The importance of Time Synchronisation in Information Security

By James Read

Introduction

Nearly all IT systems keep the time and have done since 1982.

“Information Security” often relies on accurately keeping the time for a variety of reasons.

- Quality of security
- Audit Trails
- Transaction based systems

Examples 1

- Distributed Systems
  - DFS's depend upon a synchronized clock to track changes to files.
  - For process scheduling.
  - Transaction accuracy.
- Legitimate System Use / Hackers
  - Accurate time keeping leads to an accurate audit trail.
  - Being able to follow the trail of a hacker will certainly lead to easier protection.

Examples 2

Scheduled tasks and transaction accuracy

Most budget motherboard system clocks are set by hand / generalized by machine.

Most of them use cheap oscillator chips, which are not as accurate as you would think.

- It's estimated, that most retail desktop machine, system clocks drift by up to 2 seconds/day.
- IBM compatible system clocks often return the time to the nearest 1 second.

Heavyweight IBM servers, running Z/OS, are capable of accuracy up to 244 pico seconds!

Examples 3

What are the issues?

In distributed computing, as well as clusters, changing the time of the node becomes extremely risky and complex.

Inaccurate system clocks have are likely to have knock-on effects.

A clock that is hacked to drift, can easily allow hackers into networks.

Inaccurate times can break cryptography.

Keeping time synchronized

Public external time server using NTP

Specialized external time server

Internal time server

Dedicated and specialized local time hardware

Specialized hardware on a machine basis, kept synchronized by alternative methods.

- GPS
- CDMA

Risk Analysis

Look at the a potential problems that lack of time synchronization could cause.

eg: Transaction accuracy

Analyse each problem as part of a risk analysis.

eg: Could cause horrendous concurrency errors

Put steps into place to prevent these problems before they occur

Conclusion

A risk analysis is required in any computer network that requires time synchronization.

Prevention, in mission critical systems is always better than cure.

The level of “**synchronization system**” required should be relative to the potential problems that a lack of synchronisation could cause .

End of Presentation

Thank you for listening.

I welcome any questions you may have.