Howard Shrobe
Program Manager, Information Innovation Office

Secure Computer Systems

DARPA Cyber Colloquium
Arlington, VA

November 7, 2011
Today’s Practice P4: Perimeter Protection, Patch & Pray isn’t Convergent with The Threat

- It’s not about better firewalls
- It’s not about better virus detection
- It’s not about better intrusion detection
- It’s not about better programmer practices

It’s about learning from biology and societies how to design secure, adaptive and resilient systems.
Humans Have Two Immune Systems: Innate and Adaptive

At least 20 – 30% of the body’s resources are involved in constant surveillance and containment.
Three Big Problems

1. Systems can be easily penetrated

2. Once penetrated, cleanup is prohibitively expensive, time-consuming, and unpredictable

3. If one system can be penetrated, then nearly all of them can
Mission-oriented Resilient Clouds

Using the power of a computational community to protect massively shared computational infrastructure

Your Software Lives Here

Your Software Lives On A Network with 100K Other Virtual Machines and No Firewalls

Modular Data Center Containers

Blade Server Racks

Blade Server Network

Approved for Public Release, Distribution Unlimited.
Resilient Clouds: A Community that uses the Network as a Defensive Amplifier

**TODAY**
Acting as individuals makes the enterprise weaker than the sum of its parts

- “Box” Oriented
- Vulnerable Components
- Static Sitting Duck
- Shared Vulnerabilities
- Implicit Trust is Amplifier

**RESILIENT CLOUDS (CRASH++)**
Acting as a community makes the enterprise stronger than the sum of its parts

- Mission Optimized
- CRASH-worthy components
- Moving Target
- Resilience through Diversity
- Collective Diagnosis is Damper

Approved for Public Release, Distribution Unlimited.
DARPA

Resilient Clouds Technology Areas

Combined Goal of CRASH & Resilient Clouds

Cyber-Mission Resilience

Resilient Clouds Technologies

Mission-Aware Networking

Innate Distributed Defense

Shared Situational Awareness, Trust Modeling, and Diagnosis

Optimizing Mission and Resources

Manageable & Taskable Diversity

CRASH Technologies

Innate Immunity

Adaptive Immunity

Manageable Diversity

For more info see: http://tinyurl.com/68w9wpf

Approved for Public Release, Distribution Unlimited.
Secure Computer Systems

CRASH

Clean-slate design of Resilient, Adaptive, Secure Hosts
CRASH Applies Biological Principles to Computation

I nnate Immunity:
New hardware & operating system architectures
that eliminate all common technical vulnerabilities

Adaptive Immunity
Middleware that:
• Diagnoses root causes of vulnerabilities and builds situational assessment
• Quickly adapts & reconfigures
• Learns from previous attacks and gets better at self-protection

Population Diversity
Computational techniques that:
• Increase entropy in time and space
• Make every system unique
• Raise work factor of attacker for each system
Innate Immunity: An Example Hardware Solution

Software and hybrid solutions are also possible (e.g. PROCEED)
Adaptive Immunity

1. Hardware analog of innate immune system detects anomaly.

2. Software system analog of adaptive immune system is signaled.

3. System model is used to perform diagnosis (e.g. localization and characterization).

4. System model is adapted with new attack-specific detector.

5. Adaptive immune system synthesizes plan to get around problem and patch to remove specific vulnerability.
Dynamic Diversity Makes a Single Host Different from Moment to Moment

Address Space Randomization

Code and/or data blocks are periodically repositioned in memory so that attacker has to work harder to find a target. Garbage-collected memory has the property inherently, new methods may optimize for increased entropy.

Instruction Set Randomization

<table>
<thead>
<tr>
<th>Disk</th>
<th>Memory</th>
<th>ICache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction-1</td>
<td>Encrypted-1</td>
<td>Instruction-1</td>
</tr>
<tr>
<td>Instruction-2</td>
<td>Encrypted-2</td>
<td>Instruction-2</td>
</tr>
<tr>
<td>Instruction-3</td>
<td>Encrypted-3</td>
<td>Instruction-3</td>
</tr>
<tr>
<td>Instruction-4</td>
<td>Encrypted-4</td>
<td>Instruction-4</td>
</tr>
<tr>
<td>Instruction-5</td>
<td>Injected-1</td>
<td>Encrypted-1</td>
</tr>
<tr>
<td>Instruction-6</td>
<td>Injected-2</td>
<td>Encrypted-1</td>
</tr>
</tbody>
</table>

Functional Redundancy & Decision Theoretic Dispatch

There are multiple methods for achieving each goal ("n-version programming"). Each distinct method has different qualities of service. Method selection is driven both by preferences over QoS and by need for unpredictability.

Code is encrypted as it enters memory and Decrypted as it enters the instruction cache (or translation buffer). Injected code in native instruction set is then encrypted and not executable. Encryption key can be varied by process and time.
Turn the Tables: Make The Attacker Do The Work

**Innate Immunity**
- Novel Hardware
- Separation OS’s
- Information Flow
- Formal Methods

**Adaptive Immunity**
- Policy Weaving
- Automatic Patching
- Selective Playback
- Symbiotes

**Dynamic Diversity**
- Compiler generated Diversity
- Algorithmic Diversity
- Instruction Set Randomization
An opportunity...
Smartphone > PC shipments within 2 years

Implies very rapid, land grab evolution of internet access

Global Unit Shipments of Desktop PCs + Notebook PCs vs. Smartphones, 2005 – 2013E

2012E: Inflection Point
Smartphones > Total PCs

Note: Notebook PCs include Netbooks. Source: IDC, Gartner, Morgan Stanley Research estimates.

Approved for Public Release, Distribution Unlimited.
...is to get CRASH & MRC technologies into \textit{your} machines.

- If you make computers, operating systems, middleware...
- If you use these and can influence the people who make them
- If you think there’s a great startup opportunity

- Then we want to talk with you about how to transition our technologies into the real world.
- Contact us at CrashInquiries@darpa.mil