Exploiting Ammyy Admin – developing an 0day

Background

For the past few years, a number of groups of scammers have been cold-calling thousands if not millions of people in what's been referred to as the "Ammyy Scam" or the "Microsoft Tech Support Scam" among other names. The scammers pretend to be from Microsoft or another official group and claim to have detected errors on the users' computers. They have the victims pull up internal logs that show errors, and convince them to download and run the Ammyy Admin software to allow them to remotely control the system. After that point, they may install backdoors or other malware, or simply ask for hundreds of dollars to "fix" the problem. The phone scammers have prompted numerous responses from Microsoft as well as warnings from Ammyy itself on its website. Even though at least two groups have been prosecuted, many more continue to operate. Ammyy Admin is one of many remote control software programs; it is not inherently malicious. The scammers just use it because it's an entirely self-contained executable that runs without any installation, it's the easiest to use for an ad hoc connection.

The internet is also full of technical users who have trolled the scammers, wasting their time, making fun of them, or forcing them to see disgusting images. Like most of us in the security industry, I was amused, but thought little about it until the scam hit closer to home when I discovered one of these groups had managed to scam my grandparents and leave their computer an infected mess for me to clean up. So I set out to find out if I could counter an attempted scam with a full fledged remote exploit, and turn the tables on the scammers.

The Challenge

This was also a very interesting challenge, because most of the time, exploiting software begins with fuzzing the network protocol or file formats used based on format specifications like HTTP or FTP, modifying samples of legitimate files or network traffic, and/or examining source code for vulnerabilities. Exploiters often take advantage of debug symbols, which

Microsoft provides for their binaries, or other public documentation. For example, for some targets, finding an exploitable vulnerability is as easy as throwing a long string in the protocol and watching a stack overflow give you control of the instruction pointer. And if your target is like that, awesome for you! But it gets harder for widely-used software (Ammyy claims that the software is used by over 36 million personal and corporate users) especially if it wasn't selected for being a weak target.

In this case, Ammyy Admin not only did not have publicly described protocols, source code, traffic samples, or debug symbols, as I found out, its traffic was also incomprensible. The first thing I did was to set up an Ammyy Admin connection between two virtual machines and capture the network traffic. I started comparing it against other well-known remote desktop protocols, such as VNC and RDP, but quickly discovered that Ammyy uses a completely proprietary network protocol. Not only is the protocol not well known, but all the network traffic was encrypted, making it impossible to reverse-engineer or even replay and reproduce with network traffic alone:

You can keep staring at that all day, but I'll save you the trouble; it's just encrypted data.

Being a reverse engineer by heart, I first set out to identify the code that parses the first few packets to see if there was any kind of vulnerability I could find in it. Ammyy Admin is a decently large (764 kilobytes) executable that does not include the C runtime library, and it appears to be written in C++, which means the call graph between functions is generally lost in a mass of vtable function pointers. But with a little debugging, it wasn't hard to find. This code snippet parses a number of flags that aren't really important and then begins initializating the crypto functions, but it was very small and doesn't contain exploitable vulnerabilities.

Ammyy uses the same executable for sending and receiving code, and it won't connect to itself, so I decided to use two VMs. While it would be possible to patch the Ammyy code to allow connections to another instance running on the same box, the effort needed to make that work would probably mean you weren't saving any time doing it.

Instead, I focused on reverse engineering the code the sets up and handles the encryption and decryption so that I could write code in a scripting language to simulate one end of the conversation. Although following and cataloging the thousands of binary arithmetic operations is strangely addictive, I had to stop myself before I wasted any more time. Exploring the advanced settings, you can see that the crypto is based on AES-256 and optionally RSA-1024, and I'm sure someone who is bored can finish that, but I needed to get to the core protocol parsers to look for bugs.

Vulnerability Discovery

So the next direction I went was to identify the wrapper methods around send and recv that performed the encryption or decryption and sending/receiving of data. Those methods were the ones to send and receive the plaintext of the protocol, and I needed to be able to record the data passing through and be able to modify it. There are a few different options for dynamic instrumentation; some vulnerability researchers like using Intel's Pin framework, for example. Since I had already put together a flexible hooking library for Ambush with generic function hooking library and process injection code, I just made a sniffer from a local fork of the Ambush codebase to handle hooking the internal send or receive functions and save their output to a file, each traffic chunk broken apart by four X's. The output now looked like this:

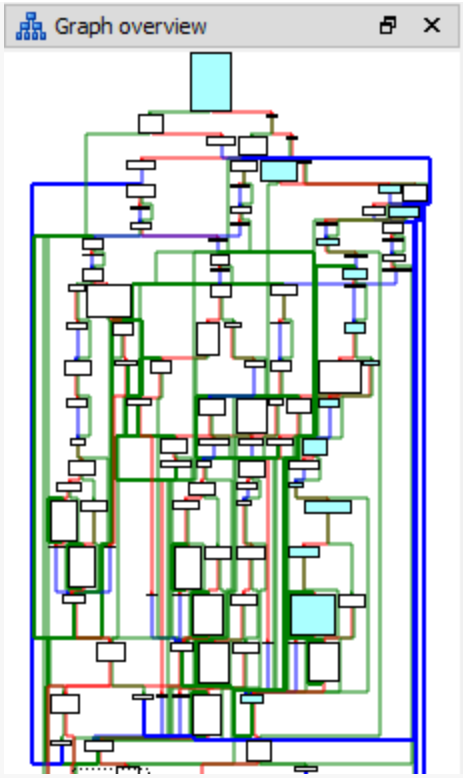
```
0000000: 5858 5858 3d58 5858 587e ccf5 ed97 1692  XXXX=XXXX~......
0000010: e296 bdf3 ffc0 ff2d 9769 f2ca 9958 5858  .......-.i...XXX
0000020: 5800 7f00 0000 5858 5858 3a00 5769 6e64  X.....XXXX:.Wind
0000030: 6f77 7300 362e 302e 3630 3031 2053 5031  ows.6.0.6001 SP1
0000040: 2e30 004d 5349 4556 4953 5441 0a4a 616e  .0.MSIEVISTA.Jan
0000050: 2031 3520 3230 3134 2061 7420 3030 3a32   15 2014 at 00:2
0000060: 353a 3139 0005 5858 5858 1558 5858 5870  5:19..XXXX.XXXXp
0000070: 0303 6518 00ff 00ff 00ff 0010 0800 2000  ..e........... .
0000080: ff00 ff00 ff00 1008 0020 0358 0258 5858  ......... .X.XXX
0000090: 586f 0000 0000 2000 2000 c000 0000 e000  Xo.... . .......
00000a0: 0000 f000 0000 f800 0000 fc00 0000 fe00  ................
00000b0: 0000 ff00 0000 ff80 0000 ffc0 0000 ffe0  ................
00000c0: 0000 fff0 0000 fff0 0000 fff0 0000 ff80  ................
00000d0: 0000 ff80 0000 f7c0 0000 e7c0 0000 03c0  ................
00000e0: 0000 03c0 0000 0000 0000 0000 0000 0000  ................
00000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000110: 0000 0000 0000 0000 0000 1a06 031a 0603  ................
0000120: 1a06 031a 0603 1a06 031a 0603 e8e6 e51a  ................
0000130: 0603 1a06 031a 0603 ffff ffe8 e6e5 1a06  ................
0000140: 031a 0603 1a06 03ff ffff ffff ffe8 e6e5  ................
0000150: 1a06 031a 0603 1a06 03ff ffff ffff ffff  ................
0000160: ffff e8e6 e51a 0603 1a06 031a 0603 ffff  ................
0000170: ffff ffff ffff ffff ffff e8e6 e51a 0603  ................
```

Much nicer, clearly plaintext and structured, and best of all, repeatable.

The next step was to turn the injected internal protocol sniffer into a fuzzer. I took a brief look at some of the publicly available fuzzers, but none of them appeared to make the process any easier. Fuzzers like minifuzz are easy for fuzzing file-parsing programs, and Peach can easily generate network traffic starting from a protocol specification, but I'm not aware of how to set up any to perform modifications via injected code, while synchronizing and looking for crashes across multiple VM's. So I accomplished this by using the "hookfuzzer" I had written. I modified it to receive a seed over the network and generate pseudorandom numbers to flip about one out of every two hundred bits. I set up the "controlled" end to send the manipulated data back to the "controller" side. There's not really any point in trying to crash the controlled side, since the controller already owns it.

After running the fuzzer manually a few times, the Ammyy controller crashed! Ammyy caught the error and displayed an error message with the faulting instruction. I modified the injecting sniffer/fuzzer to replay that transcript and verified that the crash was reproducible.

The instruction was an invalid memory access, which didn't appear immediately easily exploitable, since it didn't show control of the instruction pointer and the functions responsible seemed extra-awful to reverse, so I decided to automate the fuzzer and run it until I got a better crash.



This is some of that awfully complicated flow graph for that awful function.

I wrote a few helper executables and two PowerShell scripts, one on the controller side and one on the controlled side, to form my ad hoc fuzzing framework. They automated starting a new instance of Ammyy Admin, injecting the fuzzer, clicking the appropriate buttons to connect, waiting a few seconds for a crash, detect whether or not a crash had happened, saving the crash address and transcripts of the plaintext traffic that had caused the crash, and restarting the whole process. Next, I cloned a bunch of Windows Vista VM's, loaded the fuzzers on there, and let them go.

After running for a few days on 5 pairs of VM's, the fuzzer had collected a few thousand crashes, at 11 unique addresses. The vast majority of them fell on the same address as the first crash, and most of the unique crashing addresses were in different functions in the same executable, but two of the crashes demonstrated control of the instruction pointer.

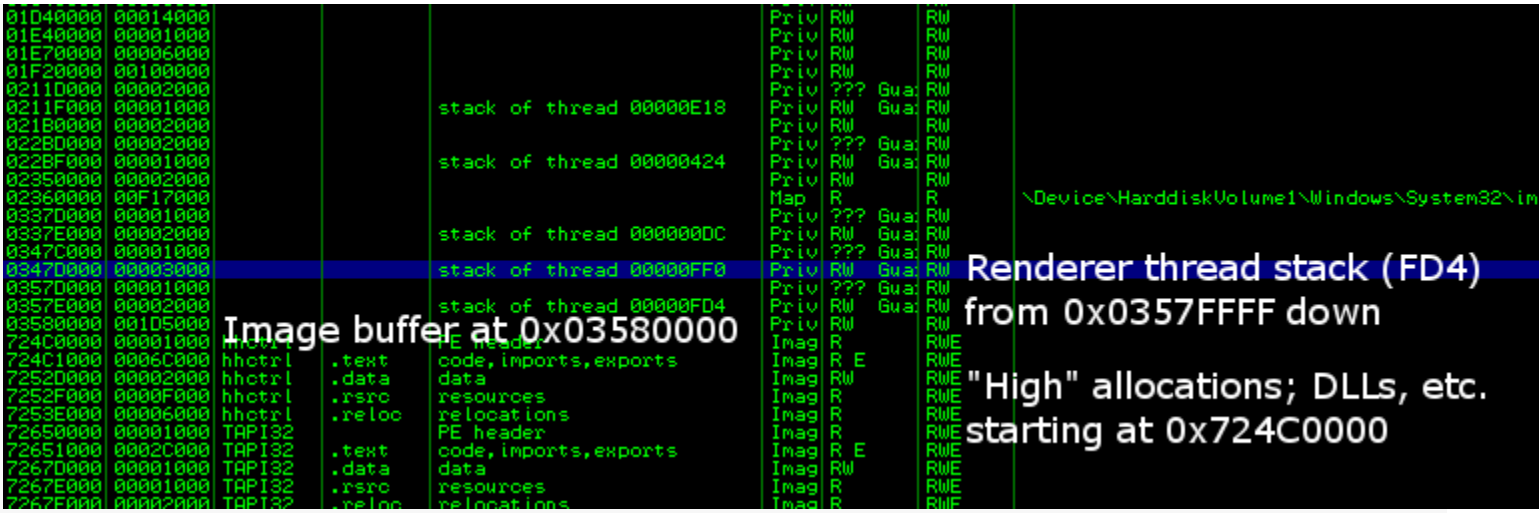
I pulled up the saved transcript and loaded a debugger into my test VM, and traced back the crashing code. For all the effort I had put into building the fuzzing framework, the flaw was the same root vulnerability in the same awful function as the first crash I found. Oh well, looked like I needed to get back into RE and find out exactly how the protocol worked.

Exploitation

After a few days tracing the code, the protocol became clearer. Upon negotiating a successful connection, the controller spawns a thread to handle rendering the remote screen. The first data sent from the controlled end includes header data and global flags for the connection. It then contains system information such as operating system and system name. Finally it includes screen dimensions and various other fields. The controller then allocates a screen buffer using Windows GDI functions based on the screen dimensions, stored in RGBA format; four bytes to a pixel. After a chunk of data describing the cursor, the data stream sends what I call "stroke sets" which draw or update a rectangle on the screen

buffer, which could be the entire screen or could just be a portion of it; each defines a start X and Y and width and height. Each stroke set then contains a list of strokes, each of which describes the pixels in up to a 16×16 pixel area. I won't go into full detail, as there are many forms the stroke can take to, for example, paint the entire block the same color in just a few bytes or draw each pixel individually, but in each case, the stroke defines the red, green, and blue portions of the pixels. The protocol uses a flipped coordinate system from GDI; the low index rows that come first are in the last memory addresses and vice versa.

Whew! All of this is important, because the crashing data in the fuzzed transcript is a stroke set that draws a rectangle just off the end of the image buffer. Since the image buffer is not in a heap or stack or other structure, if it was randomized sufficiently, there might not be any data reliably at a given offset to overwrite. However, because of the peculiarities of Windows memory allocation, even though the stack and heaps are nominally randomized, the stack of the renderer thread is allocated in 1MB of reserved memory directly before the image buffer; the last and highest allocations of the "low" allocations in the process. (the high addresses are where the DLLs are mapped) They are not randomized in relation to each other.



Memory layout of AA during exploitation

Thankfully for us, the Ammyy Admin executable does not opt-in to ASLR or DEP, which makes exploitation far simpler once you have the initial vulnerability discovered. The simplest plan of attack is to first write shellcode into the image buffer, then write the address of a pair of push esp; ret instructions over the return address of the stroke set parser function in the rendering thread followed by a jmp to the start of the buffer with an out-of-bounds array write. An alternate plan of attack is to write a ROP payload that will return to a LoadLibraryW call that will load a DLL from a remote UNC path, which will bypass Always-On DEP. However, this relies on the Web Client service to be enabled and requires waiting for a DLL to be pulled from a UNC path to load which usually takes 30 seconds to a minute.

Writing the shellcode for the direct attack entails a little bit of difficulty, since every fourth byte will be a 0, we can only control the RG and B bytes of the pixels. The good news is that we have no byte restrictions and we have plenty of room,

since we can easily reserve a million pixels (4MB) or more if we want. So I just used the Metasploit Unicode encoder to create shellcode that will work when every other byte is a 0, which will work with basically any shellcode.

As far as the out of bounds write, the stroke set parser return address is at 0325FEBC when pixel data starts at 03360000. That's a 0x144 or 324 byte OOB overwrite from start of image, which is 81 pixels. So, with an 800×600 screen buffer, a stroke set with X offset 719 and Y offset 600 (since rows go down in address) will write to the appropriate offset.

With this work done, I put together a metasploit module that will generate a plaintext transcript to send to the remote end via the injected DLL into a running Ammyy instance that will exploit the remote end trying to take over your computer. In order to run it, you still need to run Ammyy Admin, save the plaintext transcript in its directory, and inject the DLL into the process which will load up the transcript. So I put together an executable package to automate this. I wrote the exploit for Ammyy Admin 3.4, including both the direct and ROP targets, and I updated for 3.5 when it was released. The vulnerability has been present for as long as I checked, at least back to 3.0, and probably before then.

You can download the complete package here, including a fully commented metasploit module and detailed README with more information on running it: https://www.scriptjunkie.us/aaa.html The one remaining caveat is that Ammyy can connect in two main ways; either by ID, which routes a connection through relay servers run by Ammyy (rl.ammyy.com), or directly by IP. I have only written and used the exploit with a direct IP connection to avoid sending it over the internet, so although the vulnerability should be present either way, I recommend blocking rl.ammyy.com in a hosts file and simply using direct IP connections. Or at this point, feel free to look into making it work over the relays, but I have not.

Aftermath

No scammer group has ever called me, and I have never used this except to test it and in demonstrations. I don't normally release zero day exploits, but I made an exception in this case because given the reporting and usage of Ammyy Admin I consider it highly unlikely to be used to compromise innocent victims. The primary users at risk of compromise are the scammer groups. Hopefully, it will be a deterrent to those who would attempt to compromise and take advantage of innocent victims.

This entry was posted on September 11, 2014, 4:15 am and is filed under Exploits, Metasploit, Uncategorized. You can follow any responses to this entry through RSS 2.0. You can skip to the end and leave a response. Pinging is currently not allowed.

http://www.scriptjunkie.us/2014/09/exploiting-ammyy-admin-developing-an-0day/

- Links
- msfgui
- sessionthief

Important Stuff

You first touched a computer when you were `n` years old, where you discovered Carmen Sandiego/minesweeper on the generic PC your university/family had. Intrigued by the amazing abilities of the system, you immediately wanted to know how it worked, but were intimidated by the complexity. Nevertheless at `n+1` you were familiar with operating all the software you had. By `n+5` you had written a few simple programs, and by `n+10` you could bend the API's to do whatever you commanded. At some point, you went to school for your CS degree, and a few years later, you had found the world of security, and could get whatever access you wanted. Around `n+20` you had written some serious exploits. By `n+40` you were a CSO at a profitable company, and by `n+60` you were happily retired, and just trying to keep up with the news. And at the age of `n+80` you died.

Then what?

You've spent years learning about technical details of systems, and that may serve you well for the next few decades. But what about the next few centuries? Where will you be a million years from now? Most people believe everyone has a soul that will go on forever. It is a question that has more weight than anything else I can cover here. And no one should be scared, confused, uniformed, or in denial over it.

As some of you know, I am a Christian. It is a title I am proud to wear; for as I have matured, I have done my best to take a hard look at everything I have heard from my family, friends, and teachers, especially when they disagreed. So let me tell you about my faith. (Faith: the system of facts I know that are central to life, not just a hope in something I want to be true)

Mark Cahill has done a good job putting down his thoughts on the matter, and you can take part in a Q&A conversation by going to his website: http://www.markcahill.org/. I highly recommend reading this excerpt from One heartbeat Away as well. If you have read that and want to read the book (woah! book! no way! **relax.** It only took me a few hours. It's brief.) let me know, and I will get you a copy, and would love to talk with you about it.

But maybe you need to see more of those technical details. Like many educated people, such as those in the security and other technical fields, you want to base your view of life, the universe, and everything in terms of the best deductive logic and peer-reviewed science. Good for you! I feel the same way. So I encourage you to please review just four of the reasons I believe, and read and consider them. And as the stakes of eternity imply, it is well worth your time.

Why God?

Creation

Christians have always insisted that the universe had a beginning; that it was created by God, the First Cause. Since Einstein's discovery of general relativity in the past century, scientists have also become convinced of this simple fact; that

everything in this universe began at a point in the limited past. Yet, I'd point out, one of the most basic laws of nature, the first law of thermodynamics, insists that matter and energy are conserved; they can neither be created nor destroyed. (Just trust me) And I don't think it needs to be any more complicated than that to show that Someone outside of this system created it, because the system cannot explain it.

Also, consider the laws of nature themselves. There are no serious explanations outside of God for the existence of the laws of nature in the first place, because there can be none. They describe the way things are, and they can link one effect to a cause, and that cause to a previous cause, but they can never explain the first cause. Naturalism is destined to fail. Making the assumption that this universe is all there is is not good science; it is a logical fallacy. Science is reasoning from observations to explanations, and it not limited to naturalistic explanations. In fact, it points to a Creator outside. I'll call him God.

Design

It has been rigorously scientifically documented in hundreds of ways: the world and whole universe we live in has been designed within an extremely narrow set of parameters necessary for the our existence. One relatively exhaustive compendium of scientific evidence for this fact is here: http://www.reasons.org/fine-tuning. **tl;dr?** Some stats: Based on the requirements to sustain bacteria for 90 days or less: "less than 1 chance in 10^{311} exists that even one such life-support body would occur anywhere in the universe without invoking divine miracles." Or, for three billion years: "less than 1 chance in 10^{556} exists that even one such life-support body would occur anywhere in the universe without invoking divine miracles." And yes, that is taking into account all thousands of billions of billions of possible planets.

And that doesn't even take into account many requirements for basic matter, and all the requirements for intelligent life. What are some of these parameters? For example, consider "the ratio of the gravitational force constant to the electromagnetic force constant. It cannot differ from its value by any more than one part in 10^{40} (one part in ten thousand trillion trillion trillion) without eliminating the possibility for life" or "the space energy density (the self-stretching property of the universe). Its value cannot vary by more than one part in 10^{120} and still allow for the kinds of stars and planets physical life requires." source Or another fundamental force: "If the strong nuclear force were just 4 percent stronger, the diproton (an atom with two protons and no neutrons) would form, which would cause stars to so rapidly exhaust their nuclear fuel as to make any kind of physical life impossible. On the other hand, if the strong nuclear force were just 10 percent weaker, carbon, oxygen, and nitrogen would be unstable and again life would be impossible." source A few others are discussed here: http://www.reasons.org/design-and-anthropic-principle. Over the past few decades hundreds of parameters have been found that need to fall within a restricted range for life to be possible. This place was designed. Looks like this God is smart.

Why the Bible?

At this point, you might say, but what about all the other religions in the world? How do you know which, if any, is true?

Fulfilled prophecies

One clear indication is in the fulfilled prophecies which would have been impossible without God. For example, many prophets foretold the exile of the Jews to Babylon before it happened. Then Jeremiah and Ezekiel prophesied their return about 70 years before it happened.

Many prophecies were fulfilled by Jesus, who also made many prophecies. Example: about 800 years before it happened, Micah foretold the birthplace of the Messiah. Jesus prophesied that the temple, the pride of Israel, would be destroyed so that not one stone was left on top, and it was fulfilled about 40 years later. He also prophesied that the Jews would be again exiled, which was fulfilled after the destruction of the temple. And the same had been prophesied by the prophet Micah about 850 years before it happened. Psalm 22 contains many details about Jesus, that were fulfilled in his life and death.

For those who like figures & numbers: This page http://www.reasons.org/fulfilled-prophecy-evidence-reliability-bible contains a few more examples of fulfilled prophecies, along with a corresponding probabilities of fulfillment. Another example: "Some time before 500 B.C. the prophet Daniel proclaimed that Israel's long-awaited Messiah would begin his public ministry 483 years after the issuing of a decree to restore and rebuild Jerusalem (Daniel 9:25-26). He further predicted that the Messiah would be "cut off," killed, and that this event would take place prior to a second destruction of Jerusalem. Abundant documentation shows that these prophecies were perfectly fulfilled in the life (and crucifixion) of Jesus Christ." In case you're wondering, the listed prophecies have a combined probability of less than 1 in 10^{138} of happening without Divine guidance; which, as pointed out, is stronger than our confidence in certain laws of physics, like the second law of thermodynamics. All Biblical prophecies have an estimated probability of 1 in 10^{2000} of just happening by chance.

A note on these probabilities. Just as a matter of perspective, if your friend asks you to pick a card out of a deck without showing him, and then he "randomly" picks the same card, you would know that it was rigged; your friend had to "cheat" somehow to figure out which card you pulled. And that's just one chance in less than 10^2. For comparison, an estimated number of atoms in the observable universe is 10^{80}. These numbers are literally inconceivable; the chance of these prophecies being randomly correct is far less than if two people each completely randomly picked a single atom out of the entire universe and they both happened to pick same one. Nerdy analogy, but you literally can't come up with a bigger deck to pick the card out of. That doesn't happen by chance; it can only happen by God's design.

Why Jesus?

The resurrection.

It is one of the central tenets of Christianity. When Jesus came, he performed many miracles that quickly drew and astonished the crowds; a big reason the number of Christians basically exploded in just a few years, only God could have done them. But the most well-known and important miracle God performed was after Jesus' death, his resurrection. A brief outline of why you can believe it is here from Stand To Reason. But I'll just list five basic facts, accepted by almost all scholars. See this page http://www.str.org/site/PageServer?pagename=PL_article_dead_or_alive_1 for a little more info.

Fact #1: Jesus died by Roman crucifixion. (numerous eyewitness accounts including medical reports, ancient historians, pre-burial procedures, and the Roman executioners all confirmed it)
Fact #2: The disciples believed they had seen the risen Jesus. (numerous eyewitness accounts; most chose to die rather than deny this fact, and no one dies for what they know is a lie)
Fact #3: Saul of Tarsus (Paul), an enemy of the church, converted because he believed he had seen the risen Jesus. (after dedicating his life to beating up, imprisoning, and killing Christians – no other believable explanation)
Fact #4: James, the brother of Jesus and a skeptic, converted because he believed he had seen the risen Jesus. (a skeptic his whole life until this event)
Fact #5: The tomb of Jesus was empty. (Once again, numerous eyewitnesses, as well as the inability of religious & political leaders to produce a body)
Over 500 individuals saw, met, touched, ate with, and/or talked with the risen Christ. From which I conclude that Jesus in fact did rise again from the dead.

So what does all this mean?

This faith is not a nice story, it's a fact. There is a real God who is beyond our universe and our conception. Yet he has put this incredible design together for us, and has given us his word, with a seal of authenticity. Jesus, who told us how to live, who claimed to be God, equal to the Father and the only way to God, proved it with his life, death, and resurrection. What does that mean for you? You can trust what the Bible says. You can trust in Jesus as your Lord and Savior and know where you are going after your death. Then love the Lord with all of your heart, soul, and mind and love your neighbor as yourself. It's the best way to live.

1. 

   #1 by **Adam** on April 26, 2011 – 2:17 am

   No offense is meant by the comments below but I have just a few questions…

   Why Jesus and why Christianity? Isn't it possible that some other force or being is responsible? I agree that it is very remarkable how the universe works and that in order for our existence things need to be a very specific way. But, is that to say there are NO other intelligent beings in the universe? If God put all those circumstances in place to allow us as humans to live, why would He leave the rest of the universe empty? And if they are other intelligent beings in the universe, which it is almost impossible to deny in my opinion, Do they also believe in God in the same sense as you? Or have they more scientifical answers for these questions than we do, and therefore have no "faith", but only science and fact?

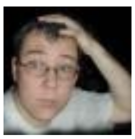
   - 

     #2 by **scriptjunkie** on April 26, 2011 – 11:40 pm

And no offense taken. Some of the reasons why Jesus and why Christianity is the fulfilled prophesies, resurrection, and other miracles, which are likewise supported by much evidence, and specific to Christianity.

I won't speak for God, but I don't see why there needs to be other intelligent life in the world. He could have created the vast universe because it makes a point about our relative size and abilities, or just because it's awesome. I don't think other intelligent life would happen by chance, given the research in the design section. But if he did create others, I am sure he would make available all the information he required of them.

As far as whether there could be a naturalist scientific explanation, I don't think so. The scientists (such as Dr. Ross above) who have been researching design predicted years ago that rather than finding a common natural cause of the disparate parameters finely tuned for life, scientists would continue to find more diverse parameters requiring fine tuning for life. That is exactly what has happened over the past few decades, which has really been amazing for me to watch. The more we learn, the more reason to believe in design we have. Everyone has a faith, a belief, in something. I want to base mine on the best explanation for the facts that we have, and that would be God.

2. 

#3 by **Kim Guldberg** on April 26, 2011 - 1:50 pm

IMHO your thoughts about design are wrong and you are jumping to conclusions. There is a perfectly simple and scientific explanation outside god for why everything seems to fit a design her on eath.

The simple explanation is that it fits because it is her. Out of the (undeliverable huge number of planets out there) her is where it fits. If something had been off, we would have existed on another planet where it would have fit and some people would have claimed that it is by design. It's not, it's by equilibrium, it had to happen somewhere and that's not design that the true strength of god, the force of life

○ 

#4 by **scriptjunkie** on April 27, 2011 - 12:17 am

Sorry, maybe I wasn't clear. According to our best estimates there **are** a huge number, about 10 000 000 000 000 000 000 000 (10^22), stars in the universe.

The chance that any individual star could support even the most basic bacterial life for a short time is one in 1 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000

000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 (10^333).

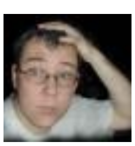
So the chance that even one such life-support body would occur **anywhere in the universe** without invoking divine miracles is 1 in 100 000. (10^311)

Yes, there is a huge number of stars. No, there aren't nearly enough for this to happen by chance. And to support advanced life is about 1 in over 10^1000. (See linked research compendium for source) And those figures do not even take into account the requirements for matter to exist as we know it at all. Unless things like the strong nuclear force and the ratio of the gravitational force constant to the electromagnetic force constant were precisely within 1 part in about 10 000 000 000 000 000 000 000 000 000 000 000 000 000 (10^40), there wouldn't be **any planets at all** to fit into. The universe still speaks of design.

Even if there could be another chemical basis of life, or heck, another billion ways life could happen, you still have to explain the fine tuning of the universe to within one part in over 10^150 for basic chemistry and then you have a billion (109) chances in 10^1032 for long-term life support, or still 1 in 10^1023 in total. The evidence is so overwhelming for design, even the vast number of planets in the universe cannot explain it.

Some people still argue that well, since we are here, everything that needs to be fine-tuned must have been. Unfortunately, that's not an explanation. To borrow an analogy, suppose you faced a firing squad of a hundred executioners with rifles, and after they all fired, you had not been hit. You don't say "of course they didn't hit me, I'm still alive" to explain why no bullets hit you. That doesn't explain anything. You know it didn't happen by chance. You know they didn't hit you by design. Either by choice (they all decided to aim away), or since someone replaced all the ammo with blanks, or some other design, you were not hit. And there is a much much much better chance of that happening by chance than the design of the universe. This universe didn't happen by chance.

edit:stars

3. 

#5 by **Kim Guldberg** on April 27, 2011 - 12:43 pm

its not 10^22 planets, it's 10^22 stars and if the solar system is average (and why shouldn't it be) every star has an average of 10 planets. Anyway it's a matter of faith and for me the whole idea of intelligent design is ridiculous and

unnecessary. your estimate of the chance is a arbitrary number. I could with just as much credibility state that the chance is one in 10^12 in which case many many millions of stars has planets that potentially holds life.

The problem is the word “theory”. The theory of relativity is a theory. The theory of Darwin is a theory. My theory that pigs can fly is a theory, so is intelligent design. you just cant compair the two. One s substantiated by science and can be replicated in a lab one is….heavily advocated by religious fanatics and has nothing to do with science.

But as with all faith you are welcome to belive what yu want, just don’t call your beliefs science

4. 

#6 by **scriptjunkie** on April 29, 2011 - 9:51 pm

Corrected on the stars. It is true, you can believe in whatever theory you want. But I would prefer to believe in the theory that is backed by the best analysis of the most evidence. The difference in the theory that pigs can fly or pegging the chance at 1 in 10^12 and what I am presenting is that the parameter fine-tuning I presented is all backed by peer-reviewed research. You may check the references. We may never agree, but I wish you the best.

5. 

#7 by **Kim Guldberg** on April 30, 2011 - 3:28 pm

That’s the problem. The “theory” of intelligent design is not “backed up by the best analysis of the most evidence”. It is often not backed up at all and when it is, it is backed up by pseudo scientifically analysis of what can best be described as possible interpretations of possibilities. I have searched high and low and not for evidence and analysis based on science. Let me give you an example of that kind of interpretation.
When I look at life here on earth, I see it in the most extraordinary places, where life shouldn’t exist. Thousands of meters below the surface of the ocean, where sunlight never reaches, with no oxygen, close to hydrothermal vents where the water is several hundred of degrees warm one moment and close to freezing the nest.
You would probably take this as a sign of the genius of the divine god and as a fact that this planet has REALLY been designed well.
I take it as a sign that life really does not need very specific conditions to spring and that life in fact will be quite abundant in the universe
I do however understand why people would find the “theory” of intelligent design enticing. Think about the alternative, that I am right. That we are not created by a divine god, in his image. What would that make us?
Just another ape really. And not even a cool, admirably, just ape that “one” could look up to. Rather a greedy, vicious, self-righteous, selfish ape with as much right to live as the next ape or common slug for that matter.

And there is more. What if I am right and that life is abundant in the universe. That would leave the possibility open for the fact that somewhere out there exists another “thing” that is more advanced than us but has the same ideas that it is created by a divine god in the image of that god, with the divine right to control and command everything else.
Where would that leave us?. If we are lucky we’d be pray, less lucky we’d be livestock and if we are unlucky we’d be a pest to be exterminated.
I don’t have any problems with individuals, such as yourself, believing in intelligent design. I have grown up (sort of) friends that believe in the old Nordic gods and some believe fiercely in Santa Claus.
My problem begins when the believers of intelligent design start to claim that it’s a prober scientific theory that should be taught in schools alongside the theories of Darwin. It’s a belief, not science and our school children should not have to be subjected to one belief any more that they should be subjected to any other belief and never have that belief presented as science.
You and I don’t have to agree as long as we both respect each other and leave open space for everyone to have his own believes. You might think that I don’t believe in god. You are wrong, I do. I would claim that I believe in a much bigger god then you do. I also believe in life, that it’s strong, abundant and beautifully diverse and I hope that it is spread all over the universe and that god lives in every living creature.

6. 

#8 by **scriptjunkie** on May 1, 2011 - 10:05 pm

I think schools should be run differently in other ways, but that’s another debate. I am not sure how you would define science, I would just call it an inductive search for facts based on observations, tests, and reasoning. And of course, I see it pointing toward design.
After all, without carbon, oxygen, nitrogen, etc. even the extremophiles can’t exist.

7. 

#9 by **Adam** on May 2, 2011 - 5:11 am

Perfect..exactly what I wanted my comment to do…start a debate. I didn’t even get involved and that was a better read than I could have posted. Good job, guys.
To each his own.

8. 

#10 by **mu'men** on May 11, 2011 - 3:14 am

This is an interesting topic, and I would like to join and talk about what I believe in (That there is God) from the point of view of another religion (Islam) and thanks in advance for giving me the chance.

—

Usually when people talk about God, the views are 1)there is God (regardless of religion or of it's nature) or 2)there is no God.

What I usually hear as an explanation as to why there is no God, comes to a scientific evidence. There is no scientific evidence to support the existence of God, and hence there is no God. Despite how the universe is complex, and that it came/happened by chance is almost none.

God in Quran asks people to look into the creation of themselves, the creation of the heaven and earth, the creation of oceans, of trees. How our body works? How babies grow in the womb? The stars in the sky and their locations and a lot more.

Travel in the land and see how He originated creation (29:20)

We shall show them Our portents on the horizons and within themselves (41-53

Verily! In the creation of the heavens and the earth, and in the alternation of night and day, there are indeed signs for men of understanding. (3:190)
Those who remember God (always, and in prayers) standing, sitting, and lying down on their sides, and think deeply about the creation of the heavens and the earth, (saying): "Our Lord! You have not created (all) this without purpose, glory to You! (3:191)

Today we know about the universe, the stars, about ourselves, etc. and how complex they are. We know more than any of the previous centuries ever knew.

We can insiste that despite all the knowledge we have that there is no God, or we can believe based on this knowledge that there must be a Creator.

God gives us the choice
And say: "The truth is from your Lord." Then whosoever wills, let him believe; and whosoever wills, let him disbelieve." (18:29)

On the day of Judgement one will know if he made the right choice or not.

Peace

9. 

#11 by CJ on June 7, 2011 - 10:40 pm

Hello, first of all let me say that it is absolutely amazing to see people stand up and support their faith. It is hard to find someone who proudly exclaims that they are a christian, so kudos on that. Secondly, I would like to point out that the bible is the most accredited piece of literature we have today. It is extremely hard to argue that we were made by a product of chance, and that we all are endowed with perceived morals. So even though it should be a simple assumption that there is an infinite being who is the creator, there is plenty of evidence to also point you in the right direction.

10. 

#12 by packetdude on August 11, 2011 - 12:48 pm

Pretty gusty and honest move to include this information on your site. I think infosec is the kind of field where people can do this, as we are used to fierce debate coexisting with collegiality.

I'm with you. I think it's important for people to understand that evolutionary thinking is essentially what nearly every religion other than Judaism and Christianity teaches. Look at the Norse/Germanic gods — they emerged from the pre-existing physical world.

All "scientific" analysis on origins is inherently flawed. Science depends on forming a hypothesis and then testing it. We have no means to test the origins of the universe. It's not repeatable or observable, and therefore any hypothesis about it cannot be verified in a proper scientific fashion.

11. 

#13 by rk on September 12, 2011 - 1:53 pm

This is a touchy issue but as a fellow netizen/techie I would take the liberty to discuss it and no offense meant at all. I won't go into restating what majority of the world including most scientists think, but here are some good starts -
http://www.youtube.com/watch?v=9V_2r2n4b5c&feature=related
http://www.youtube.com/watch?v=SSxgnu3Hww8&feature=BFa&list=HL1316615359&lf=mh_lolz&index=91
http://www.youtube.com/watch?v=vss1VKN2rf8&feature=BFa&list=HL1316615359&lf=mh_lolz&index=92
Also dont you think it is ironic to use science when it favors your argument but disregard it when it doesn't? Another case of double standard is you like to slectively point out a few things in the Bible/Chistian texts, what about all the questionable points of how old the earth is, how Mr. 'God' preaches peace but himself commits mass murder etc. etc. Again nothing personal but please dont disrespect the humble 'Science' which accepts its mistakes and strives to find an answer verus apparently all-knowing 'God' and his 'preachings' all of which is highly dubious.

#14 by **scriptjunkie** on September 12, 2011 - 2:42 pm

Thanks for your comment on my blog. I also believe it's totally possible to discuss different views without any personal offense, and welcome discussion. It is an issue that many people get very upset over, and I think it is almost sad how we can discuss things like the merits of full vs. coordinated disclosure but don't want to talk about bigger issues.

It took me a few minutes to get through the videos, and once I did, I was curious as to why you posted them on this article. The first video, "Lets Test Them: Evolution vs. Creationism" was interesting. There are some some valid points, as well as assumptions which are not correct, and it would prompt some interesting discussion; but this is actually not what I would consider the most important issue. I did not mention evolution or origin of species on my page.

The second video, "Top Ten Creationist Arguments" addressed the following ten arguments:

1. Carbon Dating
2. Can't prove evolution
3. Why no more monkeys
4. Human eye
5. Atheism is religion
6. Scientist "X" believes in God
7. Everything by chance
8. America is a Christian Nation
9. 2nd Law of Thermodynamics
10. Adolf Hitler was an atheist

Most of those are obvious non-sequitors, and most of the rest don't make sense or aren't good arguments anyway. That's why I didn't make any of those arguments. I talked about the 1st law of thermodynamics, and only used the second as an example of something that we all know to be true, since the probability of it failing is ridiculously small, yet still far larger than the probability the prophesies in the Bible did not come from God. Like the video said, ask about the other laws of thermodynamics.

Anyway, the third video, "Evolution" also of course talked about evolution and addressed arguments like the following:

1. Life evolves purely by chance
2. Apes mutate into humans
3. Humans from bricks
4. Dogs giving birth to cats or your grandparents are monkeys
5. Dogs morphing to cats
6. Crocoducks

7. Nazis, eugenics

Once again, I didn't make any of those arguments (and wouldn't; they do demonstrate a misunderstanding of evolutionary theory).

You also mentioned the age of the earth debate. I personally don't know exactly how old the earth or universe is, but there are a huge number of Christians, including myself, that believe the various scientists when they say it looks billions of years old. (and the discussion of how that can be interpreting the Hebrew text is also interesting, but less important) Once again, not an argument I made or would make.

I do not believe the mass murder argument makes sense in this case. If there is a God who created everything including moral law itself, and he said that at one point in history there was a group of people who were so evil that they all deserved death, and you had never met any of these people in your life, why would you doubt it? Because you didn't feel like that was very likely and you didn't think God would do that on purpose or you never saw anything like that in your experience? I do not believe anyone alive has seen anything like that. The argument convincingly shows that a god who claims to be good and yet lies about ordering the death of innocent people is not good. This is absolutely true, and I also believe this. It does not argue against what I believe.

In summary, I appreciate your willingness to discuss these issues, and I absolutely mean no disrespect or disregard to science. I also apologize if there are dozens of illogical or false arguments going around. But I encourage you to not simply dismiss the idea of Christ, because there are many good reasons to believe as well. So don't make the mistake of some scientists and ignore any explanation involving God, assuming he does not exist. Look at all the evidence and you'll find it strongly points to Christ.

12. 

#15 by **rk** on September 12, 2011 - 3:29 pm

Again I would love to discus point to point but I can't write such long comments as you :), I'm impressed! All I would say is give a serious look at events in your own history which has shaped your point of view, then put yourself in another set of shoes and think of this issue as a child would - looking for a logical reason to everything, without exceptions. Do not fall in the trap of anything unexplained must be God. Thank you for kindly listening to me 

13. 

#16 by **Neanderthal** on September 14, 2011 - 2:58 pm

Hi

Awesome presentation on Defcon, both material-wise and orally. Really enjoyed that one. You are clearly a very brilliant

guy, so this page was a surprise. I'm not here to troll, and I'm not here to offend you, or any who hold beliefs far away from mine. People may believe whatever they want, as long as they don't impose rules and laws derived from ancient scriptures on me, my loved ones – or any other person not heavily invested in that particular belief. You seem like an open minded person, willing to air your beliefs in open unperturbed (as in "you can't say that, it's blasphemy!") discussion and take honest criticism, so I'll dare comment this. I made some remarks on a paper as I read your beliefs and I will just comment them – not necessarily in order. I'm from Norway, but my English should be understandable (thanks spellchecker).

"Soul": my personal view on this is that it's a "brain bug". Evolution have given us a mindblowingly complex structure, and there's lots of old technology in there – inherited from earlier times when that particular technology gave us an edge in life. On the way we somehow picked up the ability to attach personality to objects – children do this all the time. They give name to rocks and sticks, some sticks are bad, some rocks are sad, etc. They can't avoid projecting, and neither can we (grownups). This is why it is almost impossible to avoid the fallacies: "me and my brain", and "what happens after I'm dead". We just have to put something "living" in there.

"Mark Cahill": I have not read this particular book (read the excerpt though), but I have read others like it. Beautifully written, but you soon get a very strong feeling that you are dealing with a car-salesman. Every sales pitch is in there, screaming at you. For some good hours of entertainment, read "Influence. Science and Practice" by Robert B. Cialdini.

"First cause": 1'st law of thermodynamics – matter and energy is conserved, nothing can come from nothing, ergo there must be a God. This is not a good argument, and it is in fact a very old one. The first mover argument is broken. And for another view on that 1'st law of thermodynamics stuff, read (or see and listen on youtube) Lawrence M. Krauss: a universe from nothing.

"Designed": it has definitely not been rigorously scientifically documented that the universe is designed. The word "designed" is a trap – it psychologically invents a "designer", projection again. But the "fine tuned" argument is annoying. We should, and must, be able to explain that one more clearly. But it is only annoying, nothing more. The leap from "the universe as is, is strongly dependent on the values of constants" to "it must have been designed by a grand intellect we don't have to explain" is rather arbitrary. And all of these constants comes from the "Standard model of particle physics". Albeit amazingly accurate, consists of twenty-something parameters that must be estimated and put into the model for it to work as well as it does. I'm a strong believer in, that if there is a TOE(theory of everything), the "Standard model of particle physics" is not in it. All these probabilities of some god – or improbabilities that shit just happens, seems like a case of "I blinded you with science" to me. If you change just this or that constant everything falls apart – but what if you change 2, or 5? And what about multiverse hypotheses? Each multiverse comes with their own set of physical laws and constants – we just happens to live in one of those, and we are what we are just because we live in this particular one (read e.g. Lee Smolin/Stephen Hawking. Victor Stenger has written stuff on the fine tuning argument, worth while reading). To me, all this is blindingly simple: we are ants, amateurs, n00bs. The universe is clearly amazingly complex, and our current version of physical laws is clearly not the last version. We have just scraped the surface. And with an awesome force like

evolution, who knows what is possible or not. Finding life on Jupiter's moons Europa or/and Io, or Saturn's Iapetus – or even Mars would be fun. Then most of these "improbabilities of life elsewhere" must be thrown away. But my guess is that if we found life on moons in our solar system, Mr. fine tuning himself, Dr. Hugh Ross, would simply calculate new probabilities, saying that this is overwhelming proof of the existence of God since the probability of finding life on more than one planet/moon in the solar system is 10^(-12467), with rounding errors.

"Fulfilled prophecies": firstly, the bible is not a reliable document. We don't have a single original of any of the books in the bible. Every one of them are copies of copies of copies. Read e.g. Bart D. Ehrman. It is a chosen collection of texts – the good ones they kept, the really insane ones the threw away of course. And the ones they kept was written by persons massively invested in the new religion to be. You have to already be a Christian to accept arguments from the bible, and that makes this a very blunt tool. Secondly, it is circular reasoning. The bible says there is a god, god exists because of this and that is written in the bible…

"Resurrection": Maybe there was a person called Jesus who lived in the middle east 2000 years ago. Maybe, because there is meager evidence of this. It should be pervasive evidence at hand, if what the bible says about Jesus is true. And, as previously said: arguments from the bible…

"You can trust what the bible says": Really? Have you read the old testament? Have you found all the discrepancies, the contradictions, the really nasty parts? No, you cannot trust the bible. And Christians are not famous for loving their neighbors, trust me on that.

Well, this turned out to be way too much text. Sorry about that. But to round up, I must tell a little about what it is like to be totally godless, (I was raised in a benign Christian home, ushered to Sunday schools, given religious explanations for even the mundanest things, etc. etc. Quite normal I guess.) and I can explain that in two words: I'm free!!!!! No strings attached! No authority looking over my shoulders, reading my inner thoughts. No eternity (which sounds really scary, even if you end up in the heaven part of it). All my moral and ethics comes from my own heart (brain of course, but heart sounds more poetic), and I have a provably big heart. I don't do the good things because I'm afraid of hell, or damnation – just because it feels good. I can take all the creds myself for the good things I do. And I can take all the blame myself if shit happens – shit happens because shit happens. And I can give all the creds to other people for the good things they do. And last, Hurricane Katrina was not God's wrath over America because Ellen DeGeneres is a lesbian! (I know this really wasn't true insane ramblings by Pat Robertson, but it could have been)

Regards
Neanderthal

#17 by **scriptjunkie** on September 15, 2011 - 5:54 am

Soul – was just used an example of why this is a topic of discussion. We could discuss it, but it wasn't the point.

Mark Cahill – as Mark will tell you himself, he knows he sounds like a salesmen, even though he was never trained as one. He just figured it was the best manner to convey his points. Ultimately of course, it's what you say, not how you say it; and I think he makes good points, although I like more technical details.

First Cause – Yes, it has been made for at least a few thousand years, and there are still quite a few theoretical physicists who agree with it given the modern theory of general relativity, and also given string theory, even with quantum mechanics. Unfortunately, Mr. Krauss's video was over an hour and it has already taken me days too long to get to the comments on this page, so I was unable to find the time to watch it or find a transcript.

Design – I see you trust that the extremely precisely aligned constants of the universe have a simple explanation, but serious research that these facts have, in part, spurred has only found more factors that must be precisely aligned. While a theory of everything might explain how matter and energy behaves including quantum mechanics and relativity, I doubt it would explain how we ended up with a precise amount, and in the right places, etc., so most of the constants are still serious obstacles to a design-less view. As far as multiverses, it seems sad to me that rather than reach a conclusion supported by evidence, some physicists will bet on the existence of many, like infinite universes for which they really don't have any evidence, aside from the assumption to avoid the design conclusion.

As to fulfilled prophesies, we can definitely speak to the reliability of the Bible, and I am not relying on the fact that the Bible said it was reliable, I am relying on the fact that it said what could not have been written by humans. When looking at ancient texts, normally we have only a tiny collection of manuscripts from around 1000 years after the work was originally written (e.g. less than 5 copies of any work of Aristotle from >1400 years after it was written), and no knowledge of what could have changed from the original writing. After all, just like a game of telephone, Charlie's copy of Bob's copy of Alice's copy when written by hand often leads to changes. On the other hand, if 20 people make a copy of Alice's letter, and dozens make copies of their copies, errors are easy to spot. And this is what has happened with the Bible, especially the New Testament on which the central doctrines of Christianity are presented.

"[T]he New Testament documents have a staggering quantity of manuscript attestation. Approximately 5,000 Greek manuscripts, containing all or part of the New Testament, exist. There are 8,000 manuscript copies of the Vulgate (a Latin translation of the Bible done by Jerome from 382-405) and more than 350 copies of Syriac (Christian Aramaic) versions of the New Testament (these originated from 150-250; most of the copies are from the 400x). Besides this, virtually the entire New Testament could be reproduced from citations contained in the works of the early church fathers. There are some thirty-two thousand citations in the writings of the Fathers prior to the Council of Nicea (325).

…"Most historians accept the textual accuracy of other ancient works on far less adequate manuscript grounds than is available for the New Testament." http://www.apologetics.org/TheHistoricityoftheNewTestament/tabid/68/Default.aspx

Resurrection – There is a huge amount of evidence from not only the eyewitnesses, but how the early Christians acted, etc. You really can't believe anything from ancient history without accepting something with far less historical backing than the resurrection.

Trusting the Bible – Yes, I have read many accounts of contradictions in the Bible, which range from pulling words out of context to misunderstandings to simply not contradictions. And I know that Christians have not always acted the way they say they should. I am definitely not perfect either. But that of course does not affect whether the Bible is true, or loving those around you is a good way to live.

And no comment on Pat Robertson. He speaks for himself.

14. 

#18 by **Neanderthal** on October 9, 2011 – 7:42 pm

Hi again
Just to get things straight: you consider yourself a creationist, yes? And if you would rate your belief in what the bible says… in a scale from 1 to 10, what would it be? Is it a guideline for living as a Christian, or do you consider it hard facts – the word of God must be followed. I really, really hope you choose the right things to say here, because I really, really don't want you to kill your children if they don't respect you, or stone strangers to death which pick firewood on the Sabbath.

I read all of the prophecies in the "Evidence for the reliability of the bible", and to be frank I'm very disappointed. There is nothing tangible there at all. Everything is written for ancient middle-easterners, by ancient middle-easterners. Just to pick a short one:

"(2) In approximately 700 B.C. the prophet Micah named the tiny village of Bethlehem as the birthplace of Israel's Messiah (Micah 5:2). The fulfillment of this prophecy in the birth of Christ is one of the most widely known and widely celebrated facts in history."

No, it is not a fact (and there is that car-salesman feeling again). There is absolutely no evidence for this. And worse, since the history of Jesus is written by people heavily invested in the notion that Jesus was the Messiah, you don't need a masters degree in public relations to see the importance of locating his birth to that specific place. It is extremely biased.

If God wants to declare his (its/hers) existence, why on earth would he (it/she) do it in the lamest way possible. He (it/she) could easily have done a much more interesting job than that. Been a long time since I read the bible, but didn't Jesus himself make predictions, the end of the world is near, and so near that it should be witnessed by those living at the time?
Cite["Evidence for the reliability of the bible"] :
"The acid test for identifying a prophet of God is recorded by Moses in Deuteronomy 18:21-22. According to this Bible passage (and others), God's prophets, as distinct from Satan's spokesmen, are 100 percent accurate in their predictions.

There is no room for error."

Then Jesus does not qualify.

Now, assume that the bible said something interesting, like prophesize the internet and mobile phones – or something useful, and cool, like an elementary proof of Fermat's last theorem. Then you may argue that precognition exists, but you are not allowed to take a humongous leap of logic and infer the existence of a god.

If you find the bible convincing, then what about the Indian contemporary guru Sathya Sai Baba? There are thousands of witnesses who have seen him turning water into gasoline, multiplying food , healing the sick, etc. etc. Sounds very much like another character we know of – except the gasoline part. And here you actually have living witnesses – not 2000+ years old manuscripts. Or what about alien abduction? Thousands of normal, sane (arguably, but still..) people telling the same story. Or all the people who have met Elvis recently, been healed and given spiritual advice.

One have to already be a Christian to take the bible as evidence for God.

"As far as multiverses, it seems sad to me that rather than reach a conclusion supported by evidence, some physicists will bet on the existence of many, like infinite universes for which they really don't have any evidence, aside from the assumption to avoid the design conclusion."

Is that what you want scientists to do? Reach the conclusion that it was all God's fault? If you find something peculiar in your data, just blame God – it's all magic. And speaking of science, how would you explain God scientifically? To me God is the end of science, the end of reason. It is the ultimate answer to anything, and it gives us nothing in return – ergo we must stay clear of that path (the last part applies to godless people only of course, as religious people see huge benefits after death.)

Maybe the universe is designed. Maybe it's a huge computer simulation. Maybe the constants are what they are because of genetic algorithms in the simulation, converging to what they currently are based on some criteria. Or maybe our universe is just a little pocket of complexity in some humongous set of physical laws – spawning universes with local physical laws. Or maybe higher-dimension branes colliding, starting new big bangs. Or maybe it is just one of those things we never will know the answer to, some annoying consequence of Gödel's Incompleteness Theorem. All of the above is to me more reasonable hypotheses than jumping to the notion of a god – and especially the horrible God of the old testament.

PS: I think the dates in the comment section are off…

Regards

Neanderthal

15. 

#19 by **scriptjunkie** on October 17, 2011 - 1:08 am

Creationist is a word a lot of people use to mean different things, so I don't typically use it. I can hardly think of a better authority on where certain people were and what they did in the ancient middle east than numerous accounts written by people who were there at that time. I am not sure what tangible evidence is better than testimony from people who were present. Also, when you say that Jesus predicted the end of the world, I assume you are talking about Matthew 16:28, "Truly I tell you, some who are standing here will not taste death before they see the Son of Man coming in his kingdom" which was fulfilled in the next two verses: "After six days Jesus took with him Peter, James and John the brother of James, and led them up a high mountain by themselves. There he was transfigured before them. His face shone like the sun, and his clothes became as white as the light." The same thing is recorded in Mark and Luke as well. Although I guess I can see why people take that to refer to the end of the world, Jesus did not say the end of the world. He frequently talked about the Kingdom of God as a present reality, and it makes more sense when read in context. As far as a conflict between scientific investigation and God, perhaps I should have been clearer, but I am saying the exact opposite. Belief in God leads me to believe the well-established scientific basis for such unchanging facts as the laws of nature and fundamental facts about matter and energy, etc. I fully support continued scientific research, which by the definition I always heard was testing theories logically and experimentally. I am disappointed at some scientists who have faced evidence that world does not support their worldview, and so have decided they didn't really believe the evidence anymore and played the what-if game. "I don't like that the laws of nature are special, so rather than accept that, I am going to imagine that they aren't" And when you play the what-if game, you can ignore every experiment that shows the laws of nature for what they are. Of course, this has not explained what created the universe and its laws, it just made that problem even bigger, since now there's more laws and universes to explain. I am also surprised that creating a universe, giving prophesies of events hundreds of years in the future at personal and international levels, physically coming to earth, and performing miraculous signs including rising from the dead is considered "the lamest way possible" while stating that a proof that x^n+y^n=z^n has no integer solutions for n > 2 will be found is not lame. While I share your enthusiasm for math, I have a hunch that most people would not be as convinced.

Also, yeah, the dates/times are wrong – server clock is messed up I think and regardless it's been too long again and I've run out of time again.
Cheers

16. 

#20 by **max** on August 20, 2013 – 8:43 am

It's sad that someone who knows how to think (=create great apps) still believes snakes can talk… Wake up man! Bible? I understand you would kill your wife if she was not a virgin? YES. it is in your book. Wake up.. grow up!

17. 

#21 by **akarta** on June 15, 2014 - 11:23 am

Word Up 2 You, nice to see a page like this on a IT sec page.

Kim and Max shut up,

scriptjunkie do yourselve a favor and turn off the comments, cause everyone has an asshole just as they do opinions

18. 

#22 by **ihavoc** on July 13, 2014 - 10:01 pm

scriptjunkie, I just stumbled upon this old post and I wanted to let you know that I appreciate your courage. In today's politically correct society, Christians are "allowed" to have our beliefs so long as we concede to the apagogical argument that God==Santa Clause or the Nordic gods therefore he doesn't really exist. Many people cannot bring themselves to open their minds Christianity but I imagine this post has caused many to search for the truth. Thank you for the read

19. 

#23 by Terrance T on August 31, 2014 - 2:33 am

I was looking at a talk that was posted through Adrian Crenshaw's website and same youtube channel, through IronGeek.com. I don't remember if it was a powershell talk or an incident response related "attack path" discussion…anyway…the speaker said that he knew you and included on one of the slides a "incident Response Roadmap" he called it. He had the URL listed on the slide, but I can't seem to find it anywhere on your site. I'd appreciate it if you could link me via email. I've been looking all over for it. I don't remember if it was a talk in Defcon2013, BSides2014 (which city…geez) NotaCon, CircleCityCon2014, or another one of those…so many. My brain is overwhelmed…can you post it or relink it somewhere?

I really like your slide share slides. They make a WORLD of sense of an intrusion response analyst. I like your work. It's inspiring and great (LONG) but great blog on Building Secure Networks. Fabulous…thanks if you can help.

- 

#24 by **scriptjunkie** on September 1, 2014 - 1:06 am

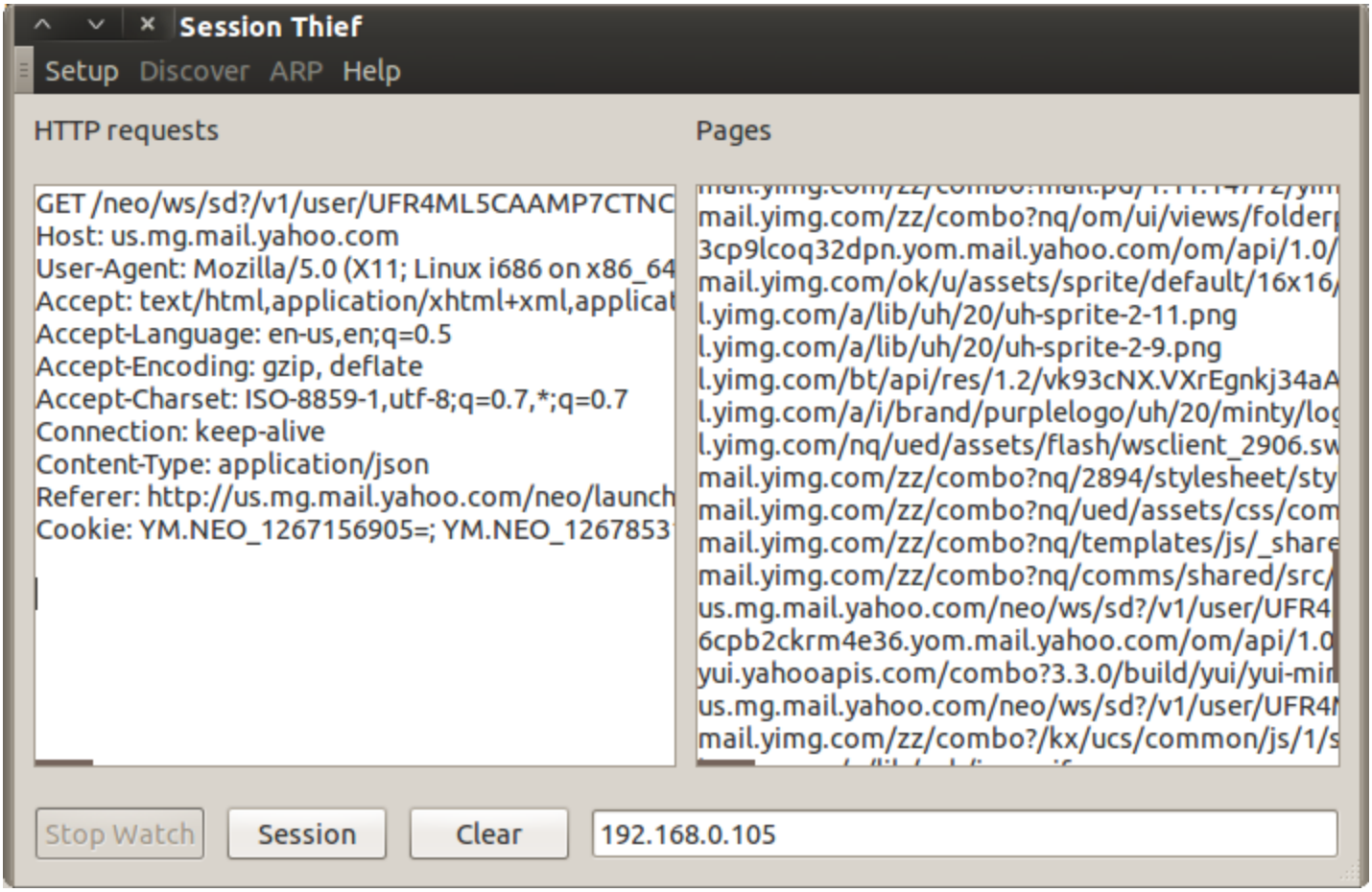
Terrance, you can find the attack graph here: networkintrusionposter. That's probably what you are looking for. You can buy a full size version here which is nice. If you haven't seen it, my latest presentation on the topic was at Derbycon which you can find here.

http://www.scriptjunkie.us/important-stuff/

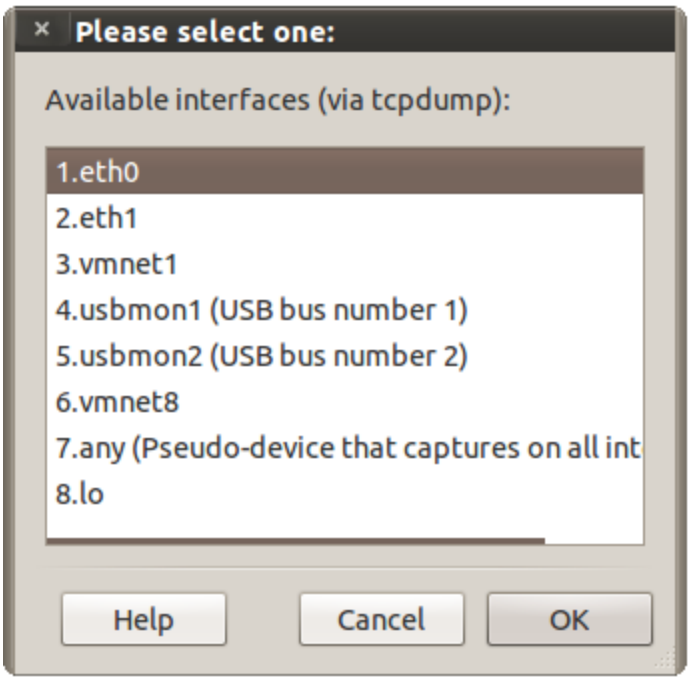
sessionthief

It's now 2013, which makes it over 6 years since sessionthief was written. Yahoo Mail and Facebook now offer SSL encryption, and GMail uses it by default, in large part due to the awareness that programs like sessionthief brought to the problem. That means that now sessionthief often does not work against the biggest targets, but there are still plenty of other websites out there that are vulnerable to hijacking.

sessionthief is a program to perform HTTP session cloning by cookie stealing. It can do some simple host discovery and can perform ARP Poison Routing to get packets if you are not connected to a hub or open wifi network.



It integrates automatically with Firefox, dynamically creating a temporary profile for each attack performed. For example, if multiple clients on the open or WEP-encrypted wireless network you are on are on facebook (or yahoo mail or just about any site you log into), you can 1. start the program, 2. select your interface, 3. hit watch, and 4. select a request from each of them to facebook, and click the session button. The program will start a new instance of firefox for each session hacked, and let you control the login of all of them at once.



It compiles and runs on linux and windows depending on the pcap and wxwidgets libraries. The source and binaries for windows and linux are at https://github.com/scriptjunkie/sessionthief or in a downloadable zip: sessionthief.zip.

If you have a different Linux version or architecture, compile it yourself. First, install the development libraries for gtk2, wxwidgets, and libpcap:

```
# apt-get install build-essential libwxgtk2.8-dev libgtk2.0-dev libpcap-dev
```

Then unzip the sessionthief folder in some directory and cd into the sessionthief folder. The complete compilation can be performed in one command:

```
$ g++ $(wx-config --cppflags --libs) -lpcap -o sessionthief *.cpp
```

Ideally, you should give it the raw net capability and run it normally:

```
setcap cap_net_raw,cap_net_admin=eip sessionthief
```

Otherwise, you will need to run as root or have tcpdump installed setuid root (run `# chmod 4755 `which tcpdump`` as root) to get packets live or you can open a pcap file saved from tcpdump or wireshark, etc.

Sessionthief also now includes an automatic update feature; it will display a message on startup when it detects a new version.

1. 

   #1 by genuix on April 25, 2013 - 9:20 am

Hi sir,

Congrat for you so great work, realy apreciate it.

I tryed to compile it in the new Kali system i just installed.

Just to tell you about a possible typo in 2 files of the sessionthiefSRC:

nviewFrame.h:44:27: fatal error: processthread.h: No such file or directory

processThread.cpp:3:27: fatal error: processthread.h: No such file or directory

in both case i just correct the “t” to “T” in the included file name and is’t compiled well.

Cheers

Jeff

- 

#2 by **scriptjunkie** on April 27, 2013 - 3:50 am

Thanks for the bug report! Should be fixed now.

2. 

#3 by **resetter** on October 16, 2013 - 4:53 pm

Hey,

compiled sessionthief on kali, but i get the following errors on running it:

http://pastebin.com/KwsguW6G

- 

#4 by **scriptjunkie** on October 18, 2013 - 3:23 am

Hi resetter, looks like I have an old version up there. Try downloading the zip file and compiling again. I don’t have Kali, but I made some changes to make it work on the system I am on now.

3. 

#5 by **resetter** on October 18, 2013 - 3:32 pm

Thanks for your efforts but I now get errors while compiling, I have all the dependencies installed.

Compile errors:

http://pastebin.com/NkS9bU0i

- 

#6 by **scriptjunkie** on October 20, 2013 - 2:03 am

Seems to be a different version of WxWidgets than I have. Try again! I went ahead and put it onto github so you can see the development if you want.

https://github.com/scriptjunkie/sessionthief/commit/47600e7a4b75969b25b52d130c75eac65719968e

http://www.scriptjunkie.us/http-sessionthief/

Read Carefully

Before you download scriptjunkie's 0day you must agree:

- scriptjunkie isn't a lawyer and can't afford one either, but he thinks there is legal precedent for this if you don't act evil.
- scriptjunkie doesn't guarantee anything and certainly doesn't condone illegal activity and won't pay your legal bills.
- Do you agree to all those conditions?

.

- Yes, I agree. Take me to the 0day
- No, I don't agree or I don't know what I'm doing here.

https://www.scriptjunkie.us/aaa.html\

sessionthief errors (more)

http://pastebin.com/NkS9bU0i

systemInterface.cpp: In static member function ‘static pcap_if_t* SystemInterface::getInterface()’:

systemInterface.cpp:309:112: error: invalid conversion from ‘void**’ to ‘char**’ [-fpermissive]

In file included from /usr/include/wx-2.8/wx/choicdlg.h:17:0,

from systemInterface.h:44,

from systemInterface.cpp:2:

/usr/include/wx-2.8/wx/generic/choicdgg.h:104:5: error: initializing argument 6 of ‘wxSingleChoiceDialog::wxSingleChoiceDialog(wxWindow*, const wxString&, const wxString&, int, const wxString*, char**, long int, const wxPoint&)’ [-fpermissive]

systemInterface.cpp:323:119: error: invalid conversion from ‘void**’ to ‘char**’ [-fpermissive]

In file included from /usr/include/wx-2.8/wx/choicdlg.h:17:0,

from systemInterface.h:44,

from systemInterface.cpp:2:

/usr/include/wx-2.8/wx/generic/choicdgg.h:112:5: error: initializing argument 5 of ‘wxSingleChoiceDialog::wxSingleChoiceDialog(wxWindow*, const wxString&, const wxString&, const wxArrayString&, char**, long int, const wxPoint&)’ [-fpermissive]