

# Protecting Your Weakest Point: On-Premise Resources

By Yuri Diogenes – ISSA member, Fort Worth, USA Chapter – and Deb Shinder

**Organizations must understand that migrating to the Cloud does not mean you can just put your trust in the cloud provider and treat security as “somebody else’s problem.” The authors describe a “defense-in-depth” security approach that operates from the edge to the endpoint.**

## Abstract

Recent high-profile incidents raise serious questions about the current state of security on the Internet. This comes at a time when many companies are moving, or considering a move, to the Cloud; but companies need assurance that their digital assets will be safe. Organizations must understand that migrating to the Cloud does not mean they can just put their trust in the cloud provider and treat security as “somebody else’s problem.” Attackers will exploit vulnerabilities whenever and wherever they can find them. Regardless of the level of security that the cloud service provides, it is still up to the cloud consumer to protect one of the weakest links in the chain: on-premise resources. The best way to do that is with a “defense-in-depth” approach that operates from the edge to the endpoint. This way, even if elements of the security chain outside your control are compromised, you can still ameliorate the damage and protect your most vital resources.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS), its newer incarnation, are standard cryptographic protocols when it comes to securing transactions over the Internet. However, many companies and individual users around the world have been questioning how secure SSL really is,<sup>1</sup> and the concern became even more urgent after the recent attack against several registration authority (RA) affiliate accounts of certification authority (CA) Comodo last March.<sup>2</sup> Fraudulent SSL certificates that had to

be revoked included those for sites belonging to Google, Yahoo, Mozilla, and other major companies. This brought into question the entire CA model<sup>3</sup> – a model that has served as the foundation of trust for Internet users and the sites with which they conduct business transactions.

While this is a legitimate and serious question, there is much more to be discussed than simply the SSL technology itself. As companies are relying more on services providers by offloading their on-premise IT services to a cloud-based infrastructure, many of them fail to understand that the need for an on-premise security infrastructure is still very high, perhaps even more so than in the past. But this is not the only issue that companies will have to address. Policy enforcement is a vital element in making sure that both the company and its users are protected against vulnerabilities that can be exploited in provided services. On the other hand, when you tie these elements together and you undertake to strengthen your company’s security, the debate about privacy in the workplace inevitably comes back to the table. A balance must be achieved by which organizations can protect their assets while preserving the privacy of individuals. These are some key challenges that companies will have to deal with in a more connected ecosystem where the Internet is going to be part of a company’s core business.

## A Matter of Trust

When something such as the Comodo incident happens with a certification authority and its affiliate registration authorities, it upsets many long-held beliefs about security and in-

1 References: [http://threatpost.com/en\\_us/blogs/phony-ssl-certificates-issued-google-yahoo-skype-others-032311](http://threatpost.com/en_us/blogs/phony-ssl-certificates-issued-google-yahoo-skype-others-032311); [https://www.secure128.com/comodo\\_certs\\_hijacked.aspx](https://www.secure128.com/comodo_certs_hijacked.aspx).

2 Comodo Incident Report can be found at <http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html>.

3 References: <https://blog.torproject.org/blog/detecting-certificate-authority-compromises-and-web-browser-collusion>; <http://arstechnica.com/security/news/2011/03/how-the-comodo-certificate-fraud-calls-ca-trust-into-question.ars/2>.

stigates a bigger wave of questions regarding the current state of the Internet's infrastructure security.<sup>4</sup> Many organizations have determined that online services are the way to go for reasons that are beyond the scope of this article. However, there is an all-too-common misconception that this scenario will also offload the company's responsibility to be diligent in securing its own on-premise resources. For example, many are under the impression that after you migrate to the Cloud, you do not need to be concerned about endpoint protection; or because they are in the Cloud, they do not need perimeter protection. That is absolutely not the case. This misunderstanding goes hand-in-hand with an excessive amount of trust in the technology, i.e., the belief that because transactions are taking place using SSL, everything will be fine. This misplaced trust encompasses several factors:

- Trust that your CA is diligent about keeping its infrastructure secure, so you should not be concerned about it.
- Trust that because your service provider uses two-factor authentication, nothing bad will happen.
- Trust that your users will take standard precautions to prevent their own machines from being compromised.

This chain of misplaced trust goes on until one link fails and you realize that you did not do your homework to protect your own assets. At this point, you might be asking, "but why are you pointing the finger at me if they were the ones who failed?" Let's look a little more closely at the chain and you will see why you are the target.

The Internet momentum behind cloud services is resulting in a new trend, where attacks are going to increasingly target services providers and authentication mechanisms. This is inevitable, because these providers comprise a large attack surface and this is where the attacker gets the most "bang for the buck." Here's an analogy: in the real world, terrorists prefer to go after big targets such as a major event (e.g., a Superbowl game) or a place where large numbers of people are gathered (e.g., the Trade Center Twin Towers). There are two reasons for this: population density means they can do more damage, and the location is more difficult to protect. Because there are many people coming and going, there will be more possible avenues by which an attacker can infiltrate.

But in looking at the Comodo incident, the greatest damage from such an attack does not happen when the RA is compromised. The real damage will occur when attackers start to direct forged/illegitimate credentials against users in order to steal their information. A core security principle will be come into play at this point: the less secure element(s) in the chain will be exploited. In other words, breaking the security of an

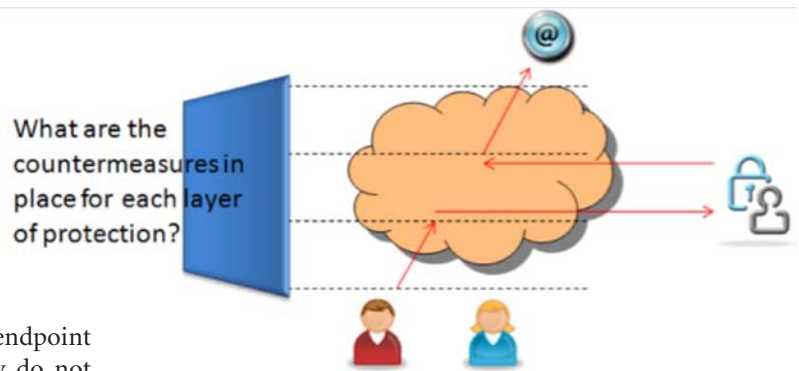


Figure 1 – The multilayer of protection approach, also known as defense-in-depth, is more essential than ever.

RA system and forging certificates is only the first step in the plan; the next and more important step comes when users start to log in with their credentials on sites that are using the compromised certificates and a man-in-the-middle attack takes place, stealing those users' information. This damage can be irreparable. Clearly the user is the most fragile element in this chain.

When companies are planning their security policies with the objective of avoiding scenarios such as described above, they should not focus only on the technologies used to protect the users' and company's assets from potential damage. They also need to address these additional factors:

- Privacy issues
- Security awareness program
- Policy enforcement

We'll look at each of these in a little more detail in the following sections.

## Privacy issues: We will inspect your traffic

In the United States, each state has its own regulations regarding the privacy rights of employees using workplace computers and networks, but the core principle is the same: if the employer monitors employee network activities and/or reads employee data traffic, the company should make the employee aware that the traffic is being inspected and ensure that each employee signs an agreement, stating that he is aware of this policy. This should be part of your security policy and your security awareness program.

In addition, it is also a good practice to encourage this awareness through other venues, such as banners, email messages, dialog box warnings that display when users are browsing Internet, etc. The balance is achieved by properly holding companies accountable for keeping users' records in a safe place. Organizations should be transparent with the users about data collection (how the data is collected and for what purpose) and provide clarification about potential scenarios in which the data will be disclosed. While inspection is necessary, it should never open a breach on a user's data privacy.

4 Reference: <http://www.eweek.com/c/a/Security/Fake-SSL-Certificate-Incident-Highlights-Flaws-in-DNS-Comodo-CEO-440985/>; <http://www.usnewsลาสвеegas.com/foreign/%EF%BB%BF%EF%BB%BFbi-probes-breach-into-internet-security-firm.>

## Security awareness training: We're all in

Security awareness training for all employees should cover the following topics:

- Security concepts and terminology
- Employee responsibilities in handling of sensitive company information
- Identity theft prevention
- Safe web browsing and email practices
- Key vulnerabilities and threats
- Viruses and malware
- Phishing
- Social engineering
- Physical security
- Security for mobile devices and remote workers
- Password management and two-factor authentication
- Firewalls
- Acceptable use policy

Security awareness training should be standards-based. Many companies use the ISO 27002 standard covering information security best practices, as it is internationally recognized. If your organization is part of a regulated industry, such as financial services, health care, or retail, training should include the applicable industry standard (Gramm-Leach-Bliley, HIPAA, PCI). Another useful guideline is the NIST/FISMA security awareness and literacy framework.

The training should take place at least once per year to ensure that new threats and potential countermeasures are covered in the training. You can conduct the training with in-house instructors or you can contract with one of many companies that provide security awareness training. For example:

- SANS offers a number of free and paid security awareness training courses, as well as papers on security awareness training<sup>5</sup>
- The FEMA Federal Emergency Management Institute provides an interactive web-based course on workplace security awareness<sup>6</sup>
- Private IT education companies such as Global Learning Systems offer a variety of security awareness programs<sup>7</sup>

## Policy enforcement: Be diligent

After the security policy has been adjusted to cover privacy issues and to mandate security awareness training, it is important to ensure that employees are required to comply with those policies. At a minimum, policy enforcement should include the following elements:

- Ensure that only authenticated and authorized users are able to access corporate resources
- Scan user workstations, laptops, smartphones, tablets, and any other devices upon connection with the corporate network to ensure that each device complies with the minimum security profile (e.g., has up-to-date antivirus signatures, OS and applications are fully patched, host-based firewall is enabled and properly configured, etc.)
- Enforce network-based access controls to protect corporate resources and control Internet usage, and enforce on-site access controls to protect the physical resources within the organization's premises
- Be sure to implement appropriate mechanisms to prevent data leakage in the company's network (e.g., by employing an identity management system)

Different vendors offer many different solutions to assist with policy enforcement. The most important point to consider when planning your policy enforcement approach is to make sure that it is effective and fits the corporate needs.

## Protection from the edge to the endpoint

In a common scenario, a user tries to access his email, which is located in a cloud service solution. Our first step is to perform a risk analysis so we can provide edge-to-endpoint protection. This involves answering the following questions:

- What are the steps involved in this simple access?
  - 1 – User will connect to the cloud provider, authenticate, and send the email.
  - 2 – Cloud provider's email server will authenticate the user, scan the message, and route the email to the destination server.
  - 3 – Destination server will receive the email, perform the appropriate scan, and notify the destination user that a new message arrived.
- What are the potential risks that can be mitigated?
  - 1 – Workstation: a breach in the user's workstation due to an operating system or application vulnerability that was exploited because a patch was not applied could compromise the system; malware installed on the user's workstation because the user opened a malicious email attachment could compromise the system; attack code that gets through because a user clicks a malicious hyperlink in an HTML email message could compromise the system.
  - 2 – Information in transit: Data could be intercepted in transit and a security breach could occur because it was not encrypted.
  - 3 – Cloud provider: Breaches in the cloud provider's authentication, authorization, or validation systems could allow hackers to access and compromise user data. Internal threats from the cloud provider's personnel could result in compromise of user data.

5 SANS [http://www.sans.org/security\\_awareness.php](http://www.sans.org/security_awareness.php).

6 FEMA <http://training.fema.gov/EMIWeb/IS/IS906.asp>.

7 GLS [http://www.globallarningsystems.com/products/security\\_awareness\\_training](http://www.globallarningsystems.com/products/security_awareness_training).

- What technologies and policies should be in place to assist in mitigating those risks?

- 1 – Ensure that every workstation and all network-connected devices are required to be fully patched and that they all have endpoint protection such as antivirus, personal firewalls, and a properly hardened configuration.
- 2 – Employ multiple layers of inspection throughout the communication channel within the company's network as well as on the cloud provider's network.
- 3 – Verify that your cloud provider employs mechanisms to mitigate the risks that were highlighted above. Appropriate data governance while moving to the Cloud is an important point to consider.<sup>8</sup>

There will be a variety of other questions that will come up when you analyze such situations, which is normal and desirable. The more questions you have, the more prepared you will be to tackle potential issues.

<sup>8</sup> Read this document: "Moving to Cloud Computing" at <http://go.microsoft.com/?linkid=9740995> for more information about data governance consideration while moving to the Cloud.

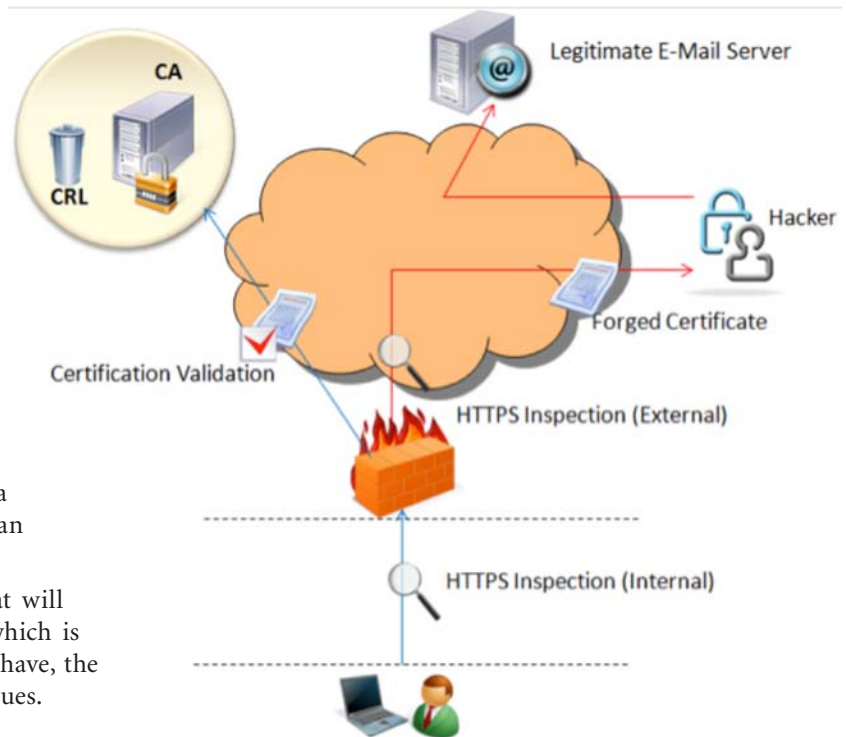


Figure 2 – HTTPS inspection assists in mitigating potential flaws in the validation process

HTTPS inspection assists in mitigating potential flaws in the certificate, as shown in Figure 2. In this scenario, the client workstation is performing the SSL handshake using a forged certificate (issued by a hacker masquerading as a legitimate CA). The edge protection system intercepts this request and sends a validation request to the CA. When the CA replies back, confirming that the certificate is not valid (forged certificate), the edge protection system will block the request and prevent the traffic from going to the destination email server (thwarting the man-in-the-middle attack).

While this mitigation primarily uses the edge security system to stop the traffic, there are many layers of protection that should be in place to enhance the security in such scenarios. To better understand the defense-in-depth approach in this scenario, we will have a look at the on-premise components that are involved:

#### Edge: Web gateway with firewall capabilities

- Performs HTTPS inspection and certificate validation; has user-notification capability
- Performs multi-layer inspection for malware detection and potential vulnerability exploitation
- Has tracking and logging capabilities
- Enforces security policy changes once changes are applied
- Has caching capabilities to enhance Internet access performance and avoid an excessive amount of traffic that can overload the Internet bandwidth

## On Demand Webcasts

### Industry Webinars

#### Powerful Control of Privileged Users

Click [HERE](#) for details and registration.  
Sponsored by CA technologies.

#### WikiLeaks: The Gateway to Insider Threat

Click [HERE](#) for details and registration.  
Sponsored by Verdasys.

#### Databases Under Attack!

Click [HERE](#) for details and registration.  
Sponsored by Oracle.

#### Inside the Latest Web Threats: From Myths to Mechanics

Click [HERE](#) for details and registration.  
Sponsored by Sophos.

#### Identities, Access & Use - The Identity Management Trifecta

Click [HERE](#) for details and registration.  
Sponsored by CA Technologies.

#### Social Networking Forensics

Click [HERE](#) for details and registration.  
Sponsored by Stroz Friedberg.

Click [HERE](#) for a list of all industry webinars

[www.issa.org/Members/Webcasts.html](http://www.issa.org/Members/Webcasts.html)

**End user<sup>9</sup>**

- Employee consistently participates in the security awareness program
- Aware that the company is inspecting the traffic and signed an agreement covering that
- Aware of potential risks involved in browsing the Internet (phishing, spyware, viruses, spam, etc.)
- Aware of what is acceptable, under company policy, to disclose in social networks and other public or semi-public forums
- Knows how to avoid personal and company information leakage

**End point: Laptop or other device plugged into the network**

- Uses a data encryption mechanism by leveraging Trusted Platform Module (TPM)
- Configured to use multi-factor authentication via the user's credentials and smart card, token, or biometric information
- Operating system is fully updated by the company's patch management solution
- Antivirus and anti-malware software installed, fully updated
- Software validation policy in place to prevent the use of non-authorized programs
- Personal firewall enabled; correct exceptions configured
- Security policies in place to prevent changes to the operating system settings and use of external storage devices such as USB drives

**Network**

- Uses encryption protocols such as IPSec to protect data in transit
- Has an intrusion detection system and intrusion prevention system in place
- Has a network monitoring system configured to trigger alerts for active network elements (switches, routers and others)

<sup>9</sup> It is very important to understand the role of the end user in this scenario. Without proper security awareness training, the end user might not know about the differences between sites that are considered secure (using HTTPS) and not secure (using only HTTP). If the user is not aware of basic security terminologies (such as phishing, virus, malware and others), he will have difficulties dealing with potential phishing emails. If a user discloses too much information about himself on social media websites, an attacker can track the user's habits and initiate an attack by using a specially crafted email message that contains material that will persuade the user to perform a dangerous action, such as clicking on a link that opens a malicious web site.

Although there are obviously other on-premise elements that were not covered in this diagram (such as directory services accounts, password policies, and others), the point here is to illustrate that even in a high-risk scenario, a well-prepared company can still reduce the risk and avoid greater damage.

**Conclusion**

By accepting responsibility for the security of on-premise components that operate in conjunction with your cloud solutions, and adopting the "defense-in-depth" philosophy in regard to those components, you can reduce the risk that a compromise that occurs in external components will have a catastrophic impact on your organization. This layered approach to security helps you focus on each element and address its specific needs. Instead of only looking to the all-encompassing solutions (e.g. "let's all migrate to the Cloud"), as a security professional you will need to step back and evaluate both the security implications of the cloud services and the necessity for adequate security measures in the on-premise resources.

**About the Authors**

*Yuri Diogenes, CISSP, CIEH, Security+, MCSE+Security, former senior security support escalation engineer in the Forefront Edge Security Team at Microsoft, currently works as senior technical writer for the Windows IT PRO Security Team at Microsoft. Yuri is the co-author of the Microsoft Forefront Threat Management Gateway (TMG) Administrator's Companion from Microsoft Press and also co-author of the Forefront book series also from Microsoft Press. Yuri can be contacted at <http://blogs.technet.com/yuridiogenes> or you can also follow him on Twitter (@yuridiogenes).*



*Debra Littlejohn Shinder, MCSE and MVP in enterprise security, is a former police officer and criminal justice instructor who has, for the past fourteen years, worked as a self-employed network and computer security trainer, author, and consultant specializing in Microsoft technologies. She has authored or co-authored 26 tech books, edited technical journals and newsletters, and has published over 1000 articles in popular IT webzines and print publications. You can contact Deb via email at [deb@shinder.net](mailto:deb@shinder.net), follow her on Twitter (@debshinder), friend her on Facebook (Deb Shinder) or visit her website at [www.debshinder.com](http://www.debshinder.com).*

