The topic for this evening
is part two of authentication
controls and let's start with the first question:

Password Authentication Protocol - Which
of the following is true regarding PAP?
Okay several responses in the chat
and they're all looks like it looks like
they're all for response C; it relies on
plain text password exchange and yes as we
discussed in the first part it absolutely does
It was developed as a means of
authenticating users over a Remote Link
- possibly but not the best answer. It
guards against replay attacks no and response
D it is an encrypted tunnel that passes a
password from one port to another - it is not.
In fact it is very weak and because of its use of
plain text. Let’s go on to the next question
proposed method a lead developer and apple
technology has proposed an authentication
mechanism to implement in their new smart
watches instead of using a fingerprint scanner
the idea of this authentication mechanism is
for the smart watch to recognize if the user
is allowed or not solely by their distinctive
walking movements what type of authentication
method is this developer proposing? Okay
we already have lots of responses here
and they are perceived and that's
that is correct - gait analysis.

Somebody's gait refers to how they walk so that
one was I think pretty easy um it is obviously not
involved with any kind of swiping patterns
or RFID or Biometrics although gait analysis.
Your gait, I suppose, could be considered biometric
but the best answer here is gait analysis.

Next question -

Security assertion markup language tokens possess
what kind of data after being granted access?
That's look at the responses
and put your choice in the chat.
0kay let's see what you're thinking.
So we have a vote for C, B, and
A kind of hitting all around it.

So the correct Choice here is D - responds to clean
data security assertion markup language is an XML
standard designed to allow systems to exchange
authentication and authorization information
this is often used with identity Federation and

claims-based authentication so claim data is the
correct answer biometric data is incorrect pkc
data this is response B public key cryptography
that's a cryptographic algorithm and
crypto system component implemented
widely PKC facilitates confidentiality data
Integrity authentication and non-repudiation
it's also a digital signature algorithm component
and used to authenticate a private Key verifiable
by anyone with authorized public key access
and of course we're talking about validating
messages between origin and sender okay
plain text Data no we were talking about
security assertion markup language; plain text is
incorrect okay let's go on to the next question.

SNMPv3 hashing algorithm - SNMPv3 authentication allows the
use of which hashing algorithm below?
Your choices are MD5 hashing; SHA; Options A and B incorrect; or None of
the options are correct.

Options A and B being correct or
dD none of the options are correct
Okay so we have some responses coming in
and let's see what you're thinking
today's favorite Choice a vote
for d a vote for a a vote for C
and in fact the correct answer is Choice
C options A and B are correct so md5
secure hash algorithm these are both used by SNMP
version three um if you need greater security
than you can use data encryption standard
okay so G is incorrect and either A or B
by themselves is incorrect options A and B
all right let's move to the next question
Which of the following is not true regarding
SNMP version 3. take a moment look at the response
and make your choice.

Okay so we have a single response okay
there's another one let's get a few more.
okay let's see what everybody's thinking we
have votes perceived Choice C and Choice C
SNMP version 3 is a network traffic monitoring is
the correct choice this is one of those not type
question which of the following is not true both
A and B are true indeed okay. So what is it about
Choice C that makes it the correct answer?

Okay so simple Network management protocol
is a protocol used in network monitoring
but this response says network traffic
monitor and that tends to lead more to

um land analyzers packet snippers okay so it's
it's too specific and it's describing something
that is more Associated closely associated with
package making okay SNMP3 is a network monitor.

Okay let's move to the next question.

SSH passphrase - Once the sys admin configured
the Linux file server to allow SSH key based authentication some users
began complaining
that their client machines are asking them
for when logging in causing key based
Authentication. What is most likely the problem?
Okay read the responses carefully
and then make your choice in the chat.

Okay so we've got some responses coming in. As you look at the responses
think about
one that you can fairly quickly eliminate.
Okay so there must be a lot
of thinking going on out there.
Let's see what we have in
the chat we have a vote for B
Okay and not another you can eliminate deep. okay one of the responses
that sticks out is
is wrong in my mind is response C, the SSH
client used the wrong SSH client options.
So if you're using the ssh-Keygen
okay which is a command line utility
and you look at some of the parameters
like Dash T, their type of key to create,
or Dash C to put a comment, this
is kind of a silly answer okay so an option
perhaps it can lead to
unexpected behavior but typically
it's not going to be a reliable
answer certainly not a good answer
so the correct answer here is response A - the
SSH public slash private key pair was likely
generated using a passphrase by the client. So if you do that you're
going to get prompted if
you don't if you leave it blank then you're not
going to get prompted get prompted for a passphrase.

The SSH server's private key did not
match the user's private key now someone said
eliminate deep and that's also a good one to
eliminate so I would say that's responses C and D
were the ones that could most easily be eliminated. What’s wrong with
response D?
Is a server going to contain the private key?

Can't mismatch so the user maintains their
private key servers typically have the public key.

This SSH server was likely configured
by the sysadmin to require passphrases and no
okay all right so again public private key
pair was likely generated using a passphrase.
That's what we'll do it okay;
let's move on to the next question.
SSH public and private keys - Your
organization's network administrator
is configuring a Linux server's SSH
Authentication to allow key-based authentication.
This setup requires that the private
key is blank and the public key is blank.
What do you think? you just kind of
touched on this in the last question.
So we have some responses coming in and
responses For C and one for D. The correct response is C. The private key
is kept with the user and the public key is on
the UNIX server and this makes sense and
this is how it works okay.
So private key kept with the user; public key kept with the user - No,
Private key with LINUX host; Public key kept with the LINUX host - No.
D - user no private key; public key kept with the LINUX host. . Check
Kept with Linus Host., Public key kept wait heh photo. Choice C -
So, the correct answer is Choice C - the private key is
kept with the user the public key is on the server.

Let's move to the next question.

This one involves security policy. A user logs
into their account from their home computer in
California; one hour later a login attempt is
made from their personal laptop in Virginia
but it is denied an alert is sent to the system
administrator and the account is disabled
What security policy is most likely
being utilized in this situation?
Okay we have a couple of responses.
Again when you're looking at this try to
think about which responses can be eliminated
or which don't make sense.

It's always helpful when you
can narrow down your choices.
So it looks like we're holding it
two responses let's see where we are.
Both votes for D - impossible travel
time policy is the correct answer.
Time of day policy restricts access to certain
resources to the time of day. No, what’s
obviously strange about this is that there's a
three hour time difference between Virginia and
California so if one hour later a login attempt is
made from Virginia right that doesn't make sense.

Firewall policy - that is not really
a reasonable option.
Location-based policy is a security
policy that restricts access to certain

resources based on the location of the user
and so as an example a company May restrict
access to files or applications based
on the network location of a user okay
The main benefit of setting up
location-based policies is to avoid data leakage.
Once you have defined trusted Network locations
no one can access resources from different say
network location or device okay impossible travel
time policy is the best and correct answer here.

On to the next question:

Smart card and key fob: Okay so 50/50 chance here
of getting this correct. Using a smart card
and key fob counts as multi-factor authentication.
Is this a true statement or a false statement?
Okay, I'm going to wait till we get
enough responses in the chat and
we've got a few. Okay, all right. Let's see what everyone's thinking.
Okay so it looks like yeah everybody's
thinking false. Okay, yeah, this is false.
Smart cards and key fobs
Will…you tell me why is it false.
Something you have - correct they are both
something you have and that does not count
as multi-factor authentication. So, very good, everyone. Let's go on to
the next question.

Something you do - All of the following is
true regarding the authentication attribute
"something you do" except which of the following?

Okay so one of these responses
is not true regarding the authentication
attribute "something you do."
We've got responses coming in
let's see what everyone's thinking.
Okay, so C, B and D.
Okay so is a user's typing speed and or a
pattern of user inputs - is that something you do?
Yes, yes. Okay.
This method is subject to higher
error rates. Is that a true statement?
I think so.
Okay may I ask why?
Why do you think that?
I don't know.
I'm thinking practically so if I'm typing

speed and pattern is like something you do that
can change.
Yes, it can, yeah because as humans we
you know that can change based on emotion, based
on physical, based on so many different things so
yeah it can sure when you're in a hurry you know
your typing speed may be faster if they're just
trying to get something done and get out of it so
yes the point very much is that things can change.
Response C - how one holds their smartphone
I mean that that's almost silly because
there's so many different ways right okay.
Yes, human error. Too many factors absolutely.
So the best choice of all of these here is
response D - this factor is practical to use
as a primary way of authentication and it's not
because something you do with the way we do things
is subject to change for many many different
reasons so it's just not reliable.
Okay, good.

Next question - type of model - The _____
model is used to allocate labels to objects

and subjects for access control clearances. Okay,
take a look at these and let's see what you think.

Okay let's see what everyone's thinking.
Indeed, yep, very good. We touched on this in part one.

That this is more related to
mandatory access control and again the text that she will be receiving
makes a point of mentioning this
so not discretionary access control. Discretionary access control
uses what you might call access control
Entities. The other term you're going to hear is
DACL - discretionary Access Control List -
and one of the more common examples of that is
as a particular user and even on your own
system you can right click on a resource on your
computer and bring up the properties dialog on a
Windows system and then you can actually see you
know in the I believe it's the security tab who
has access to one so system administrator your
user account which may be an administrator
account as well and that's a common example
for discretionary access using an access control
list. We've talked about role-based and
attribute-based and neither of those is correct so
mandatory access control is the correct response.

Okay and let's move to the next question:

Type of restriction - What type

of authentication restriction would
allow an employee to log into an internet facing
employee web portal from the U.S but not from Asia?
Which type of authentication restriction.

We have lots of responses on this one because
it's pretty obvious we're talking about
geolocation restrictions.
Okay and the last question -
Type of security control - A museum already has
security guards and security cameras near their
exhibit and they just recently upgraded their
security controls by installing light fixtures
that point to the exhibit and towards the
Crowd. Which type of security control is this?
Okay quite a few responses in the chat; let's see what you're thinking.
We have votes for C looks like the majority
proceed which is deterrent and this is the correct
choice for this question.
Detective controls are
security measures implemented by an organization
to detect unauthorized activity um or some type
of security incident in general and send alerts to
concerned individuals.
Would that also include unauthorized access?
Yes, so for example,
I mean actually there are several examples so
one of those could be the activation of say a door
Alarm, okay, which is physical control right because
if you don't have authorization to open the door
then you don't have what it takes and we're
going to hear an alarm the implementation of
an intrusion detection system.
Okay that one's
kind of obvious and that's a technical control.
If you're doing an an audit in internal
audit and you find that a user has
excessive access rights for example so there's
another type which is an administrative control.
So those are detective controls compensating
security controls. First of all very
widely and and they vary based upon what a
particular need is being met so based
on the organization's needs and in particular
um and one of those could be if you
if there's an attack okay and let's say that you
know data was destroyed do using a good
back backup a good backup after an attack that
deleted the data that would be an example of a
compensating control and then operational
security controls are primary
implemented and executed by people as opposed to
Systems. They're typically put in place
to improve the security of a particular system

or group of systems and supplement the security
of an organization in a manner which in which
both physical and technical elements are utilized.
Let's see, so operational security controls
include for example an overarching security policy, certainly acceptable use policy or
security awareness training policy and these

are examples of operational controls but in the
question the correct answer is C deterrent.

All right and that finishes up authentication controls topic area.