

Vulnerabilities in a Connected Future

“Smarthomes, Smartcars, IPv6, and Biometrics”



Sysmin Sys73m47ic

QuiGon



www.hackerpimps.com

Document Versions

- You can download this document at:
- www.hackerpimps.com/docs.html

What Are Smarthomes?

- According to Smarthome.com:
- A home where the systems (security, lighting, sensors, heating and air-conditioning, audio-video etc.) are interconnected to allow the automatic or remote control of the home to save energy, improve comfort, safety and or convenience for the homeowner.
- Wow, That's a lot of possibilities!
- Smarthomes are the homes of the future.

Couple of Smarthome Projects

- GA Tech's Aware home
 - <http://www.awarehome.gatech.edu>
- MIT's House_n
 - http://architecture.mit.edu/house_n

Info In This Presentation

- Some of the technology discussed in this presentation is not available yet.
- It would be good to address vulnerabilities early in production or pre-production.
- Some vulnerabilities are difficult to mitigate.
- It doesn't matter because companies are going to sell it to people knowing it isn't ready and safe for use.

Motivation for Presentation

- Program on TV
 - Nerd!
- Current Trends in Technology
 - Stupid companies trying to scare customers
- Idiots for elected officials

A Shift In Focus

- **Smarthomes have typically been focused on luxury. (Not everyone can afford the Clapper!).**
- **There has recently been a shift in Smarthomes toward assisted living.**
 - **Elderly, disabled, etc..**
 - **This is important for later.**
- **In the future Smarthome components will be a standard part of everyone's life.**
 - **Why? Because we love getting 0wn3d!**
- **Smarthomes change not only how we interface with the home but also how the home interfaces with us.**

Focus on the Elderly!

- Sorry, we know this is twisted, but mildly amusing at the same time!

My sons hit me, says wheelchair-bound man



Wheel-chair bound Mr Lo Ghee Chua, 80, has accused two of his sons of slapping him. He is with another son, Mr Loh Peng Boo, 42.

The 80-year-old alleges that two of his sons slapped him and one had tried to push his wheelchair down a slope

Contents of a Smarthome

- Servers
- Connected Appliances
- Cameras
- Furniture
- Jewelry
- Etc, Etc, Etc
 - Many newer devices will come with some sort of connected capabilities, even if it is only for updates.

Interfacing with a Smarthome

- Phone
- Web
- Wireless
 - 802.11x
 - Bluetooth
 - etc, etc, etc.
- RFID
- Power outlets
- Cat5, Fiber, etc..
- Countless future interfaces that haven't even been thought of yet

Smarthomes Interface with Us

- **Smarthomes are Intrusive!!!!**
 - **News to you right?!**
 - **Technology can affect the way we feel**
- **Mood pendants**
- **Photo albums**
- **Prediction of activities**
- **Prediction of content**
- **Decision Making**

Prediction Technologies

- **What you want for breakfast.**
- **What you watch on TV.**
 - **What type of pr0n you like.**
 - **This could be interesting.**
 - **Favorite Television Shows.**
- **What type of food you like.**
- **Systems hold vast amounts of trended data about us.**
 - **An advertising company's dream.**
 - **3rd parties may be interested in getting this data.**
 - **Embedded spyware for your smarthome systems?**

Prediction Technologies

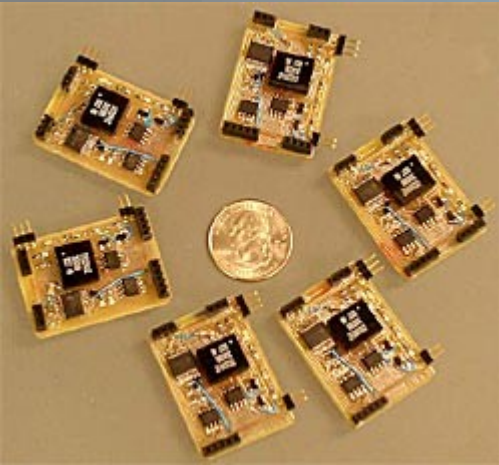
- So what does all of this stored, predictable information about us mean?
 - We are going to have to read our usage agreements very closely.
 - We are going to have to be mindful that exploitation of systems could result in far greater personal information being stolen.
 - Our personal pr0n archives could be ripped off!

Context Aware

- Context aware computing involves using sensors and logic in order to analyze movement and activities.
- An oversimplified example might be recognizing that you are about to walk in to a room and turning on the lights with a red tint, while when your friends enter the room it would turn on a green light.

Environmental Sensors

- These pictured are from MIT's House_n



Impacts of Vulnerabilities

- Think about the impact of your computer being compromised. Bad right?
 - Passwords?
 - SSN?
 - Bank Account?
 - Credit Cards?
 - Tax Returns?
 - pr0n?
 - Browsing Habits?
 - How stupid your screenname is?
 - Etc, etc, etc...

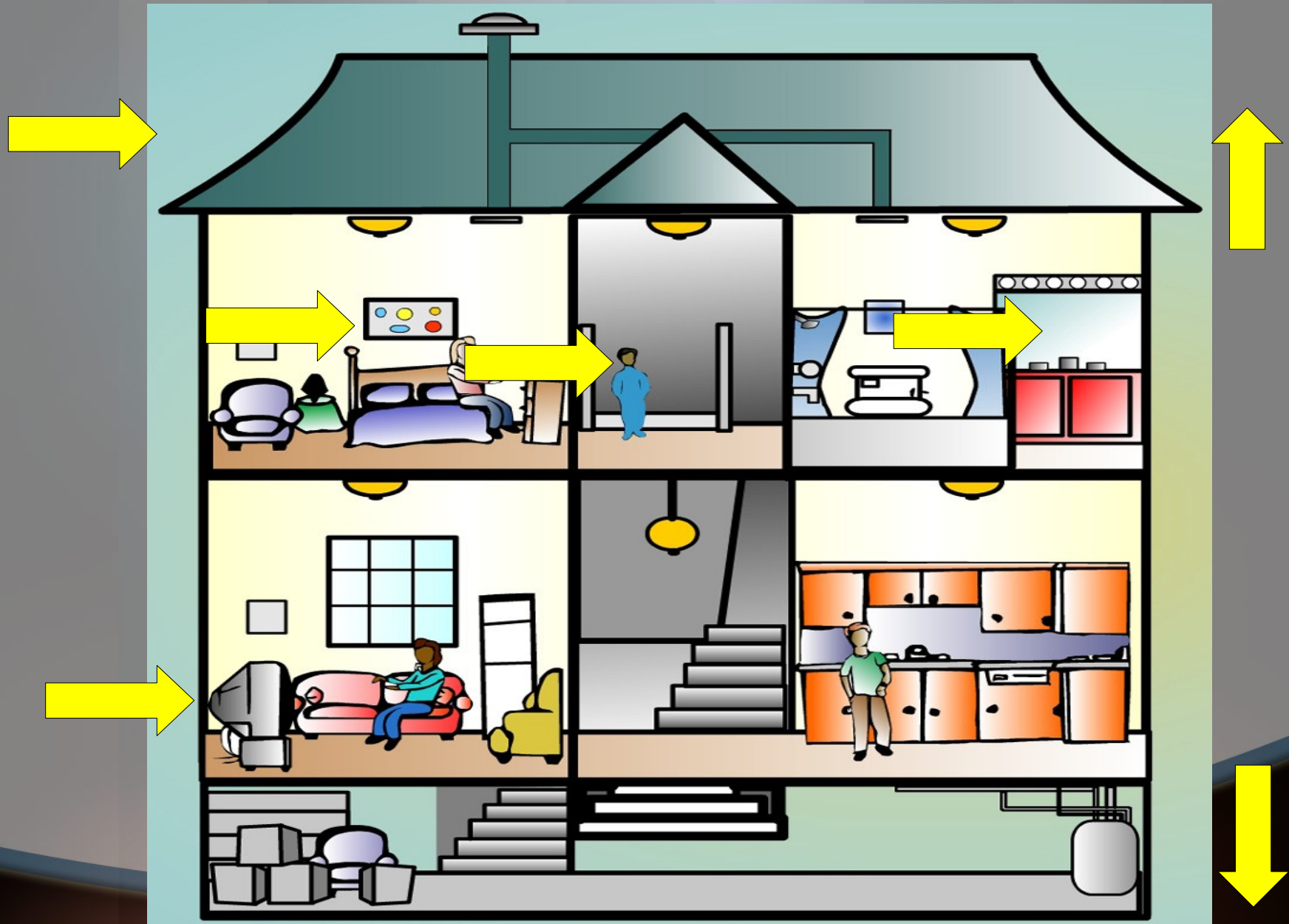
Impacts of Vulnerabilities

- With a Smarthome, it could be way worse!
 - Internal video cameras?
 - Arm/Disarm Alarm?
 - Change Prescriptions?
 - What you like to DVR?
 - Temp you like in your house?
 - Mischief with connected appliances?
 - Learn true habits?
 - Location Technologies?
 - Know if just your kids are home?
 - Etc, etc, etc...

Places for Vulnerabilities

- **Countless places for vulnerabilities:**
 - **In Equipment.**
 - **In Interfaces.**
 - **In Administration.**
 - **In Access.**
 - **In Protocols.**
 - **In Filtering.**
 - **In Processes.**
 - **In 3rd Parties.**
 - **In the medium used.**

Attack Vectors



Administrative Interfaces

- **Plaintext Authentication**
 - Password Sniffing (Although companies are getting better about this)
- **Plaintext Protocols**
 - Man in the Middle Attacks
- **Telephone**
 - Wardialing
- **Wireless**
 - Wardriving
- **Basically, Admin interfaces will be known to an attacker ahead of time.**

3rd Party Issues

- New technologies may require a connection to a 3rd party for:
 - Monitoring
 - Operation
 - Administration
- This all depends on how the technology is marketed and maintained. Most likely people will need to be connected to some third party for some form of maintenance.
 - Hmm... I wonder how secure that third party will be?
 - How vigilant or mature do you think the employees will be?

3rd Party Issues

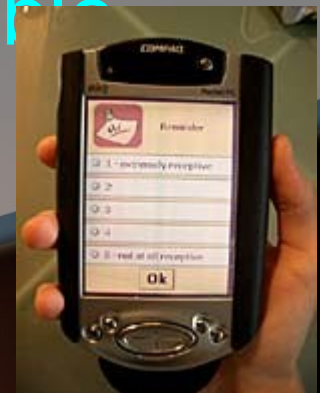
- Big potential for misuse and exploitation by insiders. Let's think about these people.
 - Possibly not even in this country.
 - Probably not paid very well.
 - They could be paid for information gathered.
 - Relatively unskilled.
 - Vast amount of information at their finger tips.
 - What about just good ole' fashioned mischief.
 - Voyeurism in its multiple forms.

Admin / User Interfaces

- Weak protections in place?:
 - Admin / User lockout.
 - Caveman and the wheel.
 - Although technology changes, stupidity is timeless.
 - No lockouts could mean better chances for automated attacks.
 - Manufacturer Backdoor accounts.
 - 3rd Party / Support accounts.
 - Possibly installed 3rd party backdoor accounts.
 - Possibly weak or well known reset procedures.
- People will still choose weak passwords and PINs.
 - They also might share this information with others.

User Interfaces

- Phishing Attacks for home logins
- Home logins could be the keys to the castle allowing an attacker to:
 - View if anyone is home.
 - Disarm alarms.
 - Steal personal information from network.
 - Voyeurism. (the only one we agree with ;) Just kidding
- Access home technology through portable devices. (phones, PDAs, Laptops)
 - Theft and credential recovery



Servers and Operating Systems

- Smarthomes are going to require multiple centralized computer systems to function properly.
- What os are they going to be using?
 - Microsoft
 - Linux
 - Cisco
 - ????
 - We all of these OSs have never had security problems right?

Servers and Operating Systems

- From an OS level all of the same vulnerabilities will still exist.
- These systems are still going to require:
 - Malware protection
 - Security Patches
 - OS updates

Exploiting the Medium

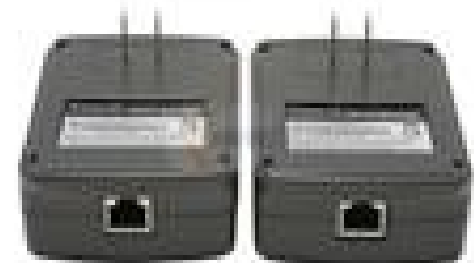
- Smarthomes use multiple mediums in order to communicate with devices and equipment. This might be any combination of:
 - Wireless
 - Fiber
 - Coaxial
 - Power lines
 - Cat5
 - Etc, etc, etc...
- All of these mediums can be tapped or just connected to.

Exploiting the Medium

- From a protocol perspective, it looks like one network.
- The IP address of your fridge plugged in to the power lines could be pinged from your computer connected to Cat5.
- This means the lowest hanging fruit can be exploited, from a medium standpoint.
 - Mediums can extend beyond the physical boundary of your home, two that come to mind are:
 - Wireless
 - EoP (Ethernet Over Power)

Ethernet Over Power

- Allows ethernet communications over your standard household power lines.
- Can bleed beyond the intended area.
 - We are in the process of determining just how far and it is still in early in the research.
 - This danger is compounded when in places such as an apartment complex, office complex, or skyscraper.
 - This means an attacker could be
 - In the next house?
 - In the next apartment?
 - In the next office space?



Ethernet Over Power

- EoP connections also have the potential to be exploited by plugging in to a power outlet on the exterior of your home.

Fingerprinting

- **Fingerprinting a home?**
 - **Oh yeah!**
- **Home fingerprinting takes on a whole new face with IPv6**
 - **Just think, all your connected appliances in the same network range and routed to the Internet.**
 - **This might give an attacker, or even a thief, a good idea of what is in your home.**
- **Signatures of different home appliances.**
- **Signatures of different home management systems.**
- **Just think, home fingerprinting databases, what a concept!**

Process Vulnerabilities


- Vulnerabilities don't have to be just buffer overflows and weak passwords.
 - Process vulnerabilities can be just as devastating.
 - Process vulnerabilities take advantage of steps in the process that are not properly checked.
 - Because they are not thought of ahead of time.
 - Because the manufacturer didn't care at the time.
 - Because they didn't know how to stop it, and still wanted to make money.
 - Usually an authorization issue.
 - A stupid picture frame example.....
 - It is going to take manufacturers a while to get it right.

Google Hacking the Home

- Search technologies may end up spidering information about the home.
 - These technologies can be searched for interesting interfaces.
 - Admin?
 - User?
 - Fingerprinting systems?
 - Don't worry, robots.txt will save you, right? right?

Video Services

- Marketed toward safety, but that can always backfire.
 - Sentinel Vision uses this to market fear. Look at this from their site, not worried very well.



Feel secure with panic service


(SafeScout) in their home or workplace and plugs in power and telephone cords just as they would with a common telephone answering machine. The Customer then registers online or directly with a Sentinel Vision Customer Service Agent.

During the registration process, the customer specifies who will receive notifications of events. The entire set-up process usually takes less than 15 minutes.

Our data center automatically processes this information and then sends images, audio and text alerts to the customers' and to their designated contacts' telephones, cellular phones, image capable cellular phones, pagers, email addresses and optionally to our professional monitoring center.

To use Sentinel Vision's notification services, a customer places a small, intelligent device (SafeScout) in their home or workplace and plugs in power and telephone cords just as they would with a common telephone answering machine. The Customer then registers online or directly with a Sentinel Vision Customer Service Agent.

During the registration process, the customer specifies who will receive notifications of events. The entire set-up process usually takes less than 15 minutes.



See that children are home

What

Renters people superior visual are sur

:: Hen

"I k safe

:: Mar

"It's kno from this time

Already registered?

[Customer Login](#)

Ready to get started?

[Register your SafeScout!](#)

Need some help?

[Users Guide](#)

Electronic Portraits

- Digital Family Portraits
- Connected Portrait Technologies
 - Remotely Send Pictures
 - Ceiva Currently offers this service
 - www.ceiva.com
 - Wouldn't it be funny for grandma to wake up with all of the pictures in her house displaying:
 - ????
 - ????
- The logical move is to make these wireless and then, let the games begin!

Life Threatening Consequences

- **Medical Systems**
 - Remotely Monitored
 - Remotely Exploitable?
 - What about a DoS?
- **Medicine Cabinets**
 - Order Prescriptions when you are low
 - Substitute your heart medication for Viagra?
- **What about no attacks at all, just a malfunction?**

Gesture Pendants

- Gesture pendants allow individuals to control household appliances with movements.
 - False positives.
 - This could be pretty bad depending on what are being controlled.
 - False negatives.
- Assumptions are made with this technology that it will actually be used properly.
 - We all know this has worked real well in the past.
 - Someone is going to have sex with one of these on at some point.

Gesture Pendants

- Here is a prototype from GA Tech's Aware Home Project.



Memory Aids

- Created with the intention of enhancing short and long term memory.
- Attacking them could lead to some interesting results. Mostly just having to do with mischief, but funny none the less. Here are a few:
 - Making someone think they did / didn't take their medication.
 - Messing up a recipe.
 - Creating confusing memories.
 - Replacing the icons used for a Tylenol with tubgirl!

Memory Aids

- The larger picture is, if overused isn't there a chance of lack of memory?
 - The more you use your brain, the stronger it becomes.
 - It has been proven that individuals that keep their brains active (Doctors, Scientists, Researchers) actually have less chances of memory problems and contracting Alzheimer's Disease.

Hacking Your Mood

- Increasing amount of technology surrounding our mood.
 - Sort of a digital mood pendant.
 - Items in the house may react differently depending on your mood.
- Attacking mood reactive technologies could
 - Make people second guess their true feelings.
 - Relatives and Friends may not believe you!
- I call this attack a “Mood Pendant” attack.

RFID Implants

- The thought of this is completely ridiculous, but as mentioned before. We love getting 0wn3d!
 - The technology has not matured enough yet!
 - These things are used for identification of you.
 - They can hold confidential data.
 - Can be read from devices in proximity.
 - Viruses!!! Hello!!!
- Baja Beach Club in Barcelona uses microchip implants for VIPs.
- Just think about the implications of spoofing, snarfing, MitM (unlikely, but not out of the realm of possibility) and DoS attacks.

GPS Implants

- This is also utterly ridiculous!
- Companies of the future will use scare tactics to think you need this for your kids.
 - Scare tactics worked very well for both the president and Hitler.
- What ever happened to just raising your kids?
- If people use this as a parenting device, then it is the parents who need their heads examined.
 - They aren't thinking about the future.
- Think about the actual risk of something happening to your kids.
 - It is extremely low

GPS Implants and Kids

- When advertising involves you children, think about the actual risk of something happening to your kids.
 - It is extremely low
- Think about the risk of something happening to your kids with the implant.
 - Medical issues
 - Technical problems
- Worst of all, you aren't the only one who knows where your kids are!
 - Misuse
 - Exploitation

IR and Forensics

- Having a smarthome or smartbuilding creates scenarios that provide interesting scenarios for the world of forensics.
- Are all of your devices time synchronized?
- What about logging, are the devices only logging errors?
- How are you going to determine when someone has successfully exploited a buffer overflow against your toaster?

Psychological Issues w/Tech

- Parents will use technology to raise their kids.
 - 10 times worse than just TV alone
 - Ignorant housewives everywhere are already pushing the FCC for harsher standards because they are lazy and really have nothing better to do.
- Oppressing children is not the answer.
 - Push too hard in one direction
 - Here is a true story.....
- Getting away with some things is part of growing up.

Possible Rejections

- Possible rejection of Smarthome technology because they are too intrusive to our privacy.
 - Although not very likely, we seem to like getting owned, for example Paris Hilton's Sidekick!
 - Because we don't like being tied to a vendor.
 - Because we don't want a 3rd party with access to our homes.
- Smarthome technologies are too intrusive for some people.
- Most likely we will just smile and accept the lack of privacy and intrusive nature of technology just because it is “Cool”.

Guess What?

- Vendors Lie!
- Commercials are not accurate or not even remotely true just look at:
 - Citi Identity Theft Solutions
 - Cisco Self Defending Networks
 - AT&T's New Security Campaign
- Much of the Smarthome technology will be marketed at safety and your kids.
 - Fear seems to be the best motivator, just look at some of the idiots we have in office right now.

Smartcars

- Connected
 - Back to the home
 - To the Internet
- Tracked
 - GPS
 - By Law Enforcement
 - By 3rd Parties
 - Largely because they force their technology down your throat by holding your kids over your head.

Smartcar to Home Connection

- Cars will be connected to home and control certain aspects.
 - Opening doors
 - Arming/Disarming Alarms
 - Video cameras
 - Etc, etc, etc...
- A company in Australia is already marketing this technology.
- Now look what happens.... Someone steals your car and they have a whole bunch of info they may not have had before.

Smartcar to Home Connection

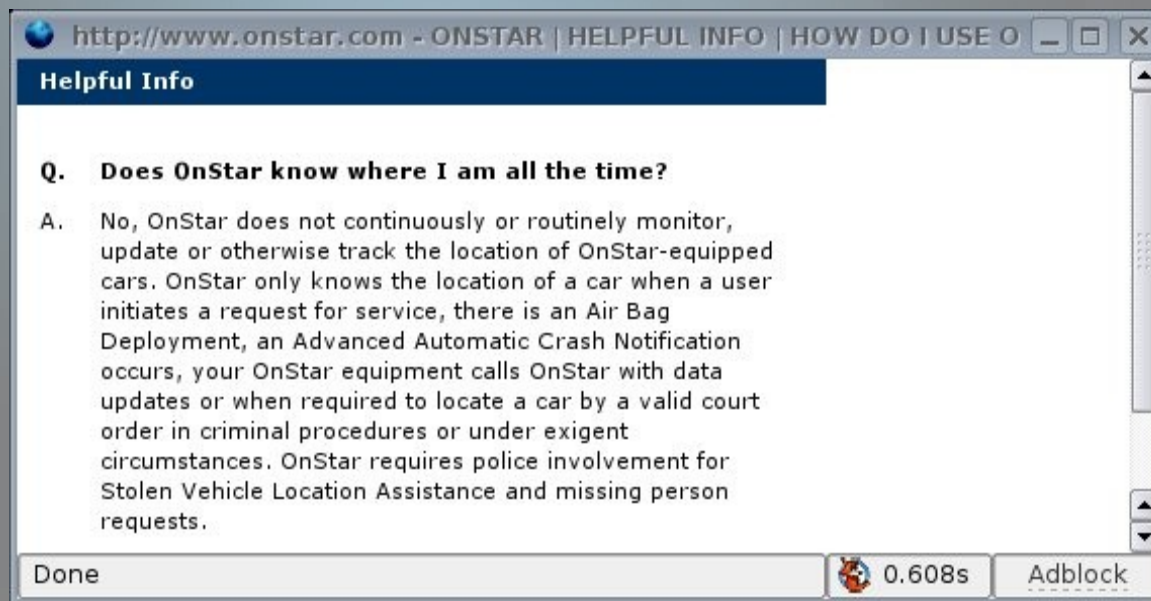
- This technology appeared to work through the cell phone network.
- The company assured that if the car was stolen there was no way the thief could get in to the home because:
 - People always log out like they should.
 - There is no way anyone would program their home address into a GPS.
 - People wouldn't want to customize any of the features and make them less secure.
 - People will always use devices for their intended purpose.

Integrating Biometrics in Cars

- Everyone knows what is about to be said, is your car more valuable than your finger?
 - To you, NO
 - To a crackhead, YES
- Integrating yourself in to your car dramatically increases the possibility that a physical part of you will have to be involved in carjackings and thefts.
 - Yourself
 - Your body parts

Smartcars/Vehicle Tracking

- Shall we discuss OnStar (and others)?
 - GPS Tracking and Remote Control of your vehicle
 - “Keep teh children safe”



Smartcars/Vehicle Tracking

ex·i·gent, adj. :

1. Requiring immediate action or remedy.
2. Requiring much effort or expense; demanding.

In other words, any time WE (OnStar) feels it necessary.

(You know....like anytime a 3LO asks us...)

Smartcars/Vehicle Tracking

- What happens when OnStar gets “hacked”?
 - Or a 3LO decides you're a terrorist
 - Or your uncle Bob gives \$50 to your cousin Vinnie who then donates \$30 to an Islamic relief effort
- They know where your vehicle is at all times.
- And it only gets worse....

YOU Tracking

- Cell Phone Triangulation
 - Only happens in TV and movies, right?
 - WRONG!!!

The screenshot shows the Wired News website interface. At the top, there is a search bar with the text 'Wired News' and a 'Search' button. Below the search bar is a navigation menu with categories: Top, Technology, Culture, Politics, Columns, News Wires, Blogs, and Wired Mag. A secondary navigation bar includes RSS and various topics: Cars, Computers, Gadgets, Internet, Med-Tech, Security, Space, Software, and Wireless.

Bomb Suspect Traced by Cell Phone

PRINT MAIL RANTS + RAUES

By Associated Press | Also by this reporter
13:25 PM May, 08, 2002

SAN JOSE, California -- Mailbox bomb suspect Luke Helder made a crucial mistake while on the run: He turned on his cell phone.

As soon as he activated it, FBI agents quickly triangulated his position between two rural towns and had him in handcuffs within an hour Tuesday, according to Nevada authorities.

Breaking
Breaking News from AP:

- ◆ Firefighters work on Ariz. protec
- ◆ Rain can't dim N.Y. gay pride p
- ◆ Kurdish immigrants facing prisc
- ◆ Floods force evacuations on Md
- ◆ Bishop defends actions on adm

Special Partner Pro

YOU Tracking

- Cell Phone Triangulation
 - 1. Triangulate Cell Phone
 - 2. Snarf all contacts/other info using Bluetooth
 - 3. Profit.

YOU Tracking

- Cell Phone Triangulation
 - Not just for the Feds anymore!!

FAQ | Features | Demo | Starter Kit | Sign Up | Login | Forums | Support



AccuTracking
Eyes
at Your Fingertips

Low Cost GPS Tracking Service for Everyone



START TRACKING TODAY >>

HOME SERVICES FEATURES DEMO STARTER KIT PRICING LOGIN FAQ SUPPORT FORUMS STORE ABOUT US

User Login

Username:

Password:

[Forgot password](#) Remember me



Low Cost GPS Tracking with AccuTracking

- No need for expensive devices
- Easy to use
- Online tracking 24/7

GPS Cell Phone Tracking & GPS Vehicle Tracking

AccuTracking software turns your Motorola iDEN cell phones or RIM BlackBerry phones carried by Nextel or SouthernLINC into a GPS tracking device. The AccuTracking online GPS cell phone tracking service lets you see real-time locations, speed, and headings of your children/family members or cars/vehicles, and receive email or SMS alerts when they move across the designated areas or exceeds speed limit. Your ultimate [low cost](#) real-time vehicle locator, child locator. [Starter Kit Sales](#)

News

YOU Tracking

- Keep track of teh children!!! YAY!!!
 - Or find out if your employees are sluffing off
 - Coworker you don't like called in sick?
 - Track his ass and get him fired for not being home
 - Or your spouse is at the bar instead of the office
 - Or at a bar CALLED “The Office”
- Some phones have the ability to turn off talking to two towers at the same time.
 - But not many....and rarely if ever by default

IPv6

- Odds are good Ipv6 will be used for many of these devices together
 - Com(a)cast will be using Ipv6 to control set top boxes
 - New technology...new exploitation capabilities
- Ipv6 Attack Suite
 - Written by THC (<http://www.thc.org>)
 - I'm sure this will be the tip of the iceberg once the protocol becomes more popular

Biometrics

- Biometrics are being touted as the be-all end-all security solution.
 - Pretty funny since Biometric data is not secret.
- Companies do not use biometrics as two factor authentication, but rather store passwords and just use biometrics.
 - From the user's standpoint this is still one factor.

Biometrics

- Biometric protections mechanisms need to be put in to perspective.
 - What is the goal of the protection?
 - What is the value of the item being protected?
 - Is the protected resource so valuable that it could cause a loss of a limb?

Biometrics

- Zamboni's DefCon 13 Presentation is a good overview of some of these problems
 - Attacking Biometric Access Control Systems
 - http://www.defcon.org/images/defcon-13/dc13-presentations/DC_13-Zamboni.pdf

“Identity Theft”

- Basically, fraud (ala Bruce Schneier)
 - Scam artist gets your info and exploits it via
 - Bank account fraud (AKA Nigerian 411 scams)
 - Paypal/EBay/Amazon logins
 - Pretty much all social engineering attacks
 - Or stolen data (more in a few...)
 - They're getting better at it
 - Better English
 - Scam sites look much more official
 - Sometimes even have valid SSL certs
 - Obfuscated URLs

“Identity Theft”

- You do not control your personal data!!!
 - Any veterans who served from 1975-present in the house?
 - This look familiar?



THE SECRETARY OF VETERANS AFFAIRS

WASHINGTON

Dear Veteran:

The Department of Veterans Affairs (VA) has recently learned that an employee took home electronic data from the VA, which he was not authorized to do and was in violation of established policies. The employee's home was burglarized and this data was stolen. The data contained identifying information including names, social security numbers, and dates of birth for up to 26.5 million veterans and some spouses, as well as some disability ratings. As a result of this incident, information identifiable with you was potentially exposed to others. It is important to note that the affected data did not include any of VA's electronic health records or any financial information.

“Identity Theft”

- How large would a 26.5 million record database be?
 - We wanted to know ourselves
 - Built a 30 column table and inserted 26500000 records
 - thank the godz for BASH scripts
 - around 40GB
 - Easily fits on an external drive

“Identity Theft”

- But they recovered the laptop
 - Yeah, after 2 MONTHS
 - Who knows what happened to it
 - Easy to mount a HD read only
- Policy Issue
 - The contractor had WRITTEN PERMISSION from his superiors to take the data home
- President Assmunch denies \$160 million for ID theft prevention for vets
 - But is more than happy to dump \$300 billion into a useless war...

“Identity Theft”

- You do not control your personal data!!!
 - Visa had records stolen
 - Mastercard had records stolen
 - State of Oregon had taxpayer records stolen
 - Etc., etc., ad nauseam
- Even places you have never done business with
 - ChoicePoint GAVE 163,000 records to ID thieves!
 - Who the hell are they?!
 - Why exactly do they have my personal data?

“Identity Theft”

- What happens when:
 - The database that contains the info for your Smarthouse/car gets stolen?
 - (And it will)
 - Full access to your vehicle and/or home

That's It!

Any Questions?

[sysmin\[at\]neohaxor\[dot\]org](mailto:sysmin@neohaxor.org)

[gene\[at\]hacktek\[dot\]com](mailto:gene@hacktek.com)