The Honeynet PROJECT®

The Honeynet Project®...improving the global security of the Internet

We all know computers, networks, and the Internet have introduced opportunities to the world that were never thought possible. However, as is true with any technology, these same opportunities also carry risks. Whether they are called "bad guys, insiders, hackers, criminals, or disgruntled employees," technology has provided individuals and organizations the means to compromise almost any resource in the world. These threats can launch attacks against systems and people whenever they want and however they desire.

> **The Honeynet Project is pure research. The stuff they produce is invaluable, and there's no other practical way to get it. When an airplane falls out of the sky, everyone knows about it. When a network is hacked, however, it almost always remains a secret.**
>
> Bruce Schneier
> Chief Technology Officer
> Counterpane Internet Security, Inc.

The Internet has created a global battlefield that spans not only governmental, military, and private enterprise sectors, but also the homes of millions of individual users around the world. Billions of dollars are being spent to protect against these threats, yet very little is known about the attackers – who they are, how they operate, or even what drives them to do what they do. To make the situation even more challenging, these threats are constantly changing, evolving, and advancing. Enter The Honeynet Project – an innovative organization creating noticeable earthquakes in technology security.

We've been improving the global security of the Internet since 1999 – free of charge to the public.

The Honeynet PROJECT®

The Honeynet Project®

The Honeynet Project is a non-profit [501(c)(3)] organization dedicated to improving the security of the Internet – for free. The Project is made up of thirty security professionals from around the world who research the modus operandi of predatory hackers.

We seek to learn the tools, tactics and motives involved in computer and network attacks and share the lessons learned.

Most security research is theoretical. At The Honeynet Project, there is a commitment to moving far beyond theory and providing solid information about common threats. This information and our tools are used to better understand and defend against threats.

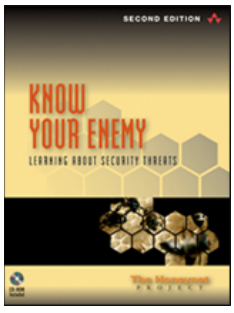
Everything we do and provide is freely available at our website, located at http://www.honeynet.org.

As a tank officer in the Army's Rapid Deployment Force, I was trained extensively on the threats I would face. I was taught the tools, tactics, and even the command structure of a typical Soviet tank unit. I climbed in T-72 tanks to better appreciate the threats I would face and to learn how I might better defend against them.

When I transitioned into information security, there were few facts about threats. How can you defend against a threat when you don't even know who or what that threat is?

That's why I started The Honeynet Project. I wanted to improve the global security of the Internet at no cost to the public.

Lance Spitzner
Founder



"The Honeynet Project recently published the second edition of their book "*Know Your Enemy*".

The Honeynet PROJECT®

The Honeynet Research Alliance

The Research Alliance is an international community of trusted organizations that come together to actively research, develop and deploy honeypots, and share the lessons learned. The alliance gives us a unique global perspective, as we have research organizations and honeynet sensors deployed around the world. Active member organizations include:

- The UK Honeynet Project
- The Norwegian Honeynet Project
- The Brazilian Honeynet Project
- The Chinese Honeynet Project
- The Florida Honeynet Project
- The French Honeynet Project
- The GA Tech Honeynet Project
- The German Honeynet Project
- The Honeynet Project at the University of Texas at Austin
- The Internet Systematics Lab Honeynet Project Greece
- The Italian Honeynet Project
- The Net Forensics Honeynet
- The Pakistan Honeynet Project
- The Paladion Networks Honeynet
- The Portugal Honeynet Project
- SIG^2 Internet Weather Forecast Centre
- The Spanish Honeynet Project
- The Azusa Pacific University Honeynet
- The West Point Honeynet Project

The activities of The Honeynet Research Alliance greatly helped to fill a knowledge void in information system security research. Before the Alliance, it was rare to read about security breaches. Even rarer, was the sharing of this information among the experts. All this has changed with the creation of the Alliance.

The collected information is helping not only improve the expertise of Alliance group members, but it has also enhanced the awareness of information security experts throughout the world. We now know how common vulnerabilities are exploited. This is the direct contribution of the Alliance, and would not have been available without it.

Antonio Montes, Ph.D.
The Brazilian Honeynet Project

The Honeynet PROJECT®

The Honeynet Project®
Our Goals

We help secure the Internet in the following three ways:

Raise Awareness

We raise awareness of the threats and vulnerabilities that exist in the Internet today. Many individuals and organizations do not realize they are a target, nor understand who is attacking them, or how they're doing it and why. We provide this information so the public realizes they are targets and learn basic measures they can take to mitigate threats. This information is provided through our *Know Your Enemy* series of papers.

Teach and Inform

For those who are already aware and concerned, we provide details to better secure and defend resources. Historically, information about attackers has been limited to the tools they use. We provide critical additional information, such as their motives for the attack, how they communicate, when they attack systems, and their specific actions after compromising a system. We provide this service through our *Know Your Enemy* white papers and our *Scan of the Month* challenges.

Research Tools

For organizations interested in continuing their own research about cyber threats, we provide the tools and techniques developed by The Honeynet Project. This information is provided through our *Tools* site.

Nobody else does what we do at The Honeynet Project. We continue to serve as an unbiased and open source, with no commercial interests. And we've been doing this since 1999.

The Honeynet PROJECT®

The Honeynet Project®
Shedding Light on the Attackers

A honeynet is not a single system, but a network of "honeypots" – systems designed to capture hackers within highly controlled and monitored networks.

This network environment uses the same systems and applications found on the Internet. When hackers compromise the honeypot, silent alarms are set off so researchers can control the attack and begin gathering critical information about the hackers.

Most security experts –even those who design products to protect against attacks – are ignorant of the tools, actions, tactics, and motivations of hackers.

The moral is that there's a staggering number of people out there trying to break into your computer network, and that the intruders succeed surprisingly often. Network administrators who don't take drastic measures to protect themselves are toast.

Bruce Schneier
Chief Technology Officer
Counterpane Internet Security, Inc.

The Project was constructed to shine a light into the darkness of the Internet. The team of Honeynet Project researchers built entire computer networks, wired them with sensors, and then deployed these networks on the Internet– across the globe. They then recorded hackers' actions – observing how they tried to break in, when they were successful, and what they did when they succeeded.

Today, this information sheds light on the attackers themselves, revealing who is launching the attacks, how they communicate, and their motivations. Armed with this information, individuals and organizations can better defend themselves.

The Honeynet PROJECT®

Products & Services

Research and Development

Research and development is the core of our mission. Our goal is to develop new tools and methods for capturing the latest advances of cyber threats. We then use these tools to capture activity and information on the latest threats and trends. We then not only share what have learned about these threats, but we share the tools and techniques themselves so others can use them and benefit.

New resources can provide critical funding for additional dedicated staff who will support expanded research that stays ahead of the hackers' advances, as well as new research projects.

A great deal of our research is conducted by talented college students, preparing for successful and ground breaking careers in technology fields. To help subsidize their work and encourage the continued involvement of some of the best new minds, we fund graduate research activities.

New resources can provide ongoing scholarship dollars that encourage innovation in security research and

As a student of information security, The Honeynet Project brings together the best of all worlds: a global set of experts from diverse fields, the motivation of working on cutting-edge technology, and a strong sense of community.

My work with The Honeynet Project has led me to study areas of information security not touched on in any of my classes, and put me in direct contact with the experts in those fields.

George Chamales
Information Security Masters Candidate
Polytech in Brooklyn, NY

The Honeynet PROJECT®

Products & Services

Tools

As cyber threats and attackers are constantly adapting and advancing, so to must we. Developing new tools are key to staying one step ahead of today's, and tomorrow's, threats. Newfound resources will support the development of additional tools that will continue to be free to the public. New tools will include:

Application Honeypots – Sophisticated honeypots that capture attackers and threats against online commerce, such as banks and online shopping.

Client Honeypots – Honeypots that capture attacks and threats against client systems, such as a browser on a personal computer, instant messaging, or e-mail, and their attachments.

Advanced Honeypots – Honeypots that capture highly organized and sophisticated attacks, such as organized crime against the financial industry.

Low-Interaction Honeypots – Honeypots designed for rapid and large-scale deployments. Used for early warning and prediction on a global scale.

Ipv6 Honeypots – Honeypots designed to operate within and understand IPv6 activity.

The work of The Honeynet Project has been of tremendous value to people new to information security, as well as established researchers.

Information security professionals have been able to translate these once nebulous ideas into actions and gain valuable insight into emerging attack techniques. This has improved our defenses. The challenges put together by the Project have taught numerous people how to analyze data and explore new tools and techniques.

The Honeynet Project has done all of this in the open, sharing your work with the world-at-large. The widespread adoption of the honeynet methodologies is testament to their real value.

Jose Nazario, Ph.D.
Security Researcher
Author: *Defense and Detection Strategies Against Internet Worms*

The Honeynet PROJECT®

Products & Services

White Papers

"Know Your Enemy" White Papers are our primary means of sharing our findings with the community. Individuals and organizations from around the world deploy honeynets that capture attacker's activity. This activity is then analyzed by a core group of security professionals, whose findings are then documented and shared at no cost to the public. The average paper takes six months to research and write, including an intense five week review period. These papers are used around the world. They have been translated into over 11 different languages, referenced in countless books and publications, and have even been used in testimony to US Congress.

- These papers share information The Honeynet Project has collected about the hackers. These are crucial elements that increase the understanding of who is attacking systems and why.
- In addition, these papers share the tools and techniques as to how that information was obtained and analyzed.

Sponsorships can provide support for:

Profiling

Paper documenting cultures and geographies heavily involved in information attacks and crimes.

Awareness Paper

A non-technical paper for the home user. This paper combines the past 5 years of our research into a short, simple to understand document. The goal is the average user understands why they are a target, who is targeting them and how, and simple steps they can take to protect themselves.

Client Threats

White Paper about how and why attackers are breaking into client systems.

IPv6 Threats – Understand how and why hackers are attacking IPv6 systems.

Honeynet Project® | w

The Honeynet PROJECT®

Products and Services

The Honeynet Project Annual Workshop

Each year, the key leadership, researchers, and developers from The Honeynet Project and the Honeynet Research Alliance meet in Chicago Illinois to brainstorm, strategically plan and conduct tactical research and development. Representatives come from around the globe to participate in this three-day event.

Sponsorship supports participation, allowing The Honeynet Project to provide transportation and lodging support to participants. Sponsors are invited to attend the Workshop and learn about up-and-coming technologies.

- **2005 will be the fifth annual workshop.**
- **An average of 30-40 members attend.**
- **Often this is the first time members have physically met, allowing people from around the world to work together in the same room for the first time.**
- **In the past, members have come from countries including Brazil, India, Germany, Pakistan, Italy, Greece, and France.**

The Honeynet PROJECT®

Exposure

Publications, Media & Conferences

The Honeynet Project uses the website to openly share and communicate with a vast and diverse audience. The website receives an average over 200,000 hits while mirrored in over 15 countries, and the expertise of our 30 security professionals is consistently sought and quoted in articles in:

- **The BBC News**
- **The Wall Street Journal**
- **The Economist**
- **On CNN**
- **In the New York Times**
- **On National Public Radio**
- **The Associated Press**
- **The Washington Post**
- **Government Computer News**
- **Internetweek.com**

In addition to publications, The Honeynet Project is asked to present at various organizations, including:

- **US President's Advisory Board**
- **Monetary Authority of Singapore**
- **Pentagon**
- **UK Government**
- **FIRST**
- **United Arab Emirates**
- **IEEE**

Articles documenting The Honeynet Project's impact include:

2000: Wall Street Journal
Around the World, Hackers Drawn to Honeypots

April 4, 2001: CNN.com/Sci-Tech
Networks use 'Honeypots' to Catch an Online Thief

Mar 29, 2001: The Economist
Diagnosing Computer Crime

2001: Newsweek
Stealth Care for Networks

2003: New York Times
A New Way to Catch a Hacker

2003: IEEE Security
Tracking the Wild Hacker

March 17, 2005: BBC News
Have hackers recruited your PC?

The Honeynet PROJECT®

Overview of Sponsorship Opportunities

The Honeynet Project asks the question: "How can we defend against an enemy when we don't know who the enemy is?" By deploying networks around the world to be hacked, everything that is captured keeps the technology one step ahead of the bad guys. Attackers can control thousands, if not hundreds of thousands, of systems around the world. The Honeynet Project serves as an essential tool and resource in defining and identifying unauthorized or illicit use of the Internet. Sponsorship and philanthropic opportunities exist to support the Project as we move towards increasing the release of information and tools at no fee.

Sponsorship opportunities are limited to the website, white papers, tools and the monthly challenges.

$25,000

Benefits

Scrolling Banner on website with corporate logo for one year.

Listing on Donors & Sponsors page for one year.

Listing in our biannual newsletter.

Know Your Enemy, Learning About Security Threats — *Book signed by the officers of The Honeynet Project.*

$50,000

Benefits

Scrolling Banner on website with corporate logo for one year.

Early access to and/or your organization associated with published papers and/or tools

Listing on Donors & Sponsors page for one year.

Listing in our biannual newsletter.

Know Your Enemy, Learning About Security Threats — *Book signed by the officers of The Honeynet Project.*

$100,000

Benefits

Premium sponsorship with your corporate logo on the website home page for one year

One-day Workshop and Brainstorming Session to explore how you can leverage your sponsorship as "value added" for your customers. The latest technology, findings and future research efforts will also be shared.

Early access to and/or your organization associaed with published papers and/or tools

Listing on Donors & Sponsors page for one year.

Listing in our biannual newsletter.

Know Your Enemy, Learning About Security Threats — *Book signed by the officers of The Honeynet Project.*

The Honeynet PROJECT®

Overview of Donor Opportunities

Endowment Needs and Opportunities

General Endowment

Endowed Chair for the President	$1,000,000
Endowed Fund for Operations	$ 250,000
Endowed Fund for Innovations, Research & Development	$ 50,000
Endowed Research Grants	$ 50,000

Named funds can be created to support general operations and can be annual or endowed gifts

Innovations Fund - Research & Development	$50,000 to endow; $15,000 annual naming opportunity
Research Grants	$50,000 to endow; $15,000 annual naming opportunity
Lecture Series	$100,000 to endow; $15,000 annual naming opportunity

Annual Gifts

Gifts of cash or appreciated securities can be given as:

Unrestricted Gifts

Restricted to a program area or specific

Tributes to honor someone important to you

Planned Gifts

Gives you an occasion to leave a legacy that promotes strength and excellence in our programs. Through a planned gift, you can help The Honeynet Project continue to innovate and stay ahead of new threats created around technology advances. You can make keeping information safe and sound through The Honeynet Project an important part of your legacy:

Through a gift provided in your will or trust

Through a charitable gift annuity

With a gift of real property or appreciated securities

Recognition opportunities are available and appropriate to the gift.

The Honeynet PROJECT®

The Honeynet Project
Board of Directors

The Board of Directors is a team of highly experienced security professionals who are leaders in their field. They have volunteered their time to help guide and lead the Honeynet Project. Directors serve a two-year term, but can be reelected for additional terms.

Jennifer Granick
Lecturer, Stanford Law School
Executive Director, The Center for Internet & Society (CIS)

Alfred Huger
Senior Director of Engineering, Symantec
Co-Founder and Vice President of Engineering, SecurityFocus

George Kurtz
CEO & Co-Founder
Foundstone (a global information software services and education provider in security solutions) and
Author: *Hacking Exposed* series

Martin Roesch
Chief Technology Officer and Founder
Sourcefire (developing real time network defense solutions)

Bruce Schneier
Chief Technology Officer and Founder
Counterpane Internet Security, Inc.
Author: *Applied Cryptography*, *Secrets and Lies*, and *Beyond Fear*

Lance Spitzner
The Honeynet Project Founder
Author*: Honeypots: Tracking Hackers*, and coauthor of *Know Your Enemy: 2nd Edition*