

Using Honeyclients for Detection and Response Against New Attacks

Kathy Wang

703-983-6976 • knwang@mitre.org

Army MOIE

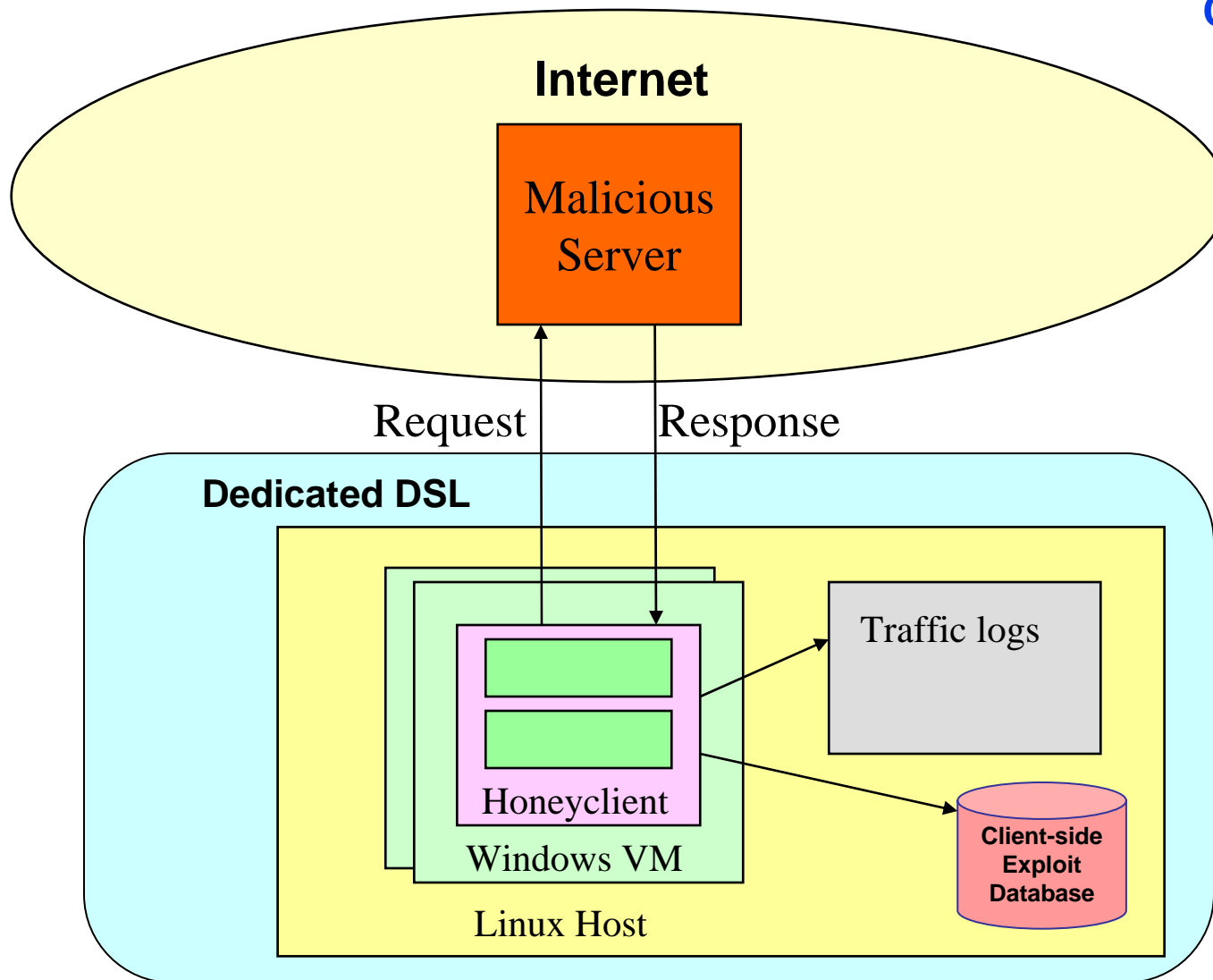


MITRE
Technology
Program

Problem

- **Attackers are becoming aware of honeyclient technology**
 - **Access to malicious Web site is blocked**
 - **Redirection to benign sites**
- **We need better honeyclient coverage of servers on the Internet**
 - **Find the bad guys before they find us**
 - **Interesting data correlation will be possible with distributed coverage**

Background



Honeyclient Prototype Capabilities

- 1) **Baseline integrity**
- 2) **Drive IE**
- 3) **Extract URLs**
- 4) **Recurse (internal)**
- 5) **Integrity checks**
- 6) **Recurse (external)**
- 7) **Virtual host**
- 8) **Protective firewall**
- 9) **Exploit DB**
- 10) **Image rotation**
- 11) **Modular clients**
- 12) **Traffic history**
- 13) **Secure logging**
- 14) **Memory checks**

MITRE

© 2007, The MITRE Corporation

Objectives

- **Extend our honeyclient technology to include capabilities to counter attackers**
- **Create capability to build distributed networks of honeyclients**
- **Gather and correlate data from honeyclients to gain comprehensive insights**

Activities

- **Detect kernel-modifying rootkits**
 - Analyze virtual hard drives outside of VM environment
- **Thwart exploits that detect virtual machine environments**
 - Add honeyclient capability for physical sandbox environment
- **Handle active content sites**
 - Be able to access and download content from these sites
- **Be difficult to distinguish from human activity**
 - Attackers now recognize and will actively counter honeyclients
- **Design and deploy distributed honeyclients**
 - This will result in much better coverage of the servers on the Internet

Highlight

- Link scoring (good vs. bad words, link location)
- Browsing order for links (breadth vs. depth)
- Bandwidth footprint (humans do not access links at the same speeds)

Honeyclient Intelligent Browsing Capability

MITRE--Applying Systems Engineering and Advanced Technology to Critical National Problems - Mozilla Firefox

http://www.mitre.org/

MITRE

About Us | Our Work | Employment | News & Events

Home | Site Map

Applying **Systems Engineering** and **Advanced Technology** to Critical National Problems.

MITRE manages three federally funded research and development centers (FFRDCs) and partners with government sponsors to support their critical operational missions and address issues of national importance.

- ▶ Aviation System Development
- ▶ Defense and Intelligence
- ▶ Enterprise Modernization

What's New at MITRE

News and Events

July 2006
[MITRE Executive Director Richard J. Byrne Awarded 2006 AFCEA Meritorious Award for Engineering](#)

[MITRE Wins Massachusetts Statewide Safety Award](#)

[Alfred Grasso Appointed MITRE President and CEO](#)

June 2006
[MITRE Engineer Receives Hobart Newell Award](#)

[MITRE Named to the "Best Places to Work in IT" List for Second Year in a Row](#)

[MITRE Opens Site in Baltimore](#)

[MITRE Receives Business Recycling Excellence Award](#)

Employment

July 2006
[MITRE's "Employee Spotlight" profiles Mike Talotta Alaska.](#)

The MITRE Digest

[What's in a Name? More Than You May Think](#)
June 2006
Nothing beats a human for translating foreign languages, but with the overwhelming amount of information out there, the role of machine translation is becoming ever more prominent. Learn how MITRE is working with the government's Foreign Language Program Office to choose the best tools for a tough job.

[Role of Unifying Disaster Response Rests on USNORTHCOM's Shoulders](#)
June 2006
MITRE is helping the U.S. Northern Command, or USNORTHCOM, to fulfill its mission of protecting our nation by upgrading communications systems and overhauling enterprise architectures.

[Zapping System Bugs Through Performance Engineering](#)
May 2006
Your home wasn't built without a master blueprint, so why are some hardware and software project components developed individually, only to fall short of big-picture performance goals? Learn how the practice of performance engineering is critical to the success of large-scale IT programs.

[A Trail of Bread Crumbs: Improving Radio Communications with Wireless Relays](#)
May 2006
Warfighters and rescue personnel operating in subterranean or urban environments often have difficulty maintaining radio contact. MITRE has designed small wireless relays that personnel can leave in a trail behind them to establish a path of multiple, short-range communication links.

[Read more Digest articles >>](#)

MITRE

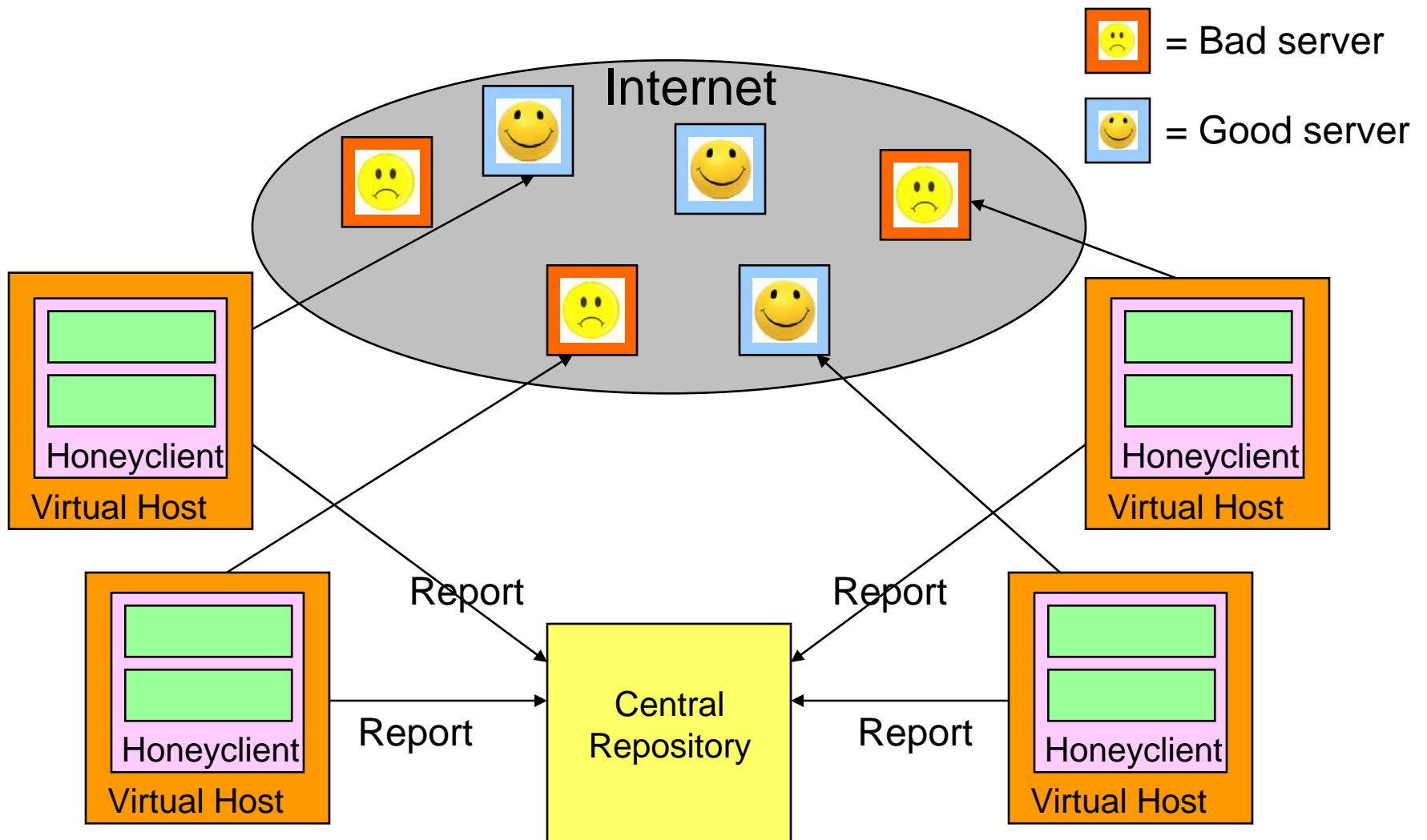
A National Resource Working in the Public Interest.
Copyright © 1997-2006, The MITRE Corporation. All rights reserved.
MITRE is a registered trademark of The MITRE Corporation.

[Privacy Policy](#)
[Contact Us](#)
[Printing Tips](#)

MITRE

© 2007, The MITRE Corporation

Highlight: Distributed Honeyclient Prototype



Impacts

- **We plan to pilot honeyclient technology for several sponsors**
- **Industry plans to run honeyclients**
- **Products and standards**
 - **Work with MITRE Common Vulnerabilities and Exposures (CVE) team to report new vulnerabilities**

Future Plans

Using Honeyclients to Detect Malicious Emails

