

What the Customer Wants



Critical Infrastructure Protection

- Control matches my needs in my terms
- Convenient to use
- Association of cause to effect
- I don't care to manage millions of bits
- My apps run fast and true, I don't trust them
- I want to chose between I, A, and C (etc.)
- The user, the world, and some trusted others

How bad is the IP covert channel



Critical Infrastructure Protection

- Trojan at U level up to TS
 - Inbound traffic via U side – 5Mb/s on 10bT
 - Outbound traffic via IP length/behavior
- How fast is the covert channel?
 - Normal packet lengths cluster at specific sizes
 - Avoid those sizes to reduce noise
 - Assume 10% for redundancy
 - ECCs per 32 bits
 - Feedback via overt channel
 - Assume I can double BW w/response packets

How fast is the covert channel?

Critical Infrastructure Protection

- 10M/sec (10bT) total BW
 - 10% of packet sized too noisy
 - Use average packet size 50 bytes
 - Of that, 32 bytes are IP overhead
 - 64 bytes of controllable length
 - 6 bits of signal per 50 bytes outbound
 - Another 6 bits in response BW
 - With redundancy, say 1 byte signal / 50 bytes carrier
 - $10\text{bt} = 1\text{Mbyte}(\text{carrier})/\text{s}$
 - $1\text{M} / 50 \text{ carrier/signal} = 20\text{Kbytes/second covert}$
 - I can tunnel 160kbit/sec covert IP with your TCB!!!