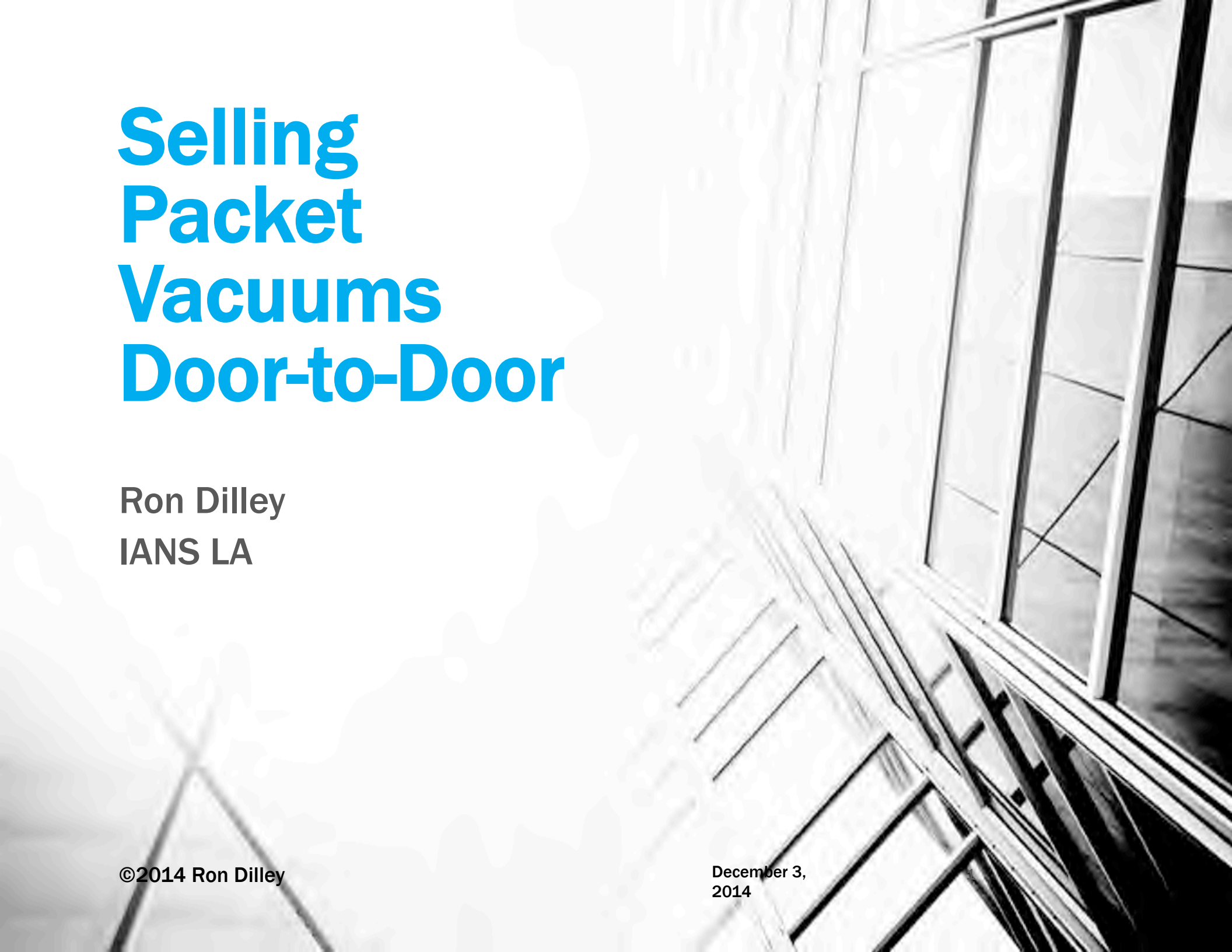
Selling Packet Vacuums Door-to-Door

Ron Dilley
IANS LA



December 3, 2014

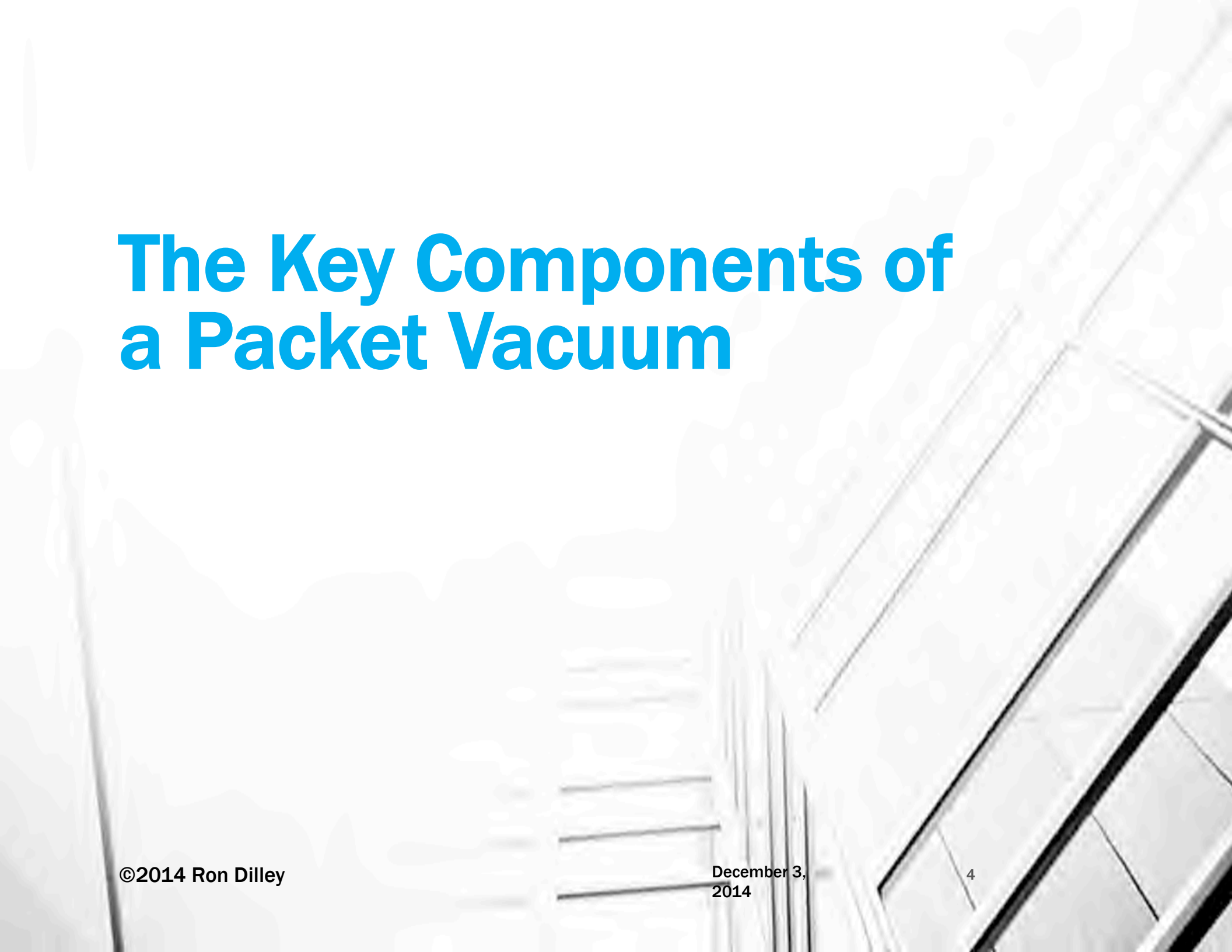
Sell the Problem

- Most understand the value of an alarm system
- When the bad guys leave, your property is still gone
- You don't know who did it or if they are coming back
- Unless they broke a window or kicked in the door, you don't know how they got in
- How can you stop or catch them next time?

The Pitch

- What is the first thing we do during a security incident?
  - I tell people to turn on verbose logging and setup a sniffer
- Sniffers are great, you can see everything except for the past
- **Packet Vacuums solve this problem!**
- They do not have to be expensive
- They do not have to be complex
- There are commercial and open source options (Moloch, NetWitness, etc)

The Key Components of a Packet Vacuum



Suction Matters

- How to get the packets into your vacuum
- How many ports, how fast are they, and how busy are they (now/future)
- Fast NICs make a difference (EnDace)
- tcpdump works, daemonlogger works better (Thank you Marty Roesch)
- TRICK: Minimize the number of IO transactions on high latency storage (RAM disks)
- Is a packet vacuum a wiretap? (Ask a Lawyer)
- HINT: If a packet vacuum is stand-alone, hardened with restrictive access, verbose logging and the raw data is only used for authorized incident response or forensic activities, that discussion may be pretty short (Even in the EU)

Capacity That Works, Even When the Bag is Full

- The lifecycle of packets in a vacuum is BASIC

```
10 SUCK
20 SAVE
30 COMPRESS
40 DELETE
50 GOTO 10
```

- What happens when the vacuum can't keep up?
- TRICK: Use parallel compression (pigz)
- What happens when you need to get packets out of the vacuum?
- TRICK: Use two bags, one for filling, one on stand-by. Switch to the stand-by and pull the full bag to preserve evidence
- I/O latency impacts packet vacuum performance, local storage is cheap and low latency

The Motor Must Be Reliable

- There is nothing more frustrating than an packet vacuum that no longer sucks or has a hole in the bag
- HINT: Physical taps are more reliable than a mirror rule (until someone disconnects a cable), pay attention to network packet brown-outs
- One month of storage is a good target
- HINT: Keep track of how many days worth of traffic is stored, network traffic may change and eat into your archive
- A well put together, sized and tuned packet vacuum can run for years without material intervention
- HINT: Pick a storage platform that is inexpensive to grow
- You don't need backups, and recovery is simple (rebuild and `goto 10`)

What Comes Out Is Way More Interesting That What Goes In

- Why wait until you have a security incident to look at those packets?
- TRICK: The packets are stored as pcap files (p0f, dsniff, snort, suricata, pproxyd) and send the output to your logging infrastructure
- You can synthesize netflow
- You can collect usage statistics and derive patterns

Use What You Sell

- I built my first packet vacuum in 2006
- It was crude, inefficient and quirky
- I have run them ever since, refining and improving year after year
- I can't imaging having to respond to a security breach without them

The Close

- We put flight recorders on planes and cameras in our convenience stores for good reasons
- **IT IS A NETWORK TIME MACHINE!**
- I have had many arguments with SysAdmins, InfoSec engineers and Executives about their utility and importance before they were installed
- I have **NEVER** had an argument after they were installed (especially after the first security incident)

The Columbo

- I bet you can't guess what I have done with my packet vacuums
- You can pull the exploit code right out of the packet trace (from two weeks ago)
- They really did use an un-published vulnerability in that application to remotely compromise a server
- Did you know that your SSL wrapped API is failing because of latency issues? It is true, I can see the error return code
- You say the backup server failed last month and the hard drive failed yesterday? You lost how many posted articles?

Q&A

ron.dilley@gmail.com