# Cortex
# A Reconfigurable and Survivable Service Environment

Christopher Geib, Vu Ha, Karen Haigh, Walt Heimerdinger, David Musliner, Jon Schewe, Ryan VanRiper

February 19, 2006

Honeywell

# Surviving Cyber Attacks

Honeywell

- **Systems must be designed that are capable of response and regeneration after deliberate attack and catastrophic failures.**

- **However, response and regeneration must be sensitive to…**
  - **the mission that is being executed,**
    - What tools and services are critical for the current mission goals?
    - What tools and services are not critical for the current mission goals?

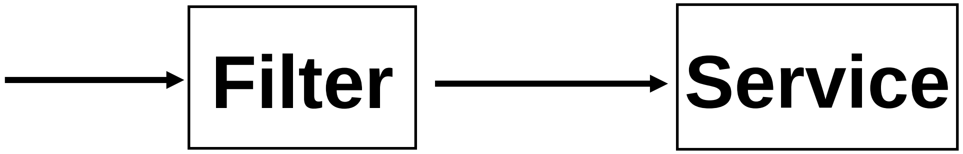
  - **and the lessons learned from the previous failure.**
    - What features of the protocol were exploited in the attack?
    - Have features of the domain changed?
      - Are there new kinds of connections that should be blocked?
      - Are some kinds of attacks more common than we thought?

# Cortex Objectives



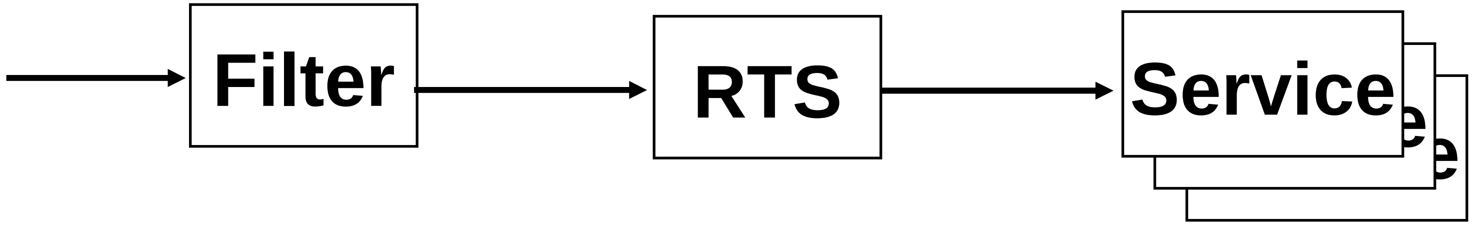
- **Prove the viability of automatically synthesizing a meta-level controller for model-based, system response and regeneration.**
- **Such regeneration control systems must have two critical capabilities:**
  - **planning that is sensitive to the system mission,**
    - How much of the systems resources should be committed or held in reserve?
    - Planning conditional responses to known threats.
    - Trading off commitments for mission critical objectives.
  - **and learning to prevent similar failures in the future.**
    - Patch the services that were exploited
    - Modify the mission model to capture changes to the world.

# Basic Service Environment



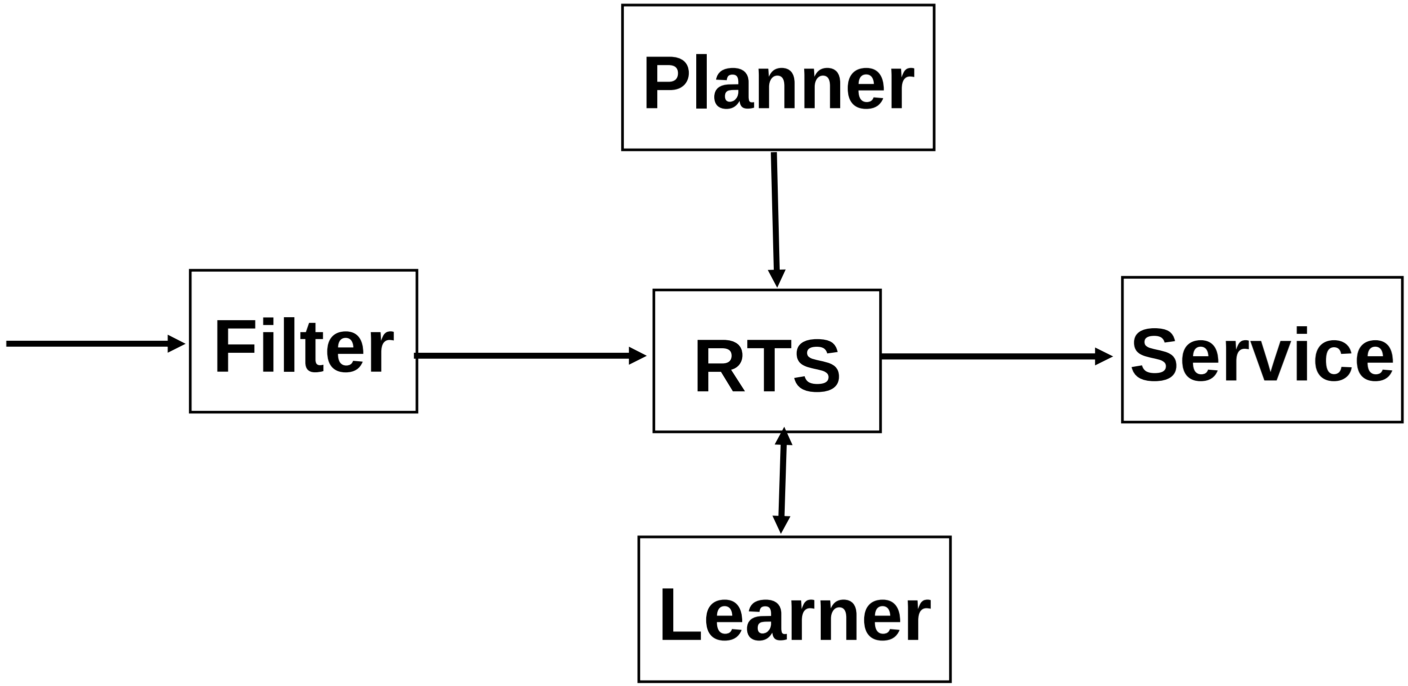
# Environment with Replicated Servers

Honeywell



# Environment with Replication and Learning

Honeywell



# Existing Practice



- Automated system rebooting will bring elements of the system back on line after an attack, but these are limited:
  - Simple scripts that are not sensitive to the mission model.
  - Can't make trade offs between competing needs.
  - Single system reboot.

- Learning of exploits and diagnosing root causes of the failure is handled offline by system experts.
  - Conclusions are not captured at the mission model level.
  - Often performed somewhere else.
  - Slow and requires significant expertise.

# Mission Model Motivation

Honeywell

- **Critical Problem Features**
  - Real world applicability and importance.
  - Military relevance clear.
  - Challenging complexity exceeds simple solutions.
  - Multiple mission phases with differing objectives requiring differing responses to attack.
  - Easy to find cyber attack methods within the literature.

- **Daily mission planning cycle**
  - Based on DARPA Cyber Panel Grand Challenge Problem
  - Defense of an operations critical MySQL database for mission planning.

# Cortex Role

Honeywell

- **Protect the MySQL database:**
  - Guarantee availability
  - Guarantee data integrity

- **Making use of:**
  - Redundant “taste tester” architecture
  - CIRCA planning for response and resource use
  - Learning based on active experimentation

- **Cortex control capabilities:**
  - Control query replication.
  - Manage tasters (which is lead-taster, building new ones)
  - Control access to DB (block known exploits)
  - Invoke learning module

# Goals

Honeywell

- **Prove the viability of automatically synthesizing a meta-level controller for model-based system response and regeneration.**
  - **Limited impact on current users**
  - **Over all improved system throughput from increased system mission sensitive availability.**
  - **Demonstrate system scalability in two mission phases**
- **Demonstrate system planning for at least two different mission phases with significantly different requirements and responses.**
- **Demonstrate the viability of learning zero-day exploits within well understood protocols for at least two different protocols.**

# CIRCA Planning: Generalized Semi-Markov Decision Processes

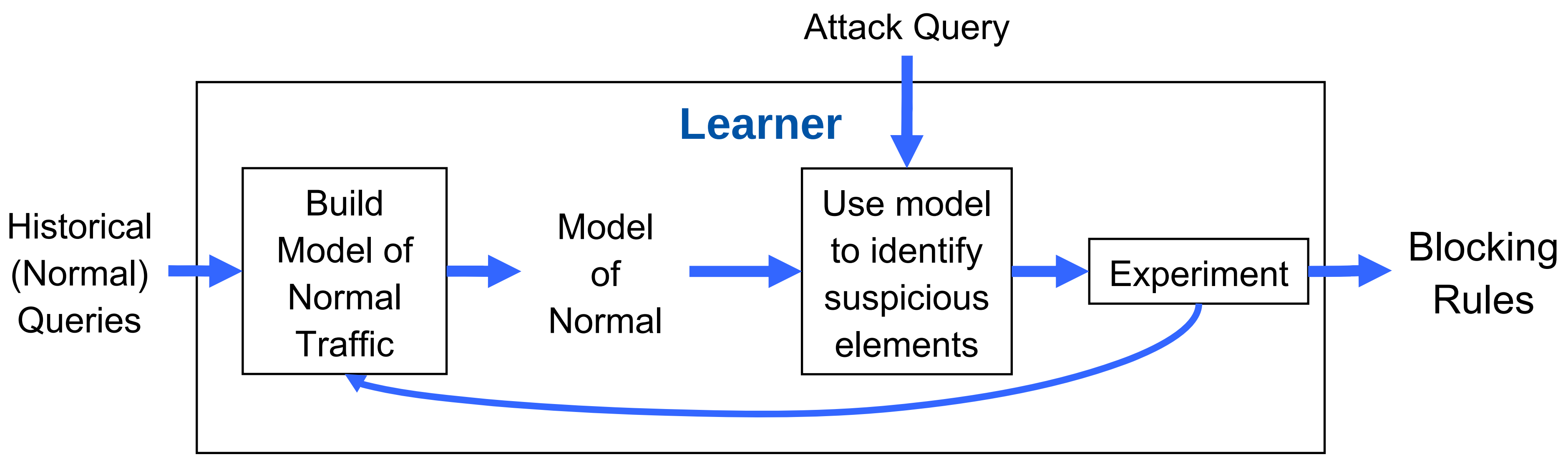
Honeywell

- **Most existing decision-theoretic planning systems are based on the Markov Decision Processes and have difficulty handling multiple, asynchronous events.**
- **GSMDP provides the most natural framework for this purpose.**
- **CIRCA (Cooperative Intelligent Real-Time Control Architecture) is the first GSMDP planner.**
  - Uses the decision-theoretic principle of maximizing expected utility (e.g. to trade off performance against safety).
  - Uses rich stochastic models of world, transitions, actions, and time to construct best defense plans.
  - Does not hand-build, but automatically synthesizes plans and can thus adapt to defend against combinations/mutations of existing exploits based on the mission model.

# Active Learning Approach

Honeywell

- We know an attack succeeded, but we don't know *why*.
  - Need an educated guess as to culprits, then validate
- We want to explore the possibilities.
  - Model normal mission traffic according to several axes of variability
    - Score each attack according to these axes
    - Experiment for most suspicious values



# Axes of Variability

Honeywell

- The different ways an attack (e.g. to MySQL) might be formulated.
  - Provided a priori by a domain expert
- Query content
  - Word order (e.g. some permutations cause MySQL to crash)
  - Binary machine instructions
  - Unusual payload (e.g. unix commands, registry keys, database administrative commands)
- Query length (single/multiple terms)
- Resource consumption patterns
- Probing (e.g. password guessing)
- Session-wide (multiple queries)

# Axes of Variability (detectors)

Honeywell

- **We currently detect:**
  - **Text Queries:**
    - String length: overall query length
    - SQL parser: term length (table, col, row), number of terms (table, row, col)
    - Word order: if there are no other suspicious elements in the attack
  - **Packet Content (Using hex values of the packet):**
    - Command type
    - Joint probability: each command has different expected byte patterns

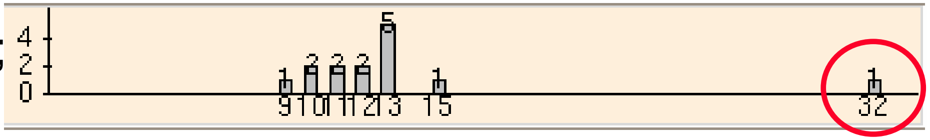
- **Plausible to design new or better detectors:**
  - **String content (e.g. look for hex)**
  - **Unusual payload (parser, keyword filter, content-filtering)**
  - **Session-wide (frequent patterns analysis)**
  - **Word order (patterns analysis)**
  - **More joint probability distributions (e.g. strings may generally be long, but passwords are short)**

# Modeling Mission Traffic



- **Model normal traffic**
  - Domain expert creates measures for each axis of variability (or combinations thereof)
  - Currently stored as histograms of the computed values
  - e.g.


- **Compare attack to the model**
  - Compute a “suspicion score”: how unusual is this attack for this axis of variability
  - Score = (value – μ) / σ
  - e.g. add “32” to above histogram; score is 12.6




- **Experiment (Active Learning)**
  - Sort the suspicion scores.
  - Experiment in the “most” suspicious axis first.
    - Test hypothesis of culprit
    - Discover the boundary conditions

# Demo

Honeywell

- Complete system protecting MySQL with normal background traffic for our mission model.

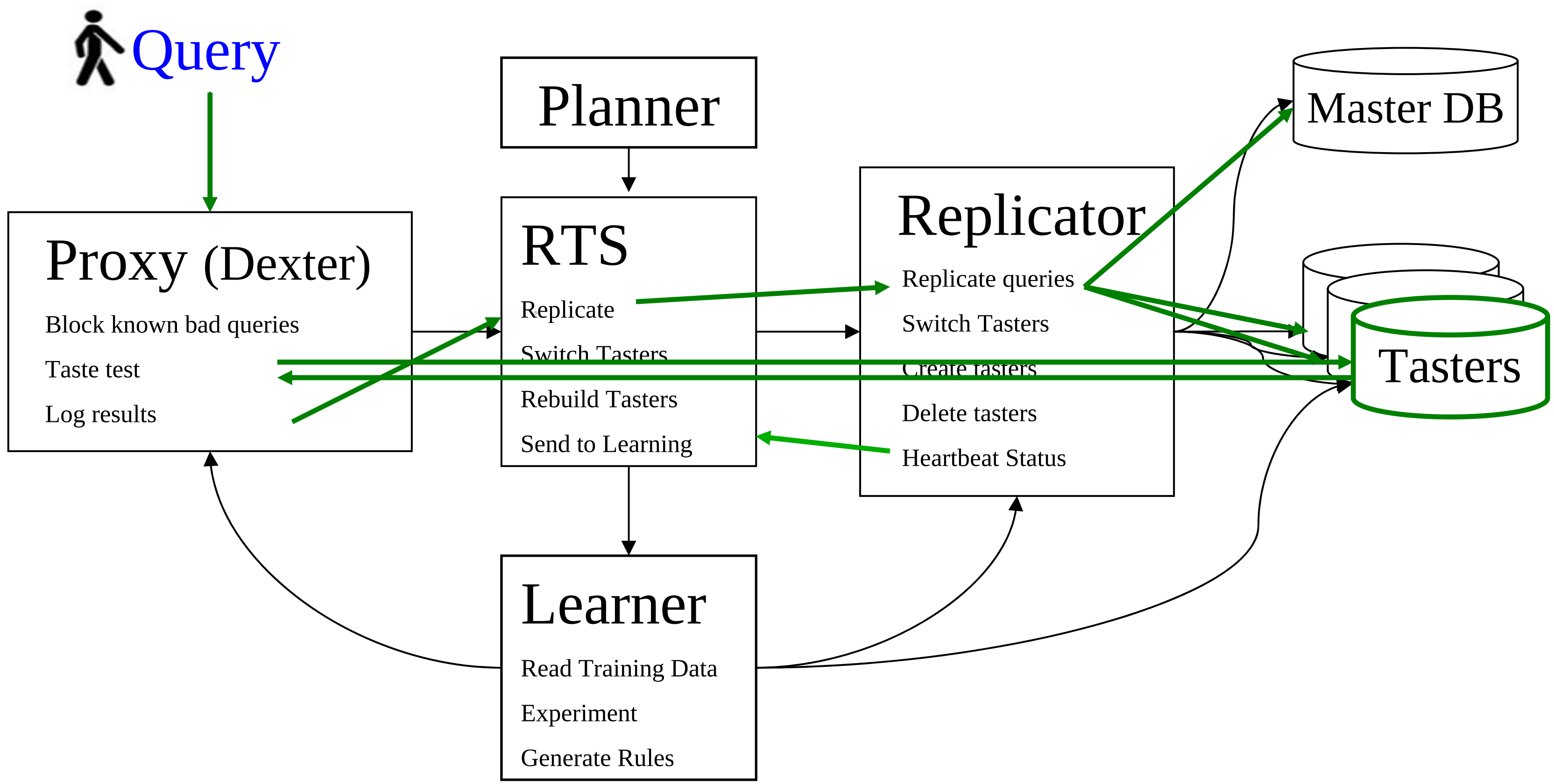
- All three end-to-end use cases.
  - Integration of CIRCA planning for single mission phase.
  - Learning via active experimentation.

- Two different attacks in Mission Model Phase 1
  - Both kill MySQL 3.23.49 server but are very different.
    - Password buffer-overflow (BID 8590)
      - Exploits the lack of bounds-checking on the password field for a user.
    - Binary attack against COM_TABLE_DUMP command (BID 6368)
      - Exploits a casting vulnerability of signed integer values.
      - Sends a negative value as one of the string length parameters to the command, and corrupts internal MySQL memory.

# Cortex Demo Architecture and Use Cases

Honeywell

## Normal Query



# Cortex Demo Architecture and Use Cases

Honeywell

Attack is blocked

Attack gets through