# Security versus Energy Tradeoffs in Host-Based Mobile Malware Detection

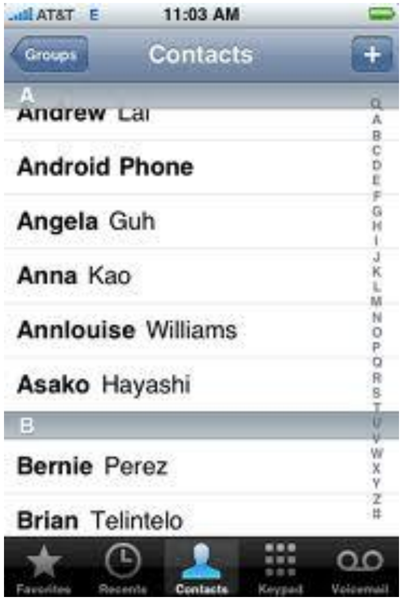
**Jeffrey Bickford *,** H. Andrés Lagar-Cavilla #, Alexander Varshavsky #,
Vinod Ganapathy *, and Liviu Iftode *

* Rutgers University
# AT&T Labs – Research

# Smart Phone Apps

## Store personal and private information

Contacts



A

Andrew Lai

Android Phone

Angela Guh

Anna Kao

Annlouise Williams

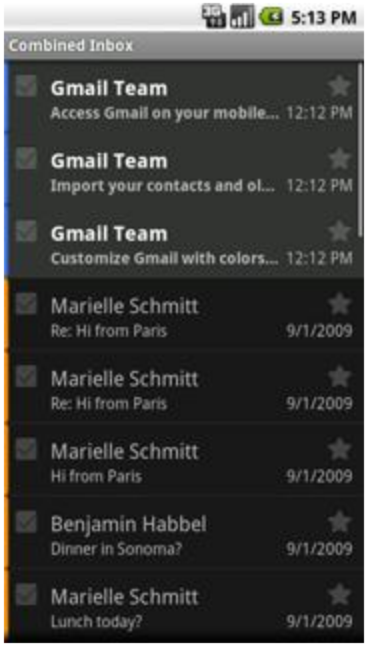
Asako Hayashi

B

Bernie Perez

Brian Telintelo

Email



Combined Inbox

Gmail Team
Access Gmail on your mobile... 12:12 PM

Gmail Team
Import your contacts and ol... 12:12 PM

Gmail Team
Customize Gmail with colors... 12:12 PM

Marielle Schmitt
Re: Hi from Paris 9/1/2009

Marielle Schmitt
Re: Hi from Paris 9/1/2009

Marielle Schmitt
Hi from Paris 9/1/2009

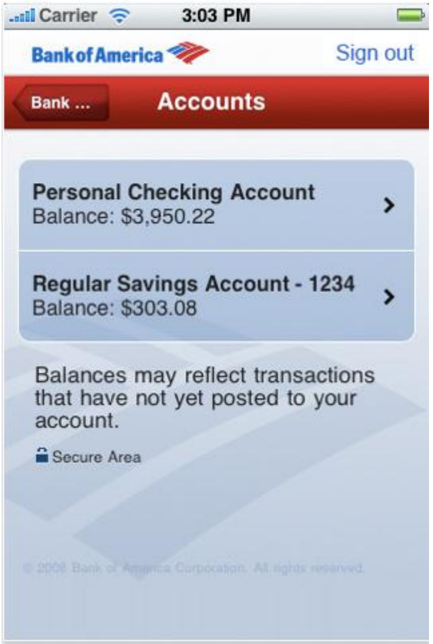
Benjamin Habbel
Dinner in Sonoma? 9/1/2009

Marielle Schmitt
Lunch today? 9/1/2009

Location

Google Maps
Business And
Retail Park
1
Glasgow
Alexandra P
A814
Glasgow
City
River
Clyde
Gallowgate
M8
Dixon Blazes
Industrial
Estate
Pollokshields
Calder St
Rutherglen
Haggs Rd
Glasgow Rd
[1] Return to Result
Zoom -
Menu

Banking



Personal Checking Account
Balance: $3,950.22

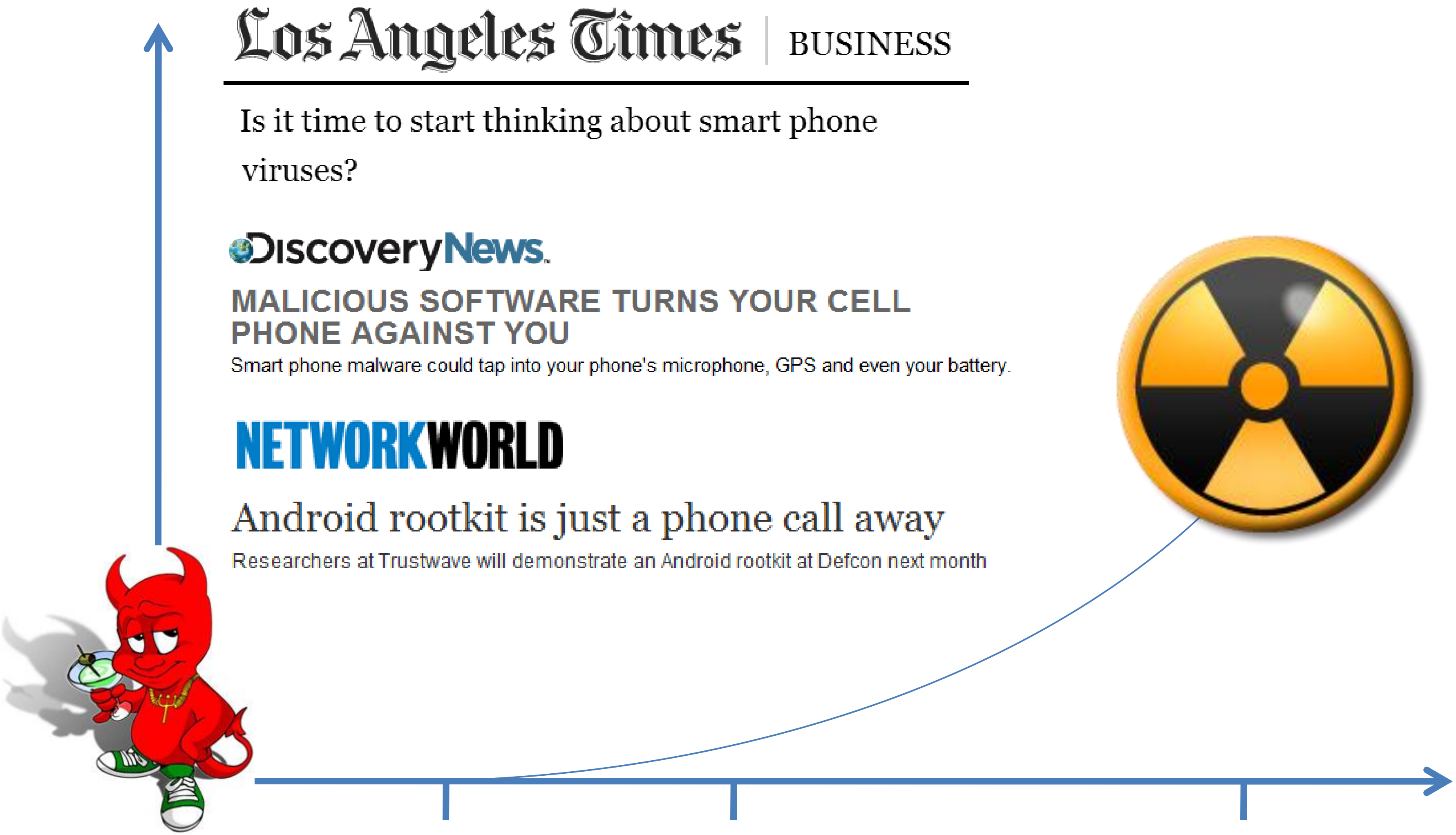
Regular Savings Account - 1234
Balance: $303.08

Balances may reflect transactions that have not yet posted to your account.

Secure Area

© 2008 Bank of America Corporation. All rights reserved.

# The Rise of Mobile Malware



Los Angeles Times | BUSINESS

Is it time to start thinking about smart phone viruses?

DiscoveryNews.

MALICIOUS SOFTWARE TURNS YOUR CELL PHONE AGAINST YOU

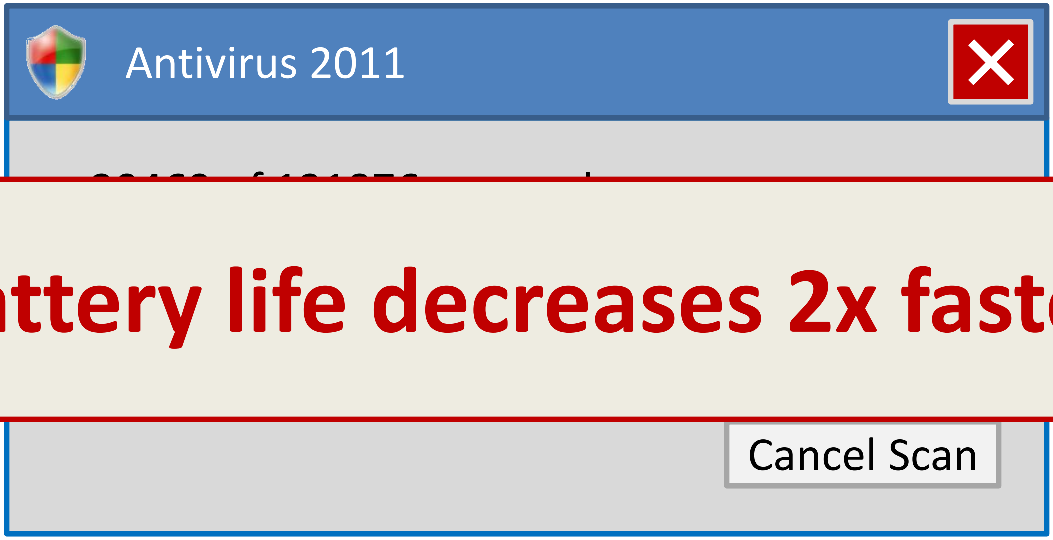
Smart phone malware could tap into your phone's microphone, GPS and even your battery.

NETWORKWORLD

Android rootkit is just a phone call away

Researchers at Trustwave will demonstrate an Android rootkit at Defcon next month

# Traditional Malware Detection



**Battery life decreases 2x faster!**

- Periodically scan the attack target
  - System comprised of code and data
- Personal files, executables, databases, network activity

# Mobile Detection Problem

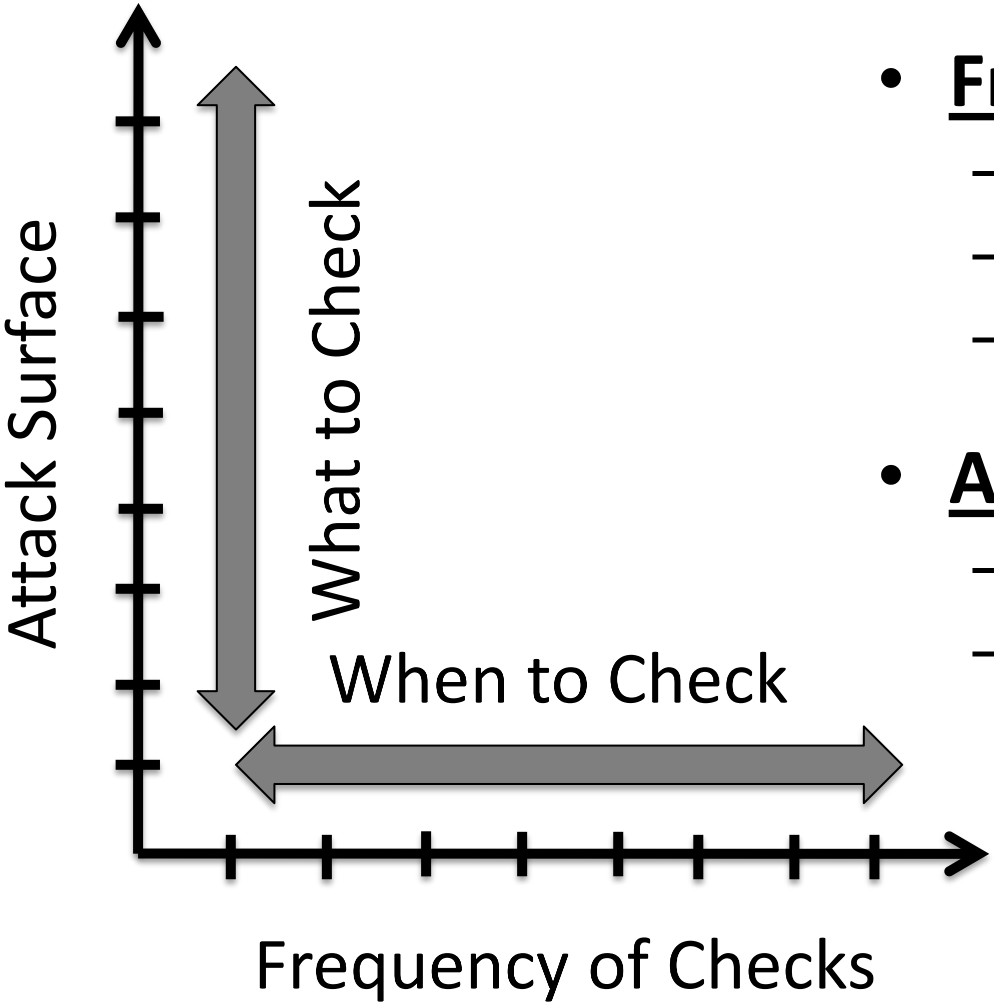
- Typical machines can execute malware detection systems 24/7
- Mobile devices are limited by their **<u>battery</u>**
- Detection mechanisms in their current state lead to **<u>high energy cost</u>**
- Executing malware detection systems only when charging is not sufficient

# Contributions

**Explore the tradeoffs between security monitoring and energy consumption on mobile devices**

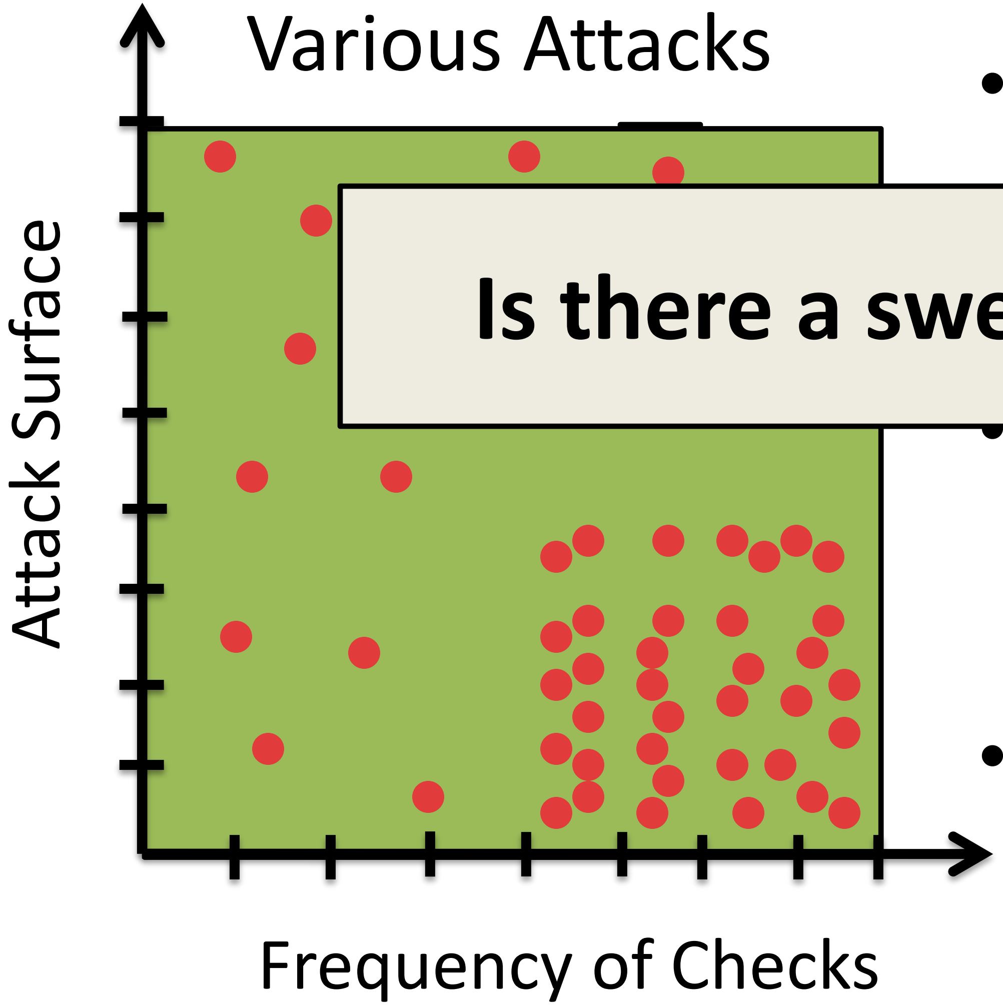
1. Framework to quantify the security vs. energy tradeoffs on a mobile device
2. Create energy optimized versions of two security tools
3. Introduce a balanced security profile

# How Do I Conserve Energy?



- **Frequency of Checks**
  - When to check?
  - Scan less frequently
  - Timing vs events
- **Attack Surface**
  - What to check?
  - Scan fewer code/data objects

# Security-Energy Tradeoff

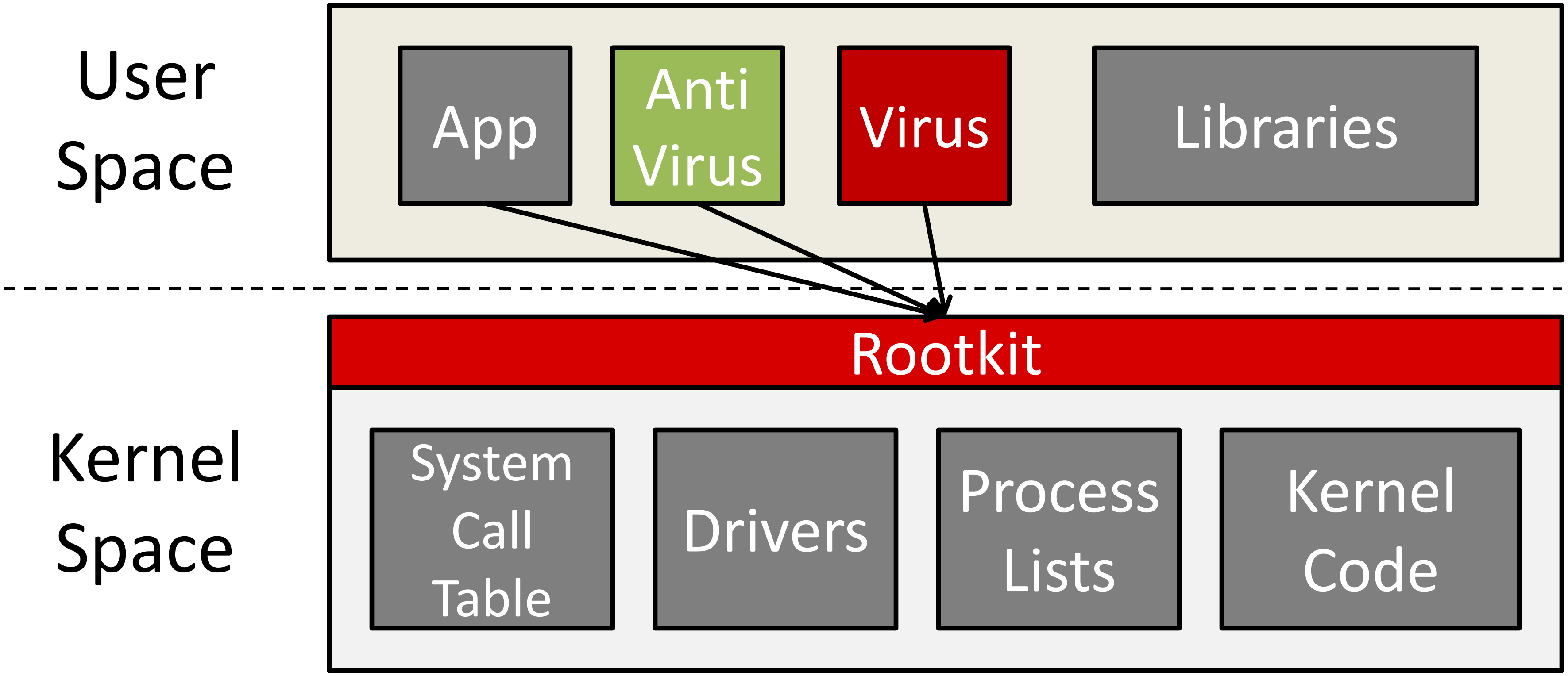


**Is there a sweet spot?**

- Scan all continuously
  - Best possible security
  - y cost
- **<u>Periodically Scan</u>**
  - Vulnerable between scans
- **<u>Scan Subset</u>**
  - Vulnerable to attacks outside of subset

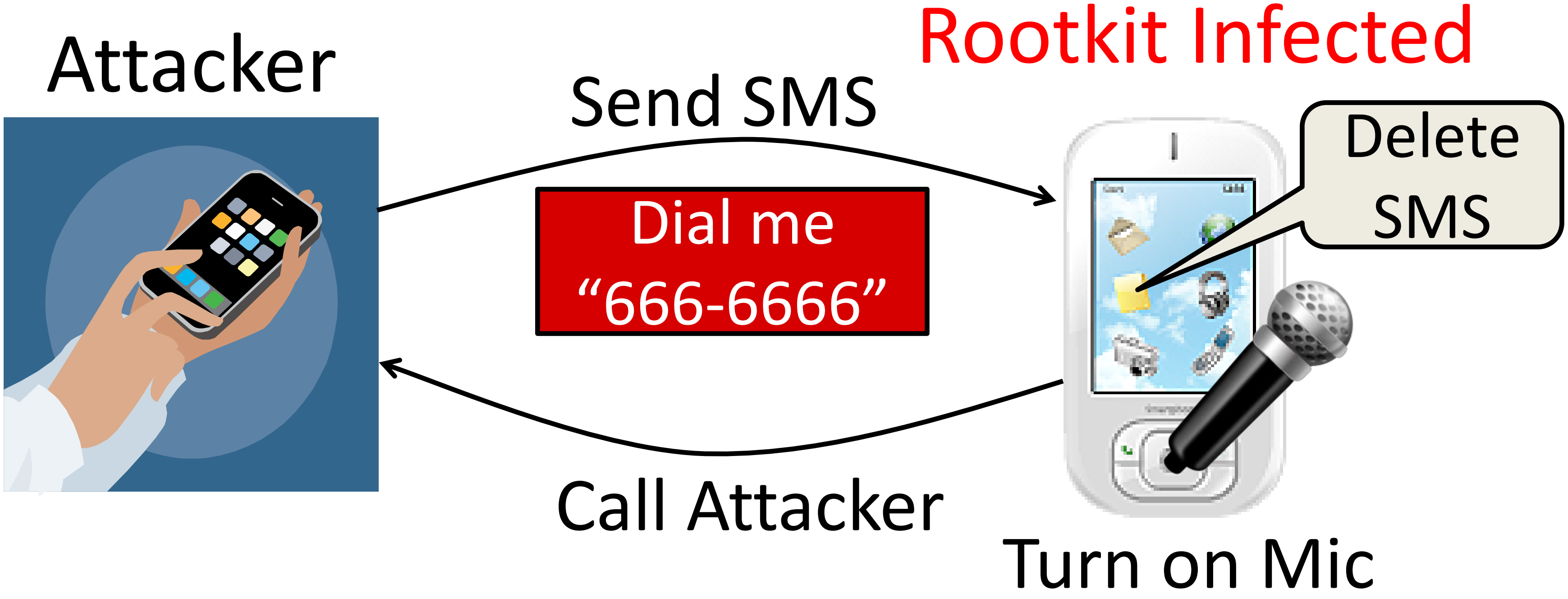
# Rootkits

**Rootkits are sophisticated malware requiring complex detection algorithms**



# Demonstrated Attack

## Conversation Snooping Attack

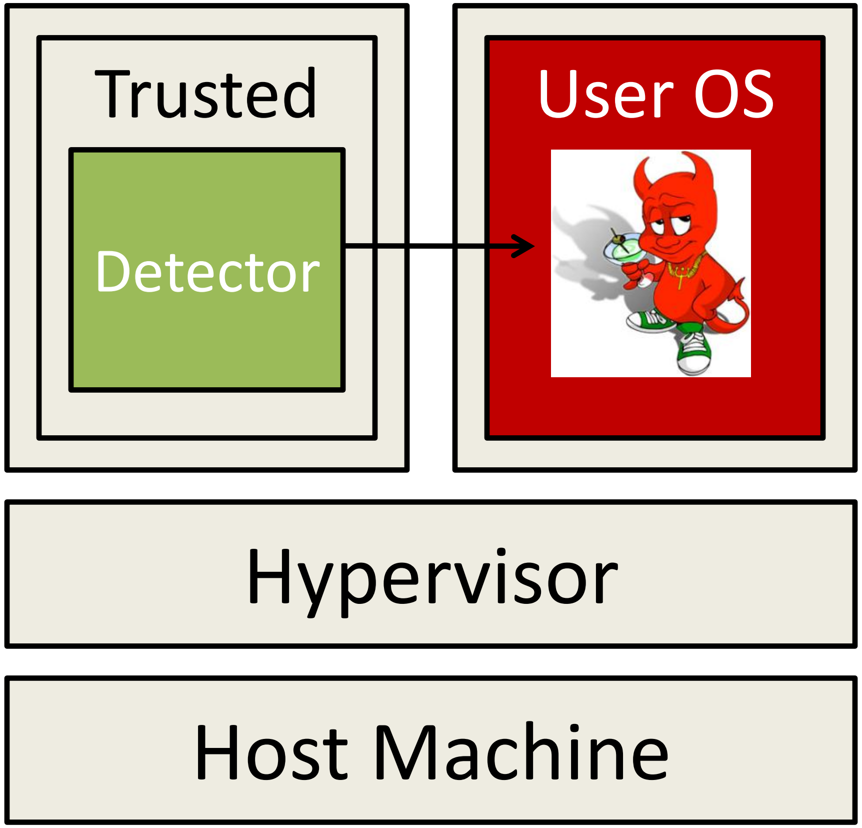


Rootkit stealthily hides from the user

[Bickford *et al.* HotMobile '10]

# Rootkit Detection

**OS must be monitored using a hypervisor**



- Detection tools run in trusted domain
- Mobile hypervisors soon
  - VMWare
  - OKL4 Microvisor (Evoke)
  - Samsung Xen on ARM

# Experimental Setup

- Viliv S5
  - Intel Atom
  - 3G, WiFi, GPS, Bluetooth

- Xen Hypervisor
  - Evaluated the tradeoff using two existing rootkit detectors within trusted domain
- Workloads
  - 3G and WiFi workload simulating user browsing
  - Lmbench for a CPU intensive workload

# Detecting Data-Driven Attacks

- **Gibraltar** [Baliga *et al.* IEEE TDSC '11]

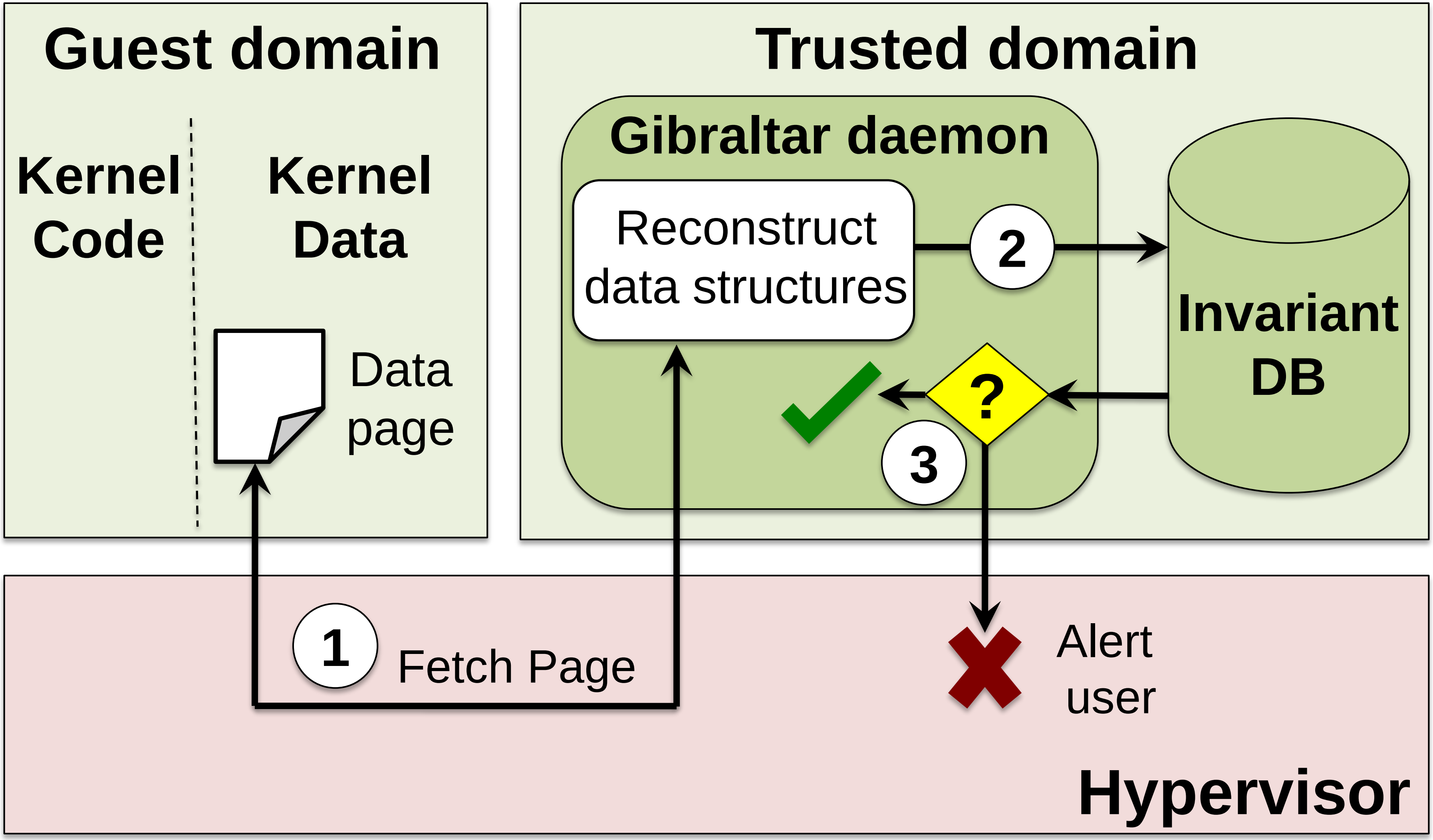
  typifies the usual form of rootkit defense for kernel data attacks

  - Primarily pointer-based control flow
  - Scans data structures within the OS Kernel

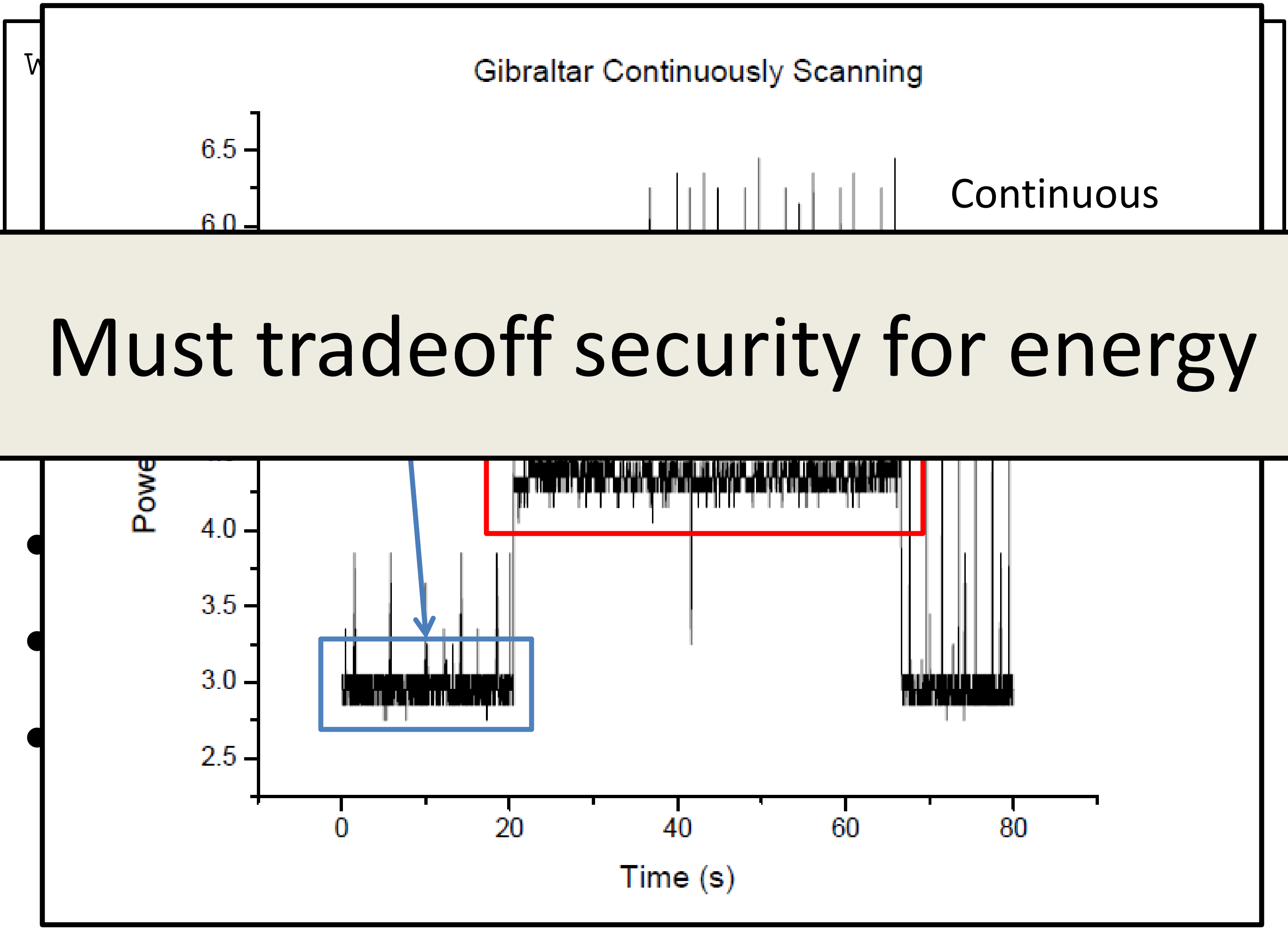
- Scanning approach analogous to antivirus scans

- Original version monitored all data structures all of the time

# Detecting Data-Driven Attacks

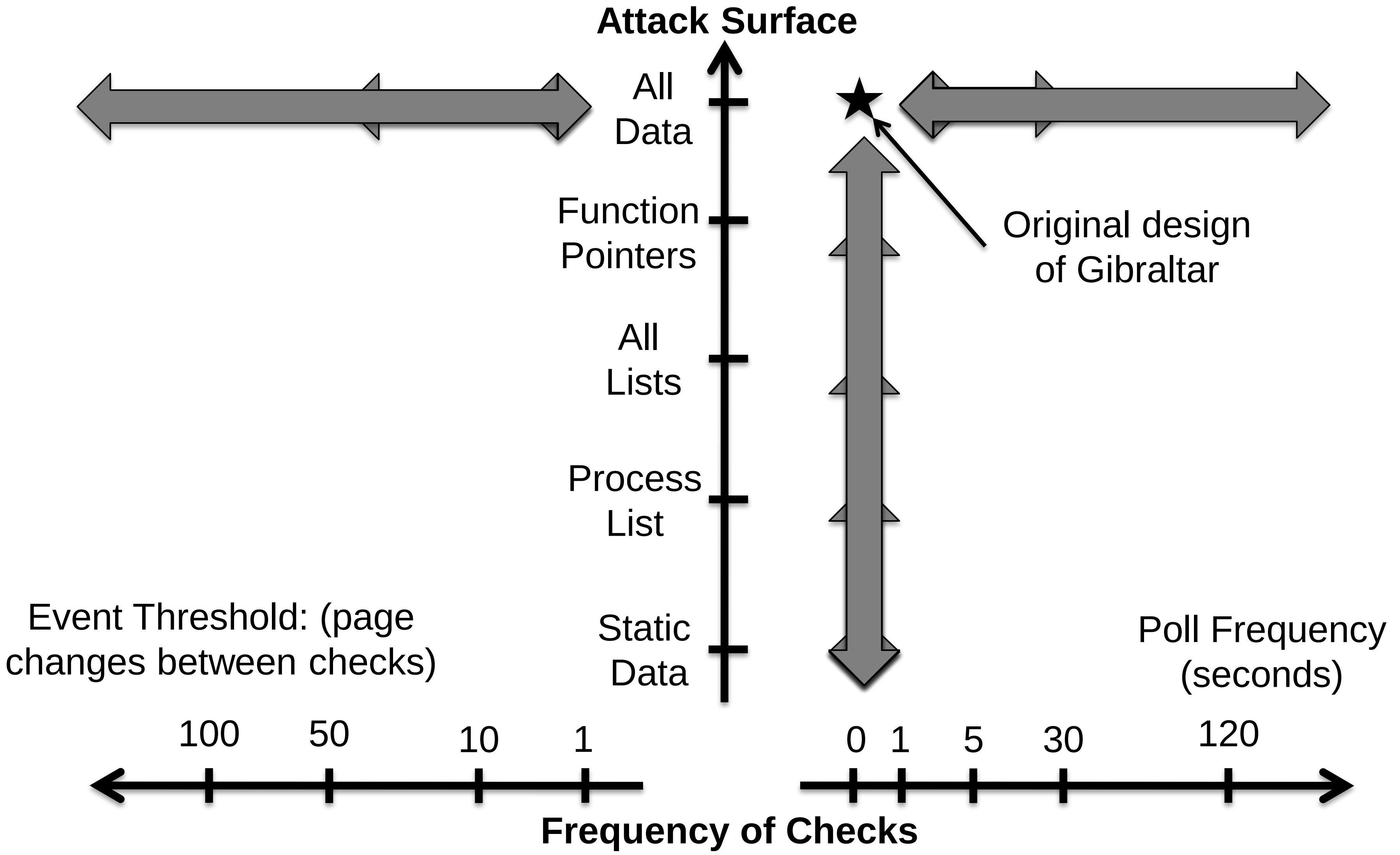


# Problem – High Energy Cost

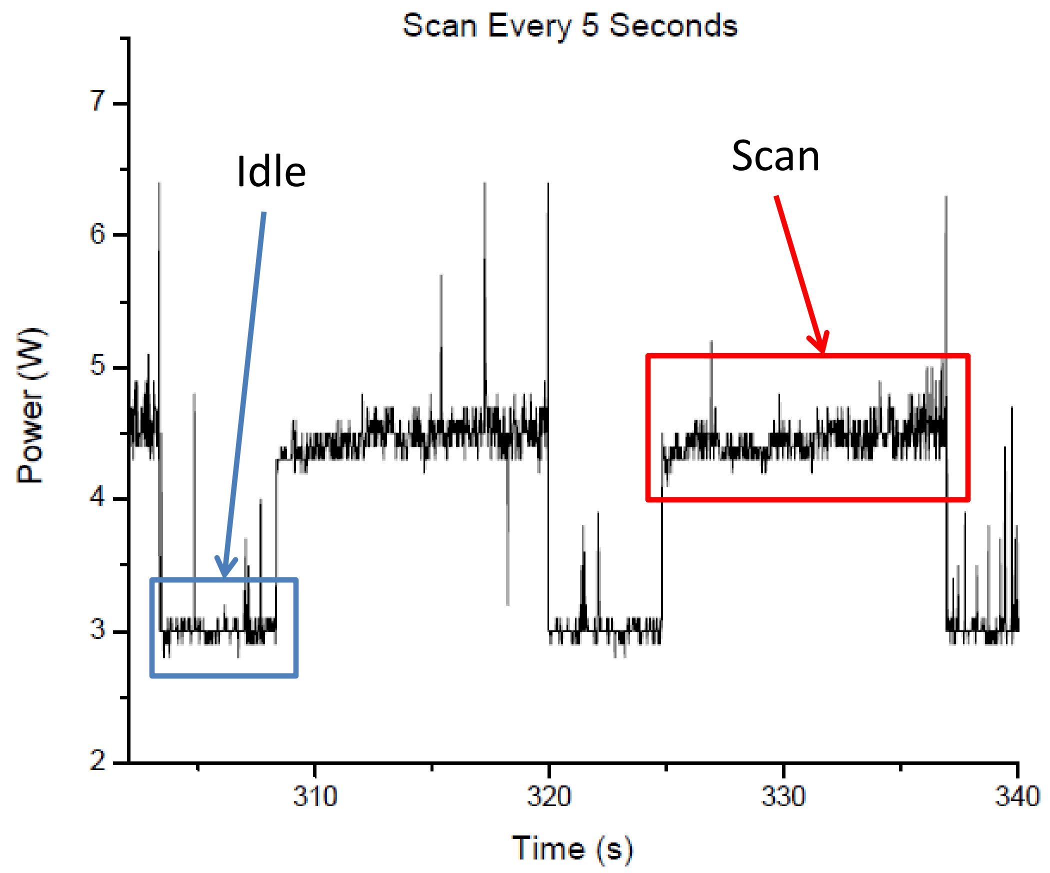


Must tradeoff security for energy

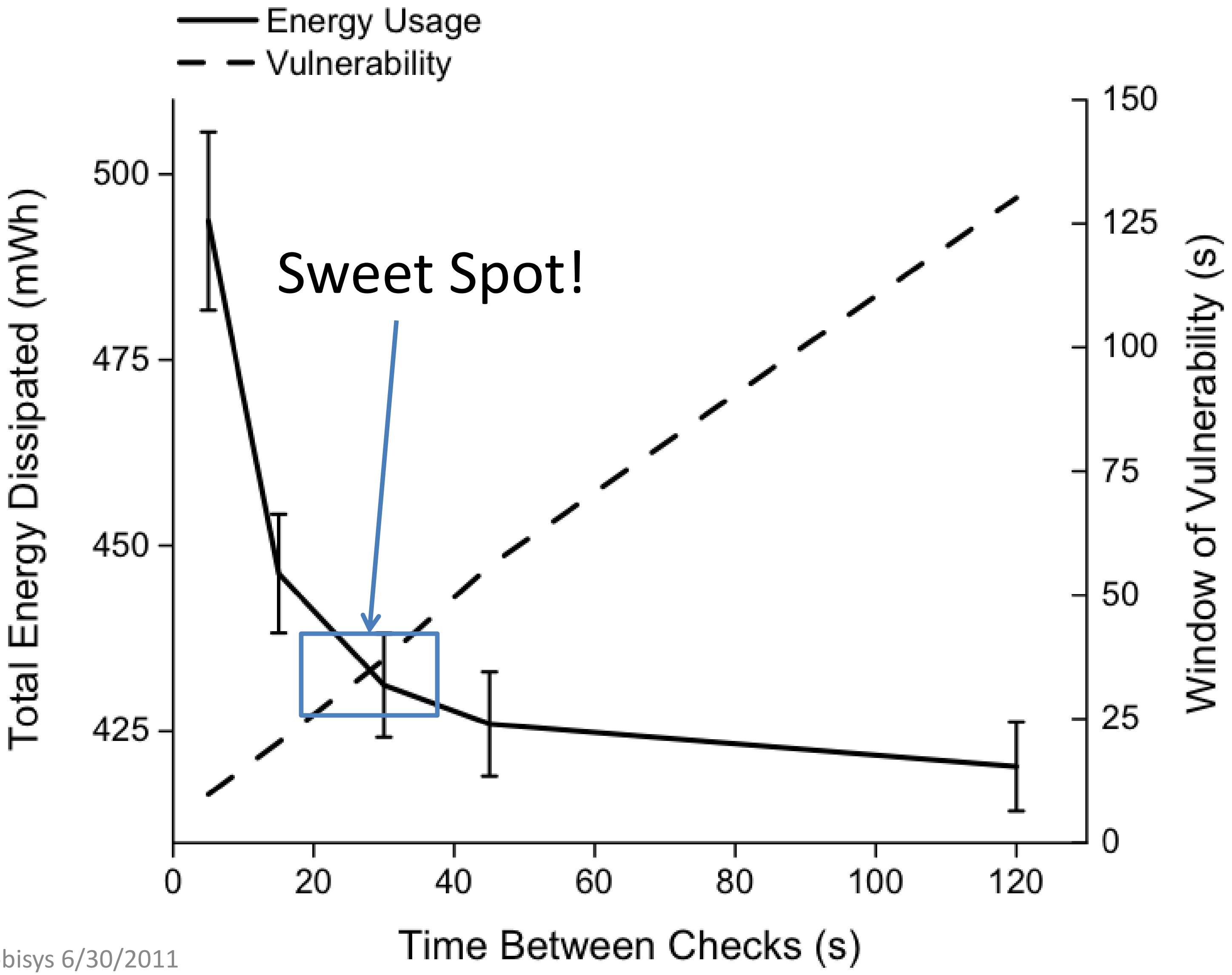
# Tradeoffs for Data-Based Detectors



# Frequency of Checks



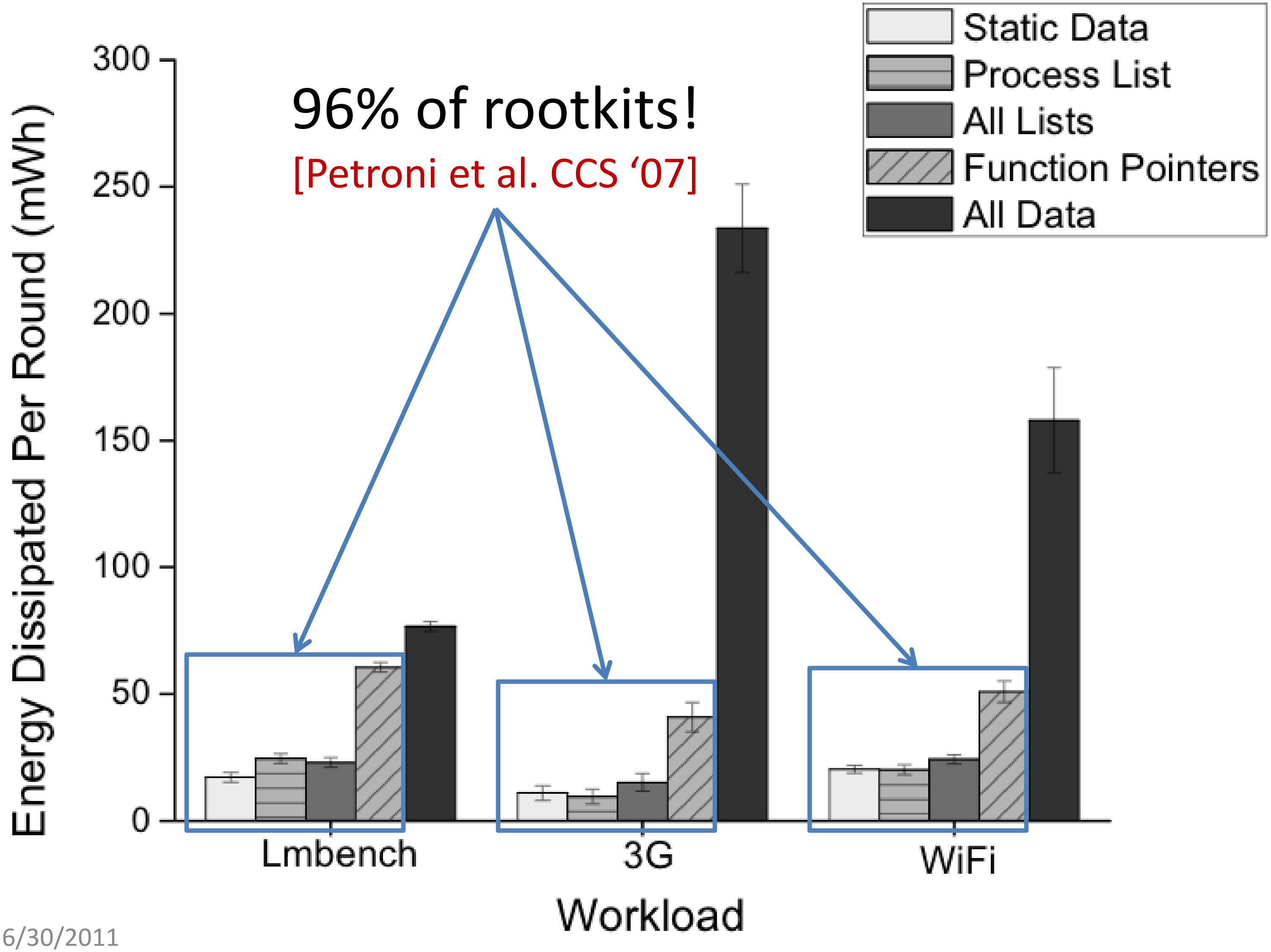
# Evaluating the Tradeoff



# Attack Surface

```
while(1) {
      ~~for all kernel data structures {~~
      for a subset of data structures {
            get current value
            check against invariant
      }
}
```

# Evaluating the Tradeoff



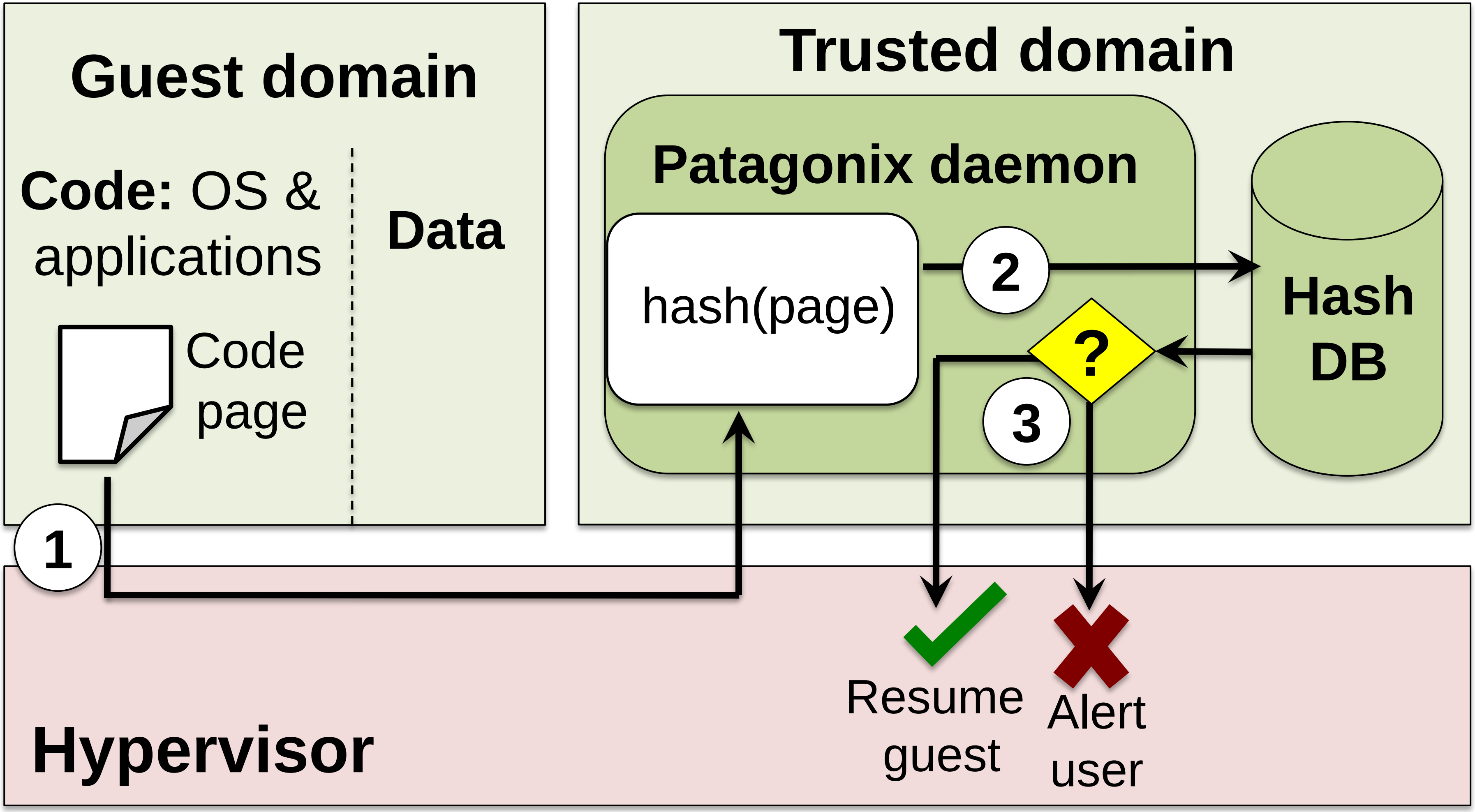
96% of rootkits!

[Petroni et al. CCS ‘07]

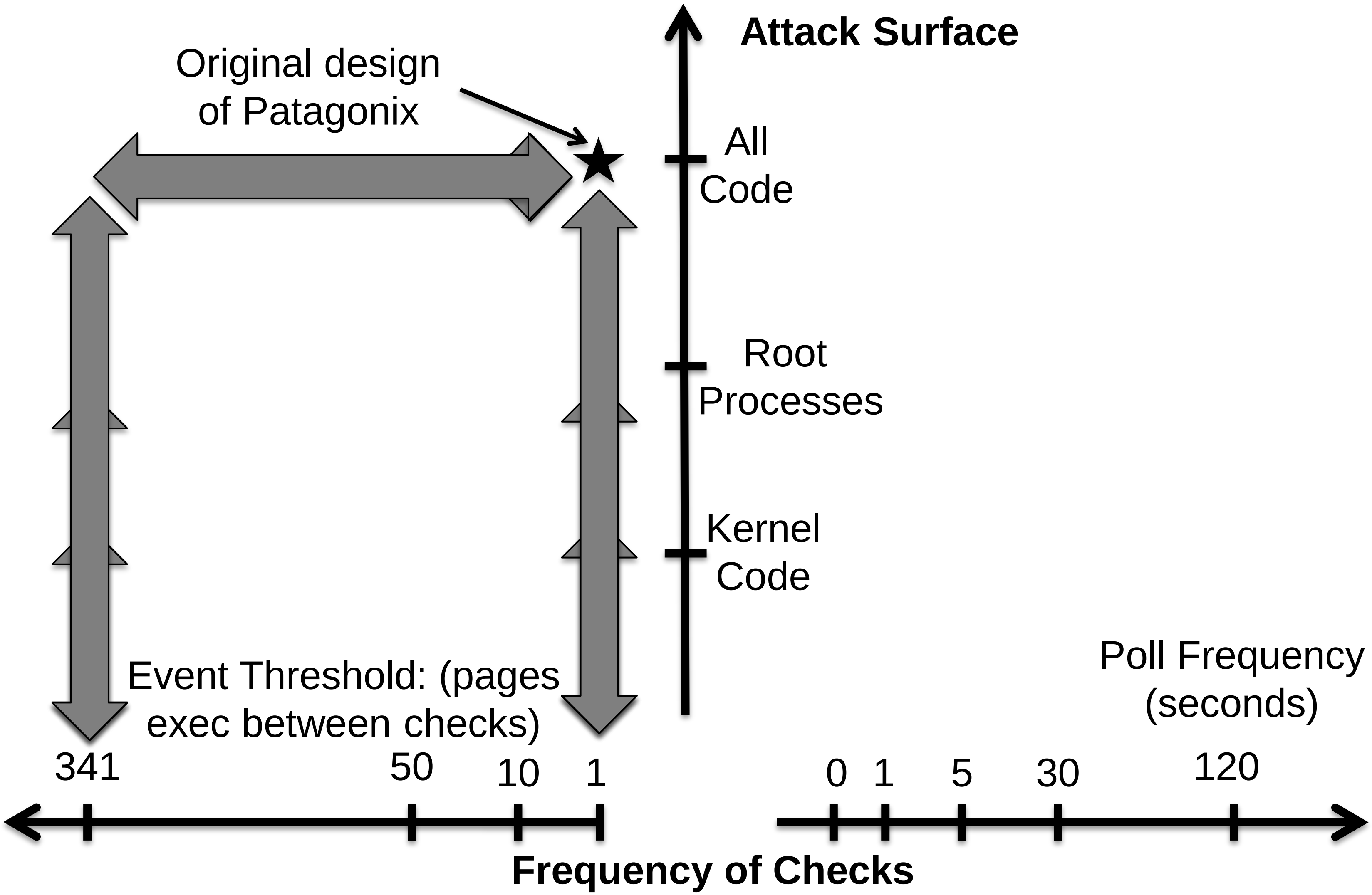
# Detecting Code-Driven Attacks

- **Patagonix** [Litty *et al.* USENIX Security ‘08] typifies most code integrity monitoring systems
- A different class of rootkits attack code
  - trojaned system utilities
  - kernel code modifications
- Can protect both kernel code and user space code
- Protects against a different set of attacks compared to Gibraltar

# Detecting Code-Driven Attacks

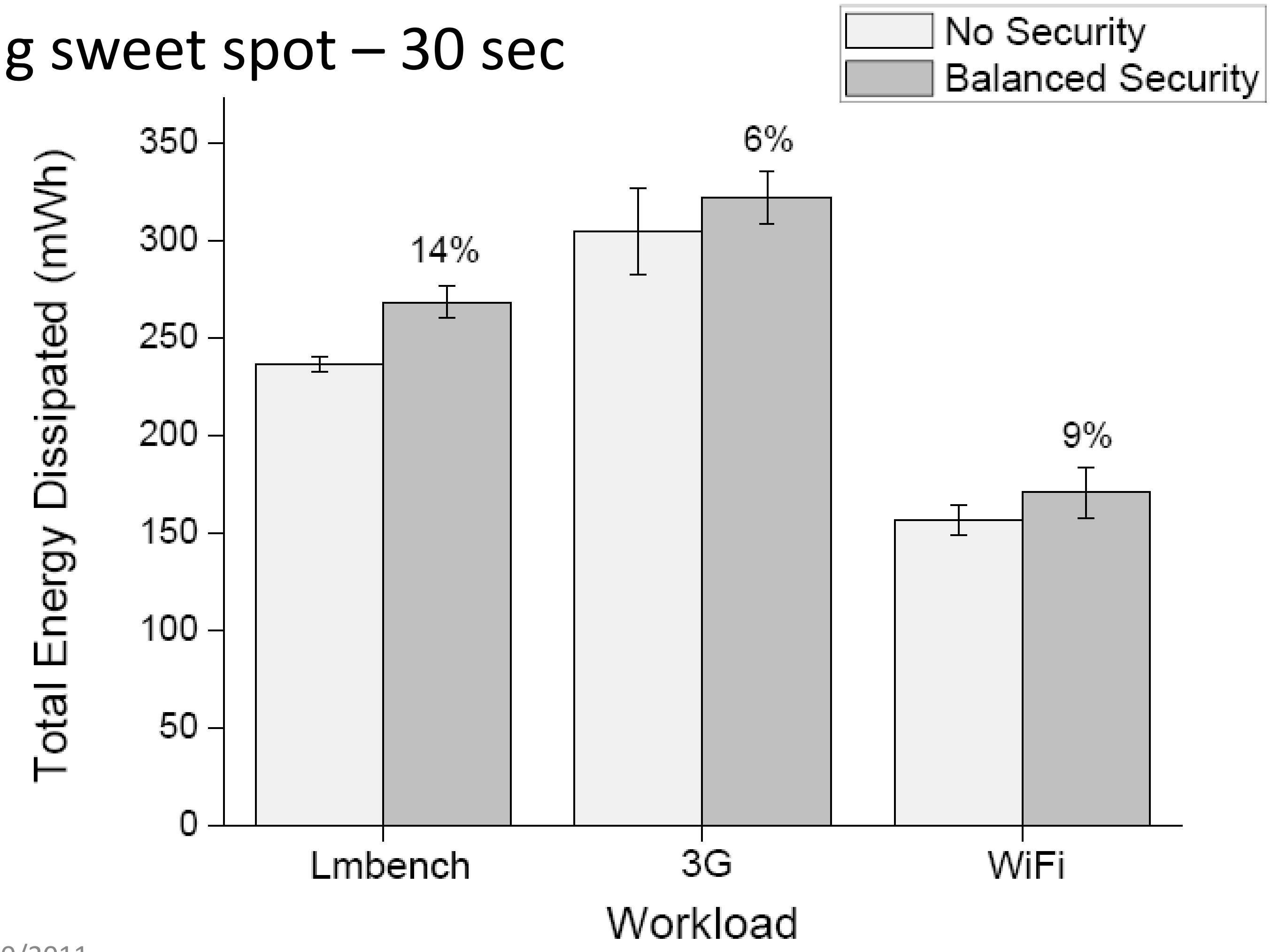


# Tradeoffs for Code-Based Detectors



# Putting it Together

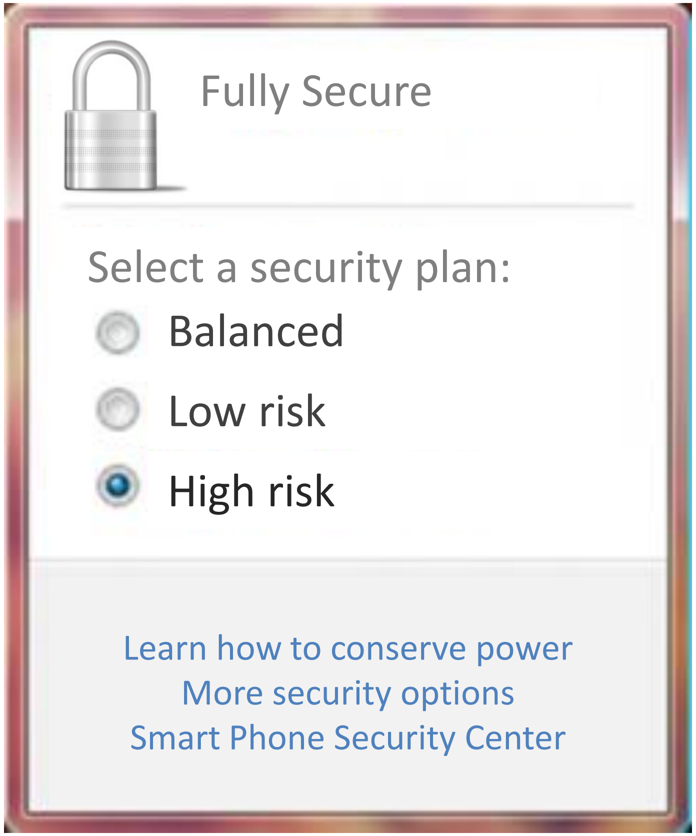
- Cover 96% of Rootkits
- Polling sweet spot – 30 sec



# Conclusion

- Mobile malware is a threat
- Security tools costly when energy constrained
- Developed a framework to quantify the tradeoff between energy efficiency and security
- Optimized two previously existing tools
- Generated a “balanced” security profile

# Thank You!



Fully Secure

Select a security plan:

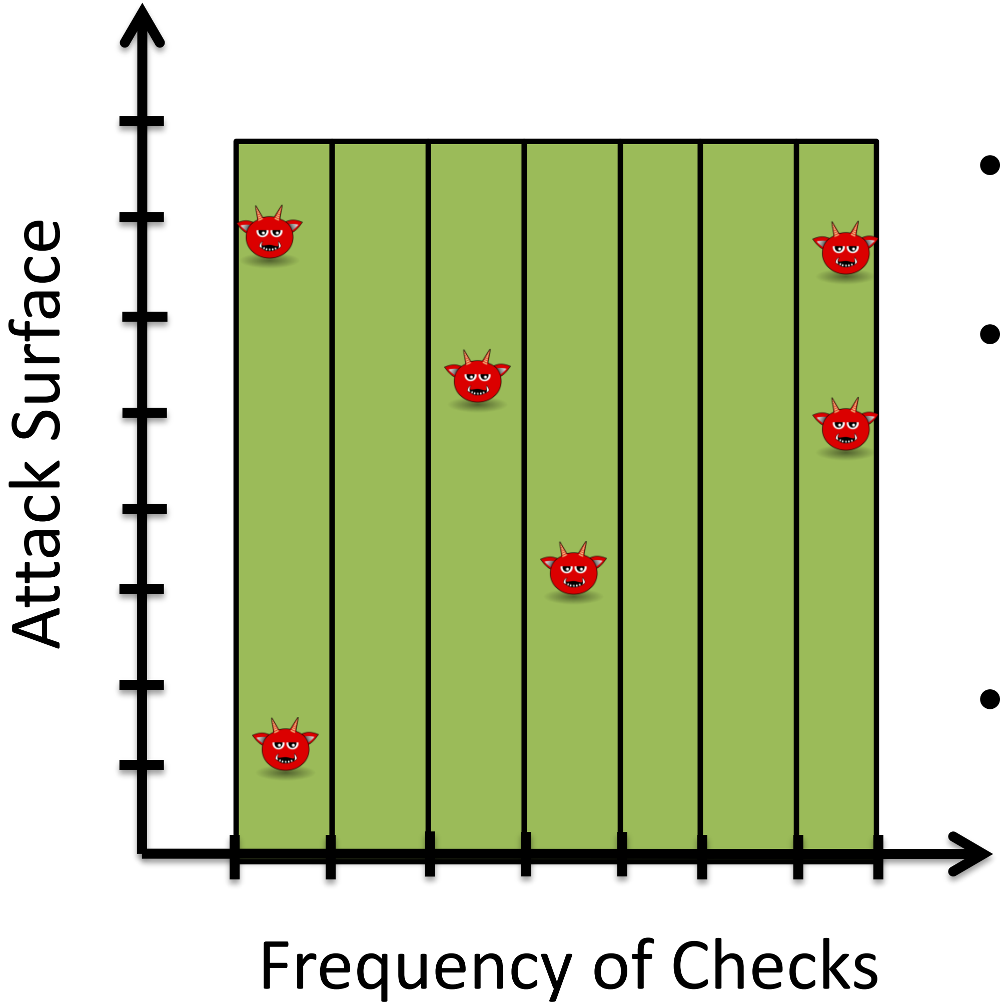
○ Balanced

○ Low risk

● High risk

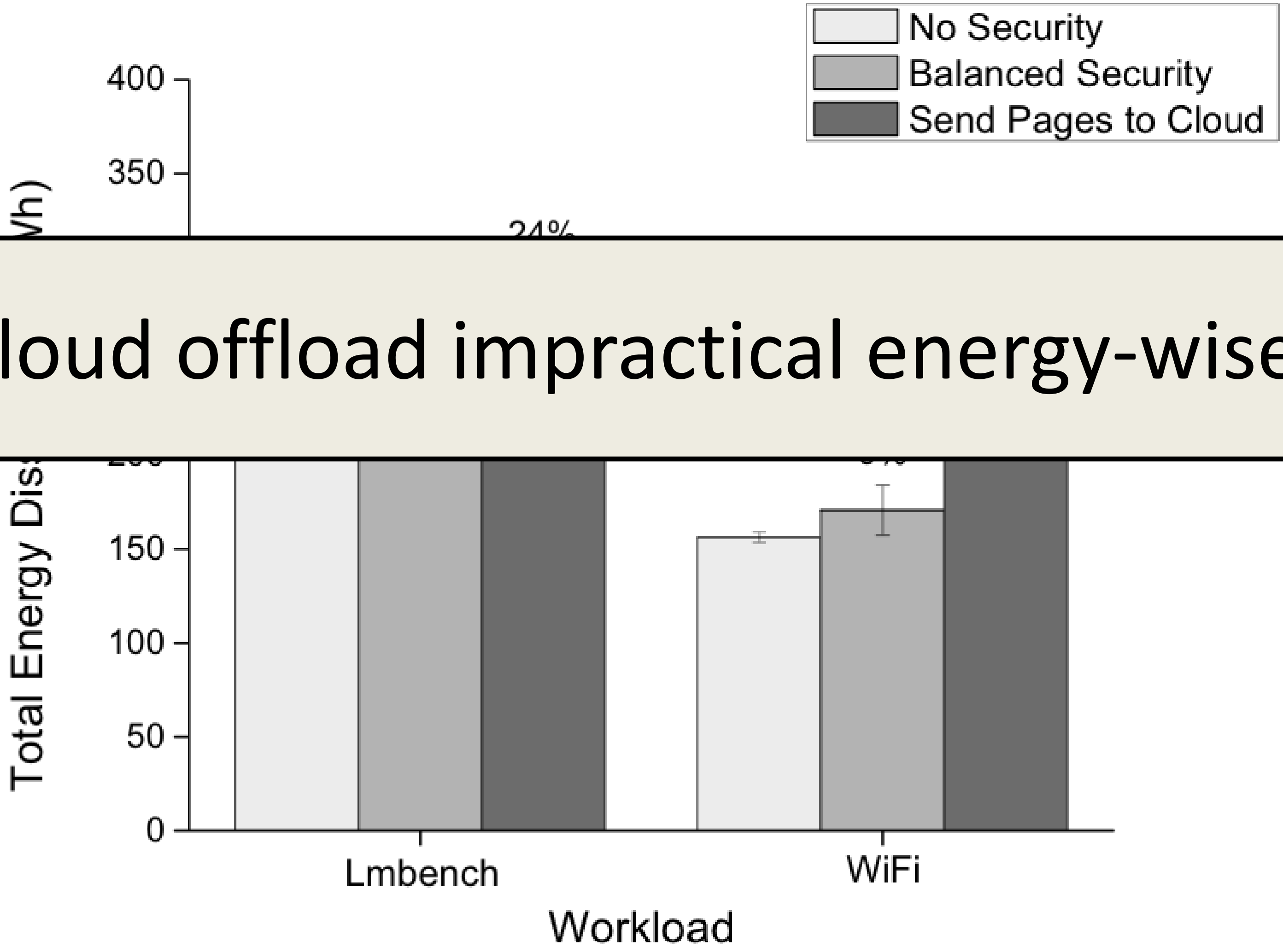
Learn how to conserve power
More security options
Smart Phone Security Center

# Randomization



- Periodically scan
- Attackers will attempt to exploit the system while idle
- Randomize the time the system is idle

# Cloud Offload Feasibility



Cloud offload impractical energy-wise