AWS Load Balancers & End-to-End Encryption

by **R. DuPlain**

Summary

The organization must decide:

1. End-to-end encryption is from the HTTPS client to the EC2 *platform*, or
2. End-to-end encryption is from the HTTPS client to the EC2 *instance*.

Implemented as:

1. Application Load Balancer terminating HTTPS.
2. Network Load Balancer with HTTPS terminated at instance.

If (1), the organization is well-served to have a *reason* for the use of self-signed certificates on target groups other than "encryption is good." Otherwise, the practice of self-signed certificates is justified only by fear, uncertainty, and doubt.

Neither option of load-balancer-terminated (1) nor instance-terminated HTTPS (2) is automatically superior to the other. What (2) brings as a "more strict" interpretation of end-to-end encryption, (1) has in a hardened and highly available HTTP implementation with preset TLS configurations, in addition to AWS Certificate Manager's functionality in auto-renewing certificates and fine-tuning alternative domain names (SANs).

Regarding the HIPAA Security Rule, the U.S. Department of Health & Human Services does not strictly mandate encryption; its addressable in consideration of reasonable and appropriate safeguards. It's up to the organization to perform the risk assessment and manage accordingly.

Do (1) or (2), and do it decidedly.

Threat Model

- Bug in VPC mapping service in routing packets.
  - How is this different than a bug in EC2?
- Attach a rogue host to load balancer.
  - Requires compromised AWS credentials.
  - Self-signed certificates ostensibly address this threat, but would be ineffective because self-signed.
- Configure VPC Traffic Mirroring.
  - Requires compromised AWS credentials.

AWS Architecture

Overall

- EC2 instances are virtualized and so are packets on AWS networks.
  - Generally, the concept is *software-defined networks*.
  - Specifically, AWS has a mapping service checked by both the sender and the recipient in AWS virtual private clouds.
- Distrusting VPC categorically is equivalent to distrusting EC2 itself.
- Implementing HIPAA is risk-based, and hosting PHI on AWS is covered by BAA.

Software-Defined Network

"The short of it is that traffic simply can't be man-in-the-middled or spoofed on the VPC network, it's one of our core security guarantees. Instances, containers, lambda functions, and Elastic Network Interfaces can only be given IPs via the secure and audit-able EC2 APIs. In our security threat model, all of this API and packet level security is what plugs in the role performed by server certificates."

Colm MacCárthaigh (AWS engineer), 2018

References

- Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
- **Is the use of encryption mandatory in the Security Rule?**
- AWS HIPAA Compliance Whitepaper
- Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- Configuring end-to-end encryption in a load-balanced Elastic Beanstalk environment
- **Amazon VPC: the Picasso of Software Defined Networking**
- Abusing VPC Traffic Mirroring in AWS
- **AWS re:Invent 2015 | (NET403) Another Day, Another Billion Packets**
- NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say
- **Colm MacCárthaigh commentary (AWS engineer, note unofficial nature of this reference)**