Forensics in the SoNIC Project on Precise Realtime Software Access and Control of Wired Networks

Ki Suh Lee, Han Wang, Hakim Weatherspoon
Cornell University

International Workshop on Trustworthiness, Accountability, and Forensics in the Cloud (TAFC)
June 6, 2013
The Rise of Cloud Computing

• The promise of the Cloud
  – A computer utility; a commodity
  – Catalyst for technology economy
  – Revolutionizing for health care, financial systems, scientific research, and society
The Rise of Cloud Computing

• The promise of the Cloud
  – ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NIST Cloud Definition
The Rise of Cloud Computing

• The promise of the Cloud
  – ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NIST Cloud Definition
The Rise of Cloud Computing

• The promise of the Cloud
  – ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST Cloud Definition

• How can we exploit the network for forensics, evidence, and accountability?
  – Public clouds: Bandwidth, availability
  – Private and hybrid clouds: exfiltration of data (covert channels)
Goal

Understand how to use the network to forensically account for and measure service level agreements in cloud

How to detect and/or prevent exfiltration of data from (private) clouds
Forensic Evidence via network interpacket delay

- Interpacket delay
  - Important metric for network forensic evidence
    - Can be improved with access to the PHY

Packet Generation  →  Increasing Throughput  →  Detecting timing channel  →  Packet Capture

Characterization  →  Estimating bandwidth
Forensic Evidence via network interpacket delay

- Valuable information: Idle characters
  - Can provide precise timing base for control
    - Each bit is ~97 ps wide
- Valuable information: Idle characters
  - Can provide precise timing base for control
  - Each bit is $\approx 97 \text{ ps}$ wide

- Characterization
  - Packet Generation
  - Detecting timing channel
  - Packet Capture
  - Estimating bandwidth

Packet $i$ to $i+1$ with one idle character $/I/$

$12 /I/s = 100\text{bits} = 9.7\text{ns}$
Forensic Evidence via network interpacket delay

- Valuable information in PHY: Idle characters
  - Issue1: The PHY is simply a black box
    - No interface from NIC or OS
    - Valuable information is invisible (discarded)
  - Issue2: Limited access to hardware
Goal: Control every bit in software in realtime

- Enable research on PHY covert challenge

Challenge
- Requires unprecedented software access to the PHY
SoNIC: Software-defined Network Interface Card

- Implements the PHY in software
  - Enabling control and access to every bit in realtime
  - With commodity components
  - Thus, enabling novel network research

SoNIC: Precise Realtime Software Access and Control of Wired Networks, Ki Suh Lee, Han Wang and Hakim Weatherspoon, Appears in NSDI, April 2013
Outline

• Introduction

• Examples of Forensic Evidence
  – Available bandwidth estimation
  – PHY Covert Timing Channel

• SoNIC: Software-defined Network Interface Card

• Concluding Remarks
SoNIC

6/14/2013

SoNIC DARPA MRC 2013
Forensic Evidence: Bandwidth Estimation

• Estimate available bandwidth
  – Traffic sent, packet trains:
  – Traffic received after going through bottleneck:

• Accurate available bandwidth estimation requires PHY
• Inter-packet gaps are invisible to higher layers, but not SoNIC
Outline

• Introduction

• Examples of Forensic Evidence
  – Available bandwidth estimation
  – PHY Covert Timing Channel

• SoNIC: Software-defined Network Interface Card

• Concluding Remarks
Forensic Evidence: Covert Timing Channel

• Embedding signals into interpacket gaps.
  – Large gap: ‘1’
  – Small gap: ‘0’

• Covert timing channel by modulating IPGs at 100ns
  • Overt channel at 3 Gbps
  • Covert channel at 250 kbps
  • Over 4-hops with < 1% BER
Forensic Evidence: Covert Timing Channel

- Modulating IPGs at 100ns scale (=128 /l/s), over 4 hops

CDF
0 0.2 0.4 0.6 0.8 1

SoNIC  Kernel

Interpacket delays (ns)
500 1500 2500 3500 4500

‘0’  ‘1’

‘1’: 3562 + 128 /l/s
‘0’: 3562 - 128 /l/s

BER = 0.37%

3562 /l/s
3562 - 128 /l/s
3562 + 128 /l/s

SoNIC DARPA MRC 2013
Forensic Evidence: Covert Timing Channel

- Prevent Covert Timing Channels?

CDF

Interpacket delays (ns)

3562 /l/s
Forensic Evidence: Covert Timing Channel

- **Router/ Switch Signatures**
  - Different Routers and switches have different response function.
  - Improve simulation model of switches and routers.
  - Detect switch and router model in real network.

Cisco 4948
Cisco 6509
IBM BNT G8264R

1500 byte packets @ 6Gbps
Outline

• Introduction
• Demo: PHY Covert Timing Channel
• SoNIC: Software-defined Network Interface Card
• Concluding Remarks
10GbE Network Stack

Application
Transport
Network
Data Link

Physical
64/66b PCS
- Encode
- Decode
- Scrambler
- Descrambler
- Gearbox
- Blocks
- PMA
- PMD

Data Link
- Data
- L3 Hdr
- Data
- L2 Hdr
- Data
- L3 Hdr
- Data
- CRC
- Gap

Network
Data

Transport

Application

Physical

64 bit
10.3125 Gigabits

Idle characters (/I/)

16 bit

011010010110100101101001011010010110100101101001011010010110100101101001011010010110100101101001011010010110100101101001011010010110100101101
10GbE Network Stack

Application
Transport
Network
Data Link
Physical
64/66b PCS
Encode
Decode
Scrambler
Descrambler
Gearbox
Blocksync
PMA
PMD

Commodity NIC

Packet i
Packet i+1
L2 Hdr
L3 Hdr
Data
CRC
Gap


0110100101101001011010010110100101101001011010010110100101101001

6/14/2013
SoNIC DARPA MRC 2013
10GbE Network Stack

Application
Transport
Network
Data Link

Physical
64/66b PCS
  Encode
  Decode
  Scrambler
  Descrambler
  Gearbox
  Blocksync
  PMA
  PMD

SoNIC
NetFPGA

SW
HW

Encapsulation
Packet i
Packet i+1

Data Link
Network
Transport
Application

L2 Hdr
L3 Hdr

Preamble
Eth Hdr

SoNIC DARPA MRC 2013
SoNIC Design

Application
Transport
Network
Data Link

Physical
64/66b PCS
Encode
Decode
Scrambler
Descrambler
Gearbox
Blocksync
PMA
PMD

Preamble  Eth Hdr  L2 Hdr  L3 Hdr  Data  L3 Hdr  Data  CRC  Gap


SW  HW

01: 01001011101001011011001001011010010110100101101001011010010110100101101101

SoNIC

SoNIC DARPA MRC 2013
SoNIC Design and Architecture

Application
Transport
Network
Data Link
Physical
64/66b PCS
- Encode
- Decode
Scrambler
Descrambler
Gearbox
Blocksync
PMA
PMD

Data Link
Network
Transport
Application

SoNIC

SoNIC DARPA MRC 2013
SoNIC Design: Interface and Control

- Hardware control: `ioctl` syscall
- I/O : character device interface
- Sample C code for packet generation and capture

```c
1: #include "sonic.h"
2: 
3: struct sonic_pkt_gen_info info = {
4: .mode = 0,
5: .pkt_num = 1000000000UL,
6: .pkt_len = 1518,
7: .mac_src = "00:11:22:33:44:55",
8: .mac_dst = "aa:bb:cc:dd:ee:ff",
9: .ip_src = "192.168.0.1",
10: .ip_dst = "192.168.0.2",
11: .port_src = 5000,
12: .port_dst = 5000,
13: .idle = 12,
14: }; 
15: 
16: /* OPEN DEVICE*/
17: fd1 = open(SONIC_CONTROL_PATH, O_RDWR);
18: fd2 = open(SONIC_PORT1_PATH, O_RDONLY);
19: /* CONFIG SONIC CARD FOR PACKET GEN*/
20: ioctl(fd1, SONIC_IOC_RESET)
21: ioctl(fd1, SONIC_IOC_SET_MODE, PKT_GEN_CAP)
22: ioctl(fd1, SONIC_IOC_PORT0_INFO_SET, &info)
23
24: /* START EXPERIMENT*/
25: ioctl(fd1, SONIC_IOC_START)
26: // wait till experiment finishes
27: ioctl(fd1, SONIC_IOC_STOP)
28:
29: /* CAPTURE PACKET */
30: while ((ret = read(fd2, buf, 65536)) > 0) {
31: // process data
32: }
33:
34: close(fd1);
35: close(fd2);
```
Contributions

• Network Research
  – Unprecedented access to the PHY with commodity hardware
  – A platform for cross-network-layer research
  – Can improve network research applications

• Engineering
  – Precise control of interpacket gaps (delays)
  – Design and implementation of the PHY in software
  – Novel scalable hardware design
  – Optimizations / Parallelism

• Status
  – Measurements in large scale: DCN, GENI, 40 GbE
Concluding Remarks

• The network is at the center of the cloud
  – SoNIC gives precise realtime software access and control of the network
  – Necessary for forensics, evidence, and accountability of network/cloud

• Network is useful to validate SLAs
  – Accurate bandwidth estimation
  – Characterize/profile/fingerprint network components

• Need to understand entire network stack to protect data
  – Demonstrate: Covert Timing Channel
  – 4 hops, 250kbps, less than 1% BER

• Status
  – SoNIC in large scale: DURIP, GENI, 40 GbE
  – http://sonic.cs.cornell.edu
  – SoNIC is available Open Source.

6/14/2013
My Contributions

• Cloud Networking
  – SoNIC in NSDI 2013
  – Wireless DC in ANCS 2012 (best paper) and NetSlice in ANCS 2012
  – Bifocals in IMC 2010 and DSN 2010
  – Maelstrom in ToN 2011 and NSDI 2008
  – Chaired Tudor Marian’s PhD 2010 (now at Google)

• Cloud Computation & Vendor Lock-in
  – Plug into the Supercloud in IEEE Internet Computing-2013
  – Supercloud/Xen-Blanket in EuroSys-2012 and HotCloud-2011
  – Overdriver in VEE-2011
  – Chaired Dan William’s PhD 2012 (now at IBM)

• Cloud Storage
  – Gecko in FAST 2013 / HotStorage 2012
  – RACS in SOCC-2010
  – SMFS in FAST 2009
  – Chaired Lakshmi Ganesh’s PhD 2011 (now at UT Austin)
Thank you!

http://sonic.cs.cornell.edu