Security Now! #726 - 08-06-19

Steve's File Sync Journey

This week on Security Now!

This week we look at a widespread false alarm about FaceBook's planned subversion of end-to-end encryption, still more municipality Ransomware attacks, more anti-encryption saber rattling among the Five Eyes nations, Microsoft's discovery of Russian-backed IoT compromise for enterprise intrusion, Chrome 76's changes, this week's Black Hat and Def Con conferences, a bit of miscellany and closing the loop with our listeners, then I want to share my recent experiences and findings about the challenge of synchronizing a working set of files between two locations, and the tools I settled on.

Security News

"The First Crypto Backdoor"

https://www.schneier.com/blog/archives/2019/08/facebook_plans_.html

That =WAS= to be the title of this week's podcast after many of our listeners tweeted links to Bruch Schneier's blog last week was titled: "*Facebook Plans on Backdooring WhatsApp.*" However, Bruce subsequently learned from sources who are far more reliable than the source of his reporting, though not from Facebook directly, that the story, which was sourced from Forbes brought new meaning to the term "extrapolation." To Bruce's credit, he immediately corrected the record once he was confident of what was going on.

Many of our listeners know that I often quote Bruce. He's credited with one of my favorite bits of pithy wisdom: "Attacks never get weaker they only ever get stronger." So for those who tweeted his first posting, I wanted to further correct the record with them.

The bogus Forbes article is titled: "*The Encryption Debate Is Over - Dead At The Hands Of Facebook*"
https://www.forbes.com/sites/kalevleetaru/2019/07/26/the-encryption-debate-is-over-dead-at-the-hands-of-facebook

The four relevant paragraphs of the now-quite-thoroughly-debunked Forbes column, within which this author twice cites his own previous Forbes articles as supporting reference, and which quite reasonably set Bruce off last week, were:

> To solve this problem, Facebook announced earlier this year preliminary results from its efforts to move a global mass surveillance infrastructure directly onto users' devices where it can bypass the protections of end-to-end encryption.
>
> In Facebook's vision, the actual end-to-end encryption client itself such as WhatsApp will include embedded content moderation and blacklist filtering algorithms. These algorithms will be continually updated from a central cloud service, but will run locally on the user's device, scanning each cleartext message before it is sent and each encrypted message after it is decrypted.
>
> The company even noted that when it detects violations it will need to quietly stream a copy of the formerly encrypted content back to its central servers to analyze further, even if the user objects, acting as true wiretapping service.
>
> Facebook's model entirely bypasses the encryption debate by globalizing the current practice of compromising devices by building those encryption bypasses directly into the communications clients themselves and deploying what amounts to machine-based wiretaps to billions of users at once.

Within that are links to the same author's previous story: On May 28th: "*Facebook Is Already Working Towards Germany's End-to-End Encryption Backdoor Vision*" ... And to support his claims there he cites two more of his previous stories:

"*Facebook's Edge AI Content Scanning Brings NSA-Style Surveillance And Censorship To The Planet*"
https://www.forbes.com/sites/kalevleetaru/2019/05/05/facebooks-edge-ai-content-scanning-brings-nsa-style-surveillance-and-censorship-to-the-planet

"*Deep Learning Will Be The End Of End To End Encryption*"
https://www.forbes.com/sites/kalevleetaru/2019/05/11/deep-learning-will-be-the-end-of-end-to-end-encryption

And in there he says:

> Even more worryingly, Facebook's presentation alluded to the company's need to covertly harvest unencrypted illicit messages from users' devices without their knowledge and before the content has been encrypted or after it has been decrypted, using the client application itself to access the encrypted-in-transit content.
>
> While it stopped short of saying it was actively building such a backdoor, the company noted that when edge content moderation flagged a post in an end-to-end encrypted conversation as a violation, the company needed to be able to access the unencrypted contents to further train its algorithms, which would likely require transmitting an unencrypted copy from the user's device directly to Facebook without their approval.

First of all, is it clear that point-to-point, user-to-user, one-to-one, end-to-end encrypted conversations should be moderation in the first place? The idea of an encrypted conservation being moderated in any way does seem to fly in the face of the whole concept of a totally private two-party dialog. I would think that the user agreement for WhatsApp would explain that user-to-user conversations are explicitly unmoderated, so use the privacy-protecting service at your own risk.

Whatever the case, Bruce can certainly be forgiven for believing the extrapolations of this Forbes author and Facebook does have a share of responsibility too, since based upon Facebook's past, and the privacy-shredding reputation they have earned, it is quite believable. But it's still wrong.

Bruce updated his blog posting, adding: EDITED TO ADD (8/2): This story is wrong. Read my correction. And then he explained what happened.

It seems very clear that something is going to be happening before long. But I suspect that it will be driven from the top down -- from government legislation down to the industry -- and that Silicon Valley will have plenty of time to implement whatever it is… doubtless some means for responding to a search warrant for the contents of a device and also some means of bringing up the equivalent of wiretaps on those devices.

"Five Eyes nations demand access to encrypted messaging"
https://nakedsecurity.sophos.com/2019/08/01/five-eyes-nations-demand-access-to-encrypted-messaging/

The Five Eyes is an alliance of national intelligence partners with members: Australia, Canada, New Zealand, the UK and the US. And the rhetoric surrounding this issue is heating up.

Last Tuesday's story in "The Telegraph" was headlined: "Facebook is threatening to hinder police by increasing encryption, warns Priti Patel" Priti Patel is the UK's new Home Secretary. The Telegraph reports that in the first intervention by a minister, the new Home Secretary says the tech giant's plans to introduce end-to-end encryption on its messaging platform would benefit child abusers, drug traffickers and terrorists plotting attacks. Writing for The Telegraph, she says it would prevent law enforcement agencies investigating and tracking down lawbreakers by enabling criminals to hide their messages.

As we know, last March, Mark Zuckerberg announced what he framed as a major, more privacy-focused strategy shift, with end-to-end encryption being a key component. He said at the time that the company would develop a highly secure private communications platform based on Facebook's Messenger, Instagram, and WhatsApp services. And this stated move has apparently set everyone off.

The prospect is unanimously seen as bad news by the Five Eyes nations. Patel's warnings come on the heels of a two-day Five Eyes meeting she hosted in London along with Geoffrey Cox, the UK's Attorney General. In attendance were security and law enforcement officials from the Five Eyes nations who said that they were worried about high-tech companies moving to "deliberately design their systems in a way that precludes any form of access to content, even in cases of the most serious crimes."

In a communique that reportedly came out of the meeting, the Five Eyes nations called for backdoors:

> Tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format.

In September 2018, Five Eyes governments had called on their governments to demand that tech giants build encryption backdoors – by force, if necessary.

From a memo that the Australian government issued on behalf of the pact at the time:

> Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions.

Reuters spoke with a former senior European security official who said that the Five Eyes is using "very general" language, at best, in its demand for government access in telecoms systems. He or she noted that there's been a proposal floated recently by some British officials that

wouldn’t drill a hole through encryption, per se. Rather, it would entail the equivalent of wiretapping encrypted systems, as in, secretly slipping a law enforcement agent into encrypted calls so they could tap a device at one end of the conversation after a message is decrypted.

The ex-official: “It doesn’t mean weakening encryption, just going around it.”

Facebook has pointed out that it just doesn’t work that way. End-to-end encryption means only the sender and recipient can read encrypted messages. That excludes everybody else, including Facebook itself.

This option to insert a government body into encrypted conversations, which was proposed by the UK spy agency GCHQ, is known as the Ghost Protocol.

In an open letter to GCHQ published in May, a coalition of tech companies, privacy experts and human rights groups claimed that letting governments listen in “would undermine the authentication process …introduce potential unintentional vulnerabilities, [and] increase risks that communications systems could be abused or misused.”

While the Five Eyes nations may want to insert their agents into encrypted messaging, they most certainly want to keep that power to themselves. The Telegraph reports that the Five Eyes nations agreed that Huawei – a company that’s worried governments for years – should be kept out of the 5G phone network unless it can be guaranteed that the Chinese government wouldn’t get unauthorized access.

Experts say that governments’ reinvigorated anti-encryption push appears to be directed not only at Facebook, but at Apple: the company that famously dug in its heels when the FBI was trying to decrypt the phone of the San Bernardino, California mass shooter in 2015.

Ben Wizner, an expert in national security law with the American Civil Liberties Union, echoed what backdoor opponents (including Sophos) have repeatedly pointed out: putting a backdoor in encryption means that you’ve broken it. Once there’s a hole, it will be found and exploited, and not necessarily by nations that (purportedly) have respect for innocent people’s privacy.

[Ben is with the ACLU, so we understand their position. But what he said is nonsense. As I've most recently stated as clearly as possible: we should tone down the rhetoric and separate the policy from the technology. The technology CAN, without any question, do anything we want it to. If we don't want it to be weakened, it needn't be. So what we need to determine is the policy we want the technology to enforce, and that technology CAN be created. We have all the tools.]

If the US and other nations get access to private messages, Wizner told Reuters, that means that adversarial nations, such as Russia, could demand that they get the same access.

[Who cares what Russia demands? We can simply say no. That's nonsense, too.]

This fight isn’t going away anytime soon. [That much is certainly true.] Last week, US Attorney William Barr – who attended the Five Eyes meeting – said that the proliferation of “warrant-proof encryption” was making it easier for criminals to evade detection.

Georgia on our mind
I'm starting to wonder whether at some point I'll start passing up reports of major ransomware attacks in the same what I sometimes don't bother reporting on every single data breach that occurs. If so, that's going to be some sad business.

So, this time it's the state of Georgia... again. We talked recently, just after the multiple ransomware attacks on Florida, about how Georgia's courts system had just been hit.

In the most recent attack, the Georgia Department of Public Safety (DPS) was hit. This encompasses the Georgia State Patrol, the Georgia Capitol Police and the Motor Carrier Compliance Division, which performs safety inspections. As a result of the attacks, many police functions have been thrown back to the days before the Internet. Steve Nichols, the Chief Technology Officer for the Department of Public Safetysaid that they were forced to take all servers offline while the Georgia Technology Authority investigates the attack, including email servers and server that support the department's public website and backend. As a result, State troopers are having to resort to old-school law enforcement: If a trooper is out on a highway writing a ticket, for example, they are now doing it with a pen and paper instead of a tablet. Or, if they're looking up a license plate, they now radio it into a dispatcher instead of using a tablet. The Georgia State Police, Georgia Capitol Police and Department of Motor Vehicle Safety have all had to switch to an older radio and phone system. (Anybody got a pencil?)

For some reason, Georgia has seen its share of these attacks. Back in March of last year, the first attack destroyed years of police dashcam video, as well as freezing systems. The outage rippled such that a week later Atlanta was still rescheduling court dates, police and other employees were still writing out reports by hand, and residents couldn't go online to pay their water bills or parking tickets.

That attack was courtesy of the SamSam ransomware, but the ransom demanded to provide decryption keys was an almost quaint -- by today's standards -- $52K in Bitcoin. The perpetrators of that attack, a pair of Iranian men were tracked down and indicted in the U.S.

Then, as we mentioned, Georgia's court systems were encrypted by Ryuk.

And also a few weeks ago, on July 17th, the government of Henry County in Georgia – the second fastest growing county in metro Atlanta – announced it had been hit by malware and county officials lost access to the Internet and most online services. And four before THAT, on July 13th, the police department in Lawrenceville, Georgia was hit with ransomware where the attackers encrypted most of the department's data, including body camera footage.

In their coverage from these attacks, Sophos provided some guidance for protection:

- Pick strong passwords. And don't reuse passwords, ever.

- Make regular backups. They could be your last line of defence against a six-figure ransom demand. Be sure to keep them off-site where attackers can't find them.

- Patch early, patch often. Ransomware like WannaCry and NotPetya relied on unpatched vulnerabilities to spread around the globe.

- Lock down RDP. Criminal gangs exploit weak RDP credentials to launch targeted ransomware attacks. Turn off RDP if you don't need it, and use rate limiting, 2FA or a VPN if you do.

- Use anti-ransomware protection.

Those are all good bits of advice. But the missing item that seemed glaringly obvious to me was:

- ***Educate and test your employees.*** Explain that they will be extremely inconvenienced by the loss of computation and network resources. Hand out pencils - ask them to practice using them. Explain that the #1 most common entry vector for malware into organizations -- especially municipal agencies -- is eMail baiting. Explain that this is **not** like being at home, because deep pocketed and insured government agencies are being actively targeted by foreign hackers… and that ALL some ONE person needs to do is click on a bad link in an eMail, or open a PDF and run its macros, or open a Word document and release it from Protected mode -- and the entire municipality can be taken down.

  And then… TEST. Send out baiting eMail to everyone and see how many and how takes the bait. If they know that management has told them NOT to do that, and that management is actively testing whether they are following the rules, they will be far more careful.

Russian state-sponsored hackers are using IoT devices to breach enterprise networks
In something of a tease for its full disclosure presentation later this week during Black Hat USA 2019, Microsoft reported yesterday that it had detected Russia's Strontium group, also know as APT28 and Fancy Bear, targeting VoIP phones, printers, and video decoders. These IoT devices provide them with an entrypoint into enterprise networks, from which they pivot to the network's higher-value targets.

Microsoft's Threat Intelligence Center said that attacks have been observed in the wild since they first spotted the campaign in April. Microsoft's researchers spotted Strontium attempting "to compromise popular IoT devices across multiple customer locations" where the hacker group exploited a VOIP phone, an office printer, and a video decoder.

Microsoft said <quote>: "The investigation uncovered that an actor had used these devices to gain initial access into corporate networks. In two of the cases, the passwords for the devices were deployed without changing the default manufacturer's passwords and in the third instance the latest security update had not been applied to the device."

Microsoft said that after gaining entry through the compromised IoT devices, they would then scan for other vulnerable systems to expand this initial foothold. <quote> "After gaining access to each of the IoT devices, the actor ran tcpdump to sniff network traffic on local subnets. They were also seen enumerating administrative groups to attempt further exploitation. As the actor moved from one device to another, they would drop a simple shell script to establish persistence on the network which allowed extended access to continue hunting."

Microsoft said it identified and blocked these attacks in their early stages, so its investigators weren't able to determine what Strontium was trying to steal from the compromised networks.

Strontium's targeting of IoT devices isn't new. The same group previously created a botnet of tens of thousands of home routers using the VPNFilter malware. And in addition to Strontium, other state-sponsored groups have started targeting IoT devices, and primarly routers.

Microsoft plans to reveal more information about the Strontium April 2019 attacks later this week at the Black Hat USA 2019 security conference. Microsoft's report about these recent attacks will include indicators of compromise (IoCs) such as IP addresses of the Strontium command and control (C&C) servers, which organizations might want to block on their networks.

So what's our takeaway from this? It's an old refrain, but it's an increasingly important one: networks MUST be segmented. It's not easy. It's not the default. It's not automatic. The easy automatic default is that, as Kahn put it in the second Star Trek movie, The Wrath of Kahn... "We're all one big happy family" -- just before he blew the crap out of Kirk, who had not raised his ship's shields for that reason.

Network segmentation can be accomplished using VLANs. "Virtual LANs" which are becoming increasingly common and therefore well supported. When VLANs are in use, and attritional VLAN tag is added to the Ethernet packets on the wire. The VLAN tag identifies which VLAN the packet belongs to. Then, smart, managed, VLAN-aware network switches are able to turn the VLAN tagging into the equivalent of physically separate LANs without all of the additional overhead of actually physically separate networks.

All the evidence tells us that we can no longer trust all of the devices we place onto a large and sprawling network, and these devices ARE biting people. So, for example, an enterprise's VOIP telephone system does not need to be on the same LAN as the enterprise's workstations and servers. So the VOIP system should be placed on its own VLAN. Then... if somehow some bad guys DO get into a VOIP phone, from that vantage point, no matter how hard they try, they will only be able to "see" the other devices on the same VLAN... which would be other uninteresting VOIP phones. Since the Ethernet VLAN tagging occurs below the IP level, at the OS NIC LAN adapter device driver level, aberrant software doesn't have access to VLAN tagging and its hands are tied.

And, since the VLAN ID tag is 12 bits, any single physical network can be configured with 4,094 separate virtual LANs... so many network subdivisions are possible. So, for example, rather than placing all of an enterprise's servers together on the same LAN, think about which servers need to see the other servers and seriously consider isolating those that can run seeing only a subset of the whole.

Google Chrome 76 released for Windows, Mac, and Linux

Thankfully, Adobe's Flash, which has caused so much destruction and disruption for decades, will finally not only be disabled by default for all sites, but per-site changes for Flash usage are also now ignored. This means that if a user had previously enabled Flash for a website that setting will no longer be remembered or honored. Starting with last week's release of Chrome 76, users will have to re-enable Flash for each page they visit, every time they visit it, and every time they

use Chrome... thus making the process of playing Flash content much more burdensome. As we've covered here previously, Google's plan is to phase out Flash by the end of 2020. So by making Flash more annoying to use, websites will have further incentive to stop relying upon it.

The other welcome change which we recently described as "coming soon" is here: That's no more Incognito Mode detection by websites through checking for the function of Chrome's FileSystem API. And Google has indicated that if sites switch to some other means of Incognito Mode detection, they will again respond to prevent it.

There were not a lot of big changes in Chrome 76, but these are welcome incrementals.

Black Hat & Def Con 2019
Despite a bizarre and almost biblical infestation of grasshoppers, the Black Hat and Def Con 2019 conferences will be underway this week with the main two-day 22nd annual Black Hat 2019 conference tomorrow and Thursday at the Mandalay Bay Resort... followed then by Def Con. So I'm sure that next week's podcast will also be our own annual Post-BlackHat and DefCon debrief.

Miscellany

OWASP / OC - Thursday, August 22nd.
https://www.meetup.com/OWASP-OC/events/263576551/
In two and a half weeks.

Closing The Loop

Joshua Kelley @joshuadkelley
Hey Steve,
I know you have talked about Firefox Send in the past on SN. I found this great command line tool for interacting with it: github.com/timvisee/ffsend

Looking forward to the next SN episode.

- Josh

Github: "Easily and securely share files from the command line. A fully featured Firefox Send client.

Requirements:
- Linux, macOS, Windows or FreeBSD (other BSDs might work)
- A terminal sunglasses
- Internet connection for uploading and downloading

My File Synchronization Journey

My experiments and findings in Cross-site file hierarchy synchronization
The challenge is that for the first time I have two work places with workstations which I need to keep synchronized. I don't need everything synchronized... only the things I'm actively working on at each location. Since I have plenty of my own resources, my first thought was to make a Drobo here at my primary location available to my secondary location. The Drobo would be my own cloud and both workstations would synchronize to it. So I tried that first. I experimented with many directory synchronization utilities and tools and finally settled upon one called "FreeFileSync". I like it a lot. It's the best thing I found. It is Open Source free file synchronization software: https://freefilesync.org/ It describes itself as:

> **Synchronize Files and Folders**
> FreeFileSync is a folder comparison and synchronization software that creates and manages backup copies of all your important files. Instead of copying every file every time, FreeFileSync determines the differences between a source and a target folder and transfers only the minimum amount of data needed. FreeFileSync is Open Source software, available for Windows, macOS, and Linux.

When used manually it's really terrific. It scans and you can see what it proposes to do before it does it. It has all the fancy rules and exceptions you could want. But I was never able to get it to work usefully automatically. For reliable synchronization you don't want some timed recheck or synchronize on shutdown -- Windows doesn't like that at all since remote network drive connections are being dropped as Windows prepares to shutdown. But I would and do urge listeners to check out FreeFileSync. For some applications it would be perfect, and the price is right.

But it wasn't my solution. I tried for a while to run it manually. Synchronizing my files before leaving here heading to home #2. It was an inherently fraught manual process and several times I forgot to send my most recent work to the other end. I looked around a LOT for some good automated cross-site synchronization, and I tried many things, but nothing ever really worked correctly.

Since I also maintain secure tunnels between the site, I did consider simply mapping a drive through the tunnel to allow my secondary location to reach into the drive of my primary location. But that meant that the end without the files was having to read and write continuously through the Internet. That's clearly not the right way to go. The right solution is to have local copies of all of the shared content, and some entirely background process that's keeping them synchronized.

Google Drive **| Free 15 GB**
Next I tried Google Drive. I hadn't had great success with it in the past, but that was on XP. I was hoping that perhaps Win7 would be more friendly and/or that it might have improved. But it didn't work right, either. I would get weird file locked errors, complaints from it and weird behavior.

***MicroSoft OneDrive* | Free 5 GB**

So I thought... what about Microsoft and OneDrive? I'd been using a newer Office 2016 which was OneDrive aware, so it was on my radar. And, indeed, it was kind of better. But after awhile and from time to time it would say that it was unable to "merge" files one end or the other and so it would create duplicates because it was unable to "reconcile." I don't want reconciliation or any sort of fancy "merging", I want the newer file to replace the older file. If I modify a file at one end I want the other end to be updated. Then it finally got really wonky, stuck trying to update with the little "I'm busy updating" spinners on the entire shared directory hierarchy. When I went looking for some way to fix that problem, I quickly found that this "making multiple copies of single shared files" has been plaguing OneDrive from the start. So I was wrong in my thinking that Microsoft would know how to do this.

DropBox

All this while, I had free 2 GB Dropbox web account. Some time before I had been looking for a simple way to send videos from my work site to my home site so that I could watch them later with Lorrie. We use a Roku there, which I'm very happy with, and a free app for the Roku called "Roksbox" is able to stream from various cloud sources.

That had been working well, though a 2 GB total storage limit for video was a bit tight. I was needing to delete anything that we had seen.

So... By this time I had tried using my own cloud, I'd tried Google Drive and OneDrive. So I decided to give DropBox a go. And to make a long story as long as it needed to be, today I am 100% happy. I have found my Nirvana. After experimenting with it for a few days, I bit the bullet and upgraded from the free 2 GB to 1 TB for $10/month. So now, instead of having 2 gigabytes, I have 1,000 gigabytes. Which is way more than I need.

I'm not trying to store my world up there. Just the various things that I explicitly wish to share between locations. Dropbox allows you to locally store instances of your shared files, or you can tag individual files or directories as "Online Only" so they only live in the cloud. This is what I do for videos that I want to send to the Roku. After editing something to strip the commercials I'll just drop it into the "Dropbox/video" directory I created and marked as "Online Only" and it disappears into the cloud ... where it will be waiting for me to share with Lorrie that evening.

Word opens files perfectly from there, and Dropbox offers some optional integration with Office, though it works fine without it. And Dropbox keeps a history of everything. Once, in the beginning, I made a mistake and deleted something important. So I just logged into Dropbox's web interface and chose the earlier version that I wanted to restore, and there it was.

I am tending to use it more and more and unlike all of the other solutions I tried first, it has never failed me. Not once. As I get to know it better and dig into its many options I just smile, since it has everything I want.

Now... nothing I'm doing at the moment is secret. I'm writing and editing the SQRL documentation which is and will be public, and various projects that will eventually become public, public domain health research documents, and such. So I cannot share my experience with operating through a TNO-style encryption solution -- since I haven't yet bothered. Our long time listeners will recall that JungleDisk was the earliest TNO self-encrypting cloud storage

provider that we loved on this podcast. And later, BoxCryptor was a favorite. But today everyone wants to sign everyone up to a service model, and I'm still very resistant to that. If I'm actively using someone's bandwidth or storage on an ongoing basis, then a pay-for-what-you-use model makes sense. But not for software. I'm just not there yet. However, the free version of BoxCryptor allows for use on a single cloud provider and two devices, so that would work for me in my simple little two-site mode. So once I have SQRL all documented and launched and I'm back to work on the next SpinRite, where I'll be more concerned about security, I'll likely give BoxCryptor a whirl. If I could split-encrypt, where only a branch of the file tree hierarchy is encrypted, that would be perfect. Or for SpinRite source, since 2GB would be massive overkill, I could create a separate SpinRite DropBox and give it to BoxCryptor.

So I wanted to share the results of my experiment into becoming dual homed, with the need to have high-reliability cross-site synchronization and backup.

Wasabi: Wasabi is a cloud storage provider and a sponsor of the TWiT network, so I was aware of them and I figured I'd see what was up. Wasabi looks like a very nice solution with quite compelling pricing. As a content delivery network (CDN) the fact that there's no egress cost -- no cost when people download -- is HUGE! I currently host some "How To" SQRL video files on AWS S3 and it looks like I could do the same for a significant savings with Wasabi. So I will probably explore Wasabi for that.

But Wasabi appears to be more enterprise than end user targeted. They export an S3 API, but they don't have any sort of multi-desktop sync. The end-user is not their target audience. They're targeted at being a very affordable CDN -- and it does appear that they have that nailed.

I'm an AWS S3 user. All of Security Now is archived in S3 buckets. There are some nice S3 API management UI tools, but I have never found a good working multi-desktop file and folder and hierarchy synchronization solution for S3. And I've looked around a lot. (There's an open source S3 synchronization project called S4 on Github, written in Python, but it also looks a bit raw.) BoxCryptor supports the AWS S3 interface, but they do not yet explicitly list Wasabi as being among the cloud providers they support. So I don't know whether BoxCryptor could be manually configured. But if BoxCryptor could work with Wasabi, that might be a slick solution for two-site sync. But then, Dropbox is intensely end-user oriented, and it offers a large array of well-tested solutions and options. And I've been extremely impressed by every experience I've had with Dropbox.

Other solutions? … ownCloud

For our much-more-technically-competent-than-typical listeners, the idea of tinkering with a self-hosting solution might be appealing. In searching around I encountered ownCloud, NextCloud, SeaFile and SparkleShare. Of them, ownCloud really looks like the one. So far I've been very impressed by everything I've seen.

Since I have Drobos at both locations, and ownCloud is available as a Drobo App, I've **just**, this morning, installed it on my local Drobo, set it up, and installed the Windows client. So far I'm very impressed by what I've seen. But I was initially impressed by Google Drive and OneDrive, and they both crapped out on me in different ways. So I'll see how ownCloud goes and I'll

report back once I have some more experience with it. I'm busy, so I just want a solution that will stay out of my way, and work reliably, so that I can stay focussed upon what I'm doing.

ownCloud servers can be self-hosted on many platforms such as Linux, FreeBSD, any of the Unix-like OSes, etc. And it has clients for iOS and Android. Though I would be terrified to expose its service to the public Internet.

I've been looking for a solution that would smoothly keep Lorrie's desktop and documents folder contents backed up, and this might be perfect. Unlike with Dropbox, where everything needs to live underneath the Dropbox folder, ownCloud allows multiple directory hierarchies on a system to be synched to directories on the ownCloud server. That's a feature I HAVE been wishing for from Dropbox.

And ownDrive natively supports prior file versions. They describe their default versioning algorithm this way:

The versioning app expires old versions automatically to make sure that the user doesn't run out of space. This pattern is used to delete old versions:

- For the first second we keep one version
- For the first 10 seconds ownCloud keeps one version every 2 seconds
- For the first minute ownCloud keeps one version every 10 seconds
- For the first hour ownCloud keeps one version every minute
- For the first 24 hours ownCloud keeps one version every hour
- For the first 30 days ownCloud keeps one version every day
- After the first 30 days ownCloud keeps one version every week

The versions are adjusted along this pattern every time a new version gets created.

The version app never uses more that 50% of the user's currently available free space. If the stored versions exceed this limit, ownCloud deletes the oldest versions until it meets the disk space limit again.