All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Security load explode!

I see all these claims about building highly complex cyber-security environments and cannot believe that this is even a concept given that we cannot seem to get even relatively simple software anywhere close to right.

Screwing us for better user experience?

When I put URLs into a calendar entry, I didn't expect them to be automatically transformed into MITM attacks by Google. But of course they were…

- A URL (like test.all.net/OK) gets automatically turned into a URL at Google that includes the original URL at the end. Since it is an https URL, the new https URL points to Google, which then launches the MITM attack by trying to create the channel. It should do a redirect (it shouldn't do any of these things actually), but of course with https this doesn't do the right thing, so users cannot get access.
- Everyone seems to want to get in between me and my endpoints. That's called a security exploit, not a feature. AT&T puts me into one of their sites whenever I type an unused URL instead of returning this proper no such domain response with ICMP[1].
- And of course this is NOT a BETTER user experience. It's just a more captive and exploitive one. They use it to generate advertising revenue. It's about taking more money from me after I have already paid them for commercial services. It's a fraud, or damned close to it.

Stop interpreting my content please!

Spell correction has gotten to the point where I have URLs that include upper and lower case that universally seem to get corrected as I type them into my cell phone. And when I say "corrected" I mean screwed up.

- I have repeatedly entered the URL http://a2e.co/GoToAngel.html
- It has been transformed in a wide range of ways, different on many different occasions, but spelling 'correctors', including introducing spaces, changing the case of the characters, putting a space before the .html, etc. And when I try to fix them, it breaks them again and again.
- Corrections should be suggestions, not background changes. I'm sure someone will claim these are notified (somewhere on the screen something might show some indicator that a change will be made unless I stop what I am doing to prevent it). BS.

AI is too stupid to let loose

Yes it is… and this one is not my claim, thought I support it. Clearly we cannot trust most modern AI even as much as we trust people when it comes to important things. But trust, that is an issue for another report.

[1] Internet Control Message Protocol – designed for that very purpose

AWS disk space leak

Eat forever… On my AWS servers, when nothing is happening for long periods, the system loses available disk space again and again, even though the disk usage is not changing.

- For clarity, disk usage includes hidden, temporary, still opened, and other such files.
- But when I reboot the system, I get lots of that disk space back!
  - Which means it was being consumed by some sort of memory hole in the disk mechanisms of the VM environments used by AWS.

I hate to reboot, but I now apparently have to reboot my servers at least weekly to compensate for AWS's bad software. It doesn't happen on my otherwise equivalent systems by the way. Same operating environment in a physical computer with physical disk space, no reboots required, no disk space consumption.,

Apple 2-factor authentication insanity

My wife got a new iPhone Saturday at the first available appointment at the Apple store.

- By Sunday, after the 2nd reload and extensive backups and restores, it was working well enough for her to use it for the day, but not well enough to integrate with everything it used to integrate with, and those apps still weren't restored.
  - I didn't count the number of times I had to enter multi-factor authentication to the device, the Macbook it was associated with, and Apple itself. I was certainly over 100. And each time it took step after step after step from device to device. It was insane. Add the screen lock to this and my wife's face had to be present until I figured out how to disable that security function.
- By Monday I managed to get it reloaded from the previous iPhone's content, but only after paying more money to Apple.
  - The backup took about 6 hours (the original projection it gave was 18 minutes, but by 1/3 of the way through it said 4 hours to go). And that was without any restoration yet. The backup to the Macbook had to be retried several times, and the progress metrics are pathetic to ridiculous.
- By Tuesday it's still not fully integrated, and she can read the headlines but not the content… their zoom function is pathetic.
  - I ultimately had to change my Mac password and hers, necessitating changes on multiple devices (not all yet changed) used for account access. And of course the multi-factor authentication used an old phone number, so I had to get rid of that, which forced me into security question land. I did not provide truthful information on the questions which anybody could look up. They won't allow the same answer to multiple questions, so I finally picked questions with different last letters and reused the same password adding the last letter of the question to the answer.

We will see how long it actually takes to get it fully working… Siri doesn't listen, and the iWatch had to be reloaded from scratch 3 times (so far), and the car is not yet connected (I wonder how many times we will have to put in the same password before it allows this operation).

Security load explode

Security load is the load on users and the enterprise from security.

- It should be that good security reduces this load to where it is transparent and automatic for normal people to do normal things. But instead, it continues to grow into a sick abuse of power by those who run security.
  - Better user experience by man in the middle causes user access to fail, and they have to type in the URL manually. **Security load explode.**
  - Instead of an automated failure mechanism, a Web page to advertise to me, and of course introduce possible Trojan horses and time wasted. **Security load explode.**
  - Spell correction creating errors where there were none – forcing retries and multiple entries of the same data. **Security load explode.**
  - Disk space denial of services forcing reboots and short outages as well as costing more time in investigating causes of outages. **Security load explode.**
  - 2-factor insanity taken to ridiculous extremes, denying services while making things less secure. **Security load explode.**

All of this, of course, forces users, even high skills very knowledgeable security conscious users, to get around the stupidity. Here are my recommendations:

- As the load gets higher, refuse to use.
  - At some point, the security is not actually improved by higher load. Repeating the same password hundreds of times just exposes it all the more. I will not buy an Apple anything unless I have to for this very reason.
- Cheat the system however you can.
  - Use the same password everywhere except for a minor variation you can predict. Otherwise you will keep forgetting the passwords and have to do resets, exposing your reset information repeatedly and lowering the security. A password manager won’t do the job across all my platforms and single (reduced) sign-on only weakens security by aggregating risk.
- Push back every way you can against STUPID SECURITY.
  - I am all for smart security. I think multifactor authentication done right is a good idea. But done wrong it simply impedes usage and denies services. Apple does this worse than anyone. But they have stiff competition.

Conclusions

Push back hard on **Security load explode.**

- Tell them to Get out of the middle!
- Stop letting them ‘help us’ by screwing us up!!
- Stop trying to interpret me with incompetent (or is it malicious) lie of AI!!!

I used to run my own infrastructure components. I am thinking of going back to it.