Security Testing — Status Report

Dr. Sajjan G. Shiva
Professor and Chair
Department of Computer Science
University of Memphis
Memphis, TN, USA

Potential attack targets in a system

- Network
  - identify security vulnerabilities on externally accessible network-connected devices such as firewalls, servers, and routers.
- Web application
  - identify vulnerabilities and abnormal behavior within the applications.

Potential attack targets in a system

- Database
  - identifying vulnerabilities in system's databases
  - due to incorrect configuration of the database security parameters or improper implementation of the business logic used to access the database
- Security subsystem
  - identify security vulnerabilities in specific subsystems

Types of security testing

- Vulnerability scanning
- Security scanning
- Penetration testing
- Risk assessment
- Security auditing
- Ethical hacking
- Posture assessment

Vulnerability scanning

- Network security
  - Nessus, OpenVAS, Core Impact, Nexpose, Microsoft Baseline Security Analyzer (MBSA), etc.
- Database security
  - DBAPPSecurity database vulnerability scanner (DAS-DBScan)
- Web application security
  - Acunetix

Security Scanning

- Network security
  - NetScanTools
- Database security
  - McAfee Security Scanner for Databases, Repscan™ 3.0
- Web application security
  - AppScan

Penetration Testing

- Network security
  - BackTrack Linux – Penetration Testing Distribution
- Database security
  - McAfee Security Scanner for Databases
- Web application security
  - Arachi

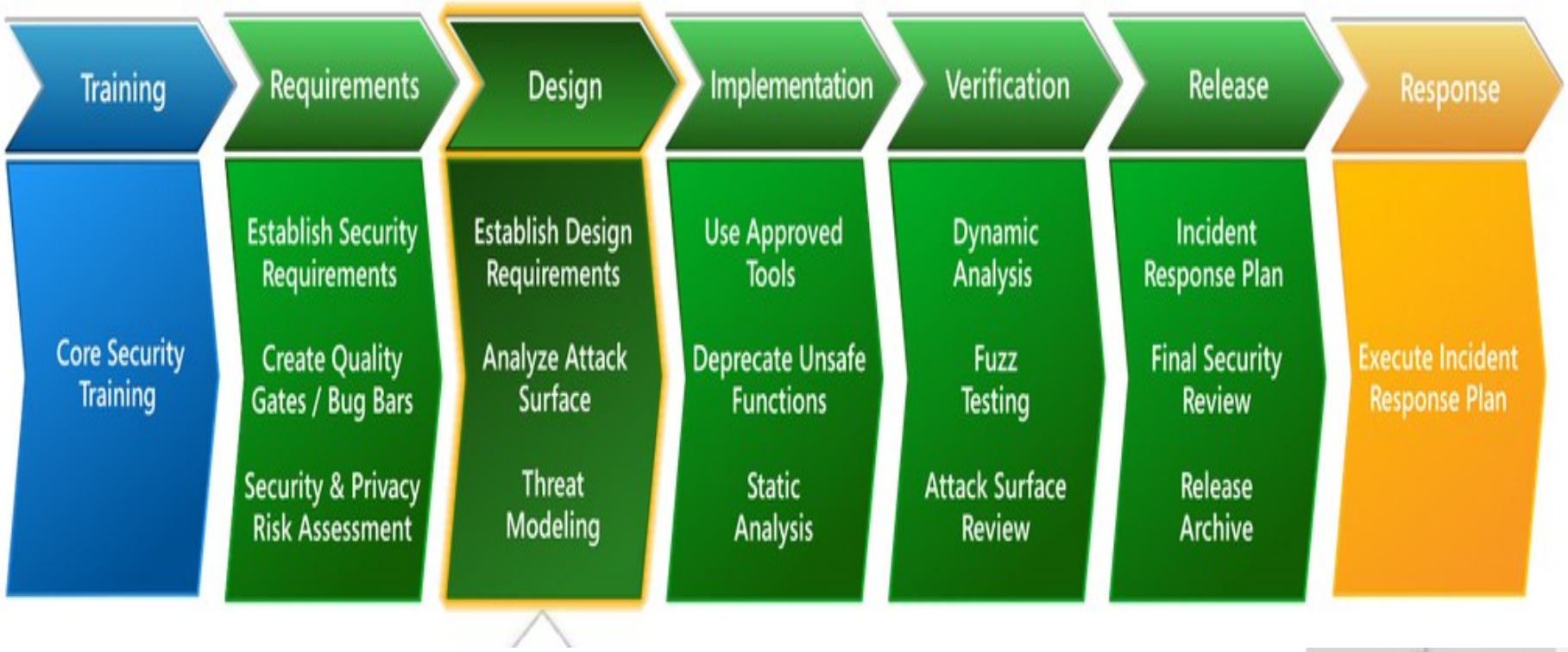
Risk Assessment

- Network security
  - Microsoft Security Assessment Tool (MSAT)
- Database security
  - SecureSphere: Discovery and Assessment Server (DAS)
- Web application security
  - WebScarab

Security Auditing

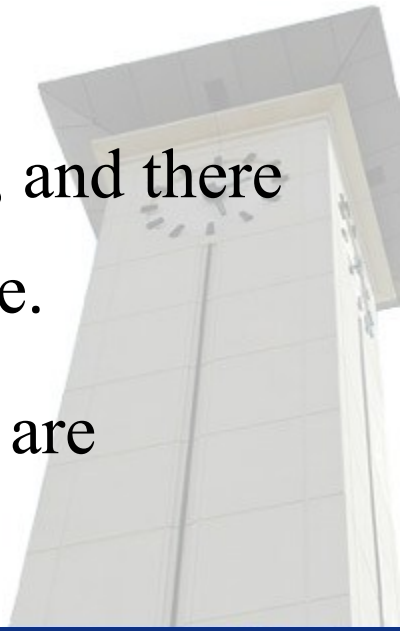
- Network security
  - Nsauditor Network Security Auditor
- Database security
  - SecureSphere: Database Activity Monitoring (DAM), DAS-DBAuditor: Database Auditor, DAS-LogAuditor: Log Auditor
- Web application security
  - Wapiti

Microsoft Security Development Lifecycle (SDL)



Are we safe?

- Significant research has been done by the research community and the industry to enhance security as a whole.
- SDLCs have evolved to incorporate secure coding and testing methodologies.
- Security testing is categorized into various types, and there are many tools available for performing each type.
- Newer testing tools are created every day, but so are attacks…



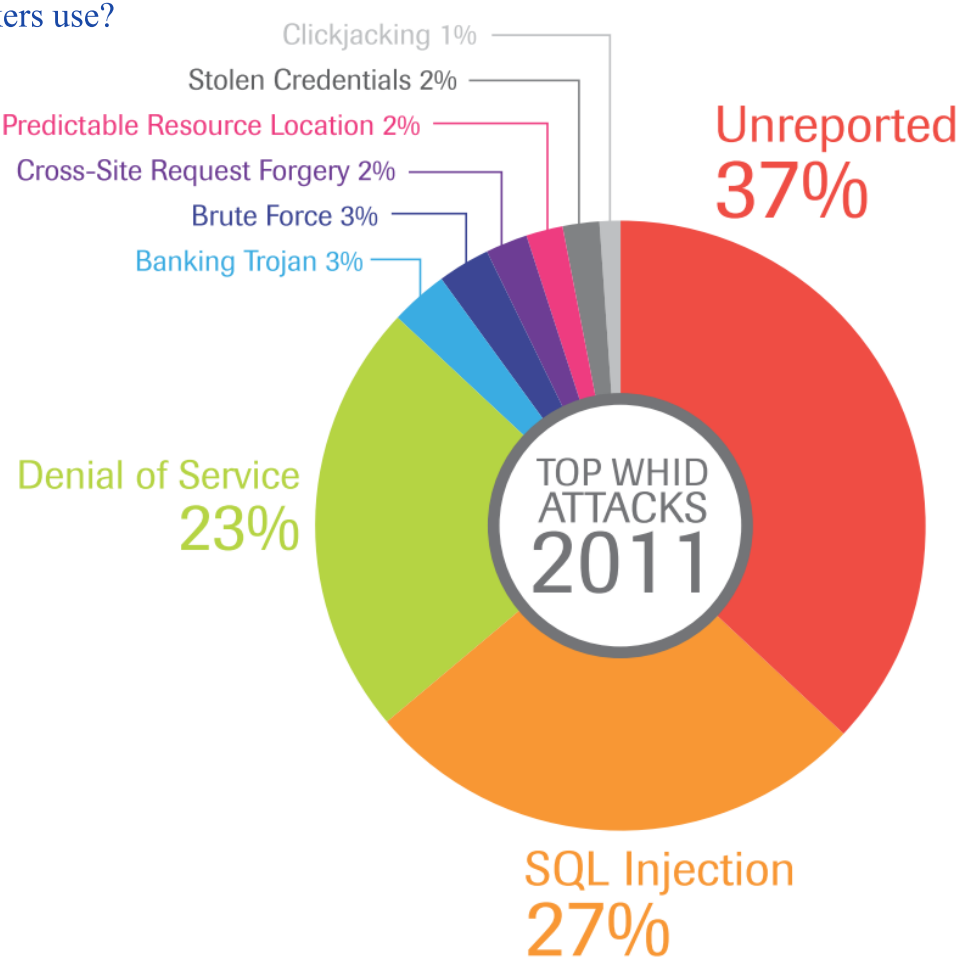
News articles in June 2012

- '*Flame*' Spreads via Rogue Microsoft Security Certificates; *Flame* authors order infected computers to remove all traces of the malware
- *LinkedIn* Password Breach Spawns Spam Campaign
- *Last.fm* warns users of password leak
- '*SwaggSec*' Claims Hack of China Telecom, Warner Bros.
- *Anonymous* Claims Attack on Facebook
- Dutch man charged with stealing credit cards

Trustwave Semiannual Report: The Web Hacking Incident Database

What attack methods do attackers use?

Period: 2011.

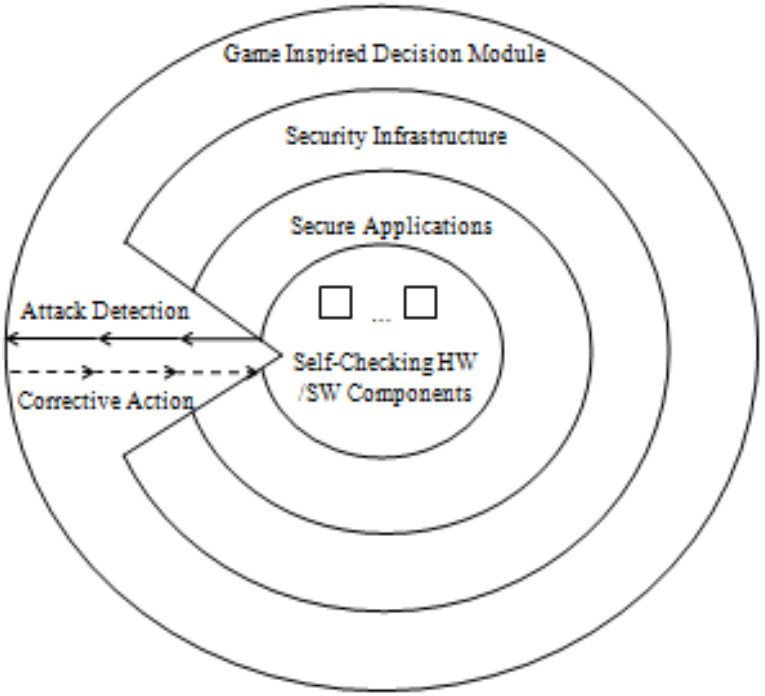


Source: https://www.**trustwave**.com/downloads/WHID_**Semiannual_Report**_2011.pdf

Our Four-layer Holistic Security Scheme

We envision a 4-layer Holistic Security Scheme:

1. Self-Checking HW /SW Components (Innermost layer *"The core"*).
2. Secure applications (Second layer).
3. Traditional network security infrastructure (3rd layer).
4. Game Theory Inspired Defense (Outer layer).



Runtime Monitoring

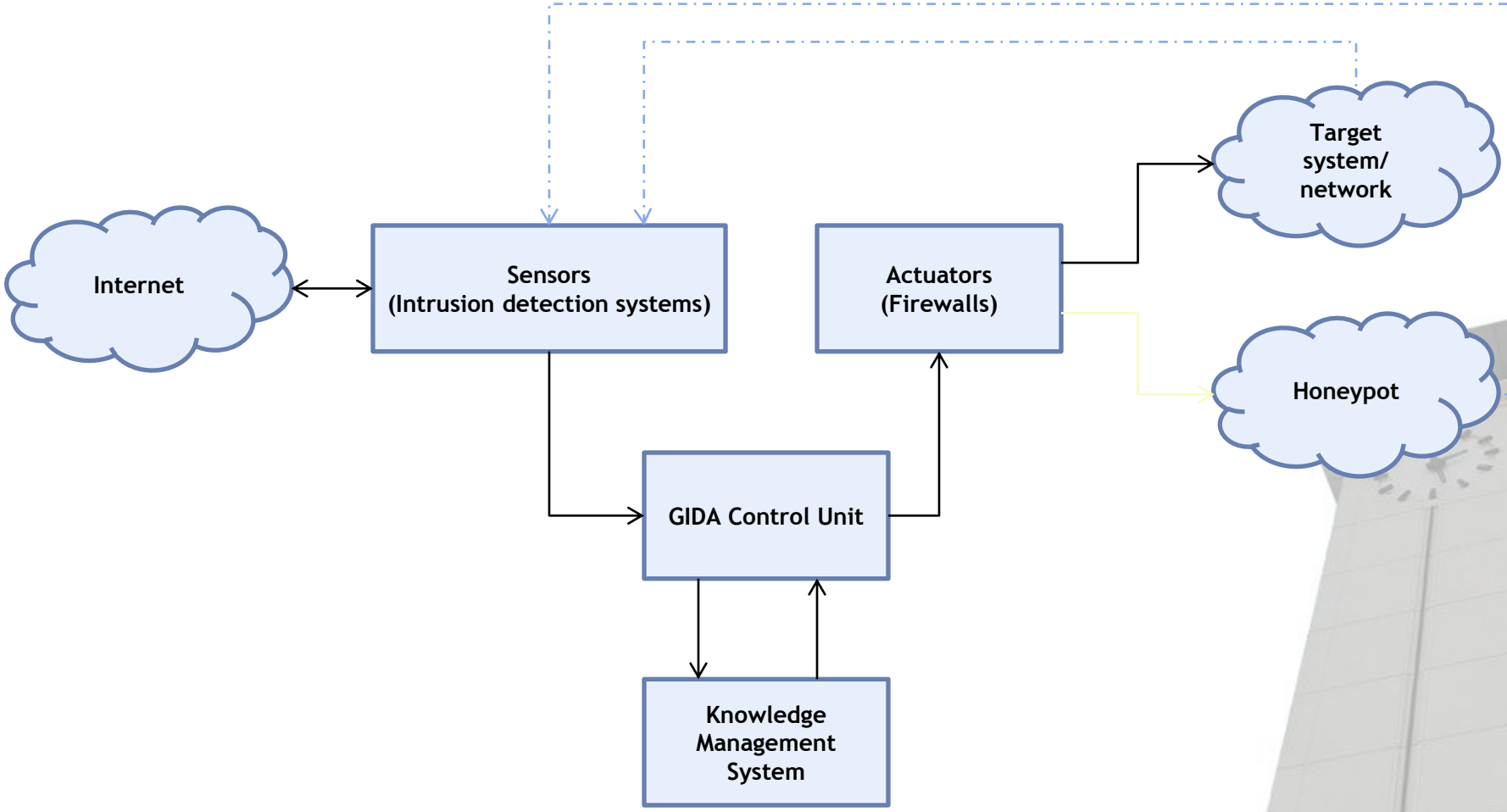
Why is it difficult to perform runtime monitoring of web applications?

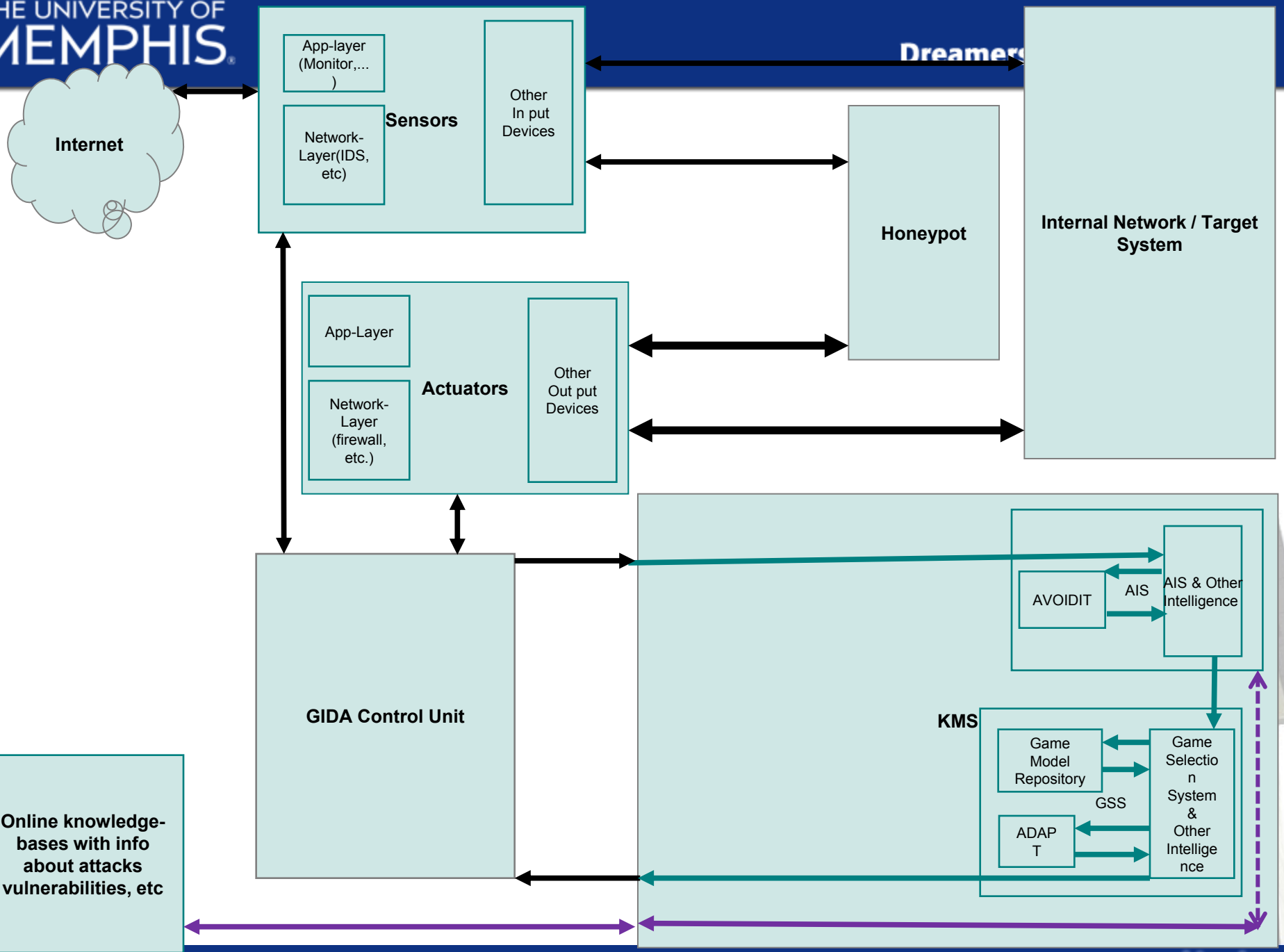
- Web applications can be compromised in numerous ways. Monitoring it in the real world is challenging.
- Estimating the extent to which the attack may affect the application is difficult.
- Identifying the possibility of the occurrence of an attack and deciding the appropriate defense mechanism is not trivial.

"Carrot and Stick" approach

- The Carrot and Stick approach refers to a policy of offering a combination of rewards and punishments to induce the adversary behavior.
- Using game theory, this defense approach can be modeled as a game between the defender and the adversary.

Game Inspired Defense Architecture (GIDA)




Internet
App-layer (Monitor,...)
Network-Layer(IDS, etc)
Sensors
Other In put Devices
Honeypot
Internal Network / Target System
App-Layer
Network-Layer (firewall, etc.)
Actuators
Other Out put Devices
GIDA Control Unit
AVOIDIT
AIS
AIS & Other Intelligence
KMS
Game Model Repository
GSS
ADAPT
Game Selection System & Other Intelligence
Online knowledge-bases with info about attacks vulnerabilities, etc

Questions?