Technical security demands for corporate cloud / SaaS services

Both cloud computing and SaaS introduce a variety of security risks for their users/clients. Some of these risks are novel, however the majority are typical security concerns of working in multiuser environments, delegating data to third parties and outsourcing, web applications and remote access security, and so on. The CSA Guidance covers management, legal, regulatory, compliance, audit, electronic discovery and incident response areas very well, here we would like to expand on more technical aspects of cloud computing and SaaS services security, starting from the specific issues and threats and finishing with an extensive safeguards and countermeasures checklist.

More specific cloud and SaaS technical security risks include:

Security baseline degradation

Many companies and organisations do take proper care and have invested plenty of time, resources and effort into building their ISMS, hiring security specialists, acquiring security appliances and applications, training personnel and so on. They have also built strong relationships with trusted third party security providers, for example 3rd party penetration testers. For such companies, it makes no sense to switch to a less secure environment just because it's fashionable or can potentially reduce future operational costs. In fact, any estimated savings would be weighted against the previous spendings on security that can simply go astray after the transition to cloud or SaaS. From the risk/benefit analysis perspective it makes no sense to abandon efficient working safeguards to compensate for such costs in a few years via lower cloud/SaaS costs, while exposing the company data and operations to reduced level of protection and increased security incident risks. We won't even mention the obvious compliance and trust issues that come with it, since they aren't exactly technical. The bottom line: a cloud or SaaS provider must convince the customers that it's security baseline is not below their currently existing level. Having the policies in place is clearly not enough – the provider must come up with the goods and demonstrate that their intrusion prevention, encryption, access control and authentication, secure backup and data elimination, and other relevant safeguards are by no means weaker than their counterparts already deployed by a prospective customer. Thus, a thorough technical analysis and comparison of all relevant security controls is an absolute requirement. It will also give a great chance to weight the level of security skills and knowledge of the company's specialists or trusted third party consultants versus their cloud/SaaS provider colleagues. And if the latter are clearly inferior, entering the deal must be out of question.

SaaS phishing and pharming

SaaS enables somewhat novel phishing opportunities. Scammers can emulate at least some popular SaaS applications in order to harvest identities and other sensitive data. The emulation can be done with different levels of depth, from deploying a simple fake graphical interface or installing the actual application (if available) on their site, to setting up a rogue fake (or even fully registered – we are well aware of one such highly suspicious case!) company for the purpose of valuable data theft, fraud and further processing. Remember, that in the past social engineers did go quite far in their attempts to gain access including getting employed by the target company. We can also recall rogue Autonomous Systems and whole ISPs being set up, as in the most recent Pricewert LLC case. Delegating valuable information to SaaS applications is akin to putting your money in a bank, however even a purely online bank cannot be easily set up by a “two men and a dog” team. While such an adventurous rogue SaaS setup would be easily discovered by professional in-house or third party investigators working for large companies or government, individual users and even SME's can easily fall into the “our cutting edge technology is fantastic, just sign for a completely free testing account, provide us with your e-mail, phone, etc. and install a helpful browser plugin” trap. Or, with an assistance of a client-side web exploit, the “helpful plugin” can always install itself, without your permission. So far, we have seen anti-phishing SaaS, but no elaborate SaaS anti-phishing.

SaaS and cloud man-in-the-middle attacks

Apart from emulating SaaS application logins and cloud entry points the attackers can try to hijack access to the existing legitimate ones. We are not going to say that “we use SSL/TLS” won't prevent

such attacks, but it may not always stop them. Taking into account that the clouds or online applications used by thousands of users are incredibly attractive targets, consider the following opportunities:

- many SSL/TLS server-side configurations allow a remote downgrade to SSLv2 and use of weak ciphers (MD4 anyone?)
- in February 2009 an efficient man-in-the-middle attack that hijacks transfers from SSL-unprotected to SSL-protected sites was demonstrated
- attackers can sign a fake certificate down the certificate chain with a fully valid one. The client-side application may not verify the whole chain, as it theoretically should do
- old Omen-style attacks may still work
- many users will still eagerly click through all the suspicious certificate warnings without giving it a second thought, as the use of expired or erroneous certificates is unfortunately abundant

Besides, when performing security audits we have often seen insecure cookies transmission despite the established secure SSL channel and a great deal of other serious misconfigurations. Thus, depending on the multitude of factors, SSL/TLS can provide strong security, or strong false sense of security with all the easily predictable negative consequences. Generally, IPSec provides a more secure alternative while being more cumbersome to configure (and remember to stay away from the aggressive mode!)

SaaS and cloud DDoS

In the past, the main targets for DDoS racket gangs were various online retailers and the Internet gambling industry. These days any company or organisation whose business processes strongly depend on cloud and/or SaaS joins this list of primary targets for obvious reasons. Of course, the cloud/SaaS provider must demonstrate their readiness to handle various DDoS types. However, the major threat is DDoS attacks against the company itself rather than the provider, which creates a paradox. Moving your operations to the cloud means that you have to boost your on-site DDoS defences, not lower them as many might think believing that the responsibility is shifted to the cloud provider. If you didn't have any strong DDoS safeguards prior to moving to the cloud as it wasn't considered a significant threat, now it is time to get very concerned. And this, of course, means additional on-going costs to be taken into account at the decision making stage. Since the main threat is a “client-side”, rather than the “server-side” DDoS, there are some peculiarities that should be noted and thought about:

- the randomization of ports used by SaaS client-side applications becomes highly important
- in order to withstand DDoS, multihomed load-balanced connection to the Internet becomes a minimum requirement
- the attackers are likely to spoof addresses of your SaaS vendor external IPs, external DNS and other servers as sources of the assault to make it more efficient and turn any automatic shunning to their advantage

non-generic SaaS DoS and local exploits

In the environment shared by multiple users that may belong to different companies or organisations every application error, whether maliciously induced or accidental, becomes critical. The applicability of local exploits becomes much wider, and if free testing, public or other easy-to-obtain form of access is provided they will be inevitably used against the SaaS application or cloud systems. Thus, the requirements for such applications and systems security testing at all development stages from policies design to UAT become far more stringent. Strong fool-proof controls must be built in and thoroughly verified, as an error that could be highly unpleasant for a single user in the past can now easily ruin the day for thousands of affected users. The controls against any type of privilege escalation attacks must be just as strong.

SaaS and cloud data leaks

In the cloud data (and metadata!) leaks can occur at multiple points, including but not limited to:

- leaks between standalone files bypassing file permissions
- leaks between directories and directory trees
- leaks between user accounts
- leaks between application instances and associated network services
- leaks between sandboxes and virtual operating systems
- leaks of multiple data streams sharing the same network path
- leaks at backup, centralized logging and other common storage points

Thus, management of permissions in vast environments with thousands of users and millions of files becomes a serious issue highly prone to human error. It has to be automated, and automated securely. But even than the common OS file and account permissions will not prevent all such leaks from happening, even if configured correctly.

delegating data to vulnerable client-side applications

The vast majority of modern SaaS is using common Web browsers as client-sideapplications. This situation is unlikely to change. Web browsers are probably the most frequent targets of today due to abundance of XSS, CSRF, URL redirection and other similar attacks that use server-side applications insecurities to steal cookies, access information in the browsers cache and so on. In a nutshell, modern SaaS easily delegate sensitive data to probably the most insecure common user-end application one can think of. Writing more protected proprietary SaaS client-side applications is viewed as daunting, cumbersome and unnecessary by many, especially startups looking for quick profit and development savings. However, it should be considered for higher security environments and, perhaps, taken into account when future security standards and compliance requirements for SaaS are defined.

Cloud and SaaS countermeasures and safeguards checklist

To reduce these and other security risks we have compiled an extensive checklist that can be used by prospective customers to evaluate the security level of SaaS and cloud providers. Since we don't live in the ideal world and the technology itself is rather novel, we do not expect that all the points on the list would be successfully met by the vendors. The key here is thorough matching of your current security demands, procedures and infrastructure with those of the evaluated provider, and prioritisation of the available countermeasures with a possibility of minor acceptable sacrifice of the low priority ones. Scalability and planning in advance must be taken into account: if you wish to implement two factor authentication and single sign-on in the future but you SaaS provider does not support it properly or works with specific vendor solutions only you'll have to think carefully.

Authentication and access control:

- two factor authentication support, including SMS-based schemes. Ideally, already existing and operational two factor authentication solutions deployed by client companies must be accommodated for.
- strong centralised password policy enforcement (although it is better to completely avoid traditional login/password authentication in cloud environments)
- secure mutual authentication scheme (e.g. DH)
- protection of secure certificates and passwords on servers, client computers and in transmission
- single sign-on support and integration with the existing singe sign-on solutions already used by client companies
- efficient and secure login credentials recovery or change for large numbers of users
- the ability to filter login attempts by their source IP ranges (optional, but desirable)

Encryption:

- data must be encrypted both in transmission and when stored in the cloud
- ideally, sensitive data processed by SaaS applications should be also encrypted on a user host, e.g. in the browser cache
- selection of strong ciphers and key sizes
- separate per account and per application key options
- secure key management procedures: keys storage, deletion and recovery, escrow and key encryption keys. Key management in the cloud is particularly difficult since the provider would have to manage the use of keys on all servers where the applicable data is dynamically stored
- verification and avoidance of issues that can arise from international use of ciphers and various import/export restrictions on cryptography

Data segmentation:

- data segmentation in the cloud must be at the very least as secure as the segmentation previously applied for such data in private systems and networks
- political issues and conflicts (such as direct competitors data stored on the same physical and logical medium) must be avoided
- secure data segmentation should be applicable for a separate client within their acquired services and resources (to distinguish between data classification levels, users and groups of a single company or organisation)

Data transmission:

- all sensitive customer data transmitted to, from and within the cloud must be encrypted and it's integrity must be preserved via strong message digests
- transmission security protocols must prevent man-in-the-middle attacks
- transmission security protocols must prevent session hijacking attacks
- political issues (data passing through undesirable Autonomous Systems and geographical locations) must be controlled and avoided

Data availability

- sufficient scalable bandwidth
- multiple redundant links to different ISP's connected to multiple Autonomous Systems
- evidence of sufficient anti-DDoS protection (appropriate policies supported by specialised anti-DDoS solutions and/or appliance capabilities, such as CAR and NBAR)
- verified operational stability of the SaaS applications
- load balancing with your cloud provider or multiple cloud providers
- fail over between several cloud providers

Data elimination:

- secure simultaneous instant deletion of data within the whole cloud
- data elimination in the cloud should be at least as secure as it's elimination previously applied for such data in private systems and networks
- secure elimination of data processed by SaaS applications on end-user hosts running different operating systems, browser versions etc.
- cloud/SaaS provider hard drives disposal method must match the methods used by the customers

Data backups:

- regular incremental backups
- proper version control of backups
- geographic distribution of backups to provide real incident and disaster resilience
- clients must be able to choose the preferred backup medium and location
- strong encryption of backups matching the encryption methods applied to the original data
- segmentation of backups must be as secure as the original segmentation of the backed-up data
- political issues and conflicts (such as direct competitors data backed up on the same physical and logical media) must be avoided
- the ease and security of recovering the needed data from backups

Audit trails:

- real time provision of log data to customers
- customers must be able to select the reporting level and scope of the logs they receive
- per user, per application and per system (PaaS or IaaS) logs
- generated logs must include user authorisation and accounting data
- strong protection of logs integrity and timestamps with appropriate message digests
- protection of all log data in transmission inside and outside the cloud
- rapid reaction to customer requests based upon their revision and analysis of logs (for example, discovered intrusion attempts and user misbehaviour, or SaaS applications errors and crashes)
- secure storage and backup of logs

SaaS software security:

- the provider must be able to produce sufficient evidence of security awareness, implementations and controls of it's SaaS application development cycle
- where possible, the SaaS application should be security certified (Common Criteria etc.)
- SaaS applications security must be thoroughly tested by an independent third party. The outcome of such assessments should be available to customers when requested
- SaaS application security assessments must include thorough input fuzzing, other forms of stress and resilience testing and, where possible, source code reviews
- SaaS application security assessments must be regular and synchronized with change control procedures of the provider
- SaaS providers must inform their customers about major security problems with their SaaS applications and measures taken to mitigate these problems

General infrastructure safeguards:

- security safeguards deployed by a cloud/SaaS provider should never be weaker than their counterparts used by customers prior to subscribing for the service. This applies to a variety of safeguards including, but not limited to
    - firewalls
    - IDS/IPS/single host IDS
    - antimalware solutions
    - content filters and other controls
    - anti-DDoS solutions
    - VPN solutions

Remember, that this checklist is only an add-on to standard information security verification procedures, such as background checks, evaluating vendor's policies and third party agreements and connections, and so forth.