Identification Evasion

Knowledge & Countermeasures

WAL★MART®
ALWAYS LOW PRICES. Always.

identix
Empowering Identification™

ViiSAGE

U.S. DEPARTMENT OF HOMELAND SECURITY
Homeland Security

- To Think About
  - How many times daily do security cameras record your actions?
  - What unique identifying features distinguish your face?
  - What methods are available to obscure and protect your identity?
  - What identification methods (fingerprint, biometric, retina-scan) are used? How much do they cost? How effective are they?
  - What personal information is commonly used to identify you and how can you control such use?
  - What is an acceptable balance between personal freedom and government necessity?

Identification Evasion

In The Beginning

- What We’re Going To Talk About
  - Answer “To Think About” questions
  - General discussion of identity, privacy and the law
  - Why avoid identification? Are these methods legal?
  - In-depth: Computer World of applications, data and the Internet
  - Demo: IP Forensics
  - In-depth: Real World of brick & mortar stores, phone and people
  - Demo: “Night As Jason Biggs” video
  - Review
  - Next Steps
  - DC12 CD

Identification Evasion
You Want Answers?

- How many times daily do security cameras record your actions?
  - Approximately 13 times a day
  - Think about it: work lobby, elevator, bank, 7/11, lunch
  - Cameras record: black & white, color, movement, heat
- What unique identifying features distinguish your face?
  - There are about 37 unique measurements and elements on the human face from a 2D perspective
  - Including: facial hair, eye separation, colors, shapes, angles
  - How does software perform face matching with so many variables?
- What methods are available to obscure and protect identity?
  - Change your features: must meet believability/acceptance tests
  - Develop alt-info: duplicate and replace frequently requested info
  - Change other characteristics: try your walk, voice or stature

Identification Evasion

You Want Answers?

- What identification methods (fingerprint, biometric, retina-scan) are used? How much do they cost? How effective are they?
  - Most common: fingerprint ~80% of use
  - Most accurate: retina-scan although NONE are 100% perfect
  - Cost: least expensive is fingerprint (~$100+), most expensive is retina-scan (~$350+), biometric ranges according to method used
- What personal information is commonly used to identify you and how can you control such use?
  - Commonly asked for: phone #, social security #, driver's license #
  - Address obscured by a PO Box as a Suite #, now legal in all 50 states
  - Disclosure of personal information can be controlled by observing a few rules: give the minimum required, use alt-info and meet requirements differently
- What is an acceptable balance between personal freedom and government necessity?
  - You have a right to privacy and due process as guaranteed by the Constitution and upheld in courts
  - You should completely control what information is revealed and/or stored
  - The government's reasonable, minimum requirements for the enforcement of the law should be the prevailing principle

Identification Evasion
Identity

- Key Concepts
  - [*noun*] The set of behavioral or personal characteristics by which an individual is recognizable as a member of a group
  - Identity Theft rose to 500,000 cases costing $400 million in 2003, according to the FTC complaint database
  - Your identity is how others see you
  - Your identity is your individuality
  - Your identity should be protected
  - Q: Do we own our identity?
  - A: Maybe. It’s interpreted differently, but we ARE afforded legal protections for our personal information. Often, public personalities don’t have the right to determine use of their public image for informational, non-commercial use

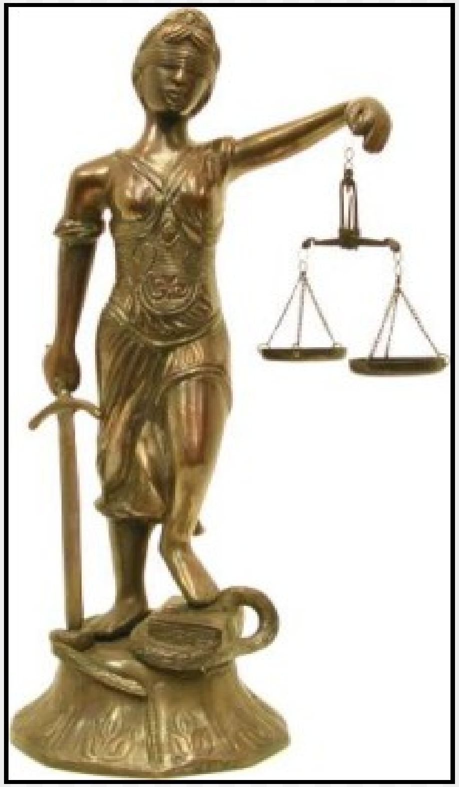
Identification Evasion

Privacy

- Key Concepts
  - [*noun*] The state of being free from unsanctioned intrusion; right to privacy
  - 83% of US citizens site privacy as their number one security concern (TIME)
  - Intruding on one’s rights, such as unsanctioned search & seizure (fourth amendment protection) is ILLEGAL
  - The right of privacy is an implied right in the Constitution enforced by precedent and upheld by the Supreme Court
  - The right of privacy is a liberty, a freedom from restriction in line with original Constitutional values
  - Notification of inquiry VERY important

Identification Evasion

The Law



- Key Concepts
  - **The Patriot Act (2001)**: "PATRIOT gives sweeping anti-privacy powers to domestic law enforcement and international intelligence agencies and eliminates checks and balances that previously gave courts the opportunity to ensure that those powers were not abused. PATRIOT and follow-up legislation now in development threaten the basic rights of millions of Americans." (eff.org)
  - *Negative 1*: No court order is required to spy on suspected computer trespassers in violation of the Computer Fraud and Abuse Act placing no limit on government surveillance of any computer user
  - *Negative 2*: Government has no reporting responsibility for surveillance making its spying targets and methods even harder to determine and analyze
  - *Negative 3*: Authorizes "sneak and peek" search warrants in connection with any federal crime including misdemeanors which means federal authorities can enter any private premise any time without informing the occupant and without a court-issued search warrant

Identification Evasion
Why Avoid Identification?

- Reasons and Benefits
  - Prevent unauthorized searches
    - You have a right to be informed
  - Prevent ethnic racism
    - For example, 75% of those targeted for further investigation by face recognition systems are Arab American (Boston Globe)
  - Prevent unfair targeting
    - If you were previously investigated or convicted for criminal activity but have been exonerated or served your time, you will be under continuous, often invasive watch by authorities
  - Prevent stigmatization
    - Being identified as a “terrorist” or a “hacker” casts a negative shadow over a person and could result in criminal investigation

Identification Evasion

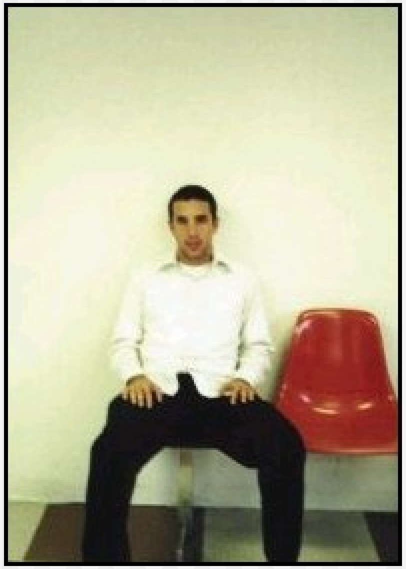
Is Identification Evasion Legal?

- Legal
  - Countermeasures are often not illegal (for example, selling radar detectors)
  - A new identity could be considered expression and we have many protections ensuring freedom of expression
  - People can be called “nicknames” and names may vary (Jr. or Junior)
- Illegal
  - Can’t invade systems (Computer Fraud and Abuse Act) or undo copy protections through disassembling code (DMCA)
  - Can’t inflict criminal damage or harm
  - Can’t endanger minors

Identification Evasion
Avoiding Identification

- *Computer World*
  - How are you identified?
  - Increasing anonymity while browsing
  - Increasing anonymity while emailing
  - Using encryption
  - Hiding personal information
  - Developing alternate usernames
  - Just Do It: Computer World
  - Demo: IP Forensics
- *Real World*
  - How are you identified?
  - Changing your appearance
  - Detecting surveillance
  - Defeating organic recognition
  - Defeating facial recognition
  - Developing alternate identities
  - Just Do It: Real World
  - Demo: “Night As Jason Biggs” video

Identification Evasion
By Adam Bresson



- Who I Am
  - 10+ years in computers with expertise in all PC OS's, Linux, PHP and Security
  - DC08 2000: Palm Security
  - DC09 2001: PHP, Data Mining & Web Security
  - DC10 2002: Consumer Media Protections (CMP)
  - DC11 2003: Manyonymity
  - Created Recommendo.com, a web community devoted to What You'll Like connections between Movies, TV, Books and Music with human-based reviews and ratings
  - Pioneered UnderMind.org, a web community that will allow people to post political questions and other members to verify facts by offering strong evidence, "Always Vote & Vote The Truth"
  - Working on CreateGreat.com, a web community for creative and business writers to organize their thoughts and make their writing stronger

Identification Evasion
Computer World

The Apple IIe has more software available for it than any other home computer.

- How are you identified?
  - Browser HTTP tags: contain your browser version, OS and even your email address (NS4)
  - Browser cookies: default privacy settings allow unrestricted cookies from origin site; just text, so may contain usernames and passwords
  - Browser history: where have you been all this time?
  - Email headers: routing information, username, meta-data
  - IP: reveals ISP, location, WINdata

Identification Evasion
Computer World

- Increasing anonymity while browsing
  - View your User Agent info fully-exposed by HTTP at http://www.rexswain.com/httpview.html
  - Use Mozilla Firefox with the Browser Identification plug-in to set your own parameters and obscure (i.e. Mozilla/3.0)
  - Use a proxy to strip information out of HTTP GET requests
  - Use a cookie blocker like Cookie Cruncher to monitor cookies and create strict, tightened rules
  - Surf the internet through a service that guarantees anonymity such as Anonymizer 2004 software

Identification Evasion
Computer World

- Increasing anonymity while emailing
  - Encrypt the text portion of your email inside a picture using a tool like H.I.P Hide-In-Picture or ImageHide [DC12CD]
  - Use an encrypted, Java email service such as Hushmail.com
  - Chain together three or more services for better protection via mail forwarding
  - Use an anonymous SMTP server which scrubs your email headers out such as http://luxsci.com/extranet/info/email-smtp-anon.html
  - Wi-fi Wardrive: install Free SMTP server [DC12CD] and send out emails with a masked IP address from any HotSpot! (SECRET: 1,600 Best Westerns in the U.S. have free 802.11b now, 100% by 12/04!)

Identification Evasion
Computer World

- Using encryption
  - Use MaxCrypt [DC12CD] to encrypt files and folders using Blowfish 448-bit
  - Encrypt text via PGP or an app like Cryptonite [DC12CD]
  - Use MD5 strings, sent separately, to verify that your content wasn’t tampered with using MD5Sums [DC12CD]
  - Encrypt EVERYTHING! Any information that might be connected forensically to you
  - COMMON SENSE: Don't use personally identifiable words (name, b-day, etc.) as decryption passwords

Identification Evasion
Computer World

- Hiding personal information
  - When registering your computer during a new OS install, enter a fake user/company
  - When registering software, use an alt-username
  - Use a non-traceable name on your Palm HotSync
  - Work hard to disassociate your username from your IP
  - Use RemoveHiddenData from MS to remove your personal information from MS Office files before sharing them
  - Use fake information when registering domains. Host your own domain and create fake chained email addresses

Identification Evasion
Computer World

- Developing alternate usernames
  - RULE: Make sure the alt-username does not relate to ANYTHING personally identifiable
  - Record your alt-usernames and where you use them to keep everything straight, create a new history
  - Use alt-usernames when registering for Web services, blind email addresses or vendor accounts
  - RULE: Safer to create three alt-usernames with different addresses, secret questions and birth dates [DC12CD]
  - EXAMPLE: notjbiggs on DEFCON forums

Identification Evasion
Computer World

- Just Do It
  1. Download and use Mozilla right now!
  2. Setup a Hushmail.com encrypted email account!
  3. Encrypt sensitive files using MaxCrypt!
  4. Reinstall your OS with a fake username/company!
  5. Create three alt-usernames using the Alt-Info Worksheet! [DC12CD]

Identification Evasion
Computer World

- DEMO: IP Forensics
  1. Determine source IP address
  2. Is it a Windows computer? (net view)
  3. Does it have open ports? (superscan)
  4. Where is it located? (reverse lookup, W3)
  5. Open services?

Identification Evasion
Real World

- How are you identified?
  - Security cameras in stores: some night-vision, some B&W, some color
  - Facial recognition at crowded public events like the Super Bowl or All-Star Game
  - Unique, important information: SSN, home phone #, address, mother's maiden name
  - Biometric, fingerprint, retina
  - RFID: radio chips that allow for tracking and association of data with movement

Identification Evasion

Real World

- Changing your appearance
  - The features 95% of people look at are eyes, hair, then nose
  - Subtle additions work best because they pass a Believability Test or The Toupee Rule. Perhaps because faces express emotion, a false feature looks unreal (think computer-animated humans)
  - Use a celebrity as a baseline. For example, you look 50% Brad Pitt. What would you need to change to increase the similarities? Are those additions believable? Ask a stranger
  - Your walk is intrinsic to your identity. Slowing your stride, increasing your pace or stepping on a different part of your foot can make it more difficult to identify you
  - QUICK TIPS: Blend colors and thickness of facial or head hair to make it more believable, add a mole or tattoo (frequently used as identifiers), change your eye color with contacts

Identification Evasion

Real World

- Detecting surveillance
  - U.S. businesses have a legal right to conduct surveillance and may record ANY person’s actions on their property
  - Start scanning for cameras outside as you walk from the parking lot. Look for flashing red lights, look for mirrored domes, check the corners of doors 8+ feet (normally set up this high to allow for wider angle of capture)
  - Assemble the location of cameras into a familiar shape in your head. For example, map three cameras to the points on a triangle with the entranceway as the center
  - Two-way Mirrors: use a keychain MAG flashlight to shine at suspect surfaces, light won’t reflect but will diffuse and show depth
  - Plain-clothes security: most often near highest-priced merchandise, tend to walk in patterns (their ‘beat’) so you’ll see them cover the same area in a predictable fashion

Identification Evasion
Real World

- Defeating organic recognition
  - Organic recognition works by taking unique measurements of your heat, retina or fingerprint. However, Gummi Bears can defeat fingerprint sensors 4 out of 5 times (The Register)
  - On average, 75% of Americans say organic recognition is acceptable in high security situations (U.S.B.J.S.)
  - Heat recognition relies on the overall pattern of heat emission from your body’s surfaces and can be fooled 75% of the time by cooling or heating your skin using ice cubes or a blow-dryer. Sample your skin temperature with a common household thermometer
  - Retina scans can be altered by changing your eye color or layout via adaptive contact lenses or by using a 5MP snapshot stretched over a cornea-round surface in Photoshop
  - Fingerprint recognition is fooled by gel overlays that match established patterns picked up by dusting or ink reconstruction

Identification Evasion

Real World

- Defeating facial recognition
  - Facial recognition works by creating a single measurement of several key vectors on a face and then comparing that numerical value to a previously stored/provided measurement
  - For example, Identix FaceIt technology starts by measuring the "pose angle" using your eye position to calculate face size and orientation. Changing your eye color to match you skin color, bloodshot eyes or a "pose angle" deviating 15%+/- from straight on can reduce the effectiveness of the system by 85%
  - Two different facial recognition systems used at Boston's Logan Airport failed to detect suspect individuals 62% of the time while also requiring two new workers' constant attention (The Register)
  - After recognizing surveillance, you can look for cameras that have Identix or Viisage logos on the stalk. They aren't domed because this would cause complete and utter failure

Identification Evasion
Real World

- Developing alternate identities
  - Any alterations must pass the Believability Test. No fake toupees or silly sunglasses. The more subtle the change to your appearance, the more it will be accepted. NOT noticing a change—having it integrated into your person—is the best tactic. [DC12CD]
  - Must create a full, well-fleshed out picture of another personality. Use included Alt-Info Worksheet to cover many aspects of another identity. Memorize everything and be prepared to answer branch questions such as, “Were your parents from there?” without hesitation or looking away (physical “tell” for dishonesty)
  - Build history: connect your alternate identity to a phone number, billing history, grocery club card or other membership services
  - SECRET: sign-up for a free 7-day, no credit card, web-accessible voicemail account with all-digital phone number, control panel, local area code and fax at http://www.reachme.com/getstart.html

Identification Evasion
Real World

- Just Do It
  1. Buy different eye-color contacts at a costume shop!
  2. Practice scanning your local supermarket for cameras!
  3. Carry Gummi Bears with you to defeat fingerprint scans!
  4. Adjust your "pose angle" when entering buildings!
  5. Sign-up for a voicemail account at Reachme.com!

Identification Evasion
Real World

- DEMO: “Night As Jason Biggs” video
  1. The Proposal: use Adam’s likeness to Jason Biggs to fake our way into Las Vegas night clubs and achieve free drinks, front-of-the-line, VIP status, a crowd and recognition
  2. Creating the Environment: alter clothes by changing into “Hollywood” club digs, alter hair by adding gel, alter buddies by designating one as my “Manager” and adding a camera, spotlight and “Director” to fit people’s image
  3. Plan Of Attack: Send in my “Manager” and “Director” to negotiate with the club’s manager on all points
  4. Barriers: one person didn’t believe that I was Jason Biggs…but thought I was Ben Stiller!, talking to the MGM Grand’s entertainment VP, not taking advantage of the situation, for fun
  5. The Video: excerpts from the DEF CON 9 Awards Ceremony

Identification Evasion

Conclusion

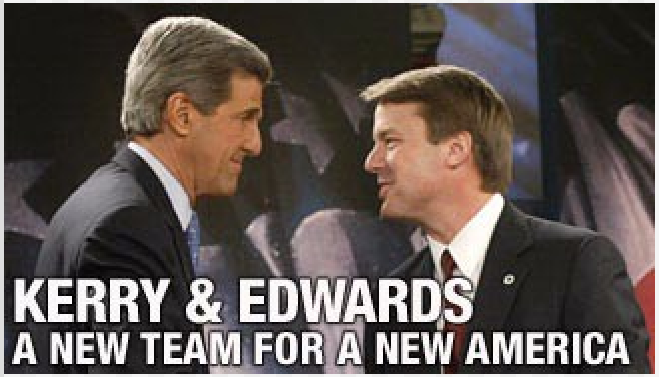
JOHNNY DEPP BENICIO DEL TORO
Fear AND LOATHING in LAS VEGAS
"EXCRUCIATINGLY FUNNY."
J. Hoberman, Village Voice

- Now You Know
  - Strategies for obscuring and protecting your identity
  - Computer World of applications, data and the Internet
  - Real World of brick & mortar stores, phone and people
  - How to wreak havoc and overcome fear & loathing
  - Identification Evasion’s Goal: respect privacy, restore personal freedom and ensure equality

Identification Evasion

Identity Activism

John Kerry
PRESIDENT



- Get Involved
  1. Sign-up at Misleader.org to learn the truth everyday
  2. Donate to the Electronic Frontier Foundation at eff.org
  3. Vote in every election you can and vote progressively
  4. Read several news sources for a more balanced view
  5. On November 2, elect John Kerry President!

Identification Evasion

Conclusion

- “dir \Identification Evasion” /DC12 CD
  - Identification Evasion Presentation (ppt)
  - “Night As Jason Biggs” video (avi)
  - Alt-Info Worksheet (pdf)
  - John Kerry For President--Flyer (pdf)
  - 01-Cryptonite 1.0 (freeware)
  - 02-FreeSMTP 2.01 (freeware)
  - 03-ImageHide 2.0 (freeware)
  - 04-MaxCrypt 1.10 (freeware)
  - 05-MD5Sums 1.1 (freeware)