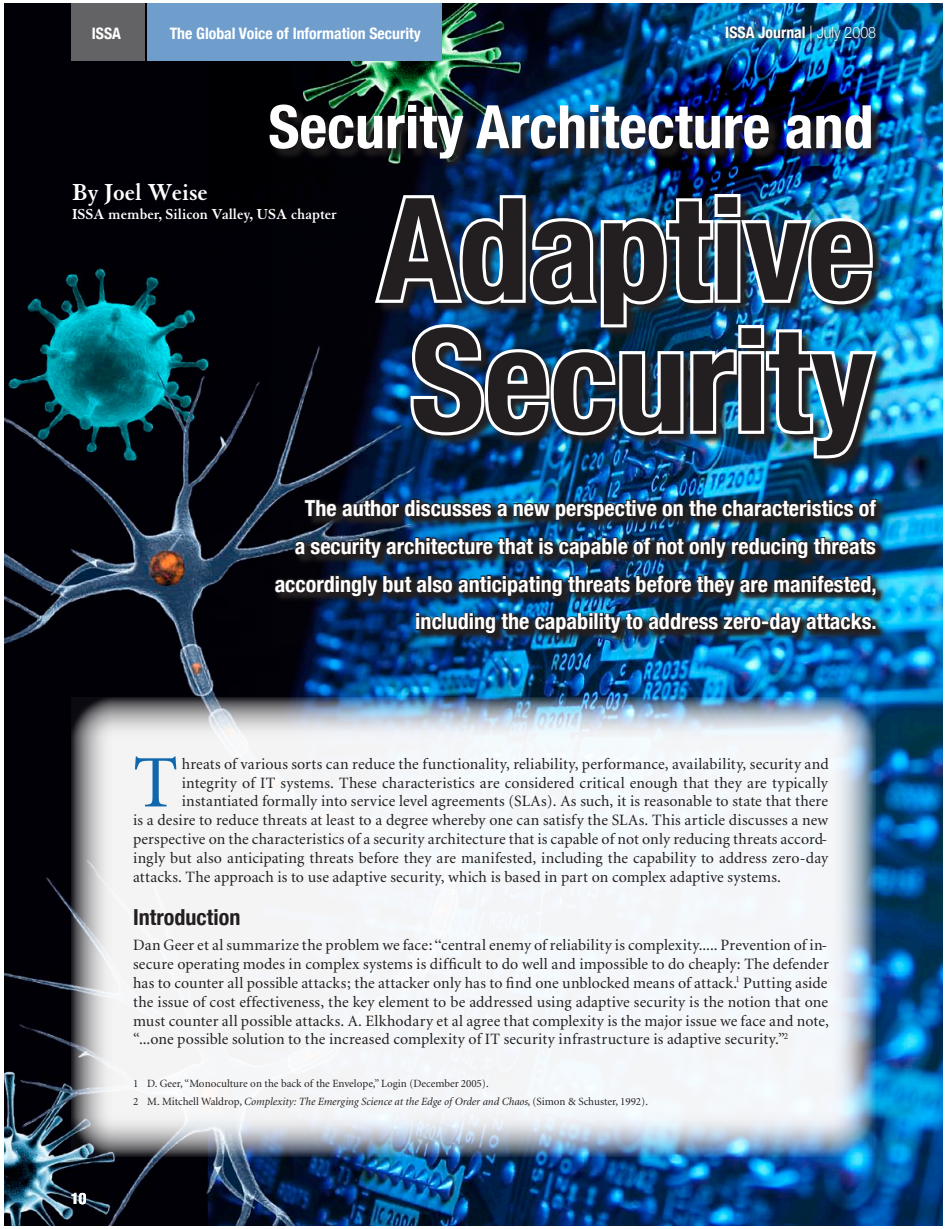
Adaptive Security

Joel Weise
Principal Engineer / Chief Technologist

Copyright © 2008 Sun Microsystems, Inc.



Copyright © 2008 Sun Microsystems, Inc.

ISSA Journal

- Charter
  - Focus on information security
  - Educate, communicate, inform
  - Provide a forum for discussion
  - Keep you abreast of current trends
  - Vendor neutral
- Editorial calendar
- Editorial guidelines

Copyright © 2008 Sun Microsystems, Inc.

ISSA
Information Systems Security Association
The Global Voice of Information Security

The Information Systems Security Association, Inc. is an international organization that acts as the "Global Voice of Information Security." The ISSA Journal *is published to support ISSA's mission of promoting management practices that will ensure the confidentiality, integrity and availability of organizational information resources.*

The *ISSA Journal* – 2008 Editorial Calendar

JANUARY
Protecting & Prioritizing Data
Viruses, Trojans, Malware
Editorial Deadline 12/7/07
Ad Materials Due 12/13/07

FEBRUARY
Service Oriented Architecture
Data Recovery
Editorial Deadline 1/4/08
Ad Materials Due 1/10/08

MARCH
Regulatory Compliance
Authentication Technologies
Editorial Deadline 2/1/08
Ad Materials Due 2/14/08

APRIL
Business Cryptography
Future of the Network
Editorial Deadline 2/29/08
Ad Materials Due 3/13/08

MAY
Making the Case: Security ROI
Enterprise Risk Management
Editorial Deadline 3/28/08
Ad Materials Due 4/10/08

JUNE
Virtualization
Cyber Crime
Editorial Deadline 5/2/08
Ad Materials Due 5/15/08

JULY
Future of Security: Reactive or Adaptive
Security and Ethics
Editorial Deadline 5/30/08
Ad Materials Due 6/12/08

AUGUST
Identity Management
Defending the Network
Editorial Deadline 7/4/08
Ad Materials Due 7/10/08

SEPTEMBER
Business Continuity Planning
Conducting a Security Audit
Editorial Deadline 8/1/08
Ad Materials Due 8/14/08

OCTOBER
Compliance Strategies
Top 10 Cyber Threats
Editorial Deadline 8/29/08
Ad Materials Due 9/11/08

NOVEMBER
Digital Forensics
Protecting Privacy
Editorial Deadline 9/26/08
Ad Materials Due 10/9/08

DECEMBER
Social Engineering and Insider Threats
Cloud Computing
Editorial Deadline 10/31/08
Ad Materials Due 11/13/08

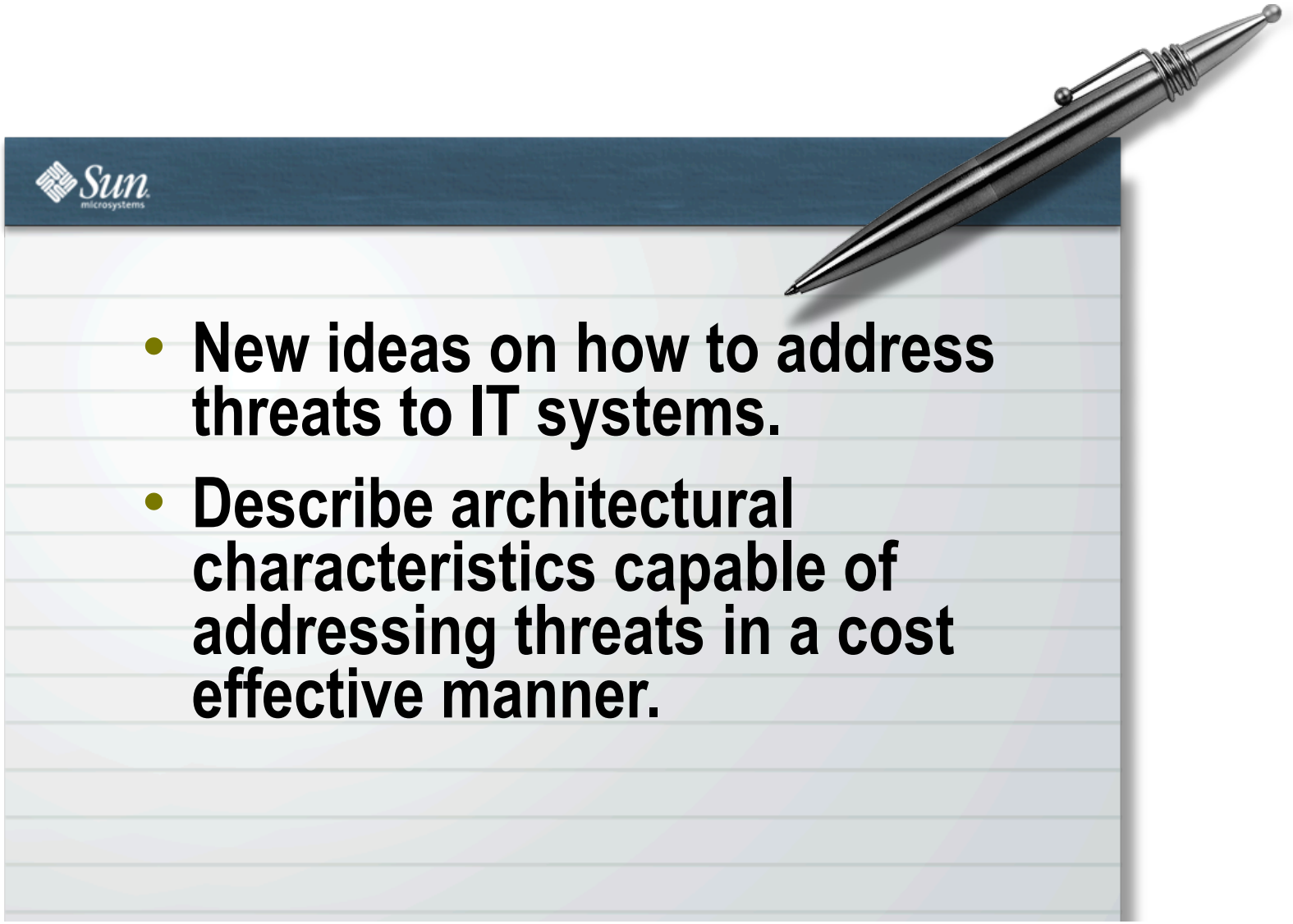
Copyright © 2008 Sun Microsystems, Inc.

Article Guidelines

- **An excellent article:**
  - is relevant to a security practitioner (including CxO level)
  - related to current trends, technologies and issues
  - leans towards practical insight
  - cites sources, and shows knowledge of the work of industry thinkers.
  - covers subject matter that piques the curiosity of readers.
  - for more details, see: http://www.issa.org/Downloads/TheISSAJournalGuidelines.pdf

Copyright © 2008 Sun Microsystems, Inc.

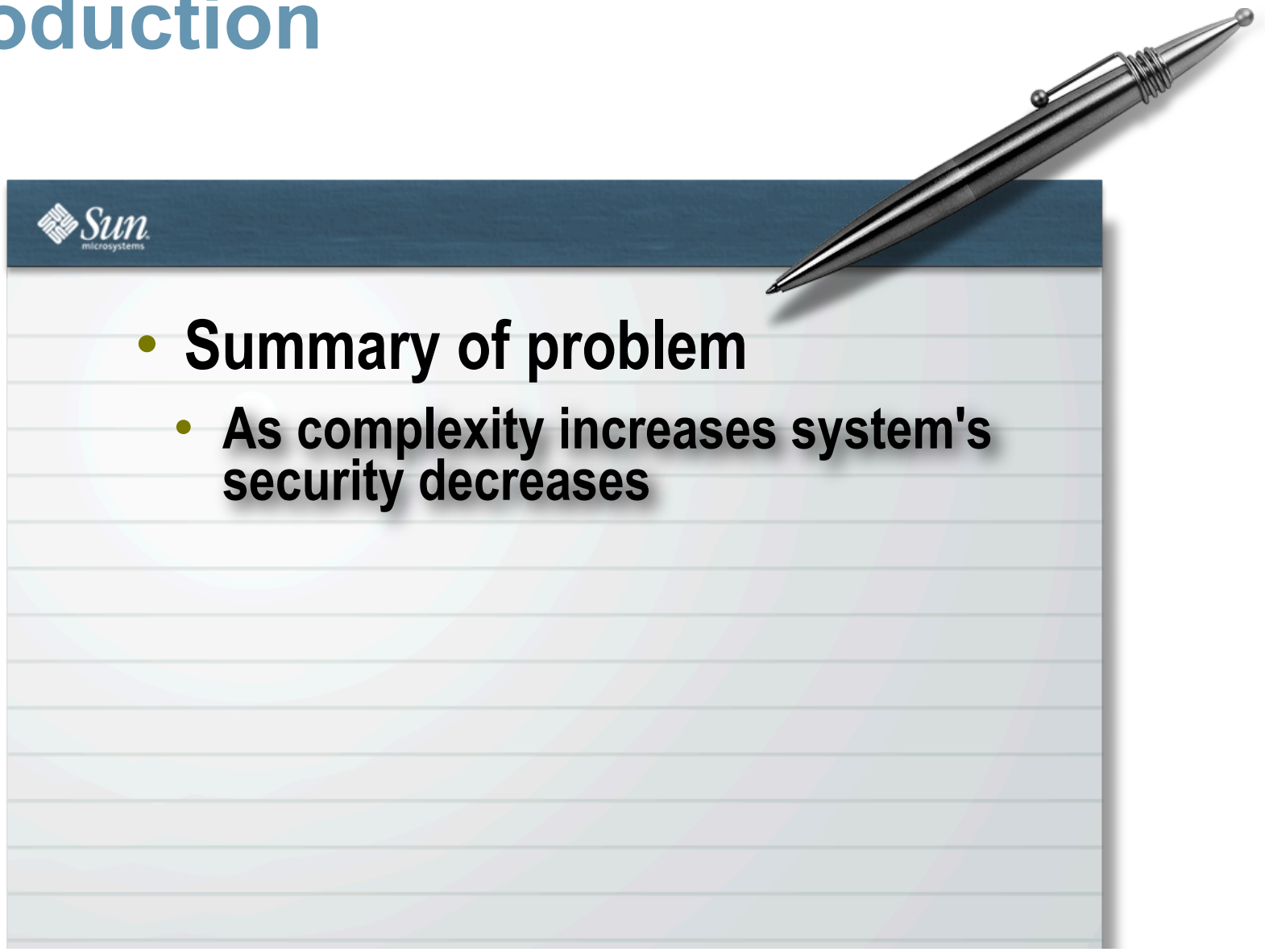
Introduction



- New ideas on how to address threats to IT systems.
- Describe architectural characteristics capable of addressing threats in a cost effective manner.

Copyright © 2008 Sun Microsystems, Inc.

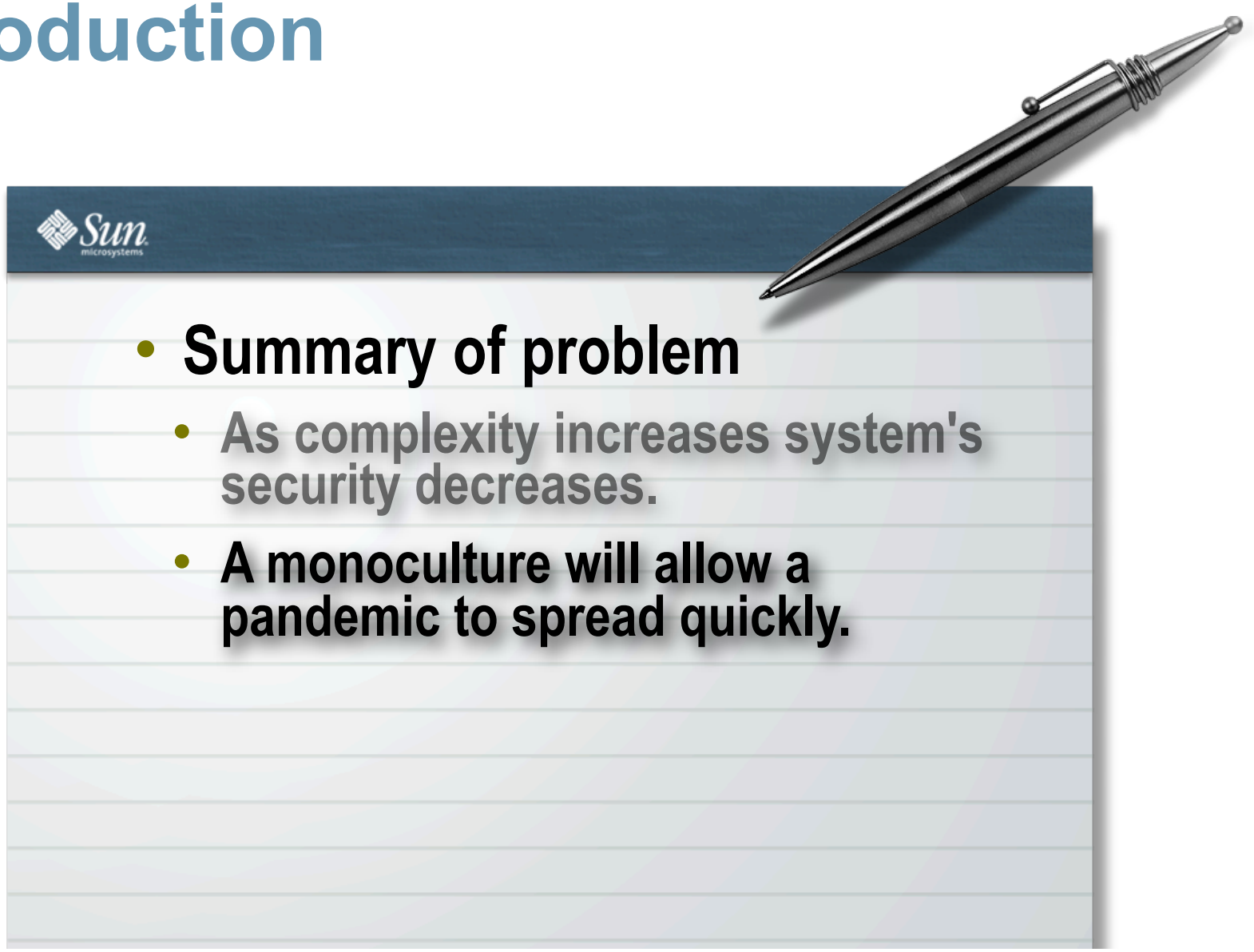
Introduction



- Summary of problem
  - As complexity increases system's security decreases

Copyright © 2008 Sun Microsystems, Inc.

Introduction



- Summary of problem
  - As complexity increases system's security decreases.
  - A monoculture will allow a pandemic to spread quickly.

Copyright © 2008 Sun Microsystems, Inc.

Introduction

- **Summary of problem**
  - As complexity increases system's security decreases
  - A monoculture will allow a pandemic to spread quickly.
  - **Threats are created faster than counter-measures**

Copyright © 2008 Sun Microsystems, Inc.

Introduction

- **Summary of problem**
  - As complexity increases system's security decreases
  - A monoculture will allow a pandemic to spread quickly.
  - Threats are created faster than counter-measures.
  - **Threat reduce:**
    - **Functionality, security, availability.**

Copyright © 2008 Sun Microsystems, Inc.

Goals of Adaptive Security

- **Anticipate threats before they can be manifested.**
- Respond to and contain threats.
- Ensure trustworthiness and system survivability.

Copyright © 2008 Sun Microsystems, Inc.

Goals of Adaptive Security

- Anticipate threats before they can be manifested.
- **Respond to and contain threats.**
- Ensure trustworthiness and system survivability.

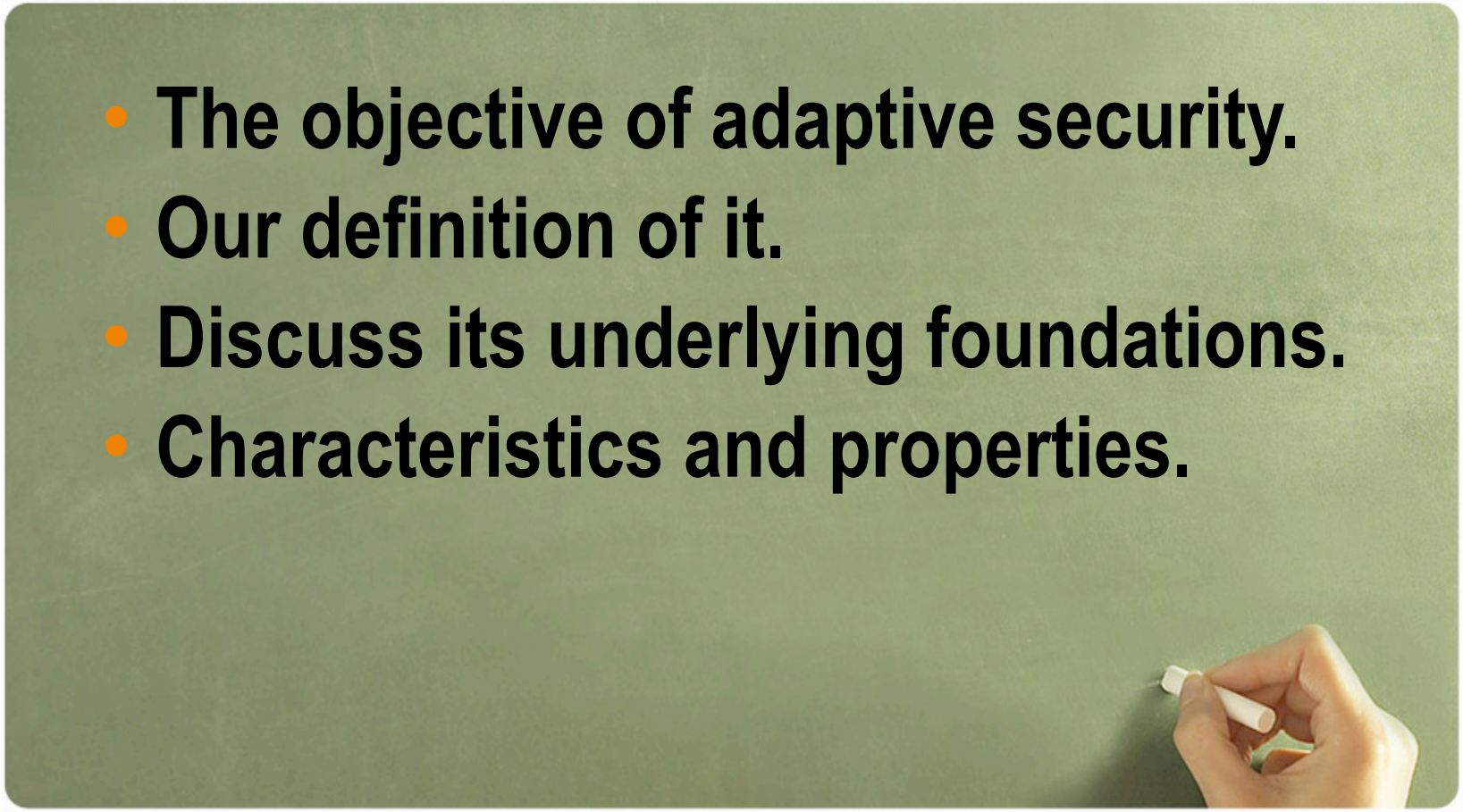
Copyright © 2008 Sun Microsystems, Inc.

Goals of Adaptive Security

- Anticipate threats before they can be manifested.
- Respond to and contain threats.
- **Ensure trustworthiness and system survivability.**

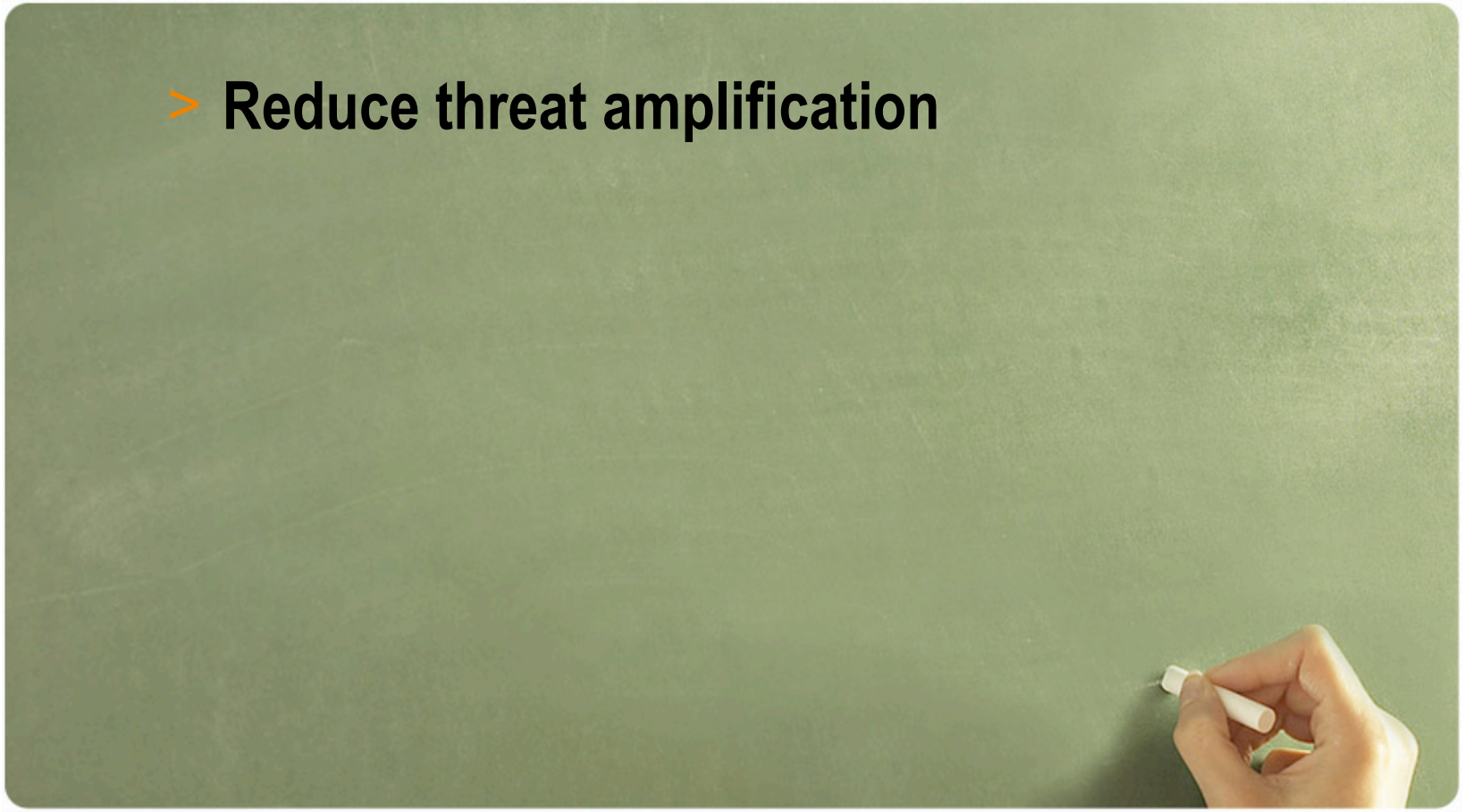
Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security



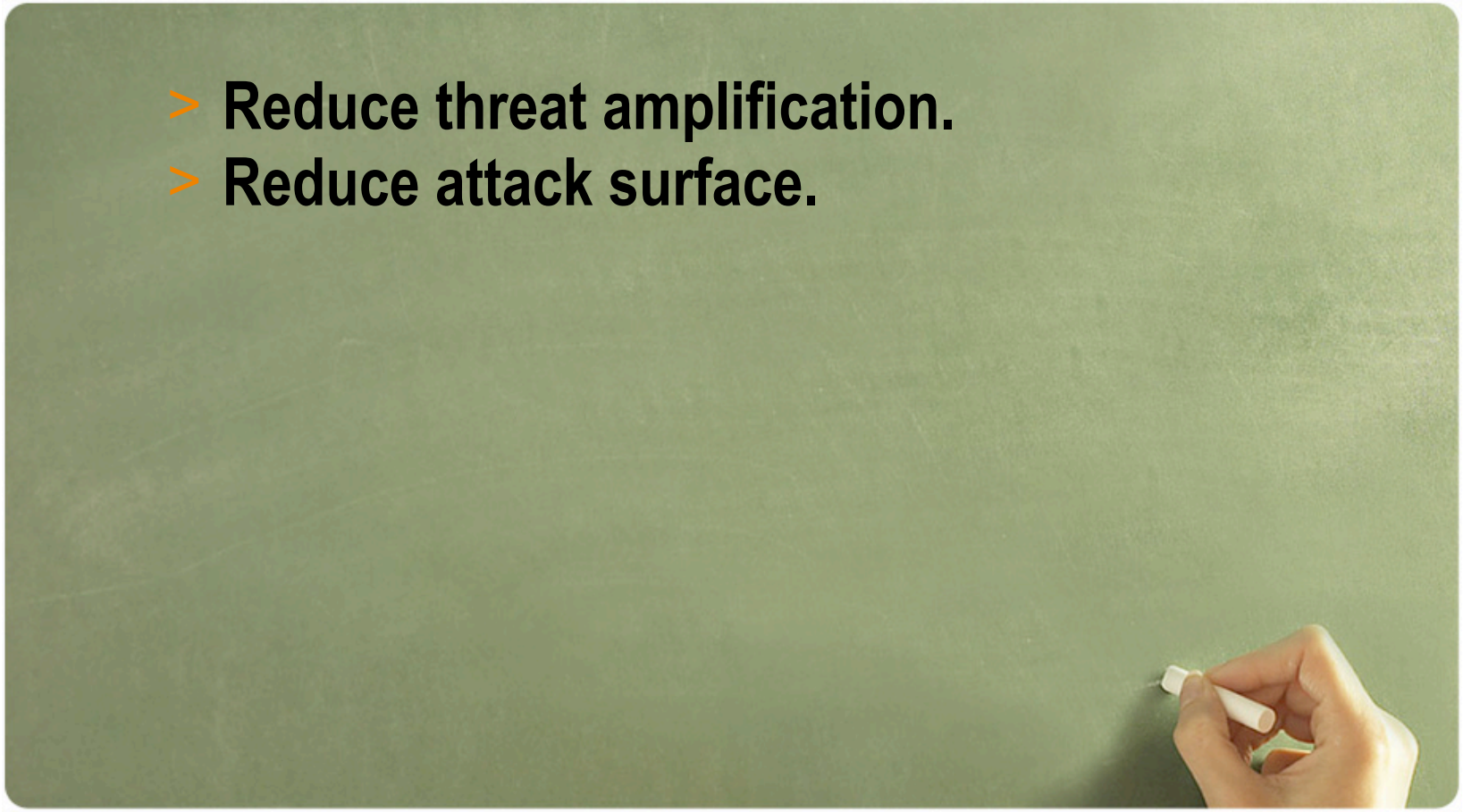
Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Objectives



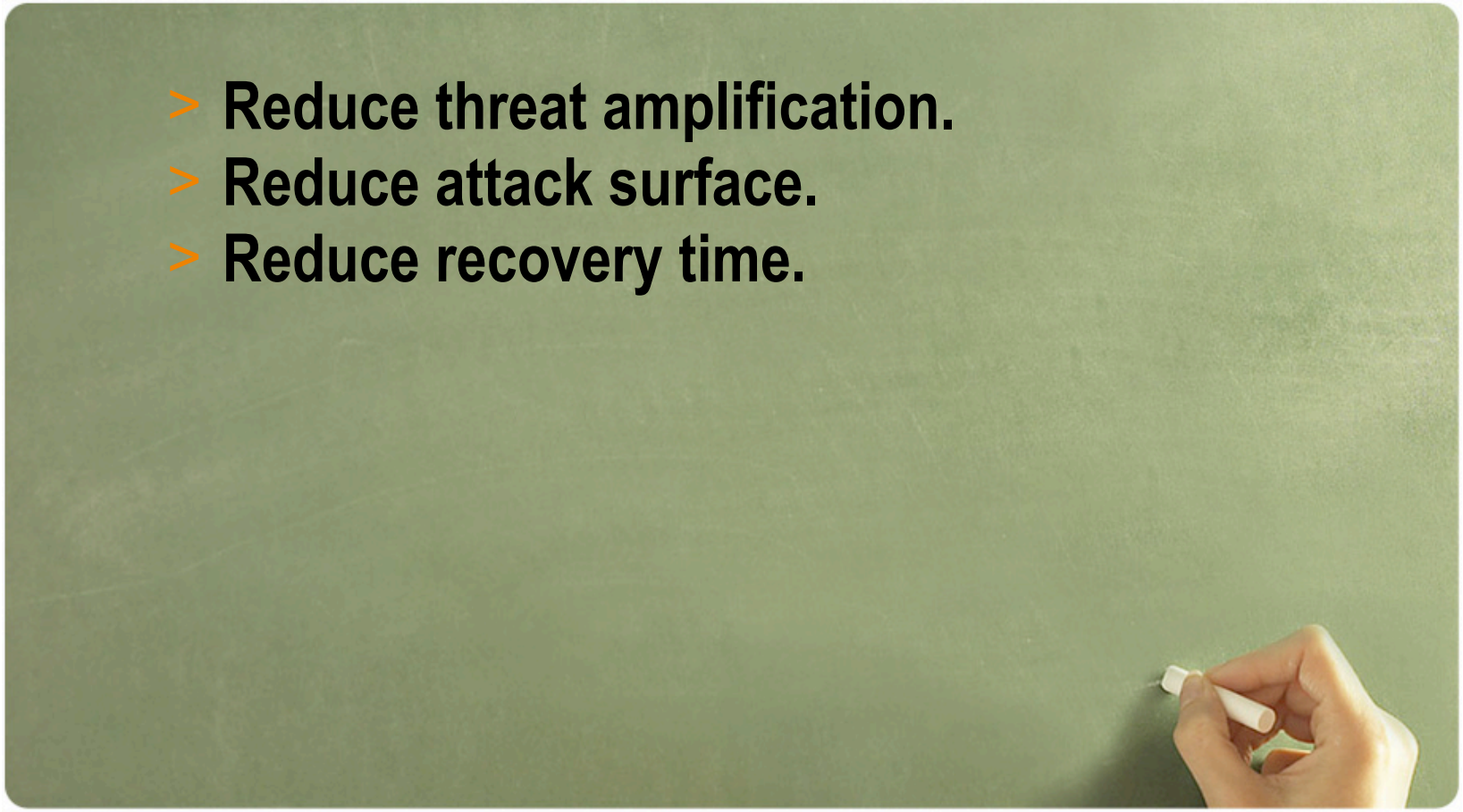
Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Objectives



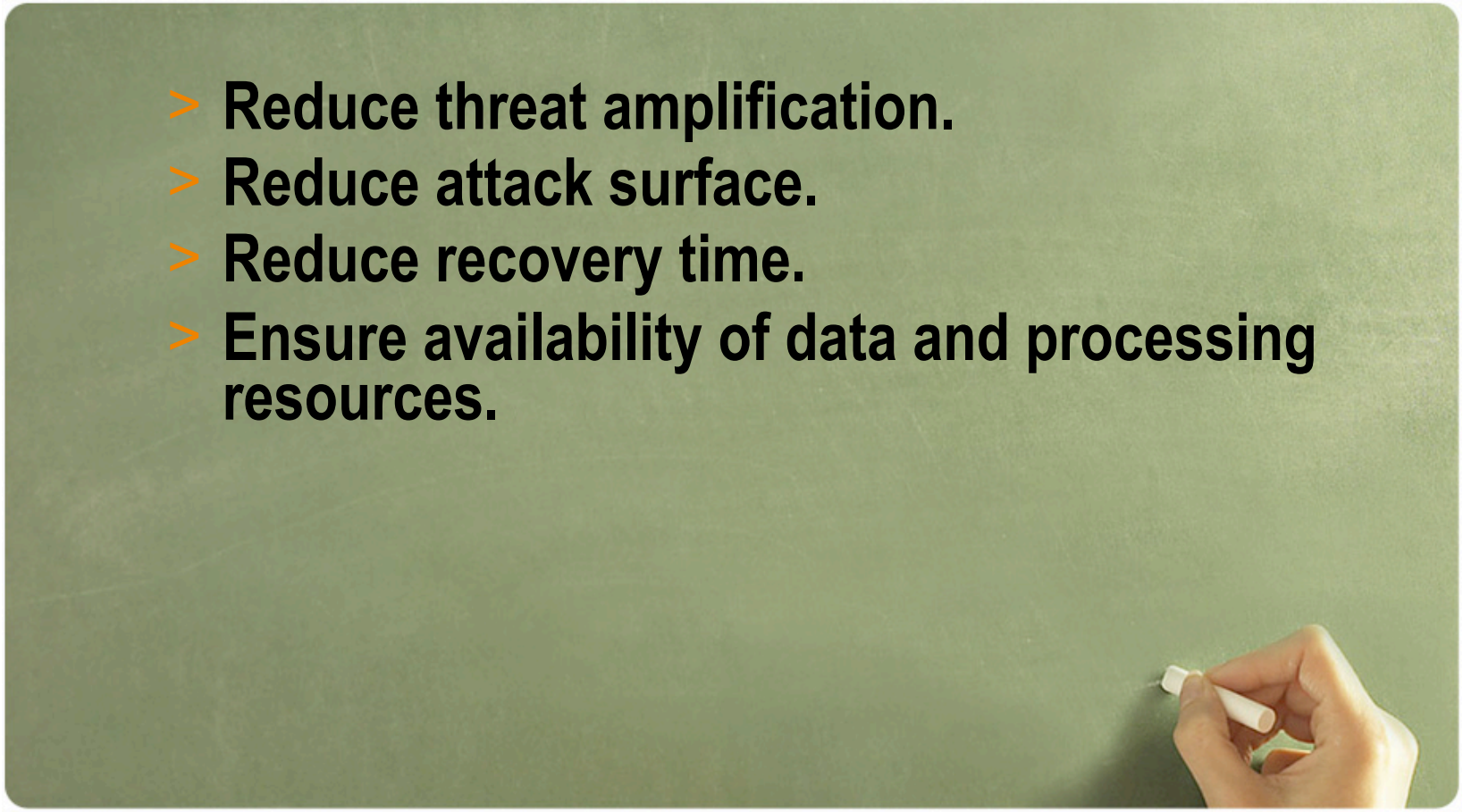
Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Objectives



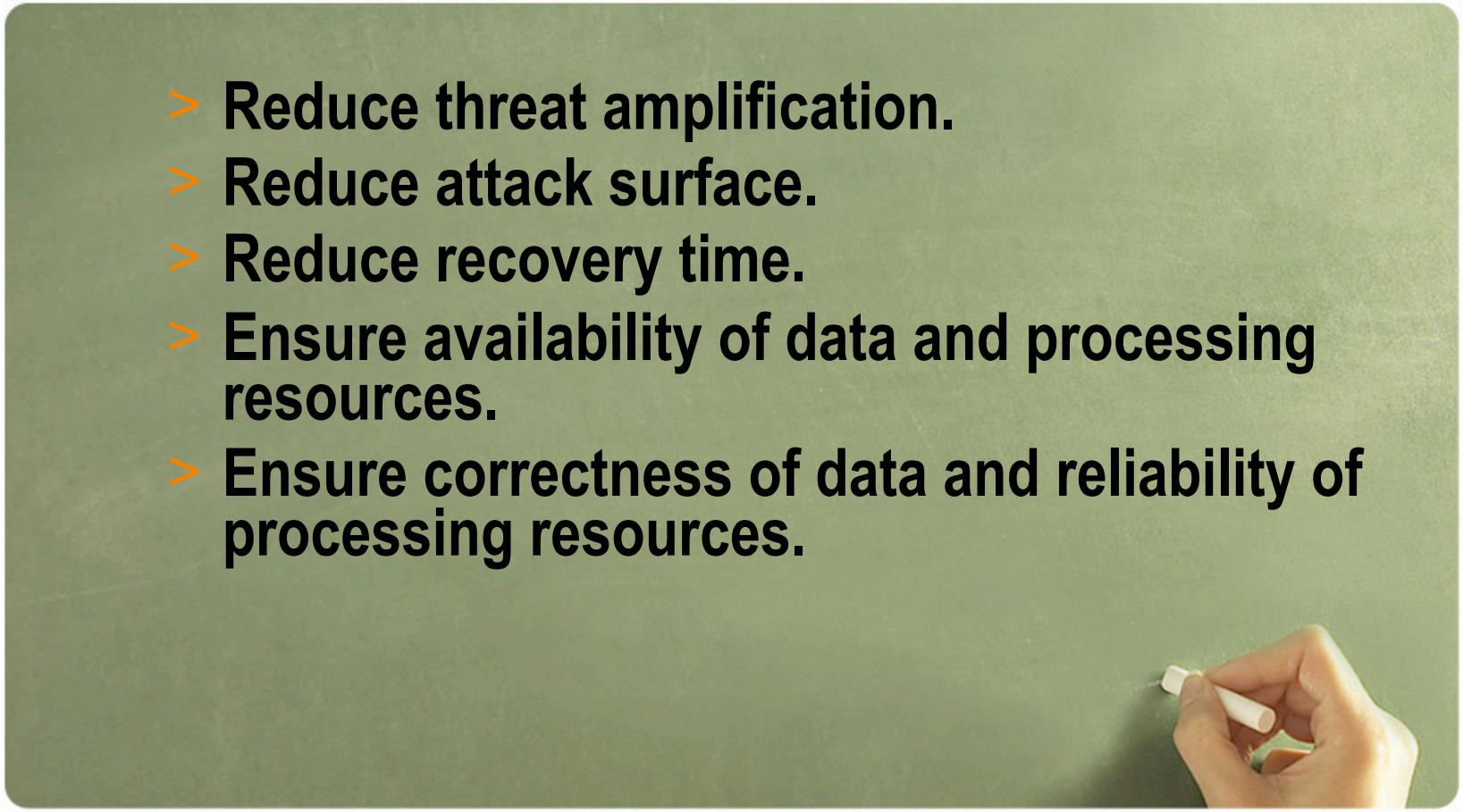
Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Objectives



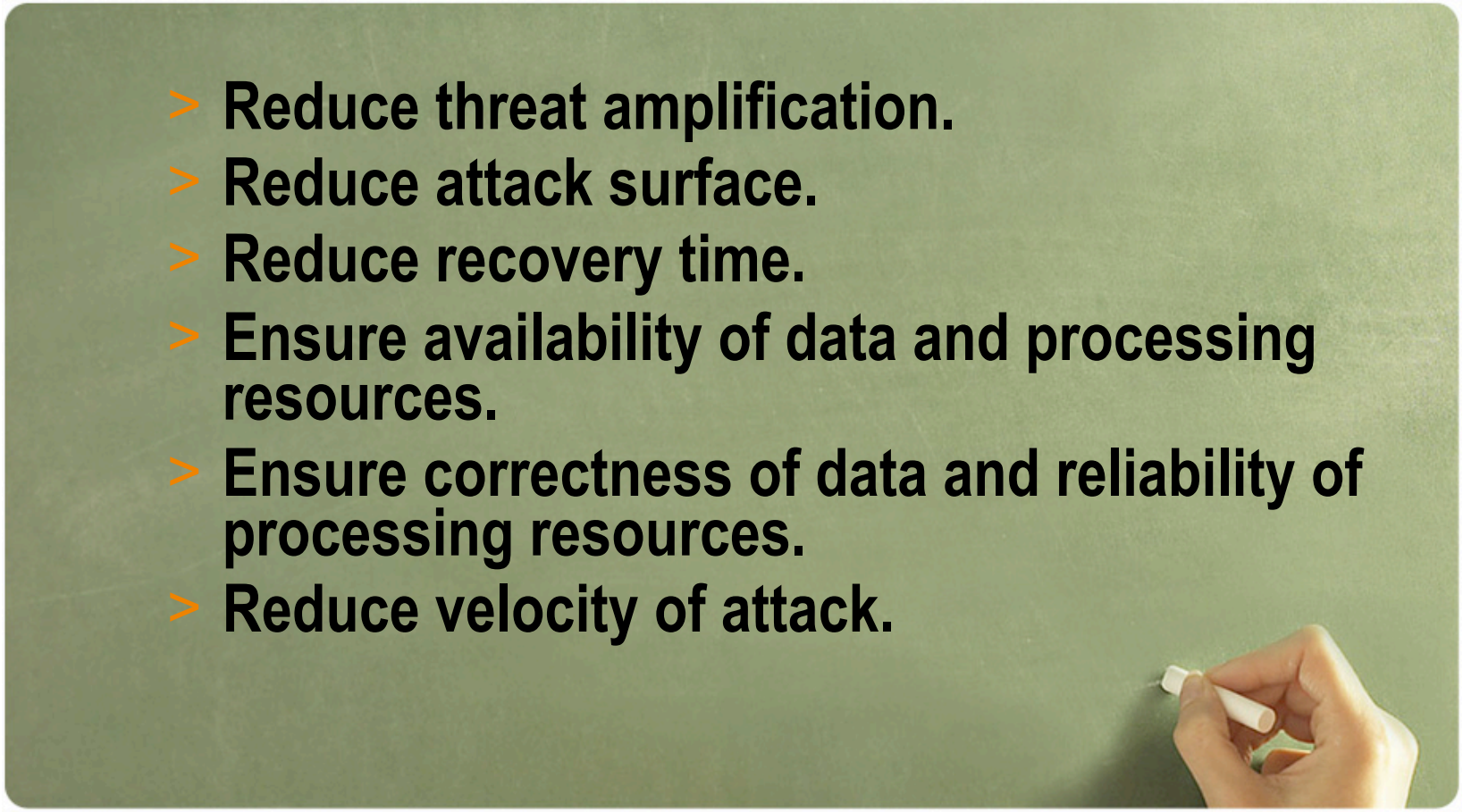
Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Objectives



Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Objectives



Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Definition

- **What is adaptive security?**
  - **An architectural model based upon the convergence of biological and ecological systems.**
  - Mimic biological autoimmune system at the microscopic level.
  - Mimic ecological systems of disparate entities at the macroscopic level.
  - Not a single system or process.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Definition

- **What is adaptive security?**
  - An architectural model based upon the convergence of biological and ecological systems.
  - **Mimic biological autoimmune system at the microscopic level.**
  - Mimic ecological systems of disparate entities at the macroscopic level.
  - Not a single system or process.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Definition

- **What is adaptive security?**
  - An architectural model based upon the convergence of biological and ecological systems.
  - Mimic biological autoimmune system at the microscopic level.
  - **Mimic ecological systems of disparate entities at the macroscopic level.**
  - Not a single system or process.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Definition

- **What is adaptive security?**
  - An architectural model based upon the convergence of biological and ecological systems.
  - Mimic biological autoimmune system at the microscopic level.
  - Mimic ecological systems of disparate entities at the macroscopic level.
  - **Not a single system or process.**

Copyright © 2008 Sun Microsystems, Inc.

Biological Systems - Foundation

- Why biologic systems?
  - Successful biologic systems are able to adapt over time to respond to new and different conditions.
  - Biologic systems use autonomic immune systems to dynamically respond to threats.
  - This dynamic behavior is what we desire to mimic.

Copyright © 2008 Sun Microsystems, Inc.

Biological Systems - Foundation

- Why biologic systems?
  - Stem Cells are unspecialized - can be use as a foundation to 'repair' other elements.
  - Self and non-self.
    - Trusted vs untrusted elements.
  - Vaccinations offer acquired immunity.
    - If one system is attacked and survives, it can share its survival strategy with other systems.

Copyright © 2008 Sun Microsystems, Inc.

Biological Systems - Foundation

- Why biologic systems?
  - Apoptosis
    - Programmed cell death.
    - Our bodies expel cells as they become old and under-performing.
  - We can treat systems in the same way.

Copyright © 2008 Sun Microsystems, Inc.

Ecological Systems - Foundation

- Why ecologic systems?
  - Successful ecological systems spread risk across themselves.
  - We draw the parallel that an IT infrastructure is in fact an ecological system comprised of various components.

Copyright © 2008 Sun Microsystems, Inc.

Ecological Systems - Foundation

- Why ecologic systems?
  - Survival of the ecosystem does not depend upon survival of any individual entity.
  - Ecosystems are by definition diverse and this contributes to their resilience.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Foundation

- Why biologic and ecologic systems?
  - Both rely upon feedback to increase ability to respond to threats.
  - Survival of the fittest – i.e., successful strategies are rewarded with survival.
  - Both function dynamically and autonomously.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Convergence

- Desired design characteristics from biologic and ecologic systems.
  - Flexible and able to adaptively respond to new and different threats.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Convergence

- Desired design characteristics from biologic and ecologic systems.
  - Flexible and able to adaptively respond to new and different threats.
  - Self-detecting, self-regulating, self-healing and self-protecting.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Convergence

- Desired design characteristics from biologic and ecologic systems.
  - Flexible and able to adaptively respond to new and different threats.
  - Self-detecting, self-regulating, self-healing and self-protecting.
  - Able to comprehend normal conditions and detect abnormal behavior and conditions.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Properties

Pattern recognition	Of normal and abnormal behavior
Uniqueness	No monoculture
Self identity	No what you are and what is not.
Diversity	Maintain different structure and configs.
Disposibility	Anything can be sacrificed.
Autonomy	No central control.
Multi-layered	Defense in depth.
No secure layer	Attacks can come from anywhere.
Noise tolerance	Specific match not needed to id threat.
Resilience	Continue to function in a reduced state.
Fault tolerant	Elements function complimentarily.
Robustness	Benefit of diversity and distributivity.
Immune learning and memory	Remember past threats.
Predator-prey response	Mediated and measured response.
Self organization	Remember successful threat responses.
Integration with other systems	Use common communications protocols.
Anomoly detection	Recognize out of norm conditions.
Dynamic changing coverage	Regularly modify threat model.
Distributivity	Spread the risk.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Properties

- **Properties**
  - > **Self Identity**
    - Know what you are and what is not.
  - > Diversity
    - Maintain different structure and configurations.
  - > Autonomy
    - Maintain different structure and configurations.
  - > Multi-layered
    - Maintain different structure and configurations.
  - > Resilience
    - Maintain different structure and configurations.
  - > Anomaly detection.
    - Maintain different structure and configurations.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Properties

- **Properties**
  - Self Identity
    - Know what you are and what is not.
  - **Diversity**
    - **Maintain different structure and configurations.**
  - Autonomy
    - Maintain different structure and configurations.
  - Multi-layered
    - Maintain different structure and configurations.
  - Resilience
    - Maintain different structure and configurations.
  - Anomaly detection.
    - Maintain different structure and configurations.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Properties

- **Properties**
  - > Self Identity
    - Know what you are and what is not.
  - > Diversity
    - Maintain different structure and configurations.
  - > **Autonomy**
    - **Maintain different structure and configurations.**
  - > Multi-layered
    - Maintain different structure and configurations.
  - > Resilience
    - Maintain different structure and configurations.
  - > Anomaly detection.
    - Maintain different structure and configurations.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Properties

- **Properties**
  - > Self Identity
    - Know what you are and what is not.
  - > Diversity
    - Maintain different structure and configurations.
  - > Autonomy
    - Maintain different structure and configurations.
  - > **Multi-layered**
    - **Maintain different structure and configurations.**
  - > Resilience
    - Maintain different structure and configurations.
  - > Anomaly detection.
    - Maintain different structure and configurations.

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security - Properties

- **Properties**
  - > Self Identity
    - Know what you are and what is not.
  - > Diversity
    - Maintain different structure and configurations.
  - > Autonomy
    - Maintain different structure and configurations.
  - > Multi-layered
    - Maintain different structure and configurations.
  - > **Resilience**
    - **Maintain different structure and configurations.**
  - > Anomaly detection.
    - Maintain different structure and configurations.

Copyright © 2008 Sun Microsystems, Inc.

Properties

- **Properties**
  - > Self Identity
    - Know what you are and what is not.
  - > Diversity
    - Maintain different structure and configurations.
  - > Autonomy
    - Maintain different structure and configurations.
  - > Multi-layered
    - Maintain different structure and configurations.
  - > Resilience
    - Maintain different structure and configurations.
  - > **Anomaly detection.**
    - **Maintain different structure and configurations.**

Copyright © 2008 Sun Microsystems, Inc.

Mapping of Objectives and Principles

Reduce threat amplification and reduce threat velocity	Dynamic threat response, intersystem communication
Reduce attack surface	Limit external interfaces, quarantine
Reduce remediation time	Redundant systems, auto-recovery
Ensure correctness	Integrity tests of data and processing resources

Copyright © 2008 Sun Microsystems, Inc.

Immutable Service Containers

- ISC concept addresses various adaptive security principles.
- Must be built within the context of a larger adaptive security model.

Copyright © 2008 Sun Microsystems, Inc.

Immutable Service Containers

- Benefits
  - Operational efficiency
    - faster deployment
    - faster re-purposing
  - Security via compartmentalization

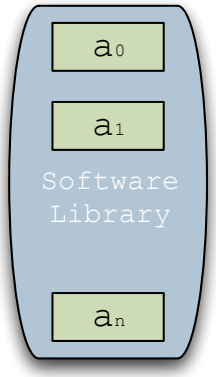
Copyright © 2008 Sun Microsystems, Inc.

Immutable Service Container Requirements

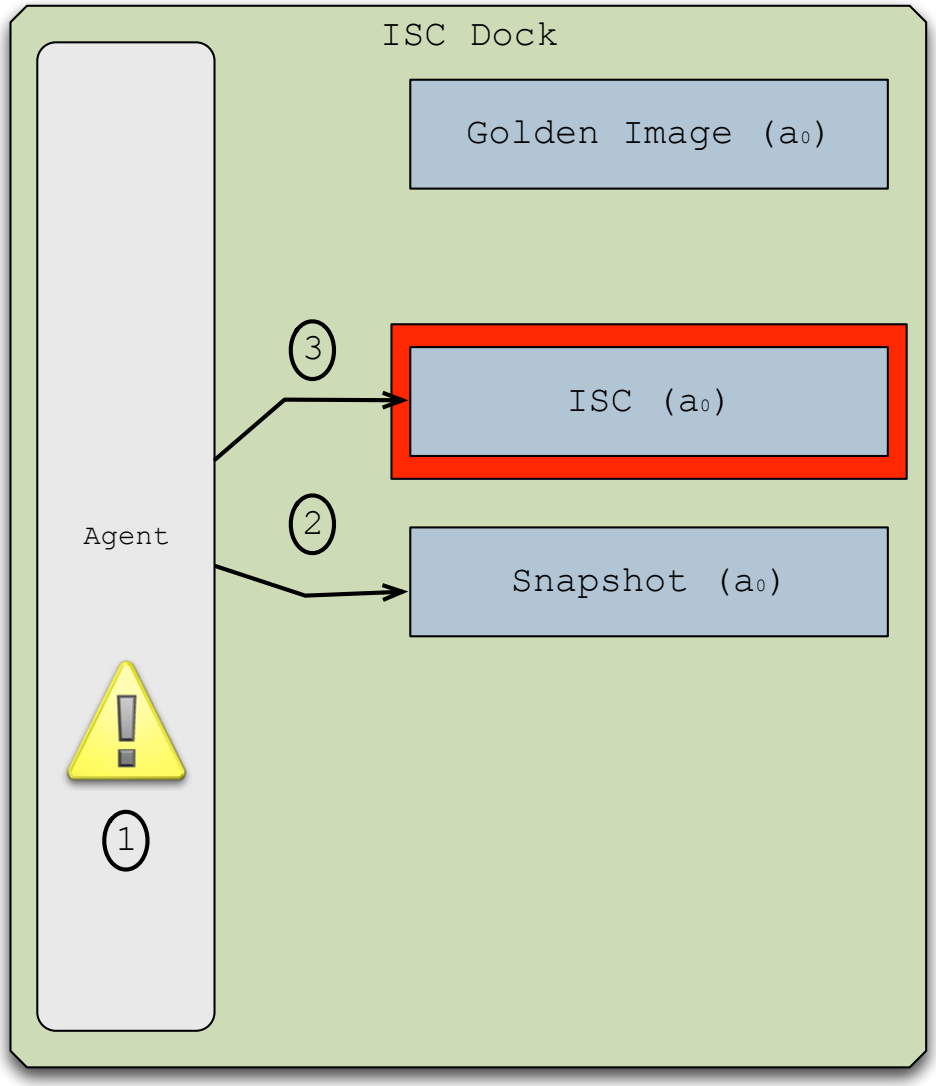
- Service is only network port exposed.
- Service is running with unique credentials.
- Service is running with least privilege.
- Service software is read-only.
- OS is running with reduced privileges.
- Most OS software is read-only.

Copyright © 2008 Sun Microsystems, Inc.

Self Quarantine



1. Agent is alerted to take a self-quarantine action in response to a security event.
2. Agent creates a forensic snapshot of the ISC for later analysis.
3. Agent isolates the running ISC with a host-based firewall or other containment mechanism.



Copyright © 2008 Sun Microsystems, Inc.

Resources

- A Software Framework for Autonomic Security in Pervasive Environments A. Saxena et al 2007
- An Immunity-Based Dynamic Multilayer Intrusion Detection System G. Liang 2006
- Artificial Immune Systems: A New Computational Intelligence Approach, L. de Castro 2002
- Autonomic Risk Management for Critical Infrastructure Protection , M. Ulieru 2006
- BeeAIS: Artificial Immune Systems Security for Nature Inspired, MANET Routing Protocol, BeeAdHoc N. Mazhar 2007
- Information Immune Systems, D. Chao 2002
- Use of Trust Vectors for CyberCraft and the Limits of Usable Data History for Trust Vectors, M. Stevens et al 2007

Copyright © 2008 Sun Microsystems, Inc.

Adaptive Security Architecture – New Models for a New World

"The central enemy of reliability is complexity..... Prevention of insecure operating modes in complex systems is difficult to do well and impossible to do cheaply: The defender has to counter all possible attacks; the attacker only has to find one unblocked means of attack." Dan Geer et al

The Problem

Our customers are constantly challenged with new threats that increase the complexity and reduce the trustworthiness, reliability, availability, security and integrity of their IT systems. Our customers rely upon their IT systems to run and grow their business; and if they are unable to trust those systems, their business will fail.

As complexity increases, security and integrity decrease.
A monoculture of systems is at risk of a pandemic.
Attacks are developed faster that defensive responses.

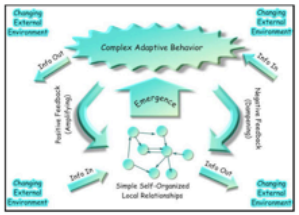
Value Proposition

The Adaptive Security Architecture approach helps customers to realize benefits such as:

Reducing threat amplification. (i.e., reduce cascading failures in mono-cultures)
Reducing attack surface. (make the target smaller)
Reducing attack velocity. (slow the attack)
Reducing remediation time (respond to an attack faster)
Ensuring the availability of data and processing resources
Ensuring correctness of data and reliability of processing resources.

Origins of Adaptive Security

Adaptive Security is base in part on Complex Adaptive Systems Theory. as well as the convergence of biological and ecological systems.

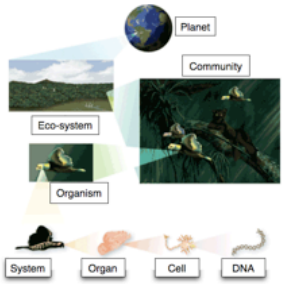


Adaptive Security Principles

Pattern recognition	Of normal and abnormal behavior
Uniqueness	No monoculture
Self identity	No what you are and what is not.
Diversity	Maintain different structure and configs.
Disposibility	Anything can be sacrificed.
Autonomy	No central control.
Multi-layered	Defense in depth.
No secure layer	Attacks can come from anywhere.
Noise tolerance	Specific match not needed to id threat.
Resilience	Continue to function in a reduced state.
Fault tolerant	Elements function complimentarily.
Robustness	Benefit of diversity and distributivity.
Immune learning and memory	Remember past threats.
Predator-prey response	Mediated and measured response.
Self organization	Remember successful threat responses.
Interation with other systems	Use common communications protocols.
Anomoly detection	Recognize out of norm conditions.
Dynamic changing coverage	Regularly modify threat model.
Distributivity	Spread the risk.

Complex adaptive systems are diverse and composed of multiple elements and adaptive as they utilize positive and negative feedback to enable modifications.

Immune systems, economies, ecosystems and ant colonies are examples of Complex Adaptive Systems.



What is Adaptive Security?

Adaptive security is:

Adaptive security relies upon the basic notion of "self" and "non-self" in that a system must be capable of understanding and recognizing what is normal system behavior and what is not; and what is not then may be a potential threat. Thus the two primary factors of adaptive security processing involved threat detection and then threat response. Our fundamental approach is to threat detection and response is:

- Telemetry – (monitoring)
- Correlation – (evaluating telemetry)
- Response – (perform some action)

An adaptively secure infrastructure must exhibit the following characteristics:

Flexibility and able to adaptively respond to new and different threats.
Self detecting, self regulating, self healing and self protecting.

Able to learn about norms related to the ecosystems and detect unauthorized modifications to data, files, file systems, operating systems, and configurations; and then:

- quarantine them so that forensics can be done and the ecosystem can learn from the breach while,
- resources are provisioned to take the place of the affected systems to ensure continuity of service.
- apply corrective measures as needed.

Uses a standardized security model that includes enforcement mechanisms to ensure compliance to a security policy.

Biological systems react to threats by adapting or dying. Biological system responses are typically focused at a microscopic level via various capabilities including immunological responses. The immunological capabilities of biological systems are autonomic in nature and have the ability to recognize and remember threats and to mount a rigorous attacks each time the threat is encountered.

Ecological systems on the other hand function at a macroscopic level. Ecological systems are comprised of many different disparate elements including individual biological entities. They react to threats by relying upon the diversity and autonomy of the elements that make up the ecosystem as well as their ability to adapt. This has the affect of spreading the risk presented by a threat to the larger ecosystem and increases its overall survivability.

joel.weise@sun.com
glenn.brunette@sun.com
650 352-8491
877 870-2993

Sun Proprietary/Confidential: Internal Use Only

Copyright © 2008 Sun Microsystems, Inc.

Thank you!

Joel Weise
joel.weise@sun.com