BIZ & IT —

New attacks on Network Time Protocol can defeat HTTPS and create chaos

Exploits can be used to snoop on encrypted traffic and cause debilitating outages.

DAN GOODIN - 10/21/2015, 6:07 PM

Matteo Ianeselli

Serious weaknesses in the Internet's time-synchronization mechanism can be exploited to cause debilitating outages, snoop on encrypted communications, or tamper with Bitcoin transactions, computer scientists warned Wednesday.

The vulnerabilities reside in the Network Time Protocol, the widely used specification computers use to ensure their internal clocks are accurate. Surprisingly, connections between computers and NTP servers are rarely encrypted, making it possible for hackers to perform man-in-the-middle attacks that reset clocks to times that are months or even years in the past. In a paper published Wednesday titled *Attacking the Network Time Protocol*, the researchers described several techniques to bypass measures designed to prevent such drastic time shifts. The paper also described ways to prevent large numbers of computers from successfully connecting to synchronization servers.

The attacks could be used by malicious actors to wreak havoc on the Internet. An attack that prevented sensitive computers and servers from receiving regular time-synchronization updates could cause malfunctions on a mass scale. In many cases, such denial-of-service hacks can be carried out even when attackers are "off-path," meaning the hacker need not have the ability to monitor traffic passing between a computer and NTP server.

Going back in time

Even worse, the attacks can be used to snoop on encrypted traffic or to bypass important security measures such as DNSSEC specification preventing the tampering of domain name system records. The most troubling scenario involves bypassing HTTPS encryption by forcing a computer to accept an expired transport layer security certificate.

The researchers wrote:

> An NTP attacker that sends a client back in time could cause the host to accept certificates that the attacker fraudulently issued (that allow the attacker to decrypt the connection), and have since been revoked. (For example, the client can be rolled back to mid-2014, when > 100K certificates were revoked due to heartbleed.) Alternatively, an attacker can send the client back to a time when a certificate for a cryptographically-weak key was still valid. (For example, to 2008, when a bug in Debian OpenSSL caused thousands of certificates to be issued for keys with only 15-17 bits of entropy.) Moreover, most browsers today accept (non-root) certificates for 1024- bit RSA keys, even though sources speculate that they can be cracked by well-funded adversaries; thus, even a domain that revokes its old 1024-bit RSA certificates (or lets them expire) is vulnerable to cryptanalytic attacks when its clients are rolled back to a time when these certificates were valid.

Besides HTTPS and DNSSEC, other security measures that could be defeated include HTTP strict transport security. The researchers also said NTP attacks could be used to trick Bitcoin users into rejecting legitimate entries in the official blockchain for the digital currency, or to tamper with user authentication systems used by websites.

To attack...	change time by ...	To attack...	change time by ...
TLS Certs	years	Routing (RPKI)	days
HSTS (see [59])	a year	Bitcoin (see [12])	hours
DNSSEC	months	API authentication	minutes
DNS Caches	days	Kerberos	minutes

Enlarge

It's not clear how practical some of the attacks would be in real-world settings. A desktop computer with a clock that was set to a date months or years in the past would almost certainly be easy to detect. And it wouldn't be surprising if the incorrect time would trigger errors from the operating system or other applications. Still, it's likely the attacks could be used in limited settings, or in combination with other hacks. It also might be possible to briefly reset the clock to an earlier date to observe an encrypted Web session, and then change it back right afterward.

Another limiting factor to such attacks is a measure built into the NTP specification that's designed to prevent time changes of more than about 16 minutes. Once the time change exceeds the "panic threshold," the client computer is supposed to reject the instruction and record an error. But the researchers said this measure can be defeated in at least two ways. One is to employ a technique known as a "small-step-big-step" attack that makes the change gradually. Another bypass method involves using NTP to reset the time immediately after a targeted computer has rebooted. The reboot time reset function is turned on by default in some operating systems.

Wednesday's paper comes 21 months after miscreants exploited separate NTP weaknesses to visit crippling denial-of-service attacks on game sites. The previously unseen amplification technique allowed a small number of attackers with limited bandwidth to bombard the targets with more than 100 gigabytes per second of junk traffic. Last December, attack code was published that exploited what was then newly discovered vulnerabilities in NTP implementation and in the process put countless servers at risk of remote hijacks.

Got crypto?

One of the key weaknesses making the attacks possible is the difficulty of ensuring computers communicate only with legitimate NTP servers. While it's possible to use symmetric encryption to cryptographically authenticate an NTP service, keys are difficult to acquire. The National Institute for Standards and Technology, for instance, distributes keys only to users who register using US mail or facsimile, and they're required to resend the application each year. The US Naval Office has a similar procedure. There's separate measure known as Autokey that's also designed to cryptographically verify that a client is connected to a valid NTP server, but many servers don't support it.

Wednesday's paper, which was written by researchers from Boston University, revisits several attacks that have been developed and presented over the past few years by independent researcher Jose Selvi. Presentation slides from a talk he gave at the Defcon hacker convention in August show he developed NTP attacks that bypassed HTTPS, HSTS, and website authentication, among other things. Selvi, who was a senior penetration tester at NCC Group when he did the research, released a proof-of-concept tool dubbed DELOREAN that streamlines many of the attacks. He published a blog post Wednesday that has additional details. The Boston University researchers credited Selvi in their paper.

The Boston University researchers have published an information page that helps people diagnose and remedy NTP weakness both on client computers and servers that provide the time-synchronization service. At a minimum, clients and servers alike should run NTP version 4.2.8p4 available here. There are a variety of other configuration settings that can be applied to better lock down the service as well.

Post updated in the second-to-last paragraph to add details about a separate researcher who has devised many of the same attacks.

Promoted Comments

Dilbert / Ars Legatus Legionis JUMP TO POST

> SixDegrees wrote:
> > rick*d wrote:
> > Back in the day my then-employer (a Fortune 500 company) considered using GPS as a time source for all their computers. I often wondered why we couldn't just do that, given how ubiquitous those things are (damn near every phone has one, they can't cost much anymore). Just make a GPS USB dongle that tells your PC the time and eliminate the need for NTP.
> >
> > Yeah, I know, NTP is cheaper. But do we really need to depend on Microsoft to tell our Windows PCs what time it is?

> One huge problem: GPS just doesn't work indoors. You need an outdoor antenna to reliably pick up the signal.
>
> It might make sense, at least in urban areas, to obtain accurate time from the cellular network, which has much better building penetration.

OTOH cell providers can screw up or get hacked, much in a way an NTP server on the internet could screw up or get hacked.

GPS time comes from atomic clocks on the satellites themselves, and they are managed by US Air Force. One satellite may break down and stop transmitting, but it's very very unlikely that they'd ever transmit wrong time.

21489 posts | registered Mar 15, 2002

---

micr0be / Smack-Fu Master, in training JUMP TO POST

Exploiting NTP is on the primary checklist of network penetration. Not to mention, the most common way to hide your tracks after successfully infiltrating a network is to hit the NTP server and bury your activity in the logs. You can do it before or after, depends on the network.

None of this is new, it's just slowly surfacing to the mainstream (sorta).

6 posts | registered Dec 4, 2013

READER COMMENTS 121 SHARE THIS STORY

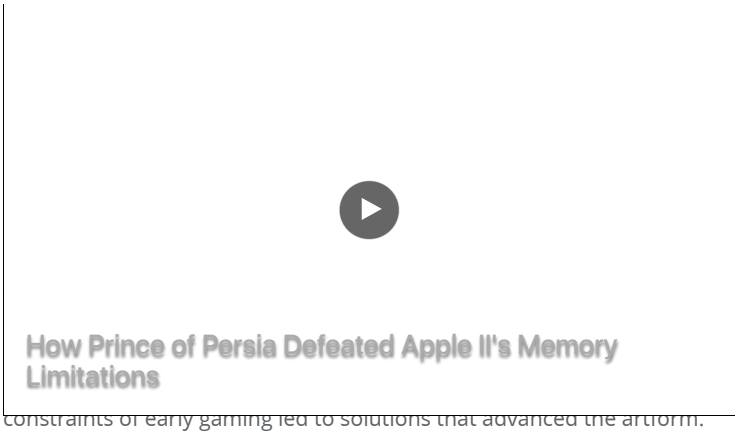
DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

How Prince of Persia Defeated Apple II's Memory Limitations

How Crash Bandicoot Hacked The Original Playstation



constraints of early gaming led to solutions that advanced the artform.

Myst: The challenges of CD-ROM | War Stories

Markiplier Reacts To His Top 1000 YouTube Comments

Customizing Mini 4WD Racers For High Speeds

More videos

← PREVIOUS STORY

NEXT STORY →

Related Stories

Sponsored Stories

Powered by

10 Best Used Cars Under $5,000
Kelley Blue Book

The Cost of a Plumber in Springfield Might Surprise You! Search For Emergency Plumbing Service In Springfield
Yahoo! Search

[Gallery] 40+ Wild Photos That The Government Has Declassified
DailyForest

About Plaque Psoriasis: Learn About Causes & Symptoms. Search For Moderate To Severe Plaque Psoriasis
Yahoo! Search

[Pics] Bo Derek Is 63, This Is Her Now
Noteabley

[Gallery] The Most Paused Movie Scenes Viewers Just Had To See More Than Once
History 101

Today on Ars

STORE
SUBSCRIBE
ABOUT US
RSS FEEDS
VIEW MOBILE SITE

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS

NEWSLETTER SIGNUP

Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox.

SIGN ME UP →