THANK YOU, EVERYONE, FOR JOINING US.
WE ARE REALLY EXCITED TO HAVE A GREAT SECOND PANEL CONSISTING OF A LOT OF THE FOLKS WHO DESIGN THE SYSTEMS THAT ARE BUILT TO PROTECT CONSUMERS FROM MALWARE. REALLY GETTING A SENSE OF HOW THEY'RE BUILDING SECURITY IN TO THEIR MOBILE PLATFORMS AND WHAT THEY'RE DOING TO ADDRESS THE THREATS THAT WE DISCUSSED IN THE FIRST PANEL.
SO WE HAVE HERE WILLIAM ENCK, AN ASSISTANT PROFESSOR AT THE DEPARTMENT OF COMPUTER SCIENCE AT NORTH CAROLINA STATE UNIVERSITY. HE SPENT MUCH OF HIS RESEARCH CAREER ON MOBILE SYSTEMS SECURITY.
WE HAVE ADRIAN LUDWIG, THE MANAGER FOR ANDROID SECURITY AT GOOGLE.
WE HAVE MICHAEL COATES, THE DIRECTOR OF SECURITY ASSURANCE AT MOZILLA CORPORATION.
[PLEASE STAND BY]
WE HAVE GEIR OLSEN, PRINCIPAL PROGRAM MANAGER FOR WINDOWS PHONE ENGINEERING, DEALS WITH WINDOWS PHONE SECURITY AT MICROSOFT.
ADRIAN STONE, THE DIRECTOR OF SECURITY RESPONSE AT BLACKBERRY. AND WE HAVE JANE HORVATH, DIRECTOR OF GLOBAL PRIVACY AT APPLE, INC.
AND TO GIVE YOU A LITTLE BACKGROUND IN TERMS OF HOW I
DECIDED TO SEAT THE FOLKS IN THIS ORDER, IF YOU SEE HERE, GOOGLE AND MOZILLA WITH FIRE FOX OS ARE OPEN SOURCE PLATFORMS AND HAVE MULTIPLE PARTNERS THEY WORK WITH IN ORDER TO CREATE THE HARDWARE THAT THEIR OPERATING SYSTEMS RUN ON. GEIR OLSEN FROM MICROSOFT, YOU KNOW, MICROSOFT WINDOWS, PHONE IS A PROPRIETARY OPERATING SYSTEM, BUT HE TOO, YOU KNOW, DEALS WITH MULTIPLE [PLEASE STAND BY]
IT'S NOT GOING TO BE ABLE TO SEND THAT MESSAGE SO THIS CAN HELP SOME INVESTIGATIONS AS WELL.
IT HELPS EXPERTS BECOME WHISTLE-BLOWERS TO FIND SKETCHY APPLICATIONS. WHEN APPLICATIONS ARE OVER THE PHONE, TYPICALLY SIGNED, SO CODE SIGNING HAS BEEN AROUND FOR DECADES IN THE PC WORLD, THIS IS BASICALLY THE IDEA WHERE YOU'RE GOING TO ENCRYPT OR SIGN WITH A PRIVATE KEY SOME APPLICATION, AND THEN ANYONE WHO HAS A PUBLIC KEY CAN VERIFY THAT ONLY YOU WERE ABLE TO SIGN THAT. THE PLATFORMS DEAL WITH THIS IN DIFFERENT WAYS, AGAIN, SOME MORE CENTRALIZED LIKE iOS WHERE IF APPLE DOESN'T SIGN THAT APPLICATION, IT CAN'T RUN ON AN iPHONE. NOW, IT'S A LITTLE DIFFERENT IN ANDROID WHERE DEVELOPERS SIGN THOSE DIFFERENT APPLICATIONS. THERE'S NO CENTRALIZED NOTION OF WHO CAN DECIDE WHAT CAN RUN OUR PLATFORM OR NOT, BUT THERE'S DIFFERENT VALUES TO THIS MODEL. ONE OF THE PRIMARY THINGS THAT
THE SIGNATURE MODEL THIS PROVIDES ONCE YOU HAVE THIS BANK OF AMERICA APP UPGRADE TO NEW BANK OF AMERICA UP, THE SAME DEVELOPER IS GIVING YOU THE UPDATE.

YOU ALSO HEAR ABOUT SOMETHINGS CALLED IPC, INTER-PROCESS COMMUNICATION, A TERM WE USE WHEN APPLICATIONS ON THE PHONE ARE TALKING TO ONE ANOTHER. AND AGAIN, THIS IS DIFFERENT AND VARIES BETWEEN DIFFERENT PLATFORMS.

THE MOST FEATURE RICH FORM OF COMMUNICATION BETWEEN APPS. TERMINOLOGY SPECIFIC TO THAT THAT MAY OR MAY NOT COME UP IN THE DISCUSSION.

THESE ARE CALLED INTENT MESSAGES ON ANDROID, SENT TO THESE ACTION STRINGS WHICH ARE BASICALLY SORT OF ADDRESSES FOR MESSAGES AUTOMATICALLY RESOLVED BY THE PLATFORM.

USED FOR INTEGRATION BETWEEN THE USER PART OF APPLICATIONS AND ALSO THE BACKGROUND PARTS OF APPLICATIONS AND CAN BE USED TO START APPLICATIONS AUTOMATICALLY.

THIS CAN TRIGGER MALWARE. FOR EXAMPLE, MALWARE CAN START WHEN YOU GET A NEW SMS MESSAGE ON YOUR PHONE. ALSO USED FOR INTERACTIONS BETWEEN APPS. BECAUSE OF THAT, THESE APPLICATIONS CAN REEXPOSE PRIVILEGED APP.

YOU HAVE AN APPLICATION, CAN MAKE A PHONE CALL, IT HAS INTERFACES FOR OTHER APPLICATIONS TO WORK IT WITH AND INTERACT IT WITH. MIGHT REEXPOSE THAT ABILITY TO
MAKE THE PHONE CALL. SO THIS CAN PRODUCE VULNERABILITIES. ONE OF THE POINTS I WANT TO MAKE HERE IN DISCUSSES IPC, IT'S NOT JUST THE PLATFORM AND THE CODE THAT IS CREATED BY THE MANUFACTURER, BUT ALSO THE DEVELOPERS OF APPLICATIONS THAT YOU RUN THAT CAN PROVIDE AND CAUSE VULNERABILITIES ON A PLATFORM. NOT JUST ANDROID. DON'T WANTS TO PICK ON ANDROID TOO MUCH. MY RESEARCH HAS BEEN. iOS HAS FORMS OF IPC, URL PROTOCOL HANDLERS THAT ALLOW ONE APPLICATION TO SEND DATA TO ANOTHER. AN INSTANCE IN SKYPE WHERE YOU COULD START A SKYPE CALL AUTOMATICALLY. IN TERMS OF MALWARE, GREAT DISCUSSION ON MALWARE IN THE FIRST PANEL. I THINK WE SORT OF SETTLED 2 FACT THAT MALWARE ON SMARTPHONES LIKE ON PCs, INCENTIVE BASED. USUALLY BOILS DOWN TO SOME SORT OF MONETARY INCENTIVE. GENERALLY NOT GOING TO SEE MALWARE DINED TO DRAIN YOUR BATTERY. THEN YOUR, DESIGNED TO DRAIN YOUR BATLY BECAUSE THEN YOUR PHONE IS PRETTY USELESS. TWO FORMS OF MALWARE, ROOLT ACCESS, ADMINISTRATIVE ACCESS FROM THE PHONE, WAS ONE OF THE PANELISTS DISCUSSING. THIS IS A DANGEROUS STUFF. IT'S HARD TO DETECT, HARD TO REMOVE ONCE IT'S ON THERE. AND SO THIS IS A PRIMARY THING THAT THE PLATFORMS WANT TO
PROTECT AGAINST.
ALSO MALWARE THAT WORKS WITHIN
THE PERMISSION SYSTEM.
INTALL AN APPLICATION, ASKS FOR
ABILITY TO SEND A MESSAGE,
GRANTED THAT ACCESS AND THEN IT
DOES IT.
A LOT OF WHEN YOU LOOK AT THE
SORT OF THE SHEAR NUMBER OF
DIFFERENT TYPES OF MALWARE, A
LOT WORK WITH PERMISSION SYSTEM
BUT WE ARE SEEING SOME WHICH GET
ACCESS AS WELL.
PROTECTING THAT, THERE'S EFFORTS
IN SORT OF IN THE CLOUD, IN THE
MARKET, USE DIFFERENT DYNAMIC,
STATIC ANALYSIS TECH SEEKSO THE
PHONE WE CAN INTALL ANTIVIRUS
SOFTWARE JUST AS ON PCs.
THE POINT HERE IS THAT THERE IS
A DISCUSSION WITHIN THE
COMMUNITY WHETHER OR NOT THIS ON
PHONE ANTIVIRUS SOFTWARE GIVES
YOU A VALUE-ADD.
I HOPE THIS IS ONE OF THE THINGS
WE'RE GOING TO TALK MORE
IN-DEPTH ON THE PANEL.
FROM THE PLATFORM SIDE,
PROTECTING AGAINST THESE NASTY,
ROOT EXPLOITS.
TECHNOLOGY FROM THE PC WORLD
HAVE BEEN MIGRATED AND ADOPTED
BY THE E-MOBILE PLATFORMS.
TERMS YOU MIGHT HEAR, ONE IS
ADDRESS SPACE LAYOUT
RANDOMIZATION OR ASLR.
THE BASIC IDEA IS WHEN YOU WANT
TO MOUNT EKES SPLOIT, OFTEN YOU
HAVE TO GUESS WHERE, AN EXPLOIT,
GUESS WHERE IN MEMORY TO EXECUTE
CODE.
IF YOU MOVE THE PAGES IN MEMORY
AROUND TO DIFFERENT LOCATION,
RANDOMIZE THAT, MUCH HARDER TO
GET, PROVIDES SOME PROTECTION.
THE OTHER TYPESCIES DEP, DATA
PROTECTION.
IDEA IS WHEN YOU WANT TO GO AND
EXCUSE SOME EXPLOIT, YOU DELIVER
THAT CODE DOWN TO THE
APPLICATION, PUTS IT IN ITS
TALK, SORT OF A SCRATCH PAD FOR
DOING OPERATIONS.
EXECUTES FROM THERE.
NO REASON FOR THE SCRATCH PAD TO
BE, EXECUTABLE.
WE ADDED HARDWARE BITS TO MAKE
SURE THE SCRATCH PAD ISN'T
EXECUTABLE, COMINGS TO MARKETS
AND CLOUD.
TWO BROAD TECHNIQUES.
ONE IS STATIC ANALYSIS, THE
OTHER IS DYNAMIC ANALYSIS IF YOU
DON'T REMEMBER ANYTHING ELSE, AT
THAT TIMIC ANALYSIS WILL LOOK AT
AN APPLICATION, NOT RUN IT AND
IT'S GOING TO FIGURE OUT WHAT
ARE ALL THE POSSIBLE THINGS THAT
CAN HAPPEN.
WHAT ARE ALL THE POSSIBLE CODE
PATHS THAT CAN EXECUTE.
NOT NECESSARILY WHAT CAN HAPPEN
WITH DEAD CODE OR CONFIGURATION
NOT TURNED ON THAT MAY NOT DO
THAT.
THAT'S WHERE DYNAMIC ANALYSIS
CAN BE USED TO RUN THE
APPLICATION, SEE WHAT'S
HAPPENED.
LIMITATION THERE, VERY HARD TO
AUTOMATICALLY TICKLE ALL THOSE
POTENTIALLY DANGEROUS PARTS IN
THE APPLICATION TO SEE WHAT WILL
HAPPEN WHEN YOUR USERS RUN THEM.
LAST SORT OF TOPIC TO BRING UP
HERE, THIS IDEA OF JAILBREAKING
OR ROOTING.
VERY SIMILAR CONCEPTS AND ARE
OFTEN CONFUSED WITH ONE ANOTHER.
YOU CAN THINK OF THEM SORT OF
THE SAME.
SUBTLE DIFFERENCES BETWEEN
JAILBREAKING OPENING UP RESTRICTIONS, OPENING UP, SELLING APPLICATIONS. ROOTING IS MUCH MORE OF A SUPER SET, MORE POWERFUL. WHOLE COMMUNITY WHO LOVES TO TINKER WITH DEVICES, TECHNOLOGY. PHONES ARE AN EXCEPTION. THEY HAVE TAKEN THESE PHONES, FOR THEIR OWN PURPOSES FIGURING OUT WAYS OF PUTTING THEIR OWN FIRMWARE ON TO GET ENHANCED CAPABILITIES.

IT'S NOT JUST BAD GUYS TRYING TO DO THIS BUT HOBBIES AS WELL. THESE HOBBIES CREATING MECHANISMS THAT MALWARE OPERATORS ARE TAKING.

MANY MOTIVATIONS.

IN THE END, DOING JAILBREAKING, ROOTING, OFTEN MAKES THE PHONE LESS SECURE, LESS DESIRABLE FOR ENTERPRISES WHO HAVE THEIR EMPLOYEES USING THE DEVICES AND MY PERSPECTIVE AT LEAST, REMOVING MOTIVATIONS CAN IN THE END HELP INCREASE THE SECURITY.

THAT'S MY CRASH COURSE.
HOPEFULLY THAT WILL GIVE YOU TERMINOLOGY AS WE TALK ABOUT THESE DIFFERENT TOPICS ON THE PANEL.

>> THANKS.
I SEE SOME CONFUSED LOOKS IN THE AUDIENCE.
HOPEFULLY PEOPLE WERE ABLE TO FOLLOW ALONG.
HOPEFULLY, YOU KNOW, THE PANELISTS WILL BE ABLE TO ILLUMINATE US AS WE CONTINUE THE DISCUSSION.

SO WE'LL DISCUSS THE FACT THAT THE MOBILE OPERATING SYSTEMS ALL USE SOME KIND OF SANDBOXING, WHICH MEANS THAT THE APPLICATIONS ARE LIMITED TO
THEIR OWN SPACE WITHIN THE DEVICE AND YOU KNOW, HAVE LIMITS ON HOW THEY CAN INTERACT WITH OTHER APPLICATIONS AS WELL AS HOW THEY CAN INTERACT WITH THE VARIOUS SYSTEM RESOURCES. AND ONE OF THE ISSUES THAT OMAR BROUGHT UP ON THE LAST PANEL WAS THAT, YOU KNOW, ANDROID IN PARTICULAR MAKES MANY DIFFERENT APIs AVAILABLE TO APPLICATIONS. AND ONE OF THE THINGS THAT I WANT TO DISCUSS IS HOW WE CREATE DESIGNS SECURE APIs. WHAT ARE WAYS IN WHICH YOU CAN CREATE APIs SO THAT YOU ALLOW LEGITIMATE APPLICATIONS TO USE REALLY COMPELLING FUNCTIONALITY THAT CREATES GREAT APPS AND GREAT USER EXPERIENCES BUT STILL ENSURE MALICIOUS APPLICATIONS CAN'T ABUSE THOSE FUNCTIONALITIES FOR NEFARIOUS ENDS. AND SO TO THAT END, I WOULD LIKE TO POSE A QUESTION TO ADRIAN. PART OF HOW I AM GOING ABOUT THE PANEL IS TO BRING UP, YOU KNOW, CHALLENGES THAT EACH OF THE PLATFORMS HAVE HAD IN THE PAST AND REALLY TRY TO DISCUSS HOW THEY RESPONDED TO THOSE CHALLENGES AND HOW THEY MADE CHANGES POTENTIALLY TO THE PLATFORM IN RESPONSE TO THINGS THAT THEY SAW WERE POTENTIALLY BEING ABUSED. SO ADRIAN, WITH THAT, CAN YOU DISCUSS A BIT ABOUT THE READ LAW API AND ANDROID? FOR THOSE WHO DON'T KNOW, THE REID LOG API ALLOWED APPLICATIONS TO ACCESS A CENTRAL SYSTEM LOG ON ANDROID DEVICES. AND ACCORDING TO REPORTS FROM RESEARCHERS, A LOT OF APPS WERE
WRITING SENSITIVE INFORMATION INTO THE LOGS WHICH COULD THEN BE ACCESSED BY OTHER APPLICATIONS, INCLUDING POTENTIALLY MALWARE. SO ADRIAN, COULD YOU GIVE A BACKGROUND ON THE REASONS WHY GOOGLE DECIDED TO INCLUDE THAT KIND OF FUNCTIONALITY IN THE SYSTEM? AND THE REASONS AND THOUGHT PROCESSES BEHIND EVENTUALLY DEPRECATING THAT API.

>> BEFORE I START, THANK YOU FOR HAVING US HERE. I'M ACTUALLY REALLY EXCITED TO BE HERE FOR A VARIETY OF REASONS BUT NOT LEAST OF WHICH IS I THINK THIS IS THE FIRST TIME I'VE SEEN A PANEL IN THE MOBILE SPACE THAT HAS ALL OF US AT A TABLE, IN THE SAME ROOM, MUCH LESS AT THE SAME TABLE. PANEL EARLIER TODAY SIMILARLY PROBABLY ONE OF THE MOST IMPRESSIVE PANELS I'VE SEEN DISCUSSING MALWARE IN TERMS OF RANGE OF INFORMATION THAT WAS BROUGHT TO BEAR. THIS IS REALLY IMPRESSIVE. I THINK IT'S GREAT TO SEE THIS KIND OF VISIBILITY BEING INTRODUCED IN TO A SPACE THAT HISTORICALLY HAS BEEN EXTRAORDINARILY CLOSED. ANDROID FOCUSED ON OPENNESS FROM THE BEGINNING. I THINK WE HAVE SEEN THE OTHER PLATFORMS REGARDLESS OF WHAT THEIR MODEL LOOKS LIKE, ALSO BRING A LOT OF OPENNESS TO THE MOBILE ECOSYSTEMS, VERY EXCITING TO SEE THAT. ALSO BEGINNING TO REALIZE THESE AREN'T JUST TECHNOLOGICAL PROBLEMS. THESE ARE REALLY PROBLEMS THAT
HAVE SOME TECHNOLOGY ELEMENT BUT
HAVE POLICY ELEMENTS AND REALLY
REQUIRE A LOT OF ENGAGEMENT.
IT'S EXCITING TO BE HERE, TO BE
ABLE TO PARTICIPATE IN THAT AND
TO BUILD THAT UP.
WITH RESPECT TO SPECIFIC
PLATFORM DECISIONS, THEY'RE
VERY, VERY CHALLENGING.
I THINK THIS IS TRUE NO MATTER
HOW OPEN OR CLOSED YOU WANT TO
MAKE YOUR PLATFORM.
WE HAVE BUILT A MULTI-TIERED
SECURITY MODEL.
I THINK WILLIAM DID A
SPECTACULAR JOB OF DESCRIBING
IT.
WHAT'S INTERESTING IS I THINK
IT'S VERY CONSISTENT ACROSS ALL
OF THE PLATFORMS.
ALMOST EVERYONE OF THE PLATFORMS
TO A T HAS BEEN VERY SUCCESSFUL
IN TAKING LEARNING FROM PREVIOUS
ENVIRONMENTS WHETHER IT'S THE
DESKTOP OR WE ACTUALLY LEARNED A
LOT EARLIER WHEN THEY WEREN'T
DESKTOP, WHEN WE WERE BUILDING
FOR LINUX AND SERVER
INFRASTRUCTURE.
TAKING, THAT BUILDING SERVICES
AND BUILDING PLATFORM LEVEL
SECURITY MODELS THAT PROTECT
USERS.
FOR ANDROID, THAT COMES IN A
FORM OF REVIEWING OF
APPLICATIONS SUBMITTED IN TO
GOOGLE PLAY, BRIEFLY CALLED
ANDROID MARKET.
SIMILARLY, EXTENDED THE
CAPABILITY TO PROVIDE INTEGRATED
IN TO THE OPERATING SYSTEM THE
ABILITY TO USE THAT TO CHECK
APPLICATIONS YOU MIGHT BE
INSTALLING EVEN IF YOU'RE
GETTING THEM FROM OUTSIDE OF
GOOGLE PLAY.
WE'RE BUILDING THE KNOWLEDGE USING THE DATA BEING PROVIDED IN GOOGLE PLAY, AWARENESS WHO HAVE THE DEVELOPERS, ARE TYPES OF APPLICATIONS BEING BUILT, WHAT ARE LEGITIMATE ACTIVITIES VERSUS MAYBE NOT SO LEGITIMATE LOOK BEING ACTIVITIES. THEN APPLYING THAT KNOWLEDGE TO APPLICATIONS THAT ARE BEING DELIVERED TO OTHER PLACES AS WELL.

AT THE SAME TIME, WE STARTED AT A PLATFORM LEVEL WITH THE FOUNDATION OF SANDBOXING, WHICH IT WAS ORIGINAL QUESTION, WHERE WE PROVIDED A VERY SELECT SET OF APIs AVAILABLE TO DEVELOPERS TO BUILD THEIR APPLICATION. WITH EVERY SINGLE ONE OF THESE APIs, THERE'S A VERY LENGTHY DISCUSSION, APIs, VERY LENGTHY DISCUSSION.

IN A MEETING WITH THE FRAMEWORKS TEAM TALKING ABOUT A SPECIFIC API I WAS ADVOCATING FOR, I WAS TOLD EVERY MISTAKE WE EVER MADE STARTED WITHIN WE PROVIDED AN API. USE THE FRAMEWORKS TEAM, THAT'S WHAT HIS TEAM DOES. IT'S TRUE, EVERY MISTAKE THEY EVER MADE STARTED WITH PROVIDING AN API. READ LOGS IS A VERY INTERESTING EXAMPLE WHERE OUR EXPECTATION FOR HOW IT WAS GOING TO BE USED CHANGED. WE LEARNED FROM DATA THAT WAS INTRODUCED AND WE CHANGED HOW WE PROVIDED IT TO DEVELOPERS. SPECIFICALLY, EARLY ON IN THE ANDROID PLATFORM VERY FOCUSED ON MAKING THE PLATFORM OPEN AND FLEXIBLE FOR DEVELOPERS. THIS WAS AN API TO ALLOW
DEVELOPERS TO MONITOR ENVIRONMENT AROUND APPLICATIONS TO SEE WHERE BUGS MAY BE INTRODUCED. THAT'S WHAT WE SAW EARLY APPLICATIONS USED FOR. WE THEN SAW BROADENING. ONE OF THE DOMINANT USERS WAS SECURITY COMMUNITY BECAUSE IT GAVE THEM THE ABILITY TO SEE WHAT OTHER APPLICATIONS WERE DOING ON THE DEVICE. THAT SEEMED LIKE A GOOD THING. THEN WE STARTED TO SEE INSTANCE WHERE'S THAT VISIBILITY PRESENTED THE POSSIBILITY OF THE ACCIDENTAL LEAKAGE OF INFORMATION. THAT'S WHAT WE SAW HAPPENING MORE RECENTLY AND AS WE STARTED TO SEE ACCIDENTAL LEAKAGE OF INFORMATION, THEN WE MADE A DECISION TO NARROW DOWN THE SCOPE OF THE INFORMATION TO PROTECT THE USER. AT THIS POINT THE API EXISTS, PROVIDED TO DEVELOPERS, SO THEN MONITOR BEHAVIOR OF THEIR OWN APPLICATION BUT NOT THE ABILITY TO MONITOR OR VIEW DATA PUT IN TO THE LOGS VOLUNTARILY BY OTHER APPLICATIONS BECAUSE WE SAW APPLICATION DEVELOPERS WHO DIDN'T REALIZE HOW MANY OTHER APPLICATIONS WERE WORKING. >> SOUNDS LIKE YOU'RE SAYING THIS IS TO SOME DEGREE A REACTIVE PROCESS WHERE YOU WATCH WHAT APPLICATIONS ARE DOING AND MAKE ADJUSTMENTS ACCORDINGLY. >> ABSOLUTELY. IT'S CRITICAL, TRUE FOR ANY PLATFORM PROVIDER, LOOK AT WHAT YOUR APPLICATIONS DO OUR PLATFORM. YOU ADD NEW API, ADJUST APIs
THAT EXIST.
ULTIMATELY SECURITY COMES DOWN TO THAT.
IT COMES DOWN TO LOOKING AT THE DATA, MAKING DECISIONS ABOUT WHERE TO ADD, ADJUST.
>> THANK YOU.
MICHAEL, LET ME TURN THIS TO YOU.
DO YOU THINK THAT THERE'S THE POTENTIAL AS A FUTURE OPERATING SYSTEM, I THINK YOU GUYS ARE STILL TO ONLY DEGREE DEVELOPING AND GETTING YOUR POLICIES IN TO PLACE, DO YOU THINK THAT THERE IS THE POTENTIAL TO BE MORE PROACTIVE IN THINKING ABOUT SECURITY AND API DESIGN?
I KNOW YOU GUYS HAVE STATED IN YOUR DOCUMENTATION YOU ARE NOT GOING TO MAKE FOR EXAMPLE THE TELEPHONY API AVAILABLE TO THIRD PARTY APPLICATION.
CAN YOU DISCUSS THAT AND THE REASONING FOR THAT POTENTIALLY ANY TRADE-OFF.
>> AGAIN, I WOULD BE REMISS TO START WITHOUT SAYING THIS IS A GREAT OPPORTUNITY TO CHAT ABOUT THESE ISSUES.
ONE OF THE BENEFITS OF WHERE WE ARE DEVELOPING FIRE FOX NOW IS LOOKING AT WHAT HAVE WE LEARNED?
WHAT HAVE OTHER PEOPLE TRIED?
WHAT'S GONE RIGHT?
WHAT'S GONE WRONG?
BEFORE WE GET TO DETAILS, ONE OF THE DIFFERENT THINGS ABOUT THE WAY WE BUILT FIRE FOX TO SET THE STAGE, IS IT'S ALL BUILT FROM THE WEB, ALL WEB TECHNOLOGY.
SO EVERYTHING YOU SEE THE HOME SCREEN, YOUR HOME SCREEN, IT'S ALL BUILT WITH HTML.
SO WHAT WE'RE DOING IS TAKING A LOT OF THE LESSONS WE LEARNED
OVER THE LAST 10-PLUS YEARS OF
FIRE FOX AND BRINGING THOSE TO
THE MOBILE DEVICE.
WE'RE NOT NECESSARILY
REINVENTING THE WHEEL, BUT WE'RE
TRANSLATING THINGS WE LEARNED IN
TO A NEW PARADIGM: THE API
FRONT, ONE OF THE MAIN ITEMS IS
PROTECTING USER DATA.
THAT'S NOT THE SAY ANYONE ELSE
IS NOT FOCUSING ON THAT.
WHAT WE WANT TO DO IS REALLY
LOOK AT HOW DOES THE USER MAKE
THE DECISION OF WHEN TO SHARE
DATA WITH APPLICATIONS?
AND WHAT DO THEY UNDERSTAND WHEN
THEY'RE MAKING THAT DECISION?
SO WE FELT THAT ONE APPROACH
THAT'S BEEN TRIED IS PROMPTING
USERS WITH A LIST OF
PERMISSIONS.
FROM OUR PERSPECTIVE THAT'S
CHALLENGING FOR USERS TO
UNDERSTAND WHAT THEY'RE EXACTLY
AGREEING TO.
THEY WANT TO INSTALL AN
APPLICATION, SEE A LARGE LIST OF
PERMISSIONS.
UNFORTUNATELY THINK A LOT OF
USERS JUST CLICK ON, GET THIS
APPLICATION RUNNING.
CLICK OKAY, GET THIS APPLICATION
RUNNING.
OUR APIs WILL PROMPT USERS AT
RUN TIME FOR SENSITIVE DATA.
IF YOU USE AN APPLICATION,
LOOKING FOR RESTAURANTS IN THE
NEARBY AREA, IT WOULD MAKE SENSE
THAT THAT APPLICATION WOULD SAY,
I WOULD LIKE YOUR GEOLOCATION, I
WOULD LIKE TO KNOW WHERE YOUR
WOULD YOU MOST LIKELY SAY YES,
THAT MAKES SENSE.
BUT AT THE SAME TIME IF YOU'RE
PLAYING A VIDEO GAME AND THE
VIDEO GAME SUDDENLY SAYS GO TO
THE NEXT LEVEL, I WOULD LIKE TO ACCESS YOUR CONTACTS, I WOULD LIKE TO SEND YOUR MOM AN E-MAIL, YOU WOULD MOST LIKELY SAY. NO THAT'S THE PARADIGM SHIFT FORKS API THAT SEND INFORMATION, CAMERA, VIDEO, CONTACTS, PRESENT IT TO THE USERS IN A WAY THEY UNDERSTAND SO THEY CAN MAKE INFORMED DECISIONS. THAT'S ONE OF THE LARGER ISSUES THAT WE'RE LOOKING TO ASSIST IN.

>> OKAY.

SO THAT MEANS GOING BACK TO THE ORIGINAL QUESTION ON THE PHONE DIALER, WON'T LET YOU GET AWAY THAT QUICKLY.

>> FOR THE PHONE DIALER, VERY GOOD POINT, SO WE HAVE A NOTION OF DIFFERENT PERMISSION LEVELS FOR APPLICATIONS. SOMETHING LIKE PHONE DIALER WOULD BE RESTRICTED TO THE MOST PRIVILEGED APPLICATIONS THAT TYPICALLY PUT ON BY THE OEM. THE REASON WE DO IT THAT WAY IS THE PHONE DIALER IS SO SENSITIVE THAT IF SOMEONE WAS TO MAYBE A MISTAKE, LOSE PHONE FUNCTIONALITY, YOU HAVE A BIG PROBLEM. THOSE APPS ARE THOROUGHLY REVIEWED TO MAKE SURE WE DO THINGS CORRECTLY.

IF AN APPLICATION WANTS TO PERFORM PHONE FUNCTIONAL, EXPOSE THAT THROUGH WEB ACTIVITIES. IMAGINE YOU WANT TO MAKE A PHONE CALL IN A DIFFERENT APP, CLICK ON SOME NUMBER, IT WOULD USE THE WEB ACTIVITY TECHNOLOGY TO THEN PROMPT, POPULATE THE NUMBER IN TO THE DIALER. AT THAT POINT ARE YOU USING THE PHONE DIALER BUILT BY THE OEM AND REVIEW, THAT WE KNOW IS
SECURE, WHERE YOU CAN THEN DIAL
THE NUMBER THROUGH THERE.
THE TECHNOLOGY, WEB ACTIVITY TO
EXPOSE SENSITIVE ITEMS TO OTHER
APPLICATIONS.
>> OKAY.
THAT MAKES SENSE.
IT'S A TRUSTED UI MECHANISM.
>> EXACTLY.
>> AND ADRIAN, HAS GOOGLE
EXPERIMENTED WITH MORE
TRUSTED UI MECHANISMS IN TERMS
OF BEING ABLE TO EXPOSE
FUNCTIONALITY WITHOUT
NECESSARILY CREATING DIRECT
ACCESS TO CERTAIN APIs?
>> THERE ARE LOTS OF INTERESTING
ANALOGUES TO DRAW, NOMENCLATURE
BASED.
I WROTE WEB ACTIVITY EQUALS
INTENT.
I THINK I BELIEVE THAT'S
ACTUALLY FAIRLY GOOD
REPRESENTATION.
WE HAVE DIFFERENT MECHANISMS FOR
APIs.
A GOOD EXAMPLE IS TELEPHONY, YOU
CAN SEND INTENT TO THE DIALER,
THAT WOULD ALLOW DIALING OF THAT
PHONE NUMBER USING THE BUILT-IN
PHONE APPLICATION.
BUT WE FOUND THAT THERE ARE LOTS
OF INSTANCE WHERE'S THERE ARE
VERY VALUABLE APPLICATIONS
PRODUCED BY THIRD PARTIES THAT
MODIFY THE DIALER T FACEBOOK
APPLICATION WAS VERY PROMINENT
RECENTLY WITH EXCELLENT EXAMPLE
OF THE TYPES OF INNOVATION THAT
ARE CAPABLE WHEN WE PROVIDE API
TO CELL SERVICE, ONE REASON
WE'RE EXCITED TO PROVIDE AN OPEN
PLATFORM SO YOU CAN SEE THAT
KIND OF AMBITION.
>> SO GOING BACK TO THIS
QUESTION OF PERMISSIONS AND WHETHER USERS ARE ACTUALLY PAYING ATTENTION, WHETHER THIS HAS BEEN EFFECTIVE SECURITY MECHANISM. WILL, CAN YOU GIVE US SOME BACKGROUND IN TERMS OF WHAT'S BEEN SHOWN IN ACADEMIC RESEARCH ON THAT WE?

>> THERE HAVE BEEN A FEW USER STUDIES LOOKING AT THROUGH WHETHER OR NOT USERS COMPREHEND WHETHER THE PERMISSIONS PROVIDED TO THEM. I THINK THE GENERAL CONSENSUS OF THE ACADEMIC COMMUNITY IS THAT GENERAL USERS DO NOT SPECIFICALLY LOOK AT PERMISSIONS. IF THEY DO, THEY DON'T NECESSARILY UNDERSTAND WHAT A PERMISSION IS GOING TO DO IN AND OF ITSELF. ALTHOUGH I THINK THAT THERE IS A GOOD REASON TO SORT OF TAKE THAT IN A BROADER PERSPECTIVE AS WELL IN TO WHAT IS THE ACTUAL VALUE OF THESE PERMISSIONS IN AS I MENTIONED BRIEFLY WHEN I WAS GIVING YOU THE OVERVIEW, ONE OF THE REALLY VALUABLE PIECES OF SHOWING THE USER PERMISSION IS IT ENABLES WHISTLE-BLOWERS. PEOPLE WHO ARE MORE EXPERTS IN AN AREA TO SEE WHAT AN APPLICATION MIGHT DO AND MAYBE INVESTIGATE THAT A LITTLE BIT FURTHER. THERE WAS A VERY INTERESTING STUDY AT A CONFERENCE EARLIER THIS YEAR THAT LOOKED AT THE SAME APPLICATION IN BOTH ANDROID AND iOS SORT OF LOOKING AT THE FREE VERSIONS OF THESE APPLICATIONS. THEY LOOKED AT WHAT ARE THE
APIs?
THE API SENSITIVE?
PRIVACY SENSITIVE, SECURITY
SENSITIVE INTERFACE.
THEY FOUND ON THE WHOLE, THAT
THE iOS APPLICATIONS ACCESSED
MORE PRIVACY SENSITIVE APIs.
SPECULATION YOU CAN MAKE FROM
THAT, I DON'T KNOW THAT YOU HAVE
SORT OF CAUSATION, DEFINITELY
CORRELATION, IS THAT HAVING
PERMISSIONS THERE GAVE A LEVEL
OF TRANSPARENCY THAT MAY HAVE
DISINCENTIVIZED.
WHETHER THAT'S CAUSE SDASHGS WE
DON'T HAVE EVIDENCE, WHETHER
THERE'S CAUSATION, WE DON'T HAVE
EVIDENCE BUT SECOND-LEVEL
ADVANTAGE EVEN THOUGH USERS
MIGHT NOT, ALL USERS MIGHT NOT
UNDERSTAND.
>> SO MICHAEL BROUGHT UP THIS
POINT OF WHAT HE SEES AS THE
ADVANTAGES OF RUNTIME
PERMISSIONS COMPARED TO INSTALL
TIME PERMISSIONS.
AND I NOTE, INSTALL TIME
PERMISSIONS.
THREE PLATFORMS HERE USING
INSTALL TIME PERMISSION,
WINDOWS, BLACKBERRY WENT FROM
RUNTIME PERMISSIONS TO INSTALL
TIME PERMISSIONS.
ADRIAN STONE, DO YOU HAVE
OPINIONS AS TO WHICH IS MORE
EFFECTIVE?
ARE USERS DO, THEY PAY ATTENTION
EITHER WAY?
OR THE BENEFITS OF PERMISSIONS
REALLY MORE OF THE SECOND LEVEL
BENEFITS THAT WILL IS TALKING
ABOUT RIGHT NOW?
>> FIRST, LET ME THANK YOU FOR
PUTTING ON THE EVENT AND
ALLOWING MICROSOFT TO ATTEND.
HAPPY TO BE HERE TO REPRESENT WINDOWS PHONE TEAM.
WE THOUGHT QUITE A BIT ABOUT PROMPTING AND HAVE QUITE A BIT OF AN EXPERIENCE FROM OUR DESKTOP SOLUTIONS AND ASKING USERS, ARE YOU SURE?
AND WE HAVE FOUND THAT IT IS NOT VERY EFFECTIVE.
TYPICALLY SOMETHING WE DO THAT'S A LAST RESORT KIND OF, IF IT'S LEGALLY REQUIRED, NOT SOMETHING WE LIKE TO DO.
THE NUMBERS THAT WE COLLECT REGULARLY SHOW THAT MOST USERS JUST BASICALLY PASS LIEU THE DIALOGUES.
PASS THROUGH.
THEY WANT WHAT'S ON THE OTHER SIDE.
COMPAARED TO GETTING BETWEEN MOTHER BEAR AND HER CUB KIND OF THING.
[LAUGHTER]
SO WE'RE LOOK AT TRUSTED UI AND WHAT MICHAEL IS TALKING ABOUT BEFORE, AS BETTER WAYS OF MAKING USERS UNDERSTAND WHAT'S GOING ON.
>> CAN YOU GIVE US A COUPLE EXAMPLES FROM WINDOWS PHONE AS TO HOW TRUSTED UI?
>> FOR CONTACT ACCESS INSTEAD OF GIVING ACCESS TO API WE SHOW A USER EXPERIENCE THAT THE USER PICKED CONTENT.
>> SO THERE'S NO WAY TO AUTOMATICALLY UPLOAD ALL THE CONTACTS?
>> WE LIKE TO DO THAT MORE.
WE SEE THAT'S THE WAY FORWARD.
>> ADRIAN STONE, ANY THOUGHTS ON BLACKBERRY TRANSITION IN.
>> SURE, AGAIN, IN LINE WITH MY OTHER COLLEAGUES, DEFINITELY APPRECIATIVE OF ALL OF US BEING
AT ONE TABLE.
LIKE ADRIAN, THE FIRST TIME I'VE HAD THAT OPPORTUNITY TO THANK YOU.
ECHOING GEIR'S THOUGHTS, WE HAVE SEEN THE SAME THING.
DATA SHOWS US USERS WILL ALMOST PAVLOVIAN STYLE CLICK THROUGH THINGS.
YOU CAN DEBATE EFFICACY OF THE DIALOGUE IF YOU WILL, WITHOUT BEING ABLE TO SET CONTEXT.
SO WHEN WE LOOK AT AS WE HAVE REINVENTED OUR PLATFORM WITH BLACKBERRY 10, YOU BRING UP THE CHANGE FROM RUNTIME BUT AT THE SAME TIME WE HAVE TRIED TO ESTABLISH MORE CONTEXT IN TERMS OF WHAT THE APPLICATIONS ARE DOING.
IN MANY WAYS, MAKE IT IN A WAY TO THE USER THAT IS SEAMLESS.
WHEN I THINK ABOUT SANDBOXING AND I THINK ABOUT APP CONTAINIZATION, WITH BLACKBERRY BALANCE FOR EXAMPLE, WE HAVE TAKEN OUR TRUSTED AREAS OF THE OPERATING SYSTEM SPECIFICALLY FOR OUR BUSINESS TYPE ENVIRONMENTS WHERE WE SAID THIS STYLE OF APPLICATION IS THAT ACCESSING CERTAIN TRUSTED APIs, WE WON'T BUSINESS-TYPE ENVIRONMENTS WHERE WE'VE SEEN THIS STYLE OF APPLICATION THAT IS ACCESSING CERTAIN TRUSTED APIs.
WE JUST WON'T ALLOW THE FUNCTION THERE OR WON'T ALLOW THE COPYING OF DATA FROM ONE APPLICATION SPACE TO ANOTHER.
IF I'M RUNNING FACEBOOK ON MY BLACKBERRY, I WON'T HAVE TO WORRY ABOUT THE INFORMATION THAT WOULD TYPICALLY BE ACCESSED FOR MY CORPORATE DATA TO BE ACCESSED
IN THE -- THE USER SPACE, 
PERSONAL USER SPACE VERSUS WHAT 
WE CALL THE WORK SPACE. 
SO REALLY IT'S ABOUT CONTEXT FOR 
US. 
I ALSO THINK, YOU KNOW, ANOTHER 
POINT THAT ADRIAN MADE THAT IS 
ON TARGET, YOU HAVE TO GO BACK 
THROUGH AND DO ANALYSIS AND YOU 
HAVE TO TRIM THE WAY THAT YOU'RE 
DOING THINGS. 
AS WE LOOK AT THE THREAT CURVE 
OVER TIME, WE'LL GO BACK THROUGH 
AND RE-EVALUATE. 
THAT'S WHAT WE DID HERE. 
WE DIDN'T SEE A RETURN THAT 
WOULD HAVE BEEN EXPECTED BY 
HAVING THAT RUN TIME. 
>> ALL RIGHT. 
THANK YOU. 
SO JANE, TURNING TO YOU FOR A 
MINUTE. 
YOU KNOW, BOTH ADRIANS NOW HAVE 
DISCUSSED -- 
>> VERY RARELY -- 
>> WEIRD TALKING ABOUT YOURSELF 
IN THIRD PERSON, 
>> THE ADRIANS HAVE DISCUSSED 
GOING BACK AND PUTTING IN, YOU 
KNOW, LIMITATIONS ON API ACCESS. 
THIS WAS SOMETHING THAT IOS 
RECENTLY DID WITH IOS 6. 
THERE WERE INCREASED LIMITATIONS 
ON ACCESS TO THINGS LIKE THE 
ADDRESS BOOK AND THE DATABASE. 
1 -- ONE OF THE ISSUES TO 
EXPLORE HERE, WHAT CAN YOU DO 
PURELY THROUGH A REVIEW 
MECHANISM OF APPs AND WHAT YOU 
REALLY NEED HARD BUILT-IN 
TECHNICAL FIXES FOR. 
AND SO I THINK A LOT OF PEOPLE, 
YOU KNOW, EXPECTED THAT APPLE 
WAS DOING INTENSIVE REVIEW THAT 
WOULD CATCH ANY SORT OF 
POTENTIAL MISUSE THAN API.
AND YOU KNOW, APPLE IS A DIRECTION OF A MORE ROBUST PERMISSION SYSTEM THAN IOS 6. YOU ENDED UP DECIDING THAT YOU NEEDED A TECHNICAL MECHANISM THERE TO HELP STOP THESE ABUSES. CAN YOU DISCUSS THAT A LITTLE BIT AND THE THOUGHT PROCESS THERE?

>> YEAH, FIRST I WANT TO ALSO THANK YOU FOR INVITING APPLE. I'M VERY PLEASED TO BE PARTICIPATING WITH ALL THE OTHER PLATFORMS. I WOULD SAY WE IMPLEMENT A MULTIFACETED SYSTEM. FIRST WE HAVE OUR DEVELOPER PROGRAM SO IN ORDER TO EVEN PUT AN APP IN THE APP STORE, YOU HAVE TO GO THROUGH THE DEVELOPER PROGRAM AND AGREE TO THE APPLE STORE GUIDELINES AND THE DEVELOPER AGREEMENT. AND IN THAT AGREEMENT WE HAVE CERTAIN REQUIREMENTS WITH RESPECT TO THE COLLECTION OF USER DATA. AND ABOUT TWO YEARS AGO, WE DECIDED THAT WE WOULD DO WHAT WE CALL ISOLATE THE LOCATION API, WHICH MEANT THAT WE POPPED UP A CONSENT BOX AT JUST IN TIME NOTICE. SO AT THE TIME THE LOCATION WAS BEING COLLECTED, THE USER WOULD HAVE THE IDEA OF WHY THE LOCATION WAS BEING COLLECTED. WE FOUND THAT THAT WAS A REALLY EFFECTIVE WAY OF COMMUNICATING TO USERS. AND THE BEAUTY OF THIS, IT'S BLIND TO THE APP. AS WE'VE ROLLED OUT THESE PERMISSIONS IN IOS 6, WE COULD DO THIS FOR CONTACTS, CALENDARS, REMINDERS AND PHOTOS AT JUST THE
TIME OF ACCESS.
THE OTHER THING THAT WE ROLLED OUT WITH IOS 6 TO IMPROVE THE
UNDERSTANDING THE PURPOSE OF USERS WAS THE PURPOSE STRING.
IT'S NOT ONLY TO SAY THIS APP WOULD LIKE THE PHOTOS.
THE APP CAN SAY WHY THEY WANT TO ACCESS THE PHOTOS.
IT MAKES IT MORE CLEAR TO THE USER.
FOR US, IT WAS THE BEAUTY OF THE OPERATING SYSTEM.
THE OPERATING SYSTEM COULD DO IT WITHOUT ANY ADDITIONAL CODING BY DEVELOPERS.
>> THANKS.
THAT'S A REALLY INTERESTING POINT, TO BRING OUT THE PURPOSE STRING.
FIRE FOX IOS IS GOING TO IMPLEMENT SOMETHING SIMILAR, I BELIEVE.
AM I RIGHT THAT IN FIRE FOX OS, YOU SAID THAT IN IOS IS AN OPTION STRING.
IN FIRE FOX OS IT'S A MANDATORY STRONG?
>> YEAH, IT'S, AGAIN, TERMINOLOGY IS CALLED DATA INTENTIONS.
THE IDEA IS TO STRENGTHEN THAT CONTEXT, THAT WHEN YOU GET A DIALOGUE BOX ASKING TO GRANT ACCESS TO CAMERA OR PHOTOS OR WHAT HAVE YOU, THAT THE DEVELOPER HAS A CHANCE TO SAY WHY.
BECAUSE IT CAN BE A BIT MISLEADING IN THE BOX POPS UP, EVEN TOTALLY LEGIT, THE CONTEXT CAN BE CONFUSING THAT IS A REQUIRED PIECE OF INFORMATION THAT WE USE SO THE USER EXPERIENCE IS STRONG BUT ALSO SO
WE AS THE REVIEW PROCESS IN THE MARKETPLACE CAN LOOK THROUGH AND SAY, THIS IS THE INTENT OF WHAT YOU'RE DOING. LET'S SEE IF WE CAN HELP YOU. IF YOU'RE TRYING TO ACCOMPLISH IT THIS WAY, LET'S MAKE SURE YOU DO WHAT YOU SAY. AND IF FOR SOME REASON THAT YOU'RE MALICIOUS, THAT WILL GIVE US INFORMATION THAT WILL HELP US TRACK DOWN. YOU SAY YOU'RE DOING SOMETHING BUT YOU'RE DOING SOMETHING DIFFERENT. LET'S MAKE SURE THAT WE'RE NOT LETTING AN INSECURE AM OR MALICIOUS APP INTO THE APP STORE.

>> DO YOU HAVE ANY THOUGHTS ON THE EFFICACY OF THESE DATA INTENTION STRINGS? YOU THINK THAT'S A USEFUL MECHANISM FOR USERS TO UNDERSTAND WHAT AN APPLICATION IS FOR AS A REVIEW PROCESS? ESPECIALLY IN TERMS OF, YOU KNOW, DETECTING ACTUAL MALWARE. >> IT COULD BE. I THINK -- YOU KNOW, ONE OF THE BIGGEST THREATS TO SECURITY WHERE I FIND MOST SECURITY ISSUES IS WHEN THERE'S INCONSISTENCY. INCONSISTENCY TO ME IS KIND OF THE ROOT OF A LOT OF SECURITY ISSUES. INCONSISTENCY NOT ONLY WITHIN THE PLATFORM BUT ACROSS THE SPACE. IF WE'RE LOOKING TO DEVELOPERS TO KIND OF -- IT'S GOING TO BE DEVELOPERS THAT ARE FULLY CAPABLE OF DOING THAT AND VERY BENEFICIAL TO THE END USER AND THEN THERE'S OTHERS THAT ARE NOT
GOING TO BE THAT GOOD AT IT AND END UP CONFUSING.
>> SO IT'S REALLY AN ISSUE OF WHETHER THE DEVELOPER CAN COMMUNICATE THE MESSAGE APPROPRIATELY TO THE END USER.
SO YOU KNOW, WITH BOTH -- WITH WINDOWS PHONE AND ADRIAN -- BOTH ADRIANS WITH BLACKBERRY AND ANDROID, I THINK THAT THIS ISN'T SOMETHING THAT YOU'VE REALLY IMPLEMENTED INTO YOUR SYSTEMS.
I KNOW THAT WITH ANDROID, IF A APPLICATION CREATES ITS OWN PERMISSION, THEN IT CAN PROVIDE INFORMATION ON WHAT THAT PERMISSION WOULD ALLOW ACCESS TO.
BUT OTHERWISE, THERE'S NO ACTUAL DATA USAGE INTENTION OF ABILITY.
WHAT WAS THE -- WHAT'S THE REASON FOR DOING THAT IS SOMETHING THAT YOU WOULD CONSIDER PUTTING INTO PLACE.
YOU THINK IT WOULD BE USEFUL?
ANYONE CAN GO FIRST.
>> WELL, FROM MY PERSPECTIVE, PART OF THE REAL QUESTION IS HOW DO YOU INCENTIVIZE THE REAL DEVELOPERS.
TO BE CLEAR, CONCISE IN THEIR INTENT.
AND HOW DO YOU MAKE IT CLEAR FOR USERS TO BE ABLE TO MAKE THAT TRACE.
GOING BACK TO THIS CONTEXT PART THAT WE'VE TALKED A LOT ABOUT.
I ALWAYS USE MY DAD AS THE PERFECT LITMUS TEST IN WHAT A USER CAN DO.
IF MY DAD INSTALLS A FLASHLIGHT APP, WE HAVE 5,000 OR 10,000 FLASHLIGHT APPs HOW DO YOU KNOW WHAT ONE TO GET?
AND I THINK LAZY IS AN INCORRECT TERM.
IT'S THERE'S EFFICIENTLY AS
POSSIBLE TRYING TO GO PRODUCE
THEIR APPLICATION AND USING ALL
OF THE PERMISSIONS THAT THEY
HAVE AVAILABLE TO THEM.
SO HOW DO YOU INCENTIIZE THAT
DEVELOPER UNDER A CONCEPT OR
PRIVILEGE?
WHAT'S THE LEAST AMOUNT YOU NEED
TO DEVELOP YOUR APPLICATION?
AND HOW DO YOU TAKE TO IT THE
NEXT STEP OF THAT WHICH TELLS
THE USER THIS APPLICATION IS
TRUSTED BECAUSE IT IS ALSO
DEVELOPED WITH THAT IN MIND.
SO FROM MY PERSPECTIVE -- WE'RE
DOING A LOT OF INVESTMENT TRYING
TO WORK WITH THE DEVELOPER
COMMUNITY TO HELP THEM TO
UNDERSTAND THAT IF YOU'RE GOING
TO GO WRITE A FLASHLIGHT APP,
HERE'S WHAT THE BASELINE
BEHAVIORS OF EXPECTATION SHOULD
BE.
HERE'S HOW WE EXPECT FOR YOU TO
COMMUNICATE THAT TO THE USER.
HERE'S HOW WE'RE LOOKING NOT
JUST ON THE DEVICE BUT IN THE
APP STORE TO COMMUNICATE THE
BEHAVIORS OF THE APPLICATION.
THERE'S A LOT OF THINGS WORKING
ON THERE.
BUT YOU HEAR TERMS -- BRETT DOES
A GREAT JOB AT ADOBE TALKING
ABOUT THEIR OWN IN-HOUSE
DEVELOPERS AND EMBRACING
SECURITY.
THAT'S ONE OF THE THINGS WE'RE
LOOKING AT, TAKING THAT TYPE OF
APPROACH IN ADDITION TO THE
PLATFORM PROTECTIONS TO
INCENTIIZE DEVELOPERS TO DO THE
RIGHT THING.
A LOT OF TIMES IT'S OUT OF
IGNORANCE.
>> SO ONE OF THE THINGS THAT WE
FOCUSED ON A LOT WITH ANDROID IS INCREASING TRANSPARENCY TO CONSUMERS.
ONE OF THE REASONS IT'S IMPORTANT FOR US TO PROVIDE PERMISSIONS PRIOR TO INSTALLATION IS THAT'S THE POINT AT WHICH THE CONSUMER IS MAKING A DECISION.
DO I WANT TO INSTALL THIS THING OR NOT.
WE LIKE TO THINK OF THIS AS THE TYPE OF INFORMATION THAT WOULD BE ON THE BACK OF A MOVIE WHEN YOU GO TO RENT IT.
WHO IS THE ACTOR, WHAT IS THIS MOVIE ABOUT, WHAT INFORMATION IS AVAILABLE.
BUT KEY BEING THAT IT'S SOMETHING THAT IS TRUSTED BECAUSE IT'S PROVIDED BY THE PLATFORM.
I'M FASCINATED BY THIS IDEA OF PURPOSE.
IT'S SOMETHING THAT WE'VE DISCUSSED REPEATEDLY WITHIN ANDROID.
I DIDN'T REALIZE THERE WAS A PLATFORM THAT WAS IMPLEMENTING IT.
I APOLOGIZE FOR MY IGNORANCE ON THE SUBJECT.
I WANT TO TAKE THE REST OF THE AUDIENCE THROUGH THE COMPLEXITIES.
ANDROID IS DELIVERED ON HUNDREDS OF DEVICES IN HUNDREDS OF DIFFERENT COUNTRIES.
SUPPORTS DOZENS OF LANGUAGES.
EVERY STRING YOU SEE HAS TO BE TRANSLATED.
I HAD THE GREAT PLEASURE OF WRITING ONE OF THE PERMISSION STRENGTHS NOT TOO LONG AGO.
AND THEN HAVING SIX DIFFERENT PEOPLE TELL ME THAT WHAT I HAD
WRITTEN COULDN'T BE TRANSLATED INTO THEIR LANGUAGE. WHICH WAS ON TOP OF THE FACT THAT WE WENT THROUGH MULTIPLE EDITS TO GET IT TO WORK IN ENGLISH. SO TO EXPECT THAT A DEVELOPER COULD DO THAT AND THEN REACH A GLOBAL AUDIENCE WITH THEIR APPLICATION, IT'S AN EXTRAORDINARY OPPORTUNITY FOR THAT DEVELOPER TO LEARN A LOT ABOUT THEIR CUSTOMER BASE. AND TO LEARN A LOT ABOUT SOME OF THE SMALLER COUNTRIES AND ET CETERA, ET CETERA. REGULATORY RESTRICTIONS. IT'S REALLY INTERESTING. WHAT COMES OF INCREASING TRANSPARENCY. THAT SAID, TO GEIR'S POINT, IT COULD BE GOOD. IS THIS AN EFFECTIVE ADDITIONAL MEASURE? THE IDEA OF KNOWING MORE ABOUT WHAT THE DEVELOPER THINKS THEY'RE GOING TO DO WITH DATA OR WHAT IS GOING ON THE APPLICATION, THAT KIND OF TRANSPARENCY TO US AND SUBSEQUENTLY TO THE USER ABOUT TO GET THE APPLICATION CAN BE IMPORTANT. AT THIS POINT WE DON'T KNOW. I'M EXCITED TO SEE THERE'S SOMETHING GOING TO DO EXPERIMENTS FOR US AND WE'LL FIND OUT WHETHER OR NOT THAT'S A NET POSITIVE. I'M VERY EXCITED TO FIND OUT. >> SO ADRIAN IS DONE. YOU MENTIONED THE IDEA OF LEASE PRIVILEGE PRINCIPAL. EVERY APP SHOULD HAVE PRIVILEGES THAT THEY NEED TO PERFORM THE FUNCTIONS.
THE IDEA BEHIND THIS IS THAT IT REDUCES A TAX SURFACE. SO THAT IF ANOTHER APPLICATION TRIES TO TAKE ADVANTAGE OF THE APP, YOU KNOW, THERE'S GOING TO BE FEWER VULNERABILITIES THAT WOULD BE EXPOSED. SO GEIR, I WANTED TO DISCUSS SOMETHING THAT YOU TRIED TO DO IN WINDOWS PHONE 7 AND THAT PERHAPS DIDN'T WORK BECAUSE YOU CHANGED IT IF WINDOWS PHONE 8. THAT WAS THE AUTOMATIC DETECTION OF CAPABILITIES WHEN AN APP WAS UPLOADED TO THE WINDOWS PHONE STORE. CAN YOU DISCUSS THE PURPOSE OF TRYING TO IMPLEMENT THAT AND THE CHALLENGES OF BACKING OFF? >> THIS IS ONE OF MY PERSONAL FAVORITES. I FEEL LIKE THAT'S THE MOTIVATING PRINCIPLE BEHIND A LOT OF THE WORK WE DO. WE NOT ONLY BUILT A BOX FOR THE THIRD PARTY DEVELOPERS BUT WE USE THE SOUND BOX HEAVILY. WE HAVE OVER 100 DIFFERENT APPLICATIONS AND EXPERIENCES ON THE PHONE. WE FEEL STRONGLY ABOUT THAT PRINCIPLE. IN WINDOWS PHONE 7, IT WAS POSSIBLE FOR US TO DO STATIC ANALYSIS ON APPLICATIONS AS THEY WERE ADJUSTED TO OUR APP STORE. BECAUSE THEY WERE MANAGED CODE. I'M USING TECHNOLOGY TERMS NOW. THE WAY THE LANGUAGE, THE APPLICATIONS WERE WRITTEN, ALLOWED US TO DO -- RUN CODE AND ANALYZE THE APPs AND WE COULD DETERMINE WHICH CAPABILITIES WERE NEEDED. BECAUSE WE COULD, THAT ALLOWED IT TO DETERMINE EXACTLY WHICH IS
OPTIMAL FOR THIS PRIVILEGE. WINDOWS PHONE 8, WE MOVE TO ALLOW A DIFFERENT LANGUAGE, NATIVE CODE, WHICH MAKES IT MORE COMPLICATED. SO IT WAS ONE OF A TECHNICAL CHALLENGE THAT WE COULDN'T OVERCOME RATHER THAN SOMETHING THAT WE BACKED OFF OF. WOULD LIKE TO DO IT -- WE'RE NOT REALLY ACCURATE ENOUGH WITH OUR DETECTION LOGIC AT THE MOMENT TO BE ABLE TO PULL IT OFF. >> INTERESTING. SO GENERALLY HOW OFTEN DO -- I GUESS ALL OF YOU MEET WITH THAT CHALLENGE WHERE YOU WANT TO DO SOMETHING SECURITY-WISE BUT IT'S TOO DIFFICULT TECHNICALLY TO ACTUALLY PULL OFF? >> WELL, I'LL JUMP IN HERE. I THINK THAT DAN AND HIS PREVIOUS AND PREVIOUS PANEL DID KIND OF A GREAT JOB OF ENUMERATING THE COST FOR AN ATTACKER. AND SO THERE ARE ALWAYS GOING TO GO -- TYPICALLY GOING TO GO TO THE AREA THAT PROVIDES THE MOST AMOUNT OF RETURN FOR THE LEAST AMOUNT OF WORK. THERE'S A LOT OF THINGS AS A SECURITY TEAM THAT MY ORGANIZATION WILL LOOK AT AND COME UP WITH A GREAT IDEA. OFTEN TIMES WE'LL GET THOSE IMPLEMENTED. BUT THEN -- WHAT WE REALIZE -- IT'S SIMILAR TO WHAT GEIR WAS JUST ENUMERATING. EITHER THE COMPLEXITY OF WHAT WE ORIGINALY ASSUMED WAS HIGHER OR IS HIGHER AND THEREFORE ATTACKERS ARE SO FOCUSED ON WHAT THE REAL WORLD ATTACKS ARE, HOW THE THREATS ARE EVOLVING.
I have to prioritize where the technology is not there yet or the community is not there yet. That's a natural part of the evolution process. That's something we do when we roll out code and develop our product, do that analysis.

Going to take that question a little bit of a different direction. Talking about technical challenges.

One of the things we've seen -- as many people know or maybe some don't, some nonprofit community-based companies speak. The interesting thing is we've seen some technical challenges. We reach out to the community at large. We're going to do the same thing with Fire Fox OS. Working on both exposing our marketplace via API so we can have security researchers analyzing the applications in there, looking at the permissions, looking for interesting trends or patterns that we either might not see and also looking at something called the Bug Value Program. We started out with Fire Fox in 2004.

And that's a way where we invite the best and brightest of community researchers for security in the world to find mistakes. You know, we do the best we can. We do a lot of great things. What is the newest thing you're thinking about. If you find that, bring that to us and let's work together and
FIX THAT TO MAKE THE WORLD SAFER.
YOU KNOW, IT'S OTHER OPTIONS WITH THAT.
SO -- SO THE TECHNICAL CHALLENGES, THEY'RE THERE.
AND I THINK IT'S A MATTER OF WHAT SORT OF CREATIVE SOLUTIONS YOU COME UP WITH TO REACH THE BEST AND BRIGHTEST MINDS.
>> GREAT.
SO YOU RAISE A VERY INTERESTING IDEA WITH THE BUG BOUNTY PROGRAM.
THIS IS SOMETHING THAT WE'VE SEEN USED BY A LOT OF COMPANIES IN THE WEB SPACE BUT NOT SO MUCH IN MOBILE.
AND I WAS WONDERING IF THE REST OF YOU CAN, YOU KNOW, GIVE A SENSE AS TO WHY YOU HAVEN'T THOUGHT IT WAS APPROPRIATE IN MOBILE OR SOME OF YOU MAY NOT THINK IS APPROPRIATE WITH ANY OF YOUR PRODUCTS.
IF YOU COULD DISCUSS THAT AND, YOU KNOW, THE REASONS FOR OR NOT HARNESING THE POWER OF RESEARCHERS AROUND THE WORLD. ANYONE?
>> I'LL JUMP IN.
SO I THINK BUG BOUNTY PROGRAMS SERVE THEIR PURPOSE. THEY PROVIDE VALUE. THERE'S A MULTITUDE OF WAYS TO COMPENSATE BRIGHT LIKE-MINDED INDIVIDUALS.
WHEN YOU LOOK AT THE MOBILE ENVIRONMENT, THERE'S SOME UNIQUE COMPLEXITIES TO THAT EQUATION. WHEN YOU TALK ABOUT IF THE END GOAL IS TO GOAL ADDRESS A VULNERABILITY ON THE PLATFORM, WHAT ARE YOU PAYING FOR IT AND HOW DO YOU GET DOWN TO THAT LAST MILE IN TERMS OF SECURING YOUR
CUSTOMERS.
SO I THINK, YOU KNOW, WHEN I
JUST LOOK AT THE ENTIRE PATCHING
EQUATION TODAY FROM MY
PERSPECTIVE, A VULNERABILITY
THAT IMPACTS ADRIAN'S PLATFORM
CAN VERY WELL ATTACK MY
PLATFORM.
A VULNERABILITY THAT IMPACTS
PLATFORM IS LIKELY TO IMPACT
MINE.
UNLIKE WHAT WE'VE SEEN IN THE
TRADITIONAL DESK TOP
ENVIRONMENT, WE ALL SHARE CODE
TO SOME EXTENT.
THAT'S KIND OF ONE INHERENT
CHALLENGE THAT A LOT OF US ARE
LOOKING OVER.
THE OTHER IS GETTING TO THE LAST
MILE OF UPDATE DELIVERY.
SO WHEN YOU MAKE THAT COMMITMENT
TO A RESEARCHER, TO ACCEPT THEIR
BUG, TO PAY THEIR BUG, PAY FOR
THEIR BUG, YOU ALSO WANT TO
HONOR THAT COMMITMENT OF BEING
ABLE TO SECURE THE CUSTOMERS AS
A RESULT OF THE BUG THEY
REPORTED SO I THINK THERE'S SOME
VERY UNIQUE COMPLEXITIES WHEN WE
TALK ABOUT MOBILE ENVIRONMENT
THAT ARE NOT NECESSARILY A ONE
TO ONE MAPPING ON THE DECK TOP
WORLD.
>> ADRIAN, I KNOW THAT GOOGLE,
THE CHROME PROGRAM HAS BEEN
REALLY BIG ON BUG BOUNTIES AND
WE HAVEN'T SEEN THE SAME IN
ANDROID.
WOULD YOU ECHO ADRIAN STONE'S
CONCERNS THAT THE THINKING IS
THERE?
>> I THINK YOU DESCRIBED SOME
DIFFERENCES BETWEEN THE DESK TOP
ENVIRONMENT THAT ARE REALLY
SIGNIFICANT.
THE INTERTWINING OF THE
PLATFORMS AND A VARIETY DIFFERENT LEVEL ARE HIGH IN THE STOCK OR LOWER IN THE STACK ESPECIALLY IN THE WEB BROWSER. THAT'S AN ISSUE.
AND DELIVERY OF THOSE UPDATES IS DIFFERENT FROM THE MODEL THAT WAS IN THE PLATFORM, ON THE DECK TOP.
THE ONE THING I WOULD EMPHASIZE IS THE DESK TOP ENVIRONMENT HAS A DEPENDENCY ON UPDATES.
IT IS -- IN INSTANCES, IT'S THE VAST MAJORITY THAT USERS HAVE FOR SAFETY OF THOUGH DEVICES.
THE ADD-ON SECURITY SOLUTIONS HAVE A PROTECTIVE BOUNTY.
THERE'S NO SURFACES BUILT AROUND THE PLATFORMS TO PROVIDE THEM WITH MULTIPLE LEVELS OF SECURITY.
THEY DON'T HAVE THE APP STORE OR INTEGRATED SOLUTIONS AS PART OF THE PLATFORM PROVIDED THOSE ADDITIONAL LAYERS OF SECURITY.
SO I THINK IN SOME WAYS, THE FACT THAT WE HAVE BUILT THOSE ADDITIONAL PROTECTIONS INTO THE PLATFORM, THIS IS ACROSS THE BOARD.
GIVES US GREATER FLEXIBILITY WHEN THINKING ABOUT VULNERABILITIES.
WE HAVE DATA.
IS THERE AN APPLICATION CURRENTLY EXPLOITING THIS VULNERABILITY?
NO.
DO I URGENTLY NEED TO GET A PATCH FOR THAT OR DO I MAKE SURE THAT NO APPs EXPLOIT IT?
SO THOSE ARE THE KINDS OF TRADE-OFFS THAT WE'RE ABLE TO MAKE NOW THAT WE WERE NOT ABLE TO MAKE PREVIOUSLY.
I'VE WORKED AT MULTIPLE
COMPANIES IN THE SECURITIES SPACE.
REALLY INVIGORATING TO BE IN AN ENVIRONMENT WHERE WE HAVE -- WE'RE MAKING THE TRADE-OFFS BASED ON DATA.
SO FREQUENTLY THE SECURITY COMMUNITY IS DRIVEN BY A FEAR THAT THERE COULD BE SOMEONE WHO IS GOING TO EXPLOIT THIS. BUT THEN YOU HAVE SOMEONE LIKE PATRICK EARLIER WHO TALKED ABOUT, YEAH, BE THERE AREN'T ANY APPs THAT ARE DOING IT. SO MAYBE IT'S MORE URGENT THAT WE HAVE A REALLY SYSTEMATIC RESPONSE.
MAYBE IT'S MORE URGENT THAT WE BUILT BROADER-BASED PROTECTIONS. THAT'S HOW WE'RE THINKING ABOUT IT.
AN EXAMPLE OF THE THINGS THAT WE'RE DOING ON MY TEAM IS WHEN WE FIND A VULNERABILITY, DON'T JUST FIX THAT ONE LINE OF CODE. ASK YOURSELF, HAVE WE TURNED ON ASLR?
WHAT CAN WE DO TO MAKE ASLR MORE ROBUST IN THIS SITUATION?
WHAT CAN WE DO WITH DATA?
IS THIS ANOTHER FORTIFIED SOURCE THAT COULD BE EMPLOYED?
WHERE WE CAN, PUT TWO OR THREE OR FOUR DEFENSES IN PLACE WHERE THOSE VULNERABILITIES ARE.
SO THAT DOESN'T FIT WELL TO A VULNERABILITY PROGRAM THAT WORKS AT FINDING A PATCH AS QUICKLY AS POSSIBLE.
THAT SAID -- [LAUGHTER]
>> DID YOU WANT TO CHIME IN HERE?
>> YEAH, SO WE SHARE COMMON CHANNELS WITH WINDOWS. OBVIOUSLY WINDOWS HAS -- HAVE
EXPERIENCE WITH HANDLING SECURITY ISSUES AND HAVE BUILT TOOLS AROUND IT AND PROCESSED IT, INFRASTRUCTURE.

>> SO ADRIAN, YOU MADE THE POINT THAT YOU CAN TACKLE THIS FROM, YOU KNOW, CONCLUDING NEW FEATURES LIKE ASLR, DUEP. YOU CAN TACKLE IT FROM ACTUALLY FIXING THE SPECIFIC BUFFER OVERFLOW VULNERABILITY OR YOU CAN TACKLE IT FROM ENSURING THAT THE APPs THAT ARE TRYING TO TAKE ADVANTAGE OF THIS VULNERABILITY. THAT'S A GOOD SEGUE INTO DISCUSSING APP REVIEW PROCESSES.

AND YOU KNOW, THE BENEFITS AND THE LIMITATIONS OF THESE PROCESSES AND WHAT EXACTLY THE PLATFORMS ACTUALLY ARE DOING TO PREVENT THE -- FROM -- TO PREVENT MALWARE FROM ENTERING INTO THE MARKETPLACES IN THE FIRST PLACE.

SO I'D LIKE TO START WITH JANE ACTUALLY. THIS IS SOMETHING THAT I THINK CONSUMERS UNDERSTAND APPLE TO HAVE BEEN AT THE FOREFRONT OF THIS AND REALLY IMPLEMENTS THESE PROCESSES TO ENSURE THAT MALWARE DOESN'T ENTER INTO THE APP STORE.

AND THERE WAS AN INTERESTING ISSUE IN 2011 WHERE, YOU KNOW, RENOWN RESEARCHER CHARLIE MILLER WAS ACTUALLY ABLE TO SNEAK SOME MALWARE PROOF OF CONCEPT APP INTO THE APP STORE THAT WAS TAKING ADVANTAGE OF A BUG AND THAT WHERE HE WAS ABLE TO UNDERMINE THE CODE SIGNING MECHANISM AND I GUESS GET -- JAIL BREAK THE DEVICE. HE CLAIMS THAT HE WAS DOING FAIRLY OBVIOUS THINGS WITH HIS
PROOF OF CONCEPT APP, THAT HE WAS TRYING TO DOWNLOAD A FILE, TRYING TO DO POINTER MANIPULATION.
AND SO YOU KNOW, THIS ENDED UP ON THE APP STORE.
CHARLIE, I GUESS, LATER, YOU KNOW, INFORMED APPLE, THEY QUICKLY TOOK IT DOWN.
AND YOU KNOW, WHAT I WANT TO ASK IS WHAT DID APPLE LEARN FROM THAT SITUATION IN TERMS OF, YOU KNOW, POTENTIAL WEAKNESSES IN THE APP STORE REVIEW PROCESS AND, YOU KNOW, HOW YOU RECALIBRATE THOSE PROCESSES AND WHETHER THIS IS INDICATIVE THAT AT SOME POINT, A SOPHISTICATED ENOUGH ATTACKER WOULD GET THROUGH ANY REVIEW PROCESS.
>> WELL, FIRST OFF, SECURITY IS DEFINITELY AN ARM'S RACE.
WE'VE DEPLOYED A NUMBER OF THINGS THAT WE THINK PROTECT USERS BETTER THROUGH OUR PLATFORM AND IT'S NOT JUST ONE THING OVER ANOTHER. IT'S NOT JUST APP REVIEW, BUT IT'S A NUMBER OF DIFFERENT THINGS THAT WE HAVE DONE TO PROTECT OUR PLATFORM.
AND THERE'S SEVEN DIFFERENT THINGS THAT WE'VE DONE.
THE FIRST IS THE REAL WORLD IDENTITY OF EACH DEVELOPER IS DETERMINED.
WHEN THEY APPLY TO BE A DEVELOPER WITH THE APPLE DEVELOPER PROGRAM, THEIR IDENTITY IS CONFIRMED.
AND THAT ACTS AS A REAL DETERRENT TOWARDS SUBMITTING MALICIOUS CODE BECAUSE IF WE CAN FIND YOU, THEN YOU CAN BE TERMINATED FROM THE STORE.
AS AN APP DEVELOPER, BEING
REMOVED FROM YOUR DISTRIBUTION PLATFORM IS LIKE A PRODUCT BEING REMOVED FROM WALMART. IT'S A PRETTY BIG STICK. THE NEXT THING IS, ONCE A DEVELOPER APPLIES, THEY'RE GIVEN A CERTIFICATE. AND THAT CERTIFICATE ALLOWS THEM TO SUBMIT APPs. ONCE THE APPs ARE SUBMITTED, WE REVIEW THEM, WE BASICALLY RUN EACH APP TO DETERMINE WHETHER THEY RUN AS -- THEY OPERATE AS THEY'RE SUPPOSED TO OPERATE AND WHETHER THEY HAVE ANY BUGS. AND OBVIOUS BUGS, OF COURSE. AND THEN THE NEXT THING, RUN TIME, WE HAVE CODE SIGNATURE CHECKS OF ALL EXECUABLE MEMORY PAGES THAT ARE MADE AS THE PAGES ARE LOADED TO MAKE SURE AN APP HAS NOT BEEN MODIFIED SINCE IT WAS INSTALLED OR LAST UPDATED. THEN WE DEPLOY SANDBOXING, HAS ALREADY BEEN DISCUSSED ON THE PANEL. AFTER AN APP IS LAUNCHED IN THE STORE, WE ACTIVELY MONITOR FOR MY THREATS. ANY DEVELOPER THAT MALICIOUSLY TRIES TO HARM A USER OR AN IOS DEVICE WILL BE TERMINATED FROM THE APP DEVELOPER PROGRAM. >> GREAT. SO THOSE ARE THE OVERALL PROCESSES THAT APPLE USES. AND I THINK THAT ONE ASPECT OF THAT THAT I FIND REALLY INTERESTING IS THE DEVELOPER IDENTITY ISSUE. YOU KNOW, DO THE OTHER PLATFORMS THINK THAT THAT IS A HIGH -- SOMETHING THAT CREATES A HIGH BARRIER OF INJURY TO MALWARE DEVELOPERS? DO YOU GUYS ALSO MAKE SURE THAT
YOU IDENTIFY EVERY DEVELOPER WHO IS SUBMITTING APPs TO YOUR STORES?

>> WE WORK THROUGH A PROCESS TO IDENTIFY DEVELOPERS ON OUR SITE. LIKE TO YOUR ORIGINAL QUESTION, DO I BELIEVE IT'S A HIGH BARRIER OF ENTRY?

NOT NECESSARILY. I THINK REALLY IT KIND OF -- REFRAMING THE PROBLEM, WHICH IS HOW DO WE GO AND ENSURE THAT OUR APP ECOSYSTEM IS FREE OF MALWARE. BROADEN THAT TO TAKE IT ANOTHER STEP. IT'S BASED ON THE DATA THAT WE SAW. MALWARE MAY NOT BE THE MOST PREVAILING PROBLEM IN THE APP STORE ECOSYSTEM. MAY BE ABOUT PRIVACY INFRINGING APPLICATIONS. WHAT ARE THOSE APPLICATIONS DOING?

SO YOU KNOW, IN THAT INSTANCE, DO I VALIDATE THE IDENTITY OF A DEVELOPER DOESN'T SOLVE THAT PROBLEM NECESSARILY.

SO WHEN I LOOK AT KIND OF OUR APPROACH TO APP, AT A HIGH LEVEL, NUMBER 1, THE APP TEAM EMBEDDED IN MY ORGANIZATION FOR SECURITY RESPONSE. THAT GIVES US A COUPLE OF INTERESTING OPTIONS.

WHEN WE'RE EXPLORING VULNERABILITIES IN A PLATFORM, WE LOOK AT HOW WE CAN PROTECT THE APP STORE. TO ADRIAN'S EARLIER POINT. THE MAIN VECTOR, THE POINT OF INTRODUCTION MAY BE IN OUR APP STORE. HOW DO WE PROTECT CUSTOMERS AND ENSURE IT DOESN'T GET LEVERAGED.
TWO, WE’VE PARTNERED EXTERNALLY. OUR PLATFORM ENVIRONMENT IS PRETTY DIVERSE. WE DO SUPPORT PORTED ANDROID APPS ON OUR PLATFORM. WE DO SUPPORT NATIVE APPs ON OUR PLATFORM. WE SUPPORT HTML 5. SO A WIDE DIVERSE AREA THAT WE HAVE TO LOOK AT. ONE OF THE THINGS THAT WE IDENTIFIED, WE’RE NOT NECESSARILY EXPERTS IN ANDROID MALWARE. SO LET’S GO PARTNER EXTERNALLY. WE MADE AN ANNOUNCEMENT EARLIER THIS YEAR AROUND OUR PARTNERSHIP WITH TREND MICRO. NOT ONLY DID THAT GET US MILEAGE IN TERMS OF PROTECTING THE APP STORE FROM MALWARE, BUT ALSO PRIVACY CONCERNS AS WELL BECAUSE THEY DO DEEP INSPECTION ON ADVERTISING FRAMEWORKS AND STUFF LIKE THAT. SO YOU KNOW, BETTER ABLE TO LEVERAGE THAT. IDENTITY IS ONE PART OF IT. YOU LOOK TO MAKE SURE THAT REAL PEOPLE ARE SUBMITTING THE APPs, ESPECIALLY WHEN WE TALK ABOUT CUTTING CHECKS TO THESE DEVELOPERS, MAKING SURE THAT DEVELOPERS CAN EARN MONEY. I THINK THAT’S ONE PART OF THE LARGER EQUATION. YOU HAVE TO WALK THROUGH HOW YOU GET THERE. >> SO GOING BACK TO THE ACTUAL STATIC ANALYSIS AND DYNAMIC ANALYSIS, ALL OF THIS STUFF. WHAT ARE -- ARE CONSUMERS TRUSTING THAT PROCESS, TO BE ABLE TO CAPTURE EVERY PIECE OF MALWARE? IS THERE -- YOU KNOW, WE KNOW
WITH THE MOST RECENT OUTBREAK OF MALWARE IN GOOGLE PLAY, WHICH WAS I THINK CALLED BAD NEWS, THAT THE MALWARE WAS ACTUALLY, YOU KNOW, I GUESS CHANGING AFTER, YOU KNOW, IT HAD GONE THROUGH THE REVIEW PROCESS. THERE WAS SOME KIND OF TRIGGER-BASED MECHANISM WHERE IT WAS DOWNLOADING OTHER CODE FROM THE SERVER. I'M NOT SURE THE ISSUE. BUT HOW DO YOU ADDRESS THOSE KINDS OF ISSUES WHEN, YOU KNOW, MALWARE AUTHORS PROBABLY KNOW THAT, HEY, YOU KNOW, THEY'RE GOING TO BE RUNNING ME FOR 24 HOURS, YOU KNOW, APPLE, THE APP REVIEW PROCESS, THE APPs GET OUT THERE IN TWO WEEKS. YOU KNOW, HOW DO YOU DEAL WITH THE FACT THAT THERE ARE THINGS LIKE TRIGGER MECHANISMS THAT CAN THWART THESE REVIEW PROCESSES.

>> THE QUESTION WASN'T EXPLICITLY DIRECTED TO ME BUT I'LL TAKE THIS ONE. I MADE SOME PROMISES TO PEOPLE THAT I WOULDN'T PROVIDE STATISTICS THAT WERE NOT PUBLIC. I'M GOING TO PROVIDE ONE HERE. BAD NEWS IS AN INTERESTING APPLICATION. THE WAY IT BEHAVES IS IT IS AN STK INCLUDED INTO APPLICATIONS. WE SAW IT ACROSS A NUMBER OF APPLICATIONS. DOWNLOADED BY A FAIRLY SIGNIFICANT NUMBER OF PEOPLE. I DON'T REMEMBER WHAT THE NUMBERS WERE PUBLICLY. LOW MILLIONS NUMBERS. THE BEHAVIOR OF THAT APPLICATION DISPLAYS ADVERTISEMENTS. SOME OF THEM ALLOW YOU TO CLICK. WITHIN THAT ADVERTISEMENT, IF
YOU WANT TO DOWNLOAD AN APPLICATION, YOU WOULD INSTALL THAT APPLICATION.
IT WAS REPORTED TO GOOGLE THAT THERE WAS THE POSSIBILITY OF SOME OF THOSE APPLICATIONS BEING MISUSING THE SMS INFORMATION. ABUSING SMS TO PERMIT TOLL FRAUD.
WE REVIEWED THE APPLICATION AND DETERMINED BASED ON OTHER CHARACTERISTICS, NOT THE BEHAVIOR OF THE APPLICATION, THAT IT APPEARED TO BE A VIOLATION OF GOOGLE PLACE POLICIES.
AT NO POINT HAS ANYONE SAID THAT GOOGLE SAID THIS IS MALWARE, SPYWARE OR MALICIOUS. I'M NOT SAYING THAT RIGHT NOW. WHAT I WILL SAY IS THAT WE REVIEWED THROUGH ALL OF THE LOGS THAT WE HAVE ACCESS TO, BY NO MEANS COMPREHENSIVE BUT THEY'RE SUBSTANTIAL, WE HAVE NOT SEEN A SINGLE INSTANCE OF AN SMS APPLICATION THAT WAS ABUSIVE AND BEING DOWNLOADED. WE LOOKED AT A LOT.
SO THERE WERE SOME TAKEN DOWN FROM GOOGLE PLAY. I DON'T WANT TO SAY THAT BECAUSE SOMETHING CAME DOWN THROUGH GOOGLE PLAY, IT'S MALWARE, IT'S MALICIOUS OR BAD. I READ A LOT OF REPORTS LIKE THAT. I HAVE A PARTICULAR VIEW OF THE NEWS. BUT A LOT OF THE REPORTS DO GO OUT. I WANT TO MAKE CLEAR THAT SOMETHING COMING DOWN FROM GOOGLE PLAY -- WE NEVER -- PROBABLY TOO STRONG -- VERY RARELY CONFIRM THE REASON WHY
SOMETHING IS TAKEN DOWN FROM GOOGLE PLAY OR COMMENT ON A SPECIFIC DEVELOPER. BECAUSE FRANKLY WE DON'T KNOW WHAT THE INTENTION WAS. WAS IT AN ACCIDENT OR MISTAKE? WE DON'T KNOW. IT'S IMPORTANT FOR US TO RETAIN THE ABILITY TO HAVE A CONVERSATION WITH THE DEVELOPERS OF THE APPLICATIONS TO MAKE SURE THERE'S AN UNDERSTANDING OF WHAT WAS GOING ON. SO SPECIFICALLY TO THE QUESTION OF WHAT ARE THE TYPES OF THINGS THAT WE DO. VERIFYING THE IDENTITY OF THE DEVELOPER IS IMPORTANT. FIRST STEP IN THE PROCESS, RIGHT? IN ORDER TO UPLOAD AN APPLICATION OF GOOGLE PLAY, YOU HAVE A VALID CREDIT CARD TO CREATE A DEVELOPER ACCOUNT. THAT IS AN IDENTITY VERIFICATION PROCESS. FAIRLY ROBUST ONE. NEEDLESS TO SAY, EVERY IDENTITY VERIFICATION PROCESS HAS MISTAKES AND FLAWS. YOU CAN MAKE CREATION OF FAKE ID's IS A LONG ESTABLISHED PAST TIME. RIGHT? SO NO MATTER HOW ROBUST YOUR IDENTIFICATION PROCESS IS, THERE'S MISTAKES. IT'S CRITICAL TO HAVE ADDITIONAL REVIEWS THAT HAPPEN AFTER THE FACT. IT'S CRITICAL TO MAKE TAKEN GOOD RELATIONSHIPS WITH THE RESEARCH COMMUNITY THAT IS LOOKING AT THE APPLICATIONS THAT CAN PROVIDE INSIGHT TO WHAT THEY'RE SEEING. THAT CAN GIVE YOU AN EARLY ALERT
THAT WAS MAKE GOING TO BECOME BAD EVEN IF IT HADN'T YET.
SO THERE'S A LOT OF THOSE KINDS OF THINGS THAT WE DO.
IT COMES DOWN TO IDENTIFICATION,
COMES DOWN TO REVIEW OF APPLICATIONS, COMES DOWN TO LOOKING AT PATTERNS OF BEHAVIOR BETWEEN DIFFERENT DEVELOPERS, BETWEEN DIFFERENT APPLICATIONS. ARE THEY SIGNING ON, DO THEY NORMALLY SIGN ON AT THAT TIME.
A LOT OF DIFFERENT COMPLEXITIES.
I WON'T GO INTO THE SPECIFICS.
ABSOLUTELY IT'S A CASE THAT EVERY DAY WE'RE LEARNING SOMETHING NEW AND ADDING NEW THINGS TO OUR SYSTEMS TO MAKE SURE WE FIND WHAT AT THIS POINT ARE QUARTER BEETLES.
>> AND I THINK THERE'S TWO KEY THINGS, RIGHT?
THAT WE NEED TO LOOK AT AS A COMMUNITY, WHICH IS ONE, INTENT.
YOU KNOW, WHAT WAS THE INTENT OF THAT APPLICATION WHEN IT'S MOVED INTO YOUR STORE.
THAT'S EXTREMELY HARD TO DETERMINE.
SO YOU KNOW, I ECHO ADRIAN'S STATEMENTS AND REALLY WORKING WITH THE DEVELOPER TO TRY TO UNDERSTAND THAT INTENT.
I THINK AT THE SAME TIME, YOU KNOW, THAT WE HAVE TO ALSO WORK WHEN WE BELIEVE THAT THE INTENT IS NOT MALICIOUS, BUT POTENTIALLY CAN HAVE NEGATIVE CONSEQUENCES TO THE USER.
WE NEED TO RESPOND TO THAT.
WE ALSO -- TO VARYING DEGREES ACROSS THE PANEL, WE NEED TO CLEARLY COMMUNICATE THAT BACK TO OUR USER COMMUNITY ONCE WE HAVE ENOUGH UNDERSTANDING.
AND THAT WAS ONE OF THE REASONS
IN THE LAST YEAR THAT WE LAUNCHED OUR PRIVACY NOTIFICATION SERVICE. THE PREVIOUS PANEL, WHAT CONSTITUTES MALWARE. YOU SAW A WIDE VARIETY OF ANSWERS. AGAIN, THE DATA DOESN'T SHOW WHAT I THINK WE SEE OR HEAR IN THE NEWS. AND AT THE SAME TIME, WHEN WE REFOCUSE ON PRIVACY, THAT'S THE AREA THAT I'M VERY CONCERNED ABOUT, RIGHT? NONMALICIOUS APPs THAT HAVE PRIVACY INFRINGING IMPLICATIONS. SO WITH THE SERVICE THAT WE LAUNCHED EARLIER THIS YEAR, WHEN WE IDENTIFIED AN APPLICATION THAT IS FAR-REACHING FROM A PRIVACY CONCERN, WE DO REACH OUT TO THE DEVELOPER. WE INITIATE A DIALOGUE WITH THE DEVELOPER. WHEN WE HAVE A SOLID UNDERSTANDING OF WHAT THE APPLICATION'S INTENT IS AND THE BEHAVIOR, WE PUBLISH A DOCUMENT FOR THE USER COMMUNITY. SO INTENT AND UNDERSTANDING OF THAT -- OF THAT BEHAVIOR AND MAINTAINING THAT RELATIONSHIP WITH THE DEVELOPERS AS WELL AS THE SECURITY COMMUNITY IS INVALUABLE THERE. CUTS THROUGH THE FUD. >> THANK YOU. SO WE HAVE A SIGN-UP PROCESS FOR THE DEVELOPERS. WE SCAN THE APPs WITH ALL MAJOR MALWARE ENGINES. WE'RE NOT FIGHTING MUCH MALWARE. SO WE -- I WOULD ALSO SAY, OUR NUMBER 1 GOAL FOR SECURITY IS END USER SAFETY AND PRIVACY. NUMBER 2 IS EARNING DEVELOPER
TRUST.
SO WE ALSO TRY TO RESPECT
DEVELOPERS AND THEIR I.P.,
INTELLECTUAL PROPERTY.
SO WHEN SOMETHING IS SUSPICIOUS,
WE DON'T AUTOMATICALLY YANK THE
APPLICATION FROM THE STORE.
WE REACH OUT TO THE DEVELOPER
AND TYPICALLY RESOLVE THE
SITUATION.
>> SO WE HAVE TOUCHED A LITTLE
BIT ON THE -- SOME OF THE
LIMITATIONS OF REVIEW PROCESSES.
YOU KNOW, ONE BIG QUESTION IS
SCALEABILITY.
WHEN WE HAVE 700,000, 800,000
APPs IN A MARKET, ARE YOU --
THAT MUST BE A TENSE, YOU KNOW,
COMPUTING RESOURCE AND HUMAN
RESOURCE IN ORDER TO ACTUALLY
SCAN AND REVIEW ALL THOSE APPs.
CAN YOU TALK ABOUT THAT, ABOUT
THOSE CHALLENGES AND WHETHER YOU
THINK THAT THIS IS SOMETHING
THAT IS REALLY SCALEABLE?
>> ONE POINT IS THAT THE
MAJORITY OF THE APPs ARE NOT
DOWNLOADED EVER.
MOST OF THEM ARE NEVER
DOWNLOADED.
AND IN SIGNIFICANT NUMBERS.
THE VAST --
>> MIGHT JUST BE AB COMPANIES.
>> THERE'S ABOUT 500 TO 1,000
APPs THAT ARE DOWNLOADED A LOT.
WE INVEST OUR RESOURCES WHERE WE
THINK IS THE MOST IMPORTANT.
>> SO YOU SAY, HEY, THIS APP IS
GETTING A LOT OF TRACTION, WE
SHOULD PROBABLY LOOK INTO IT
MORE CAREFULLY?
>> YEAH, I'LL ANSWER THE SCALE
QUESTION.
GOOGLE IS ABOUT SCALE,
ULTIMATELY.
THE ABILITY TO READ BASICALLY
ALL INFORMATION THAT HAS EVER BEEN WRITTEN, PARSE IT, MAKE IT ACCEPTABLE, MAKE IT OPEN, MAKE IT AVAILABLE WORLDWIDE IN WHATEVER LANGUAGE YOU WANT TRANSLATED, THAT'S A HARD PROBLEM. LOOKING AT A MILLION APPLICATIONS AND GET A SENSE FOR WHAT THEY DO AND WHETHER OR NOT IT'S THE REALMS OF NORMALCY, YEAH.

I DON'T WANT TO DISMISS IT BUT THAT'S NOT A HARD PROBLEM. IN THE SCALE OF THINGS THAT GOOGLE WORKS WITH WITH MANY TERMS OF PROCESSING INFORMATION. WE HAVE ABOUT 1,000 ENGINEERS IN GOOGLE THAT ARE FOCUSED ON SECURITY. COUNTLESS PEOPLE THAT ARE NOT IN A SECURITY ROLE BUT ARE IN AN ANTI ABUSE, ANTI-SPAM, ANTI-FISHING ROLE WHERE THEY'RE LOOKING TO UNDERSTAND WHAT KIND OF SOCIAL ENGINEERING IS GOING ON AND MAKE SURE THERE'S POLICIES IN PLACE. WHAT IS INTERESTING FROM MY PERSPECTIVE -- THE REVIEW APPLICATION DIDN'T COME FROM THE ANDROID TEAM. I KNEW IT WAS NECESSARY BUT TURNS OUT WHERE ALREADY HAD A TEAM THAT HAD TAKEN IT UPON THEMSELVES TO PROTECT THE ENTIRE WORLD FROM THE INTERNET IN THE FORM OF SAFE BROWSING. A PROTECT WE MAKE AVAILABLE FOR FREE, AN API. A NUMBER OF BROWSERS THAT WE USE INSIDE OF FIRE FOX, CHROME. THERE'S OTHER DEVICES THAT USE IT, INTEGRATE IN THEIR PLATFORM TO PROTECT USERS, THIS IS THE KIND OF THING THAT GOOGLE DOES.
WE PUT OUR RESOURCES TO BEAR TO THEN PROTECT USERS ACROSS THE ENTIRE WEB.
AND THAT'S REALLY HOW WE THINK ABOUT ANDROID SECURITIES AND THE CONTEXT OF ALL OF THE WAYS THAT PEOPLE WANT TO ACCESS INFORMATION, MAKING SURE THAT IT'S SAFE.
IT'S NOT JUST ABOUT ANDROID AND US PROTECTING THIS PLATFORM.
IT'S ABOUT WHETHER THEY'RE CONNECTING TO A GOOGLE SERVICE OR CONNECTING TO SOMETHING ON THE WEB, MAKING SURE THERE'S CONFIDENCE AND SAFETY AND THEY'RE NOT AFRAID.
THEY DON'T HAVE A REASON TO BE AFRAID.
THAT'S REALLY HOW WE CAME TO THINK ABOUT IT, HOW WE CAN FOCUS ON IT INSIDE OF ANDROID.
>> SO YOU MAY BE THINKING FOR YOURSELF, A COMPANY NOT AS LARGE AS GOOGLE, WHAT ARE WE GOING TO BE DOING TO TACKLE A SIMILAR ISSUE?
SO I WANT TO THROW A FEW THOUGHTS OUT HERE AS WE'RE KIND OF WRAPPING UP.
WE'RE TACKLING THIS IN THE WAY WE TACKLE A LOT OF THINGS.
WHETHER OR NOT YOU KNOW IT, FIREFOX IS HALF-DEVELOPED BY COMMUNITY PEOPLE AROUND THE WORLD.
JUST VOLUNTEERS THAT LIKE THE MISSION, YOU KNOW, SMART INDIVIDUALS AND WANT TO CONTRIBUTE.
AND WE'RE GOING TO TAKE THAT SAME THING FOR MOBILE.
WE'RE GOING TO HAVE THEM AS PART OF THE REVIEW GROUP.
IT'S GOING TO BE REVIEW-DRIVEN THROUGH THE COMMUNITY.
JUST LIKE WE DID FOR ADD-ONS FOR FIRE FOX.
SO THAT COMBINED WITH STATIC ANALYSIS FOR QUALITY, MAKING SURE APPs FUNCTION AND REACHING OUT TO THE COMMUNITY WE THINK IS GOING TO BE A DIFFERENT WAY OF LOOKING AT THE PROBLEM BUT ONE THAT HAS BEEN VERY SUCCESSFUL FOR OUR ORGANIZATION IN THE PAST.
>> GREAT.
SO YOU JUST MENTIONED STATUS AND HOW APPs FUNCTION.
THAT'S AN INTERESTING QUESTION AS TO WHAT -- TO WHAT EXTENT DOES CONTENT REVIEW ITSELF DECREASE THE THREAT OF MALWARE. THE AUTHORS AREN'T CREATING SOPHISTICATED APPs AND THAT'S WHY, YOU KNOW, THEY WOULDN'T GET THROUGH APPLE'S REVIEW PROCESS, FOR EXAMPLE.
AND MAYBE I'LL THROW THIS TO JANE.
>> I'M NOT EXACTLY SURE I UNDERSTAND THE QUESTION. ARE YOU SAYING THAT THEY DON'T GET THROUGH THE PROCESS BECAUSE WE ACTUALLY RUN EVERY APP THAT COMES IN TO APP REVIEW AND THAT WOULD BE A DETERRENT TO SUBMITTING MALWARE BECAUSE MALWARE IS GENERALLY SIMPLISTIC? IS THAT THE QUESTION?
>> I THINK THAT PEOPLE GENERALLY UNDERSTAND APPLE’S APP REVIEW PROCESS TO INCLUDE SOME KIND OF CONTENT REVIEW IN TERMS OF KEEPING APPs AT SOME STANDARD OF QUALITY.
AND IS THAT A CONTRIBUTING FACTOR IN DECREASING THE POTENTIAL FOR MALWARE BECAUSE MALWARE AUTHORS MAY NOT BE INVESTED IN CREATING HIGH
QUALITY APPs.
>> I'M NOT CERTAIN I CAN ANSWER THAT.
I THINK THAT, YOU KNOW,
HOLISTICALLY SPEAKING THE ENTIRE -- ALL THE PROCESSES THAT WE PUT IN PLACE HELP TO DETER MALWARE ON THE DEVICE AND ON THE PLATFORM.
>> SO I JUST WANTED TO ADD TO THE SORT OF SCALEABILITY DISCUSSION.
YOUR IMPORTANT ABOUT MALWARE BEING SIMPLE HELPS SCALE THE IDENTIFICATION OF THE MALWARE. AS THE MALWARE BECOMES MORE TRICKIER, TRYING TO USE DIFFERENT TECHNIQUES, VERY DELAYED SORT OF EXECUTION AND LOGIC BUGS.
THE TYPES OF TECHNOLOGICAL ANALYSIS TECHNIQUES NEED TO BECOME MUCH MORE DEEPER AND BECOME MUCH MORE PRECISE AND ACCURATE.
THEN SCALING UP THOSE APPROACHES WHERE YOU CAN THROW A BUNCH OF COMPUTATION ADDDED BECOMES LIMITED TO SOME EXTENT WHERE YOU STILL NEED TO THROW A NUMBER OF ACTUAL HUMAN ANALYSTS AT THIS PROBLEM TO IDENTIFY THE NEW SET OF ISSUES.
SO THERE'S SCALEABILITY AND SORT OF DIFFERENT ASPECTS OF HOW THIS IS GOING TO EVOLVE.
>> SO ONE THING THAT WE HAVEN'T TOUCHED ON YET IS, YOU KNOW, APPLE REALLY CREATED THIS MODEL OF A SINGLE APP STORE IN WHICH YOU ONLY GET APPs FROM ONE SOURCE.
AND BLACKBERRY AND MICROSOFT HAVE MOVED IN THAT DIRECTION WITH BLACKBERRY 10 AND WITH WINDOWS PHONE.
YOU CAN NOW ONLY ACCESS APPs FROM A SINGLE DESTINATION. CAN YOU, YOU KNOW, EXPLAIN, ADRIAN AND GEIR THE REASONING FOR THAT, WHETHER IT WAS REALLY RELATED TO SECURITY BENEFITS OR WHETHER THERE WERE OTHER CONSIDERATIONS LIKE USABILITY AND, YOU KNOW, EASE OF DISTRIBUTION FOR APP DEVELOPERS. 

>> I'D SAY NOT ONLY HAVE WE MOVED THERE, BUT THAT'S WHERE WE ARE. AND I THINK IT WAS ALL OF THE ABOVE. WE SAW THAT AS A WAY TO IMPROVE DISCOVERABILITY OF APPs FOR USERS. AND A SIMPLY WAY FOR DEVELOPERS TO REACH A LARGE MARKET. AND IT HAS DEFINITE SECURITY BENEFITS. 

>> FROM OUR SIDE, I MEAN, IT'S EASY FORMER TO POINT TO WHAT GEIR SAID. BUT I WOULD BUILD ON THAT, YES, WE DO NOW, YOU KNOW, HAVE A CURATED APP STORE THAT WE THINK WILL BE THE CENTRAL STORE IN OUR ECOSYSTEM. THE PREVIOUS PANEL TOUCHEd ON IT. WHEN WE LOOK AT SITUATIONS LIKE JAIL-BREAKING AND THE UNINTENDED CONSEQUENCES OF JAIL BREAKING A DEVICE, A LOT OF TIMES USERS WANT A CHOICE IN TERMS OF THEIR USER EXPERIENCE OR THE APPs THEY WANT TO INSTALL. SO ONE OF THE THINGS THAT WE DID WAS WE PROVIDED A MECHANISM TODAY WHERE USERS COULD SIDE-LOAD APPs TO THEIR DEVICE. THEY HAVE TO TAKE WILLFUL AND CONSCIOUS DECISIONS TO ENTER IN A SECURE PASSWORD THAT PUTS THE
DEVICE IN THAT STATE.
THE DEVICE HAS TO BE TETHERED.
MY POINT IN ALL OF THIS IS ABOUT
REDUCING THE THREAT.
YES, WE WANT A -- YOU KNOW A
VERY REFINED POSITIVE CUSTOMER
EXPERIENCE WITH ALL OF OUR APPs.
WE RECOGNIZE IT AT THE SAME TIME
THAT ESPECIALLY THE DEVELOPER
COMMUNITY NEEDS MORE ACCESS OR
MORE CAPABILITY OR EVEN TO SOME
EXTENT INDIVIDUALS WOULD LIKE
GREATER OPPORTUNITY IN THEIR
DEVICE.
SO HOW DO WE SEGMENT THE RISK
THAT THAT COULD POTENTIALLY
PRESENT FROM AN APP PERSPECTIVE?
SO WE CREATED THE -- WHAT WE
BELIEVE IS A SAY MECHANISM FOR
SIDE-LOADING APPLICATIONS IN
THAT WAY.
SO IT'S JUST ONE OF THE WAYS
THAT WE CAN HELP TRY TO MINIMIZE
RISK WHILE STILL AT THE SAME
TIME GIVING USERS A SAFE OPTION.
>> OKAY,
SO I THINK OUR TIME IS UP, BUT
IF YOU GUYS ARE WILLING TO BEAR
WITH ME, WE'RE HITTING ON AN
INTERESTING DISCUSSION RIGHT
NOW.
AND SO YOU KNOW, WITH IOS AND
MAC OS, YOU GUYS HAVE INSTITUTED
TWO DIFFERENT TYPES OF SECURITY
MECHANISMS THERE.
AND IOS OBVIOUSLY YOU CAN ONLY
GET THE APPs FROM THE APP STORE
WHEREAS IN MAC OSX, IT SEEMS
LIKE YOU CAN CHOOSE -- USER CAN
CHOOSE TO GET STUFF FROM THE MAC
APP STORE OR TO ALLOW DOWNLOADS
FROM OTHER SOURCES.
CAN YOU GIVE US A SENSE AS TO
APPLE'S REASONING FOR MAKING
THAT DISTINCTION?
SOMETHING ABOUT MOBILE THAT YOU
THINK CREATES A GREATER RISK?
>> NO.
WE HAVE -- IOS IS BASED ON OUR
EXPERIENCE IN DEVELOPING THE MAC
OPERATING SYSTEM.
THE MAC OPERATING SYSTEM COMES
WITH GATE KEEPER, SIMILAR TO
WHAT ADRIAN WAS DESCRIBING ON
BLACKBERRY.
IN A SENSE, IT ALLOWS USERS TO
dETERMINE THE DEFAULT GATE
KEEPER.
YOU CAN DOWNLOAD APPS THAT HAVE
A DEVELOPER CERTIFICATE OR COME
FROM THE MAC APP STORE.
WE DO HAVE AN APP STORE ON OUR
MAC NOW.
AND THAT'S THE DEFAULT.
IF YOU TRY TO DOWNLOAD AN APP
THAT DOES NOT FALL WITHIN THAT
RANGE, THEN THE USERS WILL BE
PROMPTED AND THE USER HAS TO
OVERRIDE GATE KEEPER.
YOU CAN ALSO SET GATE KEEPER UP
TO THE MOST SECURE MECHANISM,
WHICH IS TO ALLOW ONLY APPS TO
BE DOWNLOADED FROM THE MAC APP
STORE OR YOU CAN TURN GATE
KEEPER OFF ALL TOGETHER.
>> SO YOU SEE A REASON FOR
MAKING A DISTINCTION BETWEEN
MOBILE AND DESK TOP IN TERMS OF
THE FLEXIBILITY GIVEN TO THE
USER?
VIS A VIS, ANDROID.
IT'S A SIMILAR SYSTEM WHERE YOU
HAVE TO CHECK A BOX TO ALLOW
DOWNLOADS FROM UNKNOWN SOURCES.
>> I CAN'T COMMENT ON THAT.
JUST TWO DIFFERENT MECHANISMS
THAT WE HAVE.
>> ADRIAN, DO YOU THINK THAT,
YOU KNOW, HAVING THAT SETTING
THERE IN ANDROID GIVES ENOUGH
PROTECTION?
WE'VE HEARD FROM THE PREVIOUS
PAM ABOUT -- PANEL ABOUT HOW THE MALWARE COMES FROM DIFFERENT APP STORES.

>> I HEARD THE WORD "CURATION."
WHAT I DIDN'T HEAR WAS "CHOICE."
WHAT I DIDN'T HEAR WAS THE IDEA THAT THE USER SHOULD BE THE ONE THAT GETS TO DECIDE WHICH THINGS THEY WANT TO CONSUME, WHERE THEY WANT TO CONSUME IT FROM.
ULTIMATELY ONE OF THE BASIC PRINCIPLES THAT GOOGLE ESPOUSES IS THAT THE USER SHOULD HAVE A CHOICE, THAT THE REASON YOU MAKE INFORMATION OPEN AND ACCESSIBLE IS SO THAT PEOPLE CAN FIND THE THINGS THEY WANT.
WE VIEW APPLICATIONS AS SOMETHING LIKE THAT.
THERE ARE MANY INSTANCES WHERE A SINGLE PROVIDER WON'T BE COMFORTABLE WITH THE PARTICULAR APPLICATION THAT LOTS OF PEOPLE WANT.
SO WE DID NOT WANT GOOGLE TO BE IN A POSITION WHERE IT COULD IMPEDE USERS FROM HAVING THOSE KINDS OF CHOICES WHICH ULTIMATELY IS WHAT CLOSED MARKETS DO.
AND THE REVIEW PROCESS THAT INVOLVES CURATION OF THOSE APPLICATIONS, THEY PREVENT USERS FROM WORKING ON THOSE CHOICES.
WE FOCUSED ON TRANSPARENCY.
SO THAT'S THE DIRECTION THAT WE HAVE TAKEN.

>> ALL RIGHT.
THAT WAS AN INTERESTING POINT TO END ON.
I HAVE A TON OF OTHER QUESTIONS THAT I WASN'T ABLE TO GET TO.
WE HAD A REALLY INTERESTING DISCUSSION AND I WANT TO THANK ALL OF YOU AGAIN.