

# *Cyber Economic Incentives*

**Alessandro Acquisti**

Heinz College/CyLab  
Carnegie Mellon University

*Toward a Federal Cybersecurity Research Agenda:  
Three Game-changing Themes*

# A problem of information, incentives, and rationality

---

- Research in cybersecurity economics has been growing (WEIS, FC, SOUPS, SHB, ...)
- Yet, we still debate basic issues – such as whether markets can provide the solution, and what business case can be made for security. Why?
  - Asymmetric, incomplete information
  - Misaligned incentives and externalities
  - Bounded rationality and cognitive biases

# Addressing incomplete information

---

- Insufficient data
  - Disorganized metrics
  - “Early stage” models
- Incentivizing data gathering and information sharing, fostering in turn better metrics and better models
- However: coordination costs, disincentives to share

# Addressing misaligned incentives and externalities

---

- Do we invest too much? Not enough? Just right?  
Or, perhaps, not *well* enough?
- ➔ Leveraging incentives, liabilities, and regulation
  - However: (not) a zero sum game
  - Holistic approach - identify roadblocks, policy will
  - Government as market maker: Cyber-insurance

# Addressing bounded rationality and cognitive biases

---

- Information and choice are good – but not enough
- Numerous cognitive biases affect security (and privacy) decision making
- ➔ Need to understand them, in order to anticipate them
  - Perhaps even “exploit” them, *nudging* users towards security
  - Security as the *default* setting

# For more info

---

- <http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm>
- Google: economics privacy
- <http://www.cl.cam.ac.uk/~rja14/econsec.html>
- Google: economics information security

# Hardware-Software Security Research Challenges

Ruby B. Lee  
Princeton University

Cybersecurity R&D Themes Panel  
May 19, 2010, Oakland, California.

# A possible rationale for a few themes

- Security must be end-to-end and top-to-bottom (preferably bottom-to-top)
- There are no silver bullets or easy answers
- However, with finite funds and the escalation of cyber attacks and increasing damages, are there some research directions that have game-changing potential?
- By proposing a shared vision and common goals, can we inspire the research community to produce novel, effective, synergistic and deployable results?

# Impact of Game-Change Vision on Research

- Goal: Significantly improve cyber security by changing the rules of the game, so that effective attacks are much harder to achieve
- Requires **out-of-the-box rethinking** of systems
  - hardware, software, networking
  - holistic, at all levels
- Implicitly includes **clean-slate designs** in security research!
  - Compatibility with existing systems not an absolute requirement, BUT
  - **new architectures should be realistically deployable**

“Security without compromising  
Performance, Energy consumption,  
Cost and Usability”

Lee's mantra

# Example: Current Game

- Applications developer may put in comprehensive security policies and mechanisms for a security-critical task, or to protect the confidentiality or integrity of secret, sensitive or critical information
- However, this can easily be undermined by
  - a compromised lower layer of systems software, or
  - independent hardware mechanisms and policies for which the application developer has no control
- **Attacker's strategy: Attack Below**
- **Problems: all-powerful and all-seeing, complex OS; security solutions that ignore hardware**

# Tailored Trustworthy Spaces (New Game)

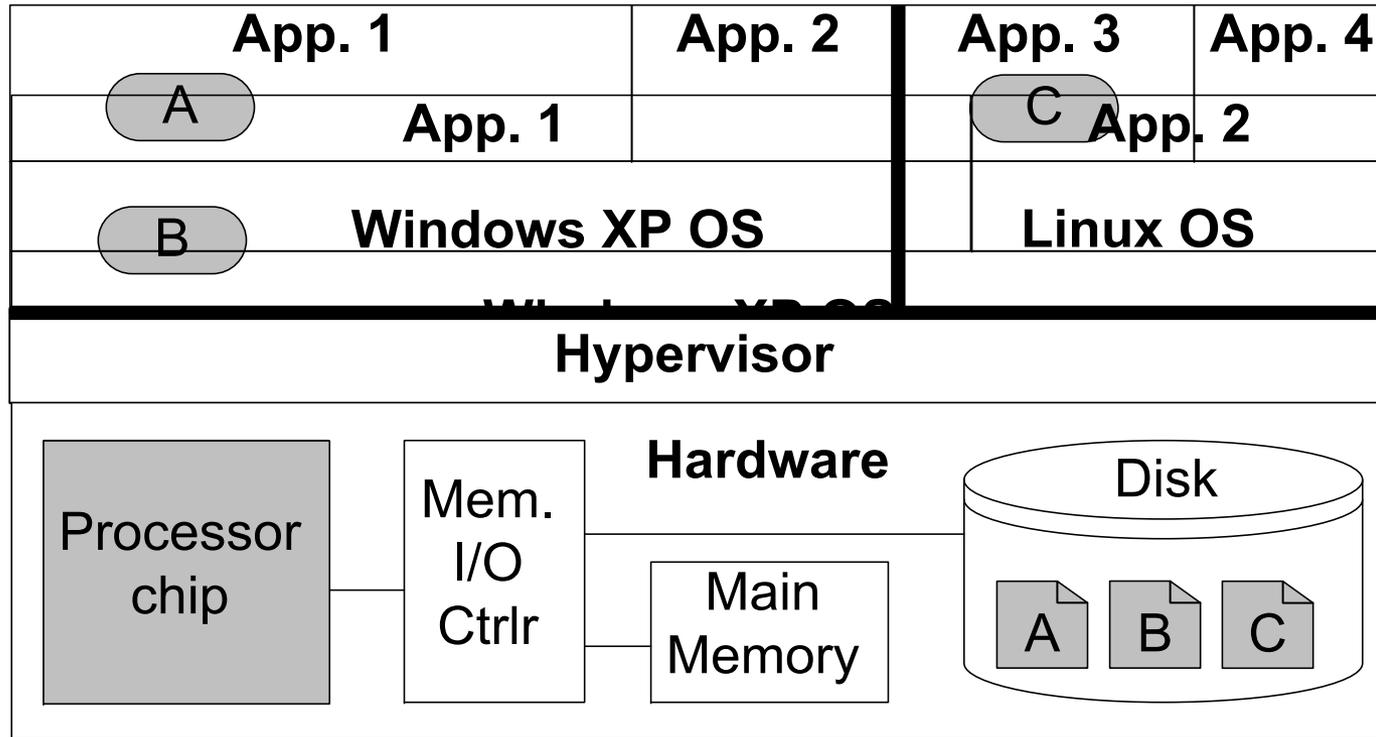
- Can we change the game so that the stakeholders **can control** their own destiny?
- Can we define new hardware-software architectures that enable applications to **be responsible** for their own security?
  - Minimize the “blame game”
  - Minimize the attack surface
  - Resilient execution of security-critical tasks even in the presence of malware in the system
  - Data that protects itself from security violations
  - “Tailored attestation” and data provenance

# Some Research Questions

- How to use the services of system software (e.g., OS) without trusting it completely?
- Can new hardware-software mechanisms provide a secure execution environment for security-critical software modules, in spite of a compromised OS and malware in parts of the system?
- How to achieve security solutions that have the flexibility and adaptability of software, with the trust anchors, non-bypassable enforcement and performance of hardware?
- How to determine if remote end-points are trustworthy, and if sufficient trust exists across heterogeneous systems?
- How to grade trustworthiness of software and hardware?

# Feasibility Example:

e.g., SP and Bastion architectures



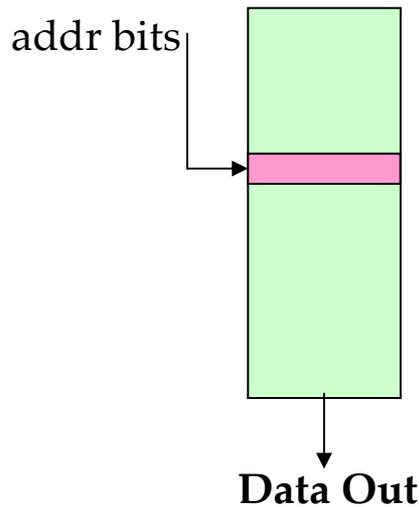
= Untrusted
  = Trusted

# Current Game

- Fundamental performance optimization methodology:  
**Make frequent paths fast, infrequent paths slow**
- Problem: enables information leakage through side-channel and covert-channel attacks;
  - Processor or cache-based side channels are extremely fast and easy to launch (through software, even remotely)
  - Undermines software isolation mechanisms, e.g., Virtual Machines
- **Attacker's strategy: Exploit hardware performance (or power) optimization mechanisms to leak information**
- **New Game:** Need new methodologies for improving performance and security simultaneously
  - e.g., based on randomization

# Feasibility example: improving Cache performance and security simultaneously

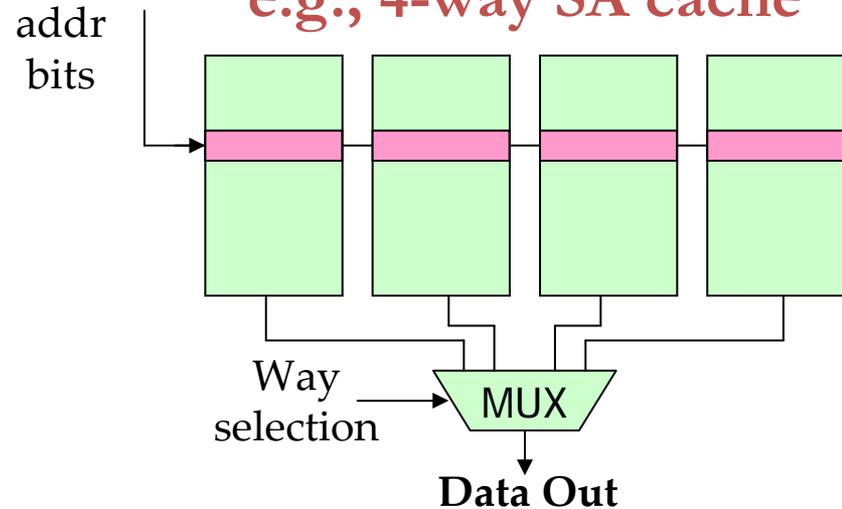
## Direct-Mapped caches



Lower access time  
Lower power per access

## Associative caches

e.g., 4-way SA cache



Lower cache miss rate

Newcache achieves best of both classes of cache architectures

# Hard Research Problems

- How to define tailored trustworthy spaces, their attack surfaces and protect them from attack?
- What are fundamental hardware-software requirements and architectures that enable tailored trustworthy spaces?
- What are new methodologies for improving system performance that do not leak protected information?
- How to employ efficient randomization techniques to provide a moving target defense, or bio-inspired computing, etc., to increase resiliency to attacks?

Challenge the status quo

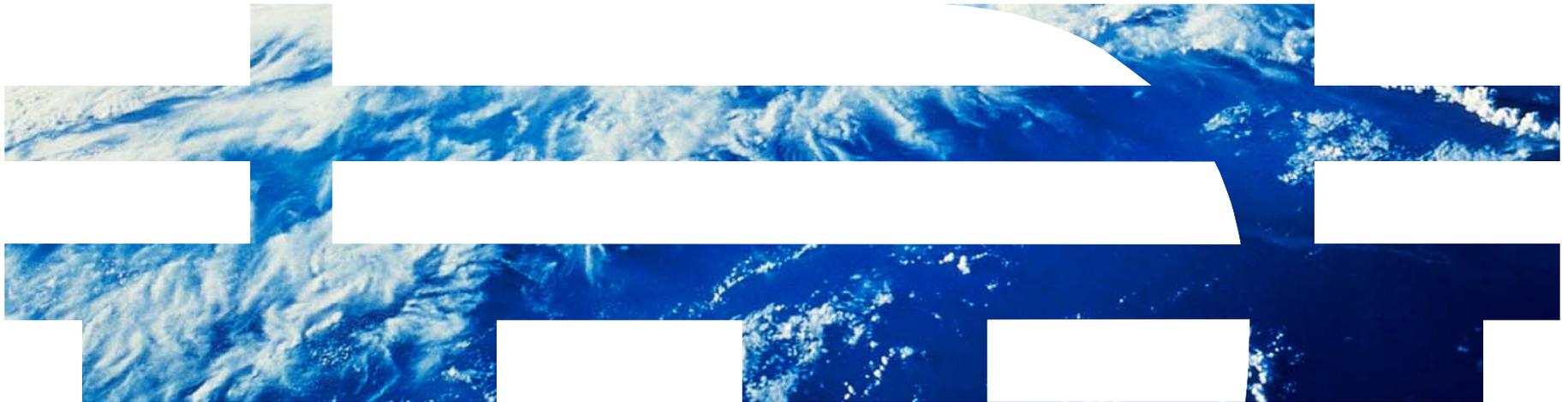
Think of facts as merely assumptions

## **NITRD Cybersecurity R&D Kickoff Event**

---

# **Industry/Academia Panel**

**Dimitrios Pendarakis, Manager, Secure Systems Group  
IBM T.J. Watson Research Center**



## What is Moving Target?

- **Moving Target enables controlled movement across multiple system dimensions to reduce the windows of opportunities for attackers to exploit vulnerabilities in our systems**
  - To an attacker, our systems look externally chaotic, however, they are internally manageable
  - Increase the marginal costs of the attacker (must do new recon for each attack), increase the range of defensive strategies available to the defender, and increase the resiliency and fault tolerance of a target
  - Maneuverability and Diversity: develop and deploy diverse and mutating systems
- **Examples Include**
  - Dynamic Networking, Just-in-time Compiling, Instruction Set Randomization
  - Non-persistent virtual machines
    - “Every time the enemy takes a hill, the hill goes away”
- **Objective: attacks only work once, if at all**

## State of the Art – Sample Moving Target Games

- **Data Chunking and Decentralization**
- **Moving target servers & decoys**
- **Dynamic code & instruction set randomization**
- **Robust Cryptographic Authentication - Moving Target Credentials**
- **Moving target networks**
- **Smart Motion Adaptation/Management**
  
- **In part excerpted from co-chairs' and participants' report from the National Cyber Leap Year Summit, August 17-19, 2009, Arlington, VA**
- **Co-chairs**
  - **Professor Anup K. Ghosh**, Chief Scientist & Research Professor, Center for Secure Information Systems, George Mason University
  - **Mr. Ivan Krstić**, Core OS Security Samurai, Apple
  - **Dr. Dimitrios Pendarakis**, Research Staff Member & Manager, Secure Systems Group, IBM T.J. Watson Research Center
  - **Professor William H. Sanders**, Donald Biggar Willett Professor of Engineering, Director Coordinated Science Laboratory and Information Trust Institute, University of Illinois
- **Reports**
  - [http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews\\_docs/National\\_Cyber\\_Leap\\_Year\\_Summit\\_2009\\_Co-Chairs\\_Report.pdf](http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Co-Chairs_Report.pdf)
  - [http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews\\_docs/National\\_Cyber\\_Leap\\_Year\\_Summit\\_2009\\_Participants\\_Ideas\\_Report.pdf](http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Participants_Ideas_Report.pdf)

## Moving Target Data Storage Chunking and Decentralization (Distributed Data Shell Game)

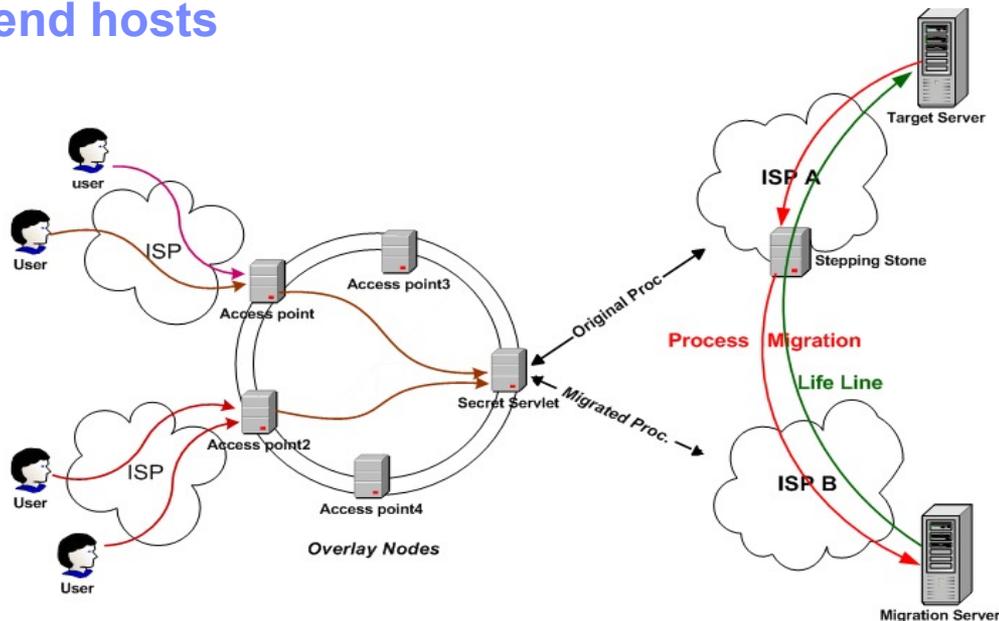
- **Stored files are broken into pieces that are encrypted and redundantly stored across multiple servers**
  - Redundancy is achieved through erasure coding and can be varied to provide desired level of availability guarantees
    - For instance, in a grid of ten storage servers, every file might be stored on five servers, of which any three need to be available to reconstruct the whole file
- **Data spread across a number of (potentially heterogeneous) machines; process coupled with strong encryption**
  - Data storage as a whole is transformed into a moving target
  - An attacker can no longer compromise a single storage server and obtain all the data; needs to compromise multiple servers as well as obtain the encryption keys
  - Example: Tahoe grid file system (<http://allmydata.org/trac/tahoe-lafs>), a cross-platform open-source software solution
- **Next steps: further research into development, experimentation and efficient application of these methods to more complex data organization systems, e.g., relational databases**

## Robust Cryptographic Authentication - Moving Target Credentials

- **Current authentication methods largely employ static credentials – phishing attacks**
  - username/password Web authentication; TLS protects credentials *only while in transit*
- **Develop cryptographic methods for secure authentication without transmitting raw credentials**
  - Explore use of zero-knowledge, password-authenticated mechanisms
  - Example: the Secure Remote Password (SRP) (<http://srp.stanford.edu>) protocol
    - Constructs a special proof that the user knows the password, incorporates random numbers that are different each time and sends that proof to the server
- **Explore widespread deployment of diversity in authentication for both human users, devices and different software components**
  - Diversity in the type of credentials, the time requested, communication channel used
  - Protect against attackers that successfully compromise one component of a system
- **Objective: *transform Web authentication to a moving target* leaving attackers and phishers with useless information**

## Moving Target Networks

- Vary addresses, names, access paths, topologies – both for physical networks & end hosts

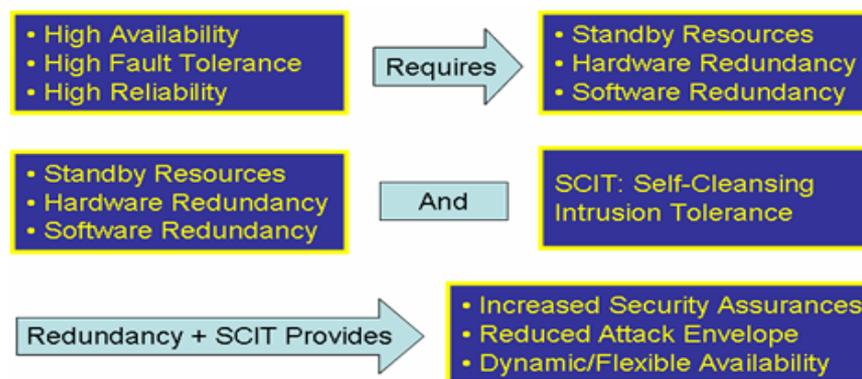


- Example: ***“MOVE: An End-to-End Solution To Network Denial of Service”***, A. Stavrou A. D. Keromytis J. Nieh V. Misra D. Rubenstein, Columbia University, NDSS 2005
  - Use an overlay network, which treats authorized traffic preferentially
  - Lightweight process-migration allows moving services; functionality residing on a part of the system that is subjected to a DoS attack migrates to an unaffected location
  - Legitimate users, who are authenticated before they are allowed to access the service, are routed by the overlay network to the new location

## Moving Target Servers & Decoys

- **Moving Target Servers: create new (or use standby) servers when attacked**

- Example: <http://cs.gmu.edu/~asood/scit/>

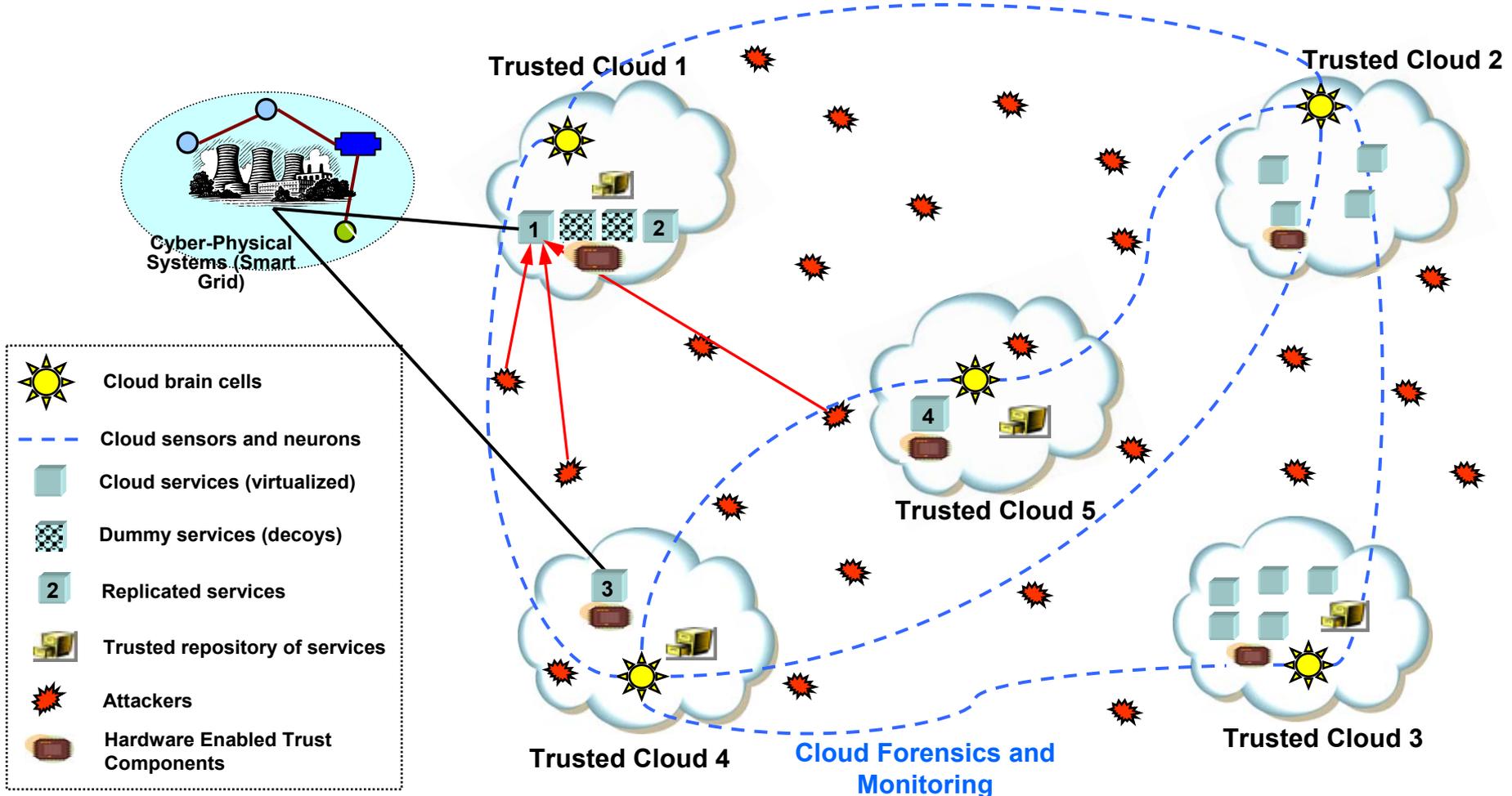


- **Decoys: dynamically deploy a large number of fake, mutating targets that appear to attackers indistinguishable from the real targets**

- Serve as sensors that can detect and analyze new attack activity, pinpoint new vulnerabilities; used in honeypots and honeynets
  - Significantly increase the attacker's work factor; and require new recon for each attack
  - Enablement: virtualization allows fast cloning of VMs; resource optimization reduces cost
  - Cooperating service providers could use a combined “dark IP” space to deploy decoys as a moving target for malware detection and mitigation

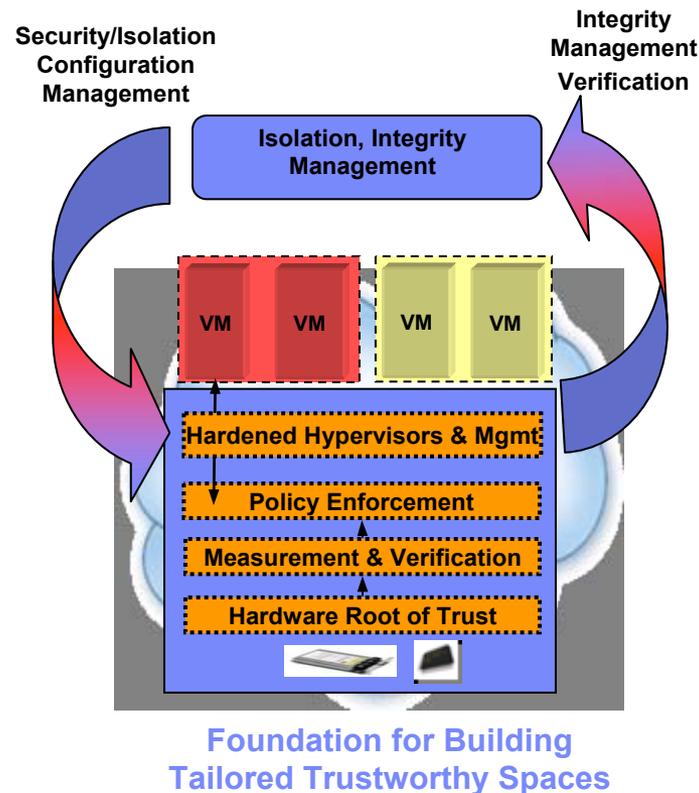
# IBM Research Vision on Moving Target Defense: Hydra

Use of virtualization, cloud computing & stream analytics technologies to construct resilient moving target defense systems



## Hydra Vision: Elements of a Moving Target Defense

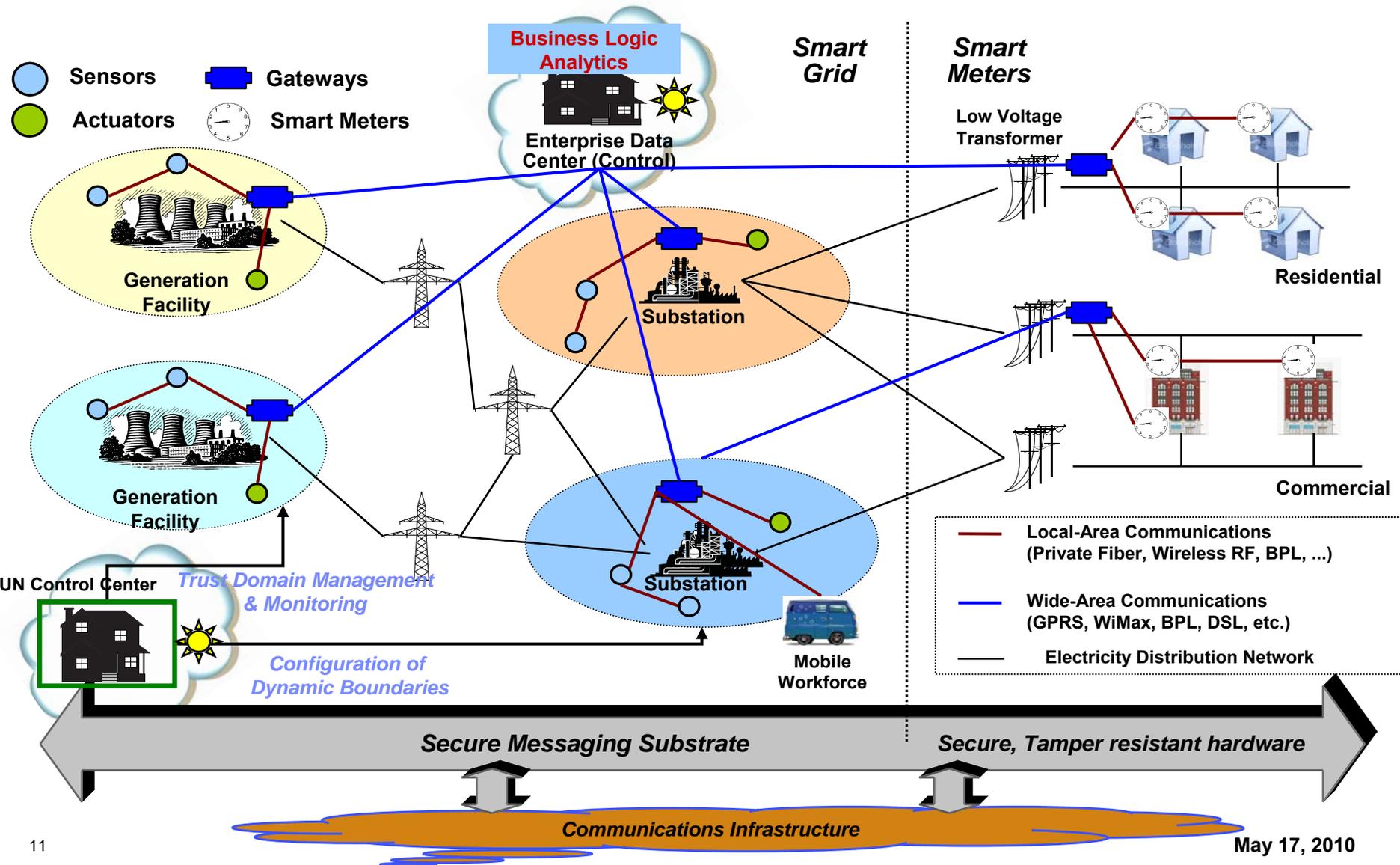
- **Current Status:** Attackers can inflict asymmetric damage by penetrating a small subset of targets; attackers enjoy relative anonymity while targets are typically well identified
- **Objective:** the attacked infrastructure can hide, evade detection and self-replicate (just like Hydra), while continuously performing analysis that pinpoints attackers and closes their window of opportunity by self-modification
- **Hardware enabled trust components** provide high integrity, tamper resistance
  - **Services and data distributed** over one or more trusted clouds, in conjunction with information dispersal, physically diverse and reconfigurable communication channels
  - **Secure virtualization:** strong isolation between different VMs and ability to verify integrity of the software stack
    - Leveraging hardware trust components
  - In response to suspected/detected attacks, **target services replicated** in multiple physical servers, some as “decoys”



## Hydra: Elements of a Moving Target Defense (cont.)

- **Large, decentralized clouds** (private/hybrid) provide a flexible pool of virtualized resources that can be replicated and migrated dynamically, creating diverse and mutating systems
  - These capabilities can be harnessed to obfuscate the identity of targets and quickly identify and respond to attackers
- **Real-time high-volume stream analytics** – enable a set of cloud “brain cells”
  - Operate in a decentralized cooperative manner, processing massive amounts of data, to detect attackers and their behavior patterns
  - Cooperation between multiple cells and clouds to perform localization of attackers
- **Micro-virtualization**: new virtualization technologies with reduced overhead appropriate for cyber-physical systems
  - Loosen binding between physical location and computing services

# Challenge: Building Tailored Trustworthy Spaces and Moving Target Defense Strategies in CyberPhysical Systems



## Research Challenges

- **Performance & Scalability:** deployment limited to small testbeds currently?
- **Power efficiency:** impact of replication, decoys, etc.
- **Provable security properties** vs heuristics
- **Measures of improvement:** risk reward ratio?
- **New analytics:** low false positives and false negatives

## Creating a Sustainable Process: Research, Policy & Commercial Deployment Considerations

- **Mechanisms to support a sustainable process to drive the envisioned game changing technologies**
  - Introspection: what technologies haven't worked so far and why?
  - **Overcoming inertia** caused by widespread deployment of legacy technologies
  - Anchor development and experimentation on **realistic settings and data**
  - Establish **metrics to track progress** towards successful development and adoption
  - Strong **partnerships** between government, industry and academia
- **What role should USG have in creating a sustainable process which could initiate and guide R&D**
  - Cybersecurity National Initiative to promote deployment of game changing technologies
  - Adopt an **urgent, but long-term view**; while essential, short term fixes insufficient
  - Promote and reward sound, consistent security engineering practices
    - Explore application of Cyber Economic Incentives to promote, verify and differentiate strong security implementations
  - Foster **partnerships of government, industry and academia** to facilitate coordinated research, development and adoption of game-changing solutions

## Acknowledgements

- Cybersecurity R&D Kickoff Event organizers, USG
- Input from government representatives, organizers
  - Pat Muoio, Martin Ross, Tomas Vagoun, ...
- NCLY Summit Co-chairs & Participants
- JR Rao, Reiner Sailer (IBM)
- Many others who have contributed to various discussions on these topics

# *Cybereconomics*

---

**Stefan Savage**



**UCSD CSE**  
Computer Science and Engineering

# *Security is a social science*

---

- There is a technical component, no doubt, but...
- Fundamental non-technical components drive real life outcomes
  - Behavior
  - Motivations
  - Relationships
  - Incentives
  - Perception
  - Value
- You have to model *these things* to model security impact

# *Two sides of cybereconomics*

---



## **Defender**

Cost centers

Return on Investment

Incentives



## **Adversary**

Profit centers

Return on Investment

Disincentives

# *Economics of defense*



- Outcomes depend on three things
  - ◆ User behavior
  - ◆ Attacker behavior
  - ◆ Defender behavior
- Things about outcomes we **don't** know, but **could** know
  - ◆ How much does it matter if you have good “Internet hygiene”?
  - ◆ How much does it matter if you patch your systems?
  - ◆ What kinds of users/systems attract the most attacks?
  - ◆ How much does it matter if you run AV and for what?
  - ◆ How much does it matter if you do quick incident response?
  - ◆ What's the best way to stop phishing: mail filters, browser blacklists or takedowns?
- **Evidence-based security**

# Offence via economics



- Adversaries increasingly have a complex value chain
  - ◆ E.g. spam-based advertising: hosting, registrar, payment processing, affiliate program, malware author, botnet operator, compromised hosts, proxy network, etc...
  - ◆ We largely ignore it today
- To build the most efficient defenses, we need to understand the attacker's cost structure and value
- To maximize impact to adversary, need to target the most valuable part of their value chain

# Example: CAPTCHAs

---

- Current **retail** cost to solve 1,000 CAPTCHAs?



- Wholesale cost can be half that...

# Example: compromised hosts

---

- Current **retail** cost to get 1,000 compromised hosts?



- For Asia... western hosts up around \$100/1000

- Договорится по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!
- Мы отслеживаем уникальность инсталлов и их чистоту перед продажей.

## УСЛОВИЯ

- Мы работаем строго по предоплате. Допускается частичная оплата постоянным клиентам на большие объемы.
- Мы не несем ответственности за то что у вас по каким-то причинам отсутствуют загрузки. Если вы не видите инсталлов с первых минут мы можем приостановить отгрузку до выяснения обстоятельств.

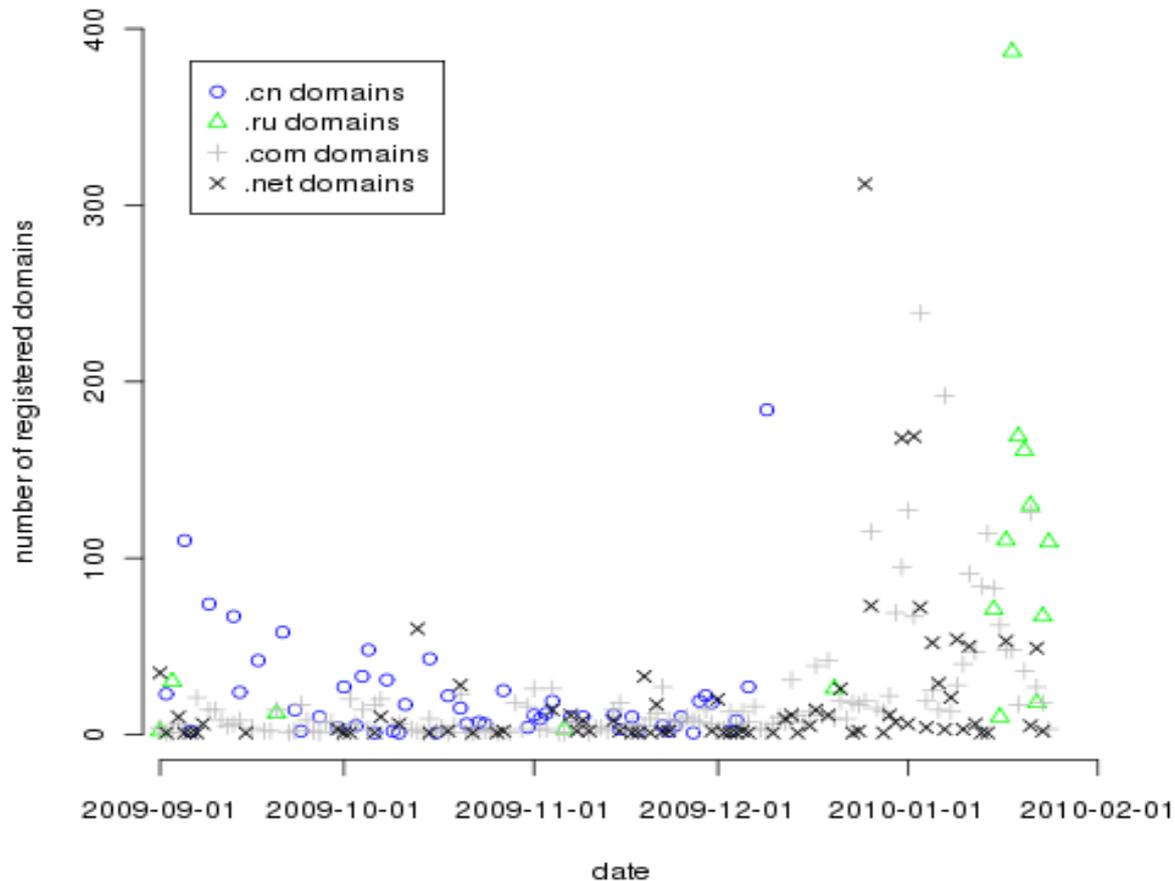
## ТАРИФЫ

GB (Англия)	150\$
DE (Германия)	150\$
USA (США)	130\$
IT (Италия)	120\$
Микс (US, CA, AU, GB)	100\$
CA (Канада)	100\$
Микс (Европа)	40\$
Азия	10\$

Все цены указаны за 1000 уникальных загрузок

# Example: domain names

- Cost depends... and it matters (e.g., for spam)



# *A research agenda going forward*

---

- Users and defenders
  - ◆ Experimentally determine which technology, processes, behaviors, etc are producing which outcomes
  - ◆ Explore how to incentivizes the best of these
- Attackers
  - ◆ Measure or infer value chain, business relationships, cost basis of today's adversaries (and technology to support such measurement)
  - ◆ Determine set of “weakest links” (most valuable, least adaptable, etc) that can be most cheaply targeted

# Lewis Shepherd

Microsoft Institute for Advanced Technology in Governments

## Where's the Manhattan Project in cybersecurity research?

# A Washington Meme

bing "manhattan project for cybersecurity"

ALL RESULTS

Results are included for [manhattan project for cyber security](#). Show just the results for "manhattan project for cybersecurity".

RELATED SEARCHES

- Manhattan Project Atomic Bomb
- Manhattan Project Tennessee
- Manhattan Project Scientists
- Manhattan Project Creation
- Philadelphia Experiment
- Foolhardy Goddess
- Jornada Del Muerto
- Manhattan Project
- The Manhattan Project Movie

SEARCH HISTORY

"manhattan project for..."

ALL RESULTS 1-27 of 27 results · [Advanced](#)

[Homeland Security Today - preparedness and s Chertoff ...](#)  
Homeland Security news original articles videos on terrorism, er public health preparedness, border security, Department of Hon intelligence ...  
[hstoday.us/content/view/2824/149](#) · [Cached page](#)

[Homeland Security Today - preparedness and s Chertoff ...](#)  
Homeland Security news original articles videos on terrorism, er public health preparedness, border security, Department of Hon intelligence ...  
[www.hstoday.us/content/view/2824/243](#) · [Cached page](#)

[RSA: Chertoff Likens U.S. Cyber Security To 'M](#)  
The Homeland Security secretary calls for beefing up the cyber agencies and making sure all of them can respond to threats arc  
[www.informationweek.com/news/security/government/showArtic](#)

Google

Everything

More

All results

- Wonder wheel
- Timeline

More search tools

cyber security needs its own manhattan project Search

About 9,420 results (0.26 seconds)

[Advanced search](#)

[Homeland Security secretary proposes 'Manhattan Project' | News ...](#)

Apr 8, 2008 ... Homeland Security Secretary Michael Chertoff says Silicon Valley should send ... that the country **needs** a "Manhattan Project" for network security, ... national **cybersecurity** initiative...almost like a **Manhattan Project**. ... computer security is to unask your **own** question because **it's** so clueless. ...  
[news.cnet.com/8301-10784\\_3-9914391-7.html](#) - [Cached](#) - [Similar](#)

[cybersecurity posts - Politics and Law - CNET News](#)

Despite that funding, a government review of its **cybersecurity** efforts last year ... **cybersecurity** defenses, but said the Appropriations Committee **needs** to provide ... can't solve **cybersecurity** problems on **its own**, Schmidt said his agenda is to .... a "dashboard" pilot **project**, measurements of hiring effectiveness, ...

[news.cnet.com/the-iconoclast/?keyword=cybersecurity](#) - [Cached](#) - [Similar](#)

[Show more results from news.cnet.com](#)

[What's Up with the Secret Cybersecurity Plans, Senators Ask DHS ...](#)

May 2, 2008 ... The government's new **cyber-security** "Manhattan Project" is so ... the Air Force is hyping **its own** efforts at cyber defense and offense. ....  
Posted by: New Obama cyber czar must balance security/economic **needs** - Telecom

# Hallmarks of the Original

- **Project Secrecy**
- **Handpicked participants**
- **No collaboration with outside groups**
- **One single goal (with end-result for use against one of two known opponents)**
- **Essentially unlimited government funds**

# Better Approach for Cybersecurity

- **Manhattan-Project-scale collaborative research**
- **Open sharing of research goals, project designs, results**
- **Viral spread of research work**

# Better Approach for Cybersecurity

Research Questions within the 3 Themes are all excellent candidates for viralness and collaboration

- **Tailored Trustworthy Spaces**
- **Moving Target**
- **Cyber Economic Incentives**

# Examples of corporate commitment to collaboration

- Deep community engagement MSR and Trustworthy Computing researchers
- Salutory but not lone example: **Yi-Min Wang**, Director of the MSR Internet Services Research Center (ISRC), and IEEE 2010 Fellow for contributions to Dependable Computing and Web Security
- Microsoft **BlueHat Security Forums** – no longer just internal, no longer Redmond only.
  - Attendees span local and regional business and industry, government, academia, CERTs and security researcher communities
  - March 2010 – BlueHat Forum in Brazil (100 attendees with us here today from across Latin America)
- Increased volume of publishing, e.g. papers this week
- Aligned with open-skies approach on SDL, vulnerabilities/patches

# Government/Academia/Industry

- **The Manhattan Project for cybersecurity already exists**
- **Government's role in funding and guiding research is appropriate and welcome**



# Changing the Game: Defining, Preserving, Enhancing Trust

May 19 2010  
Claire Vishik



# How Can We Change the Rules of the Game?

## Look at the big picture

- Not islands of new technologies
- Not only well studied and popular areas of research

## Look beyond the emergence of new ideas

- To their adoption and deployment

## Look at complex, composite problems

- Introducing broadly applicable technology approaches

## Look beyond technology

- Business models, economic incentives, users' attitudes, participation, and awareness, availability of infrastructure

Security environment makes it increasingly difficult to address threats based on improvements to existing approaches

## **WHY ACTION IS NECESSARY**



# Complex Attacks, Organized Attackers

## New threats from:

- Social networking
- Web mash-ups
- Drive-by downloads
- Mobile devices
- Hardware and firmware attacks
- Virtualization attacks
- Even power management tools

**Tools to perform security attacks are readily available and increasingly more efficient**  
The tools are increasingly adapted to the intended environments

## **Cybercrime is Funding Organized Crime**

Cybercrime has been so profitable for organized crime that the mob is using it to fund its other underground exploits. And U.S. law enforcement is reaching around the world to reel it in.<sup>2</sup>

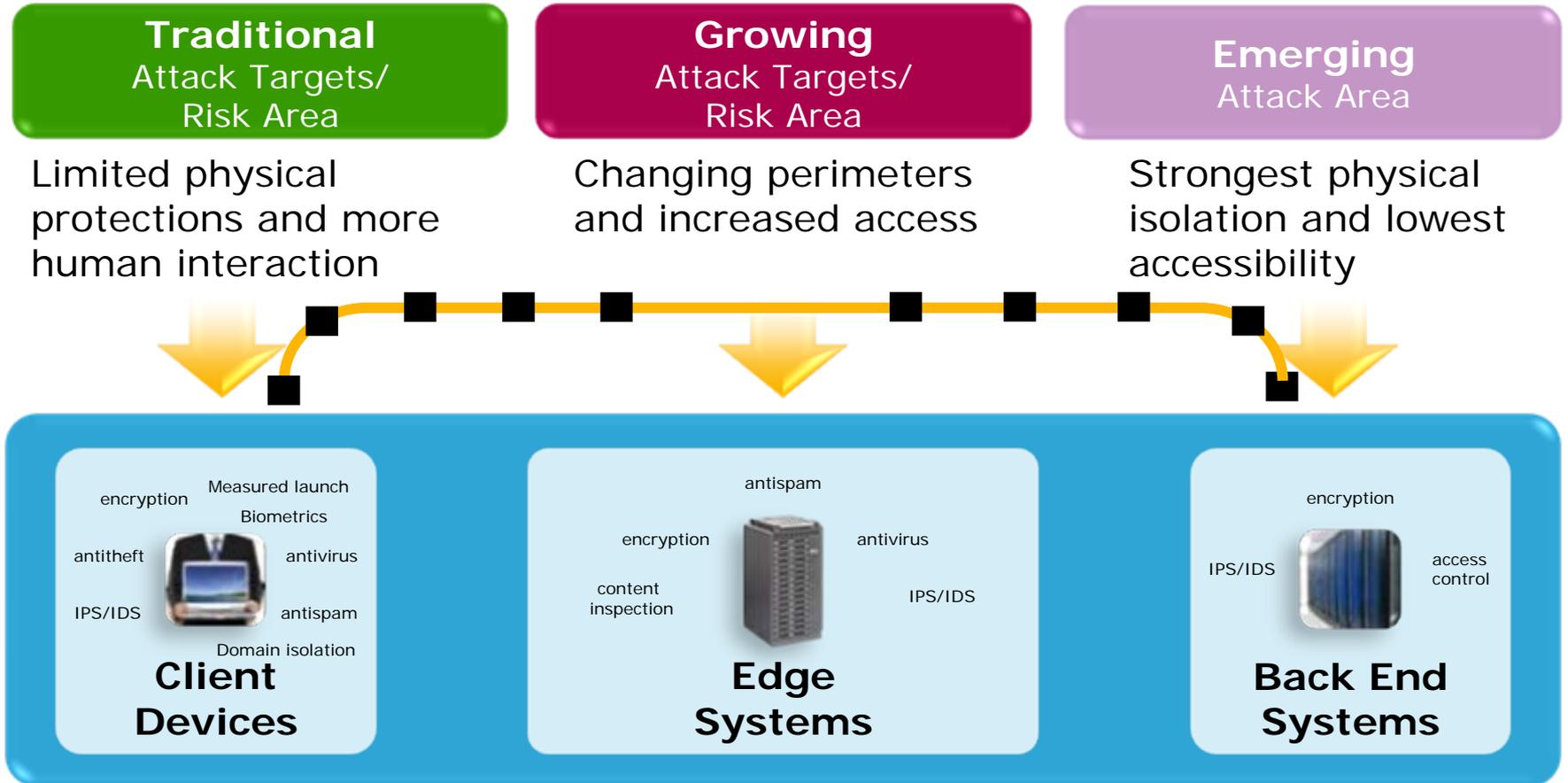
**“We see many signs that criminals are mimicking the practices embraced by successful, legitimate businesses to reap revenue and grow their enterprises.”<sup>3</sup>**

*—Tom Gillis, Vice President and General Manager,  
Cisco Security Products*

**Threats are more sophisticated and professional**



# Security Environment: Layers

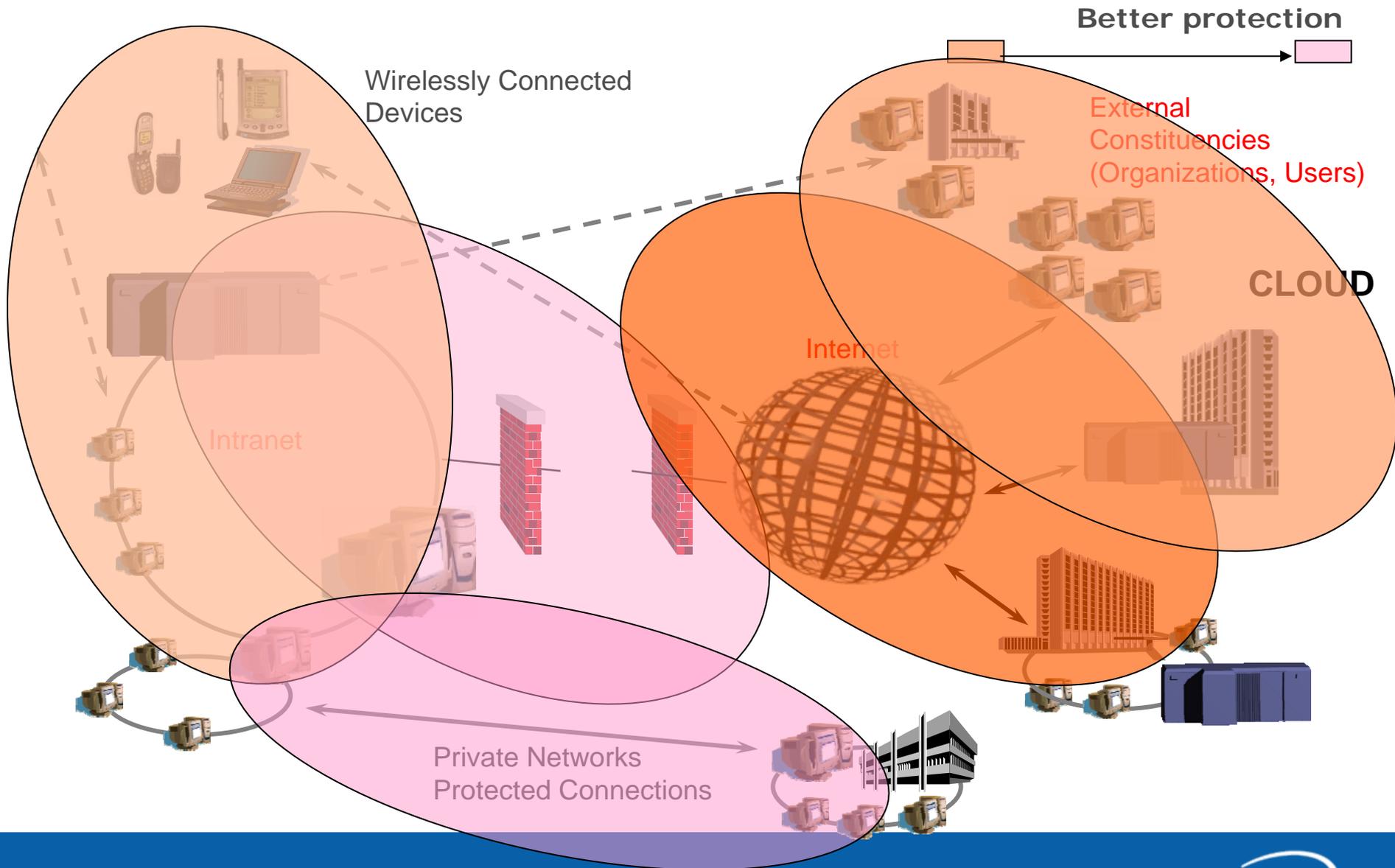


**New security threats accompany the emergence of new technologies; protecting one component is not enough**

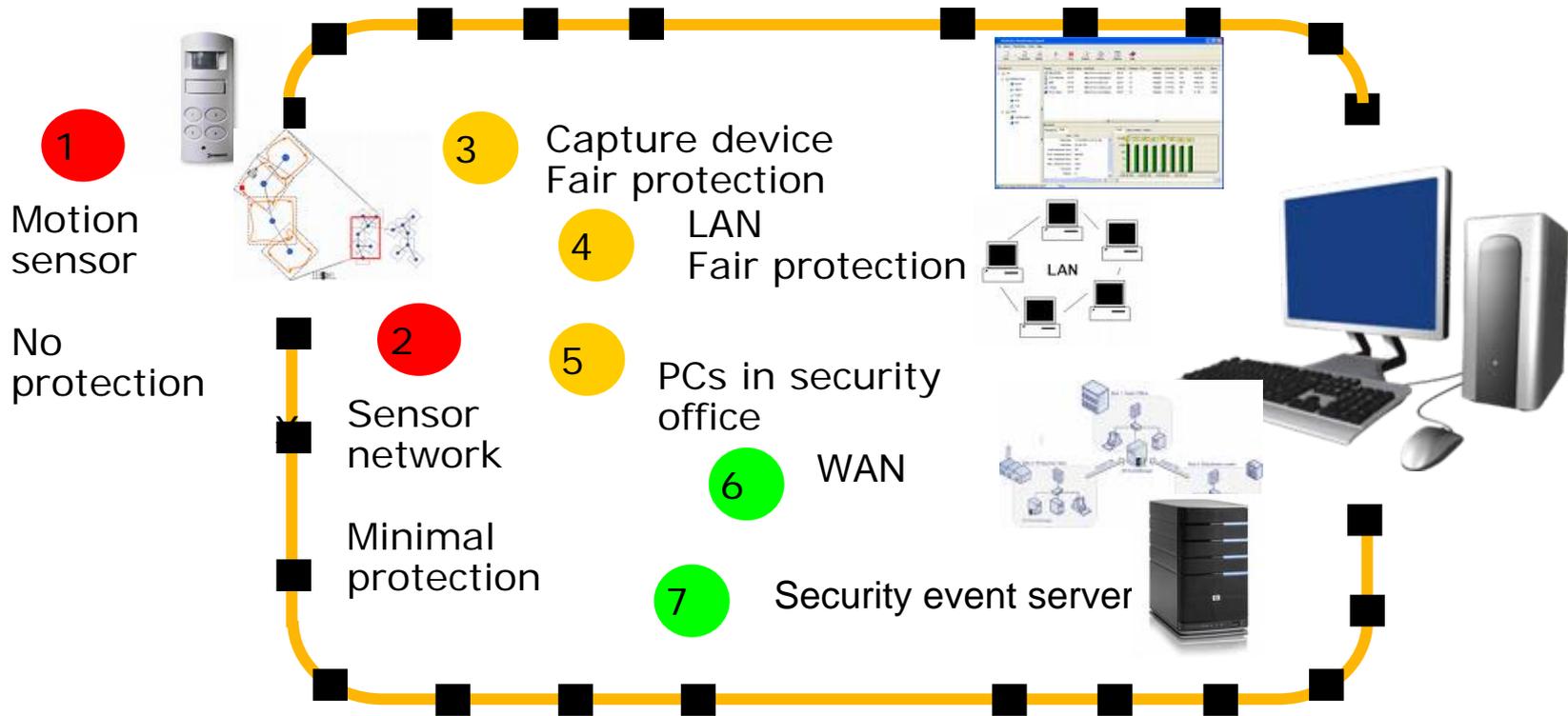
Environments, processes, and business models are very complex and diverse

# WHY CHANGE IS DIFFICULT

# Diverse Ecosystem: All Components Need to Be Considered

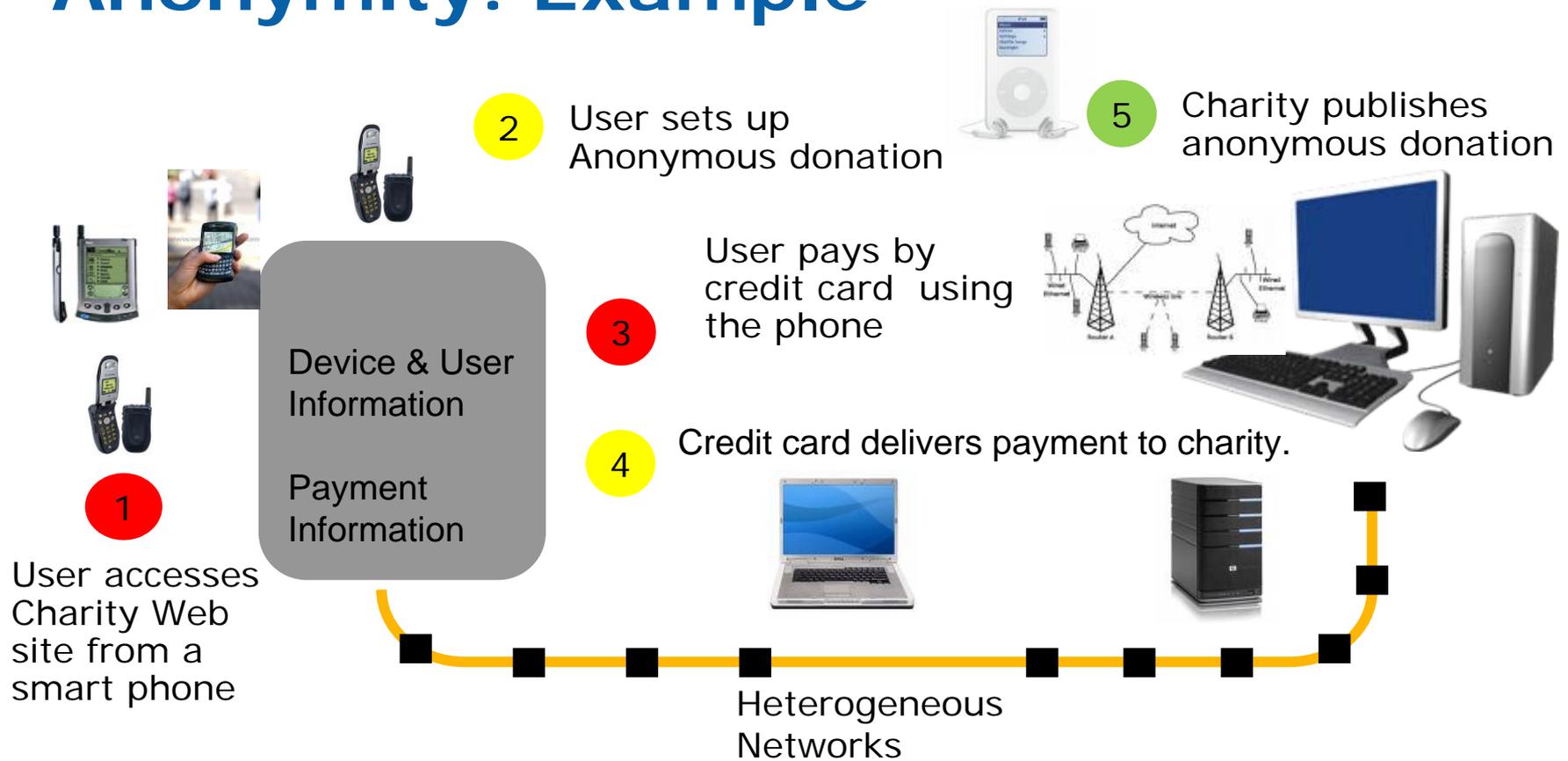


# Varying Levels of Protection in Components of Complex Processes



We need to evaluate the technology space as a whole to change the game

# Varying Levels of Privacy and Anonymity: Example



We need to evaluate many areas beyond technology to design acceptable solutions

# Example Situations Requiring Trust

- 1 Access to mission critical systems
- 2 Social networking
- 3 Online banking and e-commerce
- 4 Using an ATM in a foreign country
- 5 Using medical services and accessing medical records
- 6 Updating/synchronising your devices via your computer
- 7 Accessing premium content in a mobile setting
- 8 Setting up and updating PCs for enterprise employees

# Research Challenges

- 1 The research “subject” is very complex

  - Requires skills and input from diverse groups of stakeholders
  - We don’t have good models to work together in this fashion yet
- 2 We don’t yet know the rules of the game

  - A broader analysis is necessary to consider game change
  - New approaches to analysis are required
- 3 Defining operative trust parameters, trust information, and trust tools, from system and device architecture to behaviors and economic incentives is the type of a scientific problem we need to learn to solve
- 4 Societal and economic components are crucial parts of the “game”

  - We need to learn to study these together with technology
- 5 Significant infrastructure investment is likely to be required

We have greater ability to look at technology spaces in an integrated fashion, growing interest to search for new approaches

## **WHY IT IS POSSIBLE**



# It Is A Good Time to Start Working On Core Issues

- 1 We understand the issues – and what we do not know -- better
- 2 We have a technology foundation, access to growing computing power
- 3 We have a growing experience of collaboration among diverse technology community
- 4 Lessons learned from the earlier generation of trust technologies can improve direction and focus
- 5 We have a better ability to address technology issues in a larger context

# What We Need

- 1 New game changing ideas
- 2 Multidisciplinary innovative approaches
- 3 Early concern about adoption and deployment
- 4 Broadly applicable standards
- 5 Economic incentives and business models to support deployment of new technologies
- 6 Efficient use of diverse expertise of all stakeholders
- 7 Focus on hard problems