Leave the Theory Behind and Embrace the Code

A Practical Approach to Building a Security Data Correlation System

David Maynor
What Problems will this Solve?

• Information Overload
  – Too much information, too many devices

• False Positives
  – Alerts for IIS attacks on Linux machines with no web servers

• Time
  – Cycle of life for forensics of attacks
Why Write it Yourself?

- Vendors that do this
  - Price
- Approaches
  - Large, small, data mining
- Customization to your environment
  - Nobody knows how your network functions better than you
Before We Get Started…

- Clear goals of what we want to accomplish
  - Simple, practical
- High Tech vs. Low Tech
- Data
  - What do we need to accomplish our task?
  - How long to store it?
  - Are you violating any policy?
- Pitfalls
  - Feature creep
  - Complexity
Architecture

• Different models
  – Three tier
  – Client-server
  – Distributed

• Pros/Cons

• Model we will use and why (Three Tier)
Design

- Design considerations
  - Languages
    - Things to consider
  - Storage
    - Data retention
  - Traffic
    - Data reduction
    - Bottlenecks
  - Interoperability
    - Third party tools
Design (cont.)

- Communication
  - Data from point a to point b
  - Normalization
    - Xml
    - Custom
  - Reduction
Design (cont.)

- Sensors
  - What will be used?
  - Effective placement
  - What will be important to the overall design?
  - Active sensors vs. Passive sensors
Engine

- What it does.
- Keep it simple.
- Feature creep
- Heart of the program: main resolve loop
  - Step-by-step
  - Data
  - Logic
    - How engine actually works
  - Eliminating false positives
- Concerns
  - Bottleneck
  - Extendibility
Sensors

• Sensor goals
• Simple design
  – Choice between fat/thin client
  – Data reduction at the client level
• Types of sensor needed to make the system effective
  – Vuln scanner
  – IDS
  – System integrity checker
• Sensor security
Problems

• You are only as good as your tools
  – Updates
• Attacks against your system
  – Secure communication
  – Authorization
• Maintenance