

# Security Technologies: Where do we go from here?

**Jerry Brady, CTO/CSO**



**GUARDENT<sup>SM</sup>**



# Current Security Issues

An incomplete set:

- Overwhelming vulnerability of current technology set
- A broad range of technology equipped adversaries
- Complexity of systems
- Relative lack of integration of security and business process



# Vulnerabilities

- Most applications in use today are vulnerable to a variety of well known vulnerabilities
  - A few classics seem to reappear periodically
    - Buffer overflows, format string vulnerabilities, user input validation
    - General purpose technologies are becoming available to mitigate some – kernel protections and stack protection schemes
- An difficult problem to solve – current strategies **cannot** be successful
  - Current strategies for most organizations is to find all of the vulnerabilities and patch them... care to cause a few production outages this week? For a good cause?
- Systems exploitation occurs almost immediately after a vulnerability is discovered – no time for testing of patches
  - Information is shared far more efficiently by the underground than corporate America



# Systems Complexity

Complex systems present some very difficult questions:

- Which vulnerabilities really matter?
- What is the shortest path to vulnerability remediation?
- What is the impact of not patching systems?
- Are there alternatives?
  - More on that later
- What is the net effect on the business of any given weakness or vulnerability?
- Unfortunately, complexity has a very negative affect on security management
  - Hard to analyze failure modes, hard to perform corrective actions, dependencies open up risk of failure



## What technologies solve these problems?

- The ones we already have
  - Cryptography in general
    - In highly usable models
  - Application testing tools and services
  - A few immature technologies which could be used more and better
    - Intrusion Prevention Systems
      - A big category, means different things to different people
    - Stack Protection
    - Static Analysis



## The real answers

- Reduction of complexity
- Understanding “failure modes” of systems and business processes
- Reducing probability of failure modes through design, testing, and remediation
  - Static Analysis, Application Testing, Stack Protection and similar technologies
- Using mitigating controls when appropriate (like this weekend, just in case a million workstations are compromised)
- Building systems with a rational model for survival
  - Choosing components with a good history for security defects
    - Would you buy a pinto after hearing about it's crash record?
  - Understanding what can't be done, and choosing successful mitigation strategies
    - Plenty of technology available – Firewalls, routers, IPS, etc.
  - **Developing recovery strategies when the inevitable occurs**



## Summary

- Reduce complexity
- Choose reliable components when possible
- Understand implications of “failure modes”
- Have compensating controls available
- Focus on survivability