Interception Technology

The Good, The Bad, and The Ugly!

Jeffrey I. Schiller

Massachusetts Institute of Technology

What is Interception

- Ability to list/view/record information as it travels between some number of parties, without those parties knowing that it is being captured
- Traditional Case: Phone Wire Tap
- Modern Case: All communications, Voice, Video, E-mail etc.

Where to do Interception

- At the bit level?
- At Layer 2?
- At the IP Layer
- At the application itself?

At the bit Level

- OC3 Mon is an example
  - Looks "sideways" at the light going by
  - Assembles packets from there
- Problem: Need to sort through all the "bits" to get the actual information
  - Bits move fast!

Layer 2 and IP Layer

- Need to provide hooks in layer 2 switches
  - These already exist to some degree
    - Example: Port Replication
- IP Layer
  - Need to subvert routing
    - This can be done, if you can divert packets for transparent caching, you can do it for this!
- Problem: Sorting through the packets looking for the data

Layer 3 Interception

- Need to sort through the data
- How do you know what to intercept
  - IP addresses change, most lawful interception is targeted at people, not just simple processes
- This is what Carnivore supposedly does
  - Though they won't tell us!
- Requires fast enough computers to keep up
- Requires only limited cooperation from service providers

Application Layer Interception

- Requires least computing power
- Most accurate
- Requires the most cooperation from the service provider

Application Layer Examples

- E-mail
  - Sendmail's "Milter" facility can be used to make copies of e-mail based on criteria such as From and To fields (or even subject!)
- Web Services
  - Can make copies of "interesting" targeted transactions

Goals?

- Depends on who you are
  - Law Enforcement
    - Reliable interception with maximum operational security
  - Service Provider
    - Trust of customers, shield from liability
  - Citizen
    - Accountability of Law Enforcement

      Don't spy on me!
  - Everyone
    - Secure, bad guys don't use it!

Security?

- History has shown that this required an open design
- Every security design I have seen done behind closed doors has been shown to be weak
- There is a convenience versus security trade-off
- A critical part of security is accountability
- Technology must be easy to use, or it will not be configured correctly
  - If mis-configured, security will be lost, but things will "work"

Law Enforcement

- Requirement for "Operational Security"
  - Very few people know about the intercept
- Cheap
  - Can do more intercepts
- Available
  - No technical limit on number of intercepts
- Remotely implementable
  - Makes it cheap!

Citizen

- Wants checks and balances
- Accountability
- Security
- Wants confidence in Systems in use
- Remember:
  - A loss of confidentiality is very hard to trace

Service Provider

- Wants to make $$$
- Wants protection against liability
  - This tends toward a "Hands Off" approach
- Reputation is important

Carnivore

- Internet Interception: Version 1
- Works at IP Layer
- Not Cheap
- Requires minimal cooperation from ISP
- Has reasonable operational security
  - Guys who help install it don't know what it is grabbing
- Accountability: What accountability!

The Balancing Act

- Should be designed in an "open" process
- Should be accountable
  - Should require intervention of Service Provider
  - ??? Can we do better?
- Should be secure
  - And very hard to make insecure

Can it be done?

- Maybe: If you limit who can do interception
- Problem: Do you limit it to the FBI
  - Note: There are over 19,000 law enforcement organizations in the U.S.
- What about foreign governments
  - How do you design accountability
  - Some governments may require non-accountability!

Will it be effective?

- Who are we going to intercept?
  - Stupid bad guys?
    - Are they really a threat?
- Steganography is already rumored to be in use by terrorists.
  - It certainly is readily available
- By facilitating electronic interception, we may be helping law enforcement to avoid the "hard" work of infiltrating the smart bad guys?
  - But whom am I to judge!

Quis custodiet ipsos custodes?

- So who does?
- Questions?