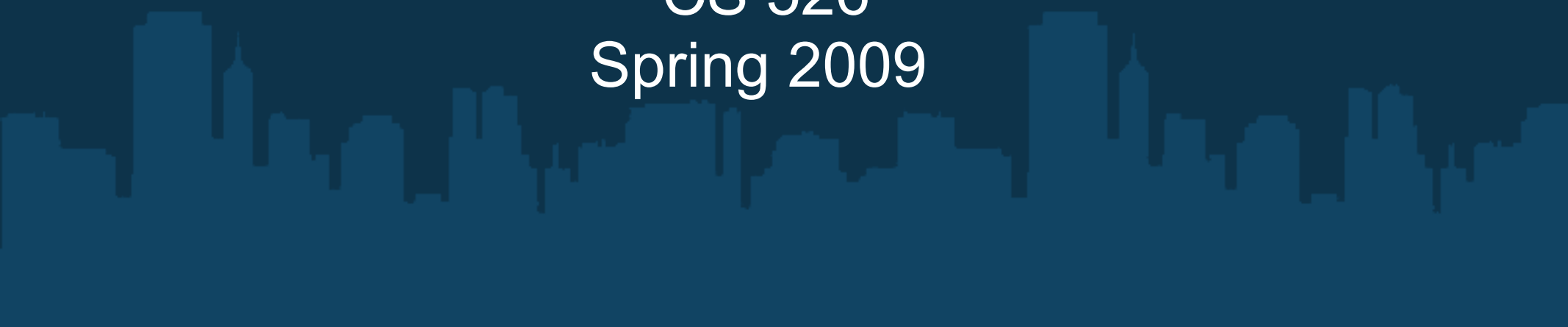
Detecting Early Signs of Insider Attack Using Role-Based Analysis and Classification

Jeff Hinson, Fadi Mohsen, Joe Taylor

CS 526

Spring 2009



Overview

- Insider Attacks
- Role-based Analysis
- Learning Classifier System
- Genetic Algorithm
- Gathering Data
- Design Problems
- Future Direction

Insider Attacks

What is an Insider Attack?
Insider attacks involve legitimate network users that have decided to act against the organization that employs them or formerly employed them.

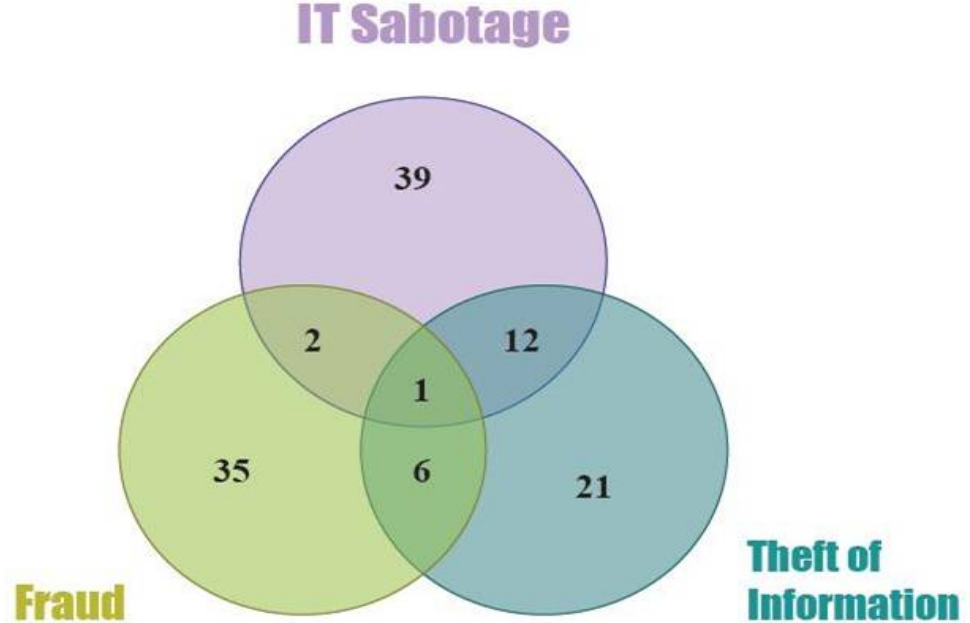
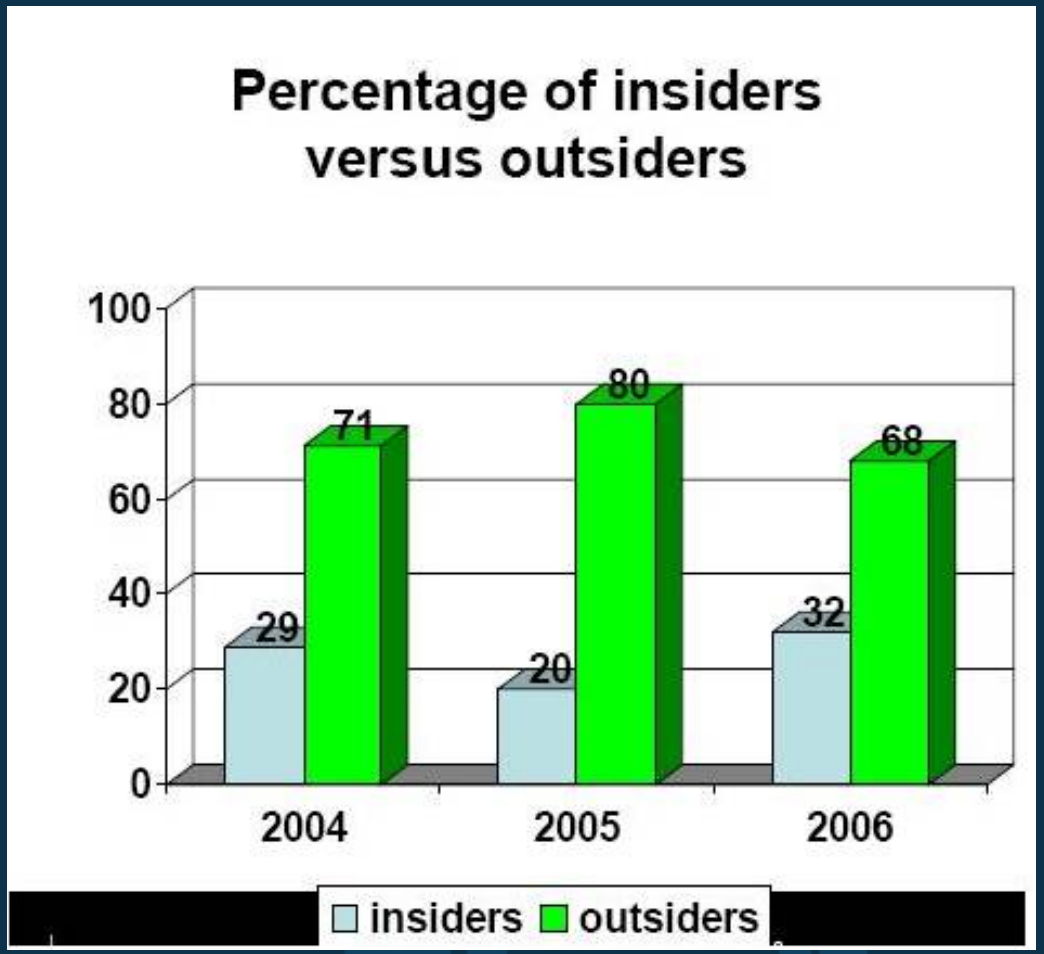


Figure 1: Breakdown of Cases

Is this really a problem?

- Because the insider has an extra knowledge about the internal system procedures, servers, and data bases, the harm will be too risky.
- Studies and researches shows that the number of insider attacks is increasing.
- In some cases the lose was millions of dollars, and in other cases the lose couldn't be estimated



What is currently being done about it?

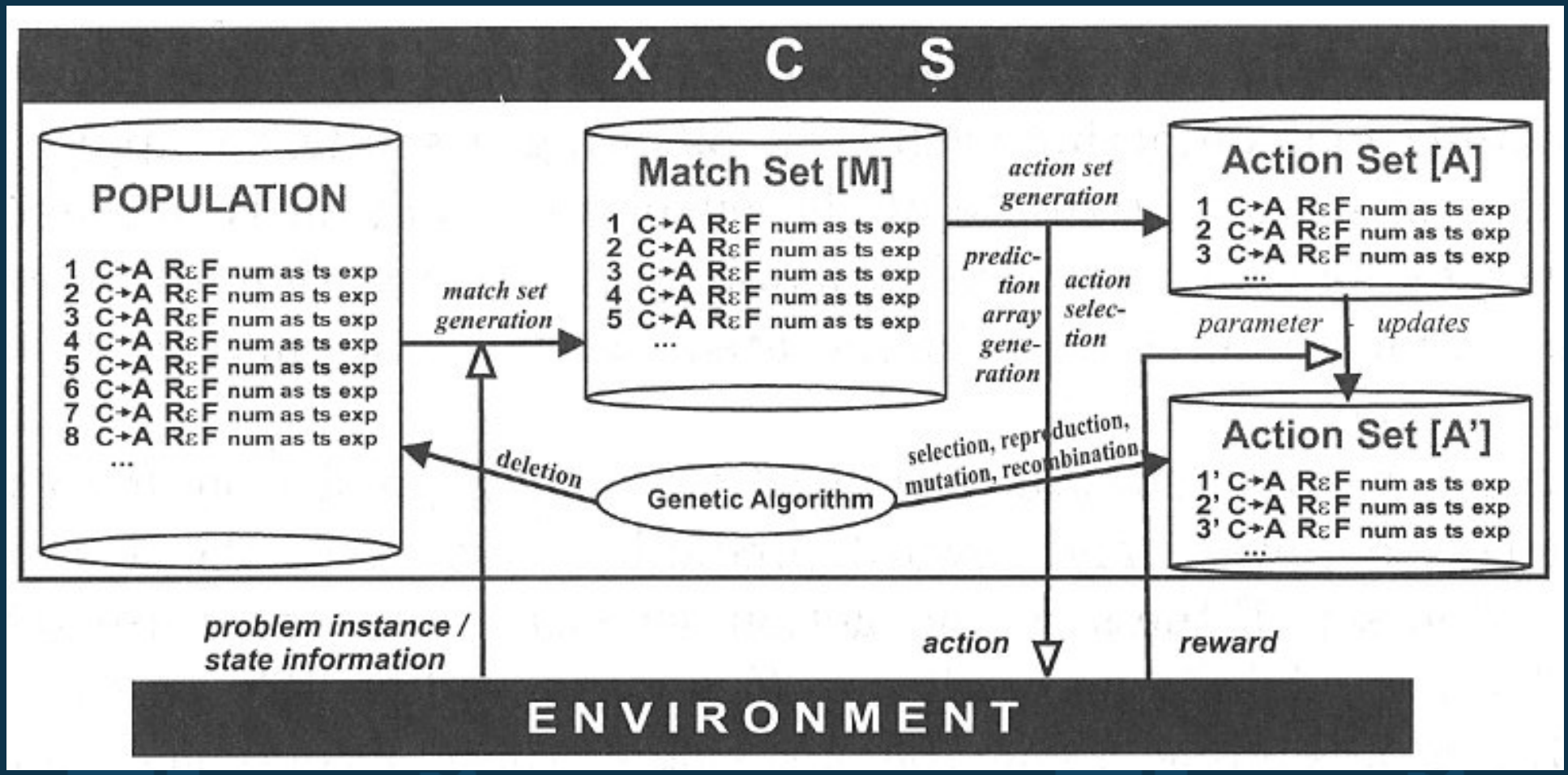
There are two main types of defense against insider attacks:

- Technical Means
  - Tools and programs that can track and restrict employee access, like IDS.
- Behavioral Means
  - Tools and programs that can track employee behavioral. This considered a new trend.

Role-Based Analysis

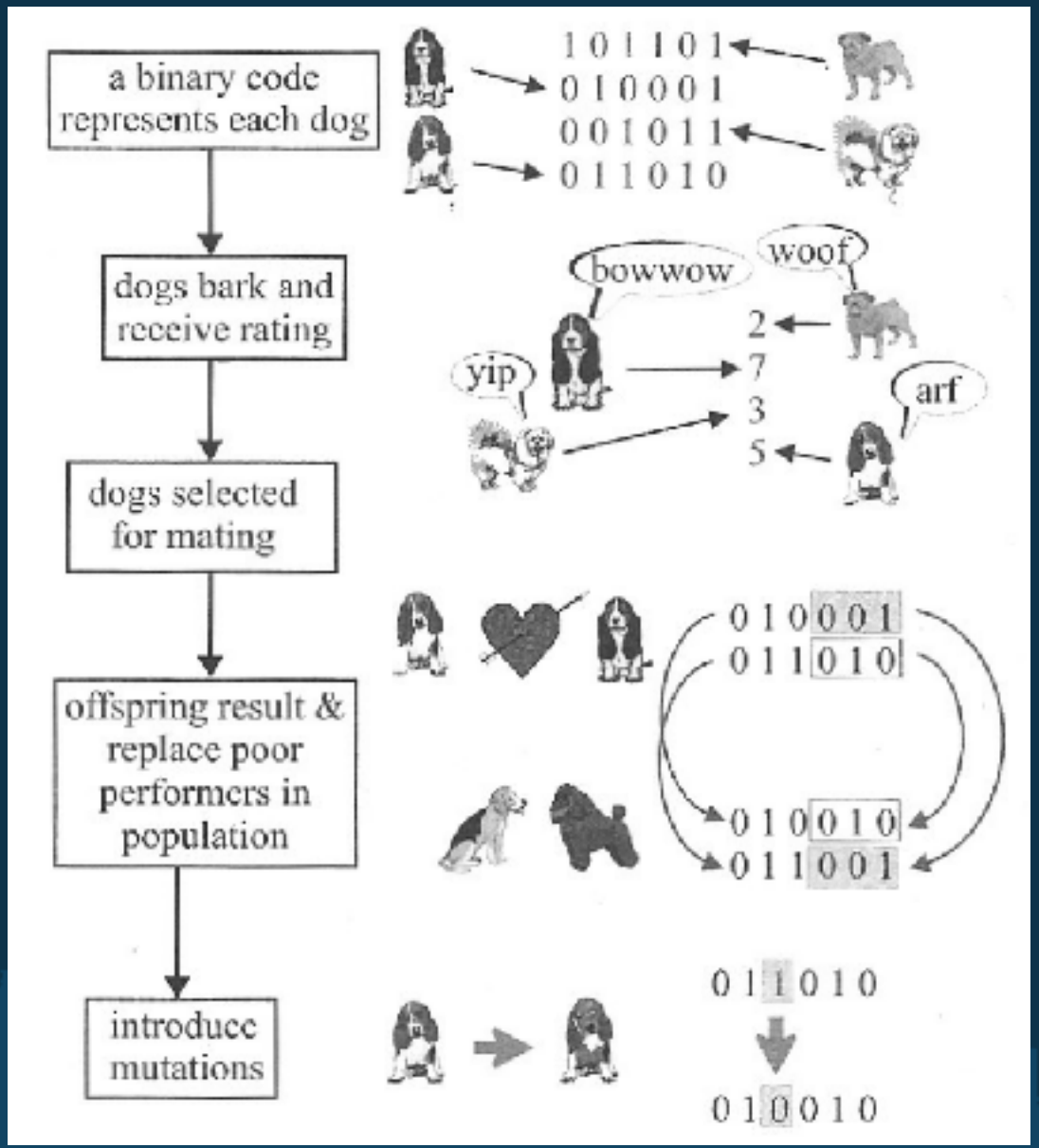
- Users classified into different groups based on needed privileges
- Every action compared to normal behavior withing user's group

Learning Classification System



Genetic Algorithm

- Reproduction
- Crossover
- Mutation



Gathering Information

- Windows Server 2008
  - Types of information collected
  - Disallow local user accounts?

- Custom Local Monitoring Client
  - Registry Scan
  - Process Monitoring
  - Peer-to-Peer Communication

Problems with Design

- Any potential problems with Server 2008?
  - local accounts?
  - can admin(s) get around it?

Points of Future Interest

- Manually collect data (instead of Server 2008)
  - clients run program, pass data to other clients
  - each client passes data to server
  - server processes data and sends alerts when a user violates a rule
- Advantages
  - more control over what data is collected
  - difficult for admins to get around

References

- J.S. Park, J. Giordano, "Role-based profile analysis for scalable and accurate insider-anomaly detection," pcc, pp.62, 2006 IEEE International Performance Computing and Communications Conference, 2006
- Liu, A.; Martin, C.; Hetherington, T.; Matzner, S., "A comparison of system call feature representations for insider threat detection," Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC , vol., no., pp. 340-347, 15-17 June 2005
- Butz, M. V., Kovacs, T., Lanzi, P. L., and Wilson, S. W. (2001). "How XCS Evolves Accurate Classifiers". In Spector, L., Goodman, E., Wu, A., Langdon, W., Voigt, H., Gen, M., Sen, S., Dorigo, M., Pezeshk, S., Garzon, M., and Burke, E., editors, Proceedings of the Genetic and Evolutionary Computation Conference (GECCO'2001), pages 927--934. San Francisco, CA: Morgan Kaufmann.
- Bauer, L., Cranor, L. F., Reeder, R. W., Reiter, M. K., and Vaniea, K. 2009. "Real life challenges in access-control management." In Proceedings of the 27th international Conference on Human Factors in Computing Systems (Boston, MA, USA, April 04 - 09, 2009). CHI '09. ACM, New York, NY, 899-908.
- D.M. Cappelli, A.P. Moore, and T.J. Shimeall, "Common Sense Guide to Prevention/Detection of Insider Threats", tech. report, Carnegie Mellon Univ., CyLab and the Internet Security Alliance, July 2006; www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf.

Questions?