Secure Cloud Computing

Prof. Dr. Michael Waidner

Center for Advanced Security Research Darmstadt (CASED): TU Darmstadt & Fraunhofer SIT
Outline

1. Security Considerations
2. Security Challenges
   - Provider Perspective
   - Subscriber Perspective
3. Security as a Service
4. Research Challenges
Outline

1. **Security Considerations**
2. **Security Challenges**
   - Provider Perspective
   - Subscriber Perspective
3. **Security as a Service**
4. **Research Challenges**
Consumption and Delivery Model for IT Services

“Cloud” represents the industrialization of delivery for IT supported services

<table>
<thead>
<tr>
<th>Deployment Models</th>
<th>Hybrid Clouds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Cloud</td>
<td></td>
</tr>
<tr>
<td>On Premise</td>
<td></td>
</tr>
<tr>
<td>Off Premise</td>
<td></td>
</tr>
<tr>
<td>3rd-Party Managed</td>
<td></td>
</tr>
<tr>
<td>Public Cloud</td>
<td></td>
</tr>
<tr>
<td>Community Cloud</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Models</th>
<th>Business Process as a Service (BPaaS)</th>
<th>Software as a Service (SaaS)</th>
<th>Platform as a Service (PaaS)</th>
<th>Infrastructure as a Service (IaaS)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Essential Characteristics</th>
<th>On Demand Self-Service</th>
<th>Broad Network Access</th>
<th>Resource Pooling</th>
<th>Rapid Elasticity</th>
<th>Measured Service</th>
<th>Service Mgmt Automation</th>
</tr>
</thead>
</table>

|------------------------|----------------|--------------------------|-------------------|--------------------|------------------------|-------------------|-------------|-------------------------|---------------------|

<table>
<thead>
<tr>
<th>Cloud Enables</th>
<th>Economies of scale</th>
<th>Sourcing Options</th>
<th>Flexible payment models</th>
</tr>
</thead>
</table>

Adapted from: [Mell, Grance: The NIST Definition of Cloud Computing; NIST SPUB 800-145]
Moving from Private to Public Leads to a Real or Perceived Loss of Control

We Have Control
- It’s located at X.
- We have backups.
- Our admins control access.
- Our uptime is sufficient.
- The auditors are happy.
- Our security team is engaged.

Who Has Control?
- Where is it located?
- Who backs it up?
- Who has access?
- How resilient is it?
- How do auditors observe?
- How does our security team engage?

33%
Of respondents are concerned with cloud interfering with their ability to comply with regulations

80%
Of enterprises consider security #1 inhibitor to cloud adoptions

48%
Of enterprises are concerned about the reliability of clouds

Source: Driving Profitable Growth Through Cloud Computing, IBM Study, 2008 (conducted by Oliver Wyman)
Workloads may be at Different Levels of Cloud Readiness

- Ready for Cloud
- Analytics
- Infrastructure Storage
- Industry Applications
- Collaboration
- Workplace, Desktop & Devices
- Business Processes
- Disaster Recovery
- Development & Test
- Infrastructure Compute
- Pre-production systems
- Batch processing
- Regulation sensitive
- Complex processes & transactions
- Highly customized
- Isolated workloads
- Mature workloads
- Sensitive Data
- Information intensive
- Not yet virtualized 3rd party SW
- May not yet be ready for migration ...
- New workloads made possible by clouds ...
- Market bias:
  - Private cloud
  - Public cloud

© IBM, 2010

CASED
Cloud Service Model Suggests Split of Responsibilities between the Provider of Public Clouds and the Subscribers

Who is responsible for security at the ... level?

- Datacenter Infrastructure
- Middleware
- Application
- Process

Provider

Subscriber

Provider

Subscriber

Provider

Subscriber

Provider

Subscriber

© IBM, 2010
Data are Central to the Analysis of Risks and Threats

*CSA (2010), ENISA (2009), Gartner (2008), IBM X-Force (2010), ...*

<table>
<thead>
<tr>
<th>Transformation</th>
<th>1. Vendor lock-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Data</td>
<td>2. Data security</td>
</tr>
<tr>
<td>Compliance</td>
<td>3. Data protection, meeting privacy needs and expectations</td>
</tr>
<tr>
<td></td>
<td>4. General and industry-specific compliance</td>
</tr>
<tr>
<td></td>
<td>5. Uncertainty over data location</td>
</tr>
<tr>
<td></td>
<td>6. Inability to respond to law enforcement requests</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>7. Data recovery, resiliency</td>
</tr>
<tr>
<td>Classical IT Security</td>
<td>8. Account or service hijacking</td>
</tr>
<tr>
<td></td>
<td>9. Insecure interfaces and APIs</td>
</tr>
<tr>
<td></td>
<td>10. Management (incl. self-service) interface compromise</td>
</tr>
<tr>
<td>Shared IT</td>
<td>11. Insecure or incomplete data deletion</td>
</tr>
<tr>
<td></td>
<td>12. Process/VM isolation, data segregation, multi-tenancy</td>
</tr>
<tr>
<td></td>
<td>13. Malicious insiders (co-tenants, cloud provider)</td>
</tr>
<tr>
<td></td>
<td>14. Abuse of cloud services (extrusion)</td>
</tr>
</tbody>
</table>
Outline

1. Security Considerations

2. Security Challenges
   - Provider Perspective
   - Subscriber Perspective

3. Security as a Service

4. Research Challenges
What is Cloud Security?

Confidentiality, integrity, availability of business-critical IT assets
Stored or processed on a cloud platform

There is nothing new under the sun but there are lots of old things we don't know.

Ambrose Bierce, The Devil's Dictionary
Very Quick Intro to Information Security
Information Security Risk Management

Threat (and Attack) Malicious / Accidental Insider / Outsider

Vulnerability

Resource
- Identities
- Information
- Applications
- IT
- Infrastructure
- Physical infrast.

Objective
- Confidentiality
- Integrity
- Availability
- Accountability
- (Manageability)

Parties Concerned
- Provider, subscriber, end-user, ..., government

Risk management
- Acceptance
- Avoidance
- Transfer
- Mitigation

Risk is estimated based on statistical assumptions, and those are changing over time. Each party needs to manage their risk towards an acceptable level (multi-party security). The residual risk is never zero, there is no absolute security.
## Security Mechanisms (Controls)

### Security Policy
- Enterprise, identity, access, retention, ...
- Ideally derived and propagated top down
- Allow/deny + mandates/obligations
- Often composite, mandatory and discr.
- Abstract, role based, class based

### Security Development
- Practices
- Security testing
- Eg, OWASP
  - [Allan 10](#)

### Prevention (Avoidance, Enforcement)

<table>
<thead>
<tr>
<th>Categorization</th>
<th>Description</th>
</tr>
</thead>
</table>
| Access Control          | • Reference monitor  
 • Authorization  
 • Data / proc tagging  
 • Hypervisor  
 • Memory protection  
 • Filesystem protection  
 • Virtual LAN |
| Intrusion / Extrusion Prevention | • Firewall  
 • Anti-virus, anti-malware  
 • Intrusion prevention  
 • Data leak prevention  
 • Virtual patching |
| Cryptography            | • Encryption  
 • Key management  
 • Channel security, VPN |
| Redundancy              | • Fault tolerance  
 • Backup & recovery  
 • Fail-over, graceful degradation |
| Intrusion & Fraud Detection | • Signature-based  
 • Behavior-based  
 • Server, network based |
| Logging & Auditing      | • Immutable logs  
 • Time stamping |

### Compensation (Recovery, Fail-over)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>
| • MAC, Hash  
 • Digital Signatures  
 • Message security |

### Logging & Auditing
- • Immutable logs  
- • Time stamping

## Cryptography
- • Encryption
- • Key management
- • Channel security, VPN

## Intrusion / Extrusion Detection
- • Firewall
- • Anti-virus, anti-malware
- • Intrusion prevention
- • Data leak prevention
- • Virtual patching

## Intrusion & Fraud Detection
- • Signature-based
- • Behavior-based
- • Server, network based

## Redundancy
- • Fault tolerance
- • Backup & recovery
- • Fail-over, graceful degradation

## Access Control
- • Reference monitor
- • Authorization
- • Data / proc tagging
- • Hypervisor
- • Memory protection
- • Filesystem protection
- • Virtual LAN

## Trusted Computing
- • Enforcement through (mutually) trusted hardware

## Identity
- • Authentication
- • Identity Management

## Logging & Auditing
- • Immutable logs
- • Time stamping

## Physical and Organizational Security

## Change and Configuration Management

## Asset Management

---

[Image 36x15 to 117x50]
[Image 553x16 to 683x48]
Information Security Certification and Audit

- Internal and external, always organizationally independent
- Three major frameworks for security audit
  - Payment Card Industry Data Security Standard (PCI DSS)
    - Fairly prescriptive. Meant specifically for protecting card holder data.
  - ISO/IEC 27001 (German BSI-Standard 100)
    - Technology neutral, but ISO 2700x provides strong security context.
  - Statement on Standards for Attestation Engagements (SSAE) No. 16
    - Successor of SAS 70.
    - Very open, meant for service providers operating transaction systems, and de-facto standard framework for IT outsourcing.
    - Additional requirements (e.g. affirmation of business management) increase quality of audit.
- Typically significant leeway for auditors
- Related but not yet relevant for cloud computing outside government context
  - Common Criteria Certification

“Trust is good, control is better.” Vladimir Ilyich Lenin

“My job is not security, my job is making sure we pass the audit.” Anonymous CISO
Information Security Process and Management System

Information Security Risk Management requires

- Policy and Process
- Service Management and IT Governance
- People and Organization
- Education and Incentives
- Measurement and Reporting
- And Security Technology

Our focus:
Done, back to cloud ...
Data are Central to the Analysis of Risks and Threats

CSA (2010), ENISA (2009), Gartner (2008), IBM X-Force (2010), ...

<table>
<thead>
<tr>
<th>Transformation</th>
<th>1. Vendor lock-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Data</td>
<td>2. Data security</td>
</tr>
<tr>
<td>Compliance</td>
<td>3. Data protection, meeting privacy needs and expectations</td>
</tr>
<tr>
<td></td>
<td>4. General and industry-specific compliance</td>
</tr>
<tr>
<td></td>
<td>5. Uncertainty over data location</td>
</tr>
<tr>
<td></td>
<td>6. Inability to respond to law enforcement requests</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>7. Data recovery, resiliency</td>
</tr>
<tr>
<td>Classical IT Security</td>
<td>8. Account or service hijacking</td>
</tr>
<tr>
<td></td>
<td>9. Insecure interfaces and APIs</td>
</tr>
<tr>
<td></td>
<td>10. Management (incl. self-service) interface compromise</td>
</tr>
<tr>
<td>Shared IT</td>
<td>11. Insecure or incomplete data deletion</td>
</tr>
<tr>
<td></td>
<td>12. Process/VM isolation, data segregation, multi-tenancy</td>
</tr>
<tr>
<td></td>
<td>13. Malicious insiders (co-tenants, cloud provider)</td>
</tr>
<tr>
<td></td>
<td>14. Abuse of cloud services (extrusion)</td>
</tr>
</tbody>
</table>
Simplified Model

- Multi-tenancy / Virt
- Cloud Management
- Cloud Data Center
**New Threats**

External Threats

- Co-tenants
- Empowered end-users
- Cloud insiders (½ new)

**New sources of threats**

**New technologies**

- Physical-to-virtual: Multi-tenancy, virtualization
- Cloud mgmt: co-management of security, self-service
- Web 2.0-ish cross-domain SOA
Old Threats

- Network vuln's
- Malware
- Force majeur

New sources of threats

- Co-tenants
- Empowered end-users
- Cloud insiders (½ new)

New technologies

- Physical-to-virtual: Multi-tenancy, virtualization
- Cloud mgmt: co-management of security, self-service
- Web 2.0-ish cross-domain SOA
### New sources of threats
- Co-tenants
- Empowered end-users
- Cloud insiders (½ new)

### New technologies
- Physical-to-virtual: Multi-tenancy, virtualization
- Cloud mgmt: co-management of security, self-service
- Web 2.0-ish cross-domain SOA

- At the core this is all well known
- Many system aspects do not change at all
- But: many new details and constraints
Two Parallel Trends: Mobile Access to Cloud-delivered Services

Cloud model suggests and supports ubiquitous access via resource constrained and often personally owned devices

- Mobile access and public cloud both blur the enterprise perimeter
- New endpoints (e.g., iOS, Android) with new security characteristics and challenges,
- Often used for personal and business purposes
- “Bring your own device”: Consumerization of IT often collides with enterprise security principles
Cloud computing also provides the opportunity to simplify security controls and defenses

<table>
<thead>
<tr>
<th>People and Identity</th>
<th>Cloud Enabled Control(s)</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Defined set of cloud interfaces</td>
<td>Reduced risk of user access to unrelated resources.</td>
</tr>
<tr>
<td></td>
<td>Centralized repository of Identity and Access Control policies</td>
<td></td>
</tr>
<tr>
<td>Information and Data</td>
<td>Computing services running in isolated domains as defined in service catalogs</td>
<td>Improved accountability, Reduced risk of data leakage / loss</td>
</tr>
<tr>
<td></td>
<td>Default encryption of data in motion &amp; at rest</td>
<td>Reduced attack surface and threat window</td>
</tr>
<tr>
<td></td>
<td>Virtualized storage providing better inventory, control, tracking of master data</td>
<td>Less likelihood that an attack would propagate</td>
</tr>
<tr>
<td>Process &amp; Application</td>
<td>Autonomous security policies and procedures</td>
<td>Improved protection of assets and increased accountability of business and IT users</td>
</tr>
<tr>
<td></td>
<td>Personnel and tools with specialized knowledge of the cloud ecosystem</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SLA-backed availability and confidentiality</td>
<td></td>
</tr>
<tr>
<td>Network Server and Endpoint</td>
<td>Automated provisioning and reclamation of hardened runtime images</td>
<td>Reduced attack surface</td>
</tr>
<tr>
<td></td>
<td>Dynamic allocation of pooled resources to mission-oriented ensembles</td>
<td>Improved forensics with ensemble snapshots</td>
</tr>
<tr>
<td>Physical infrastructure</td>
<td>Closer coupling of systems to manage physical and logical identity / access.</td>
<td>Improved ability to enforce access policy and manage compliance</td>
</tr>
</tbody>
</table>
Two Perspectives

Provider perspective:
How to provide a secure cloud service?

Subscriber perspective:
How to select a cloud?
Who to use a cloud securely?
Outline

1. Security Considerations
2. Security Challenges
   - Provider Perspective
   - Subscriber Perspective
3. Security as a Service
4. Research Challenges
Components of a Cloud Security Solution

- Isolation
- Identity
- Compliance
Isolation – Software, Server, Network
Coloring/Labeling Resources, Events, ...

- State of the art
  - Service and Application
    - Can be done at all levels of the stack
  - Server
    - Hypervisor: z/VM, LPAR, pHype, Xen, VMware ESX, ...
  - Network
    - Security Zones, Trusted Virtual Domains
    - VLAN (IEEE 802.1Q)
    - Trusted / Secure Virtual Private Networks (VPN)
    - Encryption of data in transit (SSL/TLS, SSH, IPSec)

- Key Issues
  - Standardized policies
  - Verification of isolation
  - Application security → VM security
  - Network security → VN security
Isolation and Integrity Management: Multi-tenancy

- Users from *different trust domains are drawing on a shared pool of resources*
  - Network, storage and server virtualization
  - Shared file system, database, middleware, application, desktop, business service, ...
  - Stack architectures offer choices for implementing multi-tenancy (lower or higher in the stack)
  - Isolation is the key security requirement

- Basic mechanism is *coloring (aka tagging, labeling) and enforcement of isolation between domains (aka zones) of different colors*

  - Enforcement through
    - Reference Monitor: provisioning, runtime, de-provisioning / cleanup
    - Cryptography (encryption, key management)
Hypervisor-level Security Services – Physical

What changes in a naïve transition from physical (this picture) to virtual?

- **Security becomes harder**: VM sprawl, hypervisor as a new component
- **Services unnecessarily replicated**
- **Security becomes easier**: move security services out of the OS into the Hypervisor, security system can *introspect* the virtual hardware

Diagram:
- App 1
- App 2
- App 3
- AV/FW
- OS
- HW
- Switch / NAC / Firewall / IPS ...

CASED

Fraunhofer SIT
Hypervisor-level Security Services – **Virtual**

![Diagram showing Hypervisor-level Security Services]

- **Security VM**
  - Policy
  - Hardened OS
  - Discovery, license mgmt, update, congestion control + ...

- **Switch / NAC / FW / IPS**
- **Rootkit Detection**

Source: IBM Tivoli Virtual Server Security for VMware

Source: IBM Tivoli Virtual Server Security for VMware
Isolation – Data, Storage, Backups
Coloring/Labeling Resources, Events, ...

- **State of the art**
  - Label-based Access Control (LBAC)
  - Storage zoning (Virtual Storage Area Network, ...)
  - Enforcing location (per privacy laws)
  - Cleanup of caches, files, disks, backups, ...
  - Encryption of data at rest
    - Data deduplication vs. encryption
    - Provider vs. individual keys
    - In-cloud vs. extra-cloud key management
  - Fully homomorphic encryption

- **Key Issues**
  - Standardized policies
  - Standardized data portability
  - Meaningful key management
  - Research in advanced crypto
Secure Cloud Storage

OmniCloud
Analysis of Cloud Storage Services

Fraunhofer SIT Technical Report:

- Analyzed cloud storage providers:
  - CloudMe, CrashPlan, Dropbox, Mozy, TeamDrive, Ubuntu One

- Result: Providers are security aware

- However, there are some typical security issues:
  - No data encryption or server side encryption, only
  - No filename obfuscation for public files
  - Registration: weak passwords, no email verification
  - Shared files are indexed by search engines
Identity

Main types of identities to consider in a cloud

- **Standard identity management + access/usage control**
  - Major risk: reinventing the wheel ...
  - Major challenge: correlation of identities and security events across multiple layers in the cloud stack

- **Cloud subscriber administrators**
  - Initial enrollment and proofing of cloud subscriber
  - Trust depends largely on proofing of identities
    - Valid email address
    - Upfront payment
    - Out-of-band signed service contract

- **Cloud subscriber end user identities**
  - Subscriber's employees, customers, ...
  - Efficient on-boarding / off-boarding
  - Directory synchronization (bad idea)
  - Federated identity (good idea, standard in SOA)

- **Cloud provider administrators**
  - Major issue: Control over privileged identities
Compliance
Meeting Regulatory Requirements

- Provider auditing
- Subscriber-level auditing
  - Practically often very hard
- Privacy
  - Data encryption and suitable key management
  - Enforcing data location
  - Prevent cross-border data flows
- Cloud Forensics
  - Discover evidence related to a specific cloud subscriber
  - Freezing and surrendering virtual resources
  - Protect confidentiality of third parties resources
Outline

1. Security Considerations
2. Security Challenges
   - Provider Perspective
   - Subscriber Perspective
3. Security as a Service
4. Research Challenges
Components of a Cloud Security Solution

- Isolation
- Identity
- Compliance
- Trust in Cloud Provider
- Secure Usage
Trust in Cloud Provider

• **Subscriber perspective**
  - “Secure Virtualized Runtime” is the provider's responsibility
  - No direct control, hence provider must be trustworthy
    • Reputation
    • Stated provider security policies
    • Service-level agreements with regular audits and defined compensations
    • Audits may be general (low-end, standardized) or client-specific (high-end, specialized)
  - Very few technologies enable extension of control into the cloud
    • Cryptography (encryption, integrity checks), to a certain extent
    • TCG-style Trusted Computing (exists but rarely used)
    • Research: homomorphic encryption

• **Best practices, guidance/checklists and audits play major role**
  • Cloud Security Alliance [CSA 09]
  • IBM Cloud Security Guidance [Buecker 09]
Fully Homomorphic Encryption

- **Value of data-at-rest encryption in cloud computing**
  - Data on disks, data on backups
  - Storage-centric: subscriber can en/decrypt, provider never sees data
  - Does not work if & while cloud provider operates on encrypted data

- **Fully homomorphic encryption (idea: Rivest, Adleman, Dertouzos, 1978)**
  - Express an algorithm as a circuit (network): \( f(x_1, x_2, \ldots) = x_1 + x_2^* (1-x_3) \ldots \)
  - What if we had a public-key encryption function that (roughly) does this:
    - \( \text{Enc}(x_1) + \text{Enc}(x_2)^* (1-\text{Enc}(x_3)) \ldots = \text{Enc}(x_1 + x_2^* (1-x_3) \ldots \)

- **State of the art**
  - Efficient solutions for certain related subproblems (homomorphic in one operation, server-aided computations, voting protocols, …)
  - First provably secure fully homomorphic solution: [Gentry 09]
    - Shows what can be done in principle
    - Polynomial, but needs substantial work before it can be used in practice
  - Major area of research in cryptography
Trusted Cloud – Why?

- Success of the cloud model: Perceived benefits dominate stated security and privacy concerns
- Cloud users are taking more risk than they feel comfortable with
  - Market very sensitive to real or perceived cloud security incidents

- What trust is needed?
  - Varies by market segment, workload, type of data
  - Different answers for governments, regulated industries, “regular” enterprises, private users, etc.

- Business opportunity “Trusted Cloud”
Cloud Users often do not Understand Cloud Characteristics

Fraunhofer SIT Analysis of 1100 Public Amazon Machine Images, Spring 2011

About 1/3 with major vulnerabilities

- Caches, shadow files, ...
- Passwords
- Public SSH keys
- Private SSH keys
Analysis of VM Images

- Automated extraction of sensitive information from AMIs (Amazon Machine Images), available via the Cloud App Store
  - SSL private / public keys
  - SSH private / public keys
  - SVN credentials
  - AWS API keys
  - Unpublished source code
  - Private pictures and documents

- Reasons why these AMIs contain sensitive information
  - Users forgot private data in their AMIs
  - Users are unaware of the consequences not to remove sensitive data

- Enables attacks based on those information
  - SSH backdoors allowing remote login
  - SSH host key correlation (multiple instances uses the same SSH host key)

Reference:
Outline

1. Security Considerations
2. Security Challenges
   - Provider Perspective
   - Subscriber Perspective
3. Security as a Service
4. Research Challenges
Security as a Service

Good candidates for security-as-a-service are functions which

- Can be delivered without on-premises technology
- Latency-tolerant
- Require minimal customization
- Involve one-to-many data management or analysis functions
- Can be implemented through standard interfaces
- Unlike managed security services, not labor-intensive

<table>
<thead>
<tr>
<th>Function</th>
<th>Now</th>
<th>2013</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messaging / Email Security</td>
<td>20%</td>
<td>60%</td>
<td>70%</td>
</tr>
<tr>
<td>Secure Web Gateway</td>
<td>10%</td>
<td>35%</td>
<td>65%</td>
</tr>
<tr>
<td>Remote Vulnerability Scanning</td>
<td>10%</td>
<td>30%</td>
<td>45%</td>
</tr>
<tr>
<td>Security Information and Log Management</td>
<td>1%</td>
<td>10%</td>
<td>25%</td>
</tr>
<tr>
<td>Identity &amp; Access Management</td>
<td>2%</td>
<td>20%</td>
<td>28%</td>
</tr>
<tr>
<td>Security Intelligence</td>
<td>60%</td>
<td>80%</td>
<td>85%</td>
</tr>
</tbody>
</table>

Source: Kelly Kavanagh, Gartner Research
In-Security as a Service

Zeus botnet finds hold in Amazon cloud
Published: 2009-12-11

The cybercriminals behind the Zeus botnet used Amazon's Elastic Computing Cloud (EC2) to host the central server used to control a portion of the compromised machines, security firm CA stated on Thursday.

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, technical account manager Vido Vajic, told delegates becoming so business-like that online offerings of malware, support and maintenance services.
Outline

1. Security Considerations
2. Security Challenges
   - Provider Perspective
   - Subscriber Perspective
3. Security as a Service
4. Research Challenges
Areas for Research

Not a complete list ...

- Definition, Measurement and Assurance
- VM Security = Platform Security \(\cup\) Application Security
  - Provenance, trust management
  - Compliance checking, scanning and patching of dormant images
  - Reconsider proof-carrying code and other “mobile agent” security constructs
- Security Through Cloud Computing
  - Security as a service
  - Hypervisor-based security services
  - Security in emerging cloud computing programming models and languages
- Architectures for trustworthy cloud computing
  - Key management
  - TCG-style trusted computing
  - Fully homomorphic encryption, and other crypto tricks to support privacy
  - Trusted “clouds of clouds”
  - Trusted data and identity portability
Prof. Dr. Michael Waidner
michael.waidner@sit.fraunhofer.de

Fraunhofer-Institute for Secure Information Technology
Rheinstrasse 75
64295 Darmstadt, Germany
www.fraunhofer.de
www.sit.fraunhofer.de

Technical University of Darmstadt
Chair for Security in Information Technology
Mornewegstrasse 30
64289 Darmstadt, Germany
www.cased.de
www.sit.tu-darmstadt.de
Security and Privacy »made in Darmstadt«

170 employees, 70 full-time researchers, 2 TU professors

10 professors, incl. 6 chairs, with strong security focus

15 professors with more than 100 researchers in CASED

6 professors