Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Control Architecture - Access Controls

What access control model will you use? Let's start by looking at the typical options:

- **Use clearances, classifications, and compartments:** Clearances are defined by the level of trust of individuals based on background investigations, history, and other factors as defined. Clearances are defined for content based on magnitude of consequences associated with the misuse of the content. Compartments are based on the groupings of content necessary to perform kinds of work. Access is granted based on holding a clearance high enough for the classification of the content, working in an area associated with the content, and having a reasonable need to know the content in order to perform an authorized task. Separation of duties and risk aggregation limit the compartments permitted and, in more advanced cases, the set of compartments allowable to individuals over time.
- **Use roles and rules:** People are assigned roles based on what their job assignments are and access is granted based on a set of management defined rules about what different roles access under what conditions in order to perform their roles. Separation of duties and risk aggregation limit the simultaneous roles permitted and, in more advanced cases, the sequences of roles allowable to individuals and groups over time. Rules also change over time and must be analyzed for separation of duties and risk aggregations.
- **Use owner authorized:** Content and systems are "owned" on a fiduciary or actual basis by individuals who make individual determinations about what individuals or groups may access what content under what conditions.
- **Use a subject object model:** Subjects (people and automated mechanism) are granted Rights (things that they can do) to Objects (content, containers, and mechanisms) based on management decisions. Risk aggregation, if done, is done by analysis of granting of rights over time.
- **Use a possession-based model:** Access devices of various sorts (e.g., keys, certificates, tickets, tokens, money, etc.) are possessed by individuals or mechanisms, and access is granted based on possession and possible surrender of those devices.
- **Pick the best fit of these or create a different enterprise model:** It is almost always better to pick one of the above defined mechanisms since they are already realized in implementations of various sorts, however; many of the mechanisms can be repurposed for other uses, and mechanisms available should not limit the manner in which access is modeled.

Given these alternatives, and of course there are plenty more where they came from, how would you choose which one to us in what circumstance?

Here's the advice we start with when we do analysis for our clients:

IF A regulatory mandate requires it, or if you are working largely for an organization that uses it, **THEN** Use clearances, classifications, and compartments.

OTHERWISE IF A model is already in use and changing it would be too expensive or difficult **THEN** Use the current model.

OTHERWISE IF Workers change tasking often, have many areas of responsibility at a time, and many workers do the same tasks, **THEN** Use roles and rules,

OTHERWISE IF Content and systems have ownership assigned and delegate work based on their ownership, **THEN** Use owner authorized,

OTHERWISE IF Well defined individuals or mechanisms have rights or privileges with respect to well defined content, **THEN** Use a subject object model,

OTHERWISE IF Anyone should be allowed to do anything if they can "afford" it or have been "given" access by someone possessing access **THEN** Use a possession-based model,

OTHERWISE Pick the best fit of these or create a different enterprise model.

But of course this is only the starting point. The reality on the ground dictates different models of access control in different situations, and while we try to codify what we think are reasonable decisions, when we meet with our clients, we often find that other considerations overrule even the most sensible ideas we might seem to have. A good example might help.

It's not uncommon for clients to be audited and be found wanting on one area or another. In the case of one of our clients, the audit indicated that they were using controls that were not appropriate to the regulations they were under. While we could hardly advise them not to follow the legal and regulatory mandates they faced, making the changes that the auditors had in mind would likely have been a very big challenge. So we took a different tactic. We identified the potential that they could push back on the auditors and, while they were going through the process of negotiations, change certain facets of how they did business so that it would limit the areas of the enterprise that were under these constraints. By reorganizing while using the delaying tactic, they were able to reduce the need to meet the requirement and then agree with the auditors to a new approach that would meet the requirement only for the newly segregated part of the enterprise to which the particular regulations applied. They got a warning instead of a violation, fulfilled their obligations before the next audit, and didn't have to follow regulations that were not really fruitful except where this was really required.

While "control architecture", which this particular issue falls under, is a theoretical concept and not directly connected to technical implementation, making sensible decisions about the structure of your controls is fundamental to both getting the controls to work and controlling the costs and consequences associated with the technical implementations you put in place. A little bit of theory mixed in with the practicality of everyday operations helps keep the enterprise health for a long time to come. And in lots of cases, it can save you more than just money.