Intrusion Tolerance – An Approach for Proactive Risk Management

Next Generation Security Technology

Current Research Funding: Lockheed Martin, Virginia CTRF/Northrop Grumman

Presentation to

4th Annual GFIRST Conference

Arun Sood Ph. D.

George Mason University

Department of Computer Science and Lab for Interdisciplinary Computer Science

http://cs.gmu.edu/~asood/scit

703.347.4494

International Cyber Center

- Proposed interdisciplinary center at GMU
- First event on March 14
  - Symposium on International Cyber Security Collaboration on Research and Development
  - EU and US Government, private sector presentations
  - http://cs.gmu.edu/~lics
- Cybercrime is not contained by national boundaries
- Illustrative center activities
  - Consolidation of data security compliance regs
  - State CERTs

SCIT: Self Cleansing Intrusion Tolerance

Next Generation Server Security Technology

Infrastructure Servers in DMZ

Short Transactions

Recent Reports

- Hackers Cracked Charities' Addresses and Passwords, NYT, 27Nov07
- Hackers hijack web search results, BBC, 29Nov07 http://news.bbc.co.uk/2/hi/technology/7118452.stm
- Foreign hackers seek to steal Americans' health records, www.govthealthit.com, 17Jan08
- Bush Order Expands Network Monitoring Intelligence Agencies to Track Intrusions, Washington Post, 26Jan08
- Bush Looks to Beef Up Protection Against Cyberattacks, WSJ, 28Jan08.
- Hacker steals Davidson Cos. clients' data, www.greatfallstribune.com, 30Jan08
- Government Computers Under Attack Authorities Are Making Plans To Protect Online Systems From Hackers, Spies And Terrorists, CBS News, 01Feb08

Intrusion Tolerance

- **Introducing SCIT, the Intrusion Tolerance System**
  - Optimizes application-specific exposure windows (AEW)
- **Targets "overexposed" applications (transactions)**
  - Focus initially on Websites, DNS,
  - Ongoing R&D Authentication (LDAP), Firewall and Single Sign On
  - Not targeted at applications with inherently long transaction times (FTP, VPN, etc)
- **Leverages virtualization technology to reduce intrusion risk and costs**
  - Reduces exposure time to limit intrusion losses
  - Adds time-based exposure control to intrusion prevention and detection solutions
    - SCIT is based on a new paradigm, but is easy to integrate with existing systems
  - New level of "Day-Zero" protection
- **Increases security through real-time server rotation and cleansing plus:**
  - Enhances security of high availability systems
  - Enables more flexible patch scheduling

SCIT Products

- SCIT deploys on existing servers - does not require additional physical servers
- SCIT is cost effective, uses virtualization technology and increases system security
- SCIT augments existing IPS and IDS solutions with limited incremental cost

Recent Multi-national Security Breach

- http://news.bbc.co.uk/2/hi/technology/7118452.stm
- “A huge campaign to poison web searches and trick people into visiting malicious websites has been thwarted.”

Recent Multi-national Security Breach

- http://news.bbc.co.uk/2/hi/technology/7118452.stm
- “A huge campaign to poison web searches and trick people into visiting malicious websites has been thwarted.”

- If a user searched Google for terms such as
  - "hospice", "cotton gin and its effect on slavery", "infinity" and many more
  - The first result pointed to a website from which malicious software was downloaded and embedded on user system.

Recent Multi-national Security Breach

- http://news.bbc.co.uk/2/hi/technology/7118452.stm
- “A huge campaign to poison web searches and trick people into visiting malicious websites has been thwarted.”

- If a user searched Google for terms such as
  - "hospice", "cotton gin and its effect on slavery", "infinity" and many more
  - The first result pointed to a website from which malicious software was downloaded and embedded on user system.

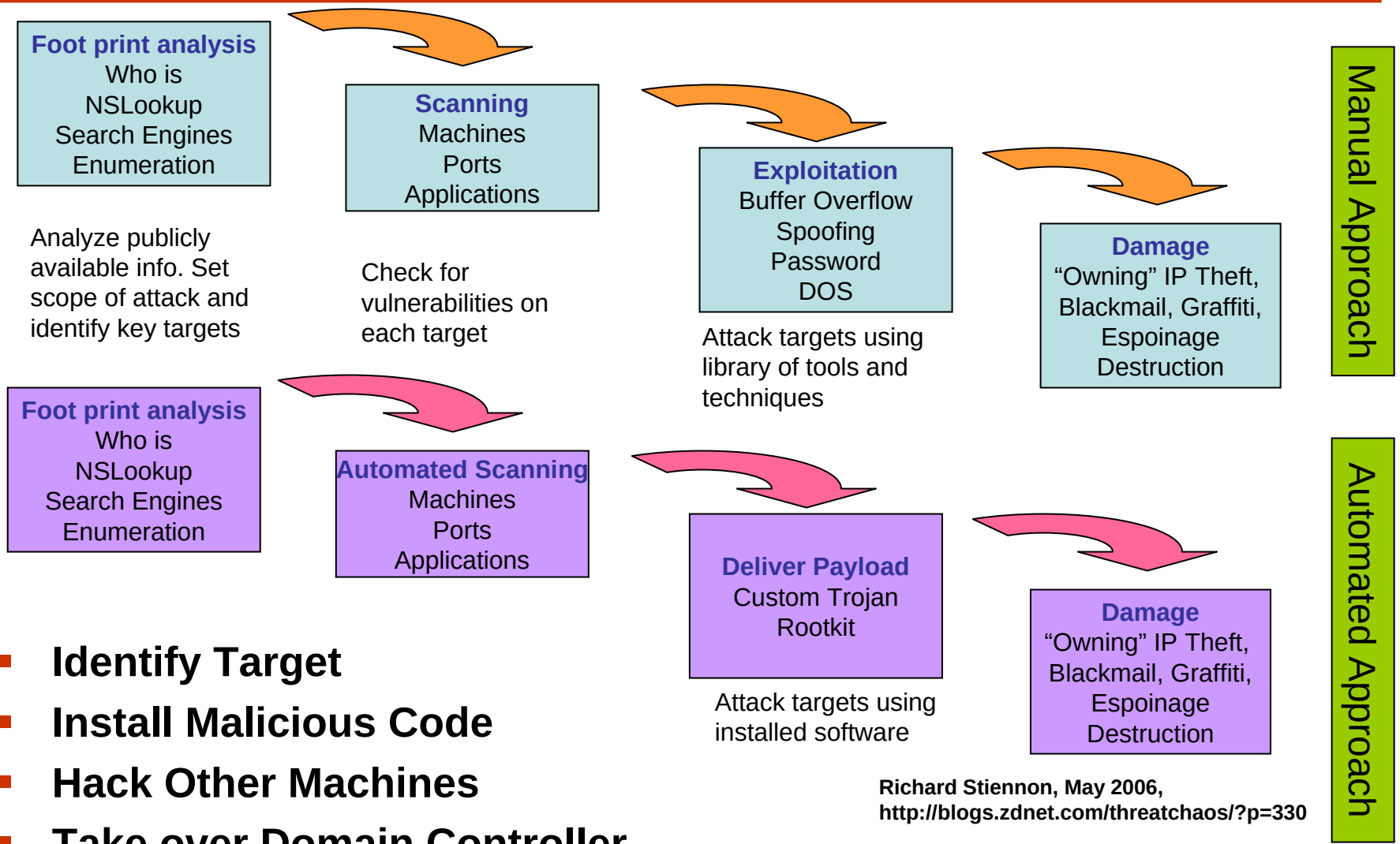
- Criminals in country A created domains that were mostly bought by companies in country B and hosted in country C. Tens of thousands of domains were used.

Recent Multi-National Security Breach

- http://news.bbc.co.uk/2/hi/technology/7118452.stm
- “A huge campaign to poison web searches and trick people into visiting malicious websites has been thwarted.”
- If a user searched Google for terms such as
  - "hospice", "cotton gin and its effect on slavery", "infinity" and many more
  - The first result pointed to a website from which malicious software was downloaded and embedded on user system.
- Criminals in country A created domains that were mostly bought by companies in country B and hosted in country C. Tens of thousands of domains were used.

- These domains tricked the indexing strategy of Google to believe that these web pages were good and reliable source of information.

Anatomy of an Hack



- **Identify Target**
- **Install Malicious Code**
- **Hack Other Machines**
- **Take over Domain Controller**

Richard Stiennon, May 2006, http://blogs.zdnet.com/threatchaos/?p=330

Attacking a Multi-tier Architecture
Web-App-DB-Domain Controller

- **Step 1: Identify Target**
  - Network address ranges
  - Host names
  - Exposed hosts
  - Applications exposed on those hosts
  - Operating system and application version information
  - Patch state of both the host and of the applications
  - Structure of the applications and back-end severs
- **Step 2: Initial Compromise**
  - Web pages are always exposed – opportunity for ingress
- **Step 3: Elevate Privileges**
  - Become a privilege user – like internal user on the target system
- **Step 4: Hacking Other Machines**
  - Own the network.
- **Step 5: Take over Domain Controller**

Jesper Johansson and Steve Riley , Protect Your Windows Network: From Perimeter to Data, Addison-Wesley Professional, 2005.

How Does SCIT Provide Additional Security?

- SCIT servers
  - Regularly restored to a known state and remove malicious software installed by attackers.
  - Provide protection while manufacturer is developing a patch, i.e. SCIT servers are protected in the time period between vulnerability detection and patch distribution.
  - Gives data center managers an additional level of freedom in developing a systematic plan for patch management.

- SCIT DNS servers
  - Domain name / IP address mapping is protected from malicious alteration, thus avoiding improper redirection of the traffic.

- SCIT Web servers
  - Protect the corporate crown jewels, front ends for sensitive information, e.g. customer or employee data sets, and informational web sites.
  - Regularly restores the sites to known states, and makes it difficult for intruders to undertake harmful acts such as deleting files.
  - Avoid long term defacements.
  - Reduces the risk of large scale data ex-filtration.

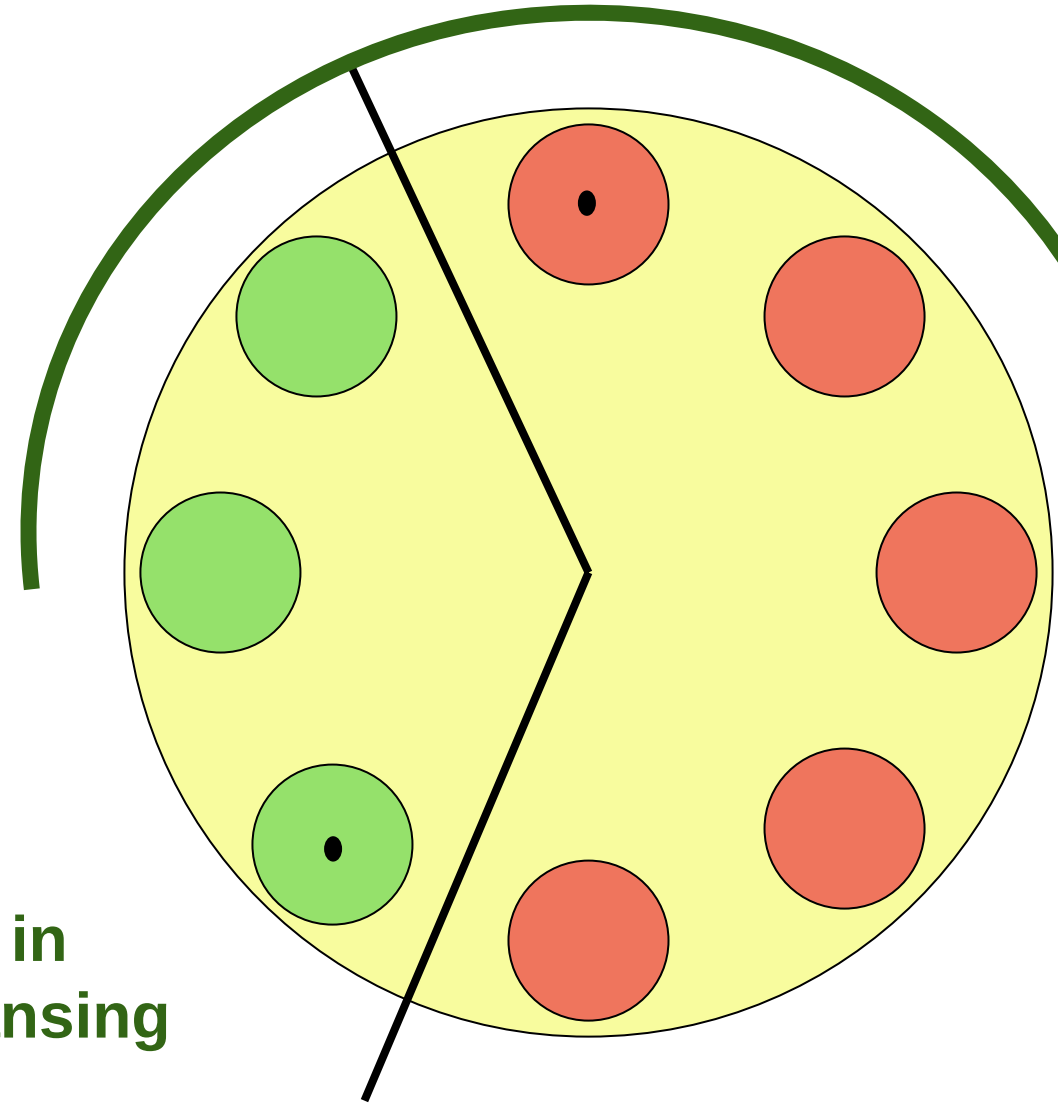
Comparison of IDS, IPS, IT

Issue	Firewall, IDS, IPS	Intrusion tolerance
Risk management.	Reactive.	Proactive.
A priori information required.	Attack models. Software vulnerabilities. Reaction rules.	Exposure time selection. Length of longest transaction.
Protection approach.	Prevent all intrusions. Impossible to achieve.	Limit losses.
System Administrator workload.	High. Manage reaction rules. Manage false alarms.	Less. No false alarms generated.
Design metric.	Unspecified.	Exposure time: Deterministic.
Packet/Data stream monitoring.	Required.	Not required.
Higher traffic volume requires.	More computations.	Computation volume unchanged.
Applying patches.	Must be applied immediately.	Can be planned.

Server Rotations

Example: 5 online and 3 offline servers

Servers
-Virtual
-Physical



Server Rotation

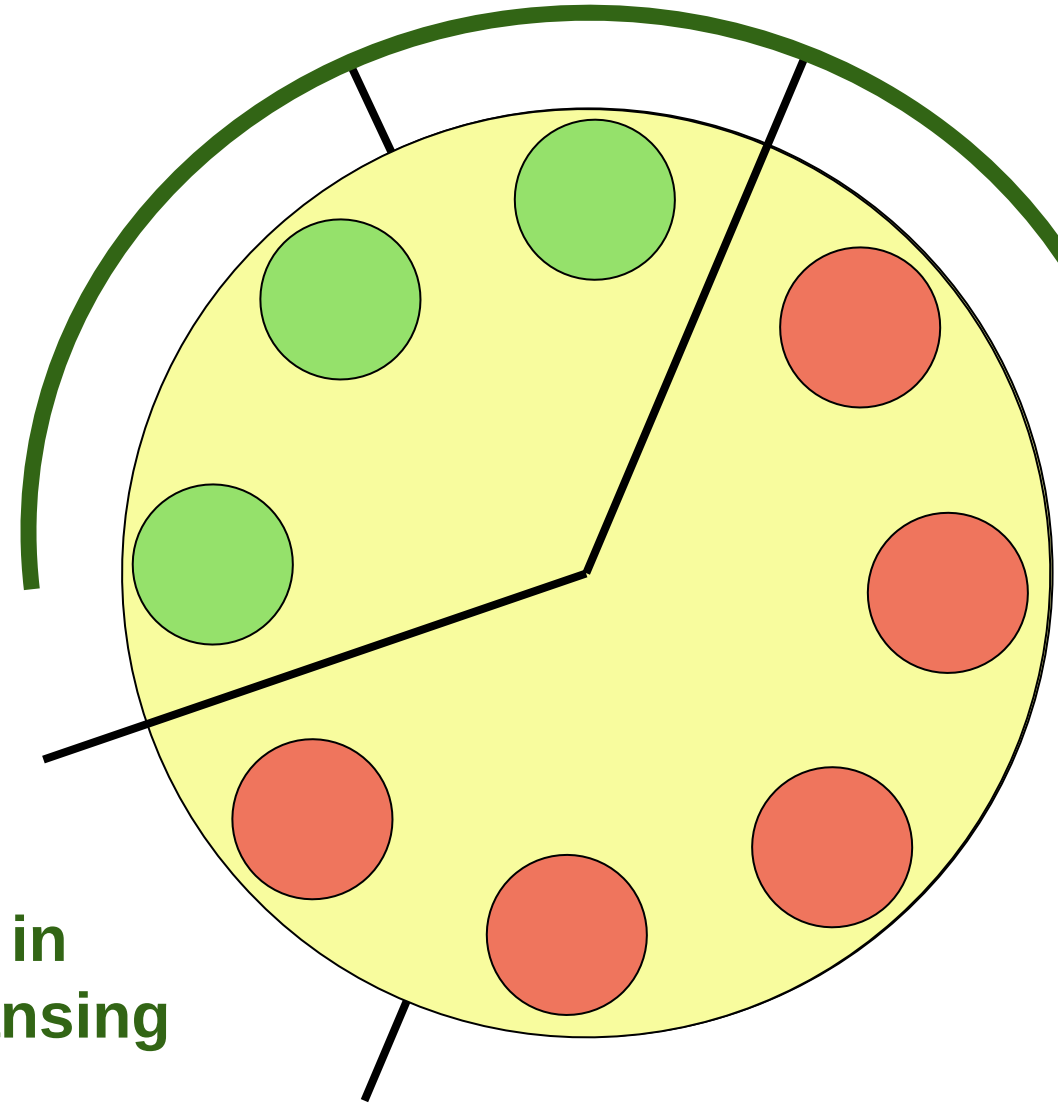
Online servers; potentially compromised

Offline servers; in self-cleansing

Server Rotations

Example: 5 online and 3 offline servers

Servers
-Virtual
-Physical



Server Rotation

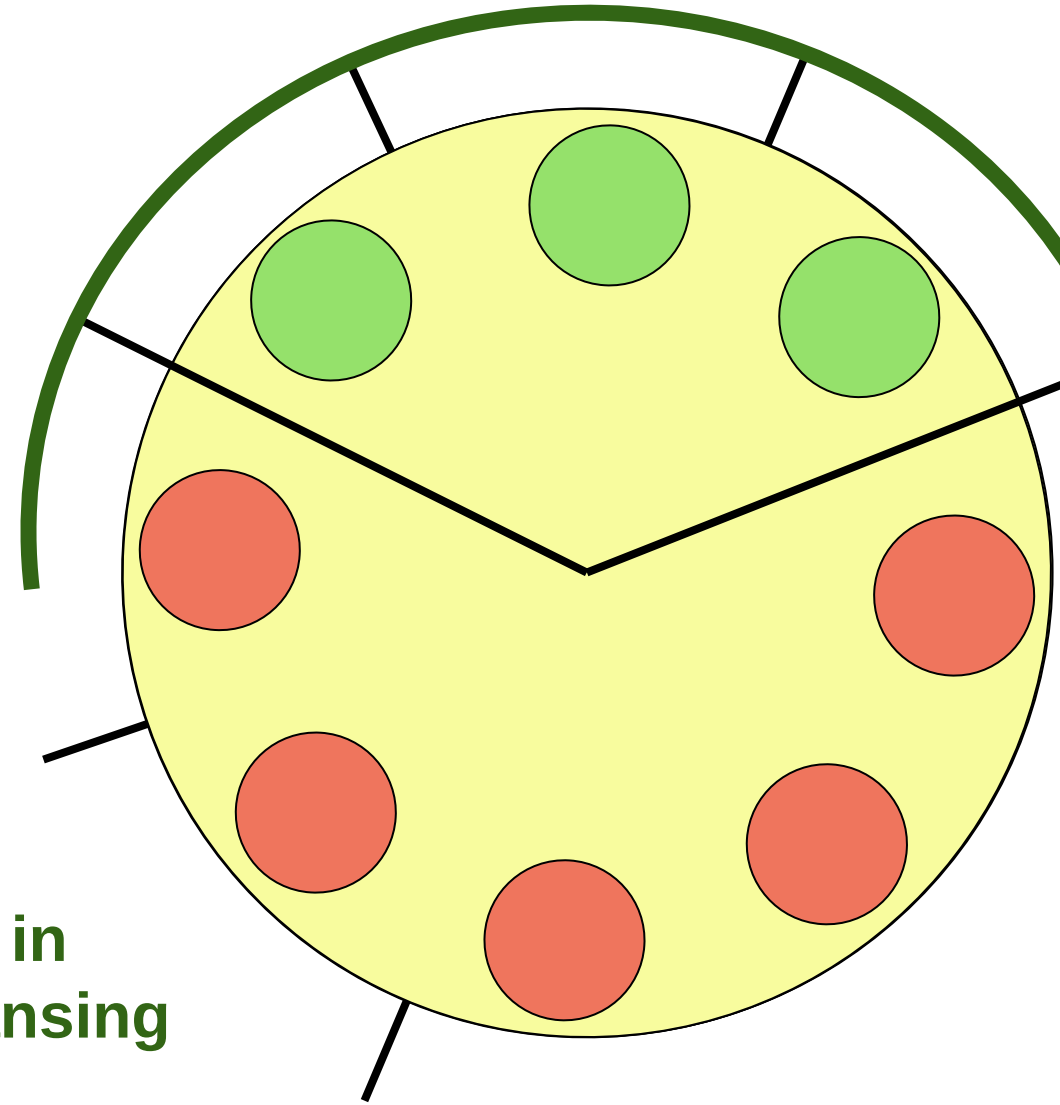
Online servers; potentially compromised

Offline servers; in self-cleansing

Server Rotations

Example: 5 online and 3 offline servers

Servers
-Virtual
-Physical



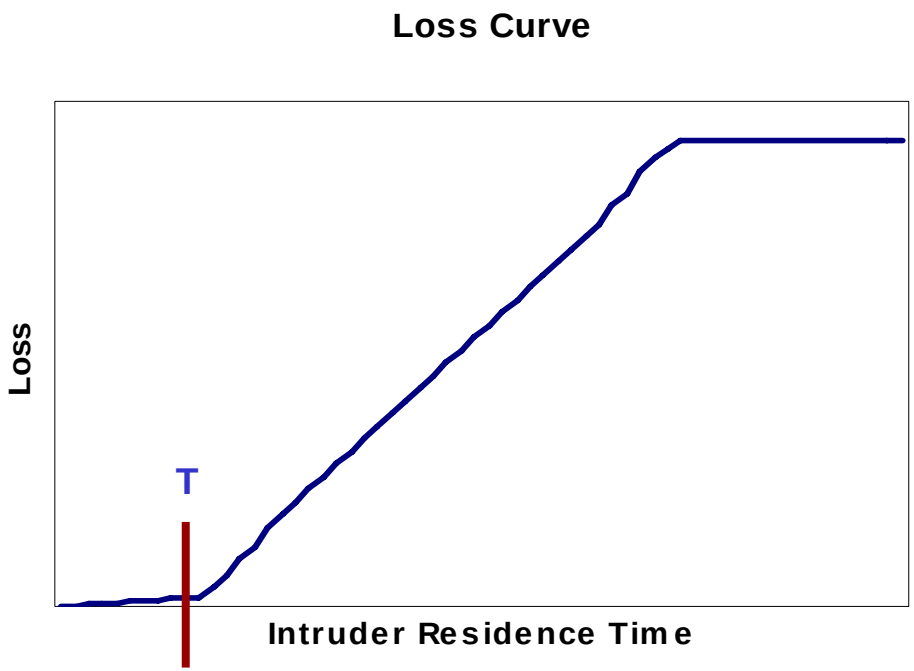
Server Rotation

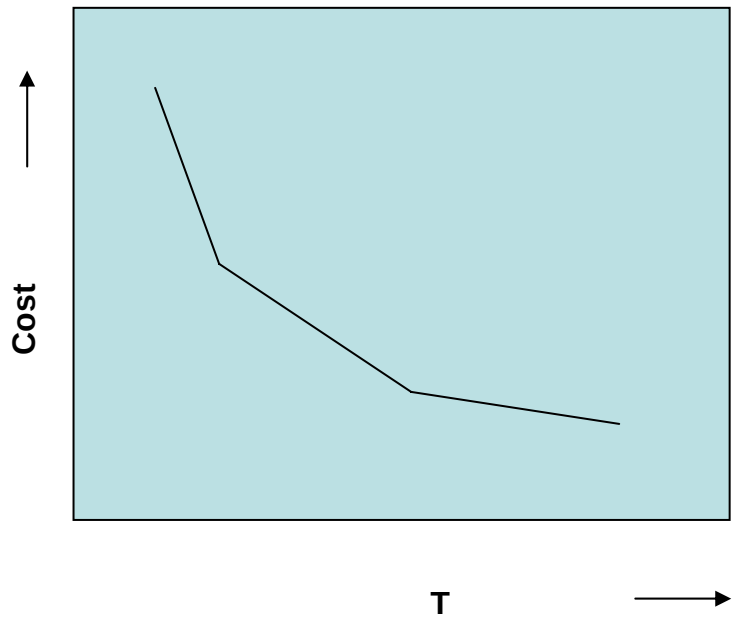
Online servers; potentially compromised

Offline servers; in self-cleansing

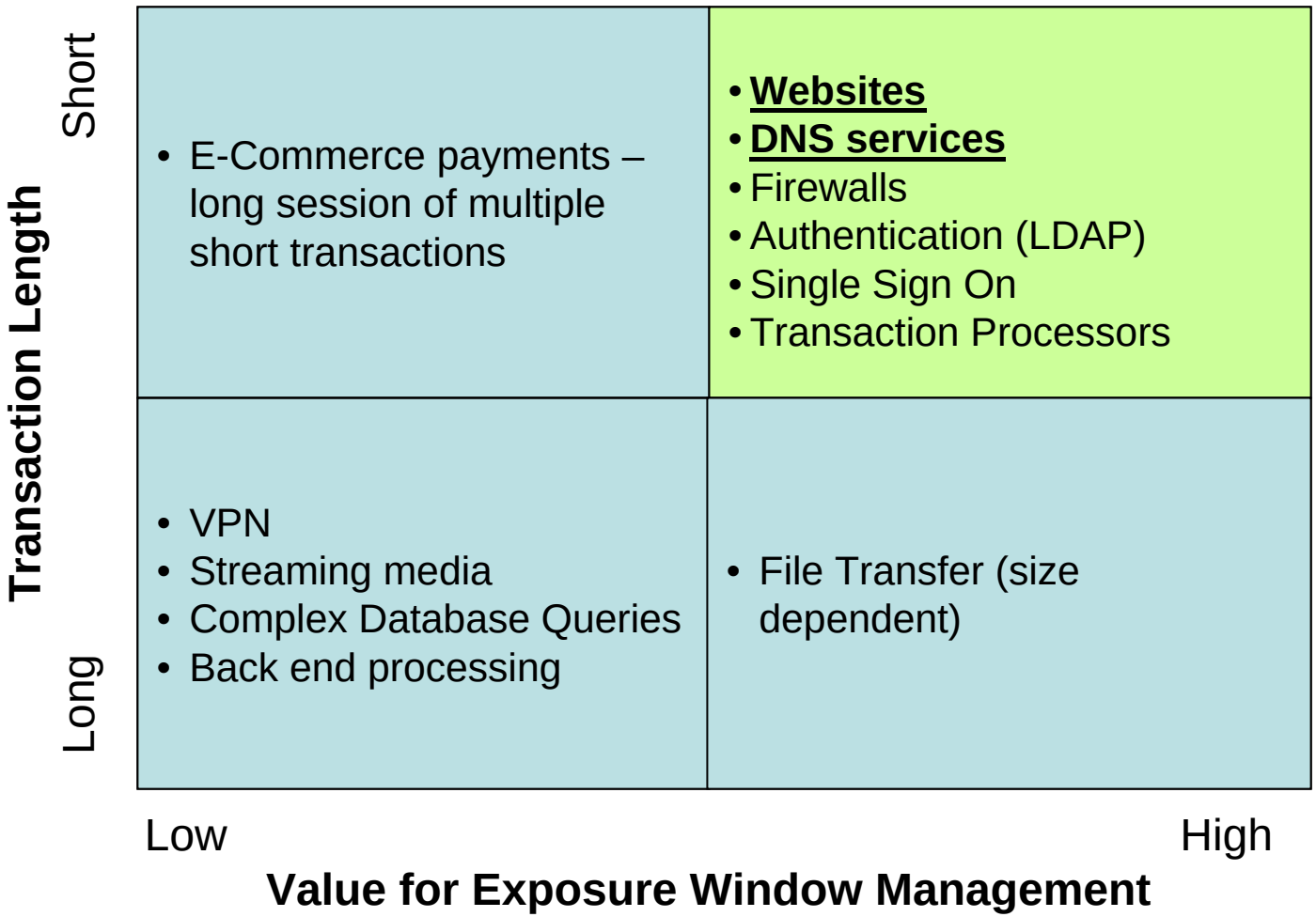
Intrusion Tolerance

- Increase security by reducing exposure window
  - Exposure window is the time a server is online between rotations
- Optimizes application-specific exposure windows (AEW)
- Decreasing available time for intrusion, reduces potential losses





Target Applications



Transaction Length in Multi-tier Architecture

Layer	Implementation	Transaction Length
Client Layer	Web site, DNS service	Short
Middle Layer	Authentication, Single Sign On	Short
	VPN, Streaming Media	Long
Back End Layer	Transaction Processing	Short
	File Access	Mixed
	Complex Database Queries	Long

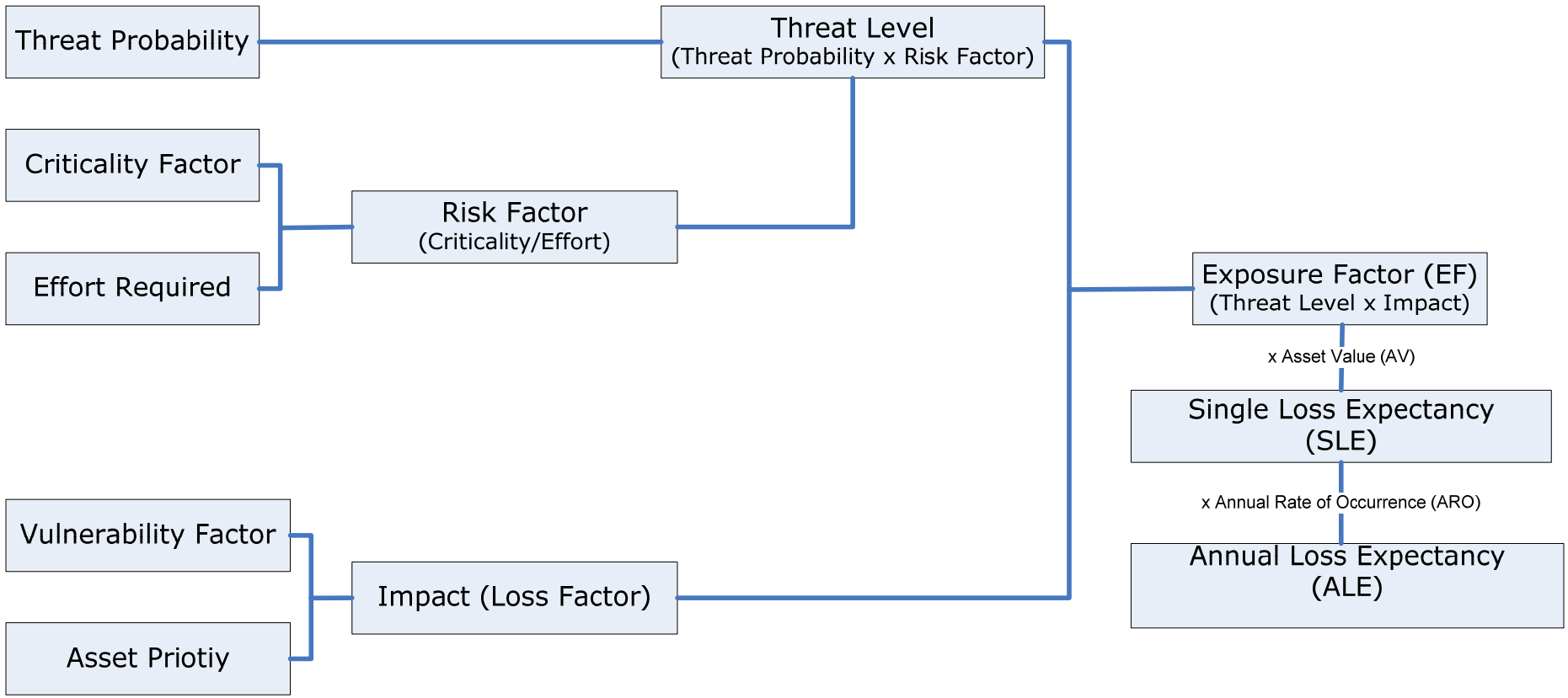
Exposure Time Reductions

Application	Current Server	SCIT Server
Websites – Windows Server	1 day to 3 month	60 seconds
Websites – UNIX Server	1 month to 6 months	60 seconds
DNS services – Linux Server	3 months to 1 year	30 seconds

In the following slides we show that:

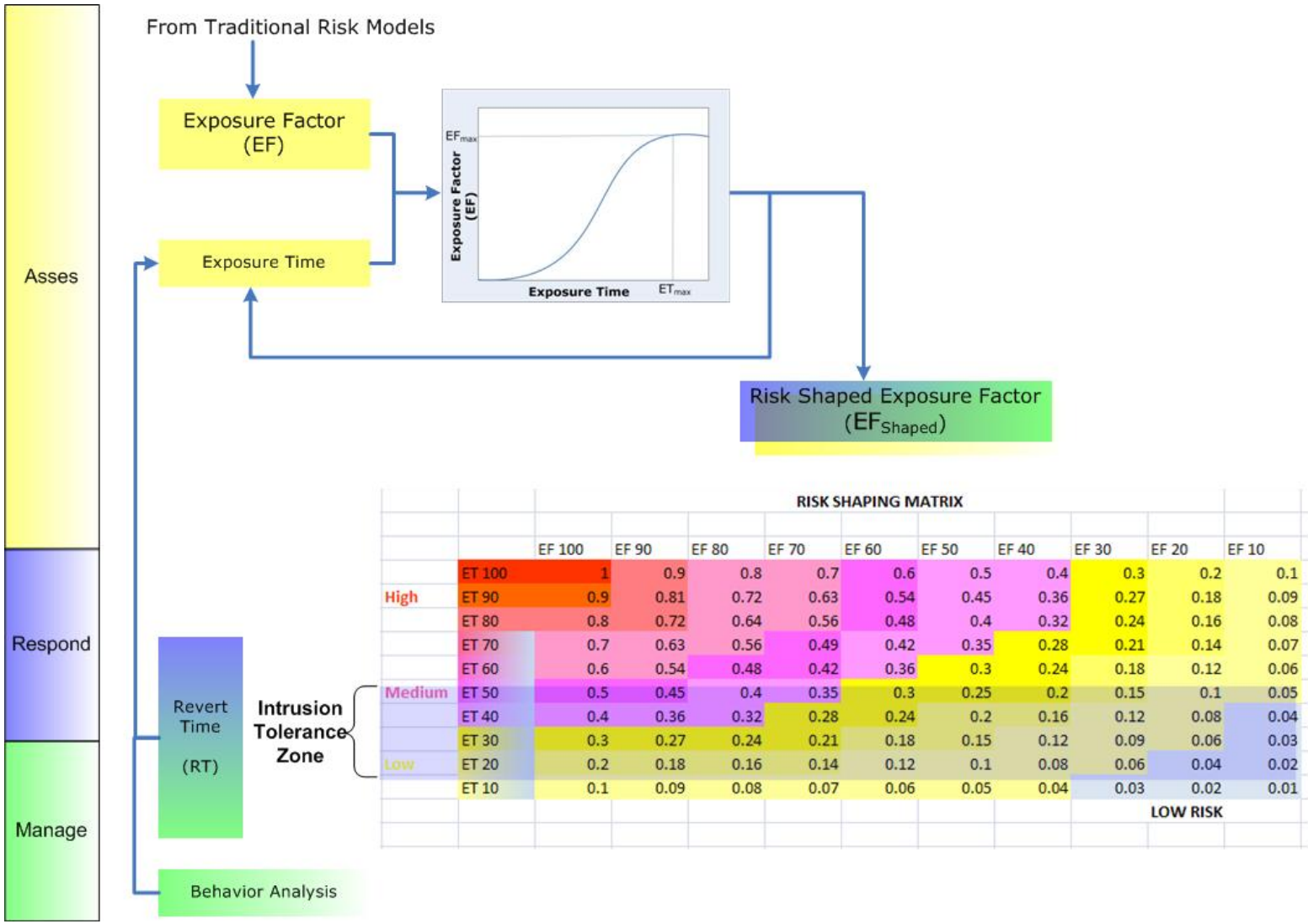
Reducing Exposure Time Significantly Reduces Expected Loss

Security Risk Assessment



Follows SecurityFocus.com (Symantec), Microsoft

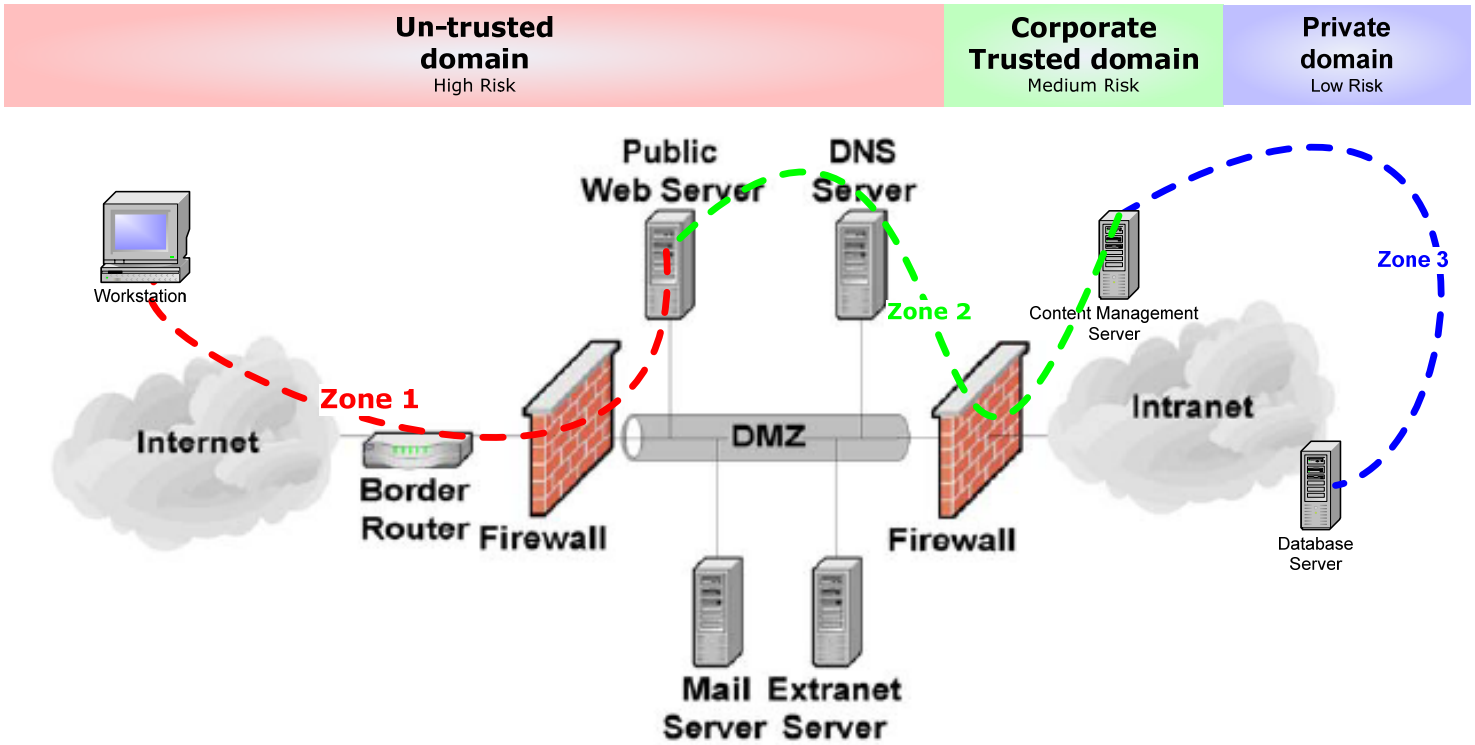
Risk Shaping by Exposure Time



RISK SHAPING MATRIX

		EF 100	EF 90	EF 80	EF 70	EF 60	EF 50	EF 40	EF 30	EF 20	EF 10
	ET 100	1	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1
High	ET 90	0.9	0.81	0.72	0.63	0.54	0.45	0.36	0.27	0.18	0.09
	ET 80	0.8	0.72	0.64	0.56	0.48	0.4	0.32	0.24	0.16	0.08
	ET 70	0.7	0.63	0.56	0.49	0.42	0.35	0.28	0.21	0.14	0.07
	ET 60	0.6	0.54	0.48	0.42	0.36	0.3	0.24	0.18	0.12	0.06
Medium	ET 50	0.5	0.45	0.4	0.35	0.3	0.25	0.2	0.15	0.1	0.05
	ET 40	0.4	0.36	0.32	0.28	0.24	0.2	0.16	0.12	0.08	0.04
	ET 30	0.3	0.27	0.24	0.21	0.18	0.15	0.12	0.09	0.06	0.03
Low	ET 20	0.2	0.18	0.16	0.14	0.12	0.1	0.08	0.06	0.04	0.02
	ET 10	0.1	0.09	0.08	0.07	0.06	0.05	0.04	0.03	0.02	0.01
										LOW RISK	

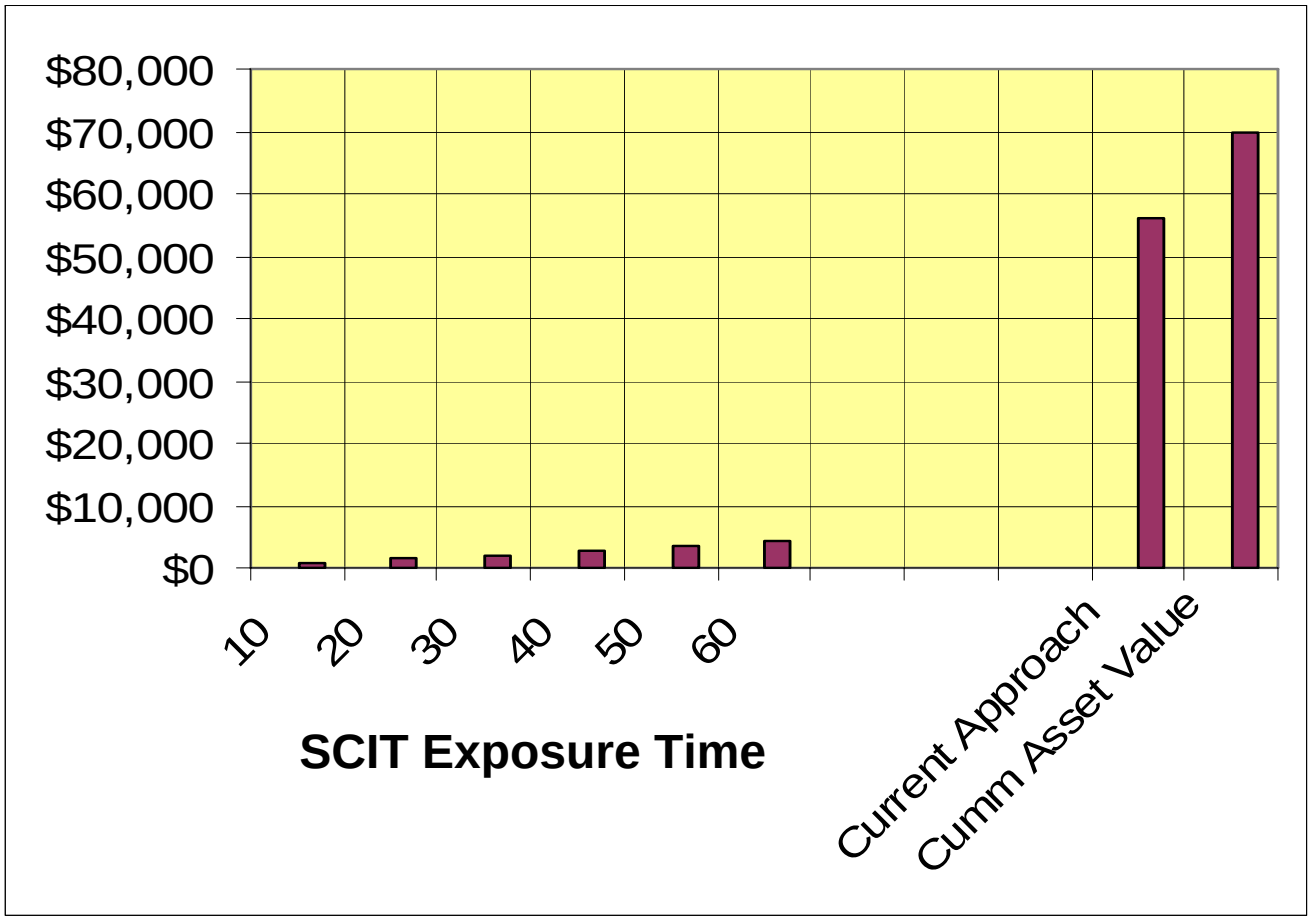
Multi Tier Example



SCIT vs Traditional Cumm Single Loss Expectancy

Multi Tier Architecture

Web server
DNS server
Content Manager
Database server



Reducing Exposure Time Significantly Reduces Expected Loss

Avoidance is Better Than Cleaning

- *You cannot clean a compromised system by*
  - *patching it*.
  - *removing the back doors*.
  - *using some vulnerability remover*.
  - *using a virus scanner*.
  - *reinstalling the operating system over the existing installation*.
- *You cannot trust*
  - *any data copied from a compromised system*.
  - *the event logs on a compromised system*.
  - *your latest backup*.
- *The only proper way to clean a compromised system is to flatten and rebuild*.

- CLEANING COMPROMISED SYSTEMS IS DIFFICULT. IT IS BETTER TO AVOID HACKING.

Case Study: Payment Card Industry

- Cost per exposed accounts (legal and professional fees, customer contact, post event clean up and improvements)
  - More than 1M accounts compromised: $50 per account
  - Few (1500) accounts compromised: $1500 per account
- Cost for protecting data – 100,000 customers

Method	$ per customer		Comments
	Year 1	Recurring	
Encrypt data at rest	$5	$1	Application Changes
Host IDS	$6	$2	False Alarm management
Continuous security audits	$3 - $4	$3 - $4	Vulnerability scanning

- **Bottom Line: Cost of exposed accounts >> Cost of protection**
- **Reducing Exposure Time provides additional layer of defense - makes it more difficult to exploit vulnerabilities and steal data.**

Source: Rapid 7 – Vulnerability Management Trends. Also Gartner Group

Comparison of IDS, IPS, IT

Issue	Firewall, IDS, IPS	Intrusion tolerance
Risk management.	Reactive.	Proactive.
A priori information required.	Attack models. Software vulnerabilities. Reaction rules.	Exposure time selection. Length of longest transaction.
Protection approach.	Prevent all intrusions. Impossible to achieve.	Limit losses.
System Administrator workload.	High. Manage reaction rules. Manage false alarms.	Less. No false alarms generated.
Design metric.	Unspecified.	Exposure time: Deterministic.
Packet/Data stream monitoring.	Required.	Not required.
Higher traffic volume requires.	More computations.	Computation volume unchanged.
Applying patches.	Must be applied immediately.	Can be planned.

Conclusion

- SCIT significantly reduces risk levels for targeted application using virtualization technology
- Augments existing IPS and IDS solutions with limited incremental cost
- Online at beta sites demonstrating protection for stored html pages website application
- Research issues: scalability, functionality under load, vulnerability assessment, penetration testing

SCIT Publications + Supporters + Contact Info

SCIT papers are available at
http://cs.gmu.edu/~asood/scit

Supported by
US Army, NIST, SUN Microsystems, *Lockheed Martin, CIT, CTRF/Northrop Grumman*

Beta Sites / Pilot Projects
XPAND, CACI, Lockheed Martin, Northrop Grumman

New International Center
IT Development and Security

Pending Issues and questions?

Arun Sood
asood @ scitlabs.com
asood @ gmu.edu
703.347.4494