Good evening everyone and welcome I'm Dr. Mann; we are going to be reviewing some Security+ exam questions.
Tonight's topic is authentication controls - Pt. 1 and 2 - Let’s get started with AAA
What does AAA refer to when concerning enforcing security policies? Take a moment look over the answers and let's see what you're thinking.

I think this one's fairly easy.
You can put your responses in the chat.
We've got responses coming in.
So let's see what people are thinking.
Looks like we have a lot of votes exclusively folks for B - authentication authorization and accounting and this is the correct answer. The answers that would be hopefully eliminated fairly quickly would be C and D - access authentication and accounting - access is definitely not part of AAA.

And then amelioration that one doesn't fit either and that leaves questions answers that leaves responses A and B. So my question to you is why is a not the correct answer?

The first A in the acronym stands for authentication and not accounting.
Okay, and I mean and that's straight up knowledge.
What else can you think of? Order matters.
So that came in the chat order matters and it does - this is backwards right first you have to be authenticated than authorization says what you can do and then accounting comes after the fact all right very good let's go to the next question.

ABAC/RBAC - Which comparison between attribute based access control or ABAC/RBAC - role-based access control - is a true statement? Take a moment look over the responses.

So we've got some responses coming in the chat; let’s see what people are thinking A and C and A and I'm not sure and that's Okay. So the correct answer here is C Choice C attributes based access control is the most fine-grained type of access control where role based is not as precise and you may recall that um role base of course allows access to resources and privileges um however a role is like a container object and the object has predefined privileges in the system so a user going into that role also receives those privileges or access control permissions. Now, ABAC configuration covers more broad access controls and that's just not true that is just not the definition.

Attributes-based access control assigns attributes or properties to users and resources and then uses those attributes. So for example you could configure a rule that specifies if the user has a department attribute of say accounting and the city attribute of Boston then then perhaps they can access a file this differs from role-based or even group-based in the sense that role-based and group based only check whether the user is in a role or a group so that's a much wider thing than attributes based which is more fine-grained type of control.

Role-based and attribute based are the same level of access but they just look at two different parts and that's not true. So, again, correct answer here is C attribute based is the most fine-grained type of access control whereas role-based is not as precise.

Let's move on to the next question.

Account policy settings - While attempting to log into your account a message pops up telling you that your password is about to expire and you need to create a new one soon.

After clicking the prompt to change your current password you attempt to enter a password you have previously used before. Which user password setting would be the reason that another message pops up saying that the password you entered does not meet the password policy requirements?

Take a look at the responses.

And put your responses in your chat.
We have several responses coming into chat.
And their votes or Choice C password history and this is correct. Maximum password age policy determines the period of time and days that a password can be used before the system requires the user to change it. Account lockout not the correct answer nor is password complexity. Those are kind of obvious very good and let's go on to the next question.

Authentication title - When a user is logging onto a service via their desktop computer they have the options to choose between being sent to

push notification or getting a phone call after
entering their username and password what
type of authentication is being used?

So we've got some
responses coming in the chat
Let's see what's on your mind.
So A, B but not sure.
So a PKI is public key infrastructure, which is a system for creating
storing and distribution of digital certificates
that really does not apply here
and that leaves us with out-of-band authentication
digital signature and Mac and seems the rest of
the responses were for being and that is
correct B is the correct choice.
When you put in your password your username
and your password you are on a system
but when you get a push notification or even a
phone call we call that out of band authentication
because it is going to another device that is not
in the data path so to speak of the same system
that you entered your username and password on
so we call it out of band authentication.
This description does not align with the
response digital signature nor does it align with
the response mandatory access control so again
the correct answer - out of band authentication.

Next question:

Conditional Access

Which of the following is the best
example of conditional access control?
Take a moment and review the responses
and then put your response in the chat.
So we've got some responses coming in
Let's see what you're thinking.
You have a choice for D, a vote
for D and several votes that could be
answer B. A user is given access to a
certain level of sensitive files based on the
project they have been assigned to and this
is in fact an example of conditional access.
Take a look at the first response - a government
employee is only allowed to access information
that their security clearance allows
them to access. What is that an example of?
Role-based access?
Could be but the wider access
in the resources for this exam and notably I
believe the book that you're going to be getting
they make a point of stating that
MAC involves employees gaining access to

resources based on their clearance level and the data classification of the resource and they have to match up. So the response A would be more correctly described as MAC. What about C? An individual who created a document gives access to their friend for peer review.

What does that sound like?

Temporary access?

In terms of the main types of controls what do you think it would be? Direct access control? So it is discretionary. It is the definition because the access is determined by the owner of the resource and it says an individual who created a document that's the owner and the owner of the resource can decide who gets access and who does not get access and then of course what kind of access they get. Then take a look at the last response a subject's account approval. Is evaluated based on your current operating system

What do you think there?

So these examples and associated with Access Control can be a little tricky so this sounds very much um again like Mandatory Access Control and in this type of environment a Mac and environment so access to research resource objects is controlled by the settings defined by say a system administrator and so that would mean that access to resource objects controlled by the operating system is going to be based on what the sysadmin has already configured in the system.

Let's go ahead on to the next question.

Describing MFA - Wwhen 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?

Read over the responses and put your choice in the chat. We have a few responses; let's wait a second and get a few more. All right let's see what you're thinking. So we have votes for D, C.

So the correct answer here is Choice D.
Does this describe MFA and the answer is
no because it is not using a combination
of different authentication types - the
response a yes because it is requiring the
user to present at least two different credentials
doesn't hold up that is an incorrect response.
You enter a PIN and the last four digits of your
Social Security number. What
are those both examples of?
Something you know - that’s correct and
so that does not qualify as multi-factor.
Response B - no because it is not requiring the user
to present more than two different credentials.
Two different credentials is fine as long
as the types are different and can be more.
Response C - yes because it is adding a
layer of protection to the authentication. No.
incorrect answer. Very good. Let’s move on to the next question

Directory service -

Which of the following describes a directory service
take a moment read the responses carefully
and then put your choice in the chat.
Wow, great we've got a lot of responses.
and the majority are for Choice D
a network service that stores all user account
information on a centralized database and
that is the correct choice.
Take a look at response A, a technology service that allows
a user to authenticate once then passes over to
multiple other services. What is that describing?
Single layer Authentication?
Single sign-on - SSO - right response;
B, a protocol that can be implemented
as special types of OAUTH flows with precisely
defined token fields. Anybody know what that is?
So what's being described there
is Open ID Connect.
and response C a data format service
based on XML that is used to exchange user
information between a client and a service
and this is simply an XML web service.
So again the correct answer D Choice D a
network service that stores all user account
information on a centralized database. Very good, let’s move on to the
next question.

Document workflow -

You are helping Implement
a document workflow system
and need each document to be legally traceable

to its creator using your corporate PKI system.
Which of the following solutions
would best provide this form of
non-repudiation at the file level.
Take a moment put your choices in the chat.
Got some choices in there all
right and it looks like most are.…
In fact all of them are for response B document
digital signatures this is the correct response.
document encryption does
not provide non-repudiation
S/MIME encryption, secure multi-purpose
internet mail extensions. So this is a
widely accepted and used protocol for sending
it digitally signed and encrypted messages,
so not really involved with
non-repudiation at the file level.

And then the last Choice document hashing
is incorrect as well. Why would that be?
What is the hash used for?
So if we do some type of hashing, what
we're really trying to do is…
Let's check the chat

We've got some responses in would just
be able to tell if the document has changed;
exactly does not prove who it belongs to correct
so what we're doing is trying to ensure that the
original data has been preserved. Very good everybody is doing very well.
Let's go on to the next question - 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?
So we have several responses in the chat:
and they are:
a couple for A, three for B, so the correct answer here is Choice B and
that is a
time-based one-time password code generated by an
authentication system. This is the correct response.
In the First Response TGT this involves Kerberos
authentication and we're talking about ticket
granting tickets, so that's user authentication
token issued by the key distribution center
that is used to request access tokens
from the ticket granting service.

For specific resources or
systems joined to the domain;
and then response C short message service - I think
we all know what that is - yeah why is that wrong.

I'm sure you send and receive these things all the
time; it's not it's not a text message yeah exactly
so SMS involves settings text messages so no and
certificate or authority certificate authority.
A CA is used or responsible for creation and
management of digital certificates in public
key infrastructure. So the best answer the one that
is correct here is time-based one-time password.

All right let's go on to the next.

Geotagging - Which of the following
is the best example of geotagging?
Take a moment look at the responses
you put your choice in the chat.
We have some responses coming in we'll
wait just a few seconds let's see
if we can get some more responses.
So we have some responses in the chat
and it looks like they are for Choice A - a user takes a photo that gets
GPS coordinates embedded into
It. This is the correct answer.

If we look at response B someone can locate
a person's location in real time by tracking
the coordinates of their mobile device so
what does that describe? What do we call that?
I don't see any responses; that describes geolocation.
Choice C - a device that can report its location
very accurately while outdoors. What is that?
What does that describe?
Everybody some responses. Yeah, GPS, that's correct - global positioning
system
and in the last response a storefront can send
push notifications when you are driving past it.

What do we call that? What is that an example of?
A response in the chat - NFC. Definitely.
And RFID yeah.
and so it's one of those Geo names.
Anybody want to take a guess?
So Choice D is referring to geofencing
and it's a location-based service and as you've
mentioned yes it can use GPS Wi-Fi cellular RFID
to create a boundary around a real geographic area
and then when somebody enters or exits
this boundary it can trigger an
event such as a push notification. Let's go to the next question
IdP: What does an identity provider
do in a federated network?
Take a look at the responses
put your choice in the chat.
We have several responses.
and it looks like they're all for Choice C.

Stores identity information about all
the objects in a particular network
including users groups servers
client computers and printers.

So Choice C is actually referring to
a directory service; it's all inclusive
so we're going to obviously eliminate Choice
C. That leaves A, B and D. Let's try this again.
And we have a few responses in the chat.

Let's see what you're thinking. Hey, and one vote for D. So the correct
answer here is A
an identity provider holds user account
information and performs authentication.

Choice B stores metadata data about when
files were created, accessed and modified.
so this is response B stores metadata about
when files were created accessed and modified
and metadata is created when you basically create
documents or files the information is included now
there are tools that you can use to access and
edit metadata such as metadata++ or EX IF
tool. Finally response D securely holds
the key used to encrypt network drive contents.
This is describing data encryption
key encrypted hard drives utilize
two encrypted keys on the device to control
the locking and unlocking of data on a drive.

These encryption keys are the data
encryption key and the authentication key.
The data encryption key is the key used to
encrypt all of the data on the drive.

Let's go on to the next question.

Microsoft active directory domain services -
Microsoft active directory domain services
use the _____ Authentication Protocol.
So this is going to be a straight up
knowledge-based question. What do you think?
You have responses coming in
and looks like everybody is choosing
D Kerberos and that is correct.

Response A - security assertion markup
language XML standard to designed
or designed to allow systems to exchange
authentication and authorization information,
radius remote authentication, dial-in user service,
networking protocol that provides centralized

authentication authorization and accounting for what we call AAA management for users who connect and use a network service. And 802.1X - this is response C - common Authentication Protocol that controls who gains access to a wired or wireless network by requiring the client to authenticate

against a central authentication database.
All right, doing good. Next question.

Multifactor Authentication - Which of the following terms most closely relates to multi-factor authentication. Take a moment and let's see what you're thinking.

We have several responses in the chat:
It looks like everybody's chosen response - a token key - and that is the correct response.
SSO single sign-on that is not what we're talking about; PAP - what is pap?
Is it Password Authentication Protocol?
Yes it is and what's the problem with PAP?
It's not necessarily multi-factor and when we use PAP the big
problem is that information is sent in plain text so kind of really cool and response D - HSM - is also incorrect; HSM is a Hardware Security Module so that's not correct.

What is the difference between HSM and TPM?
What is a TPM?
We have a response.
Trusted platform module - great. So TPMS are typically chips included in the laptop and they can you know work to
provide full disk encryption.

A Hardware security module is either removable or an external device that can generate store and manage RSA Keys so I guess the noteworthy difference between the two is that again HSMS are removable or external and TPMS aren't embedded into the device.

Let's go on to the next question:

On premises to cloud companies are starting to shift from using on-premises authorization solutions to public cloud provider authorization services solutions.
How might the change in processes be depicted? Take a moment and carefully read through these choices.
And then put your choice in the chat.
So two for D, 1 for C and

the correct Choice here is D.
Many organizations originally used lightweight
directory access protocol technologies
but are now using some type of federation
technology and that is the correct response.

So on-premises authorization refers to a system
where authentication and authorization services are hosted locally within the organization's
infrastructure cloud-based authorization
services are delivered from the cloud and
do not require as many resources as an
on-premises multi-factor authentication
surface all right so response A
- not correct; Response B administration of accounts
and devices change from being decentralized to
centralized not the best answer businesses start
using bold disk encryption with cloud-based
virtual machines instead of on-premises; virtual machines again not the best answer.