Discussion Posts

Week 3: Apply a Multilevel Access Control Model to Company X

"Company X" is an organization that you currently work for, that you have worked for in the past, or that you have a solid understanding of. It is not necessary to name the company, but please provide some background about the company's industry, size, and competitive environment.

Chapter 3 of the Andress text describes three models of multilevel access control: Bell-LaPadula, Biba, and Brewer and Nash (aka Chinese Wall).

Choose one of these models and apply it to "Company X", detailing the benefits and downsides that you think would accompany this choice.

I previously worked in an I.T. department at **State College** as a user support service technician. “Company X” had around 1,500 employees, 6,000 students, with my department having around 20 people. Five were full time staff, and the other 15 were student workers. The user support service group handled compute repair, software install/removal, malware scans/removal, and remote help to assist customers when not on campus. The competitive environment didn’t really exist because state bureaucracy kept innovation from happening.

I see the Biba Access Security Policy as the most desirable fit for Company X. With Integrity as the core focus of the Biba model, it assures that only those with proper access can modify the state of data. Since the user support service grouped often used remote access to control customers computers, the importance of data integrity is important. Those who are remoted into a particular computer should not be able to make changes to its state without the user’s permission. The **benefit** of this security policy for Company X would the assurance that only those with a given access level would only be able to modify state of that same integrity level.

The big **disadvantage** with the Biga Access Security Policy is that it only enforces data integrity, and not confidentiality. Therefore, a user would not be able to grant a customer proper authorization to download gated software, nor would they be able to remove an authorization.

# Week 3: Identification/Authorization/Access Control and the 15 Biggest Data Breaches

88 unread replies.88 replies.

This is a good time to introduce a website that we'll visit off and on during the course titled "[The 15 biggest data breaches of the 21st century (Links to an external site.)](https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html)"  
**First** select one of the breaches described on this site that you believe could have been avoided by improved

* Identification,
* Authorization,
* OR Access Control.

Explain what type of change you recommend and what the impacts would be on the breached organization, e.g., in terms of profitability, etc., and on the (non-criminal) users.

**Second**, reply to at least one other student posting to comment on or question their analysis.

The **Adult Friend Finder** breach is an example of an avoidable situation, if the company had stronger **identification** methods. After researching the breach a little further, I found that 340 million records were compromised, and of those, 103 million passwords were stored in plain text, and the others were hashed with SHA-1. The hackers were able to guess the common passwords and crack the unsafe SHA-1 hashing algorithm. SHA-1 was considered unsafe to use as early as 2011, so there was no excuse for it to have bene implemented on the website.

My recommendation would be to implement a multi-factor **identification** process, based around something the person knows, something they have, and something they are. The breach would have been avoided because even if an attack were to guess or crack a password, they would still require other forms of identification to prove user authenticity. Though in 2016 MFA wasn’t a common practice, more and more organizations such as WPI are implementing it because they see the clear security benefits. I would also recommend that the company switch to a more secure hashing algorithm such as SHA-3 as well.

In terms of my identification recommendations hurting profitability, the only thing I could see is perhaps it would raise the barrier of entry to signing up for the site. In the short term this may decrease the average revenue per user, but the added security more than pays for itself in the longer term. I would advise them to not be penny wise and pound foolish, and that the investment would add to profitably in the long term by avoiding major hacks and public relation damages.

# Week 3: Identity Management

No unread replies.88 replies.

Hovav and Berger write in their 2009 paper, "Tutorial: Identity Management Systems and Secured Access Control": **"Identity Management has been a serious problem since the establishment of the Internet. Yet little progress has been made toward an acceptable solution."**

**Part 1.**Indicate whether you agree with this assessment.  Then choose **ONE**obstruction to effective identity management and discuss the prospects for overcoming it . . .

OR choose **ONE**standard approach presented in the paper and describe the benefits and downsides that you believe to be associated with the standard.

(In order to preserve opportunities for other students, please **DO NOT** present a "laundry list" of responses when you are asked for **ONE**response in a discussion topic.)

**Part 2.** Reply with a question to at least one other student's posting.  Comments are allowed but will not be scored.  Reply to all questions you receive.

I agree completely with Hovav and Berger’s assessment on the serious mess that is the current state of identity management. One of the bigger issues that they cite as a challenge to identity management is **trust**. Whether it be trust of the system, trust among the service and identity providers, or trust among the agents and services.  Therefore, I see **trust** as being one of the biggest obstructions in the way of the industry when it comes to identity management.

However, I believe that are some prospects for overcoming it, and I look at blockchains with their use of consensus algorithms as being one of the top prospects. Using consensus algorithms such as Proof-of-Stake or Proof-of-Work, we’re able to remove trust from a middle party, and validate trust using the consensus of a distributed network. This gives us an opportunity to create new protocols to help solve identify management. I could see a future where there’s a version of DNS, but for your digital identity, which is written as smart contracts on a blockchain. With the network validating trust, it removes a tremendous hurdle from the process of solving the identity management problem.

The "web 3" community holds the idea that distributed networks are the foundation of how we’ll solve some of the bigger issues around our digital identity management, and our personal data management in the 21st century. With the ability to tokenize protocols, therefore being able to manage how we interact with them inside a crypto wallet, there could be some real innovation ahead of us in the next 10 years. However, with all new uncharted territory there will be unknown dangers, and that's something that must be kept in mind when attempting to build a better foundation than the one we're working with now.