



It's About Time

Introduction

- ✓ *Who am I?*
- ✓ *What will we discuss?*
- ✓ *What's the objective?*

The Importance of Time

- ✓ *Regulatory Example: PCI DSS*
- ✓ *Legal Defensibility & Evidence*
- ✓ *Incident Investigations*

The Problem with NTP

- ✓ *Caveat: Not a Sales Pitch*
- ✓ *Who's Your Time Source?*
- ✓ *Certichron - CertifiedTime.com*



10.4 Synchronize all critical system clocks and times.

10.4 Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:

10.4.a Verify that a known, stable version of NTP (Network Time Protocol) or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2, is used for time synchronization.

10.4.b Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]

10.4.c Verify that specific external hosts are designated from which the timeservers will accept NTP time updates (to prevent a malicious individual from changing the clock).

Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers).

See www.ntp.org for more information

```
purseute:~ falcon$ nslookup pool.ntp.org
```

```
Server:      192.168.1.1  
Address:     192.168.1.1#53
```

```
Non-authoritative answer:
```

```
Name:  pool.ntp.org  
Address: 207.150.167.80  
Name:  pool.ntp.org  
Address: 169.229.70.64  
Name:  pool.ntp.org  
Address: 208.75.88.4  
Name:  pool.ntp.org  
Address: 198.186.191.229  
Name:  pool.ntp.org  
Address: 64.6.144.6
```

```
purseute:~ falcon$ nslookup 207.150.167.80
```

```
Server:      192.168.1.1  
Address:     192.168.1.1#53
```

```
Non-authoritative answer:
```

```
80.167.150.207.in-addr.arpa  name = nonce.prolixium.com.
```

```
Authoritative answers can be found from:
```

```
purseute:~ falcon$ nslookup 169.229.70.64
```

```
Server:      192.168.1.1  
Address:     192.168.1.1#53
```

```
Non-authoritative answer:
```

```
64.70.229.169.in-addr.arpa  name = ntp2.Housing.Berkeley.EDU.
```

```
Authoritative answers can be found from:
```

```
purseute:~ falcon$ nslookup 208.75.88.4
```

```
Server:      192.168.1.1  
Address:     192.168.1.1#53
```

```
Non-authoritative answer:
```

```
4.88.75.208.in-addr.arpa  name = clock.trit.net.
```

```
Authoritative answers can be found from:
```

```
purseute:~ falcon$ nslookup 198.186.191.229
```

```
Server:      192.168.1.1  
Address:     192.168.1.1#53
```

```
** server can't find 229.191.186.198.in-addr.arpa: SERVFAIL
```

```
purseute:~ falcon$ nslookup 64.6.144.6
```

```
Server:      192.168.1.1  
Address:     192.168.1.1#53
```

```
Non-authoritative answer:
```

```
6.144.6.64.in-addr.arpa name = triangle.kansas.net.
```

```
Authoritative answers can be found from:
```

