Physical Attack Protection with Human-Secure Virtualization in Data Centers

Jakub Szefer[§], Pramod Jamkhedkar, Yu-Yuan Chen and Ruby B. Lee

Princeton University

WORCS 2012 – July 25, 2012

[§] contact: szefer@princeton.edu

Data Centers as Cyber-Physical Systems

- Cyber-physical systems are tight integrations of computation, networking, and physical objects
- Data Centers are are one example of cyber-physical system:
  - Physical components: utilities, physical constraints, etc.
  - Cyber components: management software, servers, networking, etc.

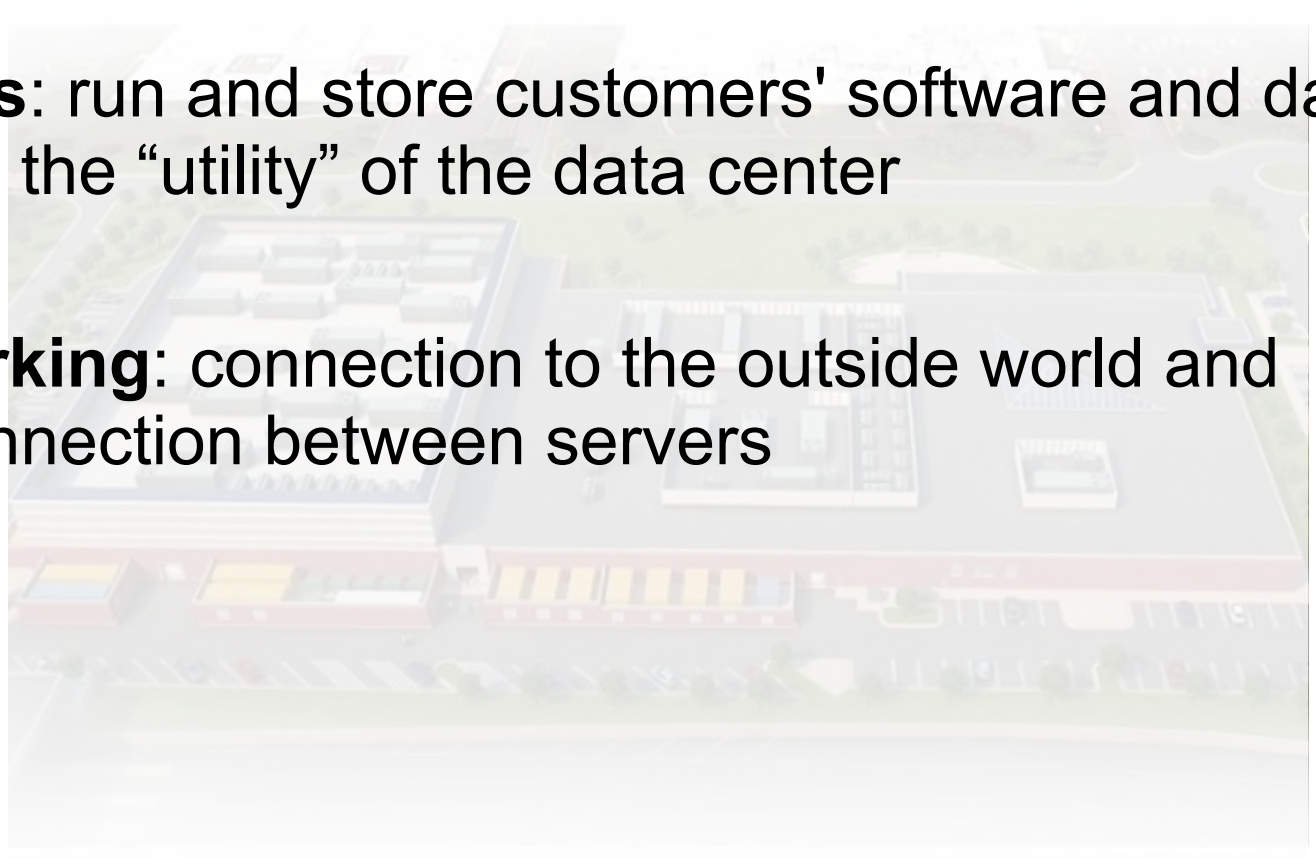
Physical Aspects of Data Centers

- **Utilities**: cooling, power supply, backup power, etc.
- **Physical constraints**: barriers, checkpoints, floor plan, etc.
- **Sensors**: cameras, climate control

Background image source: http://www.datacentermapping.com

Cyber Aspects of Data Centers

- **Management software**: software framework for management of the resources
- **Servers**: run and store customers' software and data; they provide the “utility” of the data center
- **Networking**: connection to the outside world and interconnection between servers



Data Centers as Cyber-Physical Systems

- Data enters tie in many cyber and physical aspects:

Management Servers Networking		Utilities Physical constraints Sensors

- Data centers are becoming utilities

- Like any utilities, there face security concerns

What is coming up...

- Data Center Security
- Human-Secure Design
- Cyber-Physical Defenses
- Human-Secure Virtualization
- Conclusion

Data Center Security

- Data center security needs to combine all three aspects of security:

Data Centers Security Concerns

- **Availability**:
  - Support infrastructure (water, cooling, electricity, etc.)
  - Customer's access to their software or data
- **Integrity**:
  - Modification of software or data running in data center
  - Software or data change in transit (e.g. over network)
- **Confidentiality**:
  - Customer's code or data leaking

Data Centers Security Concerns

- **Availability**:
  - Support infrastructure (water, cooling, electricity, etc.)
  - Customer's access to their software or data
- **Integrity**:
  - Modification of software or data running in data center
  - Software or data change in transit (e.g. over network)
- **Confidentiality**:
  - Customer's code or data leaking

Data Centers Security Concerns

- **Cyber**:
  - Software attacks on servers
  - Network attacks, denial-of-service
  - Exploits in management software
- **Physical**:
  - Physical intrusion
  - Probing of hardware
  - Equipment theft
  - Infrastructure alterations

Data Centers Security Concerns

- **Cyber**:
  - Software attacks on servers
  - Network attacks, denial-of-service
  - Exploits in management software

- **Physical**:
  - Physical intrusion
  - Probing of hardware
  - Equipment theft
  - Infrastructure alterations

Why focus on physical attacks?

Thursday, March 17, 2011

A Second Data Breach at Health Net Affects 1.9 Million Consumers

On Monday of this week, Health Net announced a data breach and the company's ongoing investigation into lost/stolen server drives from its data center in Rancho Cordova, Calif. According to the press release:

"This investigation follows notification by IBM, Health Net's vend
responsible for managing Health Net's IT infrastructure, that it c
locate several server drives. After a forensic analysis, Health Net
determined that personal information of some former and currer
Net members, employees and health care providers is on the driv
may include names, addresses, health information, Social Securit
numbers and/or financial information."

Server Hard Disks Stolen 2012-02-29

The Haslingden, Lancashire offices of Avnet were broken into on December 21, 2011. Server hard disks -- and not the servers themselves -- were stolen. These contained data on staff and customers related to the acquisition of Bell Micro. While *channelregister.co.uk* originally reported that addresses, bank account numbers, sort codes, passport numbers, and national insurance numbers were stolen, it was later contacted by Avnet, and a correction was issued: passport and national insurance numbers were not part of the stolen data.

Avnet would not confirm how many people were affected by the breach, or how many hard disk drives were stolen.

The Insider Threat in the Cloud

Posted by Michael Vizard Apr 18, 2011 8:38:35 AM

When it comes to **public cloud computing, there are a lot of concerns not only about security**, but about compliance and ongoing governance as well.

Within data centers, companies have become much more stringent about documenting IT processes because of concerns over insider threats. Whether those concerns are real or not is often debatable. But because the people that conduct audits have identified them as a major issue, process controls within the data center need to be consistent and well-documented.

When companies start thinking about using public cloud computing resources, however, this becomes an issue. There is usually no procedures in place to document who accessed what server when, which can be especially problematic when it comes to shared infrastructure scenarios where multiple administrators are accessing the IT infrastructure in support of applications owned by different companies.

Biggest insider threat? Sys admin gone rogue

IT workers with privileged access seen as high risk

By Ellen Messmer, Network World
September 27, 2010 06:08 AM ET

2 Comments Print

What's one of the biggest insider threats to the corporate network? The high-tech folks that put it together, make changes to it, and know more about what's on it and how it works than anybody else.

When the database, network or systems administrator goes rogue -- stealing data, setting up secret access for themselves, even in anger planting logic bombs to destroy data , or just peeking at sensitive information they know is off limits -- they become the very insider threat that the IT department is supposed to be guarding against.

What's coming up...

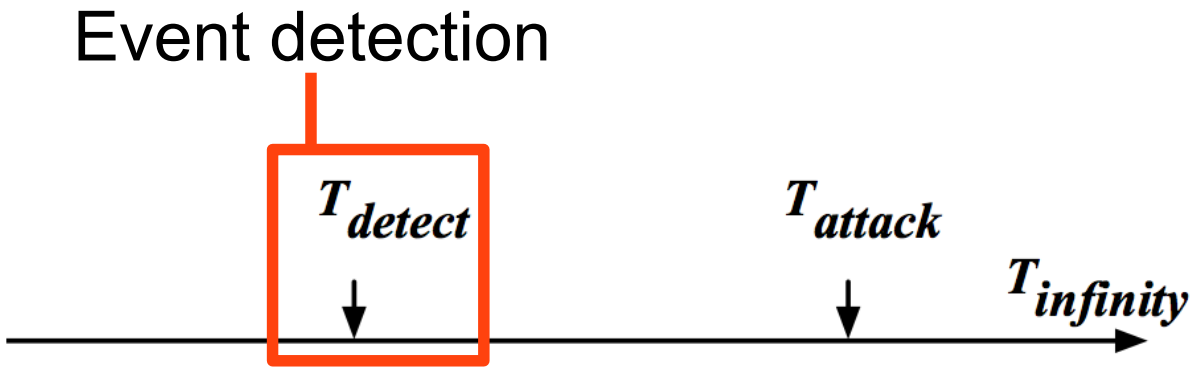
- Data Center Security
- Human-Secure Design
- Cyber-Physical Defenses
- Human-Secure Virtualization
- Conclusion

Human-Secure Design

- Human-aware design:
  - Use existing infrastructures to track humans in data centers
  - Use information to predict potential risks
- Self-adapting design:
  - Adjust security measures to keep track with infrastructure changes
  - Apply security measures suitable for given estimated defense time

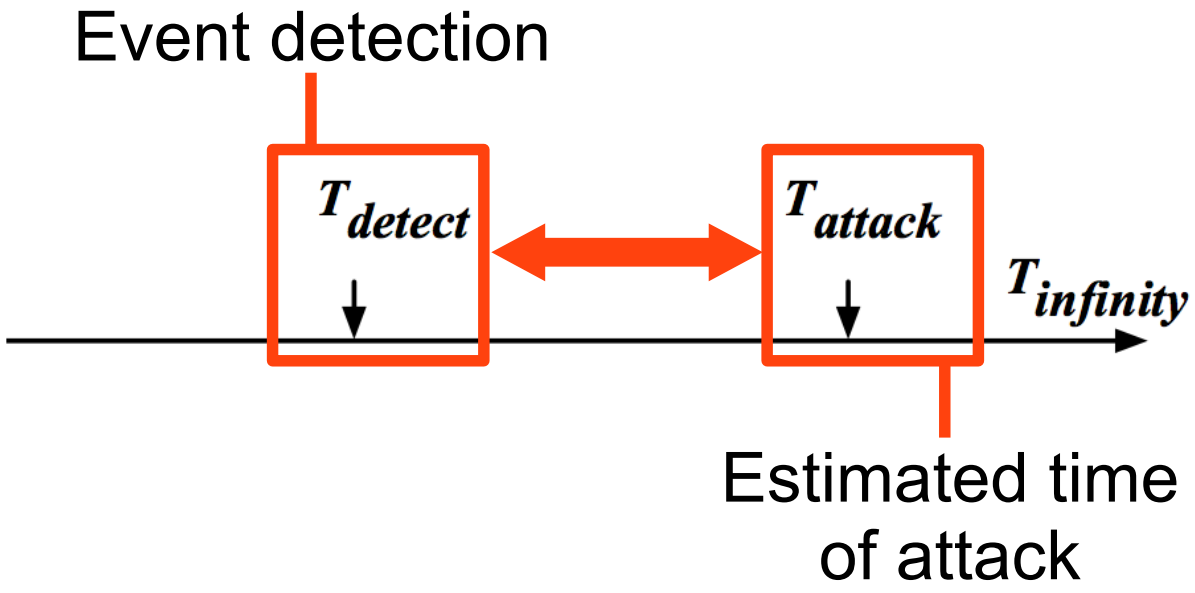
Activating Defenses Ahead of Attack

- Existing sensors can give warning time before potential threat



Activating Defenses Ahead of Attack

- Existing sensors can give warning time before potential threat
- Physical constraints give time delay to take protective actions



Past Physical Defenses

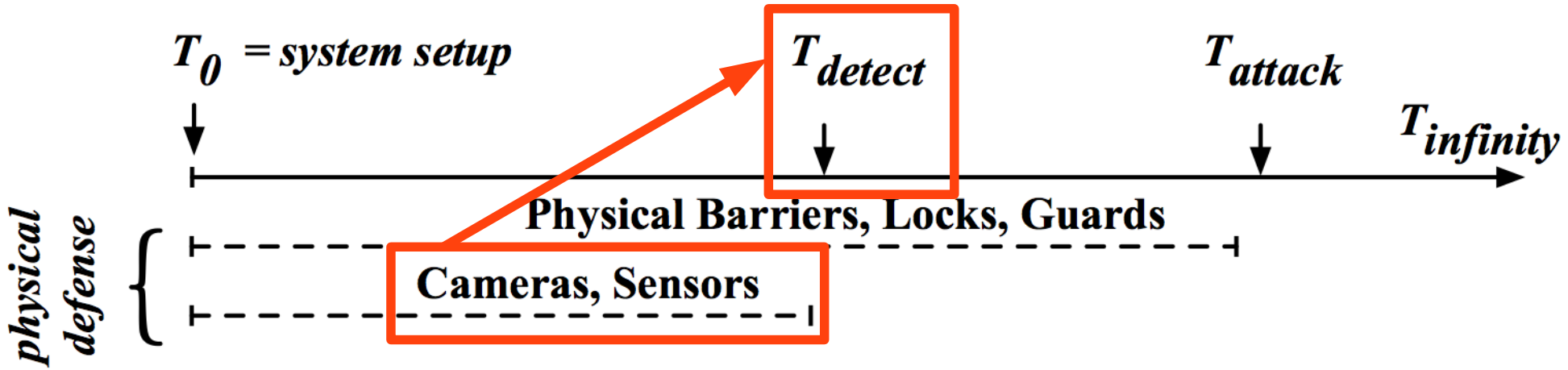
- Physical threats have motivated physical defenses in the past
  - Locks, barriers, monitoring, etc.
- Good measures but have shortcomings:
  - Reactive
  - Ineffective after attack
- Still, can leverage the physical defenses...

What's coming up...

- Data Center Security
- Human-Secure Design
- Cyber-Physical Defenses
- Human-Secure Virtualization
- Conclusion

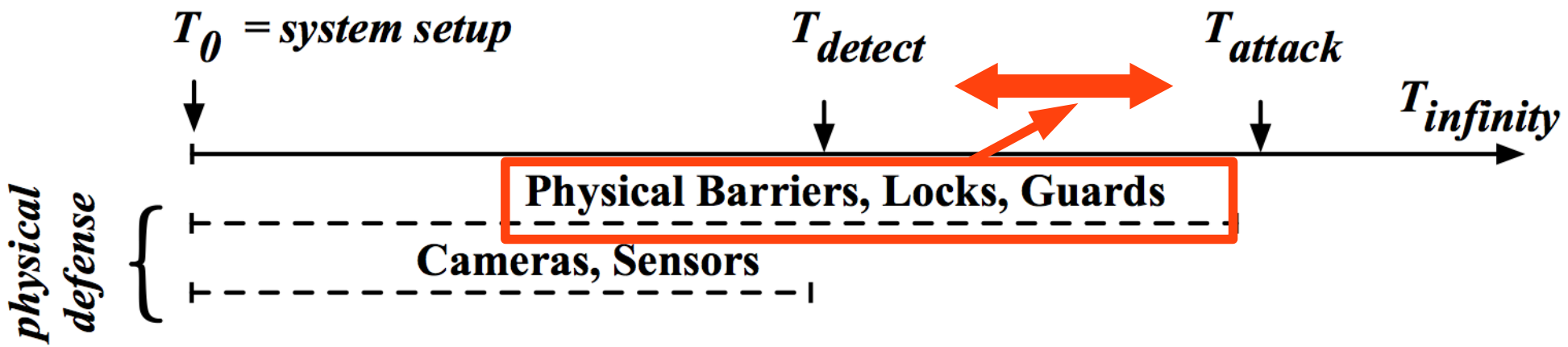
Leveraging Physical Defenses

- Physical defenses can provide:
  - Warning time
  - Attack delay



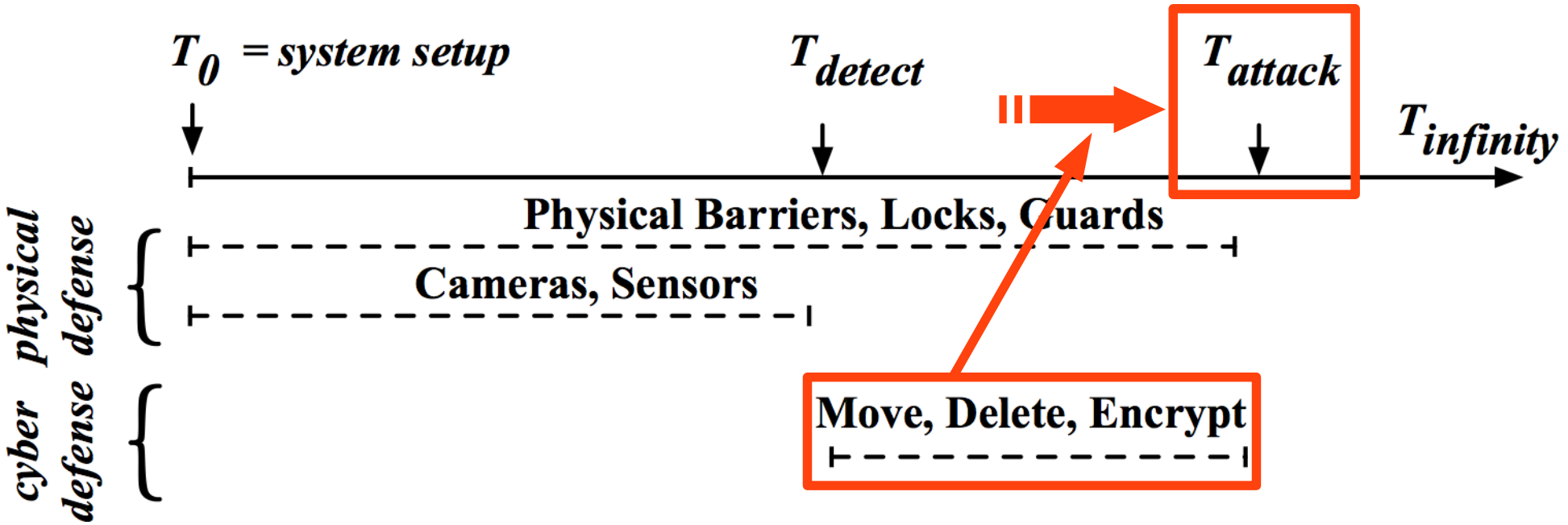
Leveraging Physical Defenses

- Physical defenses can provide:
  - Warning time
  - Attack delay



A Cyber-Physical Defense

- Cyber defenses are activated when a threat is discovered
- Estimated attack time guides choice of defense mechanisms



Cyber Defenses and Virtualization

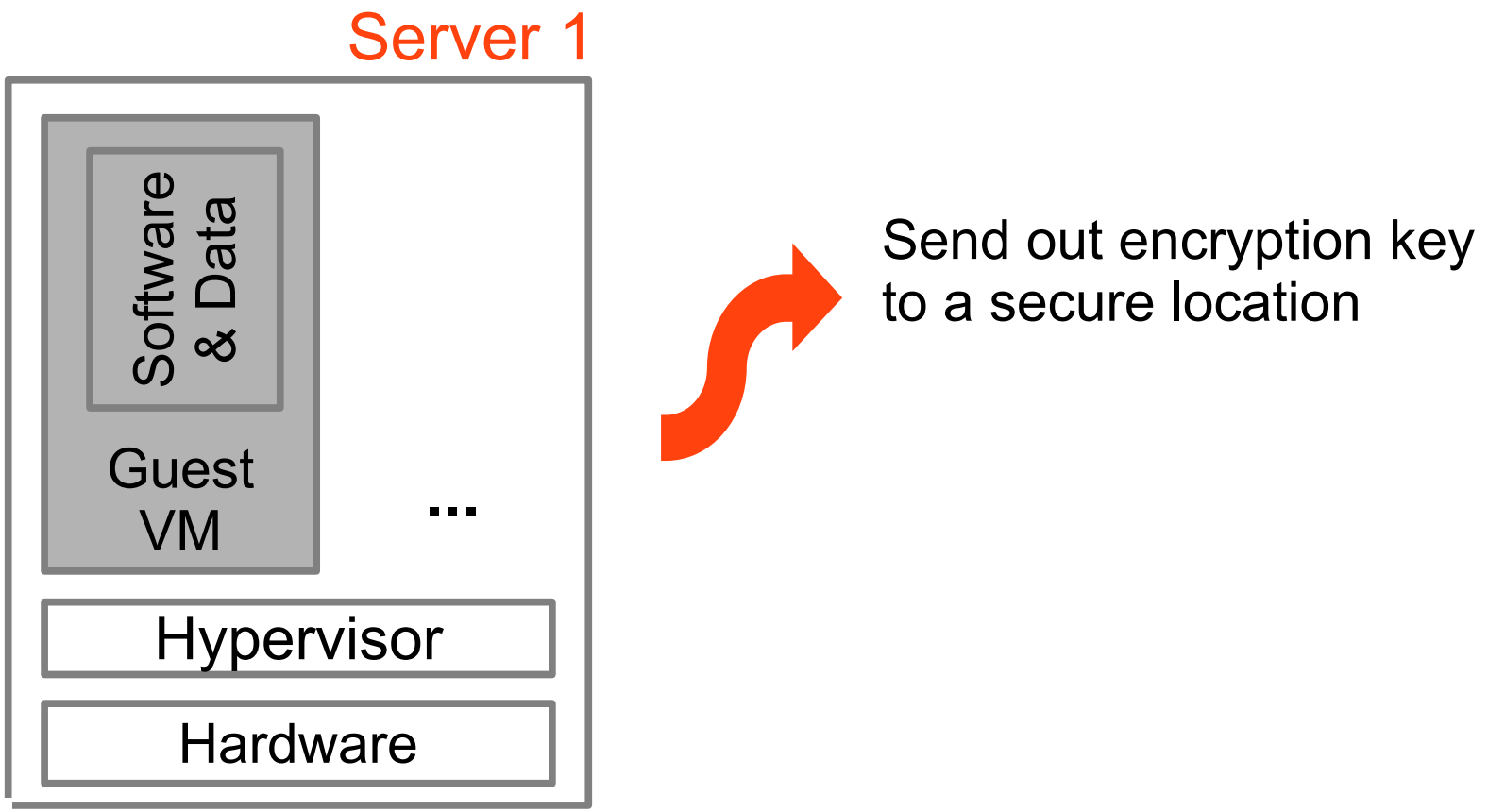
- Software and data are conveniently contained inside virtual machine
  - A virtual server, same properties as physical server
  - But not bound to a specific physical machine
- Virtualization software supports or can be modified to support:
  - Moving virtual machine → migration
  - On-demand encryption of code and data
  - Deletion of code and data

Defense: Move

- Relocate software and data to avoid threats
- Virtual machine migration can be used to move the software and data anywhere

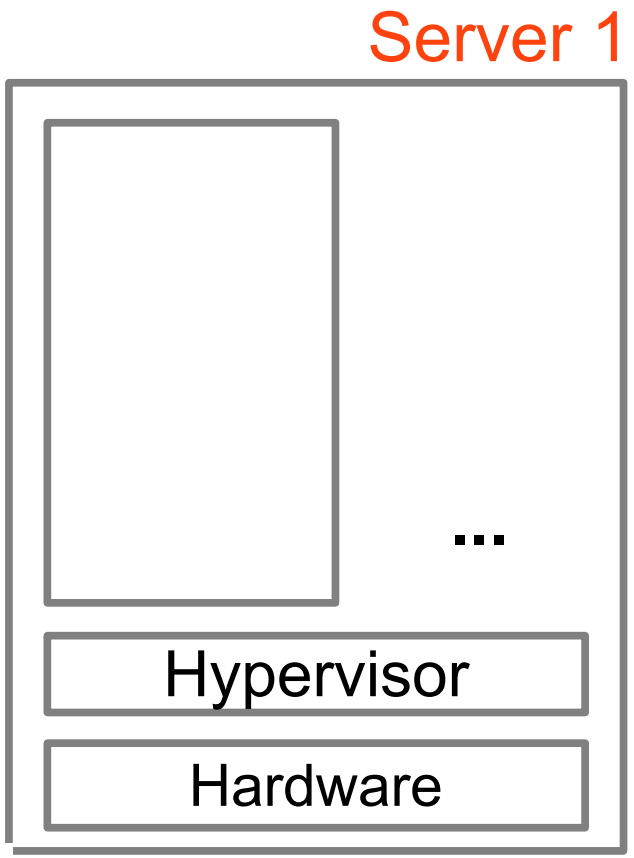
Defense: Encrypt

- Lock down applications and data with encryption (and hashing) to protect confidentiality (and integrity)



Defense: Delete

- A last resort is to delete all the sensitive software and data



Defense Strategy Comparison

- No one strategy is best
  - Each offers different protections
  - Each has different cost (time, compute power, network bandwidth)
- An algorithm is needed to match the estimated time for defense and expected protections to the strategy

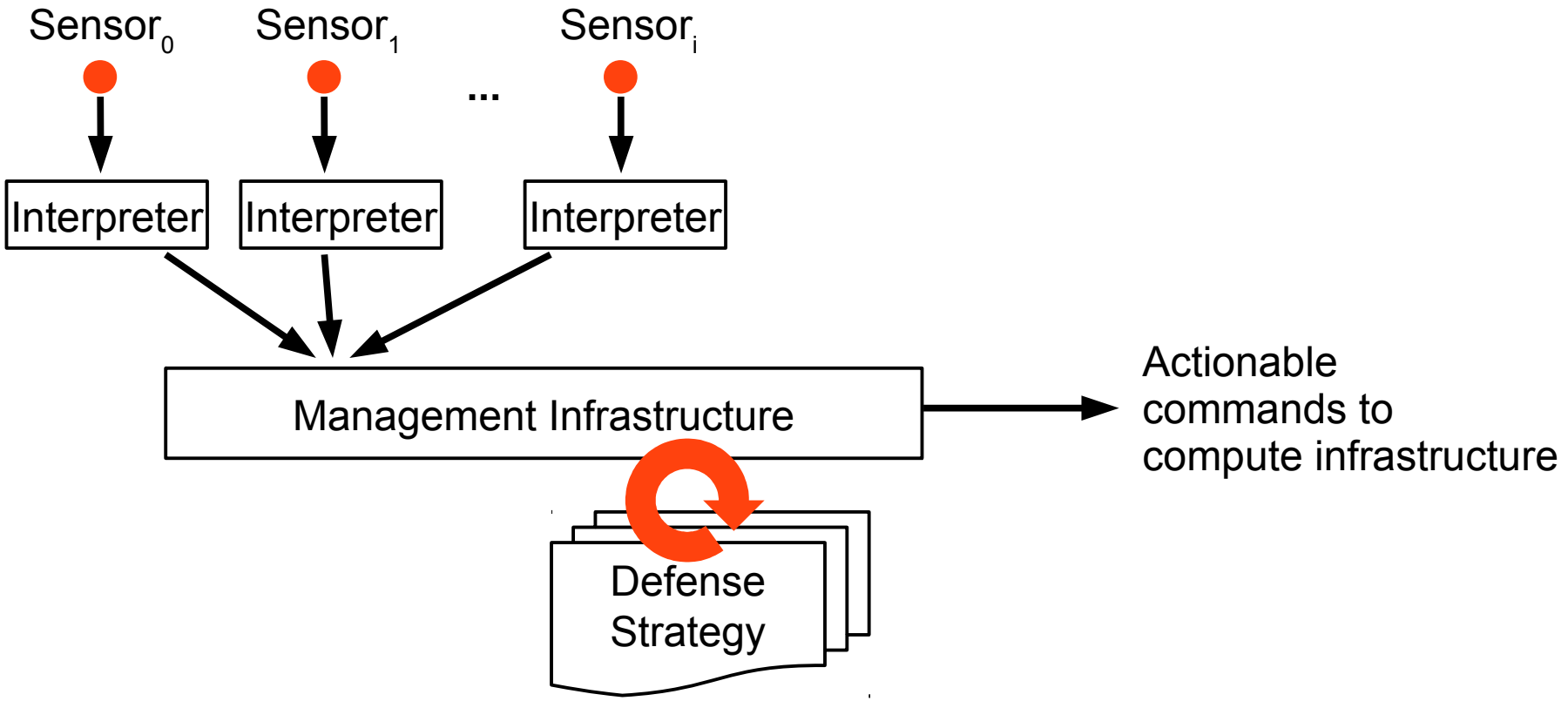
Defense	Confidentiality	Availability	Integrity	Cost
Delete	Yes	No	No	Low
Encrypt	Yes	Limited	No	Medium
Move	Yes	Yes	Yes	High

What's coming up...

- Data Center Security
- Human-Secure Design
- Cyber-Physical Defenses
- Human-Secure Virtualization
- Conclusion

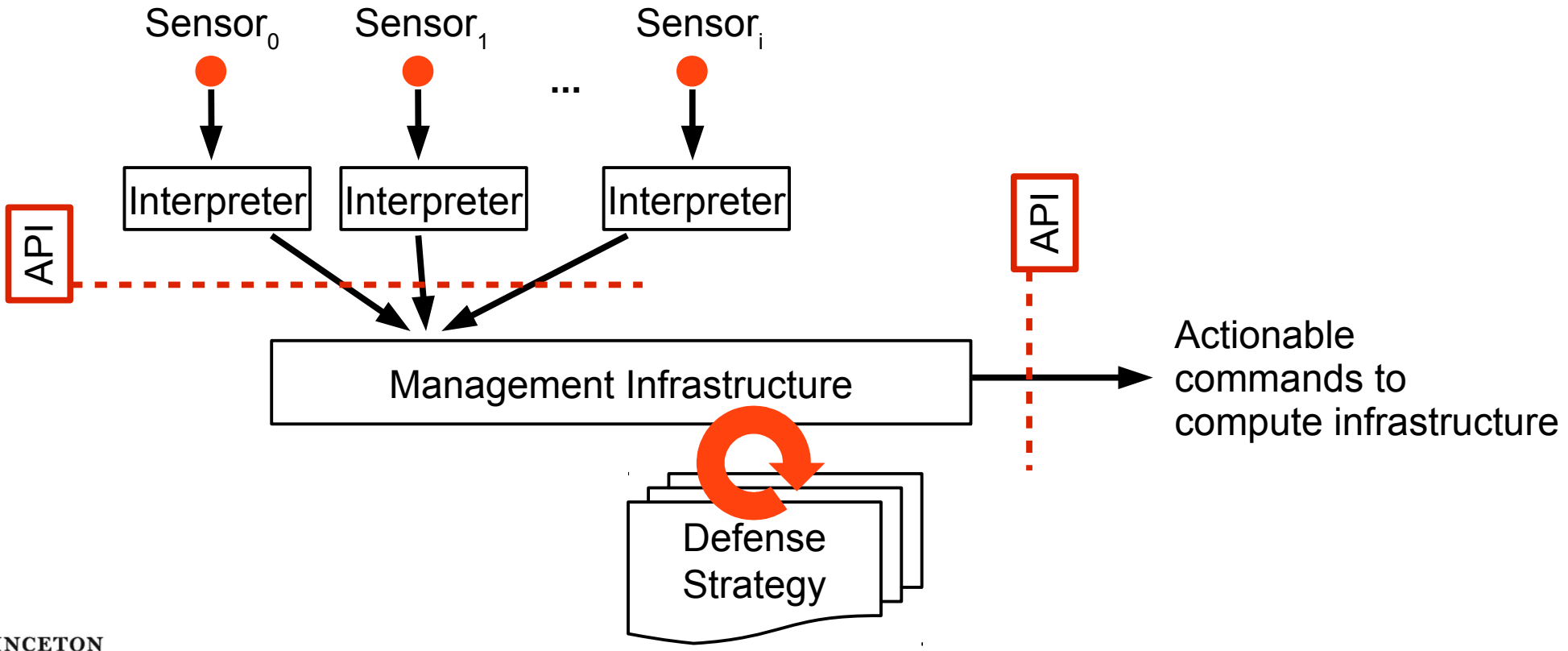
Human-Secure Virtualization

- Human-secure virtualization combines the three techniques of move, encrypt and delete to protect virtual machines from human attackers



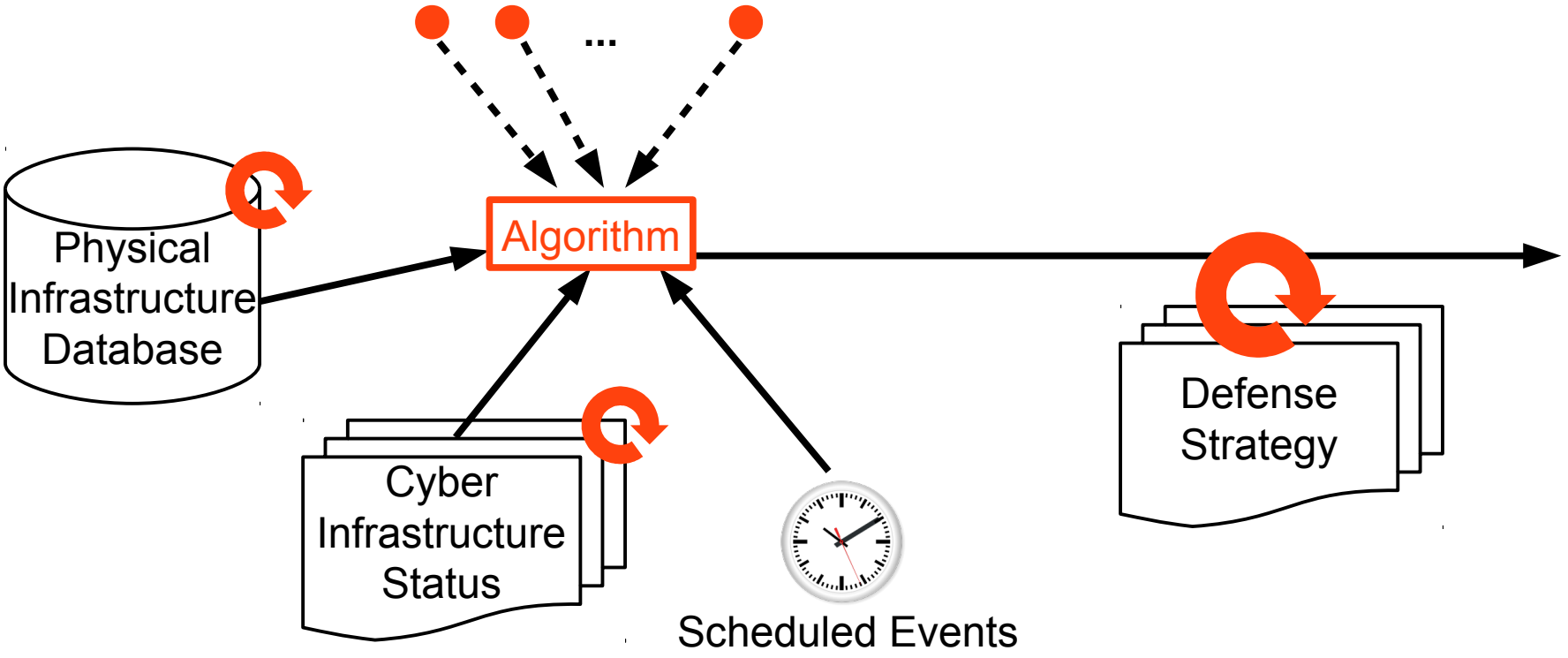
Human-Secure Virtualization

- First, focus on APIs for management and compute infrastructures



Human-Secure Virtualization

- Next key part is the algorithm for managing defenses:



Next Steps

- Our work is on implementing the full system
  - APIs for management and compute infrastructures
  - Next steps to develop the algorithms
- Focus on OpenStack open-source management software
- Looking for collaborators in areas:
  - data center design
  - algorithms
- Many interesting research issues still to solve!

Continuation of Virtualization Security Work

- **Hypervisor-Free Virtualization**
  - Jakub Szefer and Ruby B. Lee, "Architectural Support for Hypervisor-Secure Virtualization," in Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), March 2012.

- **Hypervisor-Secure Virtualizaiton**
  - Jakub Szefer, Eric Keller, Ruby B. Lee and Jennifer Rexford, "Eliminating the Hypervisor Attack Surface for a More Secure Cloud," in Proceedings of the Conference on Computer and Communications Security (CCS), October 2011.

What's coming up...

- Data Center Security
- Human-Secure Design
- Cyber-Physical Defenses
- Human-Secure Virtualization
- Conclusion

In Conclusion...

- Data centers are interesting and important example of cyber-physical systems
- Defined human-secure virtualization
- Design of a system needed for physical attack protection in data centers:
  - Focus on human attackers
  - Leverage physical sensors for detection
  - Leverage virtualization for cyber defenses

Thank you.

Physical Attack Protection with Human-Secure Virtualization in Data Centers

Jakub Szefer[§], Pramod Jamkhedkar, Yu-Yuan Chen and Ruby B. Lee

Princeton University

WORCS 2012 – July 25, 2012

[§] contact: szefer@princeton.edu