



SECURITY NOW!



Transcript of Episode #123

Jungle Disk

Description: Steve and Leo invite Jungle Disk's creator, Dave Wright, to join the podcast to talk about his \$20 product that allows for extremely economical, efficient, seamless and absolutely secure online storage of any user data within Amazon's high-performance, high-reliability "S3" storage facility.

High quality (64 kbps) mp3 audio file URL: <http://media.GRC.com/sn/SN-123.mp3>

Quarter size (16 kbps) mp3 audio file URL: <http://media.GRC.com/sn/sn-123-lq.mp3>

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 123 for December 20, 2007: Jungle Disk. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now!. Here we are just a few days away from Christmas, celebrating the holiday season. And most of the TWiT shows have gone dark and are quiet, and there's - we put up the stockings by the chimney with care, and not a mouse in the house. But no, Steve Gibson, he's an animal. He says, "I'm not missing a show, dagnabit." So we're do a show this week. We'll do a show next week. We'll even do a show the week after.

Steve Gibson: We're doing a show while you and your family are in Egypt, Leo.

Leo: Right now, let's see, we're not there as this airs. But we will in a few days. And so next week's show, by then I'll be in Egypt.

Steve: And a week after.

Leo: I'm training Dane on how to post these, so if it's late, it's not my fault. I didn't do it. No, it'll all be fine. In fact, I think I can get wireless in Cairo. The hotel we're staying at I believe has wireless Internet. So Happy Holidays, first of all.

Steve: Yes, to all of our listeners.

Leo: Yeah, and to you, too, Steve. And I guess we should - coming up in just a little bit we're going to talk to the guy who writes Jungle Disk. Tell me a little about that. He's Dave Wright.

Steve: Dave Wright, W-r-i-g-h-t. It's funny, in their online forum postings he goes by "Jungle Dave."

Leo: I like that.

Steve: And this is something I think that a questioner, one of our Q&A people, brought to my attention, said hey, what about Jungle Disk and the Amazon S3 service? Is it secure? And I took a look at it...

Leo: Well, the best way to find out is to ask the guy who wrote it.

Steve: Exactly. So we have him on the show today. And he's going to answer all of our questions.

Leo: We, I'm sure, also have some errata. Before we get into that, some follow-ups, and in fact the first one I know is something that's been bugging me, but we'll talk about that. And then we both have our Kindles, and we'll talk a little bit about the Kindle. Let's start by answering my question. It was bugging me. I keep trying to vote for you, your Kindle review.

Steve: Oh, Leo, you and a large body of our listeners.

Leo: Oh, good.

Steve: First of all, of course, I spaced out last week and the week before because I was saying "snipurl/skr," forgot to say "snipurl.com."

Leo: Oh, well, everybody knew that.

Steve: Well, I hope so. Anyway, it turns out that you were exactly right when you were trying to do this when I was giving you that shortcut. It must be that Amazon has some bot prevention technology.

Leo: Oh, so you can't go directly in.

Steve: Exactly. And of course we know from our episodes about how the web works that if you click on a link from within Amazon, there will be a referrer field in the query that says hey, the user was on this page and clicked a link to come here. So it's trivial for them to, for example, remove the voting buttons if you jump directly into Amazon rather than click on links in Amazon to go here.

Leo: They don't like deep linking probably. That's probably what it is.

Steve: Exactly. So a bunch of users wrote and said hey, Steve, love to vote for you, but Leo's right, there's no buttons. Well, enough people apparently poked around, I know that Elaine is one of them, our transcriptionist...

Leo: She really wanted to give you her vote. That's cute.

Steve: Yeah. So I was back on like the fourth really, really long page back, and I thought I would never surface. But enough listeners made the trek in that I'm now on the - my review of the Kindle is now, like, the fifth one on the first page.

Leo: Oh, good. We're trying - we should explain. The reason is there's so many reviews of the Kindle that aren't really very substantive, in fact many of them by people who don't own Kindles. And so we've been just trying to get Steve's ranking up a little bit on the Amazon page so people can read a thoughtful, I think a very thoughtful review.

Steve: Well, and Leo, most of them are by people who don't own a Kindle. They just think it's a bad idea. And it's like, okay, well, that's not a review. That's just sort of an annoyed opinion. Anyway, so...

Leo: Right. Well, most reviews are annoyed opinions, let's face it.

Steve: Well, anyway, so I did want to tell our listeners, if anyone was confused, I'd still love to have people's votes just to kind of keep me in the running there with all the others because, again, the reviews are generally long, and it does take some bit of slogging along still to get down to mine. So if anyone goes to the Kindle page, a link near the top of the page is Read Reviews. And then, I don't know, I'm like the fifth or sixth one down. But again, if people like what I wrote and would say yes, we thought that was useful, that would help to keep me up there in the ranking.

Leo: So I got my Kindle about a week ago, and I traveled with it. You know, I was gone to New Haven for five days, and it was a really good time to try it. And my initial reaction is, if you're going to buy an eBook reader, it's certainly the one to get. There's just - there's no question. It's easy, it's actually, because of their choice of fonts, it's much easier to read.

Steve: Yes, the fonts are much better, aren't they.

Leo: Yeah. And you can get the font size bigger, which as a person over 40 I appreciate. And the wireless, as we've talked about, the wireless really does make it so much easier to put stuff on it. I haven't ever hooked it up to a computer. I get a number of newspapers. And so for that reason alone the hundred dollars differential between that and the Sony is, I think, well worth it. But I think that there are also lots of people, a great many people, probably the vast majority of people who will never buy an eBook reader, at least not until the eInk technology improves and is crisper and so forth. Those people aren't going to like it anymore than they'd like the Sony. But I think it's certainly true, if you're going to

choose between a Sony and the Kindle, that the Kindle is far superior.

Steve: I agree. I think certainly people who own prior generation eBooks, I mean, if somebody already has a Sony, they'll probably be inclined to continue purchasing Sony eBook content, even though Sony has only about a quarter of the...

Leo: Much more limited, much more expensive, and much more difficult to put on. You need Windows; you need a USB connection. I just, you know - for instance, I was looking for a book on Egypt. I wanted to do some reading before we go to Egypt. I went, I searched, found several hundred volumes on Egypt, available through the Kindle store. You can search online. And I bought a book. Wasn't cheap. Now, it's funny, they have very expensive books on Egypt, I guess. And it was 35 bucks, which was still cheaper than the hardcover.

Steve: The pyramids are those pointy things, Leo.

Leo: Yeah. See, that's the problem, is most of the books -oh, another thing I want to say that I love that you can't do in the Sony store is you can get samples. And so instead of buying kind of sight unseen, I was able to get - I got samples of the top five books I was interested in, read one, and it was just so bad, I was able to reject it. So I was able to pick the right one. And that saved me a lot of money right there. And if you're into the bestsellers, you could before you go on a trip get samples of all of them, read them on the plane, and pick the ones you want to finish.

Steve: I think also you are able to have multiple Kindles associated with the same account.

Leo: Oh, that's interesting.

Steve: Yes. And so you're able to buy a book once and read it on multiple Kindles.

Leo: Now, why would you do that?

Steve: Well, husband and wife might. I know a lot of couples who, like, hand books to each other. It's like, okay, I'm done with this, you want to read it? And so you're unable to do that with the periodical content. You have to individually associate those with individual readers because they don't want that to be shared. But book content you explicitly can share among multiple Kindles.

Leo: That's interesting. And that is one of the complaints, and I think rightly so, although it's inevitable, that people have is the copy protection on the Kindle. But there's no way a publisher is - that's not an Amazon issue, that's a publisher issue.

Steve: Exactly. That's not going to go away. And the point I made in my review was that I've already got copy-protected content spread around. I was an early adopter of the Mobipocket format, which of course Amazon ended up buying as part of their move into eBooks. And then Palm, and then Sony, and finally now Amazon. And my feeling is, okay, sure, this feels like the

first-generation device. The screen's going to get better. The UI is going to get better. There will be lots of things about it that improve over time. I mean, that's been the history of eBooks, rocky as it's been. But if I'm going to be investing now in a format, it seems to me Amazon's going to win this.

Leo: Yeah, I agree.

Steve: Already, right out of the gate, this is the best eBook reader there is.

Leo: You know, the paperback is not going away. And I will still buy books. So it's going to be more the stuff that I read once and I don't want to have a copy of it. So I'm not really too worried about whether I'm going to be transferring stuff over to a new Kindle. I have to say the cover stinks. They've got to get a better cover.

Steve: Yeah, the cover's not good.

Leo: The Sony cover is, in fact, in general the Sony design is much more elegant all around.

Steve: I was thinking that I was forgiving the fact that there was a keyboard there because you end up holding it down...

Leo: You have to.

Steve: ...in the keyboard area.

Leo: There's nowhere else to hold it.

Steve: Exactly, because if you hold it anywhere else it changes pages on you. But then I'm like, I've never used the keyboard. Well, maybe once or twice. But it's the most underused aspect of it for...

Leo: I've used it because I've searched for books and purchased books that way. So you need, you have to have it. Although I guess you could have some sort of strange selection technique. But I think you have to have it. And it is where you hold the darn thing.

Steve: We ought to say, though, Leo, that the comment you made early on, the reason that you made the decision to purchase was the fact that you subscribe to a bunch of newspapers. And for me, I think the connectivity is very cool because the content is just there in the morning when you go off to coffee, and you've got your newspapers and magazines and things.

Leo: One thing that is really cool that wireless allows. So I'm reading along in a book, and the guy says, "No more 'mute inglorious Milton,'" in quotes. And I'm going, boy, I know that quote, "mute inglorious." Where could that be? You scroll to that part of this thing,

you click the button, you search for it, it says Search on Wikipedia, Search on Google. I searched on Google, immediately found Thomas Gray's "Elegy Written in a Graveyard" ["Elegy Written in a Country Churchyard"], which is - that's the poem it's from. Got the full text of the poem and was able to read it. And that is a very interesting addition to a reader. You can look up words. It's got a built-in dictionary. But you can also go on the 'Net and look it up on Wikipedia, or even do a general Google search. And that kind of changes how I read. I mean, I think that's really great. Something you can't do unless you're at home with your reference library.

Steve: Yeah, it truly is connected.

Leo: Yeah. So anyway, I know people sometimes, there's a small percentage of our audience goes, no more electronic book stuff. All right. We're going to talk about security, don't worry. But I just thought we should finish that up since I have had one now.

Steve: We just lost our bandwidth.

Leo: I know, I don't know what happened. You know, I think it's probably because I went to the Kindle site. That was my mistake. It's a very - it'll get better in a second.

Steve: You want to drop me and reconnect?

Leo: You sound fine.

Steve: Oh, really, okay.

Leo: You sound a little crunchy, but not badly, so.

Steve: Okay, cool.

Leo: Let's see. So I guess we should - oh, wait a minute. Any other erranda? Errata and addenda?

Steve: I have nothing else except I do have a really unique and interesting SpinRite story to share. Around the middle of last month, middle of November, Chris Wickersham wrote an email saying, "SpinRite Saves the Encrypted Day." And he said, "Hey, Steve, I know you get a lot of emails detailing how SpinRite saved the day. But I thought my situation was unique enough that you might enjoy hearing my story." Well, you know, parenthetically, I like hearing everyone's story.

Leo: As long as it's good about SpinRite, why not?

Steve: Please keep them coming. Anyway, he says, "I work for American Express, and we have an exclusive contract with IBM to do our desktop support. We all use ThinkPad laptops. And

somewhat recently, to my great relief, our hard drives have been encrypted with a PGP tool."

Leo: Oh, that's neat.

Steve: "This makes me feel much safer as it rides home with me every day after work. Well, after a long weekend of work, I booted the machine Monday morning to check my mail, and the unthinkable happened. Windows repeatedly bluescreened during the boot process, saying that it had an unmountable boot disk. I traced the problem to a driver that was corrupted on disk and was hoping that IBM would be able to replace the fouled driver and get me back up and running once I got into work. Unfortunately, I had not checked my work into CVS when I shut down Sunday night, so I was very anxious. Well, shock of all shocks, the tech guys at work were unable to repair the corrupted file on the drive because of the encryption."

Leo: Oh. We've talked about this before because it's a big binary blob.

Steve: Exactly, I mean, it's not a file system. You can't - if it won't mount and boot it's just, I mean, it's completely opaque. Anyway, so he says, "Worse than that, they had no way to mount the drive so I could recover my data because of the encryption. They used several tools to recover the drive, but to no avail. So I threw caution to the wind and asked if I could take the drive home and try SpinRite. Surprise. After about an hour, SpinRite recovered several damaged sectors, and my machine successfully booted into Windows."

Leo: The big surprise is that they let him take his computer home to work on it with SpinRite. That's the real surprise.

Steve: He says, "I can't wait to tell them how well SpinRite worked. And I hope that this leads to another site license for you, as I can't imagine I will be the last person to lose some important information on an encrypted hard drive. Take care, and thank you for SpinRite."

Leo: That's a nice story. But really important to remember if you've encrypted is that you've got to back up because you don't have any - there's no file recovery.

Steve: Exactly.

Leo: You're kind of in trouble. All right. We're going to - let's introduce Dave. He's ready to go. And he is - David Wright is the author of Jungle Disk. Where are you calling from?

DAVE WRIGHT: I'm in Atlanta.

Leo: Great. Well, sounds very good. Steve's in Irvine. I'm in Petaluma, Northern California.

Steve: Yeah, we've had actually - David contacted me after we first responded to, I don't know if it was a user question. I think it might have been driven by a user who said hey, you know, what's the story with Jungle Disk and the Amazon S3 service. And I took a first look at it, and sort of from a cursory standpoint I was impressed. And the question I had, that I had not answered for our listeners, was whether it supported, you know, my acronym that I like is TNO,

for Trust No One, did it support a mode where it operated completely free of any sort of oversight, whether the data being stored on behalf of the Jungle Disk system was stored opaquely from Amazon's standpoint so that it was impossible for them to decrypt it and so forth. And so David shot me back a piece of email and said yes, it does support TNO.

Leo: Trust no one.

Steve: Trust no one, exactly. And then since that time we've had a bunch of listeners sort of pretty continuously, a little constant flow in the background, saying hey, whatever happened with Jungle Disk? What's the story? So I thought we'd get Dave on and talk to the man who put it all together.

Leo: So Jungle Disk is kind of like a shareware deal; right? How exactly do you do it?

DAVE: Yeah, I mean, it's a pretty typical software model. There's a free trial of the software available for 30 days. You still have to sign up for an Amazon S3 account. But after 30 days, if you like the software, you can purchase it for 20 bucks. It's a one-time purchase. We have free lifetime upgrades, as well, so you're never going to have to worry about getting the latest version.

Leo: And for people who want to use S3 as kind of a backup system, Jungle Disk just makes that completely straightforward and easy.

DAVE: Yeah, Jungle Disk has a built-in automatic backup feature. So you can just tell it what files and directories you want to keep backed up. But it also is fairly unique in that it exposes the S3 storage as a local drive letter, or a mounted volume on Mac, which allows you to use third-party backup software, too. So if you're got other backup or synch software that you prefer to use instead of the built-in functionality, you're free to use that, as well.

Leo: Why would I want to use a third-party app?

DAVE: Well, you know, the built-in automatic backup is probably sufficient for 90 or 95 percent of our users. But some users have very specific backup requirements in terms of what they want to back up, when they want to back up, either very advanced scheduling or just finer control over what they're backing up than the built-in automatic backup provides. But we find that - go ahead.

Steve: No, I'm sorry, I was just going to say, I'm actually a really good example of that. And we were talking about this just the other week, Leo. I use something called FileBack PC, which is a very sophisticated backup tool that allows all kinds of wildcard expressions and, like, bizarre limitations on the minimum and maximum rate at which files can be backed up. It allows you to do versioning and multiple versions and things. So basically I could just aim my existing tool that I'm already aware of and I own and I'm comfortable with, at a Jungle Disk volume. And these things then go to Amazon rather than being stored on another drive locally.

Leo: And the nice thing about Amazon storage is it's very inexpensive.

DAVE: Yeah, I mean, it's extremely cost effective. The basic rate is 15 cents per gigabyte per month, which is very inexpensive. Now, they do have additional fees based on the amount that you upload and download. But over the long run the bulk of your cost is going to be your monthly storage fees because that's what you're having to pay each month. And at only 15 cents per gigabyte, most Jungle Disk users are only paying, you know, a couple bucks, one, two, three dollars a month, for the actual storage that they're using. So it's pretty cost effective.

Steve: Well, now, it's also multiplatform. You've got Windows support and Mac support and Linux support. And then additionally you're able to run this, which I think is very cool, from a USB device so that it runs in a no-install sort of mode. So literally, if you had a little USB dongle, you can carry that around with you. You stick it into any machine. It's able to connect through that machine's Internet connection to Amazon. And you have then access, you basically have secure roaming access to your whole archive of data stored by Amazon.

DAVE: Yeah, that's right. That's something that we got quite a few requests from for people that wanted to use the software remotely without having to install it or keep any files on that local machine. They can just bring their USB keychain, plug it in. It's got their configuration already on it. It's got their encryption keys already on that keychain. Fire it up, copy down the files they need, upload any new files they need, pull the keychain out, and it's all gone from the machine.

Steve: So, okay. You have a 30-day trial. Right now you're calling it an introductory offer for \$20 that allows you essentially lifetime use of this. What's the model? Is there a deal with S3 where you get a piece of Amazon's action?

DAVE: No, no, no, not right now. The user pays Amazon monthly for that service, and that money goes to Amazon and pays to keep the service running. You know, our model is pretty straightforward. We're selling the software. And we're able to have the rate that low just because this is a mass-market product. This is something that at least we think everybody needs on their computer, that everybody needs to be doing backup. And online backup is really the way to go these days. So we've got a huge target audience that we're looking to sell into. And we don't want to limit ourselves by pricing it, you know, at 50 or a hundred bucks or something like that. We want to make it as easy as possible for people to sign up, download it, and start using it right away.

Steve: Very cool. So really, so the motive for you was you saw the service that Amazon was providing and said hey, you know, we can write a really cool and unique front end to the Amazon S3 service, which is not itself a turnkey end-user sort of consumer-level service, it's always meant to be a back-end data storage solution, and that it needs other front ends like Jungle Disk in order to actually make it useful for end-users.

DAVE: Yeah, I mean, a lot of people ask, well, you know, if I'm signing up with Amazon, then why do I need Jungle Disk at all? And the answer is that, like you say, there's no front end to Amazon S3. You can't go to an Amazon S3 website and browse your files or upload files. And Amazon doesn't provide any software for it yourself. So you have to use a third-party application like Jungle Disk to get access to S3. And Jungle Disk is even fairly unique in that area. A lot of other companies are using S3 as back-end storage for their filesharing or backup or whatever company. But they don't actually allow you to have your own Amazon account and have control over your own data on Amazon. Jungle Disk is fairly unique in that respect, at least among the commercial software, because even though you're buying this commercial piece of software you still have your own Amazon S3 account. You still have complete control over your data. And our company doesn't see or have access to your data at all.

Steve: I have to say, I've spent a lot of time now going over your website, reading the FAQ, looking at the instructions. I've got it installed on several of my machines. And that's one of the

other nice things that you explicitly allow is one copy, one registered copy of Jungle Disk can be used on a single individual's different machines and give them then sort of like centralized access to this repository in the sky which Amazon maintains. Amazon is storing things redundantly within their own network, which is obviously robustly connected to the Internet.

DAVE: Right. I mean, that's something we heard pretty strongly from users is that they wanted to use the software on many machines, home machines, work machines, laptop machines. And so it really didn't make sense to try to sell the software on a per machine basis. Some of our users would have to buy five, six, seven copies. So we just said, look, you know, we're going to make it as simple as possible. Buy one copy, put it on as many machines as you want. You know, it can only be used with your Amazon S3 account. So if your buddy wants the software he's going to have to buy it himself. But we don't try to limit them on what machines they can put it on or even what platforms. When you buy it, you get all three platforms. So if you've got Mac and Windows machines and you want to share files between them, this is certainly a good way to do it.

Steve: Now, in use there is a little contact by the Jungle Disk client back to you guys. What's that about?

DAVE: Well, you know, on startup we have a typical automatic update check. It reports to us the version and some information about the client so that we know who's using the software, and for the trial users we know when their trial period is up. Once you purchase the software, though, you have the option to turn that off completely. So if you're one of those super paranoid people that doesn't want the software talking to anybody but Amazon, you can certainly do that. We recommend users keep it enabled because it does provide update notifications, which can certainly be important for software like this. If some kind of security issue was discovered, we want people to be able to find out about it. So we do provide the option to turn that off, though.

Steve: That sounds cool. I mean, it's everything that I know that our listeners want.

DAVE: Sure.

Leo: I have - I use ChronoSync, and I'll probably use your program, too, Steve, on my PC. So that sounds like - I've been trying to figure out a good way to get this working with S3. Also trying to get it to work for my web server because it would be really nice to back up web server stuff to S3.

DAVE: Yeah, we've got, you know, we've got a few people already that are using it on servers. And it's not really targeted towards that market right now. It's really designed to be a desktop consumer product. But, you know, there's a lot of people that are interested in using it in offices or in servers, too. So, you know, you can certainly use this current version of the software in that space. But we're probably going to be developing some additional editions of the software that's more directly targeted towards server platforms, for example, in the future.

Leo: That'd be great.

Steve: Well, and speaking of servers, I know that, Leo, you and Paul have been talking a lot about Windows Home Server. And Paul's a big fan of that. And there is a version of Jungle Disk specifically for Windows Home Server. How does that differ, and how does that operate, Dave?

DAVE: Yeah, that's right. In conjunction with a contest that Microsoft was running earlier this

year, we developed an add-in for Windows Home Server that's based on the same technology as Jungle Disk, but it is a separate product, and it does work a little bit differently. But basically what it allows you to do is install this Jungle Disk from Windows Home Server directly on your home server machine and select which files on your home server machine you want to have backed up online. And from there it takes care of it automatically. It just keeps everything backed up that you've selected on your home server. And if you ever need to restore it because your home server crashes or because, you know, you accidentally delete something, you can use the Windows Home Server console to select the files and restore it directly back to the Windows Home Server box.

Leo: That's neat.

DAVE: So that edition of the software is in beta right now. There's actually a free beta version of it people can download from our website. And so far the response for it's been very good. We actually came in second in the Microsoft contest, so that was exciting. But the Windows Home Server audience is obviously very interested in data protection, and this really just increases the level of security that you get by backing up your important files offsite.

Leo: Well, Paul must have seen it. He was a judge in that Home Server contest. So I'm sure he voted for you.

DAVE: Yeah, yeah, Paul was.

Leo: Yeah, I'm sure he voted for you. Very cool. Very neat. And Amazon is to be praised for not only providing the service, but providing APIs that developers like you could hook into. Was it pretty easy to write this software?

DAVE: Well, you know, the initial version, it took a little bit of time to get together because Amazon built it as a very generic service. They didn't build a lot of the things that would be very handy for a backup service. But because it's a generic platform and they want it to be used a lot of different ways, they provide a very sparse API. So we've had to build a lot of functionality around it to get it to work well for customers. So...

Leo: Are they using WebDAV, or are they doing something else?

DAVE: No, they have a proprietary REST API, and they also have a SOAP API available. Now, one of the secrets to Jungle Disk in terms of how it actually works is that it exposes a local WebDAV server and proxies and changes that request into a proprietary S3 request. So on your local machine, and this is the way the drive mapping works, it actually exposes a little WebDAV server so that your local operating system can talk to it over WebDAV. And then it translates that request into the proprietary S3 API.

Leo: So that's how you do it. That's very clever.

Steve: Yeah. A perfect example, I think, of the sparsity is, for example, the way Jungle Disk handles file renaming.

DAVE: Yeah. For example, Amazon S3 doesn't have built-in support for renaming files, which would seem really simple. But again, in their design they wanted it to be a bulk object storage-oriented interface. And so they didn't provide a way to rename objects. And so what we've done is we made use of another service offered by Amazon, which is called EC2, which is a virtual hosting service that allows you to host servers within Amazon datacenters. We made use of EC2 to build functionality that allows you to rename files without pulling them down to your machine and reuploading them back to Amazon. And so it does it in a fast and secure way, directly on the Amazon network.

Steve: And I guess really the last thing to talk about, well, I don't know if it's the last thing to talk about, but really the genesis of this whole question of Trust No One is the way Jungle Disk works with sort of the keys you always have when you work with Amazon, and then the ability to create your own sort of pre-Amazon encryption which is completely separate from anything Amazon has any knowledge of.

DAVE: Yeah, that's right. So Amazon provides, you know, pretty typical authentication through a secret key that, you know, is shared between you and them. And that's used to authenticate access to your account, prevent anybody else from getting access to your files. But then on top of that Jungle Disk layers its own encryption that takes place on the client, so Amazon never sees the unencrypted content at all. The encryption takes place on the client. You can select a custom key, anything you want. It's 256-bit AES encryption, so it's extremely secure. The encrypted content gets uploaded to Amazon. And when you need to pull a file back, it pulls the encrypted data back from Amazon and decrypts it locally with your key. And if you don't have the key, you don't get the files.

Steve: Do you think that Amazon themselves uses the user's key to encrypt the data when it's stored statically at their end? Or do they just, like, just store whatever you give them and make no attempt to protect it from, like, people over on their side?

DAVE: You know, they don't really say a lot about the internals of how the service works and whether they encrypt it or not. One of the things I certainly know about it is that they use a very proprietary back end and storage system for this. So it's not like they're just dumping it on a file server that somebody even at Amazon could go browse around. It's stored in a very, you know, unique, proprietary format. So I don't know whether they layer encryption on top of that or not. But we always tell users, if you're concerned about that type of privacy for your data, then you definitely need to encrypt it on your client before it goes up because that's the only way you can have complete confidence in the security.

Steve: Right. And then I also like the way you guys have handled the issue of key migration, that is, if you have a bunch of content already encrypted up on Amazon, and for whatever reason you decide you want to change the key, the problem is of course that that prior content has been encrypted with your first key. Now you want to go to a second key. You put a little header and some metadata on the front of each file to identify which of the user's keys was used for encryption without actually having the key there, so nothing in the metadata at the top of the file allows anyone to decrypt it. However, it allows Jungle Disk to still be able to access old content encrypted with a prior key, so long as you've left that key in a list of keys that Jungle Disk has access to.

DAVE: Yeah, exactly. We basically allow you to change your key anytime you want. But again, because the encrypted content is already stored at Amazon, unless you want to reupload your file to reencrypt it with a different key, you know, we need to keep a list of your previous key so that if you ever go access that content that was encrypted with an older key, it can still be accessed. And we keep track of the key that's used for each file in a special metadata section that Amazon provides. And that lets us know how to decrypt the file when it comes back. But it's done in such a way that's secure and that it doesn't tell anybody anything about which key was used for which file, and they don't know anything about the keys.

Steve: Right. Well, I just love it. I think it's, you know, it answers, I think, a huge need,

especially as people become more mobile. I like the idea, for me, not only of being able to back things up, but to keep copies of files that I'm working on that are like ongoing references. Like I run my life on outlines. And so to be able to put the outlines there and keep them synchronized so that I'm not having to manually synchronize my various machines, I mean, it's just - it's a really cool solution.

DAVE: Yeah, I think so. I mean, that's really what our customers are saying. Everybody's been talking for a long time about storage moving into the cloud. And, you know, there's been a lot of issues around that, specifically around trust. And so that's one of the big things we've tried to address, both on the back end by having Amazon manage the back end as a large, trusted company that you know isn't going to disappear tomorrow or run off with your data; but then also address the security on the client side with the encryption so that you know that nobody, even Amazon, is able to actually access and see your data. It's completely under your control. And I think that those two things together are what are finally enabling people to say, you know what, I finally can trust to put some of my important data on the 'Net and access it, you know, wherever I travel.

Leo: That's cool. Jungle Disk is free for 30 days, \$20 for a lifetime license. You can get it from JungleDisk.com. And of course Amazon S3 is an additional charge, 15 cents per gigabyte storage per month. But it ends up being very, very affordable. And, yeah, a great place to have it in the cloud. There are, of course, packaged solutions like Mozy and Carbonite that are easier probably for people to use, but not as portable by any means. Thank you so much, Dave.

DAVE: All right, well, thank you very much.

Leo: Really appreciate your time.

Steve: Thanks, Dave.

Leo: That's Dave Wright from Jungle Disk.

Steve: I'm really glad we've covered this, Leo. As I've said a couple times, I've had a constant stream of our listeners sort of pinging me every few weeks saying hey, Steve, you were going to check in on the Trust No One operation. And I've got to say, I mean, you get a feel for things as you use them. And I really got - I have a really good feel about this. To me, the operation of the tool is very transparent. Their motivation is very transparent. They even provide an open source set of files that shows how they access Amazon. And although for \$20 I don't think there's anyone who's going to go develop their own client copying Jungle Disk, and it doesn't have all the features that their client does. But the whole thing feels just solid and open. And it's just - it's done right. So as a solution for what this is, that is, the idea of being able to use Amazon's S3 service in a very, very trust-no-one secure fashion, Jungle Disk does it.

Leo: It's neat. It's really neat. Again, I think it's cool that Amazon does API. And it's not a very sophis- as he said, it's not a very sophisticated API. It's basically just using existing technologies like REST and SOAP. But a lot of programs know how to interface with REST and SOAP. And so you kind of - it's a little bit of lowest common denominator; but at the same time you're kind of guaranteeing people are going to be able to figure it out, which is obviously important to let this kind of thing happen.

Let me see. I have a high recommendation for a website that I know called GRC.com. If you are a happy listener and you're looking for transcripts, if you're looking for 16KB versions, if you're looking for more information about security, that's the place to go. And of course SpinRite's there, too, and all of Steve's stuff, the free stuff, too, like ShieldsUP and Shoot The Messenger and DCOMbobulator and PPP and Wizmo and all that, GRC.com. And GRC.com/securitynow for show notes. There's also a great security forum there. And feedback is there, too. Is it GRC.com/feedback?

Steve: That's exactly what it is, and I really want to encourage people to keep the feedback coming. It helps us steer the show and tells us what you're interested in hearing about. Many people have said hey, you know, you guys used to do more of sort of like current events in security, a little more on, like, what happened in security this week.

Leo: We can do that. We could do that.

Steve: And I'm going to make a New Year's resolution for Security Now! as we start into '08. I'm going to return us more, well, a little bit to that, just sort of to touch in and check in and make sure that our users know of anything important that happened during the week in security.

Leo: Good idea.

Steve: After all, as someone did write, they said, you know, it's called Security Now!. It's like, oh, good point.

Leo: Well, I don't know if that means what's happening in security now. I mean, just be secure right now. Doesn't necessarily mean security current events.

Steve: That's true.

Leo: It could be a lot of different things. But, yeah, sure, of course. Whatever you want, that's the point. Securitynow.com/feedback [GRC.com/feedback].

And I'll remind everybody that we've got the TWiT discounts on ScotteVest now. I know we're all ScotteVest wearers. And if you want to give a gift for a geek, there's nothing better than a ScotteVest. Any gear on the site, ScotteVest.com. On checkout, use my name LEO as a promo code, you get 20 percent off, right off the top. This doesn't include ScotteVest material on ThinkGeek. That's a separate system. But on the ScotteVest site.

And Scott called and said, apologies that we're selling them out like hotcakes. Those fleece - I think the hoodies and the fleeces, they're backordered, and you may not get it by Christmas. In fact, I don't think you will. It's too late to get it by Christmastime. But just check the site. They'll let you know what you can get in time for the holidays. But what a great - I wanted to give you a couple - last chance, I guess, to take advantage of this at ScotteVest.com. Use my name, LEO, for the coupon code at the end and save 20 percent. We thank Scott, too for his support of the shows and the TWiT network and for all his great stuff that I wear all the time.

Steve, next week we'll do a Q&A session, speaking of feedback. That'll be our kind of mid - post-Christmas, pre-New Year's episode. So we'll see you then next Thursday, folks. Have a great Christmas, a great holiday, Steve. I hope you enjoy your time - I was going to say "time off." Whatever it is you do. You don't take time off, so I hope you enjoy the week. And we'll talk again next week.

Steve: Right-o.

Copyright (c) 2006 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details:
<http://creativecommons.org/licenses/by-nc-sa/2.5/>