Internet Anonymity
-How “They” Hide & How To Find “Them”.

Steve Manzuik
- Introductions / Outline
  - That’s this slide so we are done with that.

- Privacy vs. Anonymity
  - What is the difference?
  - Why?
  - Threat models.
  - How paranoid should you be?

- Good Intentions & Bad Ideas

- “Anonymous” Email Services
  - Hotmail, Yahoo, AOL, and GMail.

  - Proxy Servers.
  - Email Remailers.

- Not So Perfect Crime – Catching The Ghost
  - Web Bug Attack.
  - Social Engineering Attack.
  - Language Analysis.
Presentation Outline

- Normal End-User Anonymity / Privacy
  - What can you do?

- How a Hacker Could Remain Anonymous
  - Wireless Internet
  - Obtaining a Proxy
  - Cleaning the Logs
  - The “Throw Away” Laptop Concept

- Potential Solutions (Defenses)
  - Wireless Internet “Security”
  - End Point Security

- Closing
  - Future of Privacy / Anonymity.
  - Ideas to Make the EFF Squirm.

- Questions
Privacy vs. Anonymity

What is the difference?

Privacy

• Generally a “good thing”.
• Allows us to function in society free from judgment.
• Does have a level of accountability
• Is very important and should be protected.
• Online privacy is the expectation that entities in which you CHOOSE to share your personal information with protect that information and only use it for what it was originally intended for.
• Privacy is a function of Information Security.

Anonymity

• Not about functioning within society
• Provides ability to avoid social responsibility.
• Has zero level of accountability
• Also provides a way to guarantee privacy.
• Anonymity is a way around Information Security.
Why This is Worth Talking About?

• General confusion over the difference between Privacy & Anonymity.
• Everyone should have the right to their privacy.
• Anonymity or at least perceived anonymity is a “feature” of the Internet.
• Privacy has not been traditionally considered in the Internet world.
• This talk focuses on anonymity and ways it is abused.
• Defending against anonymous attacks while giving legitimate users their privacy is key.
Anonymity as a threat

- Spam
- Phishing/Pharming (Fraud)
- Virus/Worm/Trojan (Malware) Release
- Spyware
- Internet Harassment (e-harassment)
- Misinformation Campaigns
- Targeted Attacks
Threat Models

Anonymity as a benefit

• Prevent phishing and other fraud.
• Thwart unauthorized monitoring.
• Protect minors.
• Prevent Spam.
• Allow for open sharing of ideas without retribution.
How Paranoid Should You Be?

Tinfoil Hats

• My personal rule about e-mail.
• Web surfing.
• Work conduct.
• What about incoming traffic?
Good Intentions Bad Implementations

Arguments for Anonymity

• Sony XCP DRM
• Rogers Communications Cell Phone Snafu
• Cellular Phone Records For Sale
• Google (GMail, Google Desktop, etc.)
• “Network Splitting” with VPN Technologies
• ...
“Anonymous” Email Services

• Not quite anonymous.

• Gmail is better. For now.

• Hushmail is good. But is it trusted?

Received: from 64.4.51.220 by by107fd.bay107.hotmail.msn.com with HTTP; Tue, 21 Mar 2006 02:02:45 GMT
X-Originating-IP: [66.161.86.229]

Final results obtained from whois.arin.net.
Results:
SBC Internet Services SBCIS-SIS80 (NET-66-161-0-0-1) 66.161.0.0 - 66.161.127.255
eEye Digital Security 256845 SBC06616108622428040921123628 (NET-66-161-86-224-1) 66.161.86.224 - 66.161.86.239
The Perfect Crime

How Some Obtain “Anonymity”

• Proxy Servers
  • Switchproxy
  • Anonymizer
  • The Cloak
  • Others (Google returns 307 000 hits on “Anonymous Proxy”)

• Email Remailer Services
  • Anonymizer
  • Mixmaster
  • Others (Google returns 23 900 hits on “Anonymous Remailer”)

eEye Digital Security®
Not So Perfect Crime

Catching The Ghost

• Anonymous Proxy Issues
  • Who is running the proxy?
  • What is logged at the proxy?
  • Connection latency issues.

• Remailer Issues
  • No “anonymous” return path.
  • What is logged on the remailer?
  • Easy to filter at the gateway.
Not So **Perfect Crime**

**Catching The Ghost**

• **Web Bug Attack Scenario**
  • Rich Text / HTML Email is your friend (in this case).

• **Traffic Analysis**
  • Even smart attackers can forget.
  • Time consuming but can be automated.

• **Social Engineering Attack**
  • Draw target into an environment you can control.
  • Target’s greed and arrogance can be used against them.

• **Language Analysis**
  • Google is your friend.
Legitimate Anonymity

What Can You Do?

• Traffic Analysis Defense
  • Tor from tor.eff.org.
    • Distributed “anonymous” network.

• Corporate Environments
  • Force users to use VPN when remote.

• Be Aware
  • What websites you visit.
  • Where you use your credit/debit cards.
  • Who you are giving your personal information to.

• Fake Email Addresses
  • This is the true value to “free” email services.
Real Anonymity

How One Could Truly Remain Anonymous

• Do not use public open proxy lists.
  • Do use proxies in foreign countries like China.

• Wireless networks.
  • The house in a the residential area is probably safer than a Starbucks.

• Log cleaning.
  • Is it worth the risk to actually compromise a system to clean the logs?
    • A wireless router – this is easy to do in most cases.
    • Other systems not so much.
Real Anonymity

The Throw Away Laptop Concept

• Equipment Needed
  • Cheap (real cheap) laptop computer
  • Wireless card
  • Lighter & Lighter Fluid (optional)

• Software Needed
  • Whatever operating system you are proficient in
  • Netstumbler or equivalent
  • Network Protocol Analyzer
    • Ethereal
    • Iris
    • Others
  • Secure Disk Wiping or Volume Encrypting Software
    • SysInternals SDelete
    • PGP Desktop
    • Others
Real Anonymity

Step 1

• Leave your “known area”.
  • 60 minute any direction rule.

• Survey For Wireless Networks
  • I am sure *everyone* knows how to do this by now.
  • Identify at least two different networks.

• Go to Network 1 Location
  • “Pay Network” vs. Unsecured Wireless
    • Reality is both of these are insecure.

• Gain Network Access - ANONYMOUSLY
  • Resist urge to do anything “personal” from this laptop
  • Use this connection briefly to create new Internet alias’
Real Anonymity

Step 2

• Move on to a new area with a new “open” wireless network.
  • Before you connect – change your MAC address.

• Do your crime

• Wipe Evidence
  • Secure delete entire disk.
  • Pour lighter fluid on laptop keyboard (optional).
  • Put in dumpster
  • Drop in lit match (optional)

• Walk away.
Solutions

How Can These “Attacks” Be Prevented?

• Wireless Internet
  • Why not secure by default?
  • A better way to offer wireless services.
  • Better logging.

• Real End-Point Security
  • No I am not selling Blink today. ;-) 
  • Enterprises need to properly “lock down” workstations/laptops.
  • Enterprises need to invest in real end-point security measures.
  • Users need to be educated and understand the risks.
Closing

Crazy 1984ish Talk Slide

• Breaches in Privacy
  • Not enough is being done to organizations who fail in privacy.
  • Consumers are far too forgiving.

• Security Vendors
  • Need to focus on solving problems not selling product.
  • Solve a problem (do not add to one) and sales will come.

• Anonymity vs. Privacy
  • What level of privacy are we willing to give up.
  • Should we be able to so easily be “anonymous”?

• Is there really a good solution?