Trends in the Backbone and Changes from the PATRIOT Act

Agenda

- Background
- Important Changes to our lives
- Wiretapping 101
- Operational Challenges from the PATRIOT Act
- What we have recently seen in the backbone
- Questions

A few slides were deleted for posting purposes.

Before & After Sept 11

- Before:
  - Security was for technologists.
  - The critical infrastructure guys had trouble getting people to pay attention
  - *Nobody* paid for security
  - The blame game came and went.
    - (Fix your machine. Make me. No…..)
- After:
  - Security is now in everyday conversation
  - Many CxOs don't know what it is, but they need it.
  - Use Carnivore or Magic Lantern in a sentence and be loved and hated by all.
    - Most people wouldn't know a carnivore if I threw it out the window onto their car.
  - The White House, FCC, DOJ are involved now.

Recent changes (USAPATRIOT Act)

- Lots of cleanup, mostly in Computer Misuse (18 USC 1030).
- Stored Voice Mail and other 'stored communications' is done by search warrant, not wiretap.
- Fone and Internet over cable is now Fone and Internet.
  - The Cable Act does not apply to Internet comms.
- Pen registers may be used on Internet comm.
- If the Feds use their own tools, they must notify the court.
- Jurisdictional clean-up on warrants.
- Providers may voluntarily disclose emergency situations.
- No change in regulatory or CALEA impact! (47 USC 229)
- Lots of money laundering and terrorism stuff.

"I am not an attorney and yours will want the final say."

Welcome to wiretapping

Disclaimer:

I am NOT *your* attorney. You should ask them before you believe anything in these slides.

These slides may or may not reflect a public position of Genuity Inc.

Federal History

- Communications Act of 1934
  - Service providers may listen in or capture voice for "quality of service" concerns
- Omnibus Safe Streets and Crime Prevention Act of 1968
  - First Federal Wiretap law (Title III of the Act). (18USC 2510)
    - Call routing information (telephone numbers) & content (voice)
  - Applicable to most felonies
- Foreign Intelligence Surveillance Act of 1978
  - adds "national security threat" to the list of crimes
- Communications Assistance to Law Enforcement Act (CALEA) (1987) (47USC 229)
    - Requires a standard interface and results from fone providers
- Electronic Communications Privacy Act (1996) (18USC 2701+)
    - Add cellular to private communications and strengthens penalties

More History

- There are also state-by-state laws for state crimes.
  - Every state is different (MA ch 272, sec 99)

- Signaling the target that they are being intercepted is illegal (both federal and state law).
  - 5 years in jail or $250,000 fine

DOJ Reported Numbers

	1997	1998	1999	2000
Intercept apps requested	1,186	1,331	1,350	1,190
Intercept apps authorized	1,186	1,329	1,350	1,190
• Federal	569	566	601	479
• State	617	763	749	711
FISA:			780	880
Winner: Narcotics				894

Four types of intercepts

- 1/2. Subpeonas (Identification) (Records request)
  - Resolve an IP address, at a certain time, to a phone number, address, credit card, name, etc
  - This is an after-the-fact evidence gathering exercise.
    - 'Alleged' Illegal content
      - copyright & trademark; dirty pictures, etc
    - Origination of a Scan or Attack
    - Threat, harassment,or fraud.
  - PATRIOT ACT:
    - Codified the gathering of IP address & ISP account info.
    - Allows out-of-district search warrants

Four types of intercepts

- 2. Pen register (18 USC 3121, Ch 206)
  - Which fone numbers did a phone line call?
- 3.Trap-and-trace
  - Which phone numbers called a fone line?

  - Both are limited to phone traffic
  - Only Addressing or Flow information, not content
  - These are undefined for data & Internet communication
  - PATRIOT ACT:
    - Both can be used on Internet communications
      - Phone number is equiv to IP address

Four types of intercepts

- 4. Wiretap/Data Capture
  - [Title III] (18 USC 2510-2517)
  - The intent is to capture, in almost real-time, an entire conversation.
    - 1st Court Order: Lists the data and subject to collect
    - 2nd Court Order (to us): Hints from the judge
    - Capture cannot normally exceed 30 days; update court every 10 or so
  - PATRIOT ACT:
    - Government must notify court if they use their own tools
    - Stored communications (voicemail, email, etc) only need a warrant, not a wiretap order (unlike real-time comms)

Example Paperwork

Computer Fraud & Abuse Act (47 USC 1030)

- Covers unauthorized access of a protected computer
  - Requires $5000 in damages to invoke law
  - Stored data is not communications
- (Preservation Orders, too) (18 USC 2703 b)
- PATRIOT Act:
  - Reduced the $5000 limit
  - Computer owner can request LEA assistance
  - Redefined 'protected computer'
    - Any computer connected to the Internet now qualifies
  - Defines "computer trespasser"
    - No longer have to prove attack, just trespass

What happens if we/LEA screws up?

- If we collect the wrong data:
  - The collected evidence may be inadmissable
  - The LEA may personally have criminal or civil liability
  - We could get a fine
- If we ignore the court order
  - We could get a fine
  - Someone (us) may go to jail
- If we do it:
  - The addition of equipment to the network may make the network unstable
  - Adding the collector to the network may alert the subject, which is prohibited

Impacts from USA PATRIOT Act

- Unclear if the non-consumer ISPs really care.
- Not much of an impact in our Operations
  - LEA still think in voice.
  - The real "what's changed" and how to deal with it have not been settled.
- Lots of complainants quote the law.
- Biggest impact in Public Relations……

Disclaimer:

I am NOT *your* attorney. You should ask them before you believe anything in these slides.

These slides may or may not reflect a public position of Genuity Inc.

An Operations View

What we have seen in the backbone recently

- The amount of Spam is up
  - Complainants are more pissy
- Subpoenas Processing is flat
  - Child porn reports are down
  - Copyright/DMCA are skyrocketing
- Attacks are up a tad
  - Still, most DoS is against IRC servers
  - Lots of old worms from unpatched systems

Expected Future Trends

- More Copyright/DMCA stuff
- LEAs will pay more attention to data networks

- Responsibility for insecure actions will become more testy

Thank You

pcain@genuity.com
dbowie@genuity.com

www.cdt.org -- Their view of changes to US Code
www.cybercrime.gov -- Visit the search and seizure manual
-- Field operations guidance
www.house.gov -- keeper of the US Code
www.uscourts.gov -- OAC reports