SAND2015-10415C

Information Leakage in Encrypted IP Video Traffic

Chris Wampler, Selcuk Uluagac, and Raheem Beyah

Georgia Institute of Technology – Florida International University

wampler.chris@gatech.edu, suluagac@fie.edu, rbeyah@ece.gatech.edu

December 8, 2015

Outline

- It is possible to detect activity in a video stream by analyzing network packet metadata

- Background
- Early experiments and results
- Information leak origins
- Testing repeatability
- Our “Big Skype Experiment”

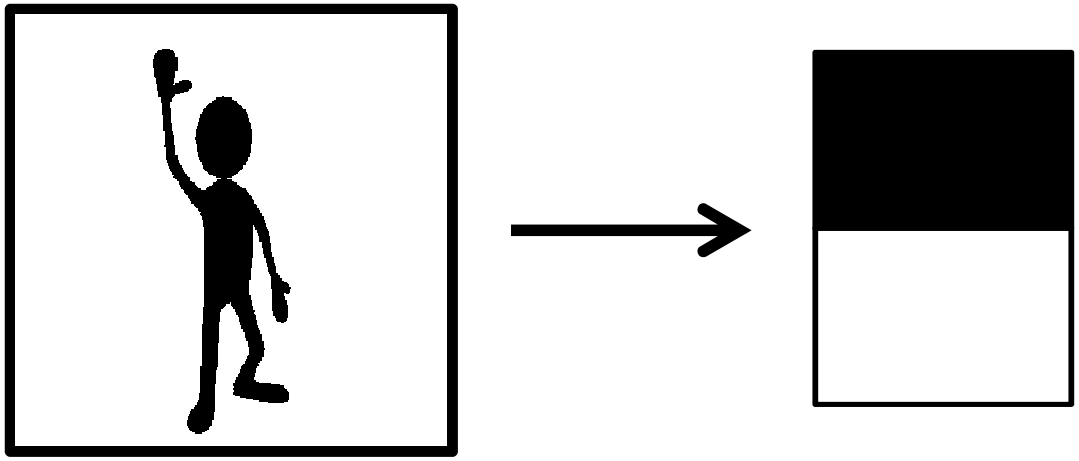
Origin

- Inspired by “Spot Me if You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations” - Wright et al.

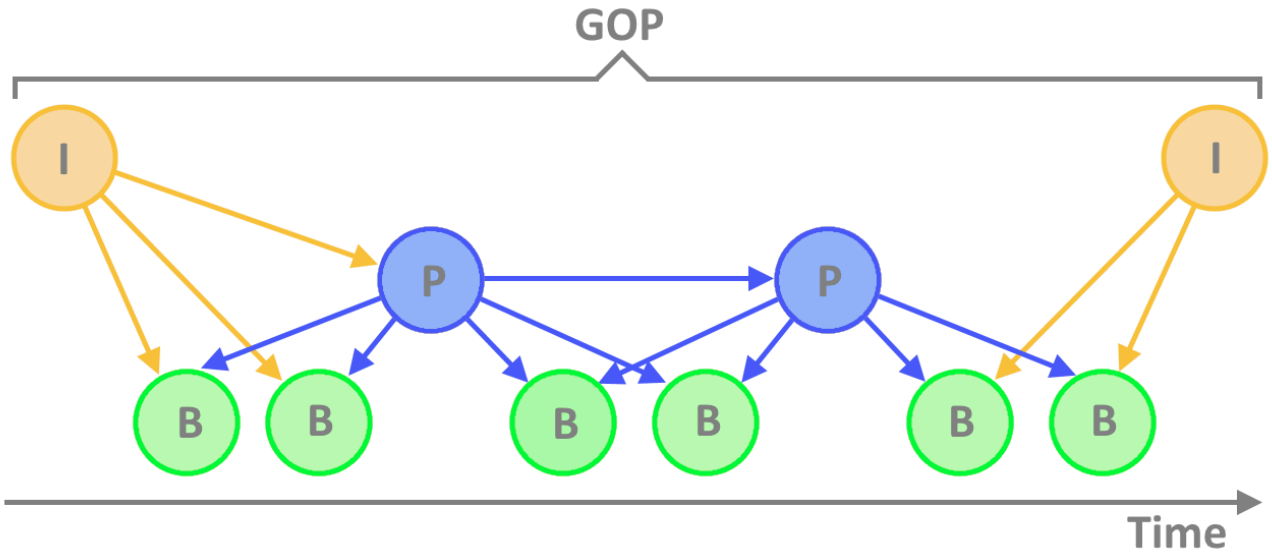
- Our question: Can network traffic also reveal activity in a video stream?

Image and Video Compression

Spatial compression



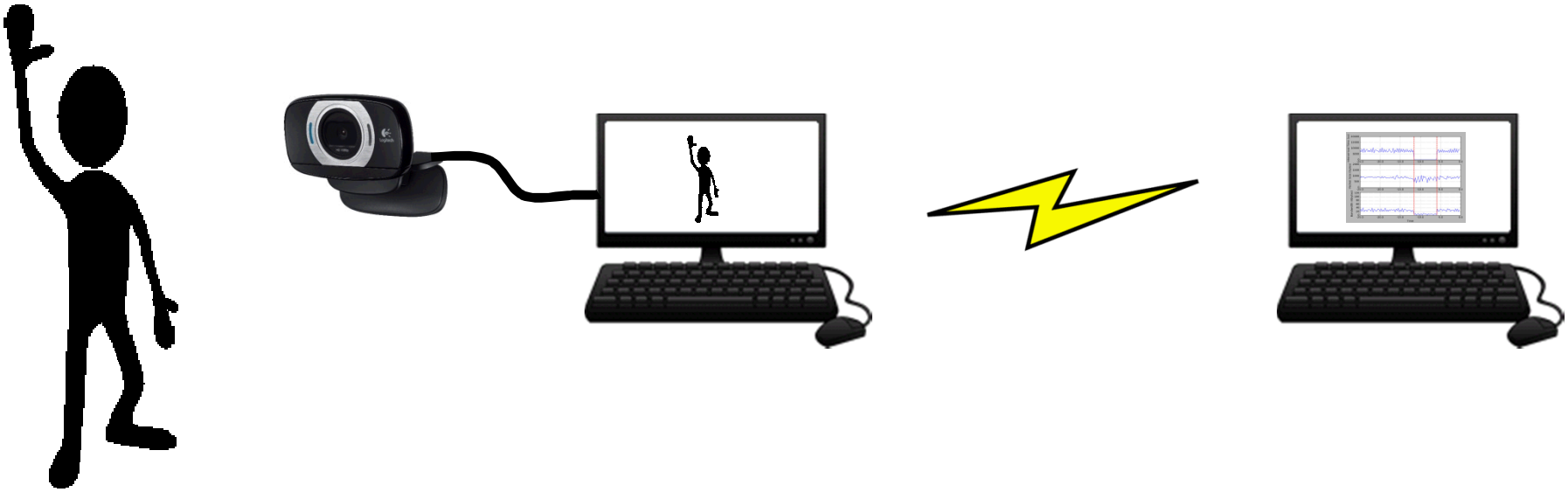
Temporal compression



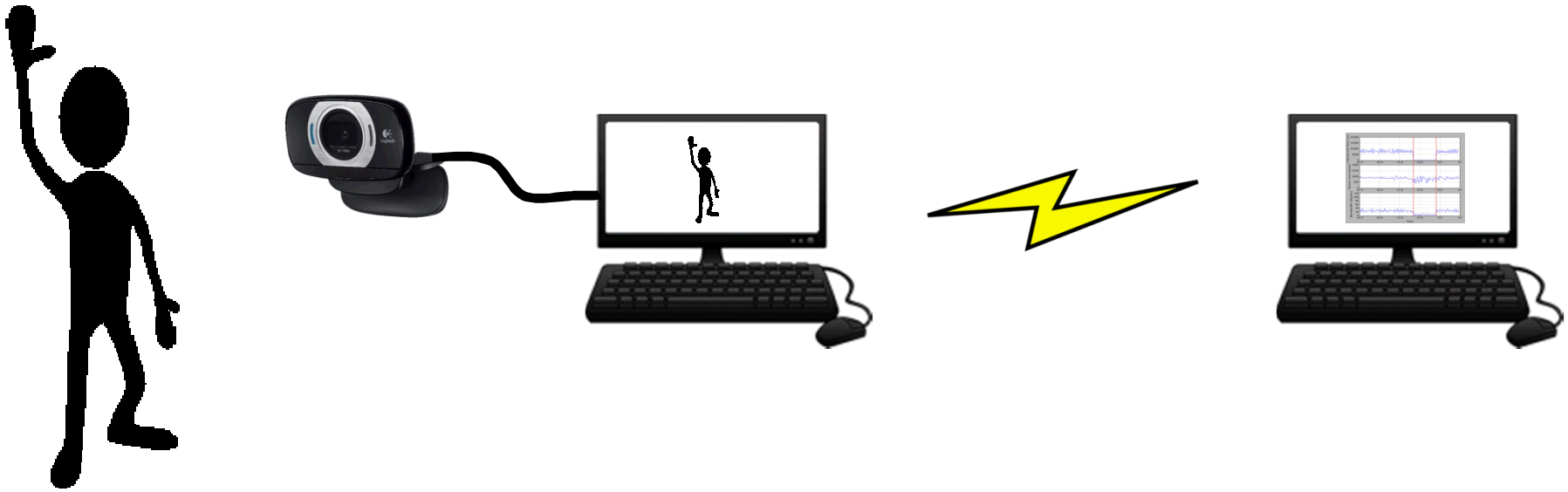
Indicators in Video Streaming Traffic

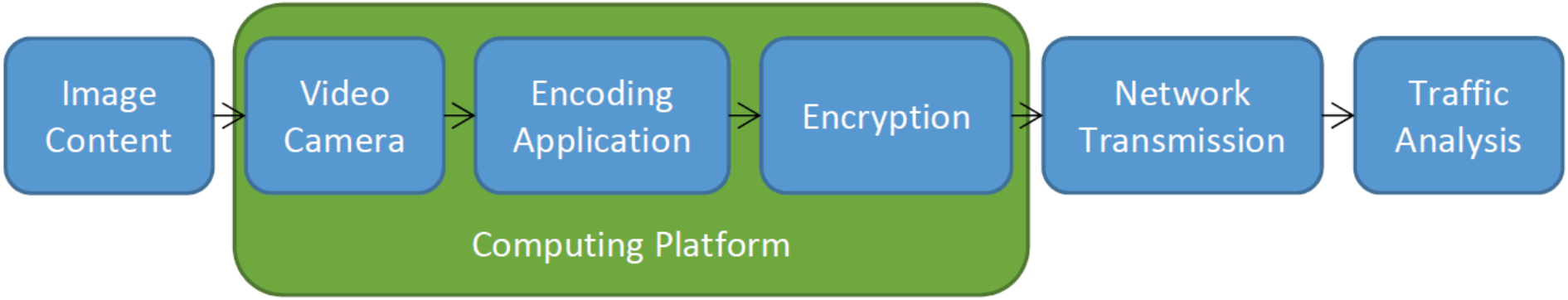
- Focus: single person in front of a still background
- Objective: classify uniquely identifiable events in video using network packet metadata

Experiment Setup



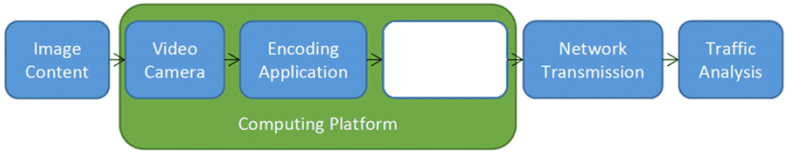
Video Encoder Pipeline



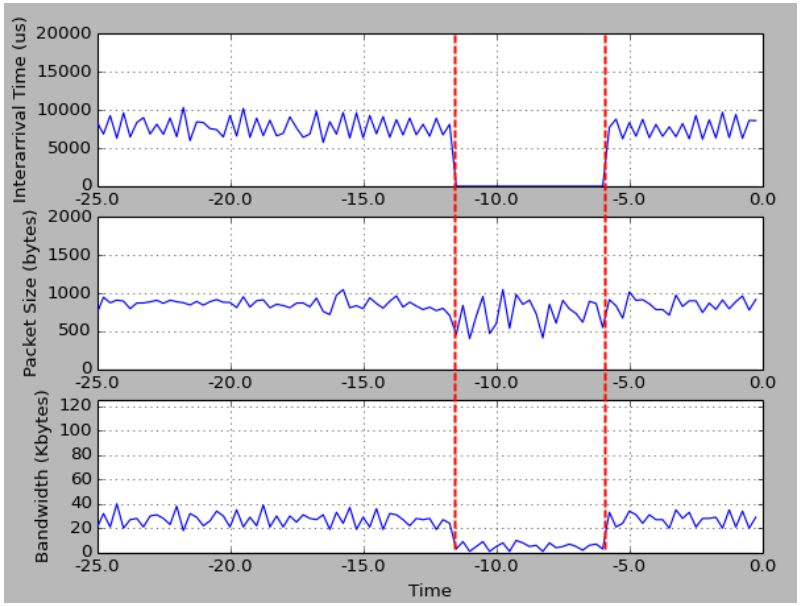


Event Detection Without Encryption

- Quickly found information leaks in three ways:
  - Time between packets (inter-arrival time)
  - Packet size
  - Video stream bandwidth

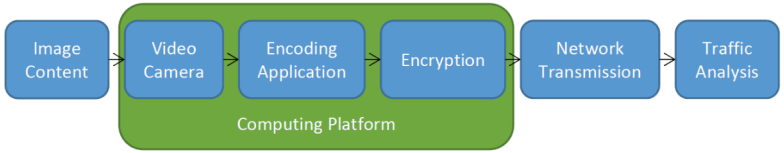


- At right: Unencrypted traffic shows lights turned off and on

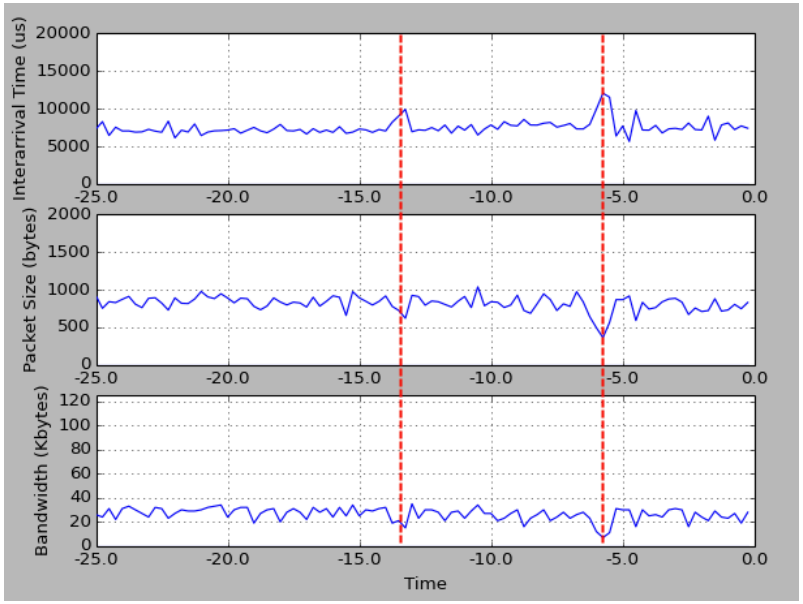


Motion Detection in Encrypted Video

- Encryption did not fix information leaks



- At right: Encrypted traffic reveals two hand waves



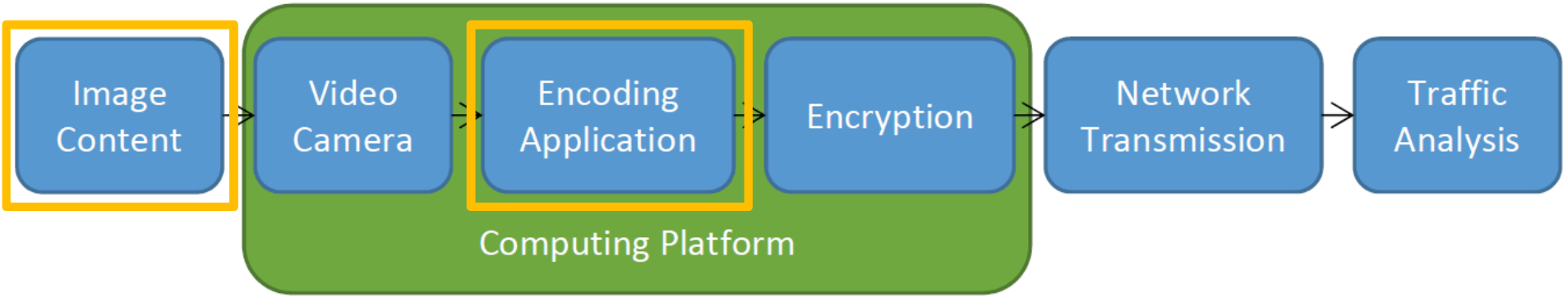
Expanding Variables

- Variety of encoders
  - Skype, Google Hangouts, GStreamer, Facetime, proprietary hardware

- Multiple video cameras
  - High, medium, low grade consumer

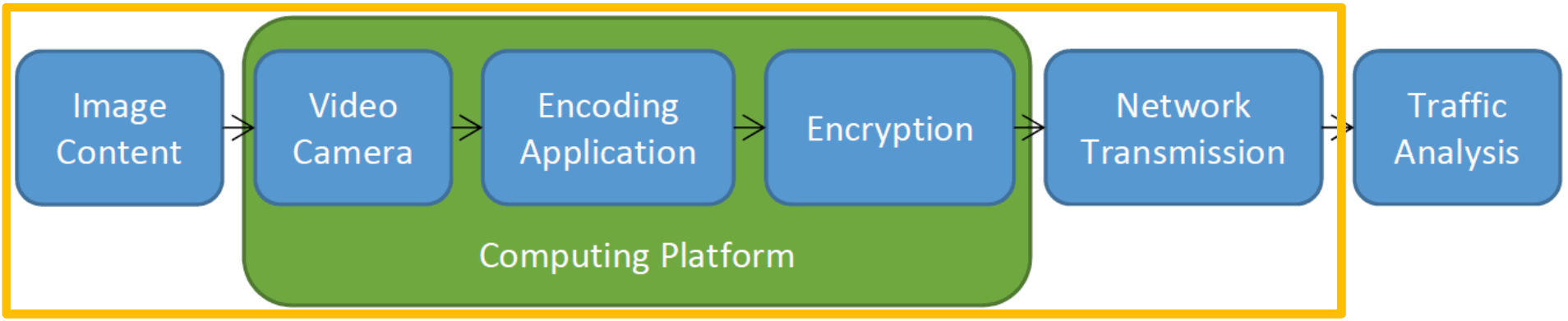
- Variation on computation capability
  - Laptop, desktop, phone

Detectable Events



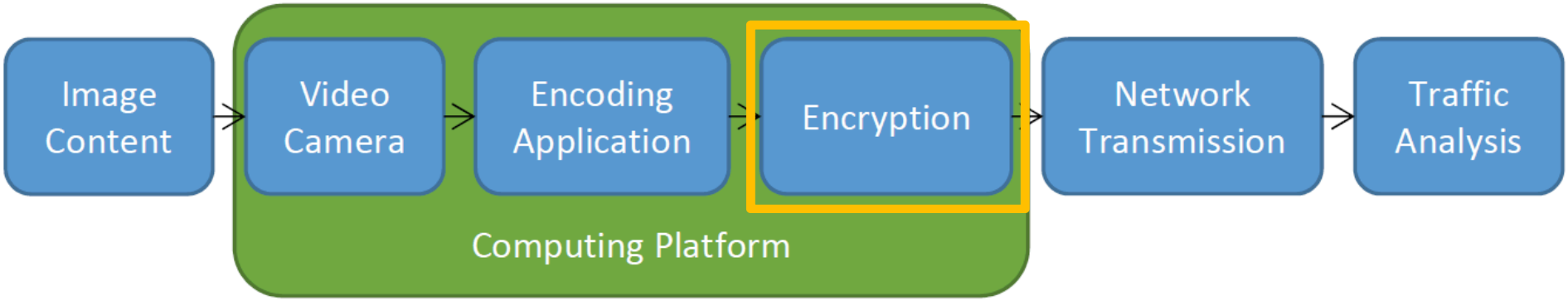
- Image Content
  - Lighting transitions
  - Hand wave past camera
  - Stand up and walk away from computer
- Encoding application
  - Start/stop encoding

Interference



- Image – too much movement
- Cameras – varying resolution and quality
- Encoders – dozens of setting in each type
- Computer – other apps and raw power
- Network – bandwidth truncating data
- Encryption – … none

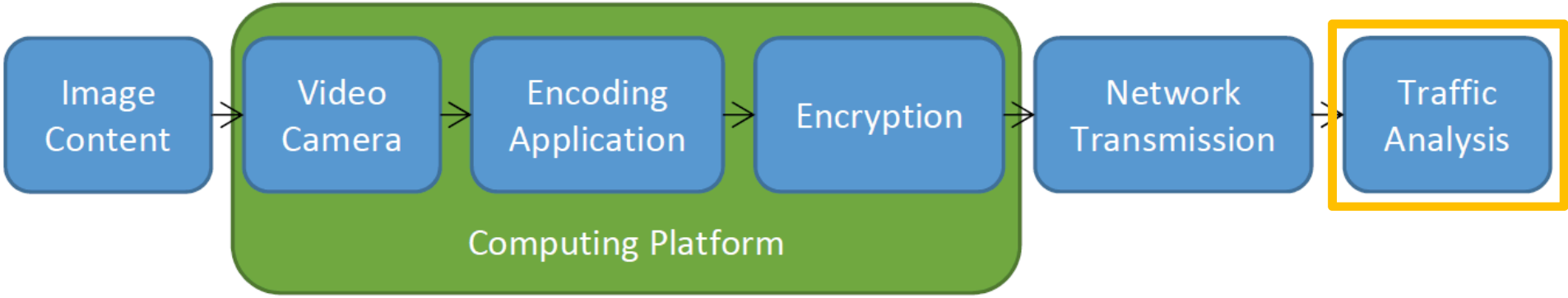
Interference from Encryption



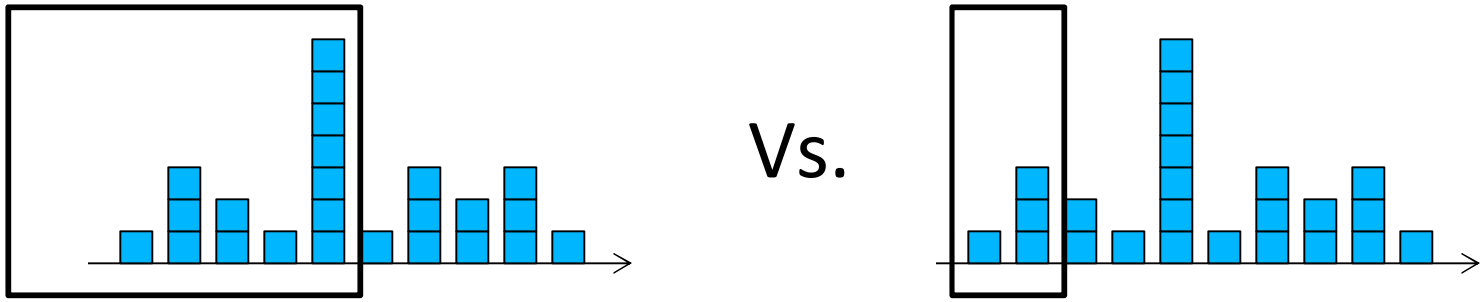
- 'Good' encryption algorithms:
  - Don't significantly expand data size
  - Don't delay transmission of data

- Packet destination and port aren't encrypted

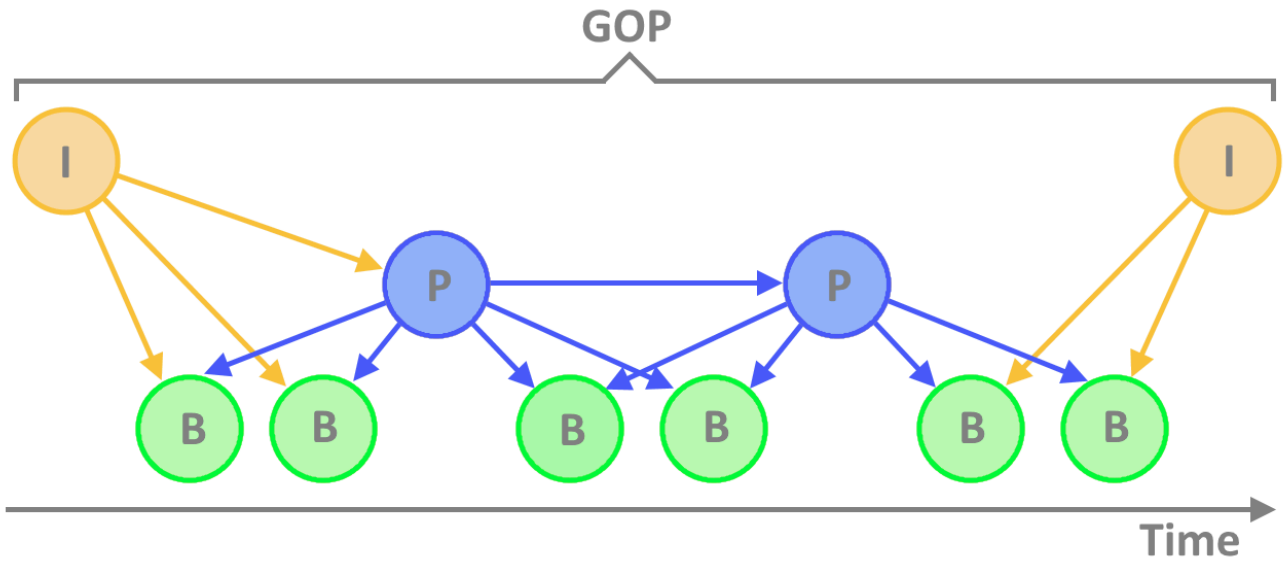
Network Traffic Analysis



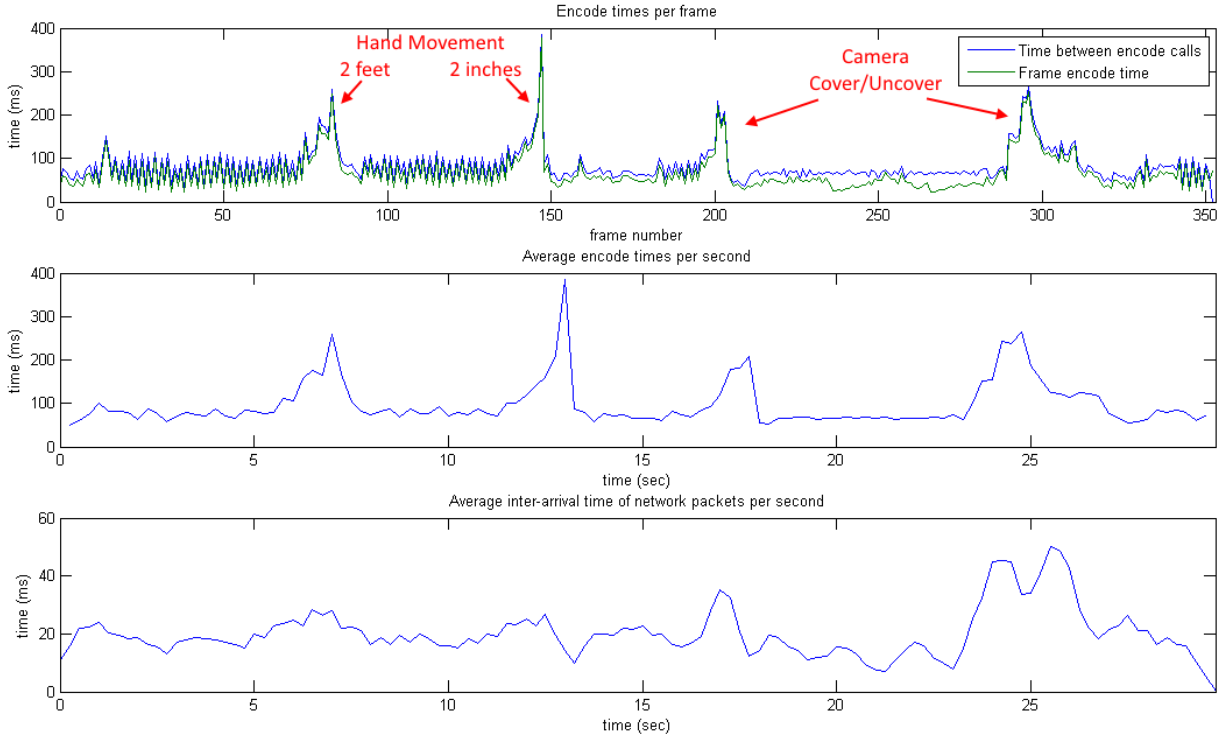
Window size



What's Leaking?



GStreamer x264 Encoder

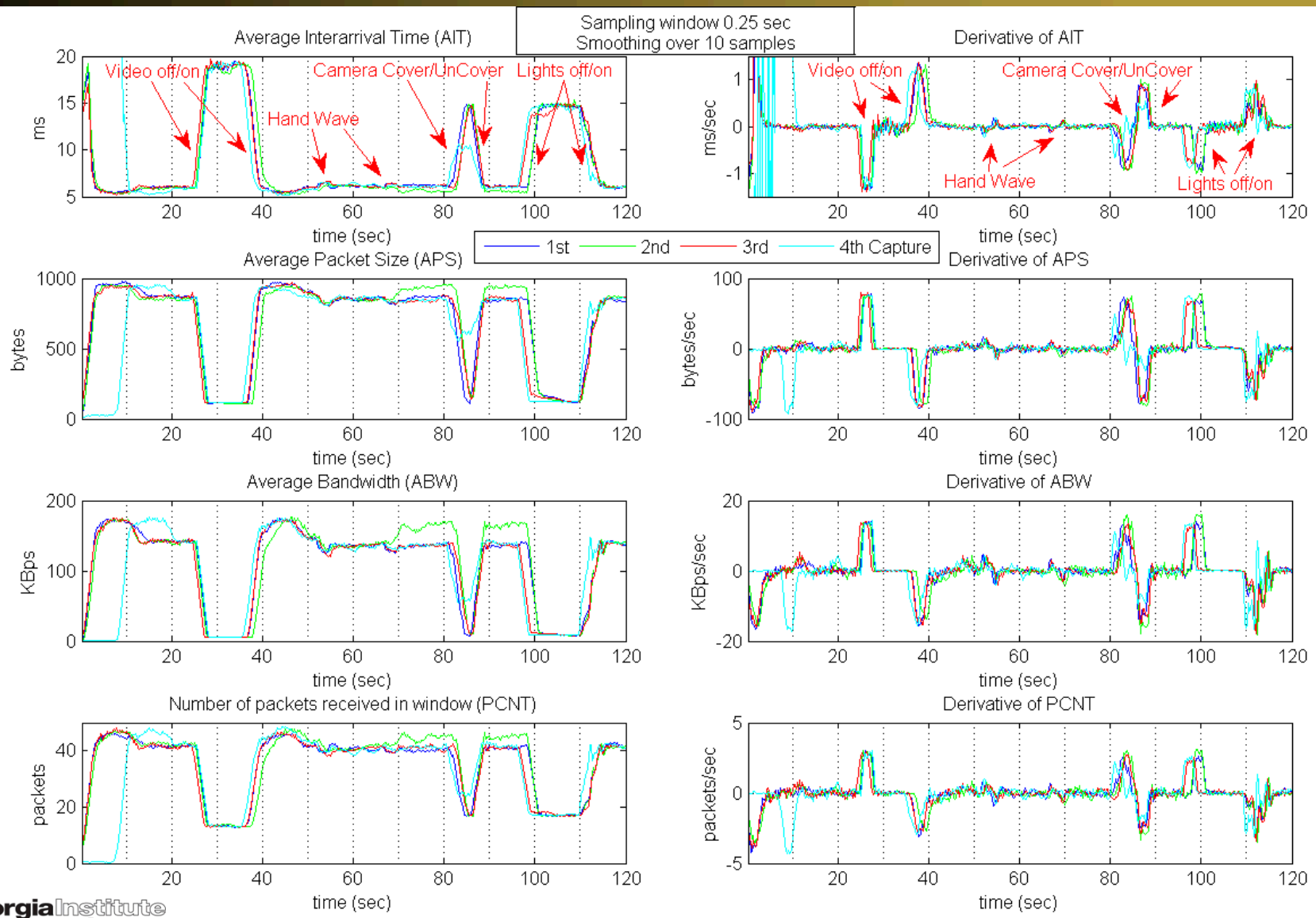


- Simple image yield fast encoding
- Adding abrupt movement slows down the encoder

Outline

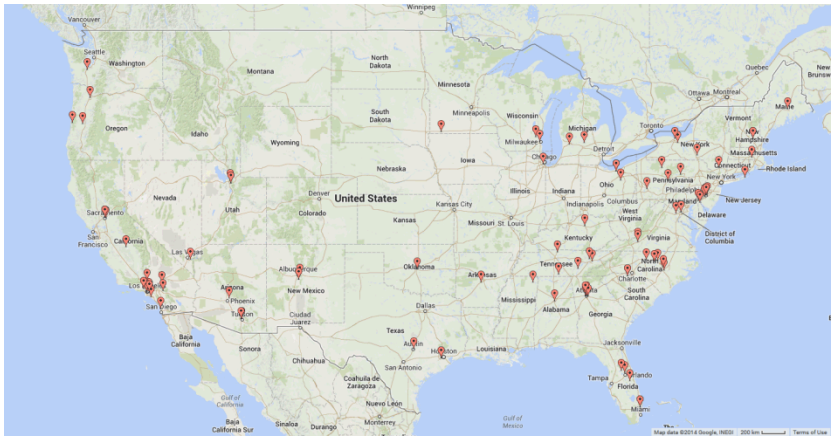
- Background
- Early experiments and results
- Information leak origins
- **Testing repeatability**
- Our “Big Skype Experiment”

Skype Traffic Analysis (Lab Results)



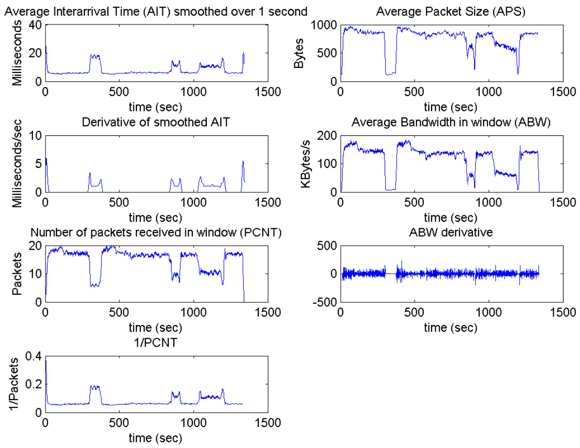
Skype Network Traffic Collection

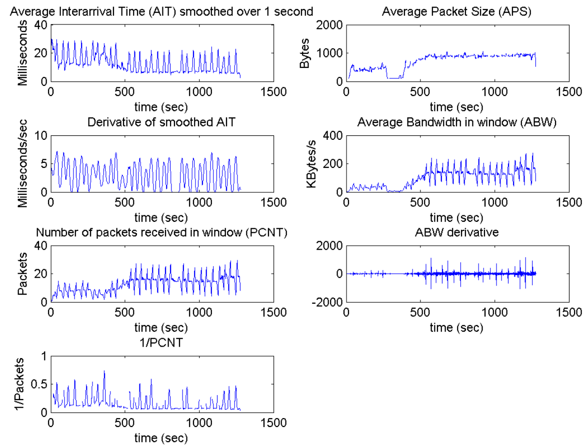
- We used Amazon Turk to recruit participants from around the country to call our lab

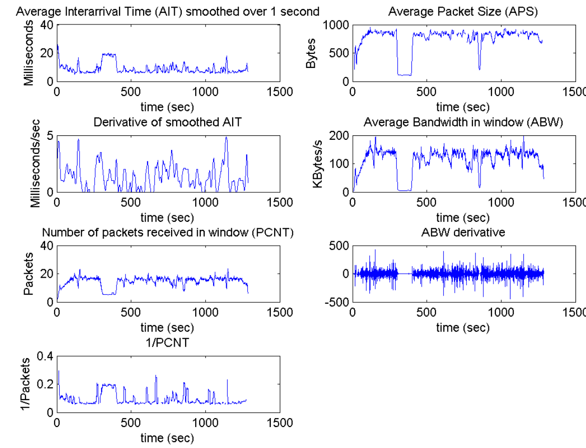


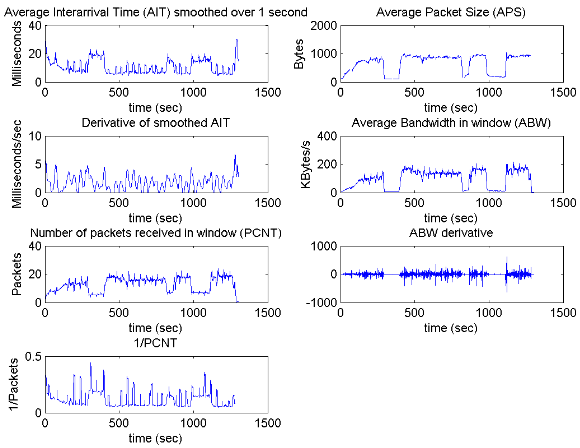
- Video calls were automatically answered and the video content and corresponding network traffic were recorded
- Participants followed a script which was transmitted to them on their screen to perform each action

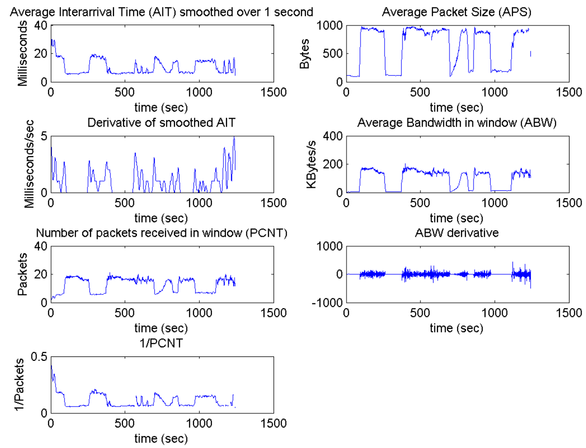
Skype Traffic Analysis (Diverse Sources)

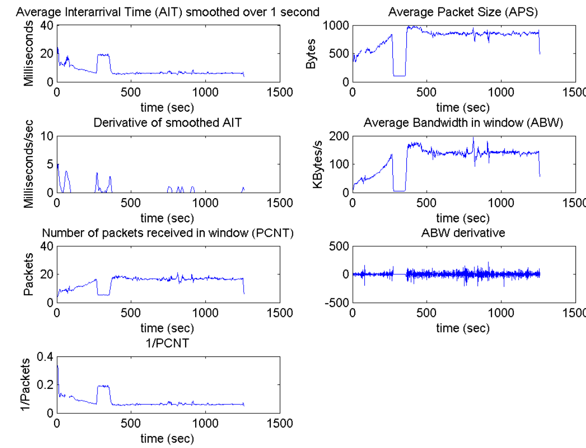












Georgia Institute of Technology

Communications Assurance & Performance Group

Conclusions

- It is possible to detect activity in a video stream by analyzing network packet metadata
  - Higher bandwidth transmissions showed activity more obviously
  - Better camera technology increases detectability
  - Better compression algorithms smooth out the inactivity and accentuate the changes
- Analysis would have worked poorly in the past, but it is starting to reveal data and could potentially become more revealing as technology advances

Questions