Security-aware Virtual Machine Allocation in the Cloud: A Game Theoretic Approach

Presenter:

Charles Kamhoua, Ph.D.

Air Force Research Laboratory

Cyber Assurance Branch

Sept 1, 2015

Integrity ★ Service ★ Excellence

Collaborators:

Luke Kwiat (Univ. of Florida)

Kevin Kwiat (AFRL/RIGA)

Jian Tang (Syracuse Univ.)

Andrew Martin (Oxford Univ.)

Outline

- Public Cloud Computing
- Challenges
- Game Theory
- System Model
- Game Model
- Game Analysis
- Numerical Results
- Model Extension
- Conclusions
- Reference

Game Theory in the Cloud?

Source: http://www.free-pictures-photos.com

What is Cloud Computing?
NIST Five Essential Characteristics

- On-demand self-service
  - A consumer can provision computing capabilities as needed.
- Broad network access
  - Capabilities are available over the network.
- Resource pooling
  - The provider's computing resources are pooled to serve multiple consumers according to consumer demand.
- Rapid elasticity
  - Capabilities can be elastically provisioned and released to scale rapidly outward and inward commensurate with demand.
- Measured service
  - Resource usage can be monitored, controlled, and reported.

Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, 2011

Benefits and Risks of Cloud Computing

Benefits

- Faster deployment
- Infrastructure flexibility
- No up-front Investment
- Fine-grained billing (e.g. hourly)
- Pay-as-you-go
- Improved productivity

Risks

- Availability of services and data
- Complexity
- Performance
- Privacy
- Security
- Interdependency
- Negative externalities

Cause of Cyber Security Interdependency in a Public Cloud

- No perfect isolation of different user.
- Sharing of common resources.
- Some of the resources can be partitioned.
  - CPU cycles, memory capacity, and I/O bandwidth.
- Some of the resources cannot be well partitioned.
  - last-level cache (LLC), memory bandwidth, IO buffers and the hypervisor.
- The shared resources can be exploited by attackers to launch cross-side channel attack.

Cross-side Channel Attack

- A malicious user can analyze the cache to detect a co-resident VM's keystroke activities and map the internal cloud infrastructure and then launch a side-channel attack on a co-resident VM.

T. Ristenpart, E. Tromer, H. Shacham, S. Savage. "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," In the proceedings of the 16th ACM Conference on Computer and Communications Security, CCS'09, Chicago, IL, USA, October 2009.

- An attacker can initiate a covert channel of 4 bits per second, and confirm co-residency with a target VM instance in less than 10 seconds.

A. Bates, B. Mood, J. Pletcher, H. Pruse, M. Valafar, K. Butler "Detecting Co-Residency with Active Traffic Analysis Techniques," in the proceedings of the 2012 ACM Cloud Computing Security Workshop (CCSW) in conjunction with the 19th ACM Conference on Computer and Communications Security, October 2012, Raleigh, North Carolina, USA.

Our Approach

- **Favorable:** *Small* organizations find that the benefit of joining a public cloud outweigh the risk.
  - Quick adoption of public cloud by small organizations
- **Problems:** Cross-side channel attack, cyber security interdependency and negative externalities prevent *big* organizations from joining a public cloud.
- **Objective**: Use an allocation mechanism based on security to help big organizations decide to join a public cloud.
- **Approach**: Apply game theory and use Nash Equilibrium as the allocation method.

Apply Game Theory in Public Cloud Game

- *Game Theory* is the study of mathematical models of **conflict** and cooperation between **intelligent rational** decision-makers (by Myerson).

- The attackers and the public cloud users are **intelligent** and **rational**.

- Rational attackers and cloud users interact in a way that can be predicted and modeled

- Allows for allocation of Virtual Machines for ideal security.

Game Theory Optimum Decision loop

Identify all the players,
their strategies,
And payoffs.

Information:
Does each player know about others' strategies and payoffs?

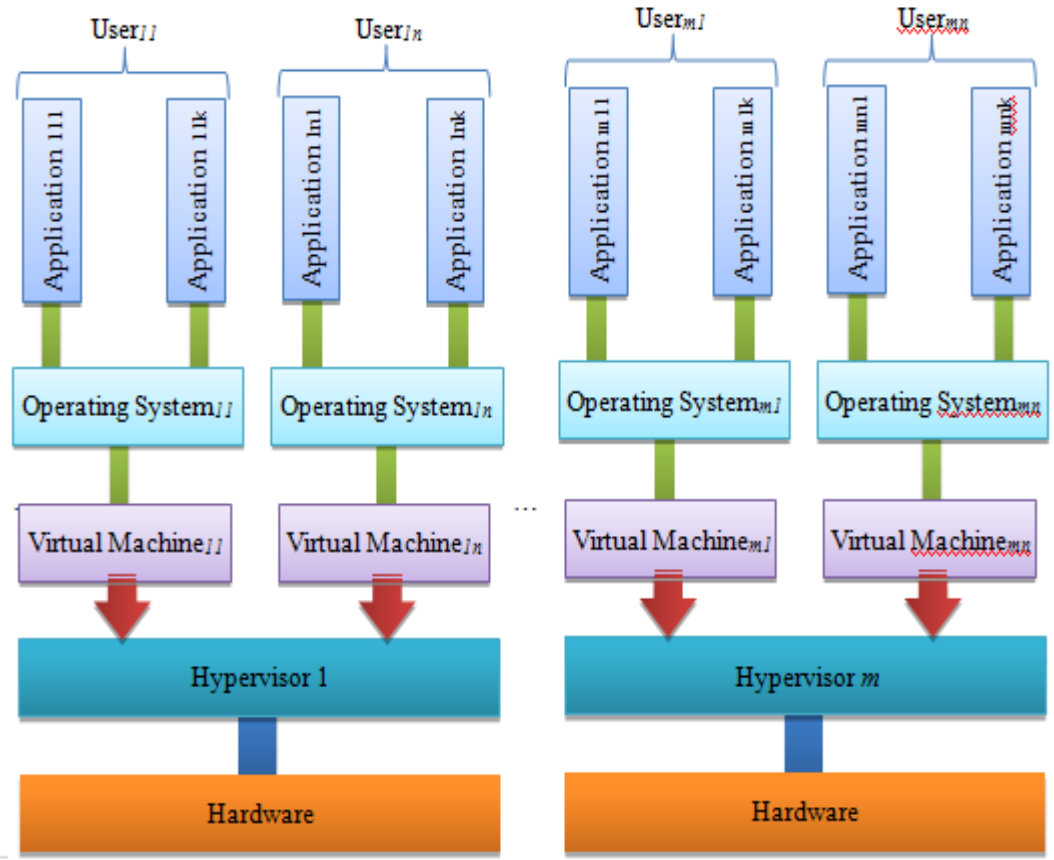
Nash Equilibrium:
Play your best response to other players' strategies

Monitoring:
Observe other action,
Update your belief

The Nash Equilibrium

- Every game has at least one Nash Equilibrium (NE) in either pure or mixed strategies.
- A strategy profile is a NE if no player can unilaterally change its strategy and increase his payoff.
  - Each player is playing its best response to other player's strategies
- The NE of a security game can be used to:
  - Predict attacker strategy
  - Allocate cyber security resources
  - Protect against worse-case scenario
  - Develop cyber defense algorithms
  - Form the basis for formal decision making

System Model



- Two hypervisors: One with higher security than the other, but more costly to use.
- For each *n* users, the best strategy (Invest or Not invest) depend on other users' actions.
- A compromised hypervisor make all users vulnerable on that hypervisor.
- Model extendable to *m* hypervisors

Game Model

Game Model in Normal Form

		User 2	
Attacker		N	I
	A_1	$q_N L_1 + q_N \pi L_2$ $R - q_N \pi L_2$	$q_N L_1$ $R - e$
	A_2	$q_N L_2 + q_N \pi L_1$ $R - q_N L_2$	$q_I L_2 + q_I \pi L_3$ $R - e - q_I L_2$
	A_3	$q_I L_3$ R	$q_I L_3 + q_I \pi L_2$ $R - e - q_I \pi L_2$

Symbol	Notation
q_I	Probability of a successful attack on a user given that he has invested in security
q_N	Probability of a successful attack on a user given that he has not invested in security
π	Probability that the hypervisor is compromised given a successful attack on a user
R	User reward from using the cloud computing services
e	Total expense required to invest in security
L_i	User i's expected loss from a security breach
I	User's strategy "Invest"
N	User's strategy "Not invest"
A_i	Attacker's strategy "launch an attack on User i"
U_i	User i
H_i	Hypervisor i

Game Analysis

Theorem 1: If $L_3 > \frac{q_N}{q_I}(L_2 + \pi L_1)$, then the strategy profile (A_3, N) is Nash equilibrium of the game in Table 1.

Theorem 2: If $L_3 < \frac{q_N}{q_I}(L_2 + \pi L_1)$ and $e > (q_N - q_I)L_2$, then the strategy profile (A_2, N) is a Nash equilibrium.

Theorem 3: If $L_1 > \frac{q_I}{q_N}(L_3 + \pi L_2)$ and $e < q_N \pi L_2$, then the strategy profile (A_1, I) is a Nash equilibrium.

Theorem 4: If $L_3 < \frac{q_N}{q_I}(L_2 + \pi L_1)$, $e < (q_N - q_I)L_2$, and $L_1 < \frac{q_I}{q_N}(L_3 + \pi L_2)$ hold, then the game admits a mixed strategy Nash equilibrium. U_2 mixes at

$$P(H_1) = \frac{q_I[(L_3+\pi L_2)-(L_2+\pi L_3)]}{q_N(L_2+\pi L_1)-q_I(L_2+\pi L_3)+q_I\pi L_2} \text{ and } P(H_2) = \frac{(e+q_I\pi L_2)}{q_N L_2 - q_I L_2(1-\pi)}$$

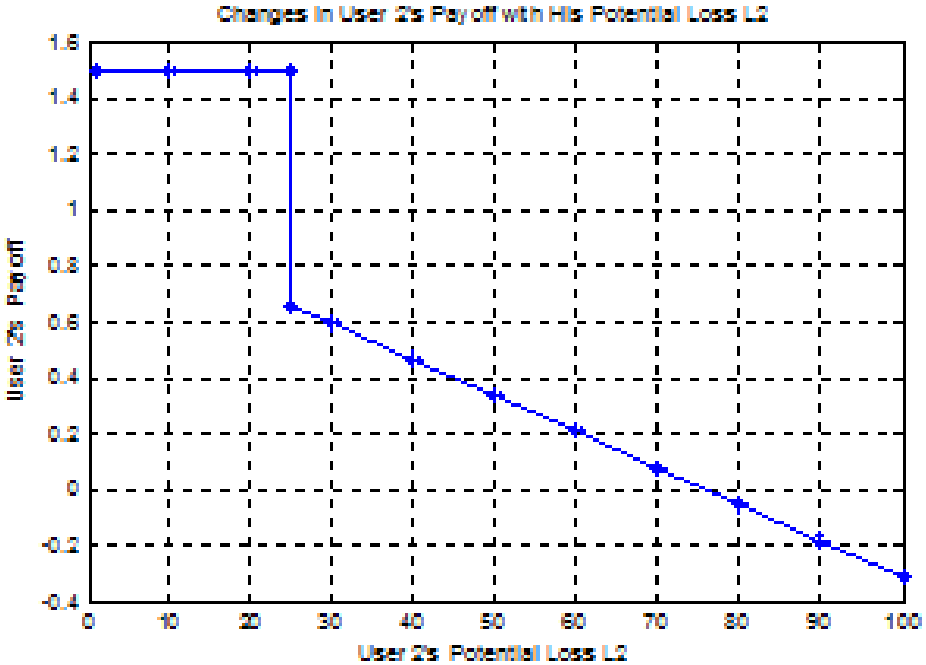
U_1 and U_n will always allocate to H_1 and H_2 if $L_1(q_N - q_I\pi) < e < L_n(q_N - q_I)$

Numerical Results

Parameters: $R = 1.5,\ q_I = .1,\ q_N = .4,$

$\pi = .1,\ L_1 = 1,\ L_3 = 100, e = .4$

Then: $.39 < e < 30$

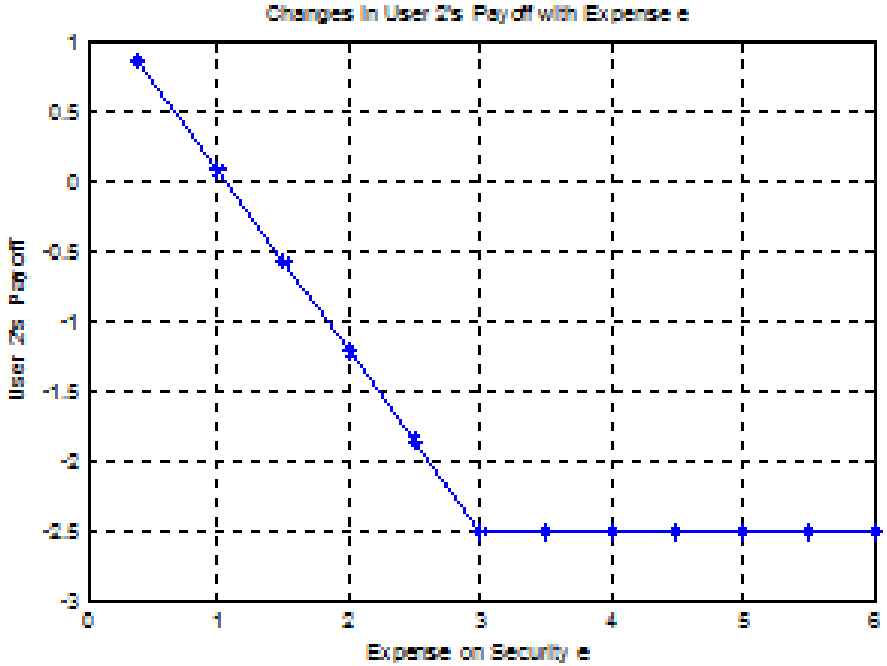


Changes in User 2's Payoff with his Potential Loss L_2.

Parameters: $R = 1.5,\ q_I = .1,\ q_N = .4,$

$\pi = .1,\ L_1 = 1,\ L_2 = 10,\ L_3 = 20$

Then: $.39 < e < 6$



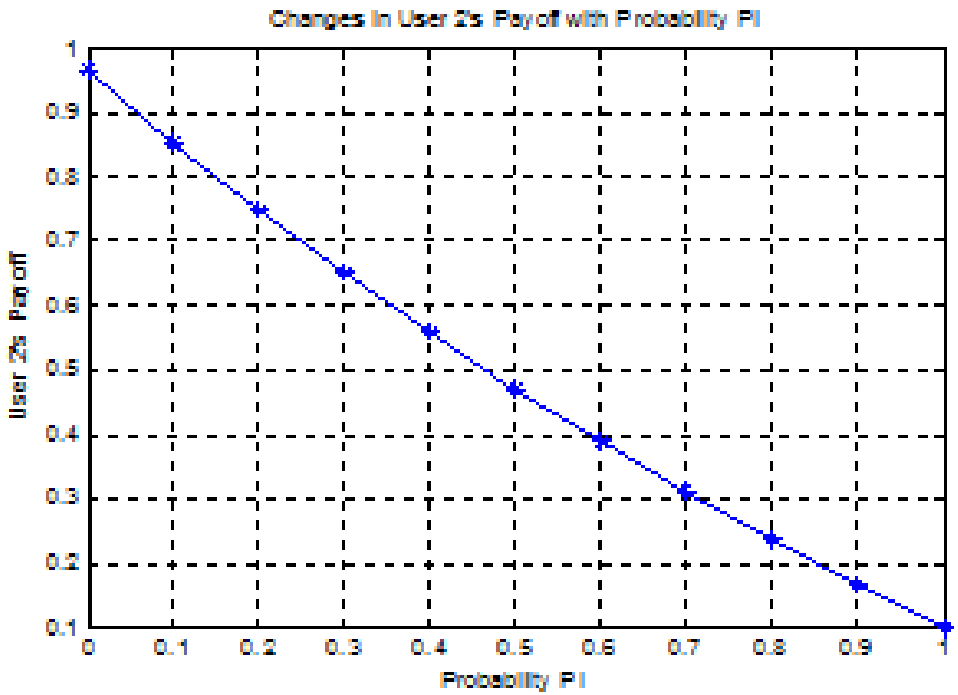
Changes in User 2's Payoff with Expense e.

Numerical Results

Parameters: $R = 1.5,\ q_I = .1,\ q_N = .5,$

$L_1 = 1,\ L_2 = 10,\ L_3 = 20, e = .4$

For $0 < \pi < 1$ there is no strategy change!



Changes in User 2's Payoff with Probability π.

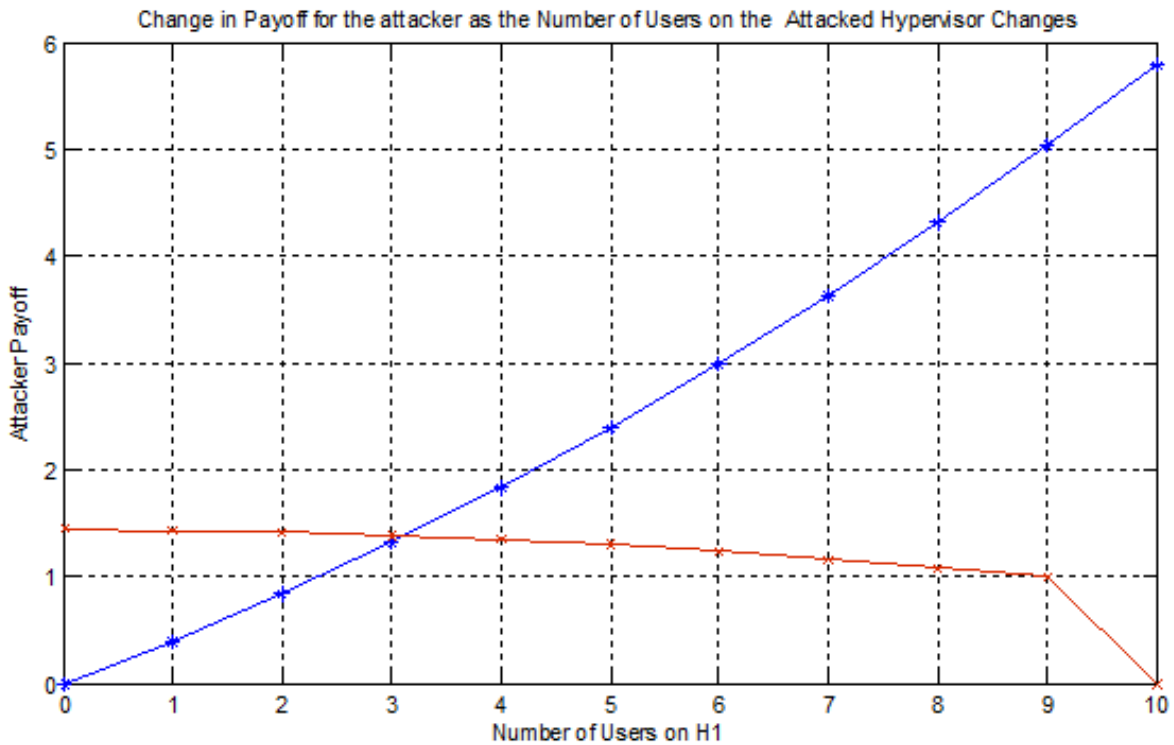
Model Extension

- A For N ≥ 3, There will only be one discrete user in which they alone will make a decision as to which hypervisor they allocate
  - i.e., all other users will remain static in their allocation choice regardless of the number of players.
- The one user will sit on the threshold of choosing between investing in security and not investing in security because all other users' expected loss magnitudes balance out.
- Find user that causes attacker to flip preferences.

Model Extension Numerical Results

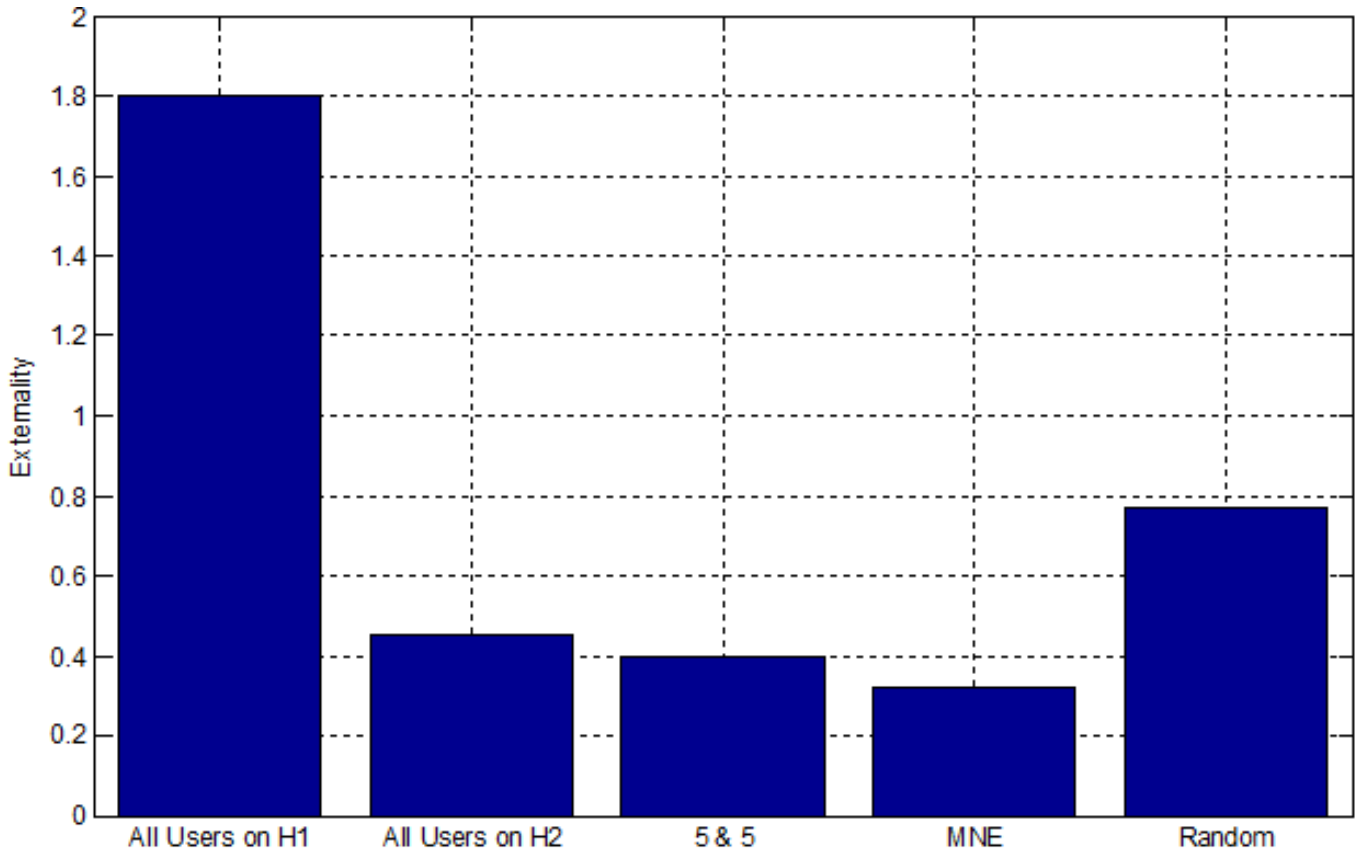
Parameters: $R = 1.5,\ q_N = .4,\ q_I = .1,\ \pi = .1,\ e = .4,\ L_1 = 1,\ L_2 = 2,\ L_3 = 3,\ L_4 = 4,$
$L_5 = 5,\ L_6 = 6,\ L_7 = 7, L_8 = 8, L_9 = 9, L_{10} = 10$

For these given parameters, User 4 causes the attacker to change preferences



Change in attacker's Payoff with the Number of Users on the attacked hypervisor.

Externality Reduction



Externality from Selected Allocation Types

Conclusions

- Previous research shows that each user's decision to *Invest* or *Not Invest* depends on the potential loss from the neighbors after a security breach.
- VMs that have similar potential loss from a security breach should be on the same physical machine.
- The allocation method based on Nash Equilibrium was shown to reduce externalities compared to other allocation methods.
- The expense factor *e* can be set by cloud provider to achieve desirable VM allocation preferences.

Reference

Luke Kwiat, Charles A. Kamhoua, Kevin Kwiat, Jian Tang, Andrew Martin “Security-aware Virtual Machine Allocation in the Cloud: A Game Theoretic Approach” in proceedings of the IEEE International Conference on Cloud Computing, (IEEE CLOUD 2015), New York, June 2015.

Q & A

Thank You!