

Welcome to your Web Meeting.

chip has joined the meeting.

Brandon Palmen has joined the meeting.

me: Welcome, chip

Dino Dai Zovi has joined the meeting.

chip: Thanks. I like to be the quiet one anyway.

me:

Ohm Prasanha has joined the meeting.

me: Welcome, Ohm

me: *Insert bad hold music here*

Bill Leninger has joined the meeting.

me: Welcome, Bill

erezson has joined the meeting.

Ohm Prasanha: thank U Maxim

bennethaselton has joined the meeting.

me: Welcome, erezson and bennett

erezson: Hey

bennethaselton: Hi everyone! I don't have a mike so I'll have to ask questions in text.

me: no problem

me: I'll try to watch for questions in the text and pass them along via audio

bennethaselton: Thanks. I hear from the crackling and breathing and fidgeting that most people do indeed have a working mike set up

bennethaselton: I have a question: Of people who get their machines compromised, do we know what percentage of those hacks are where a security update did exist at the time but people just didn't have their updates turned on, vs. what percentage were hacked by new exploits for which no patch had been released yet?

Dino Dai Zovi: Max, did you want to pass the mic to Bennett?

bennethaselton: No mike

bennethaselton: that's interesting, so we should expect that Windows and IE exploits should keep dropping off since almost all systems have automatic updates turned on now and it's hard to turn off

bennethaselton: A point about Linux auto-update disclosure: A lot of Linux servers are remotely hosted servers where the admin is never "sitting in front of them" (that's certainly the case with most of my hosted sites). So it's not immediately obvious how the server would "notify" its owner when it's updating itself. It's not like a Windows desktop where you simply flash an alert on the screen.

Brandon Palmen: A lot of corporate environments keep updates back and apply them selectively and conservatively.

Bill Leninger: One big concern we have is network bandwidth. If Adobe starts pushing down a 180MB update to v9.3, then we see impact on our network. And Adobe changes features with its updates, so a process we used before the update may not work afterward. So for those, I prefer one download to my server and then test and evaluate and then distribute.

Bill Leninger: sorry, no mic

Brandon Palmen: Perhaps there should be a clear delineation between security updates and feature updates?

bennethaselton: perhaps what we need is a protocol for auto-updates to download an update once to a company's server, and then individually re-distribute to all the client machines within that network. then it could happen seamlessly and companies wouldn't have to be as "smart" about keeping their updates small (like Google). Because if you require people to be smart in order for something to work, then it frequently won't work

Bill Leninger: Bennett's last comment is good. Our firewall blocks executables, so we see a lot of updates "fail" at the firewall. IT could still download the update and distribute.

bennethaselton: Maxim yes I think that separating security and feature updates is a good idea, it's just harder... Because then you have to provide updates to version 8.x and to version 9.x, and test both updates, rather than just one

Bill Leninger: A lot of it is how much you trust the vendor as well. Mozilla has a good track record of fixing security issues without hosing my system. Will I trust "flybynight" company to do the same? No, I have to build that trust first. Many of us don't trust Microsoft's fixes because they have broken things with "fixes" in the past.

bennethaselton: Bill, yes systems could get hosed by installing updates, but I think even in that case, it's a question of whether your system is MORE likely to be hosed by installing the updates or not installing them. I would assume that especially in the case of Microsoft fixes, your system is more likely to be hosed by not installing them.

chip: (No mic) - Companies like adobe and others seem to cater towards the home user or person that manages their own machine. they rarely make things nice for the corporate administrator dealing with a locked down environment. The applications aren't manageable via group policy, they're frequently difficult to customize and deploy and let's not even talk about how much trouble they are to keep patched. there is rarely a notification mechanism for the IT folks to be aware of updates and when they do find out, you have to jump through hoops in order to put it out there. The first thing we do during packaging is disable any update check because it just causes users to place calls when the app notifies them an update is ready and we're not.

me: Thoughts on disclosure?

bennetthaselton: Maxim I think it's an interesting abstract question in principle but not a big security problem. If a program updates itself automatically, few people are going to have a really, really big problem with that. Firefox does it after all with no complaints. I think the bigger problem is the fact of systems getting hosed for whatever reason

erezson: Regarding our trust in Microsoft, we also trust Google and Mozilla, and specially the plugins which available through their sites, but there are many addons which collect information about users behavior

bennetthaselton: a system getting hacked is an astronomically bigger problem than someone being "offended" because their software updated itself

Bill Leninger: From an IT standpoint, Bennett, you are right. For a user standpoint, if they rely on IE or Firefox to do mission critical work, and an update breaks their ability to work, then IT hears about it.

Brandon Palmen: @bennetthaselton, it depends on the application. A browser update might be welcome, but adding 'genius' to iTunes might not.

bennetthaselton: yeah I was talking about security updates and not feature updates

Brandon Palmen: ok

bennetthaselton: Bill: I think that goes back to the question: Is a user more likely to be hosed because they DID install updates or because they DIDN'T? Either option has its risks

bennetthaselton: the difference is that if they get infected because they didn't install updates, they're less likely to blame the vendor or the IT department. On the other hand, if they get hosed because of an update, they might blame the vendor and call IT.

bennetthaselton: But logically speaking, you should just choose the option that has the lower risk either way. The problem is that we've set up people's perception of the problem to disproportionately blame (or at least call) IT as a result of problems caused by updates. That results in a bias against updates, even when that might be the option that has less risk and cost overall.

erezson has left the meeting.

Brandon Palmen: But clearly, corporate users surf the internet with IE6.

Dino Dai Zovi: But no one prefers using IE6, they only surf with it because that's what's installed

erezson has joined the meeting.

Bill Leninger: Another issue would be if all our sw vendors start doing auto updates at various times. Then my PC "breaks" - which update did it? How do we manage that?

erezson has left the meeting.

chip: RE IE6: We have IE6 as a standard and are starting to feel the pain with sites shutting out IE6. the problem is that we have products that don't support later than IE6 yet. The initiative this year is to push the vendors to make their products work. In the end, it's up to companies to push vendors to make things work. Windows is out in 64 bit flavors but not widely adopted because of compat problems. When MS makes next windows only 64 bit, vendors will have to comply to keep up. Someone has to push the vendors to stop supporting that small portion of the environment. Same could be said for updates. If every app silently updated, no one would think differently about it and we'd all trust them.

bennetthaselton: Bill so maybe both of those problems could be solved if auto-updated software incorporated a protocol that let the updates be pushed to a central corporate server, and then IT could decide when to roll them out to client machines

Dino Dai Zovi: chip: Also, the big issue is that the Internet and Intranet churn at very different speeds

Dino Dai Zovi: trying to slow the Internet down or speed up the Intranet is very difficult. I think the way forward is to split them.

chip: dino: that they do. and you have developers that are just well, stupid and don't test their code for new technology.

bennetthaselton: So wouldn't this be a pretty simple protocol? Say a company like Adobe tells everybody, "Here's a URL where your IT department can automatically check for new updates to the software. And then your default config for your users could be for their software to check not OUR servers for updates, but check some server on IT. So then when IT is notified that an update is available, they test it on some test machines. Then your IT department can decide when to post it on the internal share, where people's client software checks for updates.

bennetthaselton: Bill or Chip, would that solve a big part of the problem, or would there still be issues that this wouldn't solve?

Bill Leninger: Yes, Bennett, i think you have a great suggestion. It would be nice if there was a trusted clearinghouse that could thoroughly test updates in a timely manner. Sort of a "stamp of approval".

chip: bennett, i like that idea.

bennetthaselton: by trusted clearinghouse, you're talking about your own IT department presumably, not a central clearinghouse on the Internet

Brandon Palmen: Is there a place for a centralized update notification/subscription service that allows outside vendors to use windows update, in much the same way that 'Microsoft Update' updates all Microsoft products and not just windows? I thought I read somewhere that Microsoft was considering opening that system up.

chip: supposedly, adobe has some methods that you can use SCCM to pull the adobe updates into the catalog and push like MS updates but we havne't been able to find it. it's on the list to look this year. they're one of hte few that has even tried to go down that road.

Bill Leninger: actually I was thinking an Internet clearinghouse for home consumers as well

chip: I, as an IT packager, tester and licensing person, have looked high and low for a place that can clearinghouse updates but there's not much there and what's there you get a lot of noise.

bennethaselton: hmm but I think the Internet "clearinghouse" would still leave you as the IT department with all of the headaches that you had before -- you wouldn't necessarily know when the updates were about to happen, and then if everybody updates all at once, you get phone calls asking what the hell happened, even if nothing broke

Bill Leninger: good point...

Bill Leninger: I was thinking something along the lines of PatchLink where they test patches before putting them on a PatchManagement server

chip: Also, how do you deal with users that do have the ability and rights to their machines to update on their own? While we might manage (even loosely) 80% of the machines, the rest have admin rights which is why I have 65 different versions of JRE out there.

bennethaselton: well I figured that the company itself was supposed to test the patches pretty thoroughly, more than a nonprofit clearinghouse would normally be able to

chip: re possible configs and testing, JRE is a prime example where bad programmers use "=" instead of ">=" in the code and we have to have 1.4.2_05 installed because of bad code.

bennethaselton: I thought it sounded like a lot of these problems were not from inadequately tested patches but just because of the bandwidth costs and the surprise from users when they get updated

bennethaselton: so that's where you could use a repository that IT downloads the updates to, and then pushes them out to users when they want to

Bill Leninger: admin rights is a great point too. Our folks don't have admin rights to their PCs, so we hate touching each pc to apply those patches.

Brandon Palmen: Right, develop an RSS-like specification for describing updates, and then create an aggregator of those feeds (like Windows Update) that IT administrators can use to filter and deploy.

bennethaselton: all of this chat is "public record", right? I write for slashdot sometimes about security issues and it would be interesting to make a suggestion about a protocol for downloading security updates to a corporate share and then pushing them out to users

Brandon Palmen: yeah, an extension of RSS maybe

bennethaselton: I assume the app would still need to check that the updates are digitally signed by the software company. Otherwise you'd have malware programs changing the location where your application downloads the updates from. (Of course once an untrusted exe is running on your machine, you're hosed anyway, but at least don't make it too easy for malware to change how updates are downloaded.)

bennethaselton: waaaaay back at the beginning, I wrote: A point about Linux auto-update disclosure: A lot of Linux servers are remotely hosted servers where the admin is never "sitting in front of them" (that's certainly the case with most of my hosted sites). So it's not immediately obvious how the server would "notify" its owner when it's updating itself. It's not like a Windows desktop where you simply flash an alert on the screen.

bennethaselton: perhaps what we need is a protocol whereby applications running on a Linux machine can notify the admin even if the admin doesn't sign in to the machine frequently. Like saying that when you set up the machine, you have to enter the administrator's e-mail address, and then if the machine detects that updates are available, it sends an e-mail to that address that says "Hey, you have to log in to install these updates" or "Hey, these updates will be installed automatically at 2 AM tonight"

chip: I'm all for silent updates as long as the app is manageable in some way. you have to configure it to be notified somehow or turned off altogether.

bennethaselton: is there a way to reach participants after the chat? if I'm writing a post for slashdot and wanted to ask some more questions for Bill and Chip (or anybody else) about what app features would make it easier for IT to apply updates

chip: I'm fine as long as the company name is kept out of it. they have issues when that is used. if it's me and my opinion or even that I work for a large company, I'm fine answering.

Ohm Prasanha: our email ids are registered here... for contact.

me: I can connect people if you e-mail me at contact@stopbadware.org

bennethaselton: sure I wouldn't mention who anyone works for is there a way to click on someone's name to see their e-mail address?

chip: to that point bennett, something that companies need to do is make their products easy to deploy. Don't sell me something that takes 6 months to deploy. sell it to me and have me deploying it tomorrow. that's how it should work.

Bill Leninger: I'm fine with sharing later too.

bennethaselton: if anybody wants to reach me with ideas, my email is bennett@peacefire.org

Dino Dai Zovi: Similarly, I'm ddz@theta44.org

bennethaselton: I think I'd at least like to write something about a possible protocol for pushing updates to an IT share and then letting IT roll them out to users.

bennethaselton: what do you think of the protocol for a Linux server to notify its administrator that updates are available and need to be installed? Is there a simpler way to do that?

bennetthaselton: oh wait, I guess it's almost 11, was it originally planned to wrap up after an hour?

bennetthaselton: that's a good idea. who's talking again?

me: that's Dino

bennetthaselton: I had asked some people about that before, auto-updates with no user intervention, but a lot of people said that they wouldn't want their linux machines auto-updating themselves because then if the update fails and the server goes down, they have no idea what happened

bennetthaselton: Maxim that's a good idea to use that as well, I'm concerned that for things like syslog that many "amateur" sysadmins who get cheap virtual private servers for \$10/month, might not know how to use that. But they know how to check their email

Ohm Prasanha: I've a point, the auto-update mechanism has a freedom to check the license of the installed product and distribute badware if product details are expired/out-of-date/invalid or similar...

bennetthaselton: Maxim can you take a minute to say where people will be able to view the transcript of the chat after it's over? (Is just the text transcript posted, or will the audio be archived as well?)

Dino Dai Zovi: If you have redundant machines, you can apply updates automatically to one on day 1, if it breaks, fail over to the second box

Dino Dai Zovi: otherwise, apply updates automatically to the 2nd box

bennetthaselton: yes I think that you should always allow updates even for pirated software, the main reason being that if you don't allow updates, it's *other* people who get punished, not just the owner of the box. Because the box is used to send spam, attack other machines, etc.

me: I unfortunately neglected to record the audio, which I intended to do. However, I will try to save the text chat and make it available via our blog.

Ohm Prasanha: even outdated anti-virus s/ws compell the user to renew... or threaten using this issue of supplying malware...

bennetthaselton: I think MS backed down from that after a lot of people made exactly that argument, didn't they -- so I thought now you could get updates even without checking genuine-ness

chip: vendors do enough as it is to enforce their licensing with activations and handcuffs so much so that it prevents the honest company from managing their software effectively. i have had conversations with more than one about how their scheme handcuffs me from managing the product.

Brandon Palmen: I think most security updates are available without a WGA check, but things like service packs may still check for a genuine license

chip: Updates are updates. legit or not. patches should patch, service packs should be roll ups of patches and they should keep feature updates separate.

chip: keeping them separate will allow an organization to decide what to deploy and how. they can be secure and not worry that the new version of reader now installs the google toolbar.

bennetthaselton: great job Maxim, thanks for pulling this together

Dino Dai Zovi: yes, thanks

chip: thanks! interactive chat is the way to go with a small audience.

Ohm Prasanha: thanks for this great opportunity!

Bill Leninger: dimdim was a great tool

Ohm Prasanha: yeah very much

chip: looks like you can copy/paste directly from the chat window