



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Honeynets in operational use

Gregory Travis

Indiana University, Advanced Network Management
Lab

Greg@iu.edu



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Quick Overview of Honeypot Technology

- Honeypots
- Honeynets
- IDS'



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Technology Description

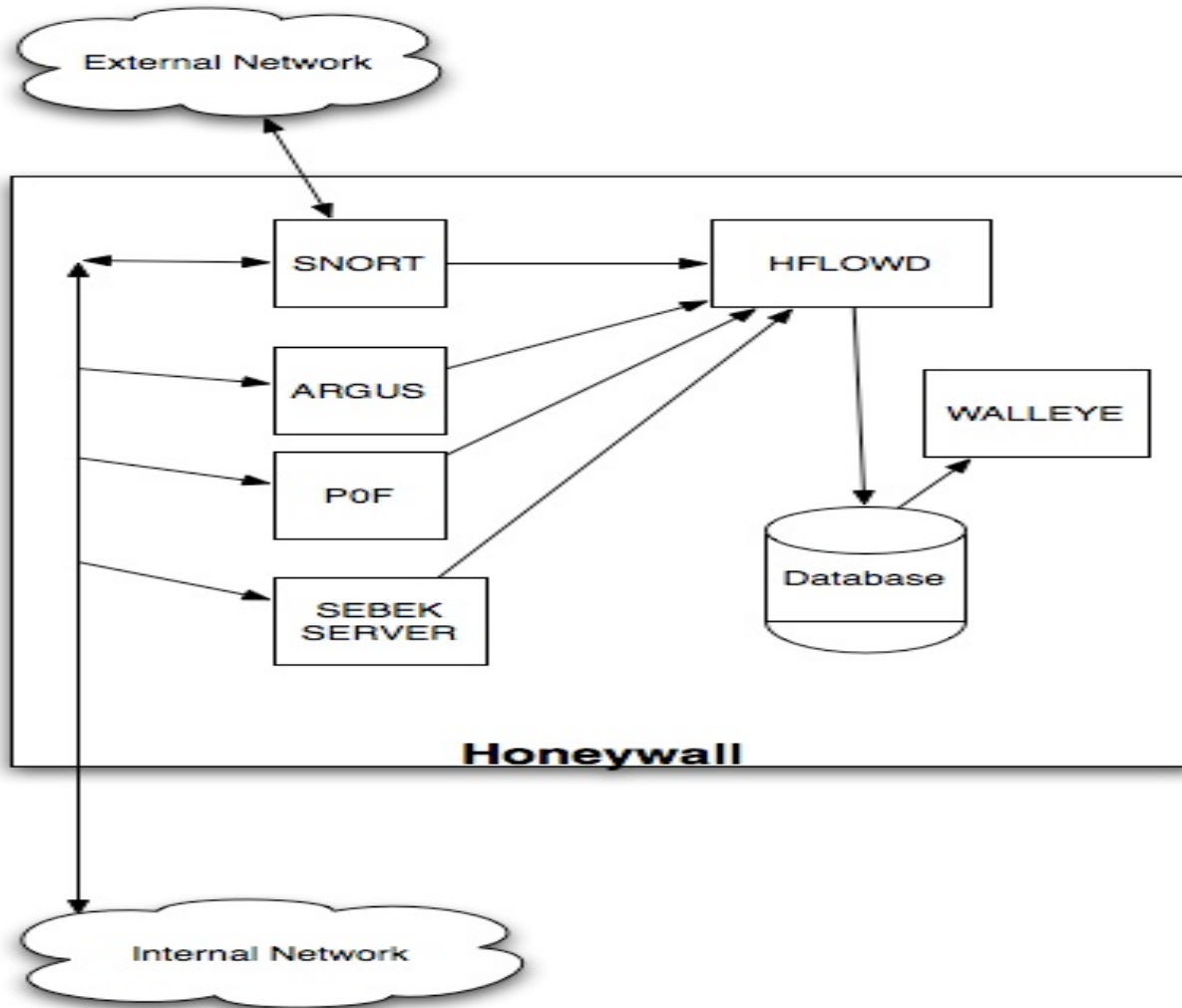
- Technology Description
 - Honeywall
 - Walleye
 - Hflow
 - Argus
 - P0F
 - Snort
 - Sebek



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Honeywall Schematic

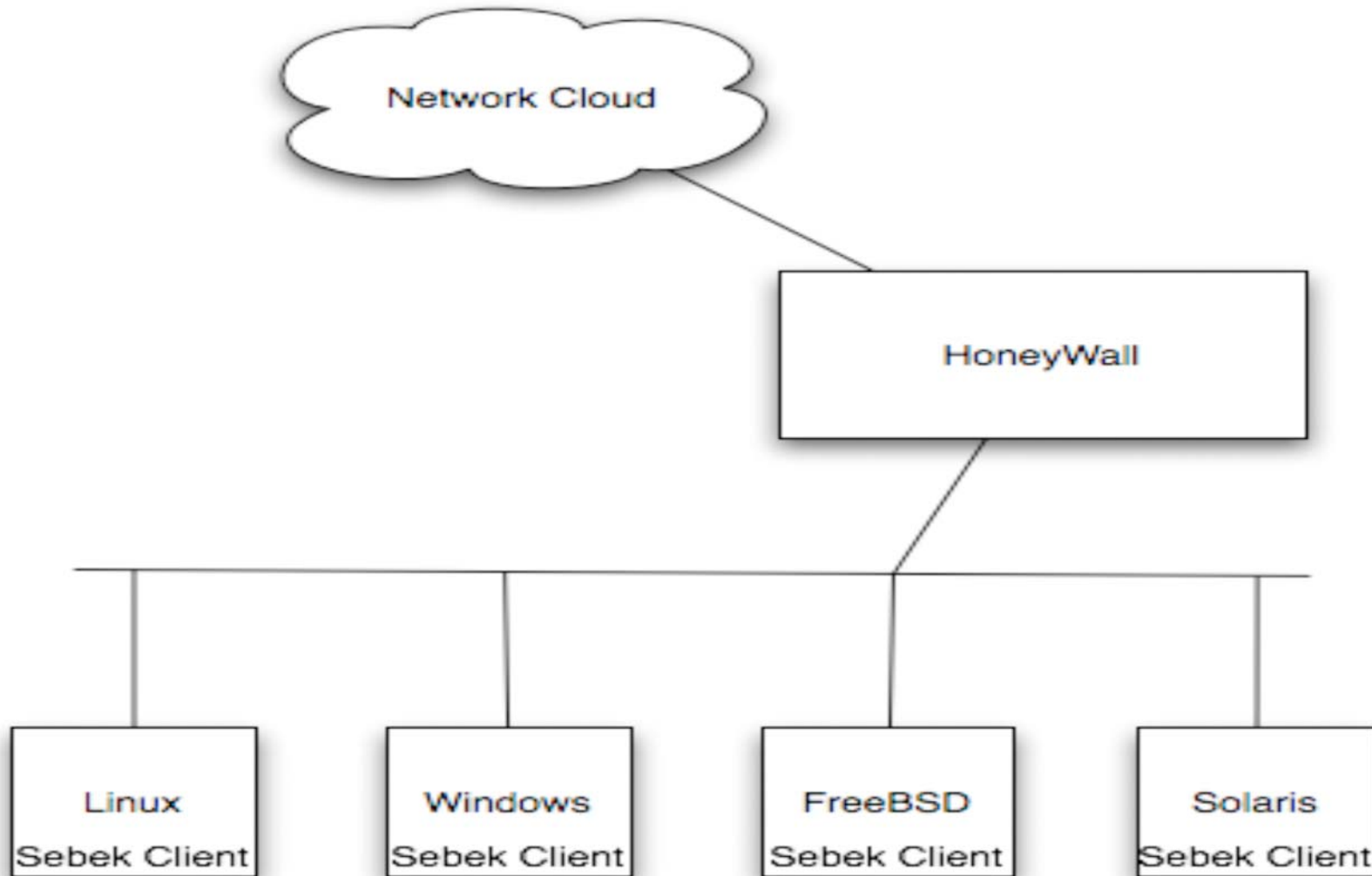




pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Deployment





pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Problems

- Randomly throwing out Honeypots doesn't necessarily help
 - If you throw them were hackers won't go, they do no good
 - Have to be placed on strategic assets (I.e. database servers)
 - In real world, you don't always know what the bad guys will go after.



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Problems

- Time management
 - Do you have the time to run all of them?



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Solutions

- Use Honeypots *reactively* in operational use
 - I.e. don't use them as first-line IDS'



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Reactive use examples

- “POP’d” box
 - Turn a production system into a honeypot reactively
- Find out what attracted the hacker and build new boxes that meet that profile to attract the bad guys
 - This is the “Honey” in Honeypot



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

How-To

- How do we actually do the “POP’d” box scenario?
- Steps
 - Deploy Honeywall upstream of compromised host
 - Instrument the actual compromised host with Sebek
 - Done! Get a beer!



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Honeywall Deployment

- Acquire Hardware
 - 3 NICs
 - 512+MB RAM
 - Fast CPUs better (~2+Ghz)
- Download ISO from Honeynet website
 - www.honeynet.org/tools/cdrom
- Install
- Configure



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Instrumenting with Sebek

- Why do you want to do this?
 - Circumvent session encryption used by intruder (I.e. ssh)
 - Identify causal relationships between network flows on the host
 - Process tree depiction



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

How do I install Sebek?

- Determine type of target host first
 - I.e. Linux/Windows/FreeBSD/etc.
- Download, compile, and configure on a *separate* box that matches the specifications of the target
 - Don't want to tip off the intruder to what you're doing
 - www.honeynet.org/tools/sebek
- This creates a binary “tarball”
 - Get that onto the target in a stealthy mode
 - Turn off shell history, etc.



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Sebek install cont...

- Run installer
 - `sbk_install.sh` (Linux example)
- At this point, Sebek data will be flowing to your Honeywall



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Now what?

- What kind of knowledge can you gain?
 - Watch keystrokes
 - Watch network activity
 - Identify correlations between keystrokes and network activity
 - You get to watch the entire intrusion sequence as it happens



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Great!...I think?

- It is! One of the first questions you'll want answered is:
 - Is this an automated attack or is there a live human on the end?
- Keystroke logs will tell you this from, for example, if there are mistakes made



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Ok...what else?

- Is this a lone wolf or am I looking at a conspiracy?
- Generally speaking, human behavior is consistent -- especially under stress
 - Look at the way that people run commands
 - Do they run “ps aux” or “ps -elf”?
 - What are the religious preferences?
 - Pico or Vi?
 - Behaviometrics



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

And ahhh?

- Determining the type and nature of the attacker is crucial to your job
- First step is to determine if you're being "nuisance attacked" or if this is a specific attack targeted at you and some asset that you hold uniquely
 - Incident scope
 - Clues about what might be next on their agenda



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Example

- Real attack
- Password harvesting
- You're watching someone actively harvesting passwords from your system
- Why might they be doing that?
- Do you have other systems, other assets, where those same passwords might be valuable?



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Example...

- You want to trace “upstream” where those passwords are going
- You want to share that data with others outside your administrative domain
 - Are they seeing the same type of activity with the same type of biometric fingerprints?
 - Work with them to follow it all upstream



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

What to do when the stream disappears underground

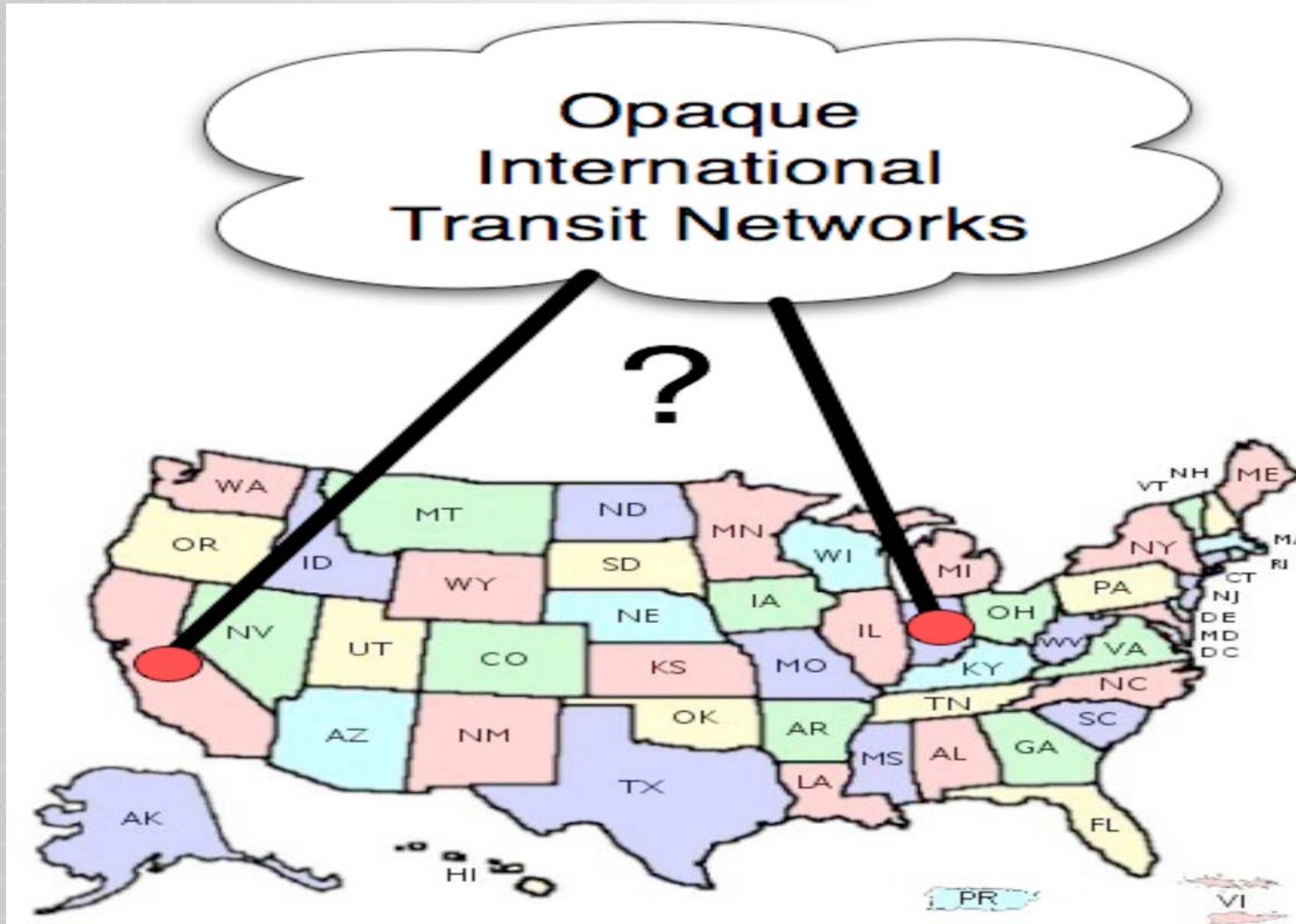
- Typically you will lose the ability to directly trace back rather rapidly
 - Everyone knows about using stepping stones
 - Traces will cross international/administrative boundaries
 - There will be areas totally opaque to you
 - You will “lose the scent”



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Losing the scent





pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

International Issues

- Language Barriers
- Motivation Barriers
- Legal Barriers
 - All of this means that any circuit that crosses a national border is untraceable with normal technology





pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Using Sebek

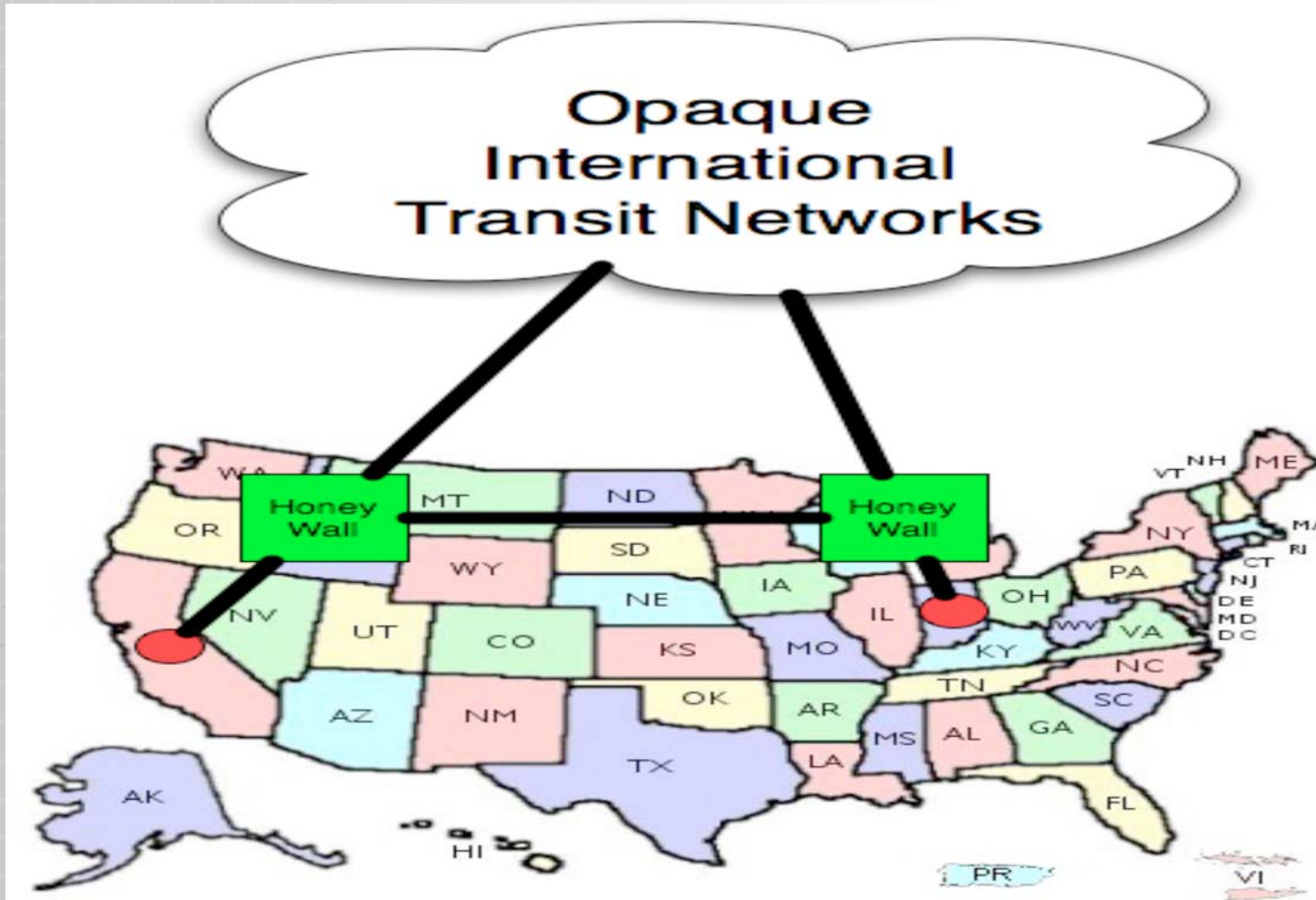
- We can use Sebek to identify similar behavior
 - Right now this is a fairly manual exercise
 - We are working on technology that will automatically correlate intrusion sequences



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Using Sebek to pick up the scent





pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

Conclusion

- Need to determine when the technology can be of value
 - No fire and forget
- Need to deploy technology in a productive manner
 - No shotgun
- Need to understand that it won't fix everything
 - No magic bullet



pervasivetechlabs
AT INDIANA UNIVERSITY

www.pervasivetechlabs.iu.edu

In a perfect world

- Every OS would have a Sebek component
 - Detection arms race is irrelevant when it's ubiquitous
- That component would be secure
- We could automatically dial the right level of detail
- It wouldn't cause a performance hit