User Privacy Suffers at The Hands of Access Controls

Chad N. Hoye
University of West Florida, cnh22@students.uwf.edu

Follow this and additional works at: http://digitalcommons.kennesaw.edu/ccerp
Part of the Information Security Commons, Management Information Systems Commons, Social Psychology Commons, and the Technology and Innovation Commons

http://digitalcommons.kennesaw.edu/ccerp/2016/Student/10

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Conference on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.
Abstract
With advancements in personal hand held devices, smaller more mobile computers, tablets, and the world’s population connected with social media the threat to the user’s privacy has been diminished. I will look at how access control policies have opened the proverbial door to user’s privacy being attacked and threatened. You will see examples of how users have to divulge personal information to get better service and even be monitored while at work to prevent intrusions into the company.

Disciplines
Information Security | Management Information Systems | Social Psychology | Technology and Innovation
INTRODUCTION
With advancements in personal hand held devices, smaller more mobile computers, tablets, and the world’s population connected with social media the threat to the user’s privacy has been diminished. I will look at how access control policies have opened the proverbial door to user’s privacy being attacked and threatened. You will see examples of how users have to divulge personal information to get better service and even be monitored while at work to prevent intrusions in to the company.

ACCESS CONTROLS
When pulling up to the front gate of a military instillation there will be a guard standing there ready to check your ID to verify that you have the proper credentials to be allowed on to the installation. The guard acts as a control point for the base verifying that you have permission to access the installation. The security guard is a type of physical access control and we are here to talk about digital controls that are implemented inside of the systems and networks where people try and access information for many different purposes. Basic access control policies include a username and password that will be entered to verify the user identity and permissions for system usage. We as a collective of data specialist and security professionals have come to the realization that these most basic controls are not viable anymore to protecting sensitive governmental and corporate information.

That’s is why there are more in depth access control policy methods such as: Mandatory Access Control (MAC), Role Based Access Control (RBAC), Discretionary Access Control (DAC), and Rule Based Access Control (RBAC) (Infosec Institute, 2012). Looking at security and the ability of control within the systems, mandatory access control is by far the most restrictive for the user. The user has no privileges or control over the systems within the computers or devices that would allow them to set access to certain data or programs. Everything is controlled by an administrator and that administrator is the one that provides the privileges for each user on their devices. The MAC method is very administrator intensive and demanding since they are the only ones that can set the privileges for each user in the system.

Within MAC there is a model called Bell-LaPadula named after its authors and creators (Infosec Institute, 2012). The US government and many other governments are famous for using this model in the form of Top Secret and other levels of security for their data and information. There is complexity to how the model sets up it access to certain documents by not allowing a person at a certain security level to access information at a higher level but can obtain and read information at a lower security level. As an example Jamie, who has a Tier 2 Top Secret security clearance,
has composed a document and saved it to her company’s server. Blake, only having a Secret level security clearance will be unable to access or read the document. In turn if Blake has written something and saved it on the same server Jamie, having a high security level, would be able to access the file and read through it. Jamie would also be able to write into the document that Blake has created. The US Government has added changes to this model to make it more secure and to not allow for the misuse use of data by implementing a need to know basis for being able to access information of the same security level or lower as the user. Meaning that if the user has no reason for accessing the data then they will not be given permission to access it mitigating internal theft and someone being able to access data that is not part of their defined job.

Fine-grained and context-based access control policies are much better at providing data and information confidentiality, integrity, and availability, also known as CIA. Context-based access controls also known as CBAC use an intelligent firewall that filters TCP and UDP packets based on application layer protocol session information (Context-based Access Control, 2016). Where Fine-Grained access control policies allow the user to only access theirs companies information during certain working hours (Brossard, 2011). The challenge with these two types of control policies is and will always be the internal threat, the user having authorization to access organizational proprietary and sensitive data for misuse and worst case theft. In 2014 the US Fraud Retail Survey found and identified that employee theft was the biggest cause of loss to retailers (Leinbach-Reyhle, 2015). Although that survey was on a retail market the same can be said about any company and its corporate structure. To improve these control policies extended access control models have been proposed, including time-based access control models, location-based access control models, purpose-based access control models, and attribute-based access control models that restrict data accesses with respect to time periods, locations, purpose of data usage, and user identity attributes (Nabeel, Shang, and Bertino), respectively.

**USER PRIVACY**

Access control policies secure and provide confidentiality, integrity, and availability for an organizations or governments data and information but what about the user’s personal information that is being collected and stored while he or she is using the system. With the growing amount of social media sites in use by people all around the world, maintain privacy for the user is a precious commodity. Facebook allows the user to dictate what he or she will have displayed on their page just as a company puts access controls on their systems. These controls can range from allowing a certain post to be viewed by the user’s friends only or by the entire world if they so choose. Not only is a user’s personal information being used for public viewing on social media but is now being used for all sorts social engineered
processes. Ranging from the advertisements that are displayed on the webpages being viewed to data inputted into algorithms that will predict what pictures to display on the users Instagram account.

All around the world we as a collective people amass 2.5 quintillion bytes of data every day being spread across massive networks of computers increasing the attack surface of the entire system (CSA, 2012). As people make searches, order items off retail websites, and post news updates to their Facebook page data is being collected about them and stored. How is this data being used and for what purpose?

Alan Westin defines privacy as “the ability for people to determine for themselves when, how, and to what extent, information about themselves is communicated to others (Westin 1968).” Abiding by this outlook of privacy, users are giving up control of their personal information at an alarming rate and most don’t know it is happening. Social media sites such as Facebook, Twitter, Instagram, and many others have privacy controls that allow the user to dictate how much of their privacy they are willing to sacrifice to the general public of the world. I use the term sacrifice because it is just that. Most of these controls are very vague and hard to interpret and makes it difficult for the user to ascertain what information he or she is making public or private. And being that no two social media sites are going to have the same privacy controls it is doubly difficult adjusting the settings between different websites and trying to maintain these controls as a user can be very difficult.

Social media sites might allow the user to control what they want to share but once the user’s personal information is out there in the world wide web there is no getting it back. In 2009 Carnegie Mellon Researchers were able to identify people by their social security numbers using just public records from the internet. Using people’s social media pages and governmental records that are public they could correctly identify one out of 20 complete social security numbers born in Delaware in 1996 (Nabeel, Shang, and Bertino). Social Security Numbers being linked to a person’s identity make them very valuable to that person. Having your identity stolen is not only a violation of a person’s privacy but also to their security in being able to protect their identity.

**PRIVACY VS CONTROL**

So if someone can so easily use social media and public records to reconstruct a person’s S.S.N so easily what’s to stop them from trying to make that person do something that they wouldn’t normally do. Having access controls implemented and monitoring the user’s online behavior allows for internal threats to be prevented or flagged for later inspection. Internal threats are not always intentional decisions and can originate from misuse of the company’s data or from a third party through and internal source that is unaware of the intrusion.
No matter intentional or unintentional organizations and governments are always trying to mitigate and lessen the amount of data loss that is due to the internal threat. They mitigate this threat with the use of the access control policies that we were talking about earlier. But on top of those policies because of Social Media sites and the abundance of scams, organizations and governments are going a step further to protect their precious data. But at what cost are they doing this? At the cost of the user’s privacy?

On a person’s profile page, they might have certain information set to allow only friends to view the information, but what is to stop a friend from divulging information about that user to another person. Because of Social media users are targets for specialized spear-phishing attacks and socially engineered scams that are designed to retrieve and ascertain sensitive and personal information that is then later used against that user and in attacks towards the organization. And there lies the dilemma of trying to balance control and user privacy. On one hand you want to prevent unauthorized access and theft of data and on the other hand maintain the privacy of the user’s personal information.

Companies with the use of Context-Based access controls are able to watch what it’s users are looking at and saying on the world wide web while using their systems. With the data that company collects on its users it is able to construct its own profile of its users. This collection of data and profiles allows the company to spot and track anomalies in its user activity. The company now has a viable way to monitor its users by looking into their personal life to keep its own information safe. When properly implemented content-based access control policies can reduce the improper data accesses and the opportunity of insiders to steal information from the company. As an employee of such a company you are giving up privacy rights to continue your working for said company and some people don’t even know that it is happening to them.

With 91% of the worlds adults owning and using a smartphone or tablet (Rainie, 2013) for work and personal use, access control policies need to be more flexible and adapting to change. That is why the models for location-based, time-based, and attribute-based models are so important now. With these control policy models users are able to be mobile and work from their personal devices on corporate data without threat of data loss in the company.

Attribute-based allows for the user to identify himself or herself to the company’s system to ask for permission to access it. With every smartphone containing GPS chipset, that most users use for directions, the company’s system can then ascertain the user’s location and check it against it authorized locations for acceptance. Then comes, time-based access controls, is the user trying to access the system during a pre-determined time of day that is within the company’s guidelines. With all three access control models plus context-based implemented, the
company’s data is a lot more protected. These controls give the company an abundance of control over its user’s privacy to maintain security of data.

At the same time access control policies alone are not always sufficient at protecting and preventing against internal threats. A user might have legitimate permission to access a certain spreadsheet from his company’s server from his personal smartphone while he not in the office. But when that user accesses and downloads the spreadsheet instead of adding to it during his normal business hours, the system will detect the anomaly and flag the event for inspection. The access controls were implemented in the system but were only able to flag a misuse and not able to prevent the misuse of the data.

MAKING PEACE

So how do we balance the scales of user privacy with the control of an organization’s personal and proprietary data? Playing devil’s advocate looking at both sides there is pluses and minus for both sides. It is a give and take scheme in that both are trying to protect the privacy of the user and the data of the organization. On the one hand there are access controls that provide a security blanket for the organization to protecting its data but the user in the organization gives up some of their privacy to help the organization maintain its security. If the user wants to maintain their personal information, it limits how much control the organization can provide for maintaining the security of data.

I propose a model that works with all previously discussed models of access control but implements notifications that notifies the users of what information is being used and for what purpose. When a user is notified about what information that he or she is about to give up they have to the choice to continue or decline to continue. Not only should the notice list what information is being requested but there should also be a statement about who will be receiving the data and for what purpose it will be used. At this point the user is dictating their own privacy model and allowing the organization to use their information for future purposes.

For example, if Jamie is using her tablet from home to access her company’s server to retrieve a spreadsheet, the system would notify her that her location, time stamp, and open applications on her tablet will be monitored to identify any anomalies or possible attacks if any were to transpire during her use of the server. If Jamie does not want to allow the company access to her tablet to monitor it while she is accessing their system, then she can simply decline the request and access the document during the normal working hours at her workplace. Two fold Jamie’s privacy and the company’s data has been maintained and nothing was sacrificed or given up without consent from either party. The same can be done if Jamie was given a work tablet and if she wants to look at her social media sites on that tablet then she will be notified by the system that if she wants to view those sites that she
will be allowing the company to monitor her sites and also be collecting data off them.

The other way that it can work is when a user is at work and they have access to both company data and personal data via social media. Blake is worried about his friend who just lost his mother in a tragic accident, so he visits his friends Facebook page to write and post message expressing his condolences. The system will then notify Blake that if he wants to continue that he will be allowing the company to gain access to his Facebook profile and be able to monitor what he is posting and reading. There is also a disclaimer in the notification that if he continues that the company will be storing any data from his personal profile and may use it later to monitor his online presence. Blake chooses to continue and allow the company to monitor and store data about his online presence through social media allowing them to look for anomalies in his behavior and Blake willing gave them the permission to do this and was given the opportunity to not proceed.

When it comes to the usage of the personal information that the user is willing to give up, the notice should be written in such a way that the user can understand and ascertain exactly what it is being used for. For instance, when entering your likes and dislikes on Facebook there would be a description of what those likes and dislikes will be used for, i.e. targeted advertising on your profile page and certain people’s postings as they pertain to the likes that you’ve set.

Ultimately the access control policies have to be malleable to allow for change and modeling to each individual user instead of an umbrella standpoint. There will still have to be a leveling as to not allow for a user to have access to data that is not intended for their eye but from the stand point that the control can be flexible to allow for changes. People are ever changing and so is the world that we live in. Technology is growing at a rapid rate and changing how people connect with and use data and to protect it and people’s personal information the two have to work together cohesively as one.

REFERENCES

   http://resources.infosecinstitute.com/access-control-models-and-methods/

2. Nicole Leinbach-Reyhle (2015), New Report Identifies US Retailers Lose $60 Billion a Year, Employee Theft Top Concern, Forbes Magazine,


   http://www.webfarmr.eu/2011/05/coarse-grained-vs-fine-grained-
access-control-part-i/


