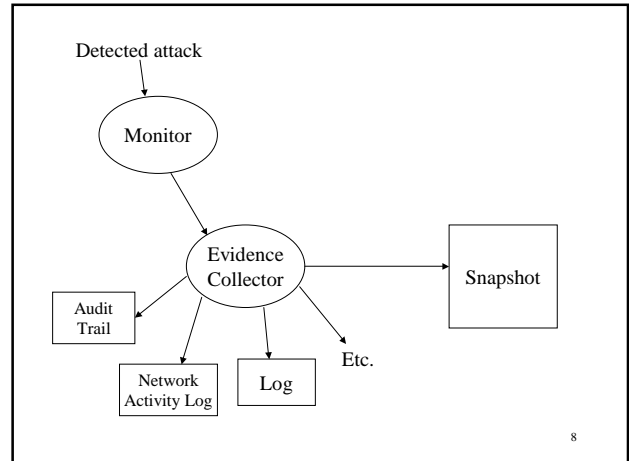


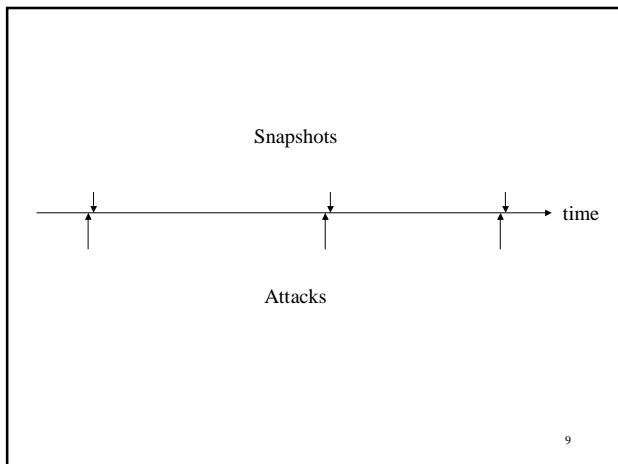
New Idea

- Instead of using IDS, keep a record/log of known attacks or abnormal behavior
 - High volume of transactions
 - Etc.
- Have a monitor watch the activity in the database system
- When an attack is detected, take a snapshot by collecting evidence

7

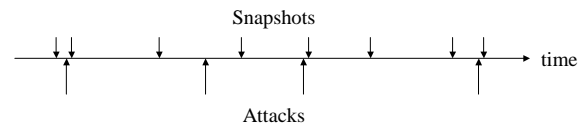


8



9

What if an attack isn't detected??



- Need to take snapshots at times other than right after an attack is detected

10

When to Take a Snapshot

- When an attack is detected
- After x number of transactions
- After every y time
- After every user login/logout
- Etc.

- Still thinking about this...

11

Where To Collect Evidence From

- Audit trail – a log of all changes to the database [SIL02, p241]
 - Inserts/deletes/updates
 - Which user performed update
 - When the update was performed
 - Outputted to stable storage [SIL02, p644, implementation on p641]
- Log – records database modifications [SIL02, p645]
 - Transaction identifier
 - Data-item identifier
 - Old value
 - New value
 - Etc.

12

- Network activity log [YAS01, p291]
 - Data packets that flow through routers and servers
 - TCP/IP packets contain info about source and target
 - Etc.
- Etc.

- Still researching...

13

References

- [CAS95] Castano, Silvana, et al. *Database Security*. ACM Press, 1995.
- [PFL97] Pfleeger, Charles P. *Security in Computing*. 2nd edition. Prentice Hall PTR, 1997.
- [SIL02] Silberschatz, Abraham, Henry F. Korth, and S. Sudarshan. *Database System Concepts*. 4th edition. McGraw Hill, 2002.
- [YAS01] Yasinsac, Alec and Yanet Manzano. "Policies to Enhance Computer and Network Forensics." *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, NY. June 5-6, 2001.

14