

Why Anomaly Based Intrusion Detection Systems are a Hax0rs Best Friend

By David Maynor
GT Information Security

David.Maynor@oit.gatech.edu

The history of the castle.

- What is a Anomaly based IDS and how does it differ from Signature based systems?
 - a. Signature based systems rely on static analysis of event.
 - b. Anomaly systems rely on creating a baseline of normal activity then flag any deviations.
- History
 - a. Where they come from.
 - b. What drives their development.

How the castle is built.

- How anomaly based systems work.
 - a. A baseline is normally gathered during a tuning phase. Gather all traffic, analyze it, store it.
 - b. Data mining process that does statistical analysis of data.
- Theory behind them.
 - a. If its traffic that hasn't been seen before, its bad.
 - b. Attacks cause things the system has not seen before.

How the castle is built. (cont.)

- Can science brewed in research labs work in the wild?
 - a. Eggheads can build rockets, but can they build security products?
 - b. Crackers excel at creating attacks that bypass security models, why is traffic analysis any different?
- Hardware based considerations.
 - a. What kind of hardware is required to make this a effective scalable solution?
 - b. Type of information that would have to be stored leads to huge hardware requirements.
 - c. Speed.
 - sniffing
 - analysis

The castle was built on a shaky foundation.

- Problems.
 - a. Unwieldy size.
 - b. Hardware limitations.
 - c. Integration of network changes.
- Things anomaly based systems assume.
 - a. If it hasn't been seen before, its bad.
 - b. Machines have normal patterns that can be easily distinguished.
 - c. Networks don't change.
 - This is somewhat of a half-truth.

The castle was built on a shaky foundation. (cont.)

- Why it is so hard to tell good traffic from bad traffic?
 - a. Anomaly based systems rarely look at the payload.
 - b. If network runs in a nonstandard configuration there are problems.
 - c. Attacks against commonly used services on the machines are ignored.
 - Web server attacks against public web servers go unnoticed.
- Configuration problems.

How to tear the castle down.

- More noise, less accuracy.
 - a. Single outside point to multiple inside machines.
 - b. Properly crafted packets will cause inside machines to appear as attackers.
- Covert channels.
 - a. Hiding the data in plain site.
 - b. How useful is this?
- Flooding.
 - a. Several outside sources to a single inside source.
 - b. Not very effective, but useful for quick and dirty.

How to tear the castle down. (cont.)

- Breaking traffic analysis.
 - a. Teaching a old dog new tricks.
 - b. Recon of target
 - c. When in Rome...
- Flaws in the System
 - a. Attacks against the system itself.
 - b. Attacks against what feeds the system.

Is there any way to fix the walls?

- Can weak science be fixed?
- Are these problems/holes fixable?

Looking back.

- Is it useful?
- Who do they keep out?
- How can they be better?
- What does this all mean for your standard system cracker?