
nic.br
Brazilian Network
Information Center
cgi.br
Brazilian Internet
Steering Committee
registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

CGI.br members and former members
(only the current members have right to vote)

# GENERAL ASSEMBLY

7 members elected by the General Assembly

**ADMINISTRATIVE COUNCIL**

**AUDIT COMMITTEE**

- ADMINISTRATION
- LEGAL
- COMUNICATION
- ADVISORIES: CGI.br and PRESIDENT

**EXECUTIVE BOARD**

1 2 3 4 5

| registro.br | cert.br | cetic.br | ceptro.br | ceweb.br | ix.br | W3C Brasil |
|---|---|---|---|---|---|---|
| Domain Registration IP Assignment | Security and Incident Response | Studies and Surveys About ICT use | Internet Engineering and New Projects | Web Technologies | Traffic Exchange | Web Standards |

1 Chief Executive Officer
2 Administrative and Financial Director
3 IT and Services Director
4 Director of Special Projects and Development
5 Consulting Director for CGI.br activities

# É hora de deixar seu provedor mais seguro com NTP + NTS

Antonio Marcos Moreiras

nic.br

# POR QUE USAR O NTP?

- Os relógios dos computadores e dispositivos de rede, por si mesmos, **não são bons em medir o tempo**.
  - podem “errar” em vários segundos por dia
  - alguns dispositivos sequer mantêm o registro do tempo quando desligados

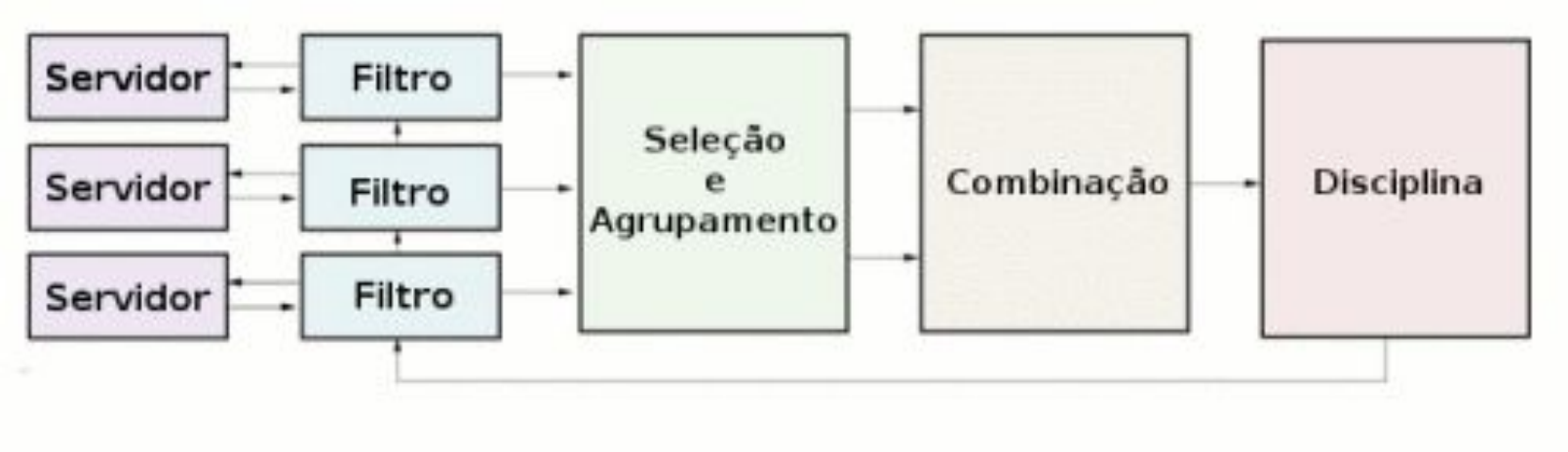
**Por outro lado, muitos softwares e sistemas dependem do correto registro do tempo. Temos também os requisitos legais!**

# NTP COMO SOLUÇÃO

- O NTP é um sistema que utiliza poucos recursos computacionais e sua configuração é simples. Em muitos sistemas hoje já vem instalado e configurado por padrão.
  - Nem sempre a configuração padrão é a mais adequada e nem sempre ela existe!
- O NTS, agora disponível, e novas implementações de clientes e servidores, tornaram o NTP mais robusto e seguro nos últimos anos.

# O NTP (Network Time Protocol)

Não é apenas um protocolo, mas também
um conjunto complexo de ALGORITMOS



# NTP: SEGURANÇA

- A **confidencialidade** não é considerada um problema, ou um requisito, no contexto do NTP
- Os algoritmos no NTP garantem de forma bastante satisfatória a **integridade** e a **disponibilidade** do serviço de manter o relógio correto
- Algoritmos de criptografia no contexto do NTP garantem principalmente a **autenticidade**.

# NTP: SEGURANÇA

- Chaves simétricas (symmetric keys)
  - existe desde o NTP v3
  - não oferece meios para transmissão ou armazenamento seguro das chaves
- Autokey
  - introduzido no NTP v4 (RFC 5906 não especifica um padrão, é informational)
  - não funciona com NAT, é complexo e inseguro
  - **não deve ser utilizado!**
- NTS

# NTP: SEGURANÇA

- Segurança não era uma preocupação na correta sincronização dos relógios no passado
- Mas muita coisa mudou:
  - a Internet cresceu e se descentralizou
  - há muitas evidências de um tratamento inadequado da segurança no NTP
  - há uma interdependência crescente entre o registro do tempo e a segurança
  - há requisitos legais e de conformidade

NEWS

# Attackers use NTP reflection in huge DDoS attack

The attack peaked at over 400Gbps, according to CloudFlare, the company whose infrastructure was targeted

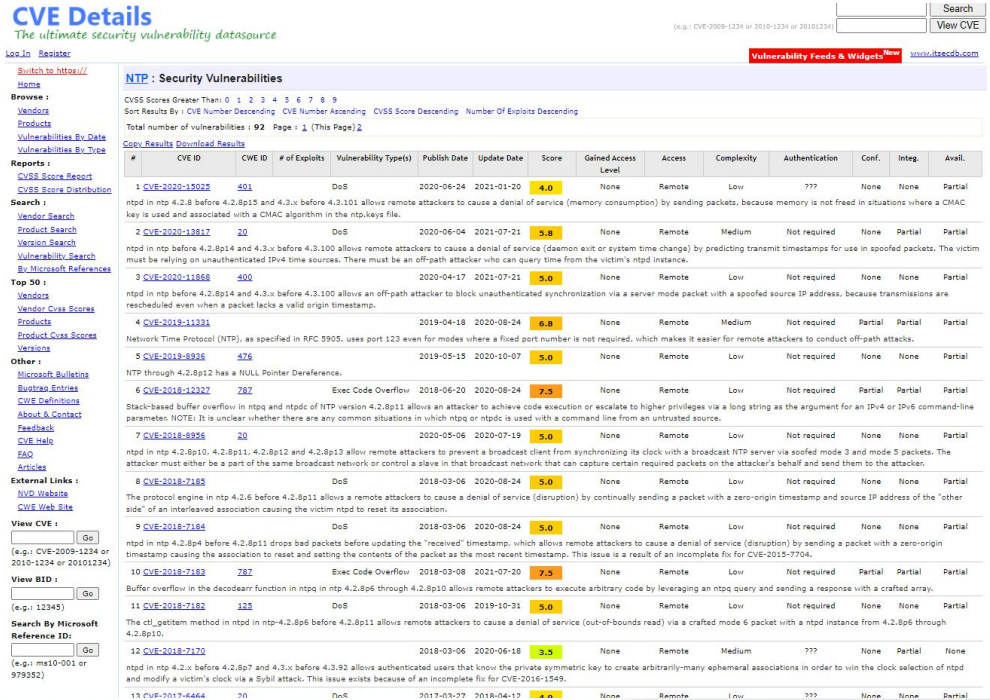
By Lucian Constantin

CSO Senior Writer, IDG News Service | FEB 11, 2014 12:25 PM PST

Attackers abused insecure Network Time Protocol servers to launch what appears to be one of the largest DDoS (distributed denial-of-service) attacks ever reported, this time against the infrastructure of CloudFlare, a company that operates a global content delivery network.

The attack was revealed Monday on Twitter by Matthew Prince, CloudFlare's CEO, who said that it's "the start of ugly things to come" because "someone's got a big, new cannon."

The size of the attack appears to have been just shy of 400Gbps, ranking it among the largest DDoS attacks CloudFlare has seen, Prince said Tuesday via email, adding that the company is still gathering data about the incident from upstream providers.



CVE Details

The ultimate security vulnerability datasource

Search | View CVE

Log In Register | Vulnerability Feeds & Widgets | www.itsecdb.com

Switch to https://

Home

Browse : Vendors, Products, Vulnerabilities By Date, Vulnerabilities By Type

Reports : CVSS Score Report, CVSS Score Distribution

Search : Vendor Search, Product Search, Version Search, Vulnerability Search, By Microsoft References

Top 50 : Vendors, Vendor Cvss Scores, Products, Product Cvss Scores, Versions

Other : Microsoft Bulletins, Bugtraq Entries, CWE Definitions, About & Contact, Feedback, CVE Help, FAQ, Articles

External Links : NVD Website, CWE Web Site

View CVE : Go (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID : Go (e.g.: 12345)

Search By Microsoft Reference ID: Go (e.g.: ms10-001 or 979352)

NTP : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 92 Page : 1 (This Page) 2

Copy Results Download Results

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Complexity | Authentication | Conf. | Integ. | Avail. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2020-15025 | 401 | | DoS | 2020-06-24 | 2021-01-20 | 4.0 | None | Remote | Low | ??? | None | None | Partial |
| | ntpd in ntp 4.2.8 before 4.2.8p15 and 4.3.x before 4.3.101 allows remote attackers to cause a denial of service (memory consumption) by sending packets, because memory is not freed in situations where a CMAC key is used and associated with a CMAC algorithm in the ntp.keys file. | | | | | | | | | | | | | |
| 2 | CVE-2020-13817 | 20 | | DoS | 2020-06-04 | 2021-07-21 | 5.8 | None | Remote | Medium | Not required | None | Partial | Partial |
| | ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance. | | | | | | | | | | | | | |
| 3 | CVE-2020-11868 | 400 | | | 2020-04-17 | 2021-07-21 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp. | | | | | | | | | | | | | |
| 4 | CVE-2019-11331 | | | | 2019-04-18 | 2020-08-24 | 6.8 | None | Remote | Medium | Not required | Partial | Partial | Partial |
| | Network Time Protocol (NTP), as specified in RFC 5905, uses port 123 even for modes where a fixed port number is not required, which makes it easier for remote attackers to conduct off-path attacks. | | | | | | | | | | | | | |
| 5 | CVE-2019-8936 | 476 | | | 2019-05-15 | 2020-10-07 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | NTP through 4.2.8p12 has a NULL Pointer Dereference. | | | | | | | | | | | | | |
| 6 | CVE-2018-12327 | 787 | | Exec Code Overflow | 2018-06-20 | 2020-08-24 | 7.5 | None | Remote | Low | Not required | Partial | Partial | Partial |
| | Stack-based buffer overflow in ntpq and ntpdc of NTP version 4.2.8p11 allows an attacker to achieve code execution or escalate to higher privileges via a long string as the argument for an IPv4 or IPv6 command-line parameter. NOTE: It is unclear whether there are any common situations in which ntpq or ntpdc is used with a command line from an untrusted source. | | | | | | | | | | | | | |
| 7 | CVE-2018-8956 | 20 | | | 2020-05-06 | 2020-07-19 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | ntpd in ntp 4.2.8p10, 4.2.8p11, 4.2.8p12 and 4.2.8p13 allow remote attackers to prevent a broadcast client from synchronizing its clock with a broadcast NTP server via spoofed mode 3 and mode 5 packets. The attacker must either be a part of the same broadcast network or control a slave in that broadcast network that can capture certain required packets on the attacker's behalf and send them to the attacker. | | | | | | | | | | | | | |
| 8 | CVE-2018-7185 | | | DoS | 2018-03-06 | 2020-08-24 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | The protocol engine in ntp 4.2.6 before 4.2.8p11 allows a remote attackers to cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association. | | | | | | | | | | | | | |
| 9 | CVE-2018-7184 | | | DoS | 2018-03-06 | 2020-08-24 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | ntpd in ntp 4.2.8p4 before 4.2.8p11 drops bad packets before updating the "received" timestamp, which allows remote attackers to cause a denial of service (disruption) by sending a packet with a zero-origin timestamp causing the association to reset and setting the contents of the packet as the most recent timestamp. This issue is a result of an incomplete fix for CVE-2015-7704. | | | | | | | | | | | | | |
| 10 | CVE-2018-7183 | 787 | | Exec Code Overflow | 2018-03-08 | 2021-07-20 | 7.5 | None | Remote | Low | Not required | Partial | Partial | Partial |
| | Buffer overflow in the decodearr function in ntpq in ntp 4.2.8p6 through 4.2.8p10 allows remote attackers to execute arbitrary code by leveraging an ntpq query and sending a response with a crafted array. | | | | | | | | | | | | | |
| 11 | CVE-2018-7182 | 125 | | DoS | 2018-03-06 | 2019-10-31 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | The ctl_getitem method in ntpd in ntp-4.2.8p6 before 4.2.8p11 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mode 6 packet with a ntpd instance from 4.2.8p6 through 4.2.8p10. | | | | | | | | | | | | | |
| 12 | CVE-2018-7170 | | | | 2018-03-06 | 2020-06-18 | 3.5 | None | Remote | Medium | ??? | None | Partial | None |
| | ntpd in ntp 4.2.x before 4.2.8p7 and 4.3.x before 4.3.92 allows authenticated users that know the private symmetric key to create arbitrarily-many ephemeral associations in order to win the clock selection of ntpd and modify a victim's clock via a Sybil attack. This issue exists because of an incomplete fix for CVE-2016-1549. | | | | | | | | | | | | | |
| 13 | CVE-2017-6464 | 20 | | DoS | 2017-03-27 | 2018-04-12 | 4.0 | None | Remote | Low | ??? | None | None | Partial |

# E se os ataques forem bem sucedidos?

# Certificados TLS

- O TLS é usado para estabelecer conexões seguras e autenticadas na Internet
  - Se um ataque NTP conseguir fazer um cliente voltar no tempo, ele pode aceitar certificados fraudados. Por exemplo certificados emitidos antes de 2014 com a falha do heartbleed.

# DNSSEC

- O DNSSEC provê autenticação para o sistema de nomes.
  - Se um resolver está configurado pra fazer “strict validation”, ou seja, não responde se as queries falham a validação do DNSSEC, então um ataque NTP que leva o resolver para frente no tempo pode fazer com que todos os certificados e chaves expirem. Um ataque NTP que leve para o passado pode permitir ataques de repetição.

# Cache-flushing

- Muitos sistemas se baseiam em algum tipo de cache para minimizar a carga de processamento ou da rede. O DNS, por exemplo.
  - Um ataque NTP que leve o relógio do DNS para trás 24h fará com que a maior parte das entradas de cache expire. Se isso ocorrer de forma massiva, pode inundar a rede de requisições DNS.

# Roteamento na Internet

- O RPKI é uma infraestrutura para a segurança do BGP, usando ROAs para autenticar a alocação de endereços IP e ASN.
  - Um ataque NTP pode levar um validador de RPKI para frente no tempo, fazendo com que apague o cache do arquivo de manifesto. Depois voltar o validador no tempo, fazendo com que aceite um arquivo de manifesto antigo como válido.

# Bitcoin

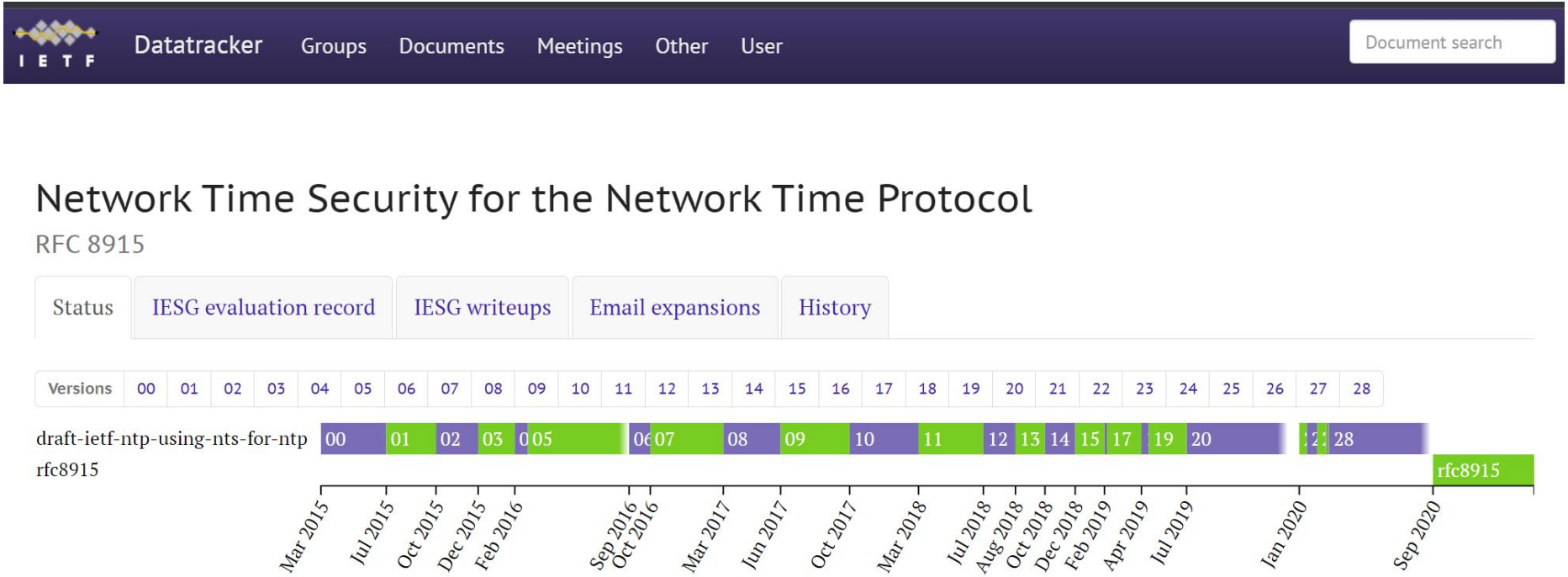
- Bitcoin é uma moeda digital que permite que uma rede descentralizada chegue a um consenso sobre a validade de uma cadeia pública de transações, a “blockchain”.
  - Um ataque NTP pode levar a vítima a rejeitar transações válidas, ou a gastar poder computacional processando transações antigas.

# Serviços de autenticação

- Muitos serviços, como o Amazon S3, o DropBox Core API, e outros, expõem APIs que requerem autenticação a cada nova requisição. Normalmente exigem registros de tempo como forma de evitar ataques de repetição.
  - Com o ataque NTP a um servidor de aplicação pode-se fazer uma negação de serviço ou ataques de repetição.

# NTS - Network Time Security

# NTS: A NOVA EXTENSÃO DE SEGURANÇA DO NTP



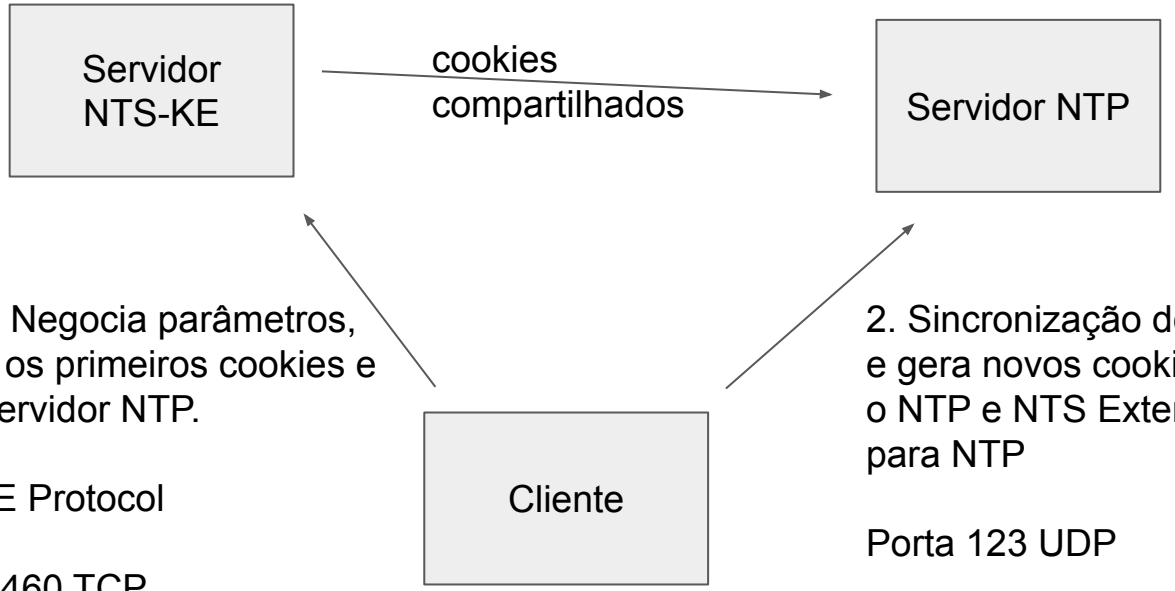
# NTS: A NOVA EXTENSÃO DE SEGURANÇA DO NTP

- O que é:
  - É um mecanismo para usar TLS para prover segurança criptográfica para o NTP no modo cliente/servidor.
- Dois componentes:
  - NTS-KE - Network Time Security Key Establishment
  - NTS Extension fields para o NTPv4

# NTS: A NOVA EXTENSÃO DE SEGURANÇA DO NTP

- **Identidade**: usa a estrutura de chaves públicas X.509
- **Autenticação**: verifica criptograficamente que a informação de relógio nos pacotes NTP é autêntica, produzida por um servidor identificável.
- **Proteção contra ataques de repetição**: o cliente pode detectar
- **Consistência entre requisições e respostas**: o cliente pode verificar
- **Privacidade**: NTS não vaza nenhuma informação que permitiria a um terceiro determinar que dois pacotes vindos de redes diferentes se originaram no mesmo cliente
- **Não amplificação**: as respostas nunca são maiores do que as requisições
- **Escalabilidade**: os servidores não guardam estado dos clientes, então podem servir a um grande número
- **Desempenho**: o NTS não degrada a qualidade da sincronização dos relógios

# NTS: A NOVA EXTENSÃO DE SEGURANÇA DO NTP




1. TLS. Negocia parâmetros, recebe os primeiros cookies e IP do servidor NTP.

NTS-KE Protocol

Porta 4460 TCP

2. Sincronização dos relógios e gera novos cookies usando o NTP e NTS Extension Fields para NTP

Porta 123 UDP

# NTS: A NOVA EXTENSÃO DE SEGURANÇA DO NTP

- **NTS-KE**
  - o cliente conecta na porta TCP 4460
  - cliente e servidor executam um handshake TLS
  - negociam alguns parâmetros de segurança extra
  - o servidor envia ao cliente alguns cookies, além do endereço IP e porta do servidor NTP para o qual os cookies são válidos
  - nessa altura a fase NTS-KE do protocolo acabou, idealmente o cliente nunca mais precisa se conectar no servidor NTS-KE

# NTS: A NOVA EXTENSÃO DE SEGURANÇA DO NTP

- **Sincronização com NTP e NTS**
  - o cliente envia ao servidor um pacote com vários campos de extensão, entre eles um cookie (dos que recebeu do servidor NTS-KE) e uma tag de autenticação
  - o servidor usa o cookie para recuperar a chave e envia uma resposta autenticada
  - a resposta inclui um cookie novo, criptografado
  - na próxima requisição o cliente enviará esse cookie, sem criptografia
  - essa constante renovação dos cookies garante a privacidade

# NTP.br

# O NTP.br e o NTS

- Estamos em fase de implementação e testes do NTS no NTP.br. Atualmente os servidores stratum 1 funcionam com NTS, em caráter experimental.
  - isso quer dizer que em caso de encontrar problemas sérios, podemos deixar de oferecer NTS até conseguir tratá-los
- {a, b, c, d, gps}.ntp.br
- o site https://ntp.br foi revisado e atualizado, e inclui agora também informação sobre o NTS e exemplos de configuração

# Utilizando o NTP e NTS

# Softwares para NTP e NTS recomendados

- **NTPsec (ntpsec.org)**
  - fork do NTPD (implementação de referência) feito em 2015
  - de 239 mil linhas de código, foram eliminadas 173 mil
  - hardening e modernização do código
  - ativamente mantido por um time experiente
  - NTS
- **Chrony (chrony.tuxfamily.org)**
  - implementação mais recente e moderna, de excelente qualidade
  - NTS
- OpenNTPd (openntpd.org)
  - implementação minimalista com foco em segurança (sem NTS)
- systemd-timesyncd
  - implementação minimalista incluída no systemd (sem NTS)

# Softwares para NTP e NTS

- NTPd (ntp.org)
  - implementação de referência
  - RECOMENDAMOS **NÃO USAR**

# Softwares para NTP e NTS

- Windows / Mac / equipamentos de rede
  - não usar como servidores
    - se não puder desabilitar a função servidor, bloquear no firewall do dispositivo
  - usar o cliente nativo
  - provavelmente em alguns dispositivos não haverá opção de suporte a NTS por um tempo ainda

**#apt-get install ntpsec**

substituir as diretivas poll do arquivo de configuração em /etc/ntpsec/ntp.conf por:

```
server a.st1.ntp.br iburst nts
server b.st1.ntp.br iburst nts
server c.st1.ntp.br iburst nts
server d.st1.ntp.br iburst nts
```

reiniciar o serviço

**#/etc/init.d/ntpsec restart**

verificar o funcionamento e a sincronização

**#ntpq -p**

```
root@debian:/home/moreiras# ntpq -p
     remote                                refid      st t when poll reach   delay   offset   jitter
==============================================================================================================
+a.st1.ntp.br                              .ONBR.          1 8    2   64    3  12.6769  -0.6477   1.7892
 b.st1.ntp.br                              .NTS.          16 u    -  68m    0   0.0000   0.0000   0.0001
+c.st1.ntp.br                              .ONBR.          1 8   52   64    1  29.4421   3.8805   5.2145
*d.st1.ntp.br                              .ONBR.          1 8   53   64    1  20.9121  -1.4399   2.0345
```

**#apt-get install chrony**

substituir a diretiva poll do arquivo de configuração em /etc/chrony/chrony.conf por:

```
server a.st1.ntp.br iburst nts
server b.st1.ntp.br iburst nts
server c.st1.ntp.br iburst nts
server d.st1.ntp.br iburst nts
```

reiniciar o serviço

**#/etc/init.d/chrony restart**

verificar
o funcionamento
e a
sincronização

```
root@debian:/home/moreiras# chronyc sources
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^- a.st1.ntp.br                  1   6    17     1  -1755us[-1755us] +/- 7860us
^? b.st1.ntp.br                  0   7     0     -     +0ns[   +0ns] +/-    0ns
^- c.st1.ntp.br                  1   6    17     1  -3994us[-3994us] +/-   14ms
^* d.st1.ntp.br                  1   6    17     1  +4990us[+4962us] +/-   16ms
root@debian:/home/moreiras# chronyc tracking
Reference ID    : C814BA4C (d.st1.ntp.br)
Stratum         : 2
Ref time (UTC)  : Wed Sep 29 06:38:07 2021
System time     : 0.000026991 seconds slow of NTP time
Last offset     : -0.000027520 seconds
RMS offset      : 0.000027520 seconds
Frequency       : 2.720 ppm slow
Residual freq   : +327.395 ppm
Skew            : 1000000.000 ppm
Root delay      : 0.032182854 seconds
Root dispersion : 11.995963097 seconds
Update interval : 1.4 seconds
Leap status     : Normal
```

# verificar o funcionamento e a sincronização

```
root@debian:/home/moreiras# chronyc -N authdata
Name/IP address             Mode KeyID Type KLen Last Atmp  NAK Cook CLen
==============================================================================
a.st1.ntp.br                 NTS     1   15  256  33m    0    0    8  104
b.st1.ntp.br                 NTS     0    0    0    -     3    0    0    0
c.st1.ntp.br                 NTS     1   15  256  33m    0    0    8  100
d.st1.ntp.br                 NTS     1   15  256  33m    0    0    8  100
```

# Servidor NTP e NTS

**Instalação do Certbot (Letsencrypt)**

```
apt install ca-certificates certbot
certbot register --agree-tos --email seu-email@seudominio.com.br --no-eff-email
certbot certonly --standalone --preferred-chain "ISRG Root X1" --domain seu-servidor-ntp.com.br
cp -L -v /etc/letsencrypt/live/seu-servidor-ntp.com.br/fullchain.pem /etc/ntpsec/cert-chain.pem
cp -L -v /etc/letsencrypt/live/seu-servidor-ntp.com.br/privkey.pem /etc/ntpsec/key.pem
chown -R -v ntpsec: /etc/ntpsec
```

**Firewall**

```
ufw allow 123/udp comment 'NTP'
ufw allow 4460/tcp comment 'NTS-KE'
ufw allow 80/tcp comment 'HTTP'
```

**Configuração do NTP e NTS**

```
driftfile /var/lib/ntpsec/ntp.drift
leapfile /usr/share/zoneinfo/leap-seconds.list

nts cert /etc/ntpsec/cert-chain.pem
nts key /etc/ntpsec/key.pem
nts enable

statsdir /var/log/ntpsec/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

tos maxclock 11
server a.st1.ntp.br minpoll 4 maxpoll 6 nts
server b.st1.ntp.br minpoll 4 maxpoll 6 nts
server c.st1.ntp.br minpoll 4 maxpoll 6 nts
server d.st1.ntp.br minpoll 4 maxpoll 6 nts

restrict 1.1.0.0/20 kod limited nomodify noquery  #(sua rede)
restrict 2001:0db8::/32 kod limited nomodify noquery  #(sua rede)

restrict 127.0.0.1
restrict ::1
```

**Instalação do Certbot (Letsencrypt)**

```
apt install ca-certificates certbot
certbot register --agree-tos --email seu-email@seudominio.com.br --no-eff-email
certbot certonly --standalone --preferred-chain "ISRG Root X1" --domain seu-servidor-ntp.com.br
cp -L -v /etc/letsencrypt/live/seu-servidor-ntp.com.br/fullchain.pem /etc/chrony/cert-chain.pem
cp -L -v /etc/letsencrypt/live/seu-servidor-ntp.com.br/privkey.pem /etc/chrony/key.pem
chown -R -v chrony: /etc/chrony
```

**Firewall**

```
ufw allow 123/udp comment 'NTP'
ufw allow 4460/tcp comment 'NTS-KE'
ufw allow 80/tcp comment 'HTTP'
```

**Configuração do NTP e NTS**

```
allow 2001:db8::/32
allow 6.7.8.9/22 #sua rede
driftfile /var/lib/chrony/chrony.drift
keyfile /etc/chrony/chrony.keys
leapsectz right/UTC
log measurements statistics tracking rtc refclocks tempcomp
logdir /var/log/chrony
makestep 1 3
maxntsconnections 1024
maxupdateskew 100.0
ntsdumpdir /var/lib/chrony
ntsprocesses 4
ntsservercert /etc/chrony/cert-chain.pem
ntsserverkey /etc/chrony/key.pem
rtcsync
server a.st1.ntp.br iburst nts
server b.st1.ntp.br iburst nts
server c.st1.ntp.br iburst nts
server d.st1.ntp.br iburst nts
```

# Obrigado!

**Antonio Marcos Moreiras**
moreiras@nic.br
@moreiras na maior parte das redes sociais
https://www.linkedin.com/in/moreiras/