When the Clouds Disperse

Data Confidentiality and Privacy in Cloud Computing

24.05.2013

C. Kauba, S. Mayer

Seminar aus Informatik - SS2013

UNIVERSITÄT SALZBURG

Outline

- Introduction
- Cloud computing security issues
- Legal aspects
- Threats and attacks
- User attitudes and beliefs
- Countermeasures
- Summary

Cloud Computing

- Use of hardware, storage and systems software located in large data centers worldwide
- Main characteristics:
  - On-demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service
- Public and private clouds

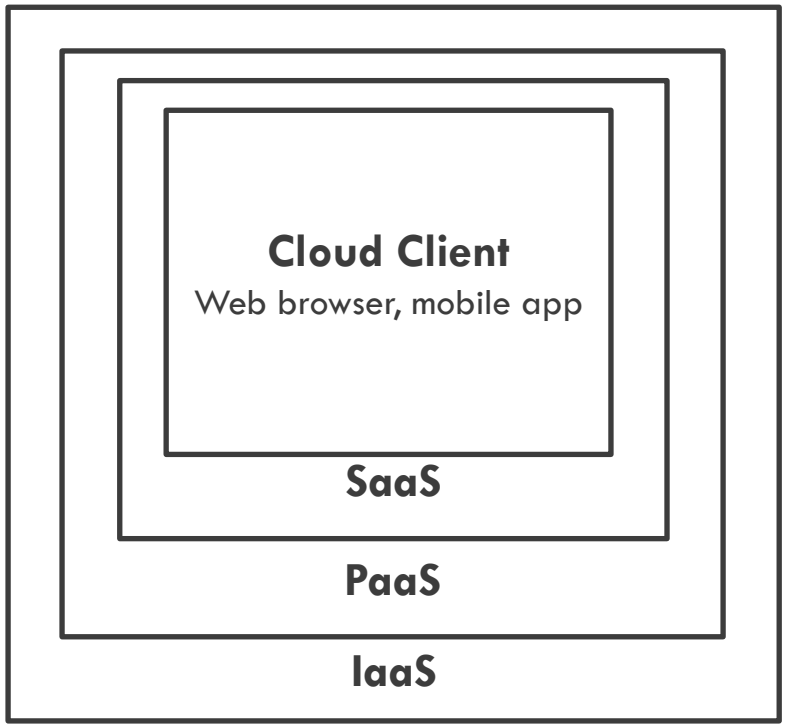
Cloud Computing Service Model (1)

- **SaaS (Software as a Service)**
  - Common delivery model for business applications
  - Extends the idea of the ASP model
  - Examples: Google Docs, Webmail, Office Software, DBMS

- **PaaS (Platform as a Service)**
  - Provides a computing platform and a solution stack as a service
  - Tools and libraries from the provider can be used
  - Network, server and storage are provided
  - User does not manage nor control the underlying cloud infrastructure
  - Examples: Windows Azure, Amazon EC2

Cloud Computing Service Model (2)

- **IaaS (Infrastructure as a Service)**
  - Providing processing power, storage, networks and other computing services
  - User has control over operating systems, storage, network, deployed applications
  - Example: Amazon EC2



Cloud Computing Benefits

- **Service Provider**
  - No more software piracy issues
  - Protection from reverse engineering
  - Vendor lock-in
  - Higher revenues than one-time purchases
  - Carefully targeted advertising, data mining
- **Customer**
  - Cost savings
  - Increased flexibility
  - Data can be accessed from anywhere

Cloud Computing Benefits for Governments

- Surveillance at near zero marginal cost, significantly reduced manpower, elimination of physical risk
- No need for physical surveillance, to install wiretaps, to do a black bag job or to steam open mails
- No raid and data extraction of data from a suspects PC
- Request to the cloud service provider is sufficient
- Deleted data is also stored
- Legal compliance departments
- Providers may charge for surveillance (paper-trail)

Cloud Computing Issues

- Data is no longer stored locally, no direct control
- Internet connection needed to use the software
- Data confidentiality threats:
  - Data is in transmission
  - Stored data
- Problems for companies due to different laws
  - Europe's safe harbour convention
  - Exact storage location of the data not known
  - Data stored on the web is treated differently by legislation than if stored locally
- Many users have no choice or are not aware that they are actually using cloud software

Attackers and their Interests in User Data

- **Third persons (Hackers)**
  - Making profit (credit card numbers, financial records, bank login details)
- **Governments**
  - Surveillance
  - Fighting crime and terrorism
- **Cloud Service Provider**
  - Achieving profit (personalised ads)
  - Data and user profile marketing

Government's legal possibilities to access personal data

- **Personal data**
  - Any information relating to an identified or identifiable individual (data subject)
- Legal authority to order firms to turn their own technology against their customers as long as there is no complete disruption of the service and to circumvent any privacy enhancing technology
- Stored communications act, Fourth Amendment, Third-party doctrine, USA Patriot Act, FISA, Wiretap Act, ToS
- Subpoena (no court order needed)
- Search warrant
- USA Patriot Act, §215 court order
- Emergency voluntary disclosure (disclosure without delay)

Terms of Service Agreement

- No guarantee that data will be kept confidential
- Right to manipulate, disclose and delete user data without notice
- No liability for service interruption, data loss, errors, inaccurate or untimely results
- ToS may change without any notification
- Capitalizing lack of knowledge about privacy issues in the cloud

ToS Examples of Cloud Services (1)

- **Google's** advertising system relies on customers' data
  - Google Terms of Service, *supra* note 126, § 8.3**.**
    "Google reserves the right . . . to prescreen, review, flag, filter, modify, refuse or remove any or all Content from any [Google] Service." [5]

  - Google Privacy Center: Advertising and Privacy, *supra* note 130.
    "[t]he Gmail filtering system also scans for keywords in users' e-mails which are then used to match and serve ads. When a user opens an e-mail message, computers scan the text and then instantaneously display relevant information that is matched to the text of the message." [5]

ToS Examples of Cloud Services (2)

- **Yahoo!** reserves the right to “pre-screen” content on its service
  - Yahoo! Mail Privacy Policy, http://info.yahoo.com/privacy/us/yahoo/mail/details.html (May. 17, 2013) (emphasis added).
    “Yahoo!’s practice is not to use the content of messages stored in your Yahoo! Mail account for marketing purposes.” [5]

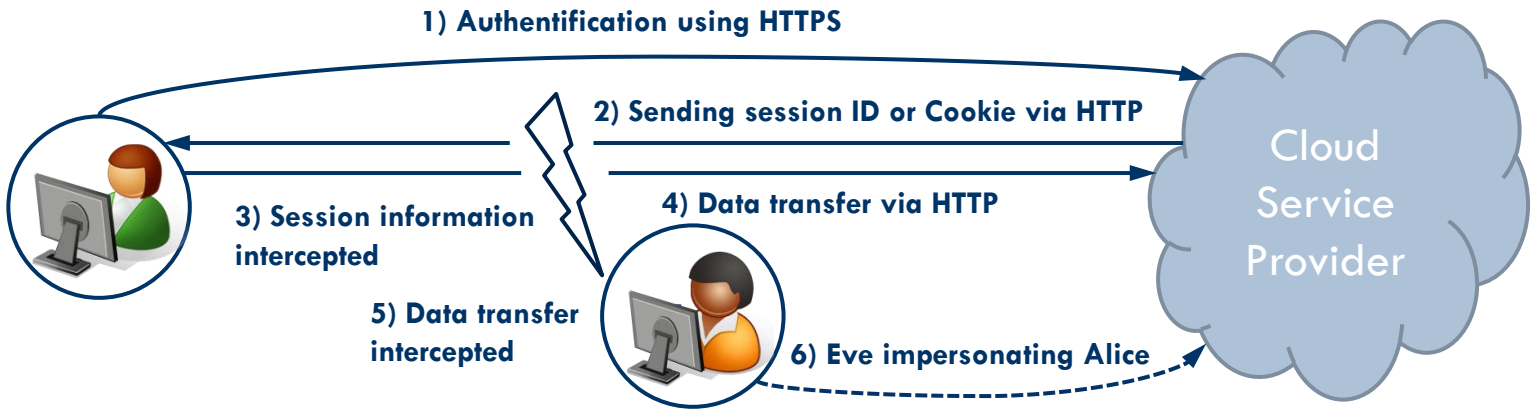
- **Mozy** (a cloud service provider) assure customers about the privacy of their content
  - Mozy: Decho Corporation Privacy Policy (May. 17, 2013), http://mozy.com/privacy.
    “We will not view the files that you backup using the Service.” [5]

Threats and Attacks

- **Hackers**
  - Session hijacking
  - Man-in-the-Middle attack
  - User interface attacks
  - TLS Null-prefix attack
- **Governments**
  - Bypassing storage encryption
  - SSL interception attack
  - Hidden backdoors and unnoticeable software changes
- **Service Providers**
  - Exploiting user data
  - Data leaks through employees of service provider

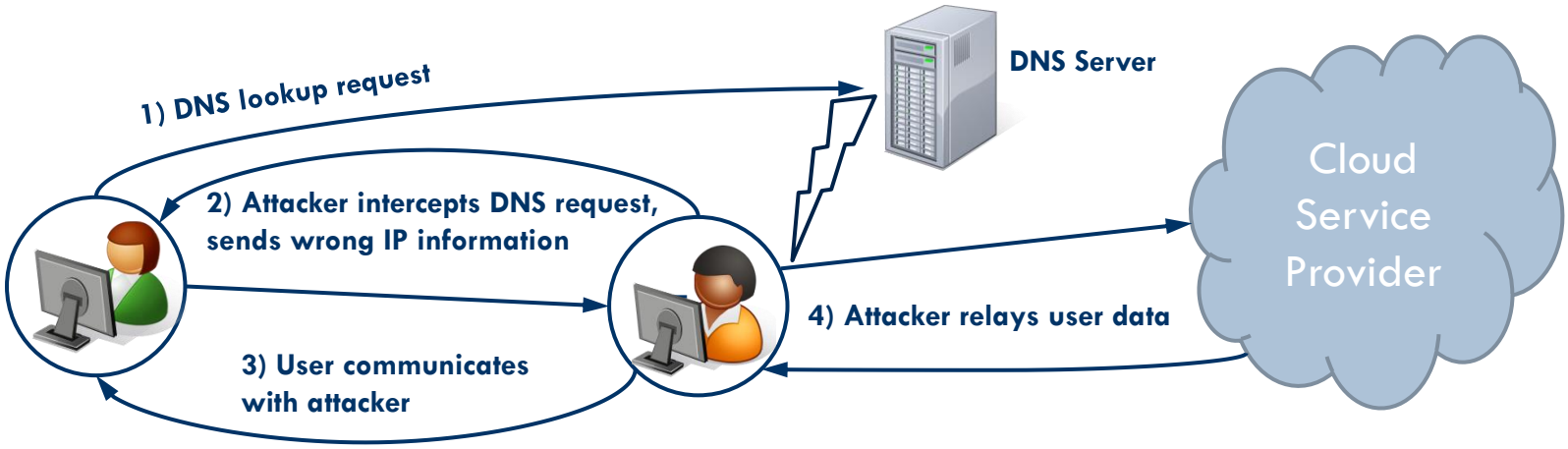
Session Hijacking

- Most providers are offering HTTPS / TLS only for login
- After the login an attacker can intercept the traffic, capture session cookies and also transferred data
- Attacker has full access as long as the user is logged in
- Economic issue: HTTPS needs more processing power, additional hardware to maintain service quality
- No demand for HTTPS due to a lack of information



Man-in-the-Middle Attack

- Login page is plain HTTP, only login data is transferred via HTTPS
- Attacker can intercept and redirect traffic and show the user a different login page
- Forging DNS packets, DNS cache poisoning, ARP spoofing
- Attacker then gets the plaintext login data without notice of the user (it is only http) and establishes a https connection with the service
- Attacker decrypts the data from the service and sends it to the user



User Interface Attacks

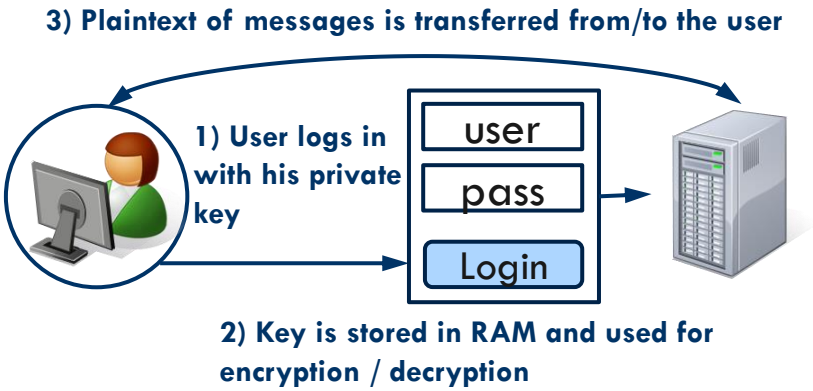
- Cloud applications are accessed using a web browser
- Browsers tend to store user data including browsing history, passwords and other sensitive information
- Exploiting browser software vulnerabilities
  - Tricking browser to show a fake URL
  - Reading browser cache
  - Tricking browser to insert auto-complete data
- Fooling users to think a fake website is the real one
- Faking https lock icon
- Homographic attacks with international characters looking like national ones

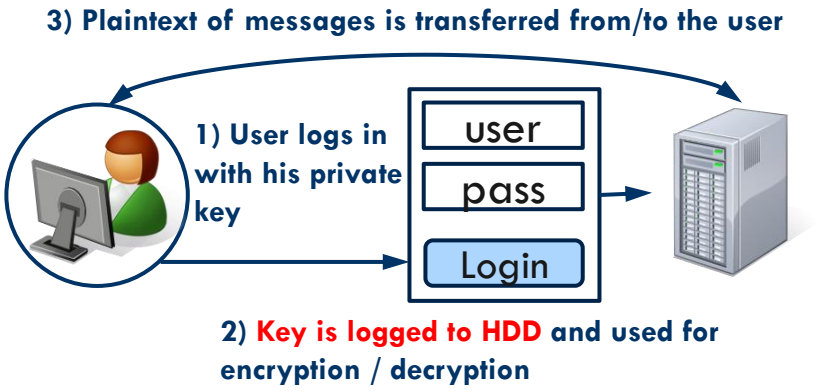
Bypassing Storage Encryption

- Provides a certain protection against insider attacks
- Not widely used because no consumer demand
- Different options where to store the key
  - Only the user has the encryption key
  - Only the service provider or both have the key
- In the second case the service provider can decrypt the users data
- Can be forced by the government to hand over the key, also without informing the user
- Key entered on a web interface or software provided by the service provider → might get to know the key

Case Study - Hushmail

- Providing a secure, encrypted mail service (PGP)
- Offering server-side and client-side encryption
- Law enforcement wanted to look at a drug dealer's emails who used server-side encryption
- Ordered Hush to record the passphrase after the dealer entered it on the web interface
- Also client-side version would not have helped him → provide an applet containing a back door



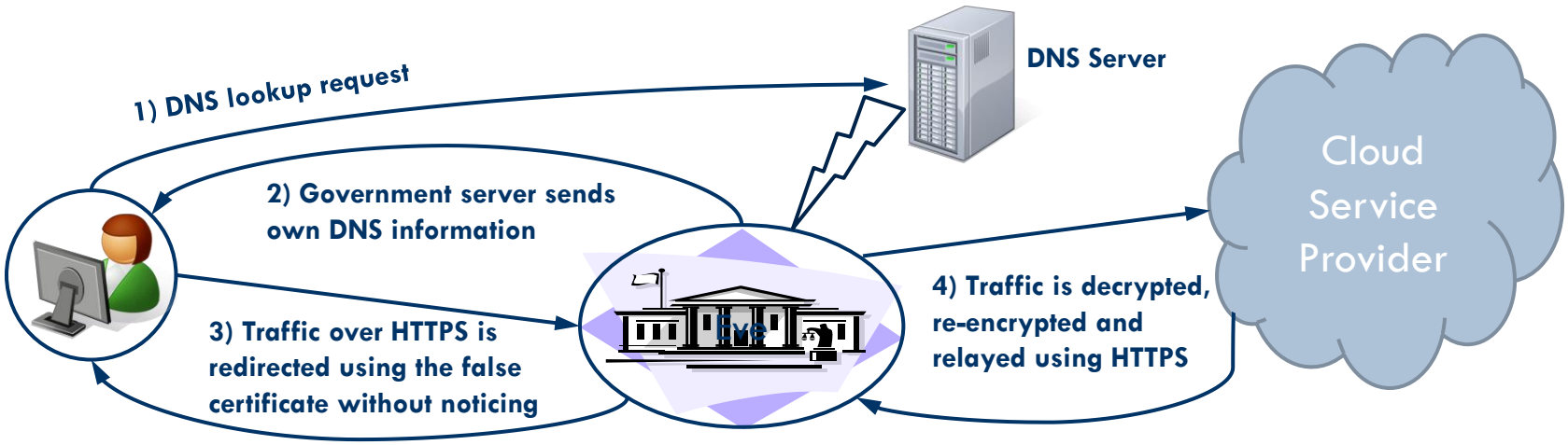


SSL Interception Attack

- SSL/TLS relies on a chain-of-trust involving several CAs (Certificate Authorities) verifying a servers certificate
- Browser vendors trust the root-CAs
- Compelled certificate creation attack
- Technically it is possible for a CA to issue a certificate for a site which has already obtained a valid certificate
- Governments either own CAs or force them to issue false certificates (also intermediate certificates)
- Users traffic is redirected using DNS or ARP spoofing
- Enables silently and covertly intercepting traffic and reading user's data
- Specific devices exists, e.g. Packet Forensics 5-Series

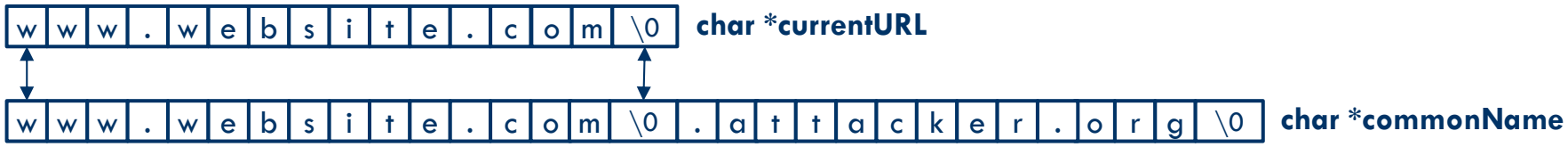
SSL Interception Countermeasures

- Firefox plugin CertLock[7]
- Caching certificates and comparing the current certificate with cached one on country level changes
- If no country change, attack is not detected
- Most certificates are issued from US CAs
  - Attacks from US government cannot be discovered



TLS Null-Prefix Attack

- Website hostname specified in Common Name (CN) field
- CAs verify ownership of the domain name specified in the CN field
- CN field is a Pascal string, different from a \0 terminated C string, TLS implementations are in C
- CN: www.website.com\0.attacker.org
- Will be signed by CA (ignoring the \0)
- Browser implementation of string compare only compares until it reaches \0, so validates the certificate for www.website.com




```
char *currentURL = getDomainWeAreConnectingTo();
char *commonName = getCommonNameFromCertificte();
bool verificationOK = (strcmp(destination, commonName) == 0);
```

Hidden Backdoors

- Regular software products require updates to be installed manually → slow adoption rates
- At least the user is able to check if an update has been performed
- Cloud software can be updated without anyone noticing
- Installation of hidden backdoors is much easier
- In addition a specific user can be provided with a specific version of the product while all other users still use the original one
- If only one user has the compromised version the chance that someone notices is very low

Case Study - JAP

- JAP – Java Anonymous Proxy
- German government forced developers to introduce a hidden backdoor which logs accesses to illegal web sites
- As it is open source, a user discovered the change
- Open-source software cannot be easily modified without someone noticing
- No technology exists to protect a company from executing a lawful order compelling to insert a backdoor into its product

Cloud Service Provider scanning data

- Most providers offering a free service are earning money by showing highly personalised ads
- Mining users private data, searching for keywords, provide these to third party companies which then place ads on the web interface
- Statistics and behaviour predictions
- Storage encryption is against their business model (monetizing user's private data)
- Users would not even pay for enhanced privacy

User attitudes and beliefs

- Users expectation of privacy
- Misconceptions about the rights and guarantees the service provider offers
- Users still consider local storage safer than the cloud
- Physical protection is considered more secure than encryption
- Users do not use the cloud as main storage
- Storing only less “sensitive” data
  - Different perception of “sensitive” data
- Loss of control over their data
- Agree to pay more for better privacy

Perceived Privacy and ToS

- Understanding of cloud infrastructure is rather limited
- Users do not read privacy policies
- Assuming higher availability, integrity, ownership guarantees and privacy protection
- Unaware of unauthorized modification, delayed deletion, arbitrary account disabling and data loss liability
- Users consider the internet as highly insecure
- Easy for hackers to access their data
- Storage provider and governments might access their data
- Data is not interesting so the practical risk is only minimal
- Unaware of the actual privacy risks they are exposed to

National differences

- **Switzerland**
  - Privacy is guaranteed by the constitution
  - Government monitoring is considered as a fundamental privacy infringement
  - Swiss are more privacy aware than Indians
  - Everybody should have the right of privacy, including terrorists
- **India**
  - Privacy is not explicitly recognized
  - Regard surveillance as necessary in combating terrorism
  - Tap-proof technology should not exist because it would be misused

Countermeasures

- Using HTTPS/TLS by default
  - Providers should be required by law to use HTTPS
- Using DNSSEC
- Homomorphic encryption
  - Encrypted data can be processed
- Encryption done independently by the user
- Single Site Browser
  - Web Browser just for a single cloud application
- Web application fingerprinting
- Using open-source software

Summary

- Data stored in the cloud has a higher risk of being accessed by unauthorized individuals
- Providers have no incentives to provide better security and privacy for economic reasons
- Governments also have a legitimate need to access data
- Governments around the globe have several legal ways forcing cloud providers to disclose users personal data
- Compelled backdoors are a serious problem
- Storage encryption is no magic bullet

End

Thank you for your attention

Questions?

“Cryptography is typically bypassed, not penetrated.”,
Adi Shamir

Literature

(1) SOGHOIAN, Christopher. Caught in the cloud: Privacy, encryption, and government back doors in the web 2.0 era. *J. on Telecomm. & High Tech. L.*, 2010, 8. Jg., S. 359.

(2) ION, Iulia, et al. Home is safer than the cloud!: privacy concerns for consumer cloud storage. In: *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 2011. S. 13.

(3) BORGMANN, Moritz, et al. On the Security of Cloud Storage Services. *Fraunhofer Institute for Secure Information Technology-SIT, Tech. Rep. SIT-TR-001*, 2012.

(4) SOGHOIAN, Christopher. *THE SPIES WE TRUST: THIRD PARTY SERVICE PROVIDERS AND LAW ENFORCEMENT SURVEILLANCE*. 2012. Doctoral Dissertation. Indiana University.

(5) ROBISON, William Jeremy. Free at What Cost: Cloud Computing Privacy under the Stored Communications Act. *Geo. LJ*, 2009, 98. Jg., S. 1195.

(6) KATZAN JR, Harry, et al. On the privacy of cloud computing. *International Journal of Management & Information Systems (IJMIS)*, 2011, 14. Jg., Nr. 2.

(7) SOGHOIAN, Christopher; STAMM, Sid. Certified lies: Detecting and defeating government interception attacks against ssl (short paper). In: *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2012. S. 250-259.