Cloud-based Security Service

Souhwan Jung
souhwanj@ssu.ac.kr
Outline

I. Cloud computing

II. Cloud Security

III. Security as a Service

IV. Direction for SecaaS

V. Conclusions
Paradigm Shift of Computing

Mainframe Computing
- Sharing of Computing resources

Distributed Computing
- Distribution and networking for computing capability

Cloud Computing
- Virtualization

- Mainframe computing
- Client-Server computing
- Cloud computing
Cloud Computing

- Key technology is virtualization
  - Computing virtualization
  - Network virtualization
  - Storage virtualization

- Virtualization is
  - Logical machine – VM on Hypervisor
  - Logical separation – no physical borderline for a company
  - Logical domain – virtual LAN, virtual storage etc…
Why cloud computing spreads fast?

- Economic reason – cost efficiency
- Smart devices – phone, car, TV etc…
- Big Data
- Productivity for distributed collaboration
- Security control at the uniform level
Types of cloud computing

- Private cloud
  - Many institute build their own clouds

- Public cloud
  - e.g. AWS, Force.com

- Hybrid cloud
  - a hybrid form of private (or legacy) and public cloud
Security appliances

- Many security appliances
  - Firewall
  - IPS/IDS
  - Web Firewall
  - AntiVirus software
  - Anti-DDoS system
  - Privacy software
  - DB encryption
  - Authentication server
  - Etc...
Secure enough?

- The answer is NOT yet.
  - Still many unknown vulnerabilities
  - Heterogeneous security solutions
  - Complicate security management
  - Too many sites to monitor
  - Hard to maintain security at the uniform level
Need to change Security Paradigm

- Appliance-based Security Solution → Cloud-based Security Service

**End points**
- Web security & filter
- Email security
- Message security
- Anti-virus

**Networks**
- VPN / SSL
- Firewall / Web firewall
- IPS / IDS, DDoS

**Security as a Service**

- Advantages
  - Centralized security controls
  - Provide stable and specialized security service
Cloud Security

- Security platform for cloud computing itself
  - Security platform and cloud platform are tightly coupled
  - Correspondence in each layer from kernel to user
  - Restriction to supporting various requirements from clients

- Security as a Service
  - Provide a reconfigurable security service for clients
  - Centralized security control
  - Maintaining a unified security level
  - Easy security patch at the cloud
SecaaS: Security as a Service

- SecaaS is a kind of SaaS
  - Software security service based on cloud computing

- Motivation
Architecture of SecaaS

- Cloud SecaaS
  - Security service for protecting its clients

- Standalone SecaaS
  - Security service for end-point

Cloud Clients

CSP (IaaS, PaaS, SaaS)
CSA (Cloud Security Alliance)

- **CSA**
  - Initiated at ISSA CISO Forum in Nov. 2008 / Published in Dec. 2008
  - The organization to provide security in cloud computing
  - Nonprofit organization for educating cloud computing security

- **Top Threats to Cloud Computing**

  - Threat #1: Abuse and Nefarious Use of Cloud Computing
  - Threat #2: Insecure Interfaces and APIs
  - Threat #3: Malicious Insiders
  - Threat #4: Shared Technology Issue
  - Threat #5: Data Loss or Leakage
  - Threat #6: Account or Service Hijacking
  - Threat #7: Unknown Risk Profile

Source: Personal Cloud Security Framework (TTA)
SecaaS WG defined 10 categories

1. Identity and Access Management (IAM)
2. Data Loss Prevention (DLP)
3. Web Security
4. Email Security
5. Security Assessments
6. Intrusion Management (IM)
7. Security Information and Event Management (SIEM)
8. Encryption
9. Business Continuity and Disaster Recovery (BCDR)
10. Network Security
IAM Service

- **Identity and Access Management (IAM) SecaaS**
  - Provide controls for assured identities and access management
  - Service: user-centric ID provider, Federated IDs, Policy provider, authorization management, Electronic signature etc…

---

**Unauthorized access**

- Fraud

**Delegation of authorizations / entitlements**

- Non-repudiation

**Privilege escalation**

- Insider threat

**Excess privileges / excessive access**

- Identity theft

---

### Security Intelligence
- Monitoring, reporting, identity context

### Policy-based Identity and Access Governance
- Business context, risk profile

### Access Management
- Web SSO, Federated SSO
  - Authorization
  - Risk-based Authentication
  - Role-based Access Controls

### Identity Management
- User profile & entitlement management
- Provisioning and deprovisioning
- Privileged identity management
- Federated Provisioning

### Standard Services (Directory, Federation)
- Database (DB)
- Application
- Desktop
- Mainframe
- Cloud computing
- Mobile
Data Loss Prevention (DLP) Service

- DLP SecaaS
  - Monitoring, protecting, and verifying the security of data in-use (endpoint action), in-motion (network traffic), at-rest (data storage)
  - Service: meta-data tagging, data-leakage detection, transparent data encryption, dynamic data masking, policy controlled data access, multilingual fingerprinting etc…

- Unauthorized access
  - Security Intelligence
    - Real-time user awareness, automated incident response, monitoring, reporting

- Data loss / leakage
  - Policy-based Access Control
    - Predefined policies, Machine readable policy language

- Data sovereignty issues
  - Protection
    - Signing of Data
    - Data labeling and Classification
    - Identification of sensitive data
    - Cryptographic data protection
  - Detection
    - Traffic Spanning detection
    - SQL regular expression detection
    - Context Detection Heuristics
    - Structured Data Matching

Storage | Endpoint | Network
- DB
- Desktop
- Mobile
- Network

Unauthorized access
- Regulatory sanctions and fines

Data loss / leakage
- Malicious compromises of data integrity

Unauthorized access and Data loss / leakage:
- DB

Unauthorized access and Data loss / leakage:
- Desktop

Unauthorized access and Data loss / leakage:
- Mobile

Unauthorized access and Data loss / leakage:
- Network

Unauthorized access and Data loss / leakage:
- souhwanj@ssu.ac.kr
Web Security Service

- **Web security SecaaS**
  - Proxying and redirecting web traffic to the cloud provider
  - Added layer of protection for entering the enterprise via web browsing
  - Service: web filtering, web monitoring, anti-phishing, email server, anti-spam etc…

    - **Domain Content**
      - Security Intelligence
        - monitoring, reporting

    - **Bot Network**
      - Policy-based Access Control
        - Web Access Control

    - **Bandwidth consumption**
      - Engine
        - Phishing site blocker
        - Malware, Spyware & Bot Network analyzer and blocking
        - Email security
        - Data Loss Prevention
        - Backup

    - **Data Loss / Leakage**
      - Content
        - Fraud Prevention
        - Spam
        - Virus
        - Malware & Spyware
        - Phishing
        - Keyloggers

    - **Network**
      - SSL, Bandwidth management / traffic control
      - Web filtering
      - Instant messaging scanning

souhwanj@ssu.ac.kr
E-mail Security Service

- **Email Security SecaaS**
  - Provide control over inbound and outbound email
  - Policy-based encryption of emails, digital signatures
  - Service: content security, anti-virus/anti-malware, spam filtering, email encryption etc…

  - **Security Intelligence**
    - real-time reporting
  - **Policy-based Access Control**
    - Flexible policies to define granular mail flow and encryption
  - **Email Security Service**
    - Deep protection against viruses and spyware
    - Accurate filtering to block spam and phishing
    - Option to encrypt some/all emails
    - Integration with various email server solution

- **Malware**
- **Spam**
- **Phishing**

Addresses spoofing

Intrusion

souhwanj@ssu.ac.kr
Security Assessment Service

- **Security Assessment SecaaS**
  - Third-party audits of cloud services or assessments of on-premises systems
  - Compliance control for IaaS, PaaS, and SaaS platforms
  - Service: internal/external penetration test, application penetration test, host and guest assessments, virtual infrastructure assessment etc…

---

Virtual infrastructure assessments

- Network / security system compliance assessments
- Server / workstation Compliance assessments
- Application penetration test

Network & system vulnerability assessments

- Internal and/or External Penetration test
- Web application security assessments

---

Computing resources

- DB
- Application
- Desktop
- Mainframe
- Cloud computing
- Network

---

Lack of continuous monitoring

- Insecure architecture
- Inaccurate inventory

Lack of complete auditing

- Lack of correlation information
- Insecure processes / processes not being followed

Lack of correlation information

- Failure to meet/prove adherence to Regulatory / Standards Compliance

Insecure / vulnerable configuration

- Compliance
- Technical Compliance Audits
- Application Security Assessments
- Risk Management

- Governance
- Penetration Testing
- Vulnerability Assessment
- Security / risk rating
Intrusion Management Service

- **Intrusion Management (IM) SecaaS**
  - Using pattern recognition to detect and react to statistically unusual events
  - Reconfiguring system components in real time to stop an intrusion
  - Service: packet inspection, detection, prevention event correlation and pattern recognition, DPI etc…

<table>
<thead>
<tr>
<th>Security Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring, reporting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy-based Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update policies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Detection &amp; Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates to address new vulnerabilities, exploits</td>
</tr>
<tr>
<td>Automatic or manual remediation action</td>
</tr>
<tr>
<td>Identification and policy violations</td>
</tr>
<tr>
<td>Workloads, virtualization Layer, Management Plane, Cloud and other APIs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computing resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB</td>
</tr>
<tr>
<td>Application</td>
</tr>
<tr>
<td>Desktop</td>
</tr>
<tr>
<td>Mainframe</td>
</tr>
<tr>
<td>Cloud computing</td>
</tr>
<tr>
<td>Network</td>
</tr>
</tbody>
</table>

souhwanj@ssu.ac.kr
SIEM Service

- **Security Information and Event Management (SIEM) SecaaS**
  - Accept log, event and flow information from a diverse set of devices
  - Conduct information security analysis, correlation
  - Real-time reporting and alerting on incidents/events
  - Service: log management, event correlation, security/incident response, log and event storage, interactive searching and parsing of log data etc…

- **Abuse and Nefarious Use**
- **Data Loss / Leakage**
- **Shared Technology Issues**
- **Insecure interfaces and APIs**
- **Malicious Insider**
- **Unknown Risk Profile**
- **Accounts or Service Hijacking**
- **Fraud**

souhwanj@ssu.ac.kr
Encryption Service

- **Encryption SecaaS**
  - One of the most effective data protection controls
  - Critical customer and enterprise data could be held by third-party cloud providers in multi-tenant shared computing and storage environments
  - Service: VPN service, Key management, virtual storage encryption etc…

- Mitigating insider and external threats to data
- Intercepted clear text network traffic
- Failure to meet Regulatory Compliance requirements

<table>
<thead>
<tr>
<th>Security Intelligence</th>
<th>Key Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring, reporting</td>
<td>Key / certificate generation and management</td>
</tr>
</tbody>
</table>

- Encryption
  - Data Protection
  - Data validation
  - Data destruction
  - Code signing
  - Digital fingerprinting
  - Data Time-stamping
  - Message Authentication
  - Message / data integrity
  - Forgery detection
  - Forensic protection
  - Pseudorandom number generation

- Policy-based Identity and Access
  - Identity validation

- Reducing the risk or/and potentially enabling cross-border business opportunities
- Clear text data on stolen / disposed of hardware

- Storages
- Data
Business Continuity and Disaster Recovery (BC / DR) SecaaS

- The contingency plans and measures to ensure operational resiliency
- How to maintain the ability to quickly and reliably recover
- Cloud centric BC/DR makes use of the cloud’s flexibility to minimize cost and maximize benefit
- Service: file recovery provider, file backup provider, Replication etc…
Network Security Service

- **Network Security SecaaS**
  - Security control at the network in aggregate
  - Requires tight integration with the hypervisor
  - Service: Firewall, DDoS protection, IDS/IP etc...

- **Application Vulnerability**
  - Security Intelligence
    - Traffic netflow monitoring, Security monitoring and IR

- **Cloud Platform Threats**
  - Policy-based Identity and Access
    - Access and authentication controls

- **Network Management**
  - Integration with Hypervisor layer
  - Data threats
  - Security gateways
  - Security products
  - Dos protection / mitigation
Security as a Service

- **Cloud-based Security Service Market**
  - To reach $4.2 billion by 2016
  - Cloud security services market by the end of 2013, with a growth rate of 30%, is expected to surpass the traditional security market.

<table>
<thead>
<tr>
<th>Segment</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>5-year CAGR(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Email Gateway</td>
<td>650</td>
<td>817</td>
<td>1,000</td>
<td>1,200</td>
<td>1,400</td>
<td>1,530</td>
<td>1,626</td>
<td>14.8</td>
</tr>
<tr>
<td>Secure Web Gateway</td>
<td>200</td>
<td>293</td>
<td>450</td>
<td>610</td>
<td>770</td>
<td>890</td>
<td>996</td>
<td>27.7</td>
</tr>
<tr>
<td>Remote Vulnerability Assessment</td>
<td>85</td>
<td>103</td>
<td>130</td>
<td>170</td>
<td>215</td>
<td>270</td>
<td>336</td>
<td>26.7</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>88</td>
<td>136</td>
<td>220</td>
<td>337</td>
<td>497</td>
<td>644</td>
<td>763</td>
<td>41.2</td>
</tr>
<tr>
<td>Security Information Event Management</td>
<td>20</td>
<td>35</td>
<td>60</td>
<td>95</td>
<td>150</td>
<td>190</td>
<td>227</td>
<td>45.7</td>
</tr>
<tr>
<td>Other Cloud-based Security Services</td>
<td>73</td>
<td>87</td>
<td>116</td>
<td>157</td>
<td>200</td>
<td>234</td>
<td>253</td>
<td>23.9</td>
</tr>
<tr>
<td>Total</td>
<td>1,115</td>
<td>1,470</td>
<td>1,977</td>
<td>2,570</td>
<td>3,231</td>
<td>3,758</td>
<td>4,202</td>
<td>23.4</td>
</tr>
</tbody>
</table>

# SecaaS Solutions

## Current solutions

<table>
<thead>
<tr>
<th>Segment</th>
<th>Core function</th>
<th>Products or Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud SecaaS</td>
<td>IAM</td>
<td>AWS IAM, IBM IAM</td>
</tr>
<tr>
<td></td>
<td>Network security</td>
<td>VPC, Monitoring, Firewall, IDS</td>
</tr>
<tr>
<td></td>
<td>Web security</td>
<td>Web firewall</td>
</tr>
<tr>
<td></td>
<td>BC / DR</td>
<td>Backup, Disaster Recovery</td>
</tr>
<tr>
<td></td>
<td>IAM</td>
<td>CA Arcot Webfort (Pendo systems), Cyber Ark Software Privileged Identity Manager (McAfee), Nevell Cloud Security Services (NetIQ)</td>
</tr>
<tr>
<td>Standalone SecaaS</td>
<td>Web Security</td>
<td>BlueCoat, RSA, TrendMicro, Websense, zScaler</td>
</tr>
<tr>
<td></td>
<td>DLP</td>
<td>Symantec (Data Loss Prevention), Websense (Data Seucriyt Suite), Zenprise (XenMobile MDM), Zscaler (Data Protection)</td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td>Gmail, McAfee, TrendMicro, Zcaler, Microsoft Cloud Services</td>
</tr>
<tr>
<td></td>
<td>Security Assessment</td>
<td>Agiliance, Core Security, Modulo, Qualys, Veracode, WhiteHat</td>
</tr>
<tr>
<td></td>
<td>Intrusion management</td>
<td>Cyntec Scout, Sourcefire, StoneGate, Symantec, TrendMicro</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>Credant, Cypher Cloud, enStratus, Novaho, Perpecsys</td>
</tr>
<tr>
<td></td>
<td>BC / DR</td>
<td>Atmos, Decco, Digital Pallels, Rackspace</td>
</tr>
<tr>
<td></td>
<td>Network security</td>
<td>CloudFlare, Imperva, Rackspace, Symantec, Stonesoft</td>
</tr>
</tbody>
</table>
Two approaches for SecaaS

- **Cloud SecaaS by CSP**
  - The security service for protecting it’s customers and cloud system
  - Cloud customers will use Cloud SecaaS
    - Major company(Hybrid cloud) : Cloud SecaaS in the public cloud
    - Small and medium businesses(Public cloud) : Cloud SecaaS

- **Standalone SecaaS**
  - Standalone SecaaS for end-point security service
    - Thin client + Public Cloud(ex: google chrome notebook) : not activation
    - DaaS(Desktop-as-a-service) : leaks of company information
    - End-user device : not easy to apply pc-level security
      - Mobile Anti-virus : SecaaS is more suitable
Our Work

- **Installing Cloud Test-bed**
  - Our test-bed was installed using CloudStack
  - **What is CloudStack?**
    - Open source software designed to deploy and manage large networks of virtual machines
    - Work as a highly available, highly scalable Infrastructure as a Service (IaaS) cloud computing platform

- CloudStack 4.0 (apache)
- Hypervisor : KVM (RedHat)
  - CPU 6 core, RAM 32GB
- Storage : NFS
Our Work

- **The Model of SecaaS Platform**

![Diagram of the SecaaS Platform]

- Tenants
- Security Agent
- Internet
- Server (web, email, etc)
- Guest VM
- SeccaS Platform
- Guest VM Service
- Packet Controller
- Guest VM Service DB
Our Work

- **The Architecture of SecaaS Platform**
  - Packet Controller: handling tenants’ packets to security service they want
  - VM Management: managing VMs to install security service
  - IaaS API Handler: APIs provided by CloudStack to manage computing resources
Our Work

- **SSP Admin**
  - Service Management: Create, delete, Subscribe, Unsubscribe services
  - VM Management: Start, stop and checks VMs status
  - Billing and Report based on Tenant users
Our Work

- **Platform Admin**
  - Account Management: Activate/deactivate admins accounts
  - System Management: Handling offering services, pricing, and metering information
Our Work

- **Tenant Admin**
  - Tenant Management: handler users’ information
  - Tenant Group Management: users who use the same security services will belong to the same group
Our Work

Design of SecaaS Platform

SSP Controller  Tenant Controller  Platform Controller  Pages

REST Applications

Web Data  CloudStack API  Testing Module  SecaaS API

Message Source  Repository Module  SecaaS Base Library

Custom User Authentication  ModelFactory

SecaaS Platform

Security  Data JPA

Internalization  Validation

Spring Framework

APIs  Cloud Infrastructure

Controller Infrastructure
Our Work

- Flexible configuration of security policies
- Apply multiple security functions to a single data stream
- Standard APIs for security modules
Conclusion

- New paradigm for security service
  - Appliance-based security solution moves to Cloud-based security service
- SecaaS is a new platform for providing security service
- Existing security services can be transformed into SecaaS (10 categories)
- Many advantages in upgrading and patching at centralized SecaaS platform
Thank you