Securing Your Data for the Journey to the Clouds

LIWEI REN, PH.D, Trend Micro™

April, 2015, SNIA DSI 2015, Santa Clara, California
Background

• Liwei Ren
  – Research interests
    • DLP, cloud data security, big data & security, math modeling & algorithms.
  – Major works
    • 10+ academic papers;
    • 20+ US patents granted, and a few more pending;
    • Co-founded a data security company in Silicon Valley with successful exit.
  – Education
    • MS/BS in mathematics, Tsinghua University, Beijing
    • Ph.D in mathematics, MS in information science, University of Pittsburgh

• Trend Micro™
  – Global security software company with headquarter in Tokyo, and R&D centers in Silicon Valley, Nanjing and Taipei;
  – One of top security software vendors.
Agenda

• A Glance at Data Security
• Three Data Security Problems in the Cloud
• A Few Technologies
• CASB: an Integrated Solution
• Can We Do Better in the Future?
• Summary
A Glance at Data Security

• Should we take a look at data security in general before flying to the cloud?

• Let me list a few areas of data security that I have some knowledge:
Data Security Problems in the Cloud

• **Data security problems caused by cloud platforms:**
  1. Data residence in cloud when using cloud SaaS or cloud app
  2. Data leaks to personal cloud apps directly from enterprise networks
  3. Data leaks to personal cloud apps indirectly via BYOD devices

• **Data classification:**
  – Data states:
    • Data at rest
    • Data in use
    • Data in motion
  – Data types:
    • Structured data
    • Unstructured data
Data Security Problems in the Cloud

• Data residence in cloud when using cloud apps:
  – Data privacy
  – Data breach
Data Security Problems in the Cloud

- Data leaks to cloud apps directly:
  1. Employees may use cloud storage applications Dropbox, Evernote as personal users.
  2. Employees may use cloud storage box.com as enterprise users.
  3. They may use personal emails that could attach confidential files.
  4. One has cloud-based business email such as Office 365 Email.
Data Security Problems in the Cloud

- Data leaks to the cloud via file sync apps:
  - Mobile device
  - BYOD
A Few Technologies

• A few technologies for solving each problem:
  – Traditional DLP: problem 2
  – Cloud Encryption Gateway: problem 1
    • Aka, SaaS Encryption Gateway
  – Cloud DLP: problem 1 & 2
    • With other security capabilities.
    • This is an overall and integrated solution for cloud data security.
A Few Technologies

• **DLP = Data Leak Prevention** (aka, Data Loss Prevention)

• Data at rest, data in motion, and data in use.

• **DLP solution architecture:**

![DLP solution architecture diagram]

- **Storage**
  - DATA at-rest at SOURCE
- **DLP DATA DISCOVERY APPLIANCE**
- **DLP MANAGEMENT CONSOLE**
- **DLP GATEWAY**
- **Firewall**
- **LAN**
- **DATA in motion**
- **Endpoint**
  - DLP AGENT
  - DATA in-use at SOURCE
DLP

- **DLP Model for endpoints**
  - Data in use or data in motion
**DLP**

- **DLP Model for network**
  - Data in motion in network

- **DLP Model for concept:**
DLP

- **DLP Security Rules** based on DLP Models:
  - DATA leaks from SOURCE to DESTINATION via CHANNEL, system takes ACTIONS
    - **DATA**: confidential data categories such as IP, PII, PCI, HIPAA, ...
    - **SOURCE**: user name, computer name, IP address
    - **CHANNEL**: USB, FTP, email, IM, HTTP/HTTPS, protocol of cloud app
      (Web mail, Dropbox, LinkedIn, Facebook, ...)
    - **DESTINATION**: cloud app, email recipients, unknown IP, USB
    - **ACTION**: log, block, alert, notification, encryption, quarantine, ...
DLP for Cloud Data Security

• Question: can we extend DLP for supporting data leak to the cloud specifically?
  – The answer is YES.

• Current DLP products & technologies provide solution to Cloud Security Problem 2 with DLP rules defined as:

  • DATA leaks from SOURCE to DESTINATION via CHANNEL, system takes ACTIONs

    • DATA: confidential data categories such as IP, PII, PCI, HIPAA,...
    • SOURCE: user name, computer name, IP address
    • CHANNEL: cloud App Protocols (such as Dropbox, web mail, Facebook, Linkedin)
    • DESTINATION: cloud apps
    • ACTION: log, encryption, block, ...
DLP for Cloud Data Security

• **Conclusion:**
  – Problem 2 can be solved by a DLP product

• **How to solve problem 1?**
Cloud Encryption Gateway

• An effective solution to Cloud Security Problem 1 should satisfy following properties;
  – The confidential information residing at cloud should only be accessed by data owners.
  – Data owners can apply data operations to the data defined by users’ functional roles.
  – When applying encryption to structured data, *data formats are preserved*.

• An ideal solution is Fully Homomorphic Encryption (FHE)
  – However, this solution is not available any time soon due to performance issue.
  – It may be available in next decades with further breakthroughs.
  – Another ideal solution is MPC (multi-party computing) ... however, not practical yet for the same reason.
Cloud Encryption Gateway

• An alternative to FHE is *Format Preserving Encryption + Tokenization* for the structured data on SaaS apps
  – Cloud Encryption Gateway or SaaS Encryption Gateway
Cloud Encryption Gateway

- **Conclusion:**
  - Problem 1 can be solved by a Cloud Encryption Gateway

- **Can we solve problem 1 & 2 together?**
Cloud DLP Gateway

- Cloud DLP Gateway:
  - DLP + Cloud Encryption Gateway.
  - It solves cloud data security problem 1 & 2 all together.
Cloud DLP Gateway

• How about problem 3?
• Can we do more with Cloud DLP Gateway?
  – Yes, let me propose this ... I am sure industry will have an implementation soon 😊.
CASB: an Integrated Solution

- Cloud Access Security Broker (aka, CASB) is a new product category defined by Gartner.
- It goes beyond data security to include more cloud security functions:
  - Anti-malware + Cloud IAM + Cloud DLP + ...
  - It is a platform for cloud data security
CASB: an Integrated Solution

- **My View:** there has been an evolution in the past few years:
Can We Do Better in the Future?

- When **FHE** advances to become practical, we have better solution for problem 1.
Summary

• Describing Three Problems of Cloud Data Security
• An Evolution of Technologies in the Past:
Q&A

• Thank you!

• Please ask questions .... so I know you were enjoying this talk😊