Time Synchronization Attack – Pulse Delay Attack

Introduction

Time Synchronization is extremely important in today's systems. Everything from managing, securing, planning, and debugging a network involves knowing when precisely events happened. Accurately correlate log files between devices on your network becomes very difficult or impossible to do without precise time synchronization. Without proper time stamps tracking security breaches, network usage, or problems with components in your network becomes nearly impossible. If an attacker were to penetrate the system and log into many different devices, modify files, or download files, linking these events together or mapping out the scope of the attack would be near impossible. Crypto systems are also often reliant on the correct time, and without proper synchronization could be left vulnerable to attacks. [2]

Sensor networks are specifically reliant on time synchronization. It is critical that that these networks work with precise time to capture and produce sensitive data. These data are often measuring the time-of-flight of sound, distributing an acoustic beam forming array, forming a low-power TDMA radio schedule, suppressing redundant messages, integrating multisensory data, or coordinating future access to name a few. [1]

The massive importance of time synchronization in sensor networks makes it a valuable target to malicious actors. Such an actor could cause significant financial, physical, or intellectual damage by affecting functionality of the systems and applications that rely on time synchronization. Attackers could create faulty estimates about locations, cause DoS due to interruption of sleep-wake cycles, create unreliable data collection, cover their tracks on a security breach, or allow them to trivially perform replay attacks in security protocols that use time stamping. [1]

The Attack

The pulse-delay attack is a very challenging attack to detect. This attack is a man in the middle attack that incorporates the delay of time synchronization pulses being sent from one node to another in a network (often a sensor network). The attack relies on abusing the time synchronization protocol (pairwise sender-receiver synchronization), between nodes A and B. T1 and T4 represent the times measured by the local clock in A and T2 and T3 are the local clock times in B. Using the information, A can calculate and subsequently synchronize its clock to B's clock ($C_A = C_A + \delta$):

Pairwise Sender-receiver Synchronization

1. A$(T1) \rightarrow (T2)$B: $A, B, sync$
2. B$(T3) \rightarrow (T4)$A: $B, A, T2, T3, ack$
3. A calculates offset $\delta = \frac{(T2-T1)-(T4-T3)}{2}$

If the attacker delays the time at which B receives the synchronization pulse, it will have effectively modified the computation of the offset at A and the system time calibration will be incorrect. This is done by jamming the initial pulse and replaying it at some time in the future. The attacker can arbitrarily change the computed clock off-set by varying the delay. It is also important to note the delay will similarly change the computed end-to-end delay. [1]

References

1. Ganeriwal, S., Popper, C., Capkun, S., and Srivastava, M. B. 2008. Secure time synchronization in sensor networks. ACM Trans. Inf. Syst. Secur. 11, 4, Article 23 (July 2008), 35 pages. DOI = 10.1145/1380564.1380571. http://doi.acm.org/10.1145/1380564.1380571.

2. "Network Time Synchronization." *Importance of Time Synchronization for Your Network*. N.p., n.d. Web. 13 Nov. 2016.