: Using End-to-End Encryption between Cloud Applications in a Personal Domain,” 2014. [Online]. Available: http://seclab.skku.edu/wp-content/ uploads/2014/07/EnCloud.pdf. [Accessed: 15- Sept- 2015].

[23] T. Okubo, et al., “Threat and countermeasure patterns for cloud computing”, in *Requirements Patterns (RePa), 2014 IEEE 4$^{th}$ International Workshop*, Karlskrona, 2014. DOI: 10.1109/RePa.2014.6894843

[24] S. Rizvi, “A Stakeholder-Oriented Assessment Index for Cloud Security Auditing,” in *AMC IMCOM 2015*, Bali, Indonesia, 2015.

# ACADEMIC VITA

**Academic Vita of William Aiken**
billzo.aiken@gmail.com
Altoona, PA

**Education:**

Pennsylvania State University
B.S. in Security and Risk Analysis, Information and Cyber Security

**Honors Thesis:**

Title: On Cloud Security And Usability: How Do We Make Security Usable?
Thesis Supervisor: Jungwoo Ryoo

Based on a culmination of all the research endeavors undertaken while studying at PSU Altoona under Dr. Jungwoo Ryoo as well as my exposure to the research done at the Sungkyunkwan University (SKKU) Security Lab under Dr. Hyoungshick Kim.

**Work Experience:**

Penn State Altoona Cyber Security Lab (January 2013 – Present)

- Penn State Altoona, 3000 Ivyside Park, Altoona PA 16601
- Job Held: Research Assistant / Student Intern
- Description: Assisted professors Ryoo and Rizvi with research about Cloud Computing and Cloud security auditing and contributed to their publication efforts.
- Supervisors:
  - Jungwoo Ryoo, Ph. D.
  - Syed Rizvi, Ph. D.

Sungkyunkwan University Security Lab (August 2015)

- 2066, Seobu-Ro, Jangan-Gu, Suwon-Si, Gyeong Gi-Do, Korea
- Job Held: Research Assistant
- Description: Actively participated in the research of reverse engineering popular Korean applications as well as the research of usable security in practice
- Supervisor:
  - Hyoungshick Kim, Ph. D.

Cenveo, Inc. (Spring 2015 – Present)

- 785 Juniata River Road, Williamsburg, PA 16693
- Job Held: Information Technology Consultant
- Description: Migrated existing systems from physical machines to virtualized machines, while maintaining compatibility and communication to legacy hardware, mostly consisting of the Allen Bradley and Rockwell Software varieties
- Supervisor:
  - Ryan Gorsuch

## Noteworthy Honors and Awards:

Dean’s List (Fall 2011 – Spring 2015)
College of IST’s Edward M. Frymoyer Scholarship (Fall 2013)
Lockheed Martin Engineering Scholar for IST (Fall 2013 – Spring 2014)
Pechter Business Competition First Place Winner (Spring 2015)

## Computer Language Competency Levels:

| | |
|---|---|
| Proficient with: | Java |
| Familiar with: | C, C++, Swift, MySQL |
| Exposure to: | HTML, CSS, PHP, Python, Bash, PowerShell |
| Interested in: | Assembly via decompiled/disassembled code |

## Supplemental Language Study:

| | |
|---|---|
| Spanish language study | (Fall 2007 – Present) |
| Catalan language study | (Fall 2012 – Present) |
| French language study | (Fall 2012 – Fall 2013) |
| Japanese language study | (Fall 2012 – Spring 2013) |
| Korean language study | (Spring 2015 – Present) |
| Sanskrit language study | (Fall 2013 – Spring 2014) |
| Hindi language study | (Fall 2015 – Present) |

## University Activities:

Penn State Altoona Honors Program (Spring 2012 – Present)

Scholar of Schreyer Honors College (Fall 2013 – Present)

## Publications:

"Auditing the Cloud for Security: Challenges and Solutions"

ICBEIT 2013 Conference, Location: Cairns, Queensland, Australia

"Auditing the Cloud for Security: Challenges and Solutions"

IEEE Security and Privacy Magazine

"A Stakeholder-Oriented Assessment Index for Cloud Security Auditing"

IMCOM 2015 Conference, Location: Bali, Indonesia

*Received "Best Paper Award" for IMCOM ACM conference

"KaaSP: Keying as a Service Provider for Small and Medium Enterprises Using Untrusted Cloud Services"

IMCOM 2015 Conference, Location: Bali, Indonesia

"Bypassing the Integrity Checking of Rights Objects in OMA DRM: a Case Study with the MelOn Music Service"

Conditionally Accepted in ACM IMCOM 2016