Opening Segment

ALLISON: Live from SOURCE Boston, this is WAIT WAIT…DON'T PWN ME!, the security news quiz. I'm ALLISON MILLER, and here's your host at the Marriott Tremont auditorium in downtown Boston, BOB RUDIS.

BOB: Thank you ALLISON and welcome everyone to the first ever WAIT WAIT…DON'T PWN ME!

BOB: Members of the audience can participate in today's show by tweeting: "**Pick me! Pick me! @SOURCEBoston #WaitWaitDontPwnMe**". If you are selected and win, you get our fabulous prize of PRIZE.

BOB: Later on in the show, we'll be talking with Josh Corman, noted zombie hunter & QSA slayer extraordinaire to see if can hack it outside his many fields of expertise.

BOB: While we're collecting our pool of volunteers, let's introduce our panel. First, we have **Wendy Nather**, security practice research director at 451 Research and a voice of reason in our ever-expanding echo chamber. Thanks for being here, Wendy. Hopefully your time in Boston has been less hectic than your RSA schedule and more sober than Shmoocon…

BOB: Next up on our panel is **Ben Jackson,** Grand Poohbah at Mayhemic Labs and an outspoken voice of the defender. Ben's also a ham radio enthusiast and we were wondering what the craziest experience you've ever had over the short, medium, -or-long waves (or the ones which were Juuuust Right:

BOB: And, last on our panel is **Andrew Hay**, a Canadian expat, living and working in San Francisco as Chief Evangelist at CloudPassage, eh. Thanks for being here, Andrew! Can you give us a sense of what it's like being exiled from the land of bacon & curling and being thrust into the world of alpha geeks and brogrammers in SF?

BOB: So, ALLISON, who is our first volunteer

ALLISON: INTRODUCES VOLUNTEER

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

SEGMENT 1: In the News : THE RED MENACE

BOB: VOLUNTEER, welcome to WWDPM. Is this your first time at SOURCE Boston? Well, you're going to be starting us off with a segment called "THE RED MENACE!" Yes, China has been in the news quite a bit and ALLISON will be presenting descriptions of three China-related stories/hacks. Successfully identify at least two of them and you'll get PRIZE. Are you ready to play? … Let's get started.

ALLISON: "Over the course of three months, attackers installed 45 pieces of custom malware. We used antivirus products made by Symantec and it found only one instance where it identified an attacker's software as malicious and quarantined it."

BOB: Alright, VOLUNTEER, which entity was that China hack referring to? ANSWER: NYTimes

BOB: ALLISON, what's our next attack?

ALLISON: "…Our position was that 'The Chinese government may authorize this activity, but there's no way to determine the extent of its involvement.' Now, three years later, we have the evidence required to change our assessment. The details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them."

BOB: OK, VOLUNTEER, can you identify what that quote is referring to? ANSWER: Mandiant APT1 report

BOB: And, here's our last story about a three year old hack disclosed just this past November…

ALLISON: "In 2009, the FBI told company executives that hackers had broken into their computer systems and spent a month 'pilfering sensitive files' about their attempted $2.5 billion pending acquisition. The Chinese hackers penetrated the network after tricking the company's deputy president into clicking on a link in a malicious, targeted e-mail and gained enough details to thwart the potentially profitable deal."

BOB: So, VOLUNTEER, can you identify the company that suffered that costly breach? ANSWER: Coke

BOB: Well, ALLISON, how many did VOLUNTEER get right?

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

ALLISON: REPORTS TALLY

VOLUNTEER got x out of 3 right, enough to win PRIZE!

BOB: Thanks for playing, VOLUNTEER!

SEGMENT 2: Practitioner Panel Round One

BOB: Later on, we'll try to pry ALLISON away from her new GRC – Gibe, Rhyme & Crambo – software to get her to do our Practitioner Limerick Challenge

Right now, panel, it's time for you to answer some questions about security industry themed news.

Wendy: What common computing component has been under such relentless attack that it has inspired the creation of a "Days since last know exploit" website that prominently displays a counter along with other exploit information?

ANSWER: Java

Yes, Oracle has released a seemingly relentless series of updates these past few months spurring pundits to advise eradicating this software menace from all your desktops with PCMag's Larry Seltzer stating that *"the Java platform as a whole is pretty clearly a failure, and all that remains is a big fat attack surface on your computer."*

BOB: Ben: Which security reporter suffered a series of online and real-world attacks, ultimately culminating in a visit from the not-so-friendly neighborhood SWAT team while he was making final preparations for that night's dinner party?

ANSWER: Brian Krebs

Yes, Krebs has his cable bill paid for a couple years and then disconnected, suffered a massive DoS attack and then was told to drop to the ground at armed gunpoint. Now there's a story for the grandkids. In all seriousness, it must have been a pretty harrowing experience for the Krebs family that thankfully turned out OK.

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

BOB: Andrew: What questionable technique did an unnamed "security researcher" use to acquire the data for the recently released "Internet Census 2012"?

ANSWER: Build a "good" botnet

Yes, this "researcher" used the Carna botnet software to repeatedly take control of 420,000 devices on the internet to facilitate his comprehensive census report. His technique even cleaned off "bad botnet software" that was already using some of the devices for things like spam and DDoS attacks. You have to wonder what was going through the researcher's head, tho, especially given that this activity is illegal in almost every country and it's only a matter of time before this big data report lands the researcher in the big house.

SEGMENT 3: Pwn the Practitioner

BOB: Now it's time to play "Pwn the Practitioner", where an audience member tries to tell truth from fiction. ALLISON, Who is our next participant?

ALLISON: HOST, we have VOLUNTEER playing from VOLUNTEER INFO

BOB: Thanks for playing, VOLUNTEER. You'll be hearing three stories from our panel and your job is to try to not get pwned and figure out which one is real. ALLISON, what's today's topic?

ALLISON: HOST, today's topic is "*Internet of Pwnd Things*"

BOB: Yes, commodity software is constantly being combined with ubiquitous connectivity and slammed into everything from toasters to pacemakers. Our panelists are going to read three stories of everyday things being compromised and used in ways not originally intended. Guess the right one and you'll win PRIZE. Ready to play?

Great. Let's hear first from Ben Jackson, about a story that's more than meets the eye.

JACKSON: When Google started equipping early adopters—their "Glass Explorers"— with their new Google Glass eyewear, it sparked a host of "Stop the cyborgs" petitions and web sites and caused some businesses to bar entrance to those wearing them. Some municipalities have even crafted legislation to ban the use of them in designated public places. But, all this uproar may be warranted as researchers from Israeli

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

security firm Cyvera disclosed yesterday in an IEEE journal that they were able to use the Bluetooth channel from a connected Android phone to gain access to protected Google Glass firmware. During their firmware dissection, they discovered hooks to a previously undisclosed hardware component of the glasses—an STMicroelectronics terahertz CMOS chip which was developed in early 2012.

"These cheap terahertz imagers work just like the airport scanners that have been under so much scrutiny by the public. It's impressive that Google was able to incorporate these new chips into their Glass units so quickly", said Hani Sherry, research director at Cyvera. "Just like the airport scanners, this sensor captures images that leave virtually nothing to the imagination. Because the CMOS component saps a decent amount of power and provides a possibly controversial visual perspective, I can see why Google engineers might not have wanted to enable it in this public prototype".

It didn't take Hani's team long to figure out how to enable the terahertz chip, effectively turning Glass devices into a working, modern day set of X-ray specs. Now, along with saying "*ok, glass take a picture*" or "*ok, glass, record a video*", Glass Explorers who use a mod developed by Cyvera can also now say, "*ok, glass, enable TSA mode*" to have all images captured with the…extra detail. No doubt, as the report makes its way to the media, we'll see further attempts by businesses and authorities to curtail the use of this enhanced eyewear.

Google did not comment on the journal article release but said they've been completely transparent about the features of Google Glass.

BOB: So, there you have it, our first story—revealed by Ben Jackson—on nude scanner tech being discovered embedded in new Google Glasses.

Our next revealing story comes from Andrew Hay…

HAY: Ira Hunt, CTO of the Central Intelligence Agency created quite a stir back in March at GigaOM's Stucture:Data conference when he revealed that members of the "cult of the quantified self" are disclosing more information then they may think when they wear activity tracking devices such as the Fitbit One or the Nike Fuel band.

"Devices—like Fitbit—have 100% accuracy in identifying people by their gaits. Fitbit also tracks calories burned, steps taken, distance traveled and sleep quality. What users of this device may not know, however, is that many other types of activities can be accurately

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

detected and reported," said Hunt during his presentation. "Two years ago, Fitbit service issues led to an embarrassing disclosure of manual intimate activity logs into Google searches. Today, I'm telling you those logs are no longer necessary."

Hunt's disclosure was reinforced by medical researchers who said they are now able to use big data mining techniques to determine when a faithful tracker user is not only walking, running or sleeping but also having an intimate moment or even making a restroom visit. "It's possible—by hacking the data—to tell when you're running late for a meeting or less than thrilled to be where you are heading, just by analyzing and comparing tracking history", said one researcher.

This discovery has obviously raised data privacy concerns but also has the potential to launch new medical-related services. One AMA-affiliated group of urologists are working with Fitbit to create the "Fitbit Flush" to help treat their patients diagnosed with incontinence by more accurately tracking restroom visits.

BOB: You said you were walking but the data doesn't lie. A story on how hacking tracker data reveals more than you might expect.

Wendy Nather heats things up with our final, embedded story.

NATHER: More and more people are using internet connected devices to help with home automation tasks to save both time and money. Unfortunately, as we connect more real-world items like heating and cooling systems to the digital world, things might not always go as planned. This was definitely the case for Jerry Harrison & Tina Weymouth, two users of the popular "Nest" thermostat who ended up having to replace their furnaces after hackers took over their devices and made them run out of control.

"I had my ticket, packed my bags and was headed on vacation. I set the Nest away schedule properly, but someone must have guessed my password and set the heat up to 365°F 24/7. It completely destroyed the burner and blew out the transformer" said Weymouth, a Coronado, CA resident.

In a similar incident, the constant use of Harrison's furnace even caused some cabling to melt and fuse together in a conduit near the duct work. "I was just lucky it didn't cause an actual fire," said Harrison.

Their respective insurance companies are covering the damages since

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

they had the Nest thermostats professionally installed and investigators could not find anything out of the ordinary. However, this has sparked debate in the underwriting community as to the need to take into account these new connected devices and the associated security protocols when writing new policy.

"We may need to start taking cyber security into account as we collect information from potential customers and review data from existing policy holders," said Chris Franz, chief underwriter at Byrne Insurance.

BOB: So, there you have it: a story on Google's hidden x-ray feature in Google Glasses, data from personal trackers disclosing more info than you might expect or hacked internet connected thermostats causing real-world damage. Which of these three do you think is the real story?

INTERACT WITH VOLUNTEER

Why, yes the answer **is** #2, the use of giant amounts of correlated quantified self data is being actively used to determine what actions people are doing and when. Perhaps this'll make you think twice before taking that tracker into certain places if you want any privacy (though they'll probably be able to determine what you **would** have been doing, too).

Well, VOLUNTEER, you've won our PRIZE. Thanks for playing!

SEGMENT 4 : Not My Job

BOB: Remember folks, members of the audience can participate in today's show by tweeting: "**Pick me! Pick me! @SOURCEBoston #WaitWaitDontPwnMe**". If you are selected and win, you get our fabulous prize of PRIZE.

BOB: So, now we're at the part of our show where we ask a noted & respected information security practitioner to answer a few questions that are completely outside their field(s) of expertise. Josh Corman has graciously volunteered to have his wits tested this afternoon. Josh, welcome to Wait, Wait Don't Pwn Me.

Now, Josh, can you tell us a bit of how you got into information security?

It wasn't easy trying to find something that could stump such a renaissance man, but it seems one of the few things you haven't pursued

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

is a career in acting (unless you count the whole security gig thing), so we're going to put you through a round of questions we've called:

ALLISON: "Just Joshing Around"

BOB: I'm going to ask you three questions about some famous Josh's in the movies. Guess the movie/TV show and the actor OR the actor's character correctly for at least two of them and you win a prize for one of the audience volunteers. ALLISON, who is Josh playing for?

ALLISON: Bob, Josh is playing for VOLUNTEER

BOB: Alright, Josh, ready to play? Here's your first question…

After he finds $2 million in the desert where a drug deal has apparently gone wrong, this Josh's character finds himself on the run. His pursuer is an unemotional killer with a unique murder weapon at his disposal. Throughout the story, the soon to be retired sheriff attempts to convince Josh's character, mostly through his wife, that he should turn the money over to the authorities or this could all end in tragedy.

SO, what movie is this referring to and who is the actor? JOSH BROLIN / LLEWELLYN MOSS / NO COUNTRY FOR OLD MEN

BOB: Here's your next acting challenge:

This Josh's character was aboard a trans-Atlantic flight after killing the man who he'd thought ruined his life, and was deported from Australia after being drunk and assaulting an Australian politician. The character was a con man that preferred to play the romance angle. The flight crashed on an island and this character was known for collecting and hoarding items from the crash site and for being the resident smart-talking rebel on the island. He was one of the island's most prolific sources of colorful, often insulting nicknames for other castaways and island locations. These mannerisms make him easily hated and despised by most of the islanders, although it is eventually revealed that he purposely incites others into hostility against him.

SO, what TV show is this referring to and who is the actor? JOSH HOLLOWAY / SAWYER / LOST

BOB: And, finally, here's the final act for this round:

Heather Donahue, Michael Williams and this actor's self-named

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

character were student filmmakers that set out to shoot a documentary about a local legend/folktale. In the forests near Burkittsville, Maryland, many children have vanished in the 1940s and people still avoid going too deep into the woods. So, the party sets out to look for facts that prove the legend, equipped only with two cameras and a little hiking gear. First, they find little piles of stone that must have been arranged artificially, later, they have to admit to be lost in the woods. Eerie sounds at night and more piles of stones in places where they have not been before cause the already desperate group to panic. And one night, days after they should have been back home, this actor's main character disappears completely. Only what has been recorded and filmed with the cameras is found a year later and shows what happened in the woods

SO, Josh, who is the actor/character and what is the name of this spooky movie (that also started the shakycam craze): JOSHUA LEONARD / THE BLAIR WITCH PROJECT

BOB: So, ALLISON, how'd Josh do?

ALLISON: Josh got x out of 3 right (then note whether he won or lost for the volunteer)

SEGMENT 5 : Practitioner Limerick Challenge

BOB: ALLISON who's our next victim–er–volunteer?

ALLISON: Well, HOST, we have VOLUNTEER from …

BOB: Welcome, VOLUNTEER to WWDPM. For this part of the show, ALLISON will read you three news-related limericks with the last word or phrase missing from each. If you can fill in that last word or phrase correctly on two of the limericks, you'll be a winner. Ready to play? Here's your first limerick.

ALLISON: *It seems hackers are all doxing crazy;*
they post your personal secrets almost daily;
but their hacked Equifax files,
might just get them exiled;
They should not have pwnd the First…

BOB: Yes, LADY. It was revealed in March that hackers stole and posted financial information of celebrities like Beyonce, Jay-Z and Ashton

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

Kutcher, but they might have wanted to stop there. It's one thing to play Pwning with the Stars, but something completely else when you start messing with the wife of **the most powerful man on the planet**. If you thought the hunt for Osama bin Laden was resourced well, just imagine what these people are in for (and we all know what happened to that guy).

OK, ALLISON, hit us with your next limerick.

ALLISON: *To boast of your own product is fine;*
Vendors do it all of the time;
But before you slam others,
close all your doors and your shutters,
or risk ending up hacked like…

BOB: Yes, BIT9! The fine marketing folks at Bit9 had been known to do more than just tout the capabilities of their own product, sometimes prominently highlighting when competitors' products failed or were hacked. Back in February, one of their own web servers was pwnd and the resulting compromise harmed both Bit9 and many of their customers when hackers used Bit9's own certificates to sign their malware code, enabling a complete bypass of the software. I hope they Bit9 folks are heeding the "people in glass houses…" now.

Here's the last limerick…

ALLISON: *Our defenders aren't cut too much slack;*
They're under almost constant attack;
But, if you're feeling frustrated,
Please keep your anger abated;
It's a bad, bad idea to hack…

BOB: Yes, BACK! Advocating hacking back has been all the rage in various infosec circles of late, with the notion that not being able to take the fight to the attacker is akin to making practitioners defend with two arms and one leg tied behind their backs. I won't try to debate this here since Steve Maske covered the topic in his talk yesterday, but the fact of the matter is **the hackers got in once already**. Hacking back is like poking a bear that decided you weren't worth mangling after taking one swipe at you and saying "please, sir, may I have another?"

So, ALLISON, how did VOLUNTEER, do?

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

ALLISON: AGAIN, GAME THIS SO THEY WIN

Well, HOST, VOLUNTEER got x out of 3 right and has won our prize of PRIZE.

BOB: Well done, VOLUNTEER! Thanks for playing!

SECTION 6 : Packetstorm Fill In The Blank

BOB: Now, on to our final game. Packetstorm Fill in the Blank. Each of our panelists will have 30 seconds to answer as many fill in the blank questions as they can. Each correct answer is worth two points. ALLISON, can you tell us the scores?

ALLISON: Wendy has #; Ben has # and Andrew has #.

BOB: So PERSON_IN_THIRD_PLACE, you're up first. The clock will start when I being your first question. Fill in the blank.

- What prominent infosec personality started the recent "awareness programs are worthless" meme: DAVE AITEL
- What state's tax department was breached in 2012, affecting over 6.4 million individuals & businesses? SOUTH CAROLINA
- What popular web application security company just received $31million in new funding? WHITEHAT
- A recent study discovered that the majority of 419 scams really do originate from what country? NIGERIA
- What Asian country was just recently hit with a debilitating country-wide DDoS attack? SOUTH KOREA
- What flight management system technology did security researches recently claim could be hacked with an Android phone? ACARS
- What supermarket chain recently had a breach that exposed 2.4m credit cards? SCHNUCKS
- What did the US President release in 2013 that will have cascading

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

information security & compliance impacts across government and many private sector entities? PPD21

BOB: ALLISON, how did PERSON_IN_THIRD_PLACE do?

ALLISON: GIVES THE COUNT AND THE PLACE PERSON IS IN

BOB: Alright, PERSON_IN_SECOND_PLACE, you're up next. Remember, you have 30 seconds to answer as many questions as you can. Ready? Here we go.

- What popular personal gadget and computer maker finally enabled two factor authentication for its identity services? APPLE

- What media & news site was hacked twice in February, including the site of one late night celebrity's show: NBC/JIMMY FALLON

- What major hacker competition in 2013 saw every major modern browser completely pwned, again: CANSECWEST/PWN2OWN

- What popular botnet was updated to mine Bitcoins and topped Fortinet's list of worst botnet of the 1Q 2013: ZEROACCESS

- President Obama increased the budget for domestic cybersecurity to what amount for 2013: THREE BILLION DOLLARS

- What popular piece of software came under massive attack this past weekend in order to expand the size of an already scarily big botnet: WORDPRESS

- What camera maker came under fire for critical weakness in their top-of-the line wireless & Ethernet-equipped camera model that made remote surveillance a trivial task: CANNON

- In 2012, what massive malware/botnet combination was discovered and taken over by the FBI, NASA-OIG and Estonian police and forced all infected users to check and change nameserver settings? DNSCHANGER

- What go-to resource site for vulnerability information had to be shut down earlier this year due to hacking? NVD

BOB: ALLISON, how did PERSON_IN_SECOND_PLACE do?

ALLISON: GIVES THE COUNT AND THE PLACE PERSON IS IN

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

BOB: Alright, PERSON_IN_FIRST_PLACE, you went into the round in first place and you're now in PLACE. You need X correct questions to regain the lead? Are you ready?

- What cloud-based note taking service had their customer database hacked, requiring a reset of all user passwords? EVERNOTE

- What programming library repository was hacked by the upload of a malicious library package? RUBY/RUBY GEMS

- In 2012, what highly visible source code management repository was hacked and allowed attackers to gain full administrative access over all source code repositories? GITHUB

- Skype & Dropbox both recently fixed a bug that could have allowed attackers to go gain control of what? FACEBOOK

- What controversial piece of legislation is back in front of Congress but has the White House threatening a veto? CISPA

- According to a recent FireEye report, how frequently do most companies experience a malware event? EVERY THREE MINUTES

- The Twitter accounts of which broadcast organization were recently hacked by the Syrian Electronic Army? NPR

- After the NYTimes disclosed their China breach, what other newspaper came out of Clark Kent's closet to say "hey, we're cool, we were breached by China, too!!"? WASHINGTON POST

- What well-known online gaming service had details of a compromise leaked during the reporting of another high-profile attack? XBOX

BOB: OK, ALLISON, did PERSON get enough points to win?

ALLISON: REPORTS THE TALLY, ANNOUCES THE WINNER

BOB: Well, that's all we have time for today. I'd like to thank our panel members, Wendy Nather, Ben Jackson & Andrew Hay for participating along with all the volunteers and everyone involved in making today's show happen. I'll ask our panelists to close us out with a prediction on what will be the next big hack of 2013…

Wait Wait… Don't Pwn Me SOURCE Boston 2013 Transcript
by Bob Rudis is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License