I’m Dr. Michael Mann and tonight's review session is on authentication controls.

This is, of course, in preparation for the Security+ Industry Certification Exam. I am using questions from the Virginia Cyber Range and we'll go ahead and get started with the first question.

What does AAA refer to when concerning enforcing security policies?

Let's take some responses. What do you think? One, two, three or four?

If you're not sure is there something that you can see to eliminate fairly quickly.

The last option?
And what makes you want to eliminate that? I agree with you by the way.

The rest of the options kind of make sense but the last option has something extra in there. That doesn't really go with cybersecurity as far as I'm aware. Sure amelioration yeah.

That’s not exactly par for the course for cybersecurity technical language and it's not like we're interested in ameliorating anything when we're talking about AAA. Is there another choice that doesn't look right?

So the third choice - starting with access - it's close, closer than the choice number four that has the term amelioration in it. But really when we're talking about AAA; we're talking about one of the first two choices. So which one is it?

Is it the first choice?
The second choice?
The second choice, so “Authentication, authorization, and accounting.” Now, what's the difference between the two choices? One and two? And it really is just the order in which the terms are presented. However, is there anything that is important about the order of the terms?

What do you think? Is it like the steps you have to take, the steps have to go in a specific order?
Yes, that is correct. First, you are authenticated before accessing a resource. Then, based upon your credentials, you are authorized to access certain resources and then, finally, the accounting part keeps track of basically what you've been doing. So “Authentication, authorization, and accounting” are the correct answers for this question.

This is it's a little tricky because you look at the first two choices and right and you're in the exam and you're like well you know they're all the same, both saying the same thing, but the order for this question - the order of the answers - is important. Let's move on to the next one.

Which of the following is the best example of conditional access control?

Choices one through four: A government employee is only allowed to access information that their security clearance allows them to access; or

A user is given access to a certain level of sensitive files based on the project they have been assigned to; choice three - An individual who created a document gives access to their friend for peer review; or choice four - A subject's account approval is evaluated based on your current operating system? What do you think? Number two sounds like a viable answer. Number two is a viable answer and in fact it is the correct answer. Yay! Very well done and what about choice number one? Does that look like conditional access control?

No it doesn’t; it's more closely related to mandatory access control and three is more closely related to discretionary access control and finally the fourth one is more closely resembling rule-based access control so knowledge of control models is important for dealing with this type of question. So our correct answer here is choice number two, “A user is given access to a certain level of sensitive files based on the project they have been assigned to.” Let's move on to the next question.

This question involves dynamic code. After entering your username and password in the login screen for your cloud account, you click submit and then a special code that changes every minute is created for you to authenticate yourself.

What security measure is deploying this dynamic code? Is it TGT, TOTP, SMS or Certificate Authority? It helps to know what the acronyms stand for the exam is and the course as you probably know already is big on acronyms. So does anyone know what TGT is?

No? Okay Ticket Granting Ticket. TGT are files created by the key distribution center portion of Kerberos Authentication.

What about TOTP? Does anyone know what that one is? TOTP - Time-based One-Time Passwords and it's a common form of two-factor authentication and SMS - obviously Short Message Service - and Certificate Authority. So, what do you guys think?

Choice number one, two, three, or four?

I know it's not number three because it doesn't get sent to the phone so maybe number two? Number two is the correct answer. Awesome. This is a time-based one-time password.

Questions about that or does everybody understand applying based one-time password?

So where would the first one be sent to? The TGT? Like where would that pop up?

It's a created file that would be used and not necessarily sent to a user in the same way that a time-based one-time password would be. Oh, okay.

Let's move on to the next question.

Multi-factor authentication: Which of the following terms most closely relates to multi-factor authentication?

Your choices are: Token key; SSO; PAP; or HSM.
They really love their acronyms, don't they?

You mind saying what the acronyms are? Sure, let’s start with first one listed, SSO. Now this one's pretty widely used. Does anybody know what this is? A single sign-on? Absolutely it is Single Sign-On and is not involved with
multi-factor authentication. How about PAP?
PAP is is Password Authentication Protocol and again not related to multi-factor authentication in networking you may have come across this as a point-to-point protocol used between two routers to authenticate but it's generally considered fairly weak. It sends passwords in plain text and in that context
it's typically not used but instead, Challenge Handshake Authentication Protocol is used in
its place. HSM - anybody know what that one is?

So HSM stands for Hardware Security Module and this is a hardware card that contains a
cryptoprocessor and is used at the hardware level.

So just from knowing the definitions of these acronyms it's pretty clear that what's left
is Token key and that is most closely related to multi-factor authentication.

So that's our correct answer for this question and we'll move on to the next one.
Okay, Security Assertion Markup Language or SAML tokens possess what kind of data after being granted access?

Does anyone think Biometric?
No. No, absolutely not biometric. And PKC data?

Okay, so there's it's not involved with Public Key Chain plain text.

So this is SAML tokens we’re talking about.

Does it make sense that these tokens might have plain text data.

What do you think? Is that a good choice?

No? No, it is not. So our answer or this question is claim data.

So SAML or SAML token encrypted claim data and that's the answer we're looking here.

So the next question involving SSH public and private keys:

Your organization's network administrator is configuring the Linux server’s

SSH Authentication to allow key-based authentication.

This setup requires that the private key is ___ and the public key is ___. Okay, so what is SSH?

Okay nobody got this?

All right, Secure Shell?

So we're talking about private keys and public keys. Your choices are:

The private key is kept with the user; and the public key is kept with the user. Or The private key is kept with the Linux host and the public key is kept with the Linux host; or The private key is kept with the user and the public key is kept with the Linux server; or, finally, the private key is kept with the Linux host and the public key is kept with the user?

What do you think is the correct answer? Is it the third option? The third option - so the private key is kept with the user and the public key is kept with the Linux server and that is correct. So probably the easiest way to remember this is that private keys are always kept with the user.

And so the public key is not. Knowing that of course narrows your answer choices down.

The second choice then is easily eliminated because a private key would not be kept on the

Linux host and neither would the fourth choice be a viable choice as well.

Okay let's move on to the next question.

The ___ model is used to allocate labels to objects and subjects for access control clearances.

So, clearly uh the question involves understanding the acronyms listed again.

Let’s start with that; how about the first one DAC.

Does anybody remember this one?

Okay so this is Discretionary Access Control. How about RBAC? Is that Rule-Based Access

Control? It's confusing; it could be rule-based; could also be something else.

Anybody know what the other thing is?

So, yes, we have rules, we have discretionary, we also have role-based access. And how about and how about ABAC?

Attribute Based Access Control? Yes, Attribute Based Access Control.

So clearly you need to know something about these different models to be able to negotiate this type of question.

DAC or discretionary Access Control involves granting access by using some type of access control list okay and I'm saying that in a very general sense although conceptually Access Control List or ACLs you may have heard of or come across using them in the sense of firewall rules or perhaps even access control configured on a router or a switch.

And the idea is kind of the same; we aren'treally or we aren't necessarily talking about ACL’s on a firewall or a router in this question. The question is talking about allocating labels to objects and subjects. Now if it hadn’t. said subjects then I would say that could be it could be talking about network appliances. But when you see the term subjects what comes to mind?

Like people? Yes, absolutely, like people so that gives us some contextual information about the question and the answer choices and would also lead me to think that in the second choice RBAC is referring to role based instead of rule based now we go back to discretionary and as I said access has granted using some type of access control list in the general sense of the term and we've already spoken about how on a network appliance you can say for example on a router set up access control list to control traffic flows and by the same token so to speak users and groups can be granted access to a file for example based on file permissions.

So the concept of the access control list applies sort of in both domains network appliances and also people so now the question is is the description in the question allocating labels to objects and subjects for access control? Is that a type of discretionary access control model?

So what do you think, yes or no? You have a 50/50 chance.

Anybody want to take a guess?
I don't know but I'll just say yes.
The answer is no; it is not discretionary. Good guess, though.

What about role-based access control?

Does that sound like it could possibly be right? I think role-based could be right. You think it's
right? I think so. You do, okay, any particular reason? Because people could have roles. Sure. That’s the kind of connection I'm making.

Okay and role-based is a type of non-discretionary access control.

Some of the characteristics and it takes a real world approach to structuring access control and as it sounds it's based on a user’s job function within the organization.

But that doesn't necessarily mean that this model allocates labels so it's not role-based.

What about Attribute-Based Access Control?

I think it's this one okay because it's attributes and it's saying labels.

So you're saying the labels that are allocated are attributes. Yeah they could be so and and I can see why that could be an appealing answer in fact I might even call this a misdirector. This is not the correct answer. Attributes are often pre-existing and not handed out necessarily on the fly which is sort of the implication in this question.

So in ABAC - Attribute-Based Access Control evaluates the attributes or what we
could think of as characteristics rather than roles to determine access. So the purpose for doing this is to protect objects such as data or network devices and other IT resources from unauthorized users and actions.

In other words, if you don't have an approved characteristic as defined by the organization’s security policies then you don't get access so we're left with Mandatory Access Control and so this is where the the allocation of labels comes into play and again knowing the different models, you kind of go through and use the process of elimination to negotiate this type of question. Once again, think it's important to point out that acronyms are a large component of this topic not just this topic but of the industry certification exam and it really is important to know them. Often I get questions about you know how to deal with so many not just pieces of of knowledge-based information that is as opposed to something that is performance oriented but rather something that is more straight-up knowledge based but also compounded by the fact that there are acronyms and you know the response is that in the first place you you have to know the acronyms. In my conversations with students over the years and even for my own purposes because if I take an industry certification exam I have to deal with the same thing you do. I’m not immune to the design of the test makers. I see the same exams you do and for me doing something with the information and it could be something as simple as creating PowerPoints is helpful because it allows me to do something to create something, to create something, some information product using the terms or the acronyms and of course when you're doing this you're going to keep the acronym and then spell it out so you understand what the meaning is. And this this type of work I've always found useful and if you really want to sort of take it to the next level, especially when it comes to creating PowerPoints, you can get Jeopardy-style templates that are pre-made and download them and use them in PowerPoint and then all you have to do is fill in the content information.

So there are two things there that can help you the act of actually doing the work to create the study tool is very helpful and then of course using it over and over again to help with your learning and your studies and when you do this kind of work it really helps you to sort of internalize the information and once you’ve done that you'll find that recognizing and understanding and knowing the acronyms becomes a lot easier. So let's move on

So in this question we're talking again about Attribute-Based Access Control and Role-Based. The question states, Which comparison between Attribute-Based and Role-Based Access Control is a true statement? Your choices are:
The ABAC configuration covers more broad access controls whereas our back controls access on a more detailed level; or number two “The ABAC does not include roles in the access control criteria because that is what the RBAC is for; number three “The ABAC is the most fine-grained type of Access Control whereas RBAC is not as precise or,
finally, “The RBAC and the ABAC 00:30:30.660 --> 00:30:36.600 are on the same level of access controls but they just look at two different parts.”

Okay so what do you think for this question?

Do you see anything that could easily be eliminated?

Let's take a look at the second answer.

It states that ABAC does not include roles in the access control criteria because that is what role-based is for.

Okay so that's not a true statement; attribute-based does include information about roles than it has to because the subject is the user requesting
access to a resource to perform an action.

So that helps us you know with eliminating the second choice.

Now if you understand that and you look at the fourth choice role-based and attribute based on the same level and they really can't be because attribute-based includes role-based information so then that knocks out the fourth choice and
that leads us with number one or number three.

Would it be the first one?
No, it would actually be the third and if you think about it obviously you have to study this and prepare for it but when we talk about attributes in attributes of something - the subject, an object - the first answer states that attribute-based covers more broad access controls 215
00:32:56.940 --> 00:33:03.000 and the third answer states that attribute-based is the most fine-grained or what we would call a granular, has a high level of granularity or type of access control and that is true and in fact that is the correct answer.

Attributes or characteristics make up something larger so attribute-based control is appropriately named and that answer choice would stand out if you were just trying to look \
at this on the basis of elimination based upon what you know and we often use this technique that becomes the clear choice so it's not a more broad focus it is a granular focus.

Okay, Describing MFA and MFA is what?

Multi-Factor Identification. Yes, so that was pretty quick; How were you able to come up with that so quickly? I just kind of memorized it

I've heard it thousands of times. You've heard it thousands of times thank you you've probably used it thousands of times as well. Do you see what I'msaying or what I'm getting at with these acronyms?

So most people understand very well; what multi-factor authentication is and you know we use it all the time right. We have to use it to get into my portal to get access to things like Canvas or SIS. So it just adds more credence to the point that the more you use something the easier it is to recognize it and recall it and deal with it.

Okay, When signing into an account you are told
to enter a PIN and the last four digits of your Social Security number to be authenticated. Does this describe multi-factor Authentication Not to put too find a point on it but what
is a PIN? What does that acronym stand for?

Is it Personal Identification Number? Yes.

Now this is kind of by the way the sort of opposite end of what I've been saying about acronyms. You can find those that you use so often that you stop thinking about what they mean or what they're what they stand for with the letter
stand for and if that goes on long enough you can actually forget. Just an interesting point. So
we're signing into an account, we enter a pin, we enter the last four digits of our Social Security
Number - Is that multi-factor authentication?

Yes, because it is requiring the user to present at least two different credentials
or no because it is not requiring the user to present more than more than two different credentials or is it yes because it is adding a layer of protection to the authentication?

Or choice number four, no, because it is not using a combination of different authentication types?

What do you think?

Yes, first one. Okay, the first one. The first one okay; anybody else?

Morgan? I agree with her choice I think that's right. I'm sorry, I was just reading it before I said something. That’s okay, so you think it’s the first one? Yessir, I agree that it's an example but then I've never - the only time I ever think of multi-factor authentication is like getting a text or an email or something. Okay. So I’m so I'm going back and forth.

So let me throw out a few phrases for you to consider: Something you are; something you have; or something you know. Does that help?

What do we think now? Is it choice number one, two, three, or four?

And remember: something you are; something you have; something you know.

So in the question you're told that you're entering a PIN and the last four digits of
your Social Security number.

Given that information, is this answer going to be a yes or a no
in terms of multi-factor authentication?

I still say yes.
Okay so we've got one vote for yes.
Yeah I think yes as well.

Which is probably not the reaction.

Well this is the fun part right we get to talk about it.

Okay so Morgan did you have a comment?
Yeah, I'm confused now. I've been confused. I'm not gonna lie. So for multi-factor, does it have to like Seth said on like text and emails? Does it have to go to
something else or is it okay that you enter it all like on the same device? Like the same portal like at the same time?

Okay so it is less dependent on things like the media or devices and it's much more dependent on is this, are they giving you something you are, something you have, or something you know?

Let's talk about a PIN and we've all come across this in various applications.

Probably one of the more obvious is uh I don't know, a credit card pin number or perhaps a debit card and number and so which category would a PIN number fall into. Is it something you are,

is it something you have, or is it something you know? Something you have? Okay, So Seth? Well I've got something you know actually, I'm sorry, okay, I feel like it's a little bit of both because you have it and you know.
Okay, I'm guessing. I think it is no.

Let's start with that determining which it is because I think it's pretty clear it's not something that we are, but the the confusion seems to be around is it something you have or is it something you know? And you know if you think about it from the point of view if you when I say pin number if you see your debit card right that kind of makes you think in your mind that it's something you have okay but you have the credit car. The PIN

Is knowledge that you've created in other words? I mean most often we choose our own maybe not initially right if it has to have something they might you know the organization might give you your PIN and go here and remember to change this but a PIN is really something we know. So is it only something we have if it's tangible yeah okay.

So your Social Security card or your social security number isn't something you have; ;
That's something you know? So that's correct because they're both knowledge-based items. So then the answer is no, right? too different? So it's easy to understand that it's not something you are the difference again is between have and something you know.

So these are both something you know so what do you think the correct answer is at this point?

289
The second one?
The second choice says no because it is not requiring the user to present more than two different credentials. Well multi-factor really means two or more.
But wouldn't it be the last one because it's authentic authentication.

Yeah that's correct.

I just re-read that I'm so sorry.
No, that's fine, that's fine so that's the real problem here. It’s not multi-factor because you're
not using different authentication types. They’re both the same and they have
to be different to be multi-factor.

All right let's move on.
This question involves geotagging. Which of the following is the best example of geotagging?

Number one - A user takes a photo that gets GPScoordinates embedded into it; number two, Someone can locate a person's location in real time by tracking the coordinates of their mobile device; or number three, A device that can report its location very accurately while outdoors; or number four, A storefront that can send push notifications when you are driving past it.

Which of those choices is geotagging.
The first one?
The first one. Okay anybody else?

Okay so yeah Seth you're correct; it is the
first name. What is the second one an example of?

Okay so the term we would use for the second one is geolocating. First one’s
geotagging; second one is geolocating. What about the third one? This is pretty common.

You're out taking a long hike or trip through the wilderness. It's a good idea to have one of these.

GPS?
Yes this is describing Global Positioning System because a device that can report its location accurately outdoors is a global positioning device. And how about the fourth one?

The term here that the fourth description is um is for is called Geotargeting. So geotagging, geolocation, global positioning and geotargeting. Let's move on.

On Premises to Cloud: Companies are starting to ship from using on-premises authorization solutions to public cloud provider auth services solutions. How might the change in processes be depicted?

Your first choice, A company's network that was open to partners, suppliers, and customers is now open to a well-defined group of employees; or the administration of accounts and devices
change from being decentralized to centralized; or businesses start using full-disk encryption

with cloud-based virtual machines instead of an on-premises virtual machines finally many
organizations originally used LDAP technologies but are now using some type of federation technology.

So the game is pretty much the same here when I take certification exams or any kind of assessment and especially if it's in this format I usually look for something that can be eliminated pretty quickly.

So do you see anything like that here?

Okay do you think it has anything
to do with full disk encryption?
As we're kind of talking - we're not kind of talking - the question’s talking about on-premises authorization versus cloud provider or off-premises.

Okay so the third answer is the one that jumps out as not really having anything to do with this. Okay so that leaves us with one, two, or four. Okay what do you think? Can we…

Thank you I'm sorry go ahead.

Does number one need to be eliminated as well?
Okay so company’s network that was open to Partners suppliers and customers is
now open to a well-defined group of employees.

I don't think that really matters because you can do the same thing whether it's on premises
or using cloud providers so good number one can be eliminated that leaves us with two or four.

So if if if these services are provided on premises…
So it's two?
What I was going to say was if they're provided on premises or off I mean as far as being a
decentralized or a centralized service it's probably not going to be that right because
if it's a centralized service and let's say you know um some type of AAA service on a server
okay and you know whether it be TACACS or RADIUS, if either of the solutions
let's say they're centralized would that necessarily change because
we went off premises to the cloud?

So that answer is kind of weak the best answer is the fourth answer and especially when they start talking about Federation technology because these type of services are what we would call and what the Security+ exam expects you to know as federated services
and especially when it comes to this this type of authentication and authorization and so the question is really describing federation services um and specific that generate access tokens

to provide access anywhere across the internet because that's what the cloud services get us.

All right.

SNMPv3 authentication allows the use of which hashing algorithm below? Your choices are MD5, SHA, Both A and B; or None.

This is pretty much a straight-up knowledge-based question so what do you think?

Somebody take a guess at it. One, two, three, or four? Three?
Both are correct and again it’s almost straight-up knowledge-based. It’s something that you just have to knoW; it can use either MD5 or SHA.

It's also probably useful to know that both of those can be brute force to recover a clear-text password so not exactly the strongest type of security.