9-23-2021

Artificial Intelligence in Cyber Security

University of Maine Artificial Intelligence Initiative

1865 THE UNIVERSITY OF MAINE

UMaine Artificial Intelligence: Artificial Intelligence in Cyber Security

Date: September 23, 2021
Run Time: 00:59:39
https://youtu.be/TgUiJVjbZF8

This webinar marks the first in the Fall 2021 series.

UMaine AI draws top talent and leverages a distinctive set of capabilities from the University of Maine and other collaborating institutions from across Maine and beyond, while it also recruits world-class talent from across the nation and the world. It is centered at the University of Maine, leveraging the university's strengths across disciplines, including computing and information sciences, engineering, health and life sciences, business, education, social sciences, and more.

Transcript is machine generated, unedited, in English.

00:00
good morning good afternoon and good
00:02
evening to all our advertisers from
00:04
various parts of the world my name is
00:06
ali abedi serving aishwarpali as region
00:09
1 assistant area chair and associate
00:11
vice president for research at the
00:13
university of maine before we start our
00:15
webinar today i would like to thank our
00:18
ieee colleagues in silicon valley and
00:20
boston sections i truly regen one uh
00:24
usa ieee india and actually china for
00:27
promoting this event which yielded over
00:30

321 registrations
00:33
a special thanks to israeli
00:34
communications society and computer
00:36
society's joint chapter here in maine as
00:39
well as university of maine artificial
00:41
intelligence initiative for planning and
00:44
hosting this event
00:45
please make sure to enter your questions
00:48
in the qr may box and we'll answer them
00:50
at the end of the presentations
00:53
it is now my great pleasure to introduce
00:56
our moderator
00:57
dr julia upton associate professor of
01:00
mathematics at austin university voice
01:03
chair of i triple e main section and
01:05
chair of i triple e main communications
01:07
and computer society joint chapter to
01:10
introduce our speakers julia
01:13
thank you ali
01:15
uh i would like to welcome everyone on
01:17
behalf of ieee main section and the join
01:21
computer society communication society
01:23
chapter thank you for joining us
01:26
uh we
01:28
will we have four speakers for you today

01:30
um and our first speaker is um
01:34
bill layer
01:36
uh rear admiral retired bill layer
01:39
served in the united states navy for 33
01:42
years in intelligence and cryptological
01:44
warfare
01:45
his career spanned the cold war desert
01:48
storm and the global war on terrorism
01:51
his minion navy assignments included the
01:53
deputy director for information
01:55
technology and communications a
01:57
commander naval security group command
02:00
for meade maryland
02:02
and at the national security agency
02:04
where he served as a senior operations
02:06
officer in the national security
02:09
operations center
02:10
he served as the commanding officer
02:13
naval information operations command in
02:15
norfolk virginia where he was selected
02:18
to flag rank in 2008
02:21
as a flag officer he focused on cyber
02:24
warfare serving as the director of
02:26
information operations on the staff of
02:28

the chief of naval operations
02:31
and as the deputy commander for u.s
02:33
fleet cyber command u.s 10th fleet and
02:36
the director of warfare integration for
02:39
information dominance on the navy staff
02:41
in the pentagon
02:43
he retired from the navy in 2014 and
02:46
worked in the defense industry focusing
02:48
on developing cyber capabilities for the
02:51
military
02:52
rare admiral lehr is a native of maine
02:55
and has a bachelor of arts degree in
02:57
political science from the university of
02:59
southern maine and a master of arts and
03:02
national security and strategic studies
03:04
from the u.s naval war college
03:07
so let's welcome our first speaker for
03:09
our artificial intelligence and cyber
03:11
security webinar today
03:14
admiral
03:16
your floor
03:19
thank you very much dr upton uh it's uh
03:22
my honor to be uh
03:24
to be part of the panel today and and
03:27
the first thing that i will do i always

03:28
get a little nervous when uh
03:31
i did in engineering intense uh
03:33
environments that i want to emphasize my
03:35
my science was political science and and
03:38
today i think you'll see
03:40
probably a lot more along the policy
03:42
implications
03:43
uh that we have in cyber security and
03:47
and uh
03:48
and
03:49
what that means and i think it tees up
03:51
some of the other panelists so i've got
03:53
a pretty short presentation and uh
03:58
you know it kind of goes along with with
04:00
some thinking that i've been doing of
04:01
late and you know how are we going to
04:04
cope with
04:05
uh
04:06
cyber security over the next couple of
04:08
decades and
04:10
you know for all that's been said and
04:12
written about the end of uh
04:15
the war on terrorism uh in afghanistan
04:18
uh
04:19

you know we were there for a reason we
04:21
were there because the united states was
04:23
attacked and
04:24
and we spent an awful lot of money in
04:26
iraq and afghanistan over the last two
04:29
decades and a lot of us will remember
04:32
exactly where we were uh 20 years ago uh
04:36
in remembrance ceremonies
04:38
this uh
04:39
this saturday
04:41
but but
04:42
thinking ahead
04:44
you know coming out of of where the
04:46
nation has been
04:48
you know i i
04:49
think i come to the conclusion that
04:51
we're very unlikely to have another
04:54
large
04:55
uh conflict that will commit what we did
04:57
over the last 20 years
04:59
and
05:01
if that's only a guess
05:03
prognosticators are horribly bad at
05:05
predicting predicting war but
05:08
what does that mean for for cyber and

05:11
cyber security in particular and
05:14
you know we all know if you're looking
05:16
in this this kind of area that the pace
05:19
and the complexity of global cyber
05:21
attacks in the last
05:23
you know 25 years has
05:25
uh changed significantly
05:28
now from my bio you you'll get pretty
05:30
quickly that i was the part of the navy
05:32
in the part of the navy that was
05:34
associated with national security agency
05:36
in fort me i spent you know most of the
05:39
last uh 15 years of my career in that
05:42
environment
05:43
and you know through that i saw you know
05:45
that really
05:47
you know how we use cyber uh as part of
05:50
espionage and
05:52
and you know as time went on and in
05:55
being involved in the stand up of you
05:58
know the navy cyber service fleet soccer
06:00
command and 10th fleet
06:02
you know there's really that that
06:04
spectrum that espionage where it
06:06

probably started in all nations
06:09
there's certainly cyber crime that
06:11
affects us all and and then you know
06:13
what i focus on what i think about is is
06:16
what cyber means for warfare
06:19
and you know for warfare it's seen the
06:21
same kind of uh
06:24
evolution that that we've seen in
06:26
protecting businesses and protecting
06:28
everything from from kitty scripts to
06:30
fishing to zero uh day exploits and and
06:33
lastly with the solar winds
06:36
uh attack uh you know a very complex
06:39
supply chain
06:41
uh exploit and and the costs are
06:44
are mind-boggling really if you go back
06:46
to
06:47
you know what was clearly a politically
06:49
motivated uh
06:51
you know attack in 2007 in estonia you
06:54
know it's really hard to pinpoint what
06:55
the costs were and you know some loss to
06:58
banking revenue is estimated around a
07:01
million dollars
07:02
you go forward you know you know eight

07:05
years uh to what happened in in saudi
07:07
arabia again probably a politically
07:10
motivated attack and retribution for
07:13
uh for stuxnet you know 35 000 computers
07:17
another 7 500 servers destroyed
07:20
and and it put the saudi arabia oil
07:23
economy at risk
07:24
[Music]
07:25
uh
07:26
a couple years later with not petya
07:28
again you know computers destroyed more
07:30
servers destroyed billions lost and one
07:32
of the interesting things about not
07:34
petya
07:35
is that a
07:37
united states insurance
07:40
carrier declared that it was an act of
07:42
war and and has refused to to pay on
07:45
insurance so
07:47
these kind of uh
07:49
challenges are in the national security
07:51
realm for all that we do with sober for
07:53
solar cyber security
07:55
and
07:56

lastly within within the year you know
07:59
solar winds which is
08:00
an incredibly complex supply chain
08:03
attack
08:04
and
08:05
what i think has
08:07
caused me
08:08
you know thought and worry as as it go
08:10
is the
08:12
you know almost the sense of
08:14
helplessness and and where do you start
08:17
to unravel this that i heard from cyber
08:19
security experts and people who are
08:22
trying to put together the solar winds
08:24
attack
08:25
and you know the study that was done by
08:28
you know presidential panel uh 2016 that
08:31
you know these costs you know amount
08:33
between you know seven
08:35
fifty seven and a hundred and uh nine
08:37
billion
08:38
uh it's incredible amount of money
08:40
that's lost to the economy
08:43
and so
08:44
if we do have this situation where we

08:47
are
08:48
you know looking for
08:51
you know what cyber security looks like
08:53
in a con
08:54
uh outside of a conflict you know we've
08:57
got to think about where we are with
08:59
deterrence and
09:00
you know we know that there's a close
09:02
relationship between criminal hackers
09:04
and nation-state
09:05
attackers that you know an example of
09:08
that is in in many pieces of
09:11
uh malware you can see that it checks
09:13
for the presence of a cyrillic keyboard
09:16
uh so it doesn't land on a russian
09:19
target
09:20
the united states has tried you know
09:22
criminal indictments but they're
09:24
incredibly difficult to act on
09:27
uh there are often conflicting roles
09:29
between espionage and cyber security uh
09:32
we saw that in the obama administration
09:35
with you know agreements with president
09:37
z that we kind of left that all off the
09:39

table because we we do want to collect
09:42
intelligence
09:43
but with with all deterrence there's a
09:47
necessity to back
09:48
up uh
09:50
what we're trying to
09:51
uh prevent with some actions
09:54
and i think we've seen a different look
09:56
with with president biden and
09:59
in the warning to russia
10:01
with ppd
10:02
21 uh warning but the the problem with
10:05
ppd21 it's incredibly broad it's
10:08
everything
10:09
and if everything is important how are
10:11
we going to really make that enforceable
10:14
and you know
10:15
followed by that did it have an effect
10:17
is the our evil uh kind of disappearing
10:20
from the uh
10:23
uh
10:24
from the you know environment for a
10:26
while is that connected yeah i don't i
10:28
think it's too early to know
10:30
but but also in a more promising thing

10:33
you know shortly after the putin biden
10:36
uh summit
10:37
there was a microsoft uh exchange server
10:40
attack that was uh attributed to china
10:43
and in both nato and the eu join the
10:46
united states and in condemning that so
10:49
there's got to be these kind of of
10:52
things uh happening in this environment
10:54
where we're
10:56
using all the tools of national security
10:58
to be able to do that and and lastly you
11:01
know i think it's you know we're gonna
11:02
have to rethink cyber security over the
11:05
long haul and what
11:07
you know it could mean over the next
11:08
couple of decades and
11:10
and you know security has to be more by
11:12
default it you turn it on it's going to
11:14
be secure that's two-factor
11:16
authentication digital identities
11:19
for most things that we do online i know
11:21
that's controversial there are some
11:23
machine learning ai things with fileless
11:26
malware detection you know a company
11:28

called blue vector
11:29
you know has advanced threat detection
11:31
that it learns pretty quickly what a
11:34
normal environment looks like and is
11:37
very quick to uh
11:39
to
11:42
identify those things that are abnormal
11:44
and and likely malware in an environment
11:47
and and work with uh traditional
11:49
cybersecurity systems zero trust it's a
11:52
huge thing
11:54
within the federal government and dod uh
11:56
i think that has to be how we think
11:59
about
12:00
uh
12:00
systems going forward
12:02
um
12:04
i have to make it more difficult to
12:05
remove information from a system and in
12:09
that area it's things you know data loss
12:12
prevention it looks again
12:13
with machine learning tools to to do
12:16
behavioral analysis in real time to say
12:19
this this is something that you don't
12:21
have permission to do

12:23
uh and one of the things we learned from
12:25
uh solar winds is you know policy
12:28
enforcement which we've generally talked
12:30
about in terms of
12:33
how
12:34
it applies to individuals but policy
12:36
enforcement also has to apply
12:39
to uh software authorities and if you
12:41
thought a little bit about the solarwind
12:43
product that was being used to
12:46
distribute patches uh what uh what can
12:49
your software access and and and what
12:51
should it not be able to access so
12:54
so uh bringing uh that thinking that
12:56
we've done uh in a human sense to a
12:58
machine sense as well
13:00
and and the last thought is it you know
13:03
comes from an article that was you know
13:05
published in foreign affairs about a
13:07
year ago by general nakasone who's the
13:09
commander for united states cyber
13:11
command and
13:13
is defending ford
13:15
in a traditional military sense
13:16

defending forward is something that
13:18
we've always thought about you if you
13:20
wait for someone to attack you you're
13:22
probably going to lose 100 of the time
13:25
i've long argued that that cyber is no
13:28
different than defending an air base or
13:30
or defending against the submarine and
13:33
general nakasoni basically says we have
13:35
to defend beyond the firmament of the
13:38
nation
13:39
and that leads to you know i think
13:41
really how we think about cyber defense
13:43
how we leverage the
13:45
practices and the authorities of our
13:47
allies to be able to do that so i think
13:50
that's about my time and i will turn it
13:52
back over to julian
13:56
thank you very much admiral
14:00
if you have any questions for the
14:01
admiral please type them into the q a
14:04
portion and we'll address them at the
14:06
end
14:07
our second speaker
14:09
is scott mcgann
14:12
scott mcgonn has been a special agent

14:14
with the federal bureau of
14:15
investigations for 25 years
14:18
during his time with the fbi he has
14:20
investigated white-collar crime the
14:22
russian and italian mafias cyber crime
14:25
counter-terrorism and espionage matters
14:29
special agent magan is an fbi certified
14:31
firearms instructor a member of the
14:34
fbi's evidence response team a certified
14:37
police instructor an fbi agent faculty
14:41
member teaching fbi coursework to police
14:43
agencies domestically and abroad
14:46
he received his undergraduate degree
14:48
from the university of massachusetts at
14:50
amherst
14:52
his master of science in criminal
14:54
justice from the university of
14:55
massachusetts at lowell and his mba from
14:59
bentley university
15:00
he currently teaches issues in cyber
15:03
crime and cyber security as an adjunct
15:06
faculty member at young massachusetts
15:08
law
15:09
in addition special agent ghan was
15:11

nominated for the 2018 attorney
15:14
general's award for fraud prevention
15:17
and the 2018 fbi director's award for
15:20
outstanding criminal investigation
15:23
for his involvement in an international
15:25
corporate espionage investigation
15:28
agent magang is the alpha team leader
15:30
for operation workspeed the government's
15:33
full-scale effort to secure the
15:35
development and delivery of the covit 19
15:38
vaccine it currently is also involved in
15:41
training and speaking to the private
15:43
sector
15:44
in academia about cyber threats
15:46
corporate espionage counterintelligence
15:48
matters insider threats and intellectual
15:51
property theft on the on behalf of the
15:53
fbi
15:54
well welcome special agent the floor is
15:56
yours
15:58
thank you so much dr upton uh i'm going
16:01
to talk about something that's a little
16:03
bit outside the normal realm for
16:05
engineers and and i i genuinely thank my
16:08
colleague for just introducing some of

16:10
the ideas of espionage and hacking and
16:14
all of those things that i talk a great
16:16
deal about but one of the things that
16:18
i've been involved with lately that the
16:20
american public generally doesn't get to
16:22
see
16:23
is a number of different aspects to the
16:27
whole subject of foreign influence and
16:30
what i'm referring to is that our
16:33
country has a number of different
16:34
adversaries out there in the world and
16:38
as as does every country certainly
16:41
but as part of this
16:43
there are adversaries out there nation
16:46
states that are looking to obtain our
16:49
technology when they can't develop it
16:51
themselves so as uh ieee a society of
16:54
engineers uh who are out there working
16:57
hard to develop these things we don't
16:59
want to see that idea uh that
17:02
intellectual property stolen by foreign
17:05
agents and so i want to talk a little
17:08
bit about that because the
17:10
how it used to happen in the past is not
17:12

how it happens now when we're discussing
17:14
espionage in the past we used to talk
17:17
about uh spies coming into the country
17:20
developing sources and assets and and
17:23
they would steal but now it's so much
17:25
broader than that and i want to give you
17:27
a little bit of an idea of how that has
17:30
developed
17:32
we've seen the headlines uh previously
17:34
all over the nation about
17:37
different entities uh different
17:39
countries obtaining intellectual
17:41
property whether at universities or
17:43
research associations or companies uh
17:46
obtaining this technology for their own
17:49
benefits certainly something that the
17:51
fbi in their counter intelligence
17:54
counter espionage divisions
17:56
try to work against
17:59
i i i'm just amazed that i can even show
18:02
you this slide that it's been
18:04
unclassified in years past we certainly
18:07
wouldn't talk about anything related to
18:10
counterintelligence but as you can see
18:12
here from uh this slide we have a number

18:15
of counter intelligence cases throughout
18:18
the government throughout the fbi
18:20
and the cases on technology transfer
18:24
have increased markedly over the last
18:27
two decades
18:29
i became involved with
18:31
intellectual property theft and economic
18:34
espionage in the middle of my career and
18:38
have not gotten away from it because
18:40
it's become so prevalent you can see
18:42
that cases on economic espionage and
18:45
counter proliferation of technology
18:48
has uh increased to about a third of our
18:52
total counterintelligence cases and
18:54
again from my perspective being a an fbi
18:58
agent for 26 years i have never seen the
19:02
fbi put out a slide like this previously
19:05
to the public um so this should be all
19:07
new information for you but it
19:09
highlights the importance of technology
19:12
transfer and i use that term in the
19:14
pejorative uh of technology transfer at
19:17
the fbi
19:20
uh and and what i alluded to previously
19:22

was that technology transfer is coming
19:26
in a lot of nefarious uh from a lot of
19:28
nefarious vectors it used to be just
19:31
spies coming here trying to find
19:33
information uh and bring it back to
19:35
their home country and certainly we have
19:37
that we uh that has never gone away but
19:40
we also have different uh entities
19:43
different nation states uh influencing
19:46
our government as we've heard about in
19:48
the 2016 election certainly in the 2020
19:51
elections this topic has come to the
19:54
fore but also more importantly and i
19:57
i'm in the boston area and work in
19:59
greater new england and i can tell you i
20:02
have seen non-traditional collectors at
20:04
the 12 o'clock o'clock position on this
20:06
graphic non-traditional collectors have
20:09
become
20:10
uh much more important to foreign
20:13
governments and so these non-traditional
20:16
collectors are people who are not
20:17
trained spies but they simply have
20:19
access to the information that other
20:22
governments want and for various reasons

20:24
and sometimes because of a little
20:27
intimidation they provide this
20:29
information uh from our country to their
20:32
typically their country of origin or to
20:35
other foreign governments there are a
20:38
number of different ways that foreign
20:39
governments will obtain
20:42
intellectual property information and
20:44
the ideas that engineers develop either
20:47
through hacking influence or a lot of
20:50
times through talent conversion where
20:53
they will have talent recruitment
20:55
programs and a number of comp uh
20:57
countries have this where they will
21:00
acquire information from an individual
21:03
who is a leader in that particular field
21:06
so if the field is nano technology
21:09
they will effectively co-op someone
21:12
through money cash or a number of other
21:14
methodologies uh in order to provide
21:17
that country with
21:19
information uh on nanotechnology in that
21:22
particular example
21:24
so some of the techniques are legal
21:26

certainly joint ventures are providing
21:28
money and investment into companies is
21:31
legal but oftentimes those techniques
21:34
are not
21:35
clearly transparent in what's going on
21:37
and certainly unethical at a minimum
21:41
i'll give you an example in the talent
21:43
plan uh case that i just mentioned
21:46
regarding technology uh some of you may
21:48
know he made headlines last year dr
21:51
lieber of harvard university uh was
21:54
arrested by myself and some of my
21:56
colleagues uh for making false
21:59
statements uh was the initial charge but
22:02
he was allegedly involved in a talent
22:04
program and i'll show you here an
22:06
excerpt from the affidavit for the
22:08
arrest warrant where it's highlighted
22:11
here that he was getting fifty thousand
22:13
dollars per month and an extra 150 000 a
22:17
year for living expenses and money to
22:19
develop a lab
22:20
over at the wuhan institute of
22:22
technology
22:23
uh

22:24
you can see here an extra 50 000
22:27
a month on top of a uh what i perceive
22:31
to be a generous harvard stipend uh an
22:34
annual salary uh was certainly
22:37
motivating for dr lieber when i arrested
22:39
him with my colleagues
22:41
um he was certainly not surprised to see
22:45
uh that this was something so if you are
22:47
approached as an engineer out there
22:49
developing some new technology
22:52
or someone at your uh company has been
22:56
approached uh there is a quid pro quo
22:59
expected when someone's paying you fifty
23:02
thousand dollars a month uh for the
23:04
information that's in your head
23:08
here is a traditional spy ms yay here
23:12
was at boston university uh posing as a
23:16
student she was a member of a top
23:19
military academy and directed by a
23:22
foreign government
23:23
last year we looked to arrest her but
23:26
she already skipped town
23:28
and
23:29
before she could be arrested
23:31

this young man was a medical student as
23:34
well in the boston area and
23:37
his uh activities were discovered at the
23:40
airport when 21 vials of a biological
23:43
substance were found wrapped in his sock
23:46
when he was trying to go back to his
23:48
country of origin he was arrested at
23:50
logan airport what's more interesting
23:53
about this particular case is that this
23:56
happened
23:57
30 times within a six-month period with
24:00
different individuals um so this is uh
24:04
the wholesale theft of intellectual
24:07
property in this case from our bio bio
24:10
uh pharma industry in the boston area
24:14
and as far as corporate espionage goes
24:16
here's a great case i like this case i
24:19
call it a great case because it was one
24:21
of my cases uh american superconductor
24:24
was a company here in massachusetts and
24:26
their intellectual property their low
24:28
voltage ride through solution for your
24:31
electrical engineers out there in the
24:32
audience uh was stolen by a foreign
24:35
company um and they used the traditional

24:39
uh money
24:41
uh ego assuasion and uh sexual favors uh
24:46
in order to uh get deion carabasovac
24:50
seen right here who was a serbian
24:52
national uh to flip for their particular
24:55
company so he was the insider at
24:58
american superconductor who gave the
25:00
crown jewels to a foreign competitor uh
25:04
a very interesting case which i can
25:06
usually talk about at length um it was
25:09
just made into an fbi documentary which
25:12
will be coming out this month so very
25:14
good case on economic espionage
25:20
and
25:23
intelligence operations will target
25:25
academics and researchers and recruit
25:28
uh people at various companies in our
25:31
country and will often make contact
25:35
through
25:36
professional networking sites i am not
25:38
immune from this uh here mandy which i'm
25:41
sure is her given name uh reached out to
25:44
me on linkedin as i get to the end of my
25:46
career i put up a linkedin page and it
25:48

wasn't very long before mandy wanted to
25:51
be friends uh for those of you who don't
25:53
know the us government isn't really
25:56
enamored with tick-tock but i'm sure
25:58
it's okay because you note down here
26:00
that the culture there is magical so i'm
26:02
sure it's okay to accept that uh
26:04
linkedin connection i just uh
26:06
screenshotted this as uh for my future
26:09
lectures because it was something i had
26:11
talked about in the past and here it was
26:14
uh actually happened to me but not only
26:17
that but more interestingly is my
26:20
uh my two sons who are young males in
26:24
their early twenties were approached by
26:27
asian individuals attractive females on
26:30
their social media right after i ignored
26:34
this uh
26:35
this connection request and certainly um
26:38
there they don't mind clicking on
26:40
connections with attractive uh females
26:42
from other countries but they came to me
26:45
having had the counter intelligence
26:47
lecture that i give my children uh being
26:50
sons of an fbi agent and i said yeah

26:53
that's because of me thanks and uh they
26:55
ignored those connections so this does
26:58
happen and it's something you're
27:01
probably not very familiar with or
27:03
haven't heard much of but it does happen
27:06
all over our country every day happens
27:09
to people in the ieee as well
27:13
um and quickly what can we do to protect
27:16
ourselves i tell everybody call your
27:18
local fbi and partner with them uh
27:22
corporations who are out there can get
27:23
better lectures uh than this brief
27:26
introduction and can get information on
27:29
risks and conflicts of interest we speak
27:32
to boards we speak to executives we talk
27:35
to administrators at research
27:37
institutions all over the country so get
27:40
with your local fbi and ask for their
27:43
private sector coordinator there's one
27:46
in every fbi office and they will be
27:49
able to assist you in protecting
27:52
yourselves and certainly they can hook
27:54
you up with the cyber uh crime squad i
27:57
worked in computer hacking for a dozen
27:59

years i was on the cyber crime squad and
28:02
even though i left it to work other
28:03
matters i never got away from cyber
28:05
crime so i still go out there and
28:07
lecture on business email compromise and
28:10
ransomware and hacking and
28:12
uh dark web and all of these other
28:15
subjects but i wanted to introduce you
28:17
to the subject of uh foreign influence
28:20
and espionage um something you probably
28:23
don't get a lot of at your regular uh
28:25
meetings and uh i thank you
28:31
thank you very much scott um
28:34
if you have any questions please post
28:37
them in q a
28:39
and it's my pleasure to introduce our
28:41
next speaker
28:44
dr dan shoemaker
28:46
dr dan schumacher received a doctorate
28:49
from the university of michigan in 1978
28:52
he taught at michigan state university
28:54
and then moved to the directorship of
28:56
the information systems function for the
28:58
medical schools at msu
29:00
he held a joint teaching at department

29:02
chair positions at mercy college of
29:04
detroit
29:05
when mercy was consolidated with the
29:07
university of detroit in 1990 he moved
29:09
to the business school to chair their
29:11
department of computer information
29:13
systems
29:14
he attended the organizational rollout
29:16
of the discipline of software
29:18
engineering at the carnegie mellon
29:20
university software engineering
29:21
institute
29:23
in the fall of 1987 and he was already
29:26
teaching an sei based software
29:29
engineering curriculum which he
29:30
established as a separate degree program
29:32
to the mba within the
29:35
udm college of business administration
29:38
dr showmaker specific areas of
29:40
scholarship publication and teaching
29:42
were the process-based stages of the
29:44
waterfall specifications sqa and
29:47
acceptance sustainment he was also a
29:50
primary consultant in the detroit area
29:52

on the cmm cmmi
29:55
dr schumacher's transition into cyber
29:57
security came as a result of the audit
30:00
and compliance elements of that body of
30:02
knowledge as well as the long
30:04
established
30:05
sqa scm elements of their curriculum
30:09
they were designated the 39th center of
30:11
academic excellence by the nsa at west
30:14
point in 2004 and they have tried to
30:17
stay on the leading edge in the
30:18
architectural aspects of cyber security
30:20
systems design and implementation as
30:22
well as software assurance
30:25
as a result of dr schumacher's
30:27
associations with nsa and his interest
30:30
in software assurance he participated in
30:33
the earliest meetings of the software
30:34
assurance initiative
30:36
he was one of the three authors of the
30:38
common body of knowledge to produce
30:40
acquire and sustain software and he
30:42
chaired the workforce education and
30:44
training committee from 2007 to 2010.
30:48
he was chair of workforce training and

30:50
education for the software assurance
30:52
initiative at dhs
30:54
and he was subject matter expert for uh
30:57
you know for nice
30:59
security provision
31:01
dr shoemaker was also a subject matter
31:03
expert
31:04
for the
31:06
human security 2017.
31:09
he also published frequently in the
31:11
build security and website
31:13
this exposure led to a grant to develop
31:16
curricula for software assurance and the
31:18
founding of the center for cyber
31:19
security where he currently resides the
31:22
center is a free-standing academic unit
31:24
in the college of liberal arts which is
31:26
the administrative locus for research
31:29
centers within udm
31:31
dr shoemaker's final significant grant
31:34
was from the department of defense to
31:36
develop a curriculum and teaching and
31:38
course materials for secure acquisition
31:41
in conjunction with the institute for
31:42

defense analysis and the national
31:44
defense university
31:46
a book was subsequently published by crc
31:49
press
31:52
welcome dr shoemaker
31:58
okay where am i
32:02
um
32:04
i can hear me i can't see me
32:07
we can see you we can hear you we can
32:09
see you and hear you okay well then i'm
32:12
here i
32:12
am um
32:15
greetings everybody
32:17
i uh
32:18
you know i when i do these things i try
32:20
to think about something that the group
32:22
would find interesting
32:24
so uh what i came up with
32:26
uh was pretty well covered by the first
32:28
two people and so i guess i'll just say
32:31
next speaker
32:33
um
32:34
i let me
32:36
get my
32:38
slides up

32:51
um
32:53
when i do these
32:54
ieee visits i
32:56
try to come up with something that is
32:59
sort of fits with the
33:01
the group i'm talking to
33:03
um
33:04
most of the time i end up talking about
33:06
supply chain risk management which is my
33:09
alleged area of expertise
33:11
um and um i
33:14
thanks to the solarwinds people i i find
33:16
myself talking to a lot of a lot of
33:18
folks about that but
33:20
um since this was ai
33:22
i kind of
33:24
uh you know sort of
33:27
tried to come up with something that
33:28
would be at least fit within that kind
33:30
of context and uh what i came up with
33:33
was uh
33:34
some work i did back in
33:36
2008 uh was it was published basically
33:39
in a book
33:40

um
33:41
uh uh it kind of on the topic of cyber
33:43
crime
33:44
um and then what do i end up doing is
33:46
following an fbi agent so you know you
33:49
can take for what i've got to say uh you
33:51
know for whatever it's worth
33:54
but it's a modest proposal and it fits
33:56
within kind of an ia context so
33:59
um
34:01
what you've seen so far in the first two
34:03
presenters uh is true
34:07
we've got a worldwide problem with cyber
34:10
crime or cyber attacks take your pick
34:13
um
34:14
microsoft did a survey that was really
34:16
eye-opening published back in december
34:19
uh about the the kind of the the cost of
34:23
of cyber attacks
34:25
uh global cost um that's not just in the
34:28
u.s
34:29
um
34:30
500
34:31
billion dollars with a b in 2015
34:35
um and kind of we worked on the problem

34:38
and
34:39
by 2020 it escalated to 2 trillion
34:43
dollars
34:46
globally
34:47
and um
34:49
by the time 2024 rolls around the
34:52
estimate is 6 trillion
34:54
so uh it looks like uh cyber crime is a
34:58
growth industry it's something that you
35:00
know i don't recommend you buy stock in
35:02
but
35:02
um and i guess it's because it's so easy
35:06
um
35:07
one of the things you might want to use
35:08
as a sense of context is
35:11
that 6 trillion is the gross national
35:13
product of england germany and france uh
35:16
you know
35:17
and so you know that's kind of a pretty
35:19
big hit
35:21
into in the global economy
35:23
um
35:24
now the reason why obviously and people
35:26
the first two presenters talked about
35:28

this at great length uh is the nature of
35:31
the internet
35:32
um
35:33
it's anonymous and it's borderless and
35:35
so how in the world do you
35:39
defend against or prosecute
35:42
some guy who is sitting somewhere you
35:44
know not where um attacking you
35:48
uh maybe from the other side of the
35:50
world
35:50
um
35:52
and um it's possible in certain
35:54
countries that if they're successful in
35:56
doing that to you um they may end up
35:59
with a uh you know a medal uh
36:02
to as a reward um and you know basically
36:05
what you've got to say is a bunch of uh
36:09
cultures um that um are not necessarily
36:14
um going to be
36:17
big fans of the united states uh and
36:20
here we are sitting there kind of like a
36:22
big fat uh
36:23
plum waiting to be picked off a tree and
36:26
so
36:27
the internet itself makes it almost

36:29
impossible to to um
36:34
find and catch the bad guys
36:36
um
36:38
obviously
36:39
some are willing to lead footprints but
36:42
the idea basically is that
36:44
um
36:45
the internet criminal is what's known as
36:47
an unknown subject um and the only way
36:51
to really kind of address an unknown
36:53
subject is by
36:54
the classical
36:56
approach known as profiling
37:00
which basically uses big behavioral
37:02
signature signatures
37:04
now profiling has been around for a
37:05
really long time
37:07
first profile was done in
37:09
for jack the ripper i don't know 18
37:11
something or other
37:12
uh and it's developed
37:16
as a
37:17
a aspect of criminology for years i mean
37:20
since then um
37:22

and there are
37:24
um you know techniques
37:26
uh that are
37:28
well recognized well known and used in
37:31
in in in
37:33
criminal justice
37:34
uh talking about them from a uh
37:38
a cyber standpoint uh it's kind of a
37:41
novel thing
37:42
because the key basically is the
37:45
behavioral signatures
37:46
um
37:47
it's all based on collecting uh what
37:50
amounts to evidence of uh you know kind
37:53
of the nature of the crime uh all crimes
37:56
have motivated opportunity and so you
37:58
can kind of classify what you see and
38:01
what you read
38:02
in those actions as um you know a means
38:06
of kind of uh characterizing the
38:08
individual that that's basically
38:09
committed to crime
38:11
um
38:13
now
38:14
since it's done on a digital device that

38:15
actually makes it sort of easier uh
38:19
because uh it's possible to build a
38:22
inductive profile uh using evidence that
38:25
you gather
38:27
from the actual actions that are taken
38:29
on the um you know by the individual uh
38:33
and recorded uh or at least available to
38:36
be
38:37
you know kind of accessed through system
38:39
logs and things like that um then
38:41
essentially what you've got is a pattern
38:44
of behavior that may or may not be used
38:46
to kind of create a typology and that
38:48
typology is something that you can then
38:50
use as a basis for
38:52
either investigating or
38:55
preventing a type of
38:58
a uh you know
39:01
certain types of attack criminal attacks
39:05
um
39:06
things like system logs and system level
39:08
reconstructions of attack behavior uh
39:12
you know
39:13
are are first of all
39:16

they exist uh you know in the sense that
39:18
that it's something that's part of
39:20
system processing um and at the same
39:23
time uh you know there are timelines and
39:26
things like that that you can use
39:28
as a basis for
39:30
um
39:32
kind of not kind of for for following
39:34
the text
39:37
and characterizing
39:40
the timestamp time pattern analysis
39:43
again is a fairly common um
39:46
method for uh incident response um
39:49
and
39:50
um
39:51
we were using uh
39:54
from a standpoint of looking at
39:56
um
39:57
the kind of coding
39:59
attacks
40:00
uh things like stylistic and linguistic
40:03
characteristics all that's something
40:06
that the machine keeps just simply as
40:08
part of its processing
40:10
but at the same time you have a

40:14
opportunity to use that as evidence or
40:17
as a basis at least for building
40:19
profiles
40:21
of of criminal activity or if you want
40:25
to use the simple term attacks
40:27
uh
40:28
on uh and and those attacks basically
40:30
can can be uh formed into
40:33
a um
40:35
type of
40:36
of uh
40:38
a proactive response
40:40
uh
40:41
now the idea here basically is that and
40:44
those of you who are sitting listening
40:46
to this are saying well that that sounds
40:48
like network uh intrusion detection
40:51
automated intrusion detection systems
40:54
which is true
40:55
but at the same time you can extend that
40:57
into
40:58
um you know the realm of actual um you
41:03
know any kind of progressive action
41:05
taken against a
41:07

target
41:10
a targeted resource
41:12
and that basically is something that is
41:16
um
41:18
then
41:19
that you can essentially build a defense
41:21
against or respond to as appropriate
41:25
um now since this is an ai
41:28
uh session uh the thing that i wanted to
41:31
raise is the fact that this can be
41:32
managed by artificial intelligence
41:35
now what you end up with is
41:37
uh you know three general types of of of
41:41
uh ai type um
41:44
profile
41:46
management systems uh one is simply to
41:48
have a baseline of profiles
41:50
uh which then ended up as a pretty much
41:54
like a virus checker you know to
41:55
identify uh
41:58
its criminal behavior
42:00
at the point of a tag
42:02
um and then do something appropriate in
42:04
terms of either shutting off the system
42:06
or shutting out the access or even just

42:09
sending a signal that says we're being
42:11
attacked um
42:13
you can also use baseline anomalies
42:15
which is basically the same thing you
42:17
got a profile but in this particular
42:19
case you get something that just simply
42:21
doesn't fit inside the profile and with
42:24
the assumption that uh if it's anomalous
42:27
it's probably enemy action
42:29
and that can actually
42:31
identify things that are not necessarily
42:34
a uh
42:35
what do you call it captured in the
42:38
behavior patterns
42:39
that you've used to build the profile
42:43
the problem with that one is can
42:44
generate
42:45
false positives a lot of false positives
42:48
and so it's not something that's really
42:49
very practical right now and last but
42:51
not least you can have anomalous
42:53
processing
42:54
which is uh
42:56
we'll identify the attack as it's
42:58

happening because essentially what's
43:00
going on in terms of the normal sequence
43:02
of events inside the computer is not
43:06
it's not kosher it's not something that
43:09
would be normal if that's the case um
43:12
you know you can get a warning at the
43:14
point where the attack's occurring
43:17
the problem with that again is this
43:18
complex is kind of hard to manage and
43:21
all this basically is nothing more than
43:23
me talking about
43:24
um kind of some novel approach that you
43:27
might take based on what amounts to
43:30
well-established
43:33
uh processes
43:35
uh both uh from a criminal justice
43:37
standpoint and also from the standpoint
43:40
of computing
43:41
and um that from my you know is
43:44
basically all i have to talk about here
43:46
uh any questions any discussions you
43:48
want i guess i'll handle that at the end
43:54
thank you very much
43:55
dan
43:56
and our last speaker today is dick

43:59
wilkins principal technology liaison for
44:01
phoenix technologies limited a us-based
44:04
independent platform firmware
44:05
development company and also an
44:07
associate professor of computer science
44:09
and cyber security at thomas college in
44:11
central maine recently retired
44:14
he sits on the board of the unified
44:16
extensible firmware interface forum and
44:19
leads our security response team he's a
44:22
leader in the ieee at the section level
44:24
and in the computer society and is
44:26
active in the acm and pmi he has over 30
44:29
years industry experience in roles from
44:32
software engineer to director of
44:33
engineering at companies like hugh
44:35
packard digital equipment corporation
44:37
microsoft amazon and several smaller
44:39
firms
44:40
professor wilkins holds a phd in
44:42
computer science from nova southeastern
44:45
university a master of science in
44:47
computer science from the national
44:49
technological university
44:51

and a bachelor of arts in public
44:53
administration from saint thomas
44:54
university in miami florida
44:57
welcome dick
45:00
thank you very much dr upton i
45:02
appreciate the
45:04
introduction um let me go ahead and get
45:07
my slides up here
45:09
[Music]
45:16
okay
45:18
so
45:19
i'm going to take this
45:21
from the general to
45:23
a little more specific i'm going to talk
45:26
about ai in relation to security around
45:30
platform firmware
45:32
now most of you may say well gee
45:35
isn't that platform firmware stuff uh
45:38
something that runs in the first couple
45:40
of milliseconds or you know first few
45:42
seconds at most of the computer system
45:45
as it boots up and then kind of goes
45:47
away and
45:48
why do i care and what does this
45:50
interest me

45:51
uh what
45:53
why do i care about the security of that
45:54
particularly
45:57
in fact
45:59
it's a serious problem in uh that i'm
46:02
going to be demonstrating to you but in
46:04
our first presentation today a couple of
46:07
those earlier and most impactful attacks
46:11
and particularly
46:13
notorious is the saudi arabian
46:17
aramco attack was a firmware attack
46:20
where they exfiltrated a bunch of
46:23
data from those systems and then bricked
46:26
them
46:27
and turn
46:28
over 35 000 computers into boat anchors
46:32
and the company had to completely
46:34
replace their entire it infrastructure
46:38
so this is an example of how serious
46:40
firmware attacks can be
46:44
so
46:48
there we go so firmware is critical
46:52
it's the runs right after power up
46:54
initials that initializes the cpu and
46:57

hardware protections updates the cpu
47:00
microcode
47:01
it controls the highly secure inter
47:04
processor modes that even the operating
47:06
system and hypervisors can't touch
47:09
it protects non-volatile memory system
47:11
updates etc it securely boots the os and
47:15
maintains a route of trust from the cpu
47:19
hardware itself that power up through
47:21
all of the initialization and boot
47:23
loaders and everything else
47:25
out to an operating system and
47:27
theoretically all the way out to an
47:29
application so that the system can be
47:32
proven to be secure at at least until
47:34
the app runs
47:36
now once it's online and connecting to
47:39
the internet of course all bets are off
47:41
and it can be attacked but
47:43
vendors software vendors and operating
47:45
system vendors have been working really
47:47
hard over the last
47:49
many years to well ever since the
47:53
internet
47:54
system started getting connected to the

47:56
internet to protect their stuff
47:59
and so it turns out that um what's left
48:02
is firmware
48:04
um continuing with my list here it can
48:07
attest to the system security the
48:09
firmware can and provide evidence to an
48:11
external verifier
48:13
that the system is okay
48:15
um and it provides critical services to
48:18
os os's and applications while they're
48:20
running and people don't realize that's
48:23
going on but the firmware is still there
48:25
and still operational and lastly it's
48:29
persistent
48:31
if you can modify change or hack a
48:34
system firmware then
48:37
it's there potentially forever
48:40
and even wiping the system and starting
48:42
with a new disk drive or something like
48:44
that can't remove it
48:46
so as
48:47
paraphrasing a google engineer from a
48:50
few a few years ago if you don't own
48:52
your firmware your firmware owns you
48:57

so
48:57
what is platform firmware it's you know
49:00
it's the thing that i've been talking
49:01
about here but
49:03
depending on the implementation and what
49:05
it's for and what kind of platform it is
49:08
it can be thousands of lines to millions
49:10
of lines of code
49:13
most commonly nowadays it follows the
49:15
open
49:16
uefi standard
49:18
and as the footnote here on the slides
49:21
is the unified extensible firmware
49:23
interface specification that defines the
49:27
interfaces between
49:29
the operating system and applications
49:32
and
49:32
the underlying firmware
49:35
during the boot process and then after
49:36
the system is up and running
49:39
there is a custom
49:42
most implementations of this are
49:44
customized from an
49:46
open source tiana core implementation
49:49
that's code name from when it was first

49:52
submitted to the open source
49:54
there are also older
49:57
boot firmware called u-boot and core
50:00
boot are the most common they're also
50:02
open source they're typically used for
50:05
embedded and iot devices and a lot for
50:09
phones and things like that they form
50:11
the basis for some of the chrome books
50:13
and things like that out there but um
50:16
nowadays they're now standardizing on
50:20
the uefi interfaces so even while it's a
50:22
completely different implementation
50:24
they're doing uefi things
50:27
lastly there's linux boot
50:30
basically a
50:31
minimal linux
50:34
piece of software that's used to boot
50:36
full linux
50:38
this is more of an experimental thing
50:40
that's going on and a lot of people are
50:42
playing around with it but it's really
50:45
uncommon in
50:46
commercial systems
50:49
modern implementations of this of all of
50:52

these use hashing and signatures to make
50:55
sure they're running secure and
50:56
unmodified code
50:58
they also use secure updates in any
51:00
rollback to make sure that nobody is
51:04
providing them bad code over the
51:06
internet and causing them to update or
51:09
roll back to older unsecure code etc
51:13
they also tend to measure themselves
51:15
also referred to as measured boot
51:18
so that they can attest
51:21
to their security and the fact they've
51:23
been unmodified to an external verifier
51:28
that may control their access to
51:29
networks and things like that
51:33
as
51:34
these things that i've been talking
51:36
about here are best practices
51:38
they're the things that should be done
51:40
to make sure firmware is secure
51:44
but
51:44
many low-cost and iot devices embedded
51:48
systems and surprisingly and annoyingly
51:52
a lot of pcs and servers out there
51:56
don't follow this or they turn it off or

52:00
and so they're not as secure as they
52:02
should be
52:03
but
52:04
this is not your 1970s bios the thing we
52:09
talked about you usually see
52:12
the industry continues to use the term
52:14
bios as shorthand for platform firmware
52:17
but it
52:18
really isn't anything like what ibm
52:21
created for their first pc back in the
52:24
1970s and early 80s
52:27
so
52:28
i put up this not
52:31
for any specific piece of information
52:33
but i want to point out just generally
52:35
the million line plus
52:38
bios is just the the first line in this
52:42
uh
52:43
chart of
52:46
the firmware that gets loaded on a
52:47
machine
52:49
um but there's all kinds of other code
52:52
that runs during the boot process
52:55
that secures the system updates the
52:58

microcode this is for a currently uh
53:01
widely available
53:03
intel processor an example of the bill
53:06
of materials of the firmware that
53:08
gets loaded at boot time and initialized
53:11
and run during the startup of an intel
53:14
uh cpu so the details don't matter here
53:17
i'm just pointing out there's a lot of
53:18
stuff here and it's really important and
53:22
if it gets
53:23
damaged in some way by a hacker bad
53:26
things can happen
53:29
oops
53:30
we somehow got ahead of ourselves here
53:35
okay
53:37
so
53:38
this is an ai presentation so i want to
53:40
make sure that we tie this back to how
53:43
does ai fit into this issue of security
53:47
of platform firmware so if i'm an i.t
53:50
manager i want to know all the devices
53:51
in my system are following the best
53:54
practices and are properly protected
53:56
they're doing the right thing with their
53:57
firmware because again if any of them

54:01
is compromised they can all be
54:03
compromised and
54:05
bad things can happen throughout the
54:07
network
54:08
i've seen baseboard management
54:11
controllers in multi-million dollar
54:14
servers with hundreds or hundreds of
54:17
processors anyway uh where the baseboard
54:20
management controller an old piece of
54:23
firmware and software that
54:26
manages the system operation where that
54:28
thing has been penetrated
54:30
and it has spread
54:33
an infection to every virtual machine
54:36
running across hundreds of processors
54:39
within the same box
54:40
and then it can then expand out to the
54:42
entire network
54:44
so
54:46
i want to be able to scan all the
54:47
devices in my network in real time and
54:50
identify vulnerable damaged devices
54:53
anything bad that could be going on and
54:56
i want to
54:57

identify devices at risk even if they're
54:59
not currently behaving badly intrusion
55:03
detraction systems are fine monitoring
55:05
the network using ai to look for
55:08
patterns and bad behaviors and identify
55:10
devices that have been damaged but
55:13
gee wouldn't it be nice to be able to
55:16
identify them before they go rogue
55:19
before they start
55:20
exfiltrating data from my from my
55:23
network etc
55:24
so
55:27
but there are thousands of devices
55:30
they're running firmware from many
55:31
sources and of many types
55:33
i've talked in the previous slide about
55:36
gee how much there is out there
55:38
um how can i make sure that they're not
55:41
vulnerable they're not damaged by an
55:44
attacker that they're not
55:47
in some way going to come and bite me in
55:49
the rear end
55:51
so
55:52
one option is use ai machine learnings
55:55
to scan them and evaluate their their

55:58
assets
55:59
so here's a
56:01
kind of a marketing picture really of
56:03
what a system might look like that does
56:06
that
56:07
we have
56:09
a user interface
56:12
it's step one there that you can
56:15
schedule an immediate scan of your of
56:17
your network or
56:19
have a
56:20
a scan that runs periodically or
56:22
whatever
56:24
then we have scanning software the red
56:26
ball in the middle
56:28
that goes out and touches everything on
56:30
my network
56:31
and
56:33
takes a look at the firmware
56:36
that's running there its attributes its
56:38
configuration etc
56:41
and then um
56:43
then sends that data out to a secure
56:45
cloud
56:46

which runs ai algorithms to uh
56:50
identify what's going on here
56:53
then
56:54
very quickly
56:55
because we're running out of time
56:58
we want to extract
57:01
an image of what's going on we want to
57:02
scout it for improper configuration
57:06
valid code signatures etc known
57:08
vulnerabilities this can be done without
57:10
machine learning but then we can use
57:14
machine learning simulate the code flow
57:17
to make sure a chain of trust is
57:19
maintained regenerate c code from the
57:21
binary image do static code analysis etc
57:25
we can identify inventabilities observe
57:27
risky code practices etc
57:29
we can
57:30
identify issues and we can take
57:32
automatic action or we can tell an i.t
57:35
manager that this device is suspect and
57:37
you want to evaluate it and do manual
57:40
analysis
57:42
and
57:43
lastly before i wrap up here i just want

57:46
to say we can apply this to other
57:48
potential kinds of networks how about 5g
57:50
networks with phones and tablets and iot
57:53
how about smart vehicle systems autos
57:55
trucks etc and what about that
57:58
autonomous vehicle wouldn't you like to
58:00
have somebody checking that the
58:01
driverless delivery truck firmware
58:04
that's traveling in the lane next to you
58:05
on the highway is actually secure and
58:08
safe
58:09
and there are potentially many other uh
58:12
things where we could apply this to so
58:15
anyway
58:16
that's it for me thank you
58:23
so unfortunately we're out of time um
58:26
excellent presentations thank you very
58:28
much it's been a pleasure to moderate
58:29
this panel and the panelists been typing
58:32
their answers for some of the questions
58:33
from the audience into the q a thank you
58:36
very much
58:37
and for closing remarks here's dr eberty
58:40
thanks very much uh again
58:43

julia our moderator and also our
58:45
speakers and also those of you who
58:47
attended this live presentation or
58:49
watching the recording later if you put
58:51
your question q a and the speakers were
58:53
not able to answer them live will post
58:57
their answers later on on our ai website
59:00
i just want to bring to your attention
59:02
that if you like this presentation we
59:03
have our october 7th event coming up ai
59:06
in space and aerospace event and also uh
59:09
we have our november four events ar in
59:12
health care and we have nasa and nih
59:15
speakers coming in so thanks very much
59:17
again everyone for joining us today and
59:19
uh you can watch the recording of this
59:21
later
59:22
uh on our website if you would like a
59:25
pdh or cu certificate you can just email
59:28
your name and email address and your
59:30
affiliation to the email i shared in the
59:32
chat box um.ai at main.tdu i received
59:36
your certificate so thanks again and see
59:38
you next time

The University of Maine in Orono is the flagship campus of the University of Maine System, where efforts toward racial equity are ongoing, as is the commitment to facing a complicated and not always just institutional history. The University recognizes that it is located on Marsh Island in the homeland of the Penobscot nation, where issues of water and its territorial rights, and encroachment upon sacred sites, are ongoing. Penobscot homeland is connected to the other Wabanaki Tribal Nations — the Passamaquoddy, Maliseet, and Micmac — through kinship, alliances, and diplomacy. The university also recognizes that the Penobscot Nation and the other Wabanaki Tribal Nations are distinct, sovereign, legal and political entities with their own powers of self-governance and self-determination.