

FUTURE DIRECTIONS IN INTRUSION DETECTION

E. Eugene Schultz, Ph.D., CISM, CISSP
Chief Technology Officer
High Tower Software
gschultz@high-tower.com
+1 (949) 330-3080 ext. 208

Interop
Las Vegas, Nevada
May 22, 2007

Copying these materials without the explicit, written permission of High Tower Software is prohibited.



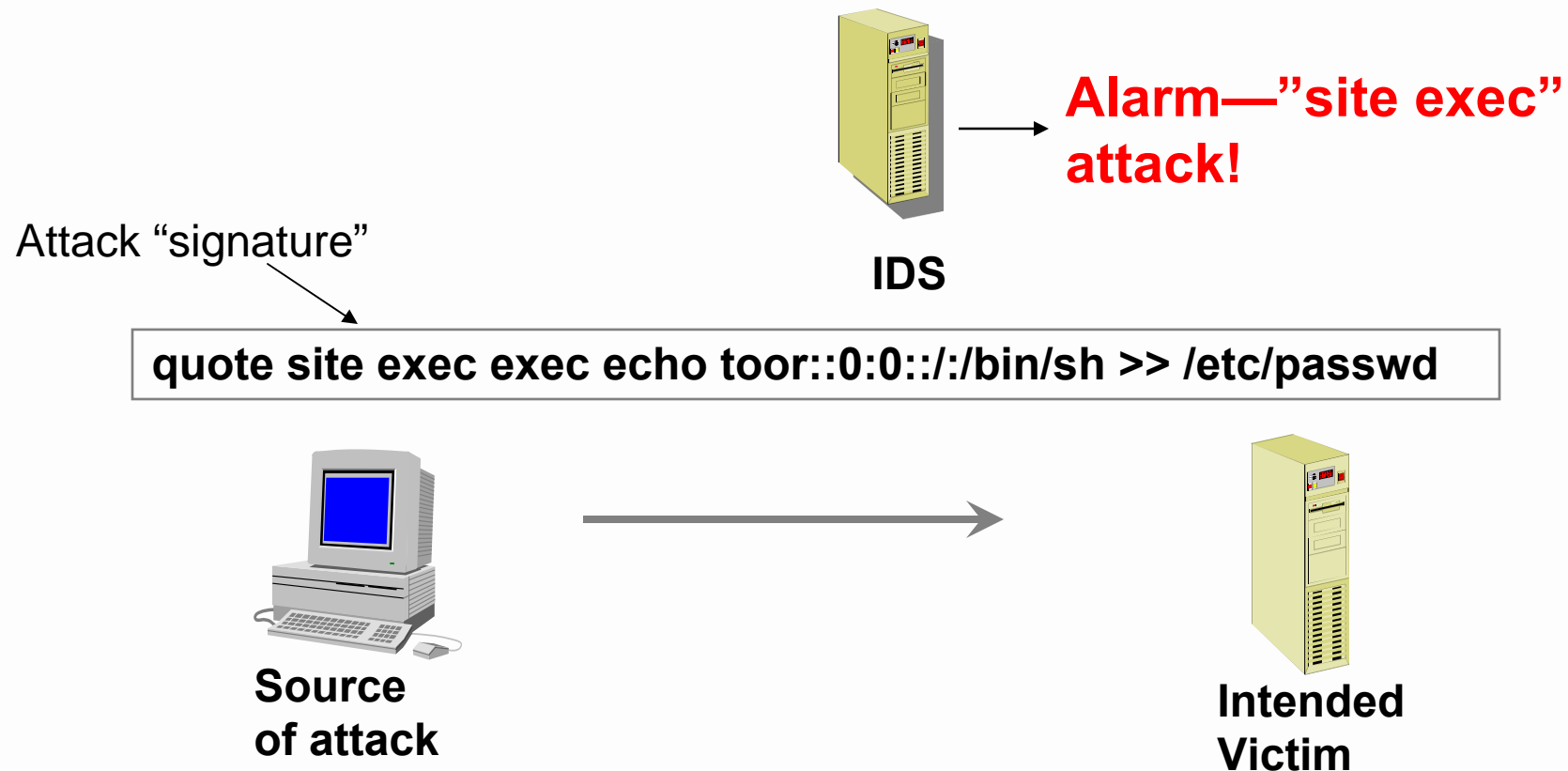
- **Intrusion detection has grown from an obscure to a much more established technology within information security**
- **New developments and directions in intrusion detection promise to push intrusion detection further ahead**
- **This presentation covers these developments and directions**

Does intrusion detection itself have a future?

- **Gartner has said “no”**
 - Claims there is too low return on investment (ROI)
 - Points out that false alarms and misses are too prevalent
 - Predicts that intrusion prevention will supplant intrusion detection
- **Gartner has recommended that IT organizations instead spend money on firewalls, not IDSs**
- **Problem for Gartner—sales of intrusion detection products have increased substantially every quarter since Gartner prediction!**



How most intrusion detection systems (IDSs) work



About current intrusion detection methods

- **Traditional intrusion detection methods (signature-based methods like Snort) have never really turned out to be that good of a way to find intruders' activity**
- **Almost overwhelming hurdles have surfaced**
 - The proliferation and increasing sophistication of IDS evasion and attack obfuscation methods
 - The complexity of Web services
 - Increased use of encryption and reverse shells using standard protocols like DNS, HTTP and SMTP
 - Sophisticated rootkits
- **SO—traditional intrusion detection is fading out—is being replaced by**
 - A combination of intelligence collection and thorough system and network forensics analysis methods
 - Sophisticated data fusion/event correlation methods

Possible clues from NextGenIDSForum

- **Perlovsky, L., Concurrent learning and fusion.**
- **Bomberger, N., Waxman, A., Rhodes, B. & Sheldon, N., A new approach to higher-level information fusion using associative learning in semantic networks of spiking neurons.**
- **Ravichandran, B., Gandhe, A., Smith, R. & Raman, M., Robust automatic target recognition using learning classifier systems.**
- **Zhu, Q., Aldridge, S., & Resha, T., Hierarchical Collective Agent Network (HCAN) for efficient fusion and management of multiple networked sensors.**

Possible clues from NextGenIDSForum

- **Mohan, C., Mehrotra, K., Varshney, P., & Yang, J., Temporal uncertainty reasoning networks for evidence fusion with applications to object detection and tracking.**
- **Rhodes, B., Taxonomic knowledge structure discovery from imagery-based data using the neural associative incremental learning (NAIL) algorithm.**
- **Deming, R. & Perlovsky, L., Concurrent multi-target localization, data association, and navigation for a swarm of flying sensors.**

Continued from previous slide



About current intrusion detection research

- **Some of the promising intrusion detection research within the last few years includes**
 - Intrusion detection event correlation/event fusion
 - Network attack detection based on protocol analysis
 - Honeypots and honeyclients
 - Insider attack detection
 - Attack modeling
 - Others
- **Problem: too much intrusion detection research still focuses on intrusion detection signatures**

- **Takes multiple isolated security events, combining them into a single relevant security incident using correlation rules (and sometimes also statistical models)**
- **Requires comparative observations based on multiple parameters such as:**
 - **Source/destination IP addresses**
 - **Identifiable network routes**
 - **Type of attack**
 - **Type of malware installed on compromised systems**
 - **The time the activity began or ended**
 - **Others**

- **Based on traffic that is**
 - Inbound
 - Outbound
 - Internal
- **Correlation rules identify attacks that would otherwise be overlooked**
 - Focus on attack models
 - Incorporate logic on a series of related events:
 - $A \rightarrow B \rightarrow C = \text{Attack}$

Continued from previous slide



Event correlation will continually improve over time

- **Future event correlation capabilities are likely to grow in ability to**
 - Distinguish parameters of interest (hit rate, range of events detected, and so on) from noise
 - Distinguish between different indicators in space and time
 - Track and capture each desired kind of event and data
 - Ensure that each measured variable really represents the desired kinds of event categories
- **User interfaces for data correlation are also likely to continue to improve**

Alert fusion will also be a critical piece of intrusion detection

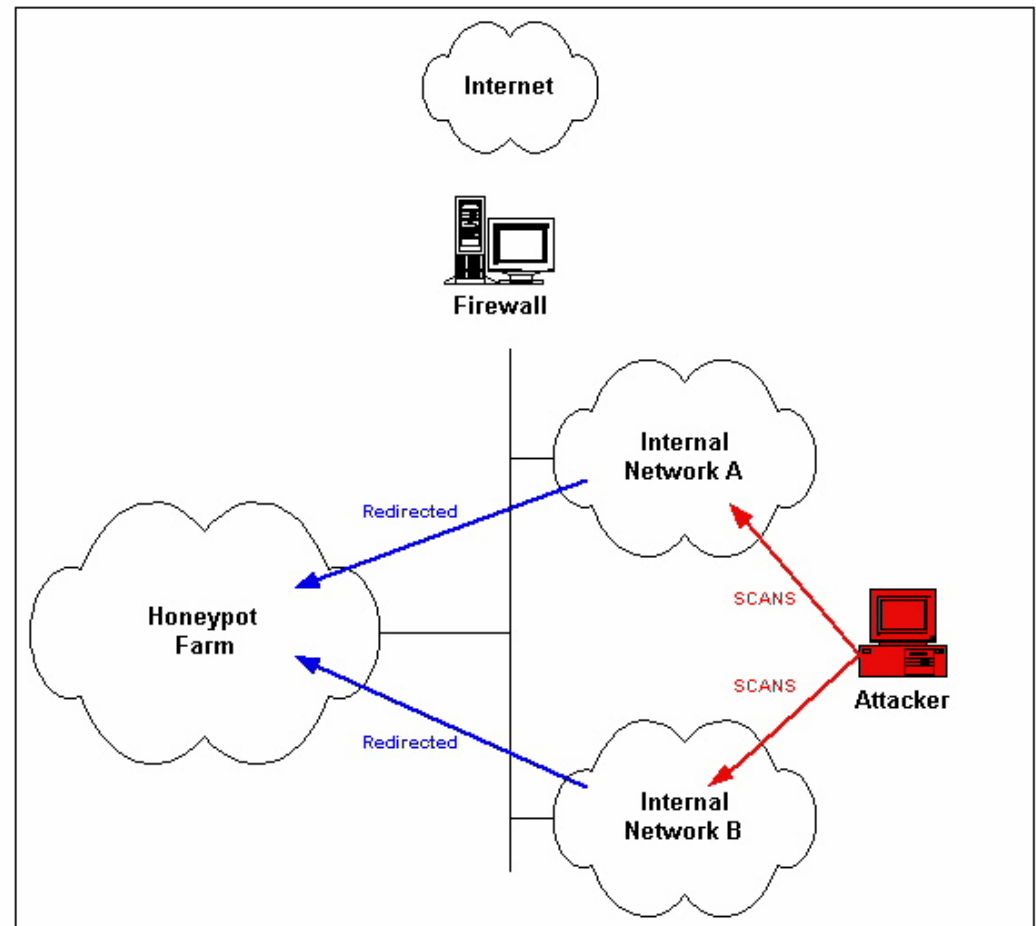
- **Numerous researchers have developed models of correlating intrusion detection data to fuse alerts**
 - **A single alert rather than multiple ones is sent if very similar intrusion detection-related events have occurred**
 - **Based upon features associated with events related to incidents weighted by values based on expectation of similarity**
 - **To trigger a fused alert, these features must reach a minimum criterion for similarity, such as when the same ports are being targeted in different observations**
- **Goal—reducing redundant alerts, keeping intrusion detection analysts from becoming overwhelmed**
- **Alert fusion in IDSs and IPSs will become commonplace**

Network attack detection using protocol analysis will get better

- **A wide range of attacks (particularly denial of service attacks) can currently be identified through anomalous protocol behavior**
 - Often based on behavioral profiles that incorporate significant communication patterns in network traffic
- **Has proven especially useful in early identification of**
 - Denial of service attacks
 - Botnets
- **Protocol analysis offers several significant advantages**
 - Parsimony/simplicity
 - Protocol behavior is very conducive to modeling
 - Is conducive to “zero day discovery”

Greater use of honeypots and honeyclients

- **Honeypots are decoy servers**
 - Allow intrusion detection (and also intrusion prevention) to occur in a safer environment (normally a virtual environment)
 - Allow
 - Early identification of new attack patterns
 - Determination of the relative frequency of each type of attack detected
 - Determination of the origin and routes of attacks



Picture for honeypot originally shown at <http://www.securityfocus.com/ids/images/farm.jpg>

Greater use of honeypots and honeyclients

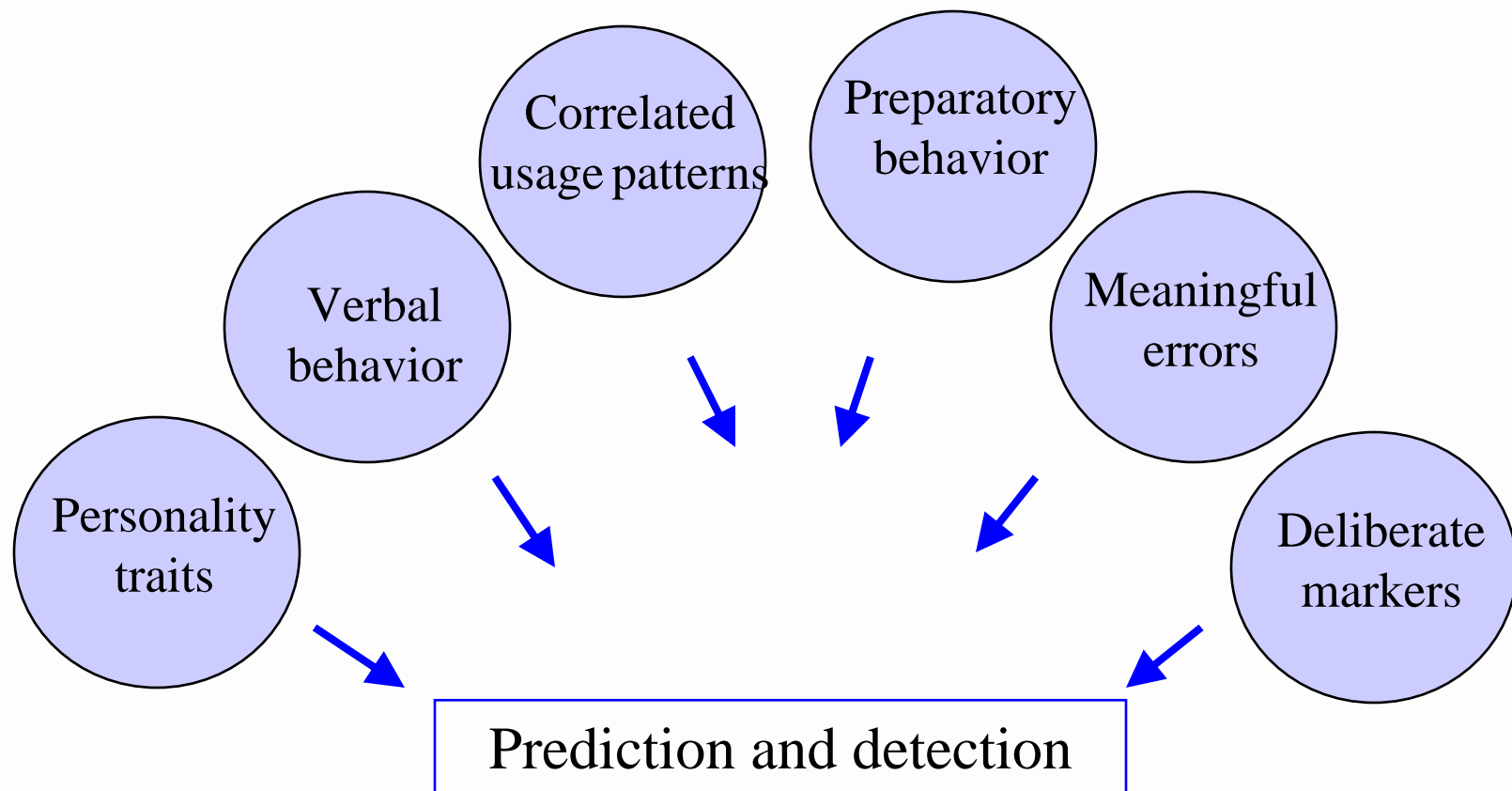
- **Honeyclients are honeypots that emulate the behaviors of clients**
 - **Are programmed to cause client applications to connect to servers**
 - **Can be used in connection with just about any client-server protocol**
 - **Proactively identify client-side exploits**
 - **Find malicious servers (especially Web servers)**
 - **Are not plagued by false alarms—every change made to a honeyclient are unauthorized**
 - **Facilitate discovery of zero-day attacks against clients**

Continued from previous slide

Insider attack detection proficiency will grow

- **Insider attack models have slowly but surely been improving**
 - Based mainly on behavioral profiles for users
 - Greater availability of information about insider incidents has helped considerably
- **A greater number of attack models covering a growing number of insider attack scenarios have been developed**
- **Predictive validity has also grown**

Insider attack detection proficiency will grow



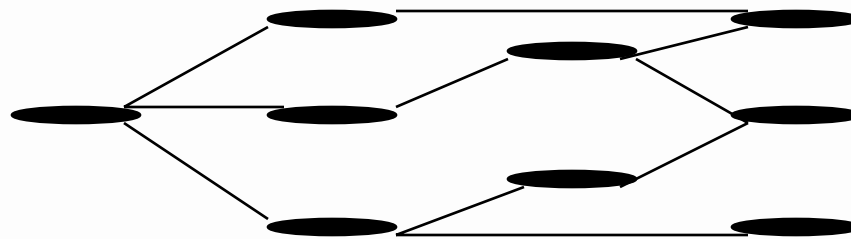
Continued from previous slide

Attack modeling will continue to improve

- **Attack models are representations of the essential components of attacks**
 - **Must include features that are observable and measurable**
 - **Most commonly included features include**
 - **System component targeted**
 - **Means of attack**
 - **Consequences of attack**
 - **Location and identity (and sometimes proficiency) of attacker**
 - **Offer greater flexibility in accommodating the many variations of attacks that may occur**
 - **Attack classifications and taxonomies are losing favor**
- **Increased emphasis on what happens at the *application* layer**

Neural and learning networks will be used increasingly

- Approach can be applied to a wide range of pattern recognition problems
- In intrusion detection no signatures or even rules are needed

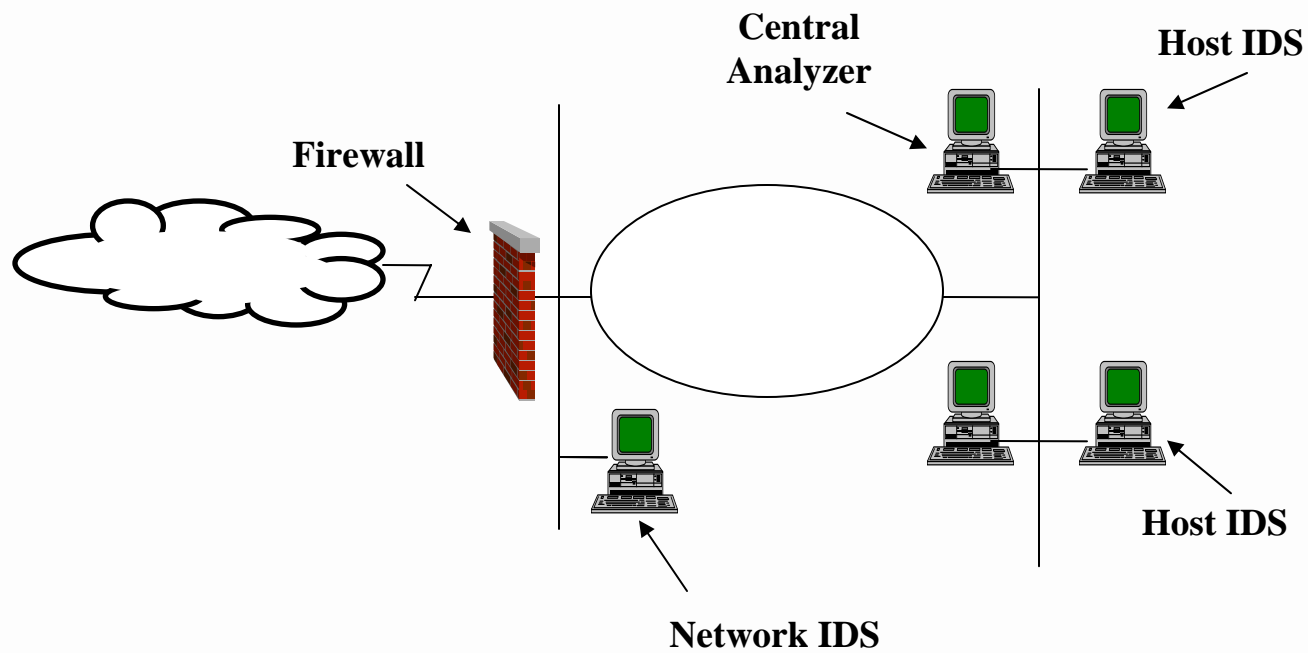




Intrusion prevention systems (IPSs) will become more sophisticated

- **IPSs are likely to incorporate “active defense” mechanisms**
 - Local data collection, analysis and blocking
 - Remote collection of external and internal data
 - Remote data correlation
 - More sophisticated attack suppression
- **IPSs are likely to be built directly into**
 - Operating systems
 - Applications

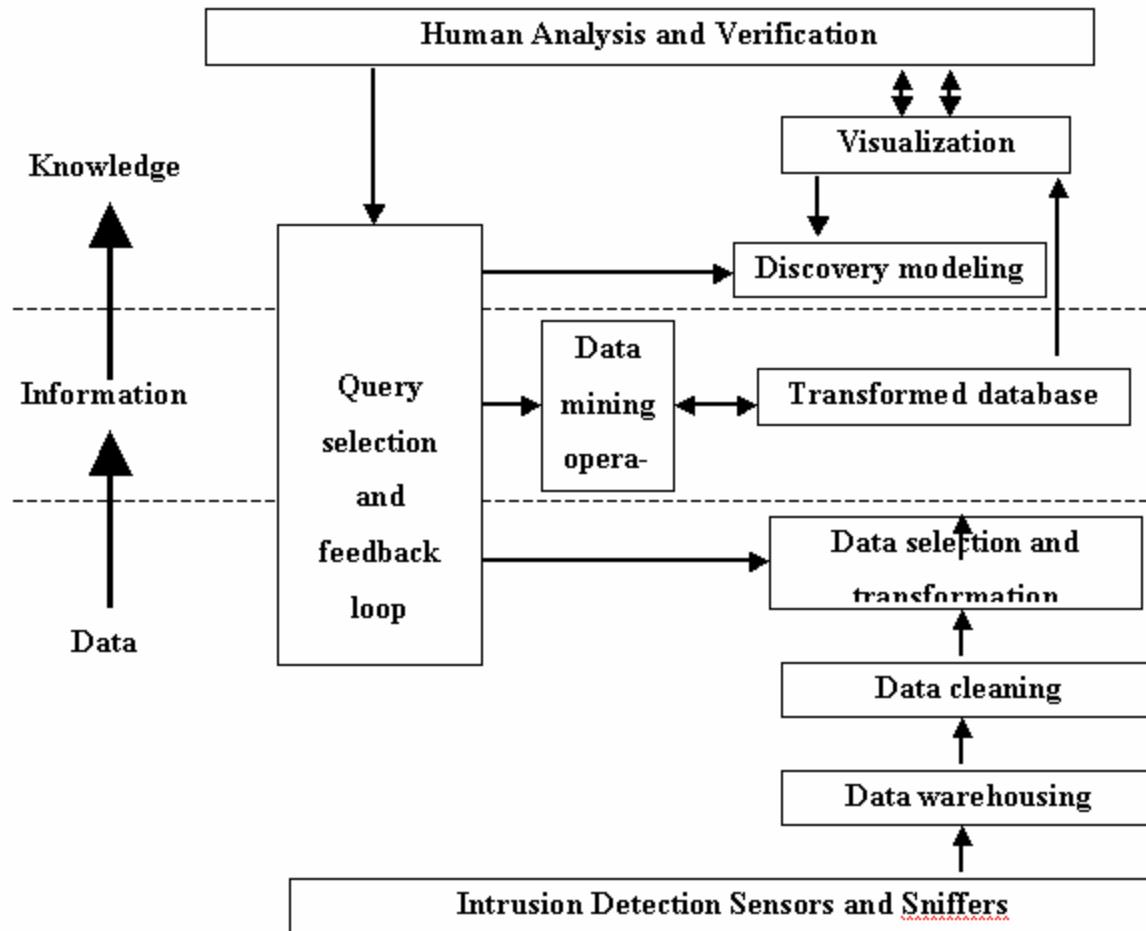
A possible future active defense architecture



Data mining in intrusion detection— an area with potentially huge growth

- **A current limitation in correlating events is the amount of data that can be stored in memory**
 - More or less limits analysis to current and very recent events
 - Memory full conditions are potentially catastrophic
- **Data mining provides a potentially very powerful solution**
 - Circumvents memory limitations
 - Provides a more complete analysis (because you can query for events that happened weeks, months, or even years ago)

A possible data correlation engine of the future



Improved source determination

- **IPv6 will be used more widely**
- **Source determination methods that are currently experimental will become mainstream (see next slides)**

New (experimental) types of tracing methods

- **Packet path determination**
 - Software records route within IP packets themselves
 - Limit: 9 addresses (so far)
 - Allows investigators to follow an active stream back through the network
 - Example: DOS Tracker (tool that logs into routers, locating the next hop back towards source of stream while stream is active)
- **Center Track**
 - Allows investigators to see where (e.g., from which particular router) traffic is coming from
 - Works best when there are few routers

New (experimental) types of tracing methods

- **ID and Isolation Protocol (IDIP)**
 - Experimental protocol
 - Keeps count of packets at each router interface
 - For an unusual stream it is possible to trace back to the source by following router information
 - Limited effectiveness (so far, at least)
- **Stream Thumbprinting**
 - You place network monitors at various points
 - Maintain a running checksum for a given stream at any point
 - Problem: intruders can tamper with any stream

Continued from previous slide

- **The future of intrusion detection (and also intrusion prevention) looks very bright**
- **More than anything else, intrusion detection in the future is likely to build on models and methods that are already working**
- **The area that is likely to experience the greatest growth is intrusion detection data mining**