Cloud-based Data Validation patterns…

DEEPSEC

We need a new approach!

Geoffrey Hill @GHill_security
Artis-Secure Ltd.

I like to think that tequila inspired this talk.

Tokyo 1999… a night to forget.

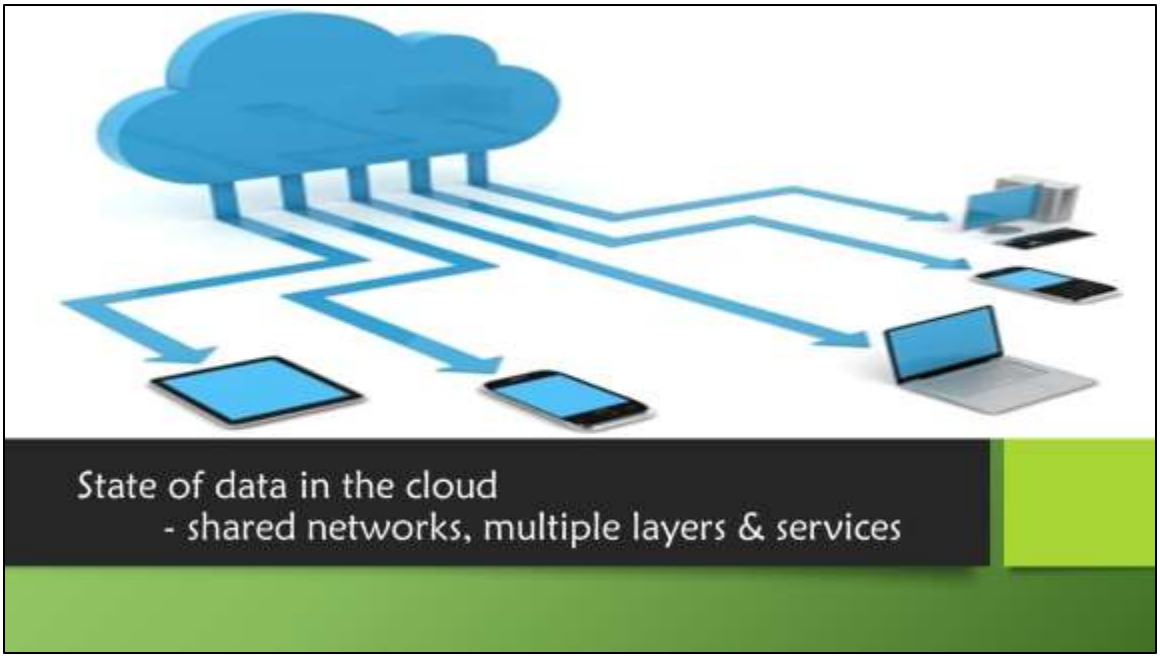
16 hours of waiting for the hangover.

I get the trampoline effect now.

How does this relate to Validation?

My body self-validates against tequila!

[**GIVE** AGENDA]



Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure.

Data will be exposed on:

multi-tenant environment storage

Spanned multiple layers in the cloud stack

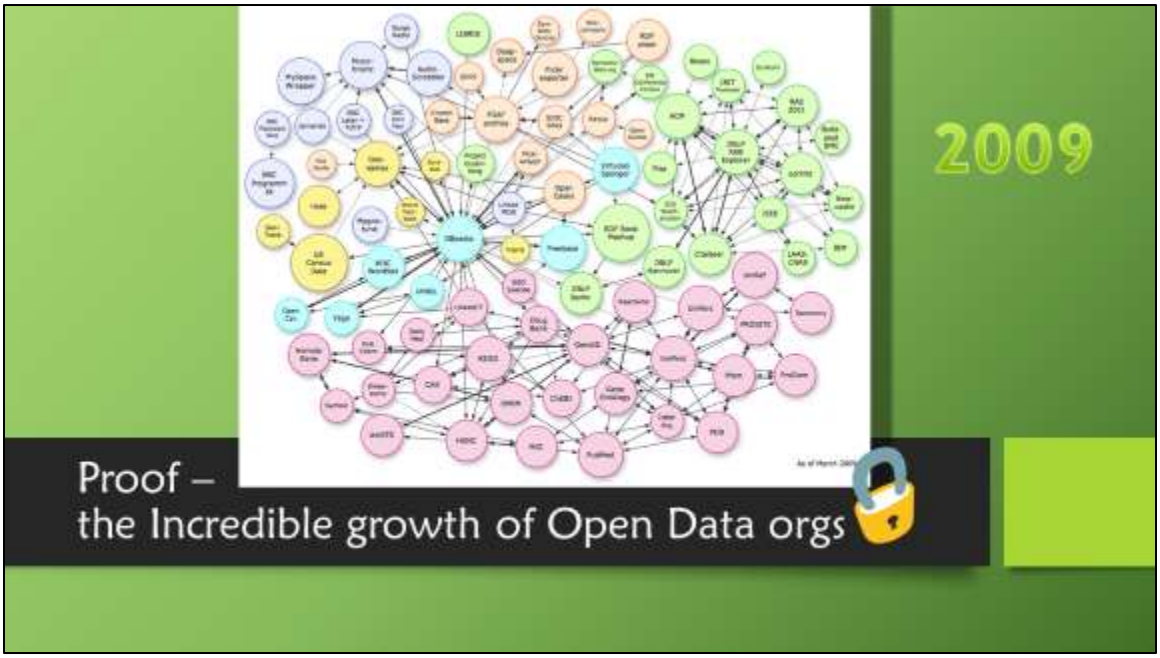
Platforms secured by multiple technologies and services

Authentication/authorization **and validation** technologies are becoming increasingly important.

Data will be exposed on:

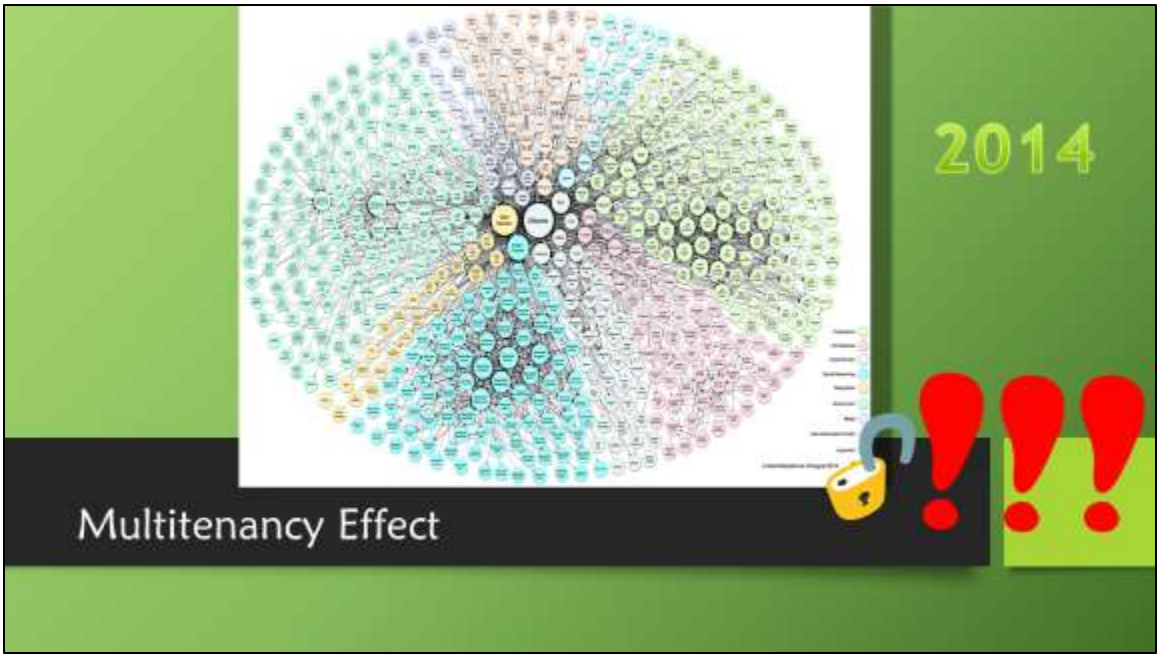
different trust levels, including anonymous, users, privileged cloud users

various geographies where it is located



Secure Socket Layers (SSL) or Virtual Private Networks (VPN) solutions **cannot address** the reality that data travels everywhere and anywhere in a cloud.

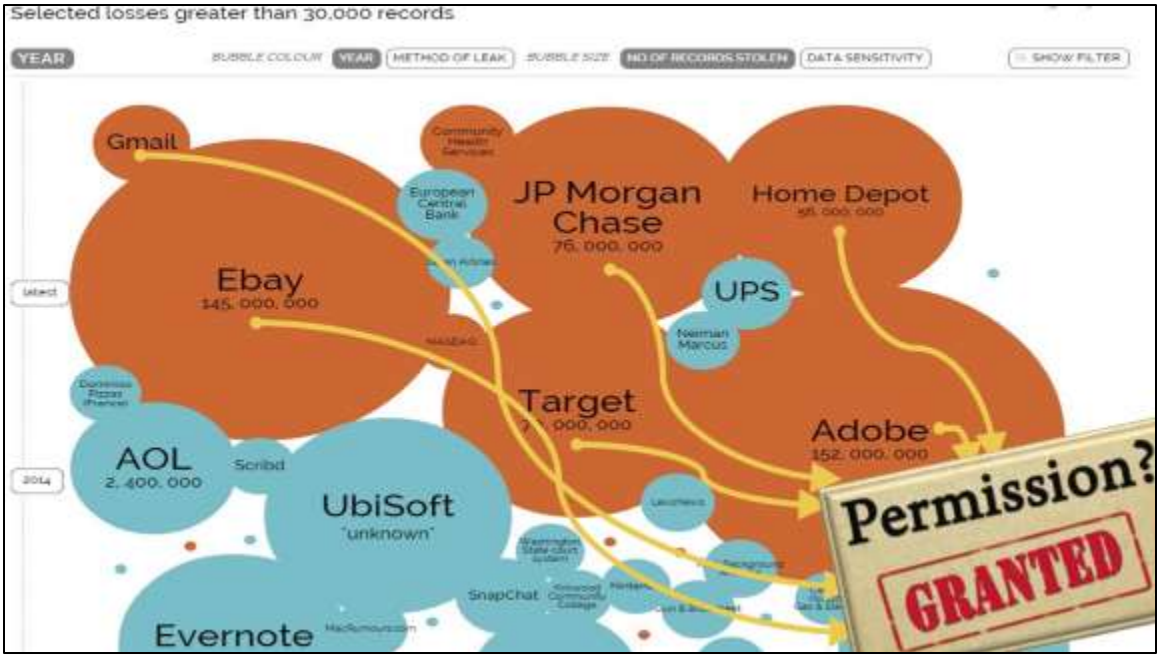
In 2009, this may have been maintainable…



In 2014, not so much.

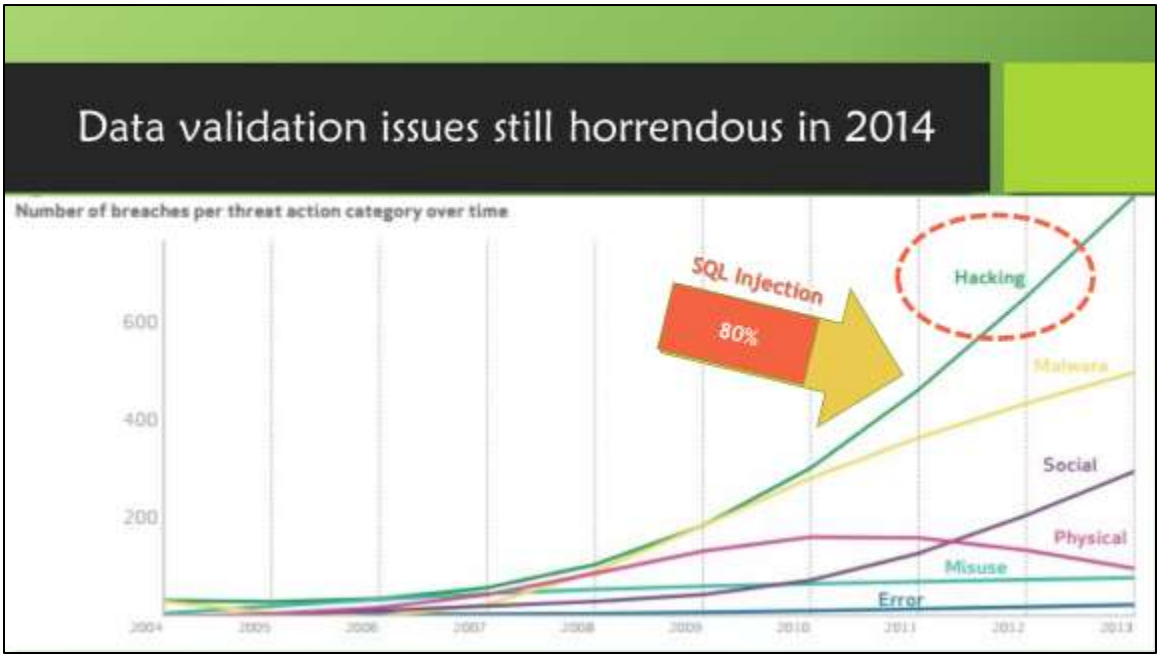
How is SSL/TLS going to solve the rapid growth of connected sites?

Call it the Multitenancy Effect.



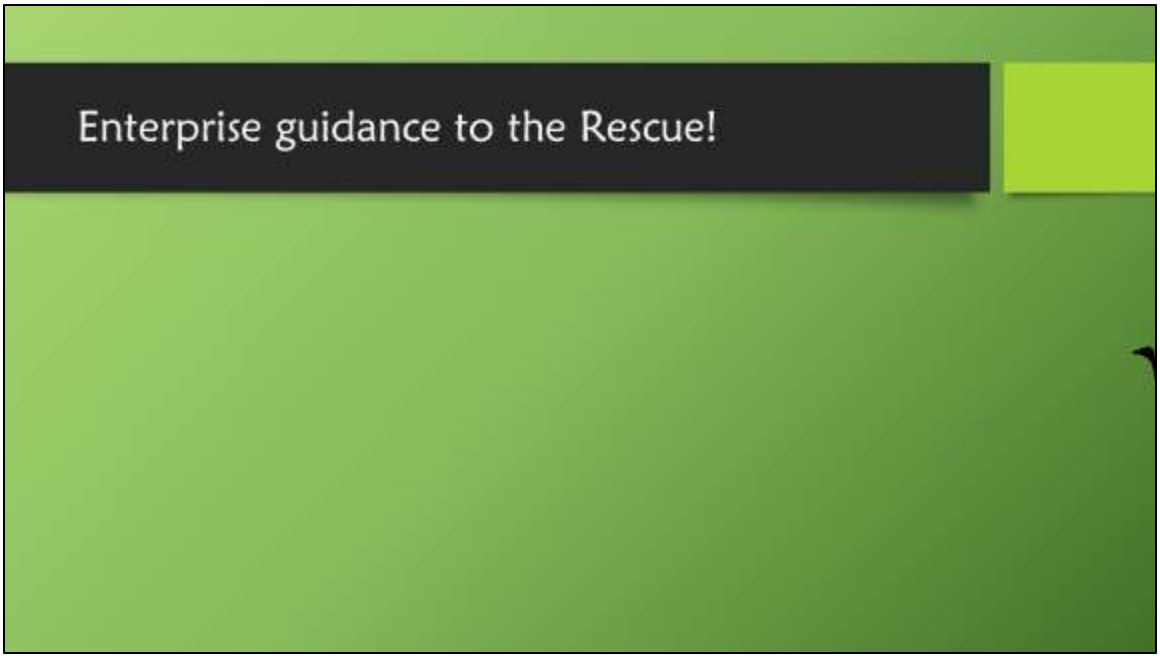
Malware attacks will make their way to internal networks via techniques such as SQL injection.

Once they're on the network, they inherit the permissions of a trusted user and find their way over to more important assets



SQL injection was leveraged in 27 of the 34 (80%) attacks against web applications in the retail industry.

Why is this still happening?


Enterprise guidance to the Rescue!

OWASP General Data Validation - https://www.owasp.org/index.php/Data_Validation_%28Code_Review%29

OWASP Entity Encoding - https://www.owasp.org/index.php/How_to_perform_HTML_entity_encoding_in_Java

OWASP Application Security Verification Standard is a step in the right direction, but still based on trusted zones - http://code.google.com/p/owasp-asvs/wiki/Verification_V5

Microsoft Guidance Share is based on centralized validation control- http://www.guidanceshare.com/wiki/Web_Application_Security_Design_Guidelines_-_Input_/_Data_Validation

http://msdn.microsoft.com/en-us/library/ee658105.aspx#ValidationDesign Steps for Validating Input and Data

Microsoft

Validation Application Block; heavyweight and complex to use
http://msdn.microsoft.com/en-us/library/dn440720(v=pandp.60).aspx

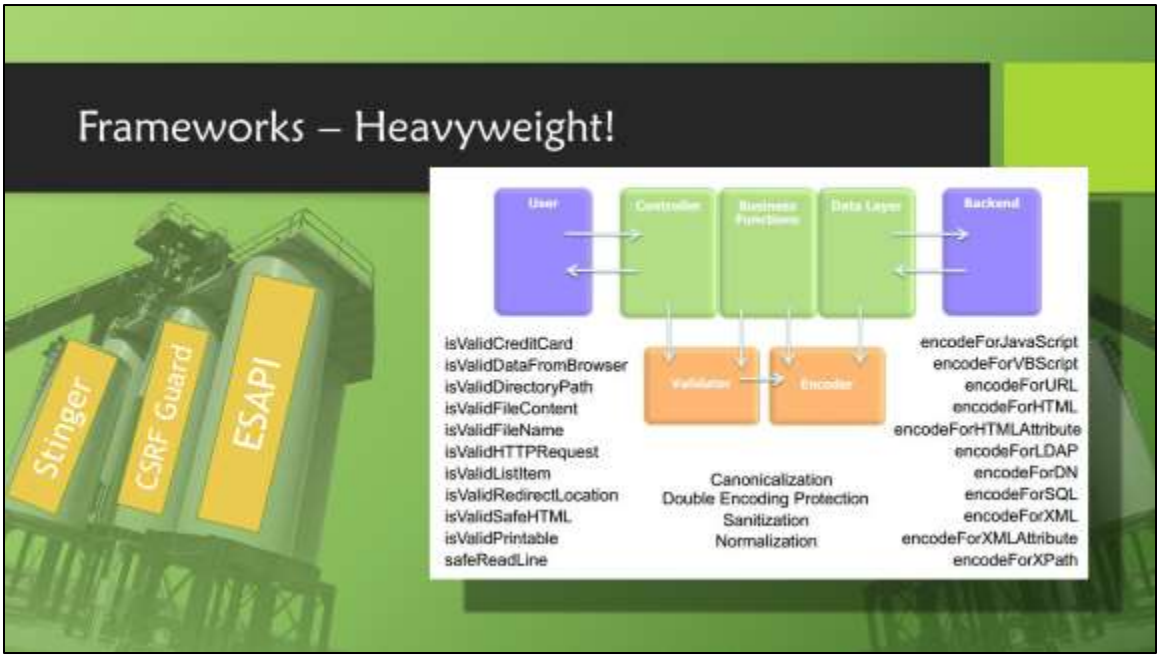
OWASP

CSRF Guard - http://www.owasp.org/index.php/CSRF_Guard

Stinger (inactive) was the start of a centralized input validation component; replaced by ESAPI? –

https://www.owasp.org/index.php/Category:OWASP_Stinger_Project

ESAPI main purpose is to retrofit security into existing applications –
https://www.owasp.org/index.php/Esapi



Microsoft

Validation Application Block; heavyweight and complex to use
http://msdn.microsoft.com/en-us/library/dn440720(v=pandp.60).aspx

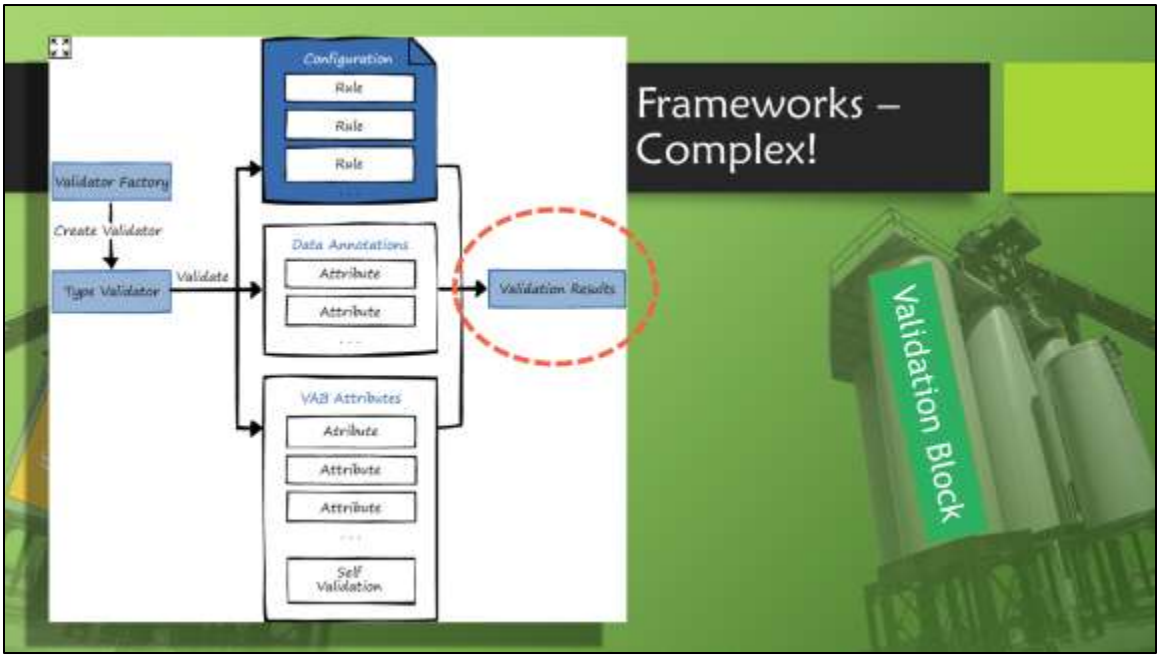
OWASP

CSRF Guard - http://www.owasp.org/index.php/CSRF_Guard

Stinger (inactive) was the start of a centralized input validation component; replaced by ESAPI? –

https://www.owasp.org/index.php/Category:OWASP_Stinger_Project

ESAPI main purpose is to retrofit security into existing applications –
https://www.owasp.org/index.php/Esapi



Microsoft

Validation Application Block; heavyweight and complex to use
http://msdn.microsoft.com/en-us/library/dn440720(v=pandp.60).aspx

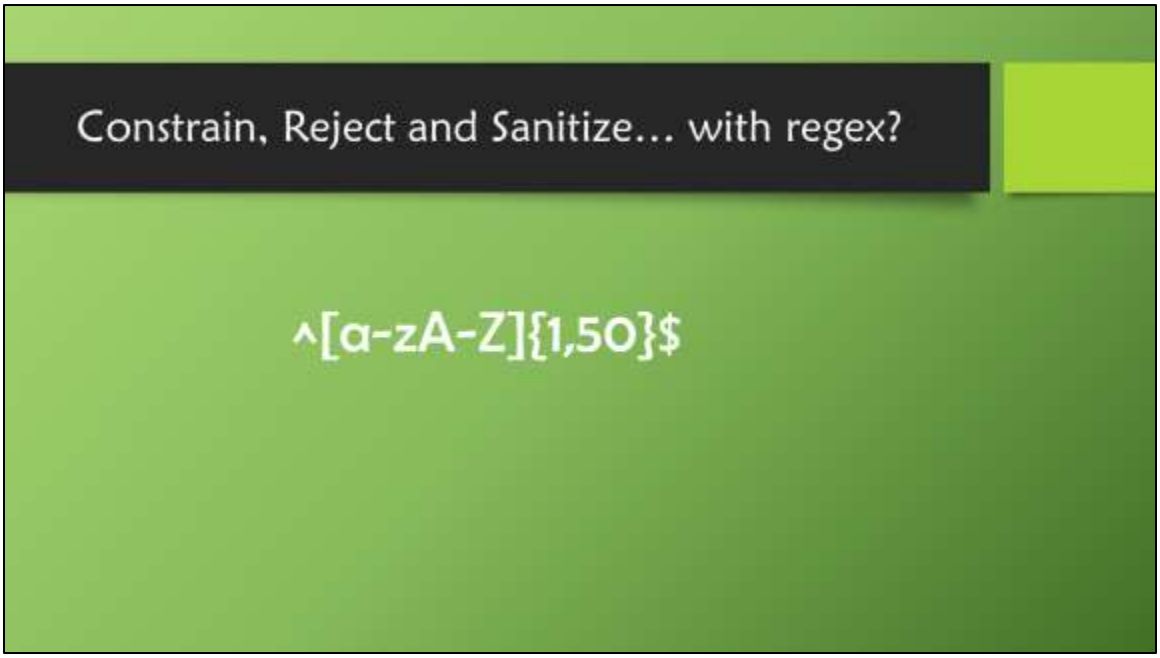
OWASP

CSRF Guard - http://www.owasp.org/index.php/CSRF_Guard

Stinger (inactive) was the start of a centralized input validation component; replaced by ESAPI? –

https://www.owasp.org/index.php/Category:OWASP_Stinger_Project

ESAPI main purpose is to retrofit security into existing applications –
https://www.owasp.org/index.php/Esapi

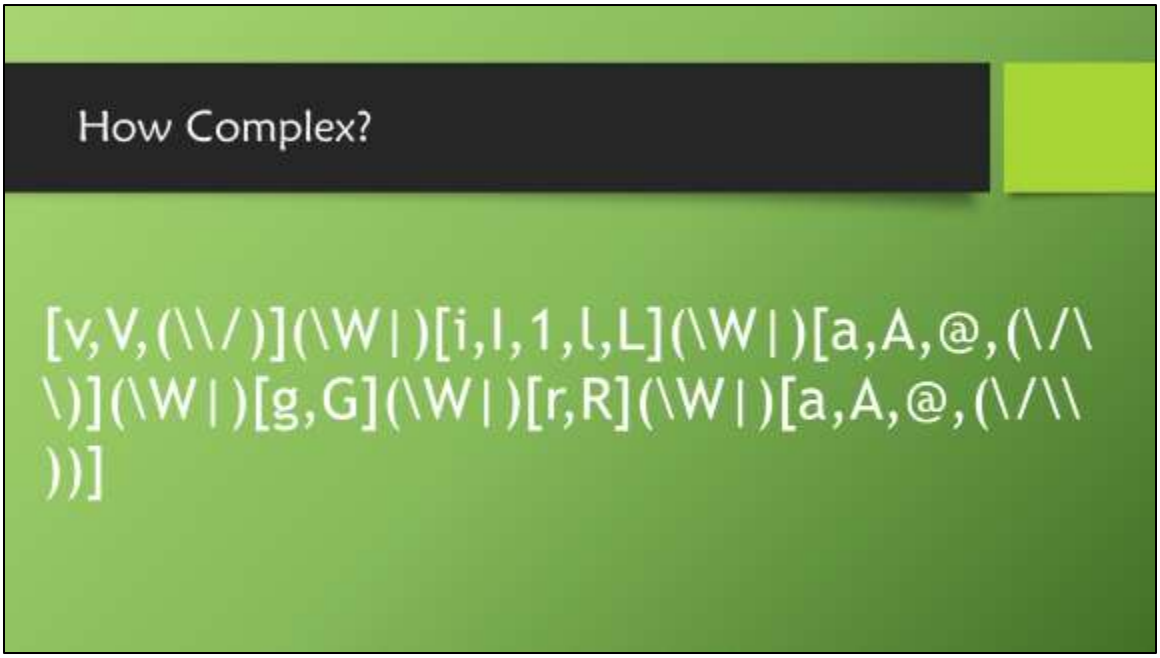


Word mapping

Hey this is easy enough

^[a-zA-Z]+$

But what if I wanted to block certain patterns…
[v,V,(\\/)](\W|)[i,I,1,l,L](\W|)[a,A,@,(\/\\)](\W|)[g,G](\W|)[r,R](\W|)[a,A,@,(\/\\))]
(**viagra** anyone?)

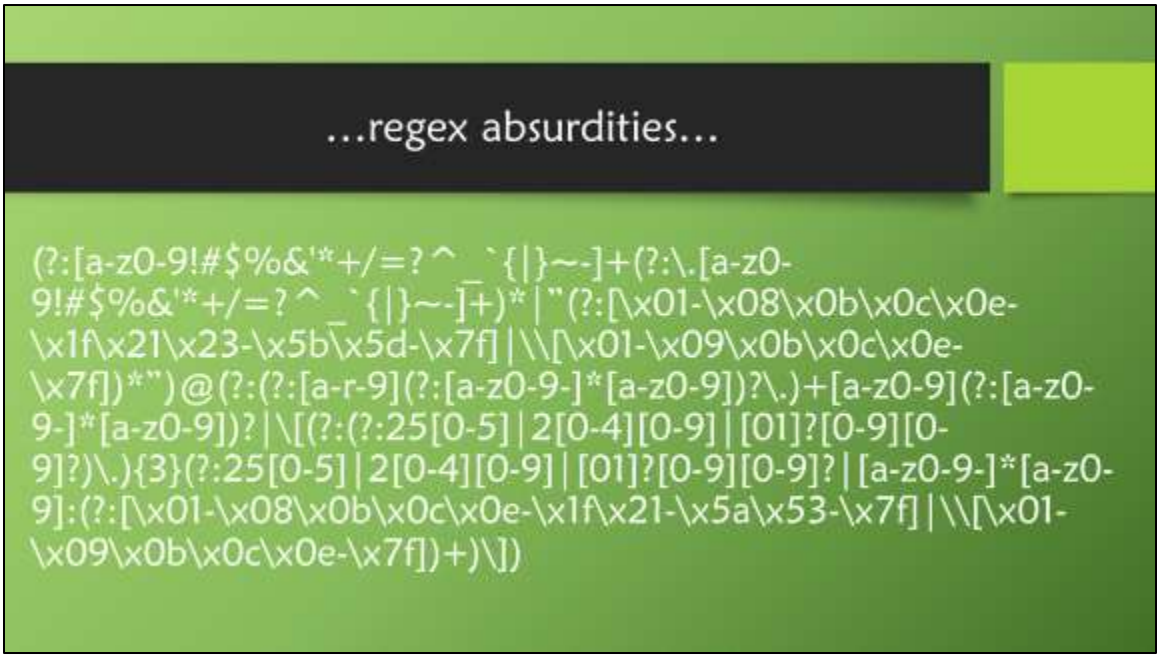


Word mapping

Hey this is easy enough

^[a-zA-Z]+$

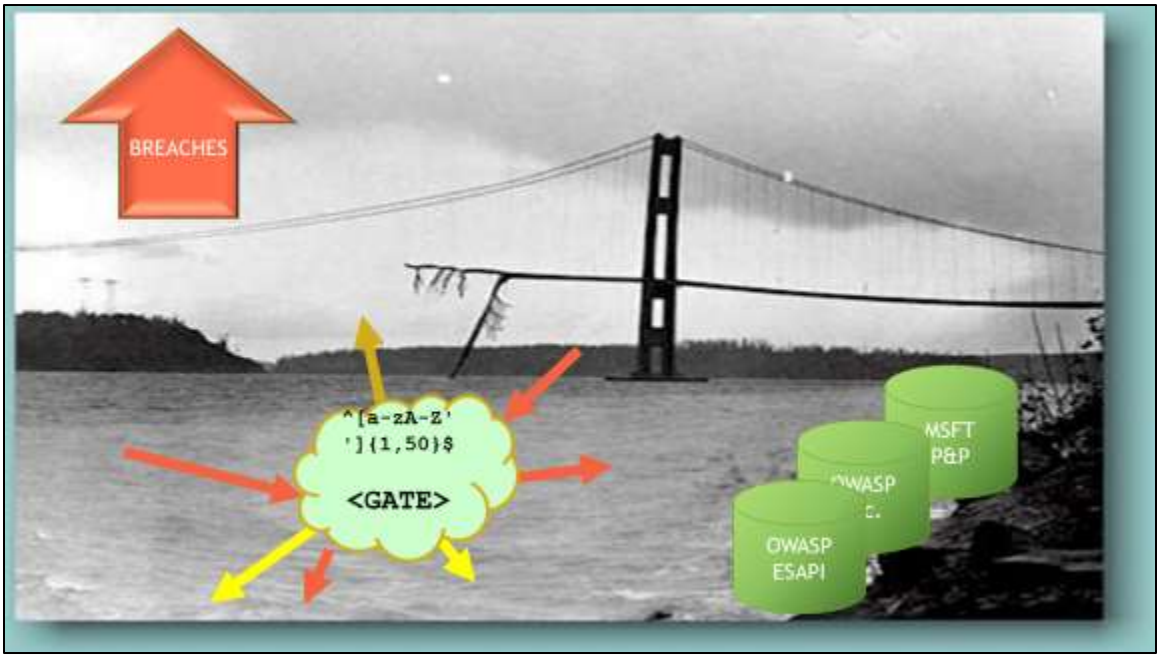
But what if I wanted to block certain patterns…
[v,V,(\\/)](\W|)[i,I,1,l,L](\W|)[a,A,@,(\/\\)](\W|)[g,G](\W|)[r,R](\W|)[a,A,@,(\/\\))]
(**viagra** anyone?)



Email address mapping

Ugh, what is this mess?

(?:[a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*|"(?:[\x01-
\x08\x0b\x0c\x0e-\x1f\x21\x23-\x5b\x5d-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-
\x7f])*")@(?:(?:[a-r-9](?:[a-z0-9-]*[a-z0-9])?\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-
9])?|\[(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-
9][0-9]?|[a-z0-9-]*[a-z0-9]:(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21-\x5a\x53-
\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])+)\])



Malicious Data breaches are increasing

The old model of validation gates doesn't work in a multi-tenancy world

Current frameworks are complex and siloed


What if… we had a pattern that could…


Prevent Injection Attacks - Integrity


Verify Good Data – Integrity (again)


Execute smoothly with Data - Availability

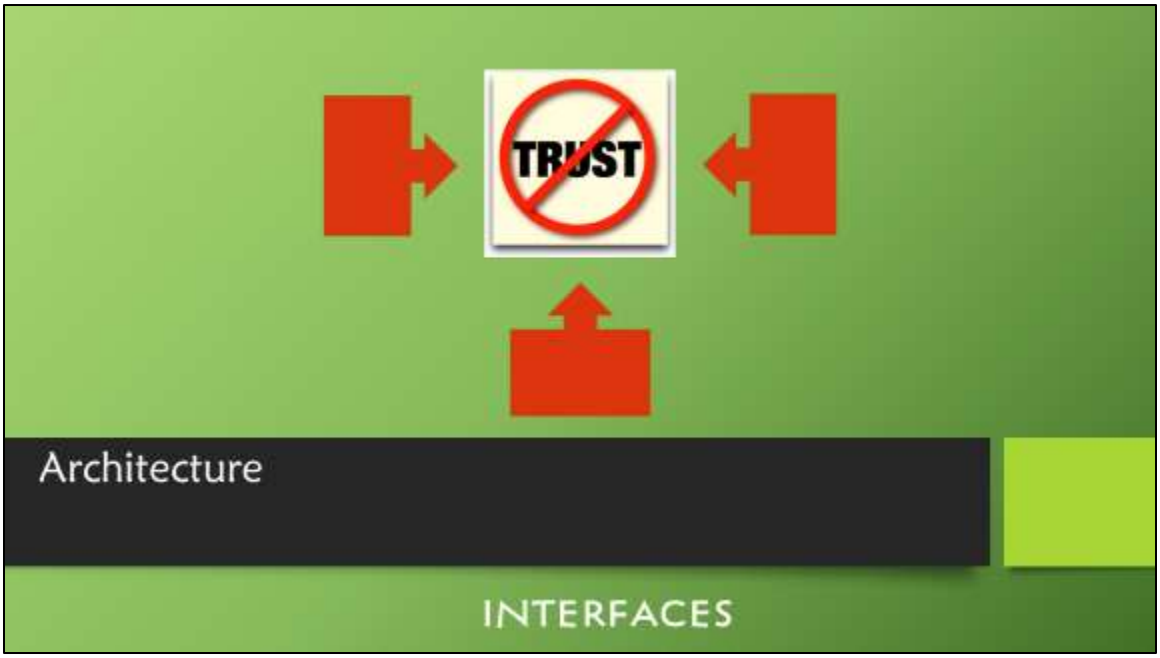
Concept of Zero-trust architecture

In Zero Trust, all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

The core concepts of Zero Trust are:

- There is no longer a trusted and an untrusted interface on our security devices.
- There is no longer a trusted and an untrusted network.
- There are no longer trusted and untrusted users

The Zero Trust model provides a data-centric approach to security that protects against sophisticated and targeted attacks



Concept of Zero-trust architecture

In Zero Trust, all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

The core concepts of Zero Trust are:

- There is no longer a trusted and an untrusted interface on our security devices.
- There is no longer a trusted and an untrusted network.
- There are no longer trusted and untrusted users

The Zero Trust model provides a data-centric approach to security that protects against sophisticated and targeted attacks

Concept of Zero-trust architecture

In Zero Trust, all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

The core concepts of Zero Trust are:

- There is no longer a trusted and an untrusted interface on our security devices.
- There is no longer a trusted and an untrusted network.
- There are no longer trusted and untrusted users

The Zero Trust model provides a data-centric approach to security that protects against sophisticated and targeted attacks

Concept of Zero-trust architecture

In Zero Trust, all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

The core concepts of Zero Trust are:

- There is no longer a trusted and an untrusted interface on our security devices.
- There is no longer a trusted and an untrusted network.
- There are no longer trusted and untrusted users

The Zero Trust model provides a data-centric approach to security that protects against sophisticated and targeted attacks

Concept of Zero-trust architecture

In Zero Trust, all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

The core concepts of Zero Trust are:

- There is no longer a trusted and an untrusted interface on our security devices.
- There is no longer a trusted and an untrusted network.
- There are no longer trusted and untrusted users

The Zero Trust model provides a data-centric approach to security that protects against sophisticated and targeted attacks

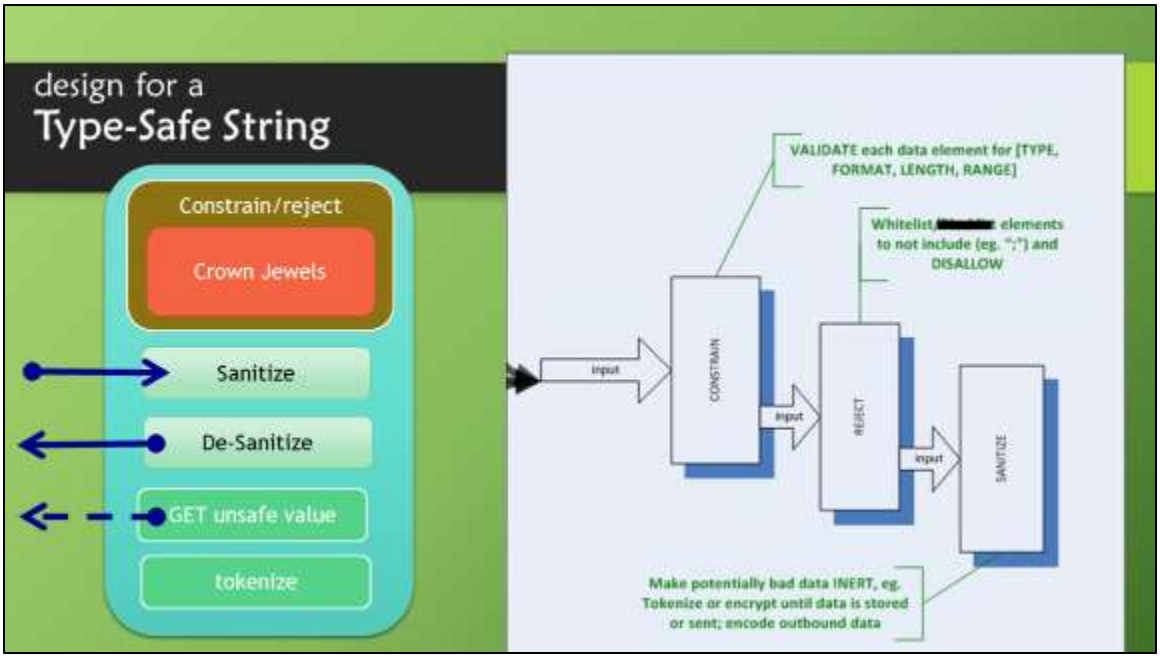
Concept of Zero-trust architecture

In Zero Trust, all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

The core concepts of Zero Trust are:

- There is no longer a trusted and an untrusted interface on our security devices.
- There is no longer a trusted and an untrusted network.
- There are no longer trusted and untrusted users

The Zero Trust model provides a data-centric approach to security that protects against sophisticated and targeted attacks



What is a "type-safe" string?

It acts like a string, but has the desired validation architecture *built into the class*! The type-safe string will take the validation with it where it gets used. Developers will no longer have to remember to also do validation because the type-safe string will take care of this.

- **Constrain and reject** when setting value
- Type
- Format
  - Simple regex
- Length
- Range
  - only applies to numbers
- **Sanitize** when passing data
  - Inert payload component

A note about sanitization during data validation. Sanitization is loosely based on the concept of tokenization. Tokenization provides a method by which to replace sensitive data with a disassociated and randomly generated alias. The process to tokenize and detokenize is strictly controlled with a special API. Data is persistently tokenized from the point of capture to the point of consumption or rest.

Sanitization doesn't rely upon a randomly generated or disassociated representation in this case as it is used to mitigate against injection attacks.

It makes the data inert.

(Setting Expectations)

I EXPECT THIS TO START A CONVERSATION, NOT BE THE END ALL BE ALL.

MANY EDGE CASES, DOESN'T SOLVE OUTPUT ISSUES CLEARLY.

As I got further into the exploration of this topic, I found more and more interesting avenues to explore.

Much still needs to be explored, such as

- serialisation (what kind)
- Output encoding
- Adoption
- Fundamentally my talk comes down to TRUST
    - Interesting talk with Simon the other night
    - Addressing the deeper need for changing languages
    - Million dollar question is how to embed trust into exchange of information!


Demo!


Questions?
DEEPSEC
Geoffrey Hill (geoff-h@artis-secure.com, Twitter @GHill_security)
Artis-Secure Ltd.