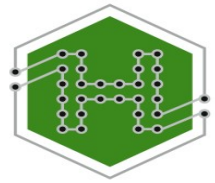
Creating Unreliable Systems

"Attacking the Systems that Attack You"

Sysmin Sys73m47ic & Marklar
From:
The Hacker Pimps





Document Versioning

- For a copy of this presentation visit:
- www.hackerpimps.com/docs.html

Warning!!!

- Some of the techniques discussed in this presentation can be hazardous to your personal freedoms.
  - Mainly the staying out of jail part
- Everything discussed in this presentation is strictly theoretical ;)

Why?

- Why do we want to create unreliable systems? Isn't that the opposite of what we are supposed to do?
- Don't people get paid to make systems reliable?
- Unreliable systems can not be counted on.

Technology Changes Everything

- We do not have new problems, we have new technology.
- We seem to love having our freedoms taken away, just because things are cool or convenient.
- Companies and the Government are finding newer more sneaky ways to get your information.

A Presumptive Right To Privacy?

Why not presume the right/need for privacy?

The number one excuse:

“I've got nothing to hide!”

This is the comfortable position of those who are not marginalized.

Are you:

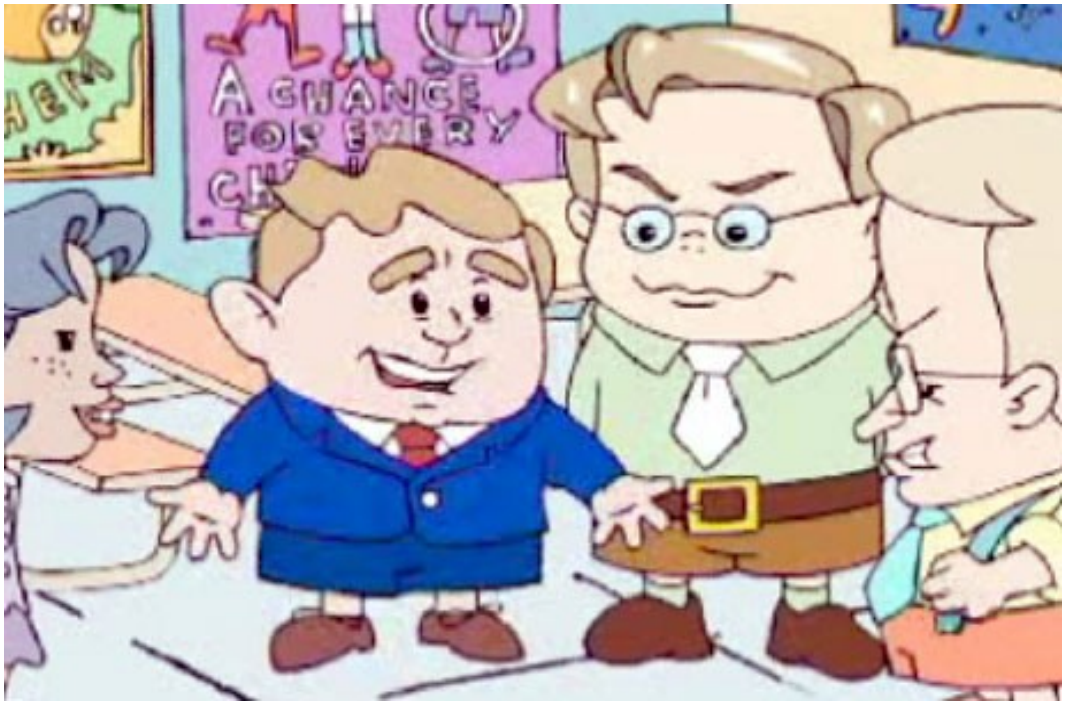
In great pain and unable to legally manage pain?
Gay and in the military?
Needing to express unpopular views that would otherwise risk your safety?
A whistle blower?
A security researcher?

Privacy

“I don't care that X is watching me. I'm not doing anything wrong!”

Who might X be?

The Executive Branch



The Other Executive Branch



double click

AMERICA Online



The Imaginary Judicial Branch



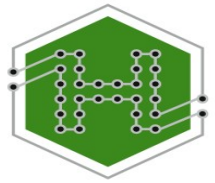
The *Other* Imaginary Judicial Branch



The No Such Branch Branch

The Branch Which Must-Not-Be-Named

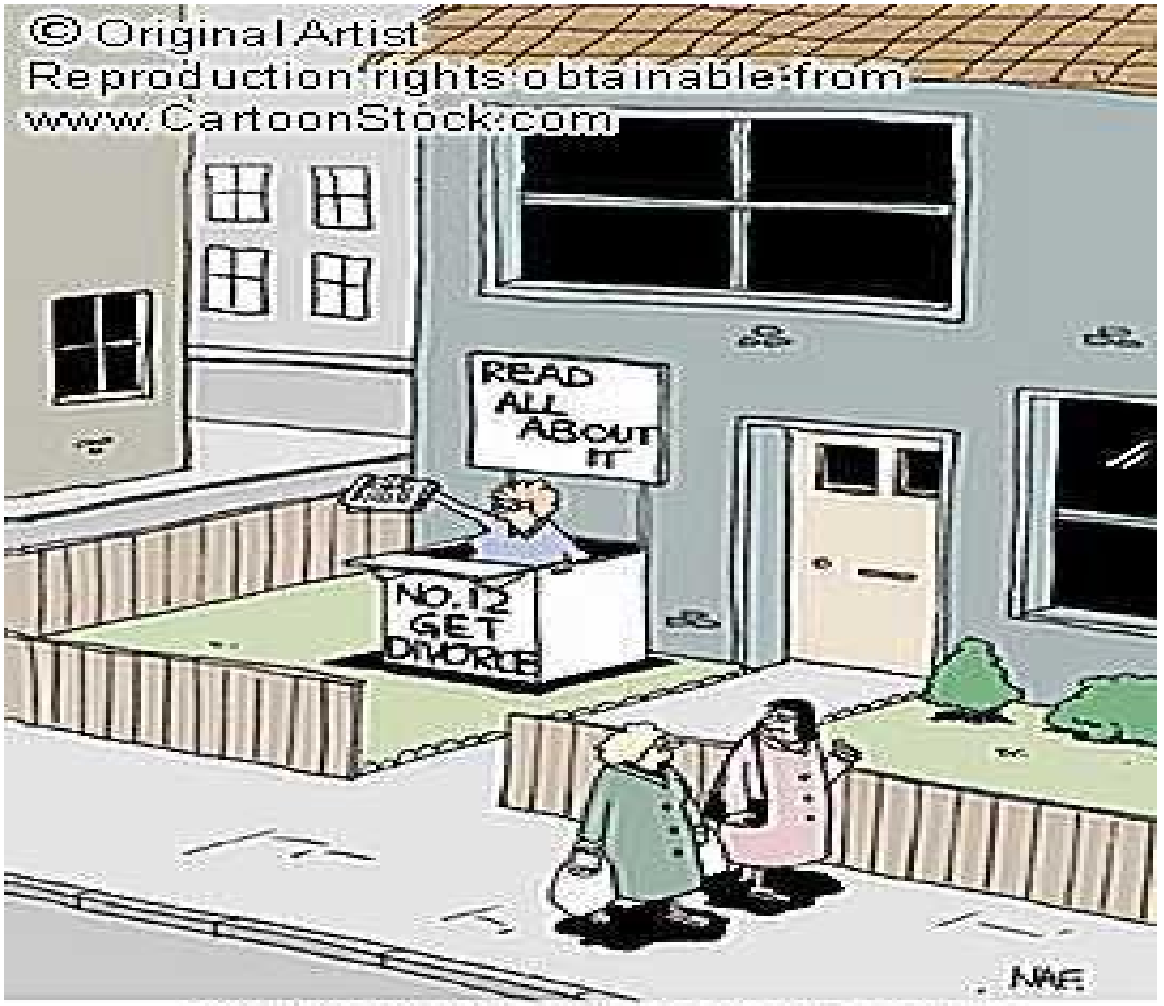




Your Bad Neighbor

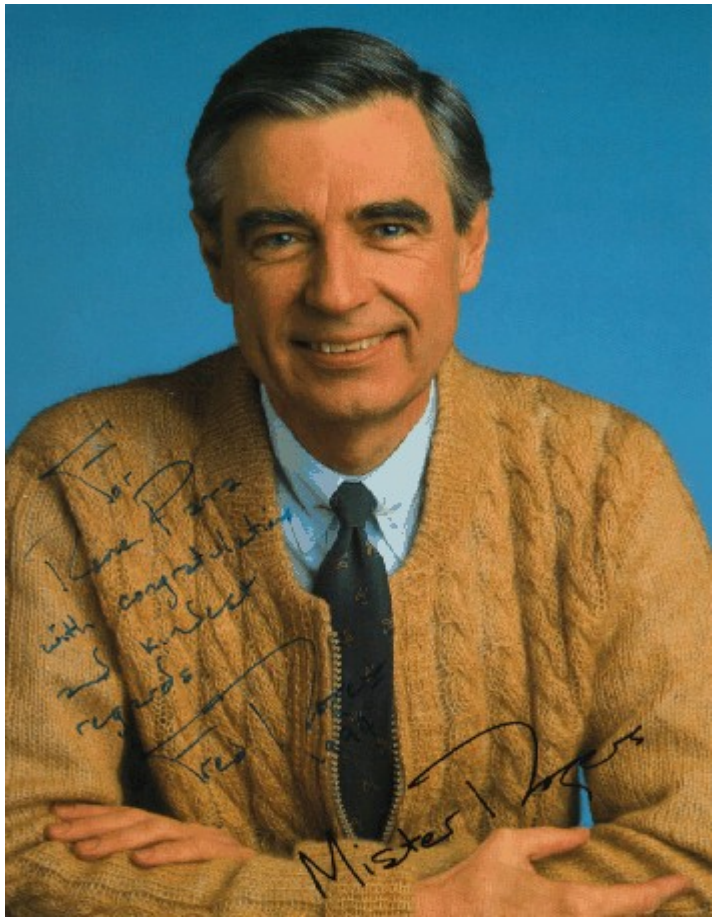


Your Nosy Neighbor



"She's the worst gossip I've ever come across."

Your Good Neighbor



Picking A Target

What Information Gathering System provides the most comprehensive aggregate of what you are thinking about?

Perhaps Web Search?

Target Information Gathering System



Web Search Privacy

Information:
IP Address
Cookies
Sessions
Browser addons / components
Flash/Java/JavaScript, etc:

The Interactive Web!

Dilemma

The things that make the web useful

are often potentially invasive

Proposed Architecture for Web Search Privacy

1. Existing: Tor + TorButton



Summary: Hide your IP Address

Proposed Architecture for Web Search Privacy

2. Proposed “Quiet” button

- Turn off automatic search completion (automatic with Tor)
- Block access to cookies: use/keep cookies, but make them inaccesable on demand.
- Alternatively, the imilly.com google cookie anonymizer (but what about other search engines)

Proposed Architecture for Web Search Privacy

3. Proposed Plugin: P2P Web Search Identity Diffusion

On demand, hide in a crowd

A Nifty, Helpful, Insufficient Idea

P2P Identity Diffusion

When you do a web search,
a. N ?= 30 instances of the query terms are put on P2P
b. the plugin downloads N queries from P2P
c. a and b are executed through Tor, hiding your IP address.
d. The N searches are executed in the background
e. the original search is executed after
(rand() % N)
P2P queries are executed
f. User-Agent is modified to indicate P2P Search

Summary: The origin of an individual query will still diffuse among N browsers

Why Insufficient?

Aggregates and Standing out from the crowd.

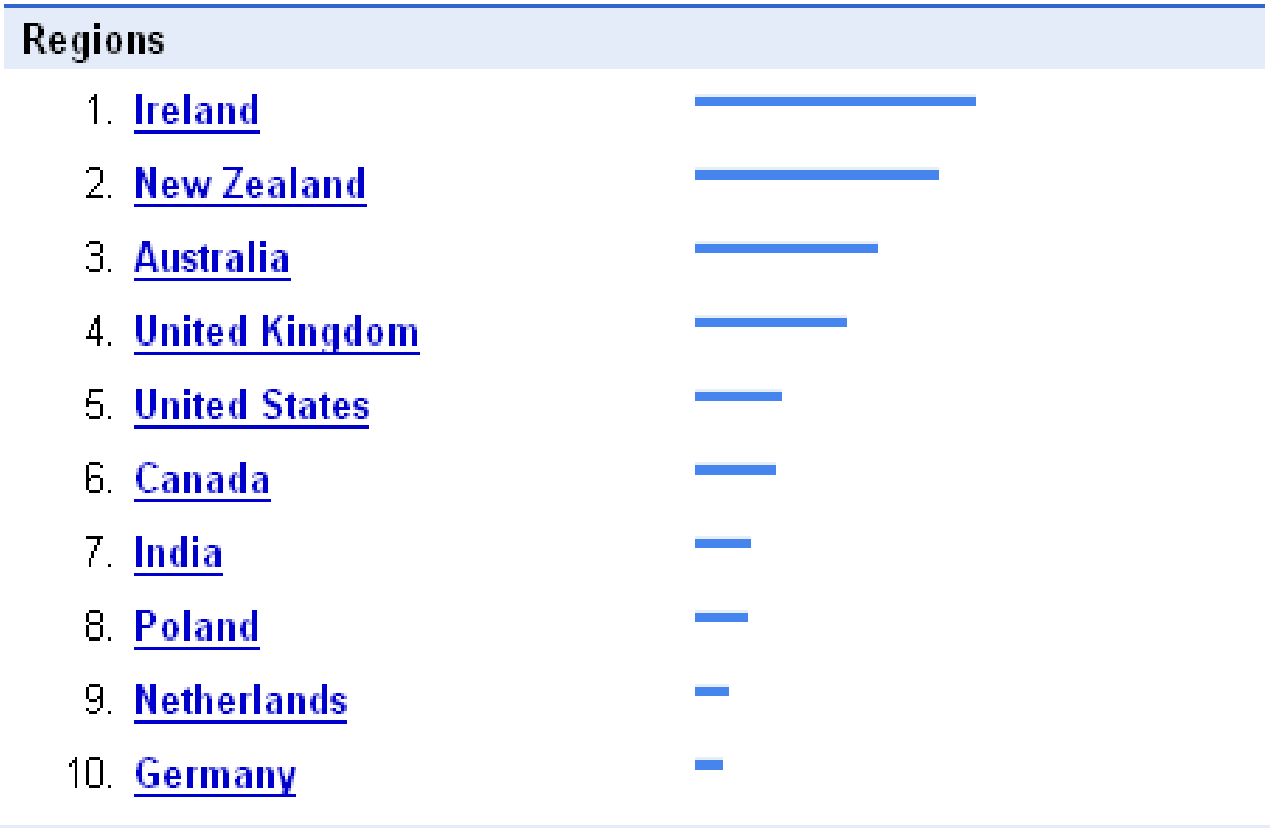
Changing Models

Where do you stand in the aggregate picture?

Google Analytics is interesting

Sometimes it's not what you'd think

Google Analytics: Sheep Sex



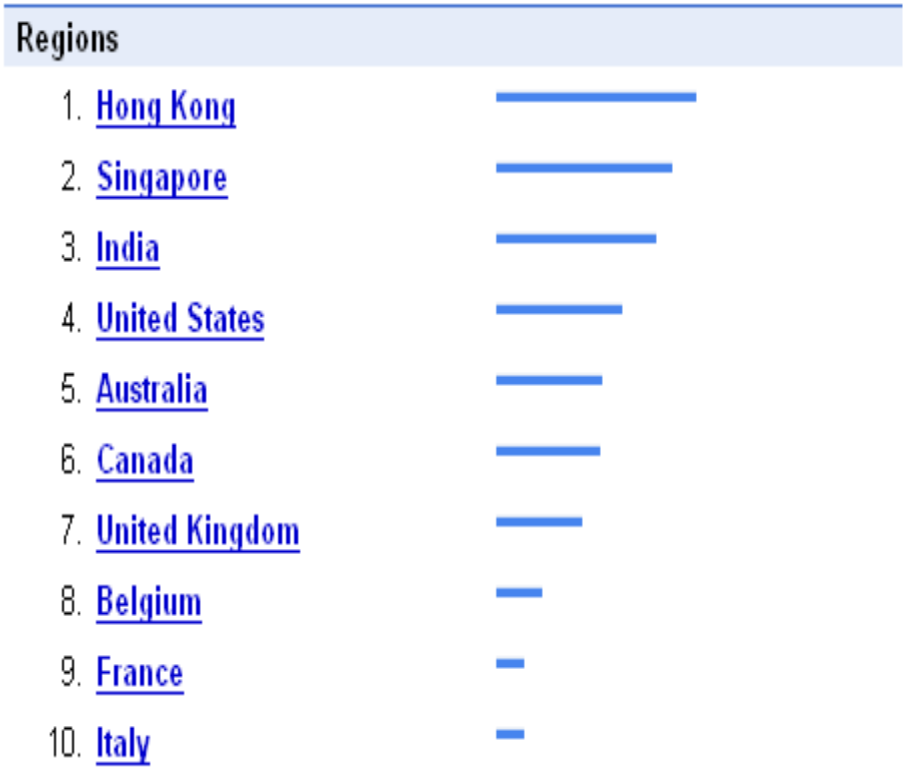
Google Analytics: Goatse

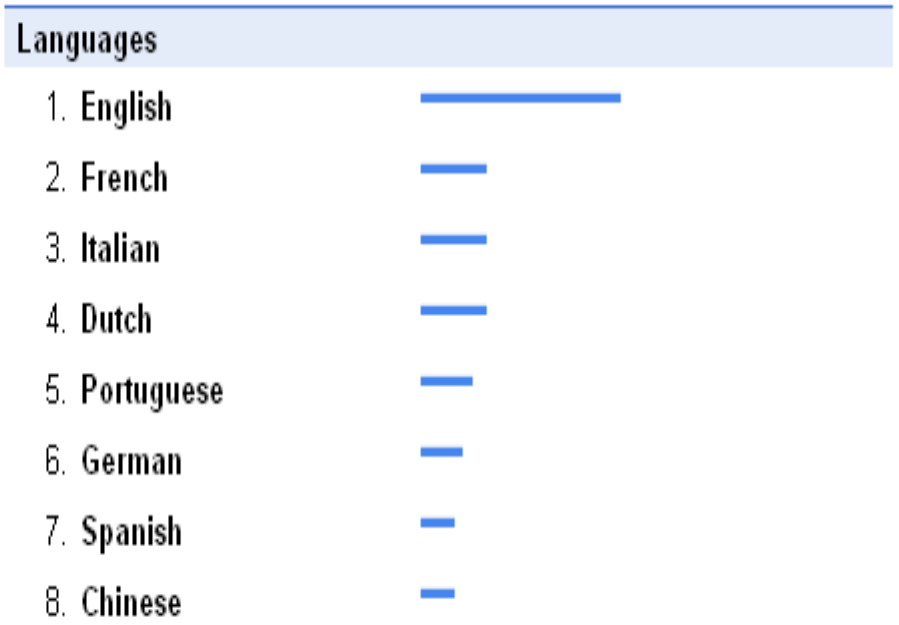


Google Analytics: Stocks

Regions	
1. United States	
2. Canada	
3. India	
4. Australia	
5. United Kingdom	
6. France	
7. Spain	
8. Germany	

Google Analytics: Stock

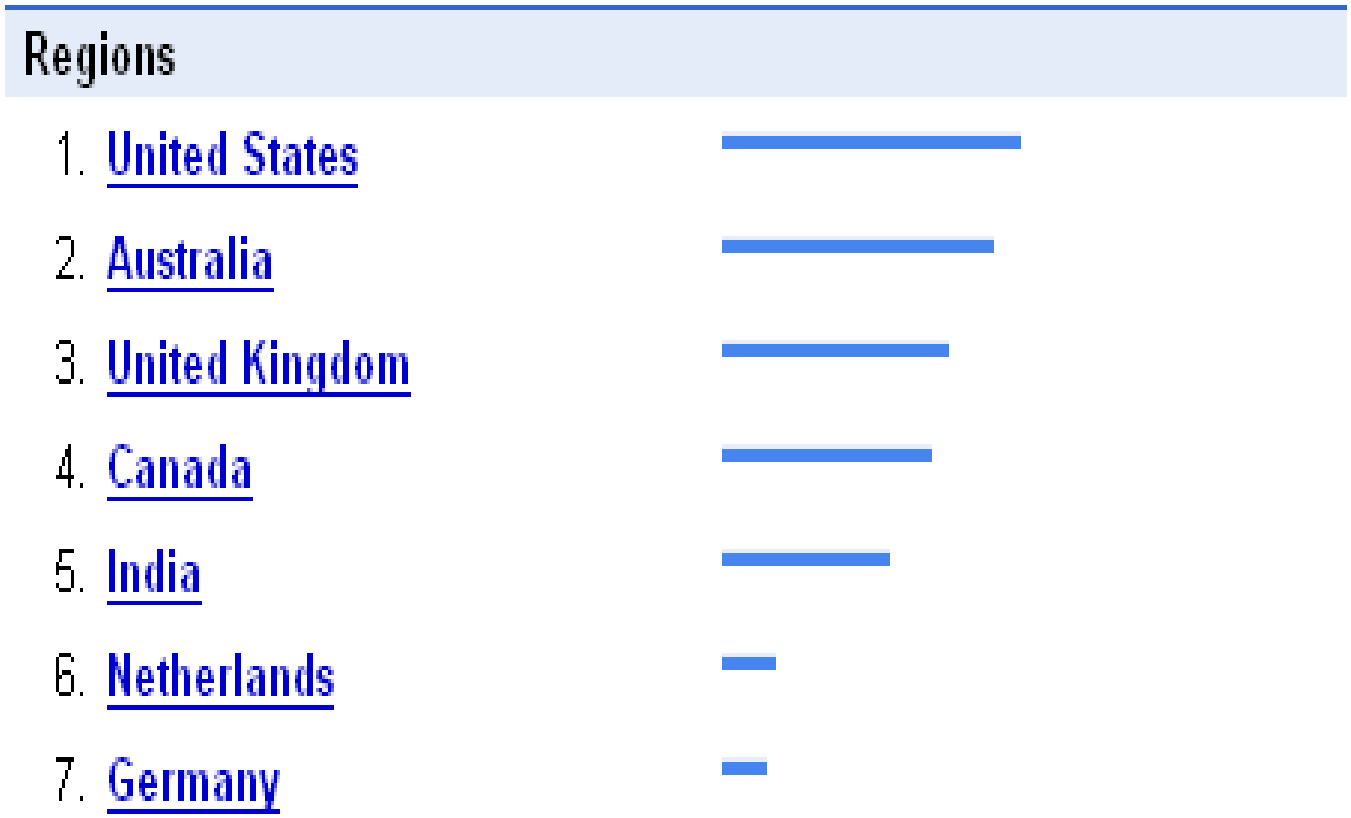




Please Note:

I AM NOT A TERRORIST

Google Analytics: terrorists



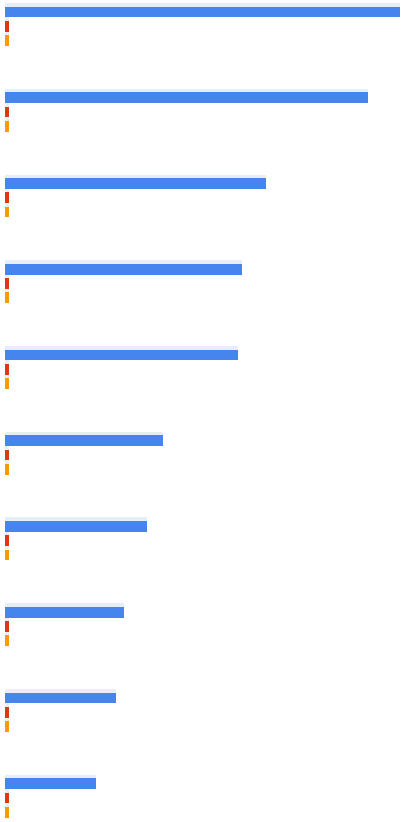
Google Analytics: terrorism

Regions	
1. Pakistan	
2. Morocco	
3. Philippines	
4. Singapore	
5. Australia	
6. India	
7. United States	
8. United Kingdom	
9. Canada	
10. Sweden	

Google Analytics: Terror, Terrorists, and Terrorism

Regions

1. Peru
2. Mexico
3. Chile
4. Colombia
5. Argentina
6. Venezuela
7. Spain
8. Portugal
9. Brazil
10. Hungary



Google Analytics: Terror, Terrorists, and Terrorism

WTF?

The Point

1. Wake Up! It's not like they say on the news

2. (The “real” point): Diffusing a query source is insufficient until N is sufficiently large to smooth your graph down into the aggregate picture

Privacy and Changing models

Keywords:

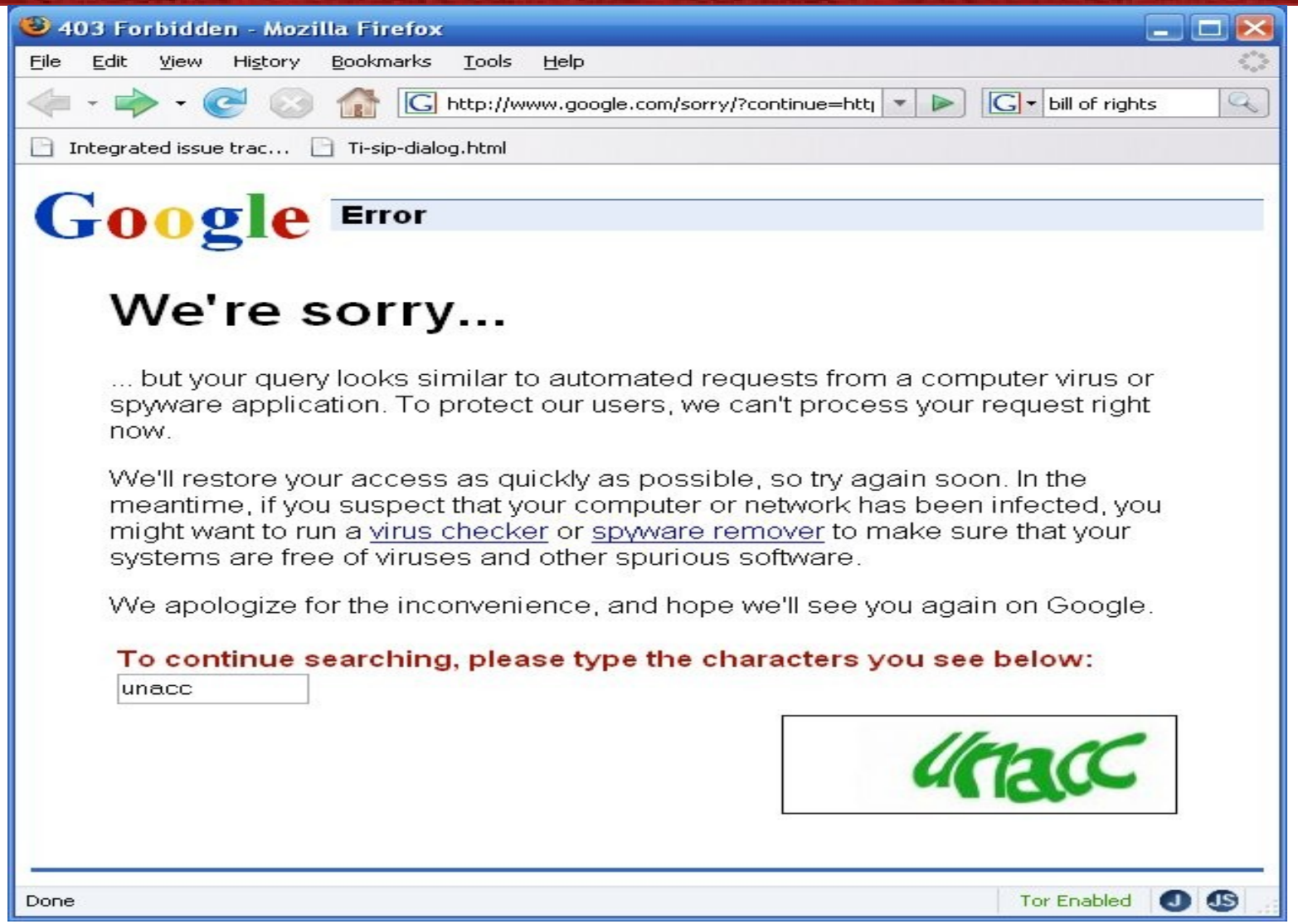
Privacy

Bill of Rights

Strict Constructionists

The Eighth Amendment

Google and Changing Models



A Change of Focus

- We spend a lot of time worrying about people knowing who we are or where we connect from.
- There is a larger problem of people knowing what we are.
  - This is the ultimate goal of collection technologies.

Who You Are

- Who you are is your identity and all of the associated items that identify you:
  - Name
  - Address
  - SSN
  - Phone Number
  - Etc.

What You Are

- Male / Female.
- Race, Non-Religious / Religious, Straight / Gay.
- Diabetic, Asmatic, other medical conditions.
- Mental issues.
- Veteran.
- Porn addict.
- Compulsive masturbator.

Who and What

- Put both the Who and the What together and it starts to get real scary.

Collected Data

- Collected data is dangerous.
  - It can be sold.
  - It can be misused. (Government creating files on all of us).
  - Incorrect assumptions can be made on this collected data.
  - May be impossible to correct inaccuracies.
- Data is collected from:
  - Aggregates
  - Inference

Aggregated Data

- Data collected from multiple sources in order in to obtain a more complete picture.
- Example: Collecting data from multiple sources to get an idea of your shopping habits:
  - Credit Card
  - Grocery Rewards
  - Mailing Lists from Businesses
  - Etc.

Inferred Data

- An inference made from collected data.
- Less accurate than aggregated data.
- Often inferences can be wrong, such as:
  - Example: You buy multiple packs of Sudafed, so you must be cooking Meth.
  - Example: You drive through bad parts of town, so you must be buying drugs.

A Step Further

- What if a profile of you was created from this collected data both aggregated and inferred.
- Think back to the previous slide about “what you are”, a couple theoretical situations:
  - Statistics could show that since you watch certain shows, download porn, and have diabetes that you are 30% more likely to kill someone.
  - 40% more likely to be guilty of domestic violence.
- Do you really want data like this in the hands of people that can't protect it anyway?

Eating Your Own Cake

- You can't freely share information, and expect to keep it private.
  - Social networks, blogs, etc.
  - Public Resumes and CVs.
- Even using an alias can be dangerous.
- Decide what you want people to know about you, and make it public.

So How Does It Work?

Recognition Technologies

- Traditional Biometrics
- Also, linguistics and web habits.
  - MS is working on technology to identify you through your web habits.
- If this technology is widespread it could be next to impossible to correct inaccuracies.

Scary S#!7



Stealthy Iris Scanner in the Works

By Bill Christensen

Technovelgy.com

posted: 06 February 2007
02:05 pm ET

A public iris scanning device has been proposed in a patent from Samoff Labs in New Jersey. The device is able to scan the iris of the eye without the knowledge or consent of the person being scanned. The device uses multiple cameras, and then combines images to create a single scan (see diagram).

Iris recognition is a biometric identification system that requires a high-resolution picture of the irides of the subject's eye. Pattern recognition software is then used to match that picture against future iris scans.

Iris scans are considered highly accurate; current iris recognition algorithms have an incredibly low false match rate. Good quality scans result in a "false match" less than one time per one hundred billion (this system has been used with excellent results in the United Arab Emirates).

The significant advantage of the newly proposed system is that it allows iris scans to be taken without the knowledge or participation of the subject. Read the relevant quote from the patent application:

It's Only Going To Get Worse

- Your information is big business $$$
  - Not just your personal information but psudo-profile information as well.
- Computers need to learn to forget.
  - Viktor Mayer-Schönberger
  - Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing
- Not to mention all of this affects our freedom of speech.

Future Connected Technologies

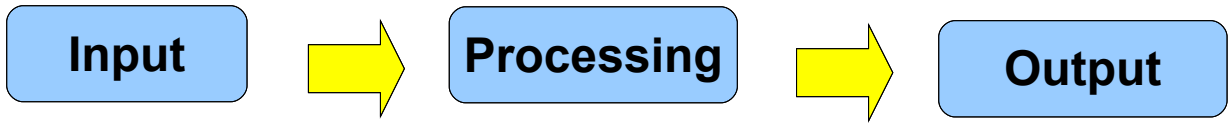
- Just think if your home could talk, all of the things it could say about you. In the future, it will talk and probably not to who you want it to.
- Future connected homes are going to become a hotbed for embedded spyware. It is inevitable.
  - Connected Devices and appliances = Collected Information
- We did an entire presentation on this at Hope Number Six last year.

Future Connected Technologies

- We freely give away our rights when we agree to the user agreement.
- We allow companies to spy on us.
- Unless we refuse to use their items, this trend will not change.
- We need to start looking at new technology as researchers and not as simple users if we care about our information.

System Models

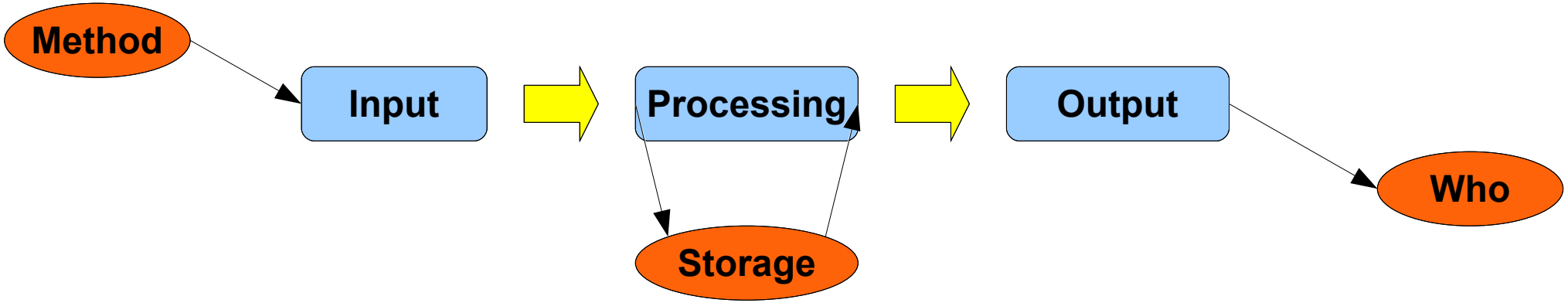
- My Co-workers Philosophy about computers
  - Way too simple, but we can start there anyway
  - The basics of a system
    - Input – Processing – Output



Now lets expand on this a bit

Slightly Expanded Model

- Let's add a couple of components
  - Method
  - Storage
  - Who does the output go to



Analyzing These Systems

- Analysis is the first step to mitigating the effects from these systems.
- Items that will affect your continued efforts will be determined by a couple of factors:
  - Is this installed software?
  - Is this black box technology?
  - System out of your control?

Analyzing These Systems

- It is not necessary to know all the pieces of the puzzle.
- Know your devices and software.
- What do you have to work with?
  - These systems are going to have to have interface with you.
  - It may only take one interface to make an attack surface.

Installed Software

- Read EULA and associated documentation.
- Remember, this is installed on your system.
- What does the software do (its intended purpose)?
  - Inventory these purposes.
  - Now what is it doing on your machine?
    - Compare the purpose with the actions it is taking on your system.

Installed Software

- Concerns
  - What files / parts of the computer is it accessing?
    - Why? Is it a function of that application?
  - Did it scatter pieces of itself all over
  - Is it sending information to a 3rd party?

Installed Software

- Use tools at your disposal to analyze behavior of software. Remember, you have full access to the system.
- Communications
  - If software is spying on you it is going to send the data somewhere.
  - Where is it sending data?
  - What protocol is it using?
  - What is the format of the data?

Installed Software

- File Access
  - What files does the software access?
  - Is it expected to access those files?
- Tools to use
  - Network (Wireshark, TCPdump, etc.)
  - File Access (lsof, filemon, etc.)
- Is the software open source?
  - Look at the code or find someone with an analysis that did.

Installed Software

- Research the web for known issues.
- Keep in mind the installed software most likely has access to all of the information on your computer.

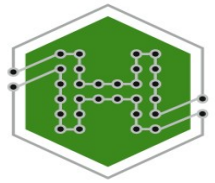
Black Box Analysis

- Read agreements and other documentation.
- Know the device.
  - What is the function of the device?
  - What medium does it use to transfer data?
  - What interfaces does it have?
- What type of information does the black box have access to?
  - Remember it doesn't have to be Credit Card data to be important.

Black Box Analysis

- Is there a way visually or audibly observe behavior?
  - Activity lights, Hard drive activity, etc.
  - Are there times when this activity can be observed being heavier than usual while certain functions are being performed?
- Can you put a device on the medium to listen for communication?
- Does it have other interfaces that can be messed with?





Black Box Example

- A Cable Box with a built in DVR
- Information
  - Has access to television and movie data you watch.
    - Real-time and recorded.
  - Your schedule.
    - Would know when you are home and when you are away.
- Medium to transfer data.
  - Transfers data over coaxial cable.

Black Box Example

- Has multiple interfaces.
  - Infrared.
  - USB
  - Serial
  - Multiple Coax inputs
  - Multiple misc video inputs
- Visual and Audible
  - Hard drive
  - Lights

Systems Out Of Your Control

- Read agreements, documentation, warnings, etc.
- Most likely you are going to have a severely lowered surface to work with.
- Identify Interfaces.
- Identify data the system has access to.

Systems Example

- Surveillance system with /detection
- Information Collected
  - Identification Information
  - Location Information
- Transfer medium
  - Wireless?
  - Ethernet?

Systems Example

- Interfaces
  - Video Camera (Probably the only one you are going to have access to)

Attacking Systems

- What is the goal of attacking these systems?
  - Affect integrity
  - Affect availability
  - Sometimes confidentiality
- Basically making the system's data so it can't be trusted.
- Simply, sometimes systems can be attacked by just not using them.

The Point of This

If a systems data can not be trusted or counted upon, then the system will not be used or rendered ineffective.

Bad data + Bad decisions = Unreliable Systems

If banks had the tendency to loose your money, would you use them?

A New Way To Look Attacks

- A new classification scheme for attacks on information gathering systems and other systems that invade our privacy.
- This classification scheme can be broken down in to three levels.
  - Level 1 Attacks
  - Level 2 Attacks
  - Level 3 Attacks

Level 1

- Level 1 Attack: Affects the ability of the input device to perform its function.
- Examples:
  - Destruction of input device.
  - Disabling of the input device.
  - Cause a malfunction under certain conditions.

Level 2

- Level 2 Attack: Affects the accuracy of the data stored.
- Examples:
  - Injecting bad data.
  - Injecting massive amounts of data.
    - May overflow the capacity of the storage media.
    - Useless data.

Level 3

- Level 3 Attack: Affects processing decisions of the system.
- Examples:
  - Falsely triggering events based on algorithms (False Positives)
  - Bypassing system by not triggering events (False Negatives)

Nice!!!

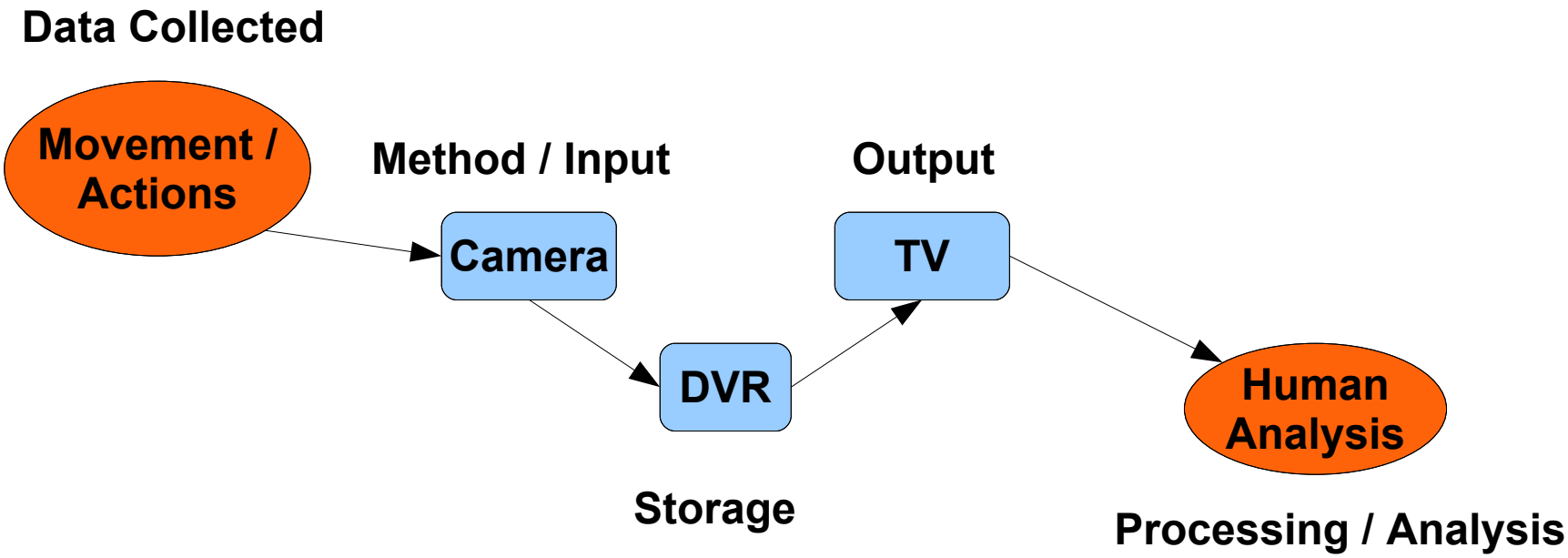
- Cell phone monitoring anyone?
  - “Hey, have you heard that new band assassination plot, they're the bomb.”
- I have a friend who seems to have the uncanny ability to work in words such bomb, nuclear, and assassin in every phone conversation we have.

Examples

The best way to have a look at this is through some examples. These are very simple examples, many of the systems in the wild will be a lot more complex.

Example 1

- Simple Security Camera (without an active watch)

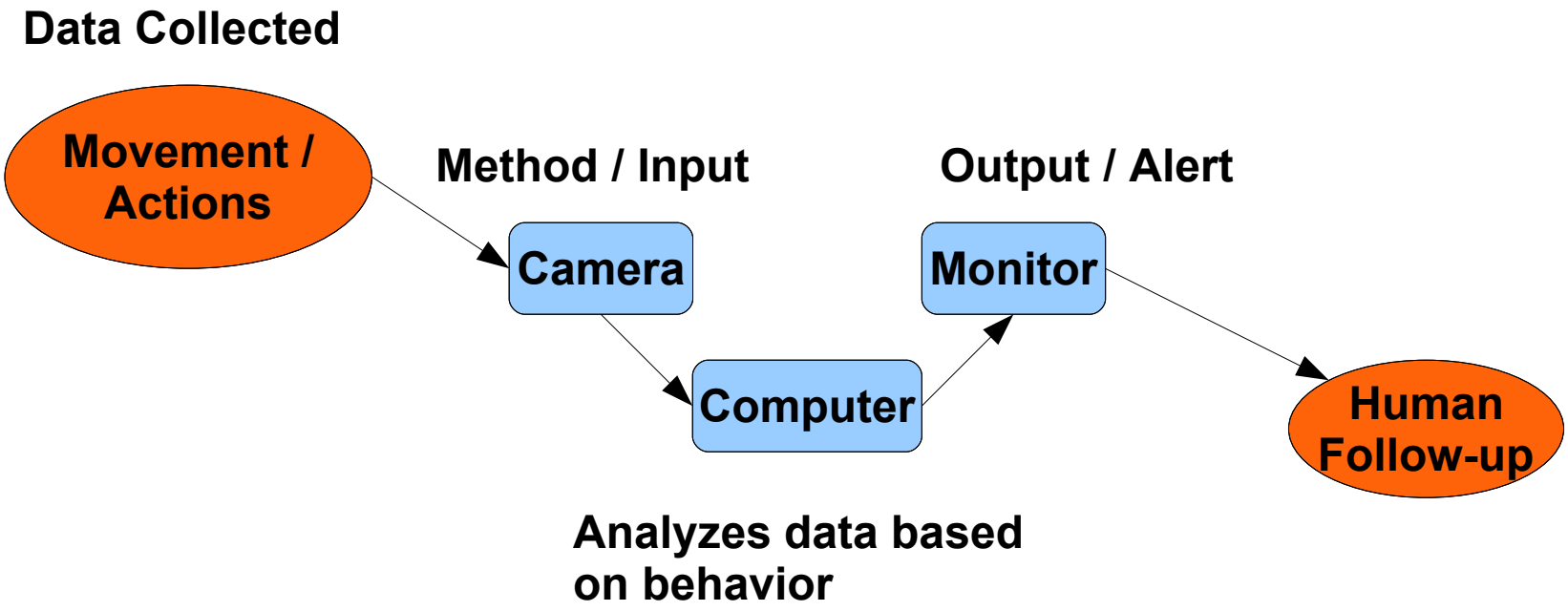


Example 1

- Most likely attack would be on the input device. (Level 1)
- Can the input device be taken out?
  - Destroyed
  - Blinded
- The data stored could also be attacked. (Level 2)
  - Dress up in a suit like a giant banana

Example 2

- Security Camera (with intelligence)

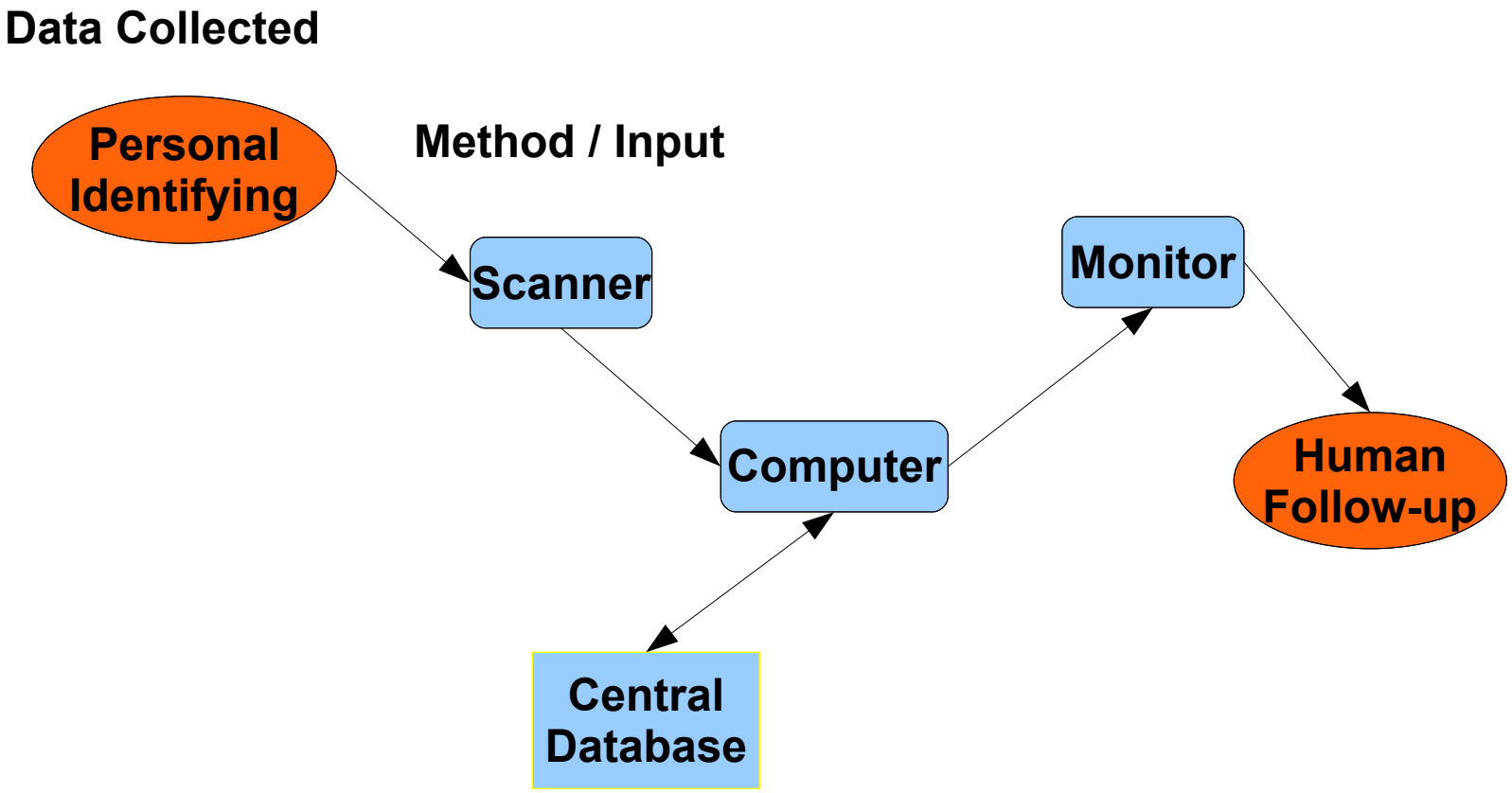


Example 2

- Can the input device be taken out? (Level 1)
  - Destroyed
  - Blinded
- What behavior triggers an event? (Level 3)
  - Falsely trigger events

Example 3

- RFID Passport

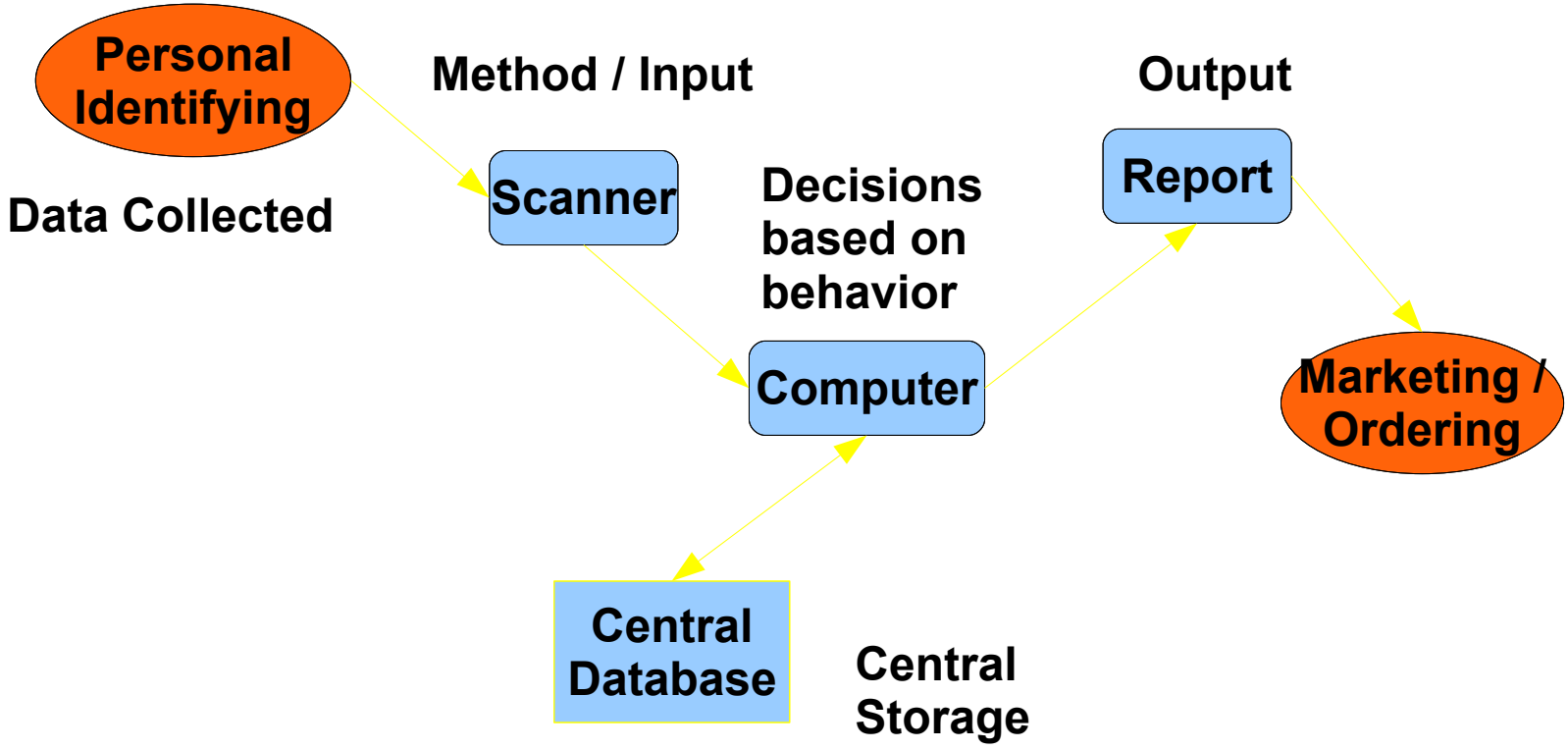


Example 3

- What if 1 out of every 5 passports wouldn't read.
  - Frying the passport (Level 1)
- What if 1 out of every 20 had wrong information.
  - Injecting bad data (Level 2)
- Think about the availability of frequent travelers.
- Think of the impact that would have

Example 4

- Stealth Retina scanning at a department store to identify those pesky customers that pay cash.



Example 4

- Just be cool
  - Wear sunglasses inside the store (Level 1)
  - Don't shop at the fscking store anymore (Level 1)

So What Can You Do?

- Avoid using systems that collect data about you.
- Encrypt communications and ensure you are communicating with who you think you are.
- Analyze systems you have and filter unwanted traffic.
- Contact companies and tell them you refuse to use their services anymore, unless they change.

So What Can You Do?

- Use a new discount card every time.
  - Or only use discount card when it is really funny for tampons and douches
  - Interesting new trend in discount cards
- Minimize use of credit card.
- Leave as little data as possible behind.
- Use encryption when instant messaging.
- Use encryption for Email.

So What Can You Do?

- Analyze new toys for potential issues.
  - Possible backdoor accounts
  - Possible hidden communication
- Beware of any technology that can track you or put you in a given place at a certain time.
- Intrusive stores should be avoided.

So What Can You Do?

- Remember, at first always view the next big thing or the newest gadget as a threat.
  - Move on when you have verified

The False Life Project

- The False Life Project is a project to open lines of communication and discuss defeating behavioral based analysis.
  - People knowing what and who we are.
- Build tools to implement ideas discussed in the project.
- Increase privacy.
- http://falselife.hackerpimps.com

Sysmin Sys73m47ic
sysmin{at}neohaxor{dot}org

Marklar
marklar51{at}gmail{dot}com

The Hacker Pimps
www.hackerpimps.com

The Hexagon Security Group
www.hexsec.com



