Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-Sensing

Babins Shrestha - University of Alabama at Birmingham, USA
Nitesh Saxena - University of Alabama at Birmingham, USA

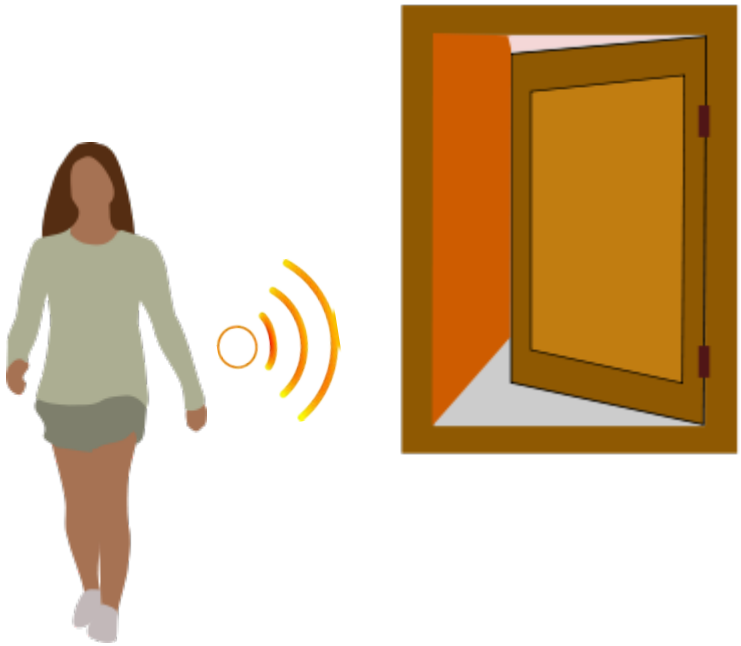
Hien Thi Thu Truong – University of Helsinki, Finland
N. Asokan - University of Helsinki/Aalto University, Finland,

Outline

- Relay Attacks in Authentication Systems
  - Example Scenarios
- Our Defense
- Experiment
- Results
- Discussion & Conclusion

Zero-Interaction Authentication (ZIA)

Zero-Interaction Authentication



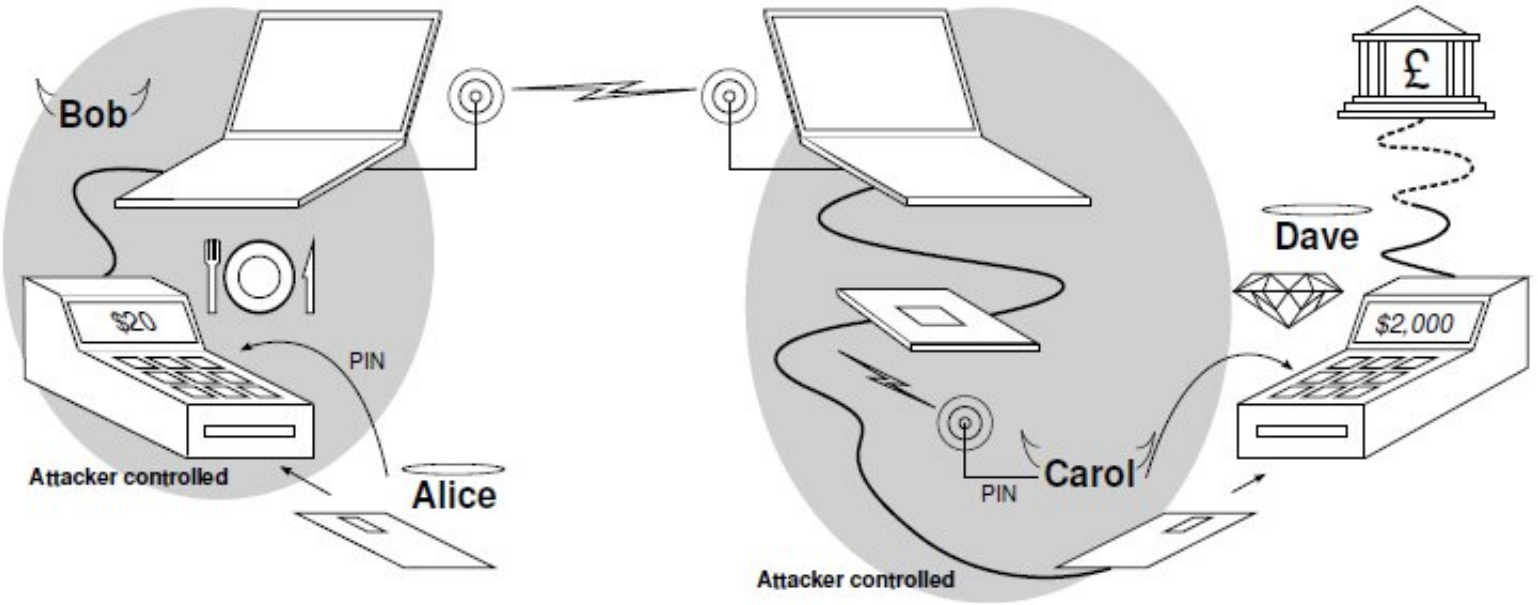
[BlueProximity project in SourceForge]

[Corner and Noble, MobiCom ‘02]

ZIA Ghost-and-Leech Relay Attack

[Kfir and Wool, SecureComm '05](#)
[Francillon et al, NDSS '11](#)

Reader and Ghost Attack (Payment Tokens)

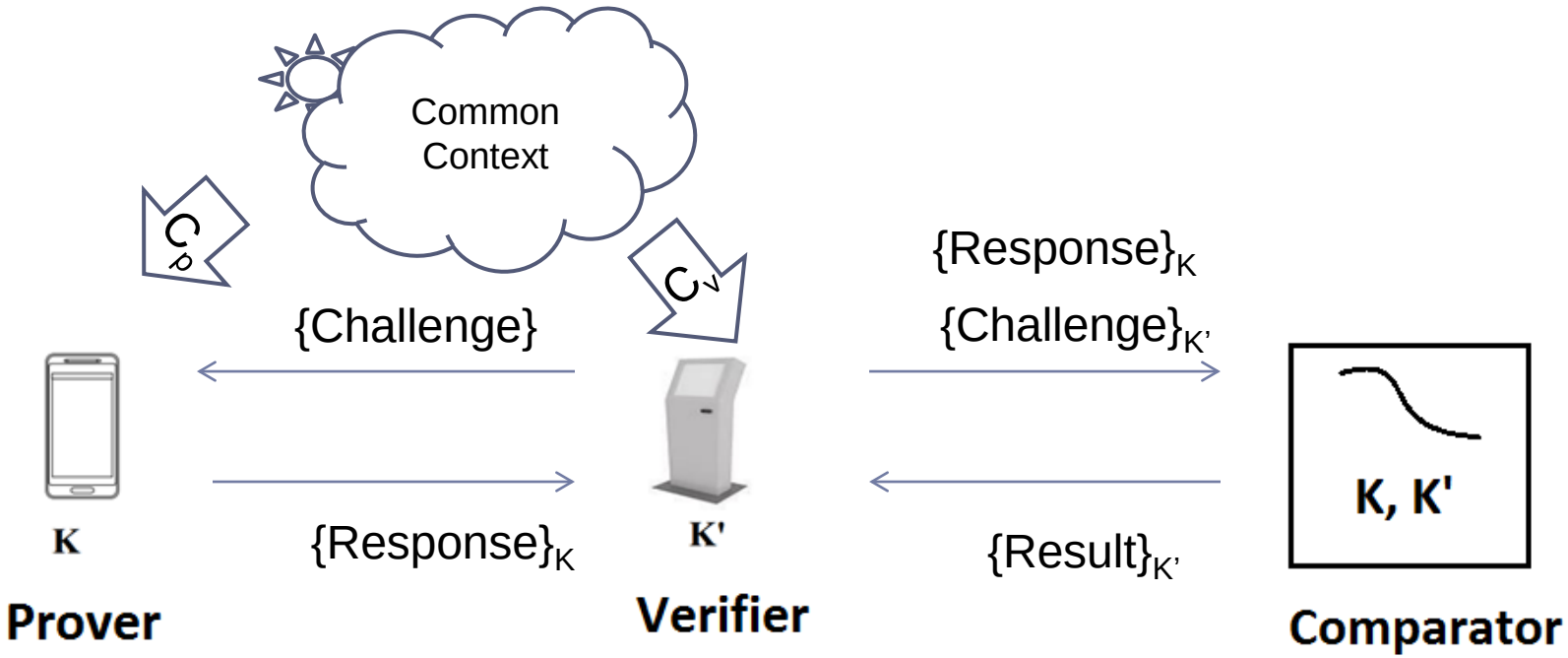


Drimer and Murdoch in USENIX Security Symposium '07

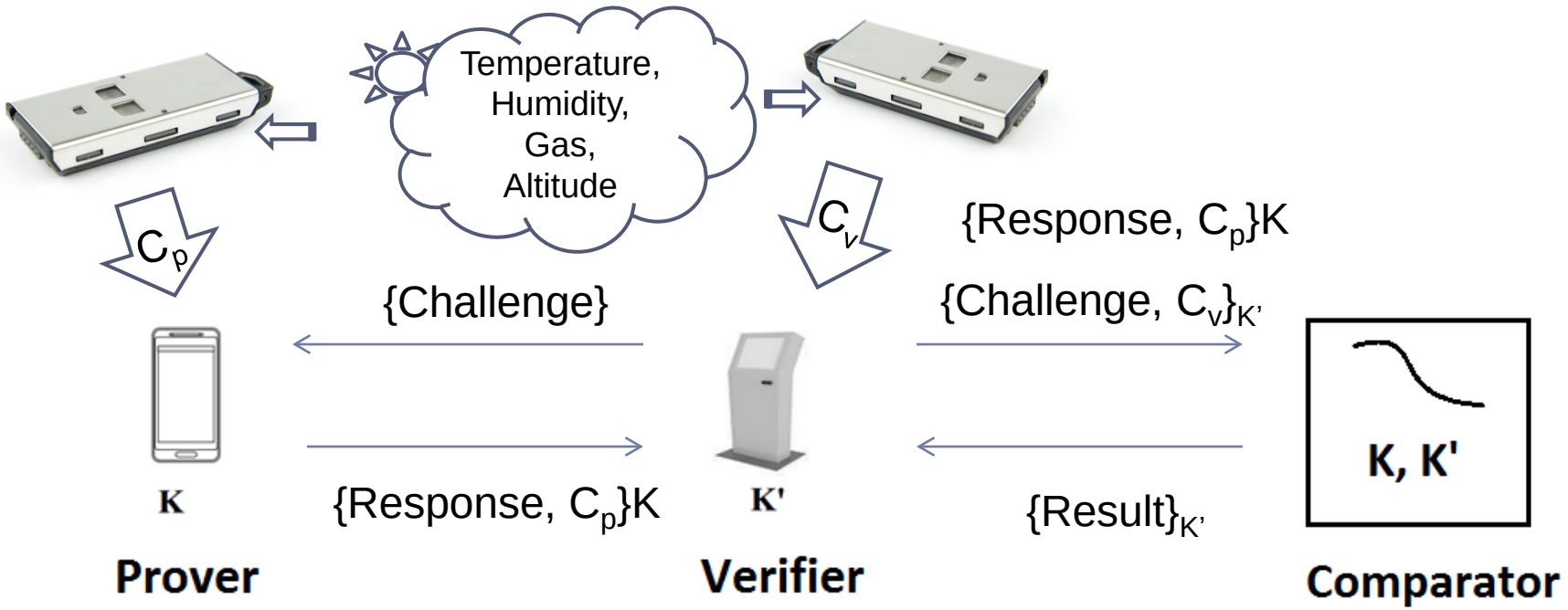
Defenses to Relay Attacks

- Distance Bounding
  - Protocol
  - Cons
- Contextual Co-presence

Contextual Co-presence



Our Work: Contextual Co-presence Using **Physical Ambient** Modalities

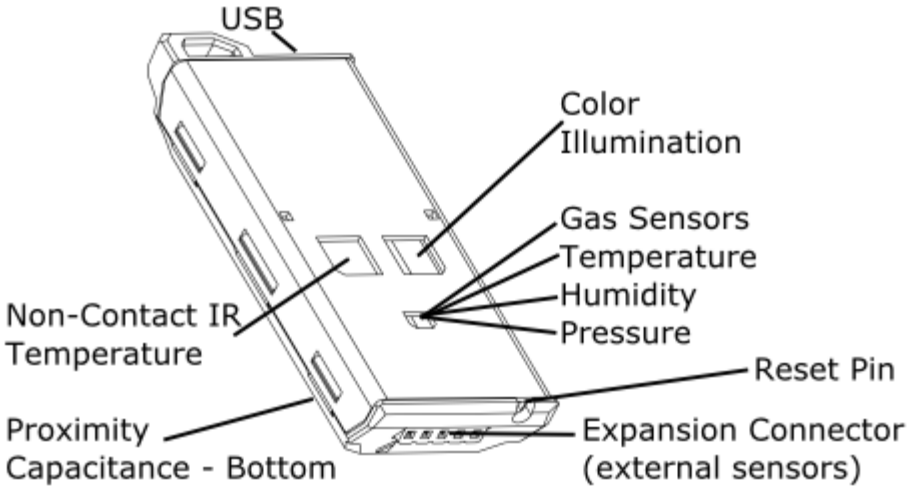


Our Contributions

- Physical Ambient Sensors for Relay Attack Prevention
  - Off-the-shelf purely environmental sensors
- Multiple Modality Combinations
- Experiments & Analysis
  - Simple data collection application, utilizing Sensordrone

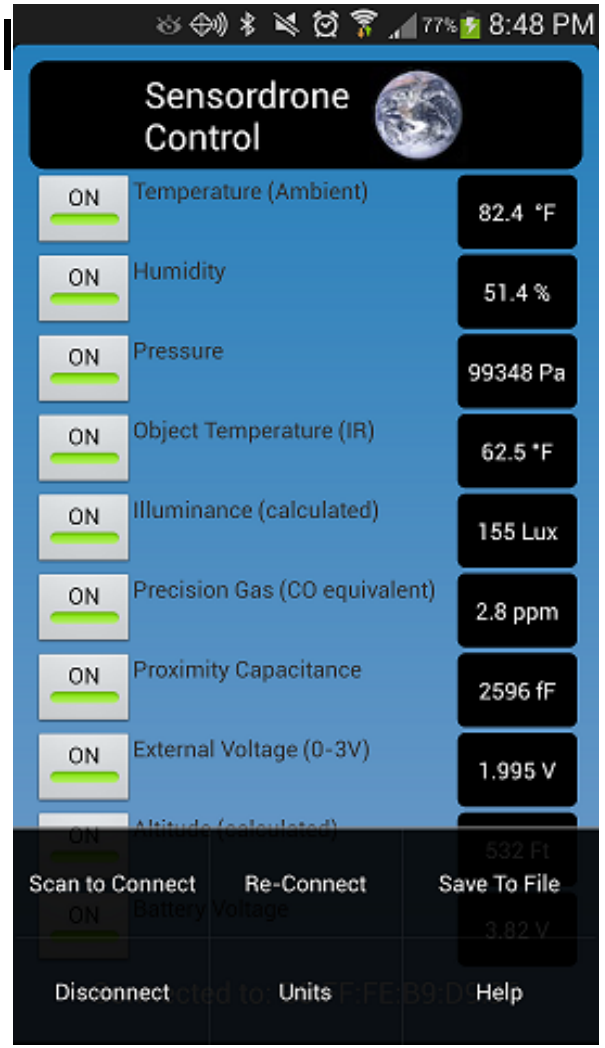
Sensor Modalities Used

- Ambient Temperature
- Humidity
- Gas (CO Level)
- Altitude and Pressure



Experiments

- Android App (Sensordrone Control)
- Devices Used
  - Two Android Phones
  - Two Sensordrones



Experiments & Analysis

- Data Collection
  - 207 samples at 21 different locations
  - Co-located samples paired to generate co-presence data
  - Samples from different places paired for non co-presence data
- Feature Calculation
  - Hamming Distance: Difference between samples of each modality at each place

Analysis

- Weka
  - Ten fold cross validation
  - Multiboost
  - Random Forest (Best Classifier)
- Classification Performance
  - False Positive Rate (FPR) => Security,
    False Negative Rate (FNR) => Usability
  - F-Measure

Results

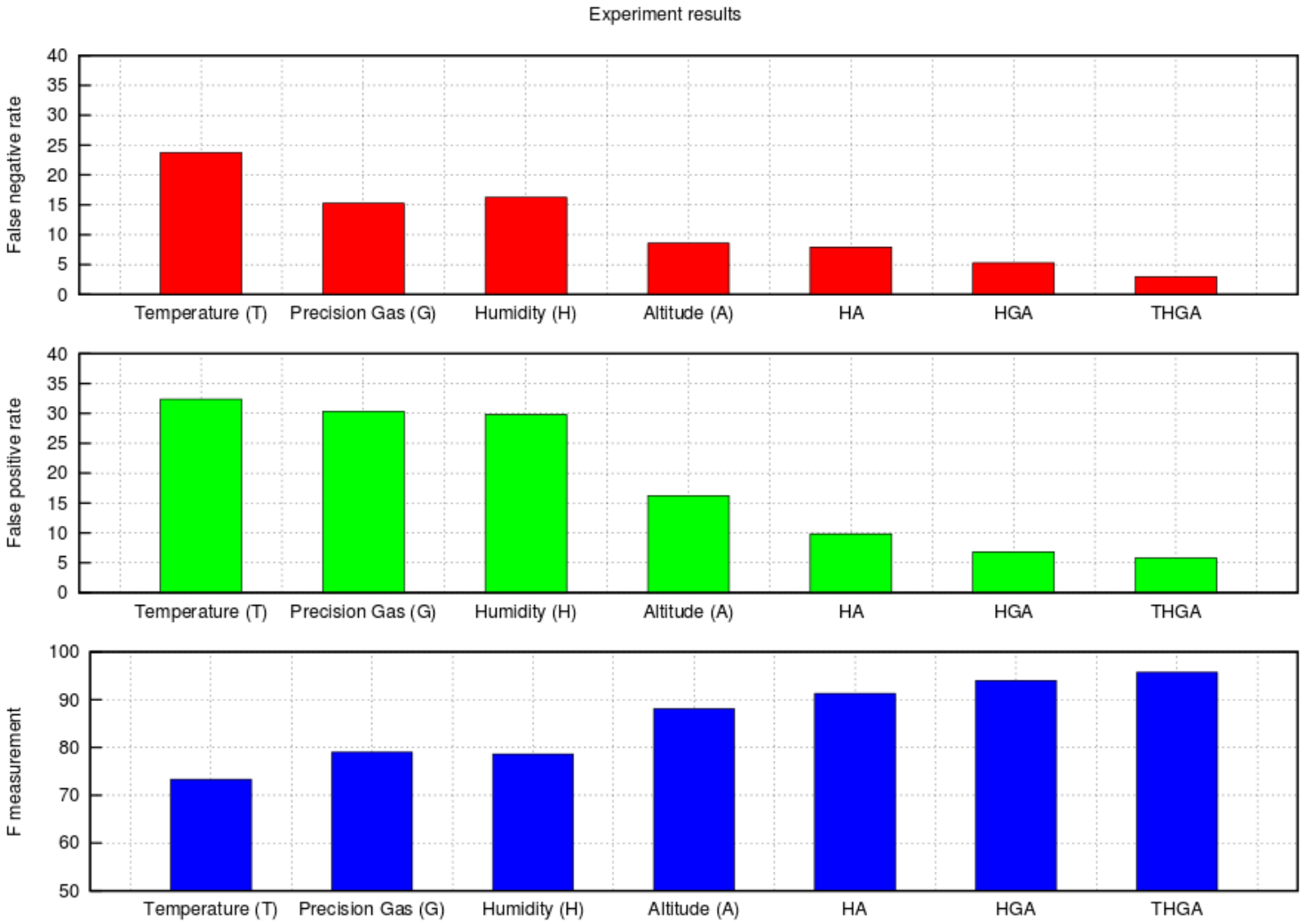
- Single Sensor Modality

Modalities	FNR	FPR	Precision	Recall	F-Measure
Temperature(T)	23.74%	32.40%	0.705	0.763	0.733
Gas(G)	15.26%	30.36%	0.739	0.847	0.790
Humidity(H)	16.25%	29.81%	0.740	0.838	0.786
Altitude(A)	8.57%	16.25%	0.851	0.914	0.881

- Combination of Multiple Sensor Modalities

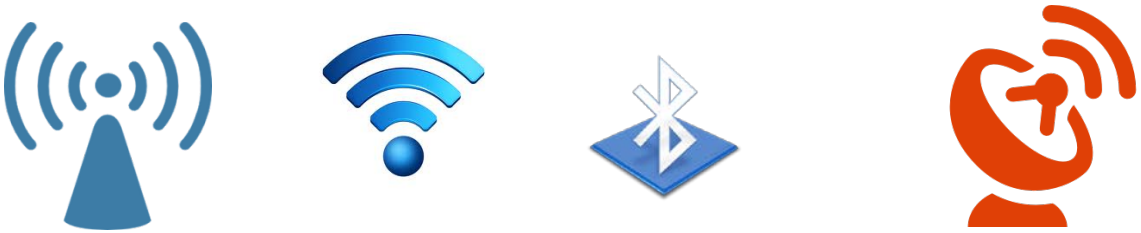
Modalities	FNR	FPR	Precision	Recall	F-Measure
HA	7.93%	9.85%	0.905	0.921	0.913
HGA	5.30%	6.83%	0.934	0.947	0.940
THGA	2.96%	5.81%	0.944	0.970	0.957

Results


Experiment results
False negative rate
40
35
30
25
20
15
10
5
0
Temperature (T)
Precision Gas (G)
Humidity (H)
Altitude (A)
HA
HGA
THGA
False positive rate
40
35
30
25
20
15
10
5
0
Temperature (T)
Precision Gas (G)
Humidity (H)
Altitude (A)
HA
HGA
THGA
F measurement
100
90
80
70
60
50
Temperature (T)
Precision Gas (G)
Humidity (H)
Altitude (A)
HA
HGA
THGA

Discussion

- How do Physical Ambient Modalities compare with other commonly available sensor modalities?
  - Temperature, Humidity, Gas, Pressure/Altitude
    vs
  - RF Sensors (WIFI, Bluetooth, GPS), Audio



Truong et al. in PerCom. 2014

Discussion

- Response Time
  - Typically faster than common sensors

Discussion

- Battery Power Consumption
  - Low power consumption compared to common sensors
  - Minimal influence on the power consumption

Discussion

- Adversarial Settings
  - Changing multiple physical ambient modalities simultaneously
    - will be harder
    - increases the likelihood of being noticed

Discussion

- Privacy
  - (Location) Privacy
  - Modalities keep on changing

Discussion

- Other Sensors?

Conclusion

Co-presence detection based on information collected from multiple different **physical ambient sensors**

- Approach for preventing relay attacks
- Improved security, efficiency & privacy

Thank You

- Any Questions?