# DNSSEC: ¿Qué es y por qué importa?

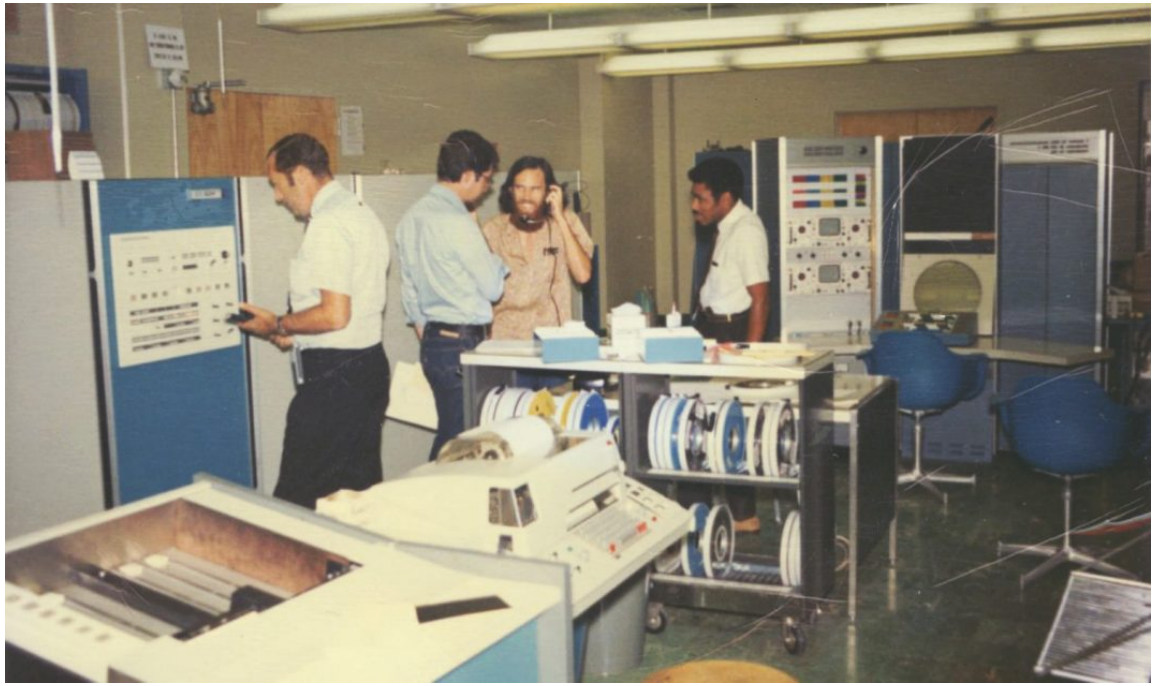
# DNSSEC: What is it and why is it important?

Dr. Pablo Rodríguez

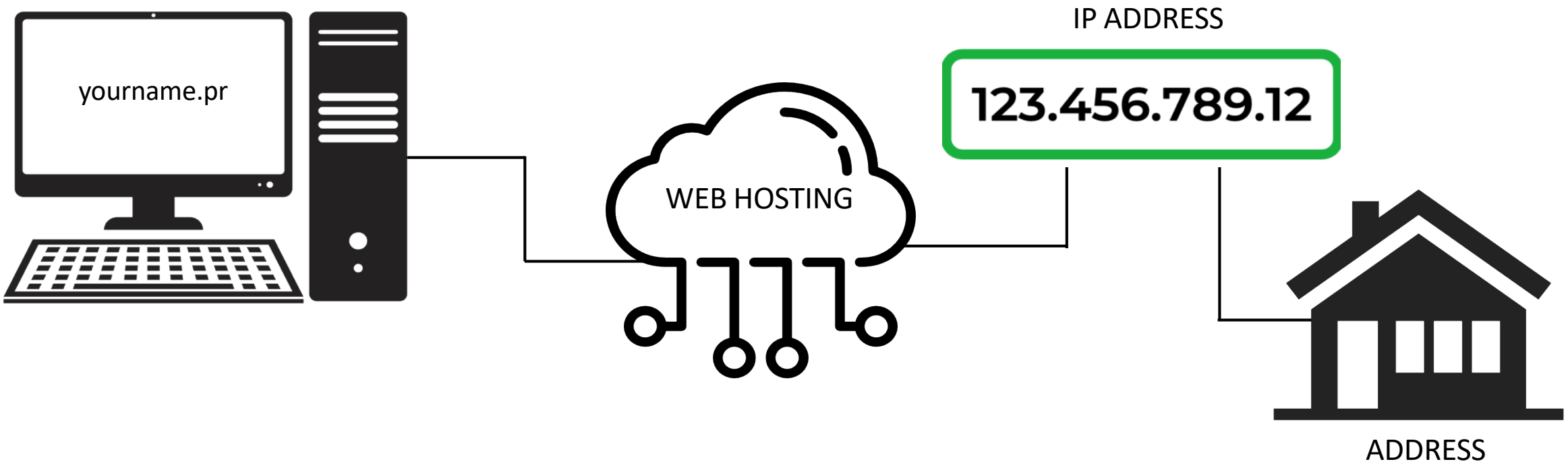
Executive VP

Puerto Rico Top Level Domain

# En el principio…
# In the beginning…

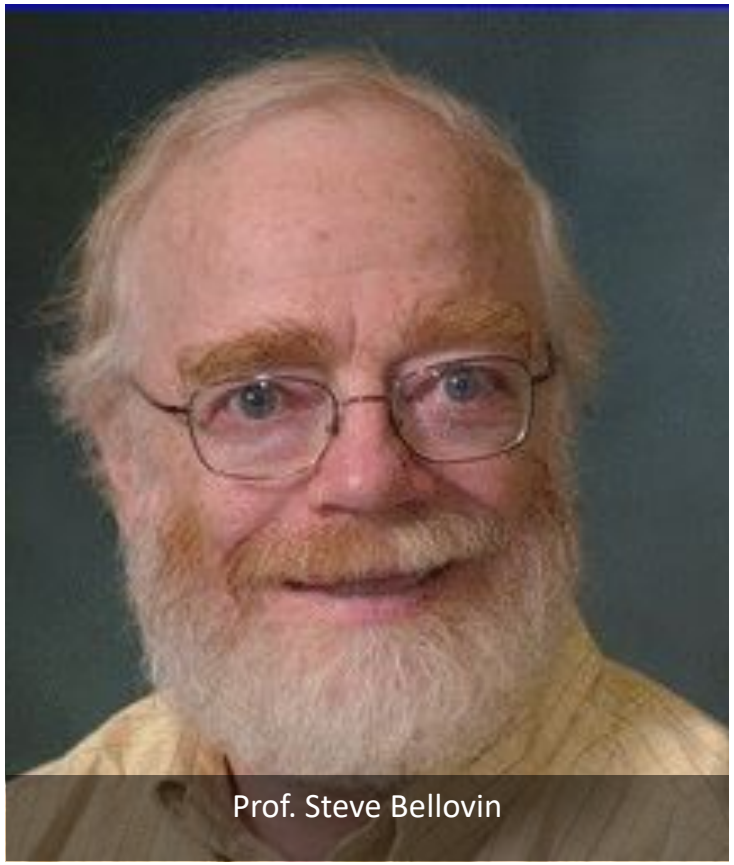
# IP Numbers & Market



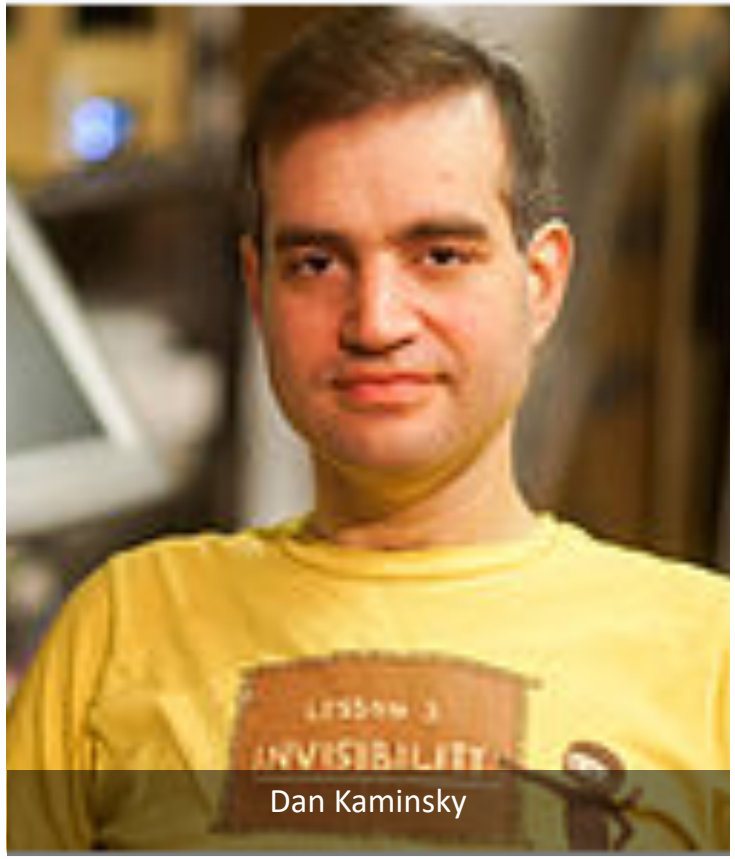

Once you select your preferred domain name and link it to a Web Hosting Service you will be able to create a personalize email, a website, and much more.

# Ellos eran tan ingenuos…
# They were so naive…

# El fin de la inocencia
# The end of innocence



Prof. Steve Bellovin



Dan Kaminsky

- 1990 – Bellovin descubre vulnrabilidades en el DNS pero no las revela hasta 1995
- Bellovin discovers vulnerabilities in the DNS but he does not reveal them until 1995
- 2008 – Kaminsky describe un ataque de envenenamiento del cache y propone una solución
- Kaminsky describes a cache poisoning attack and proposes a solution

# ¿Qué es DNSSEC?
# What is DNSSEC?

DNSSEC es un protocolo que refuerza la autenticación en DNS mediante firmas digitales basadas en criptografía de clave pública. Con DNSSEC, no son las consultas y respuestas de DNS en sí mismas las que están firmadas criptográficamente, sino que los datos de DNS en sí están firmados por el propietario de los datos.

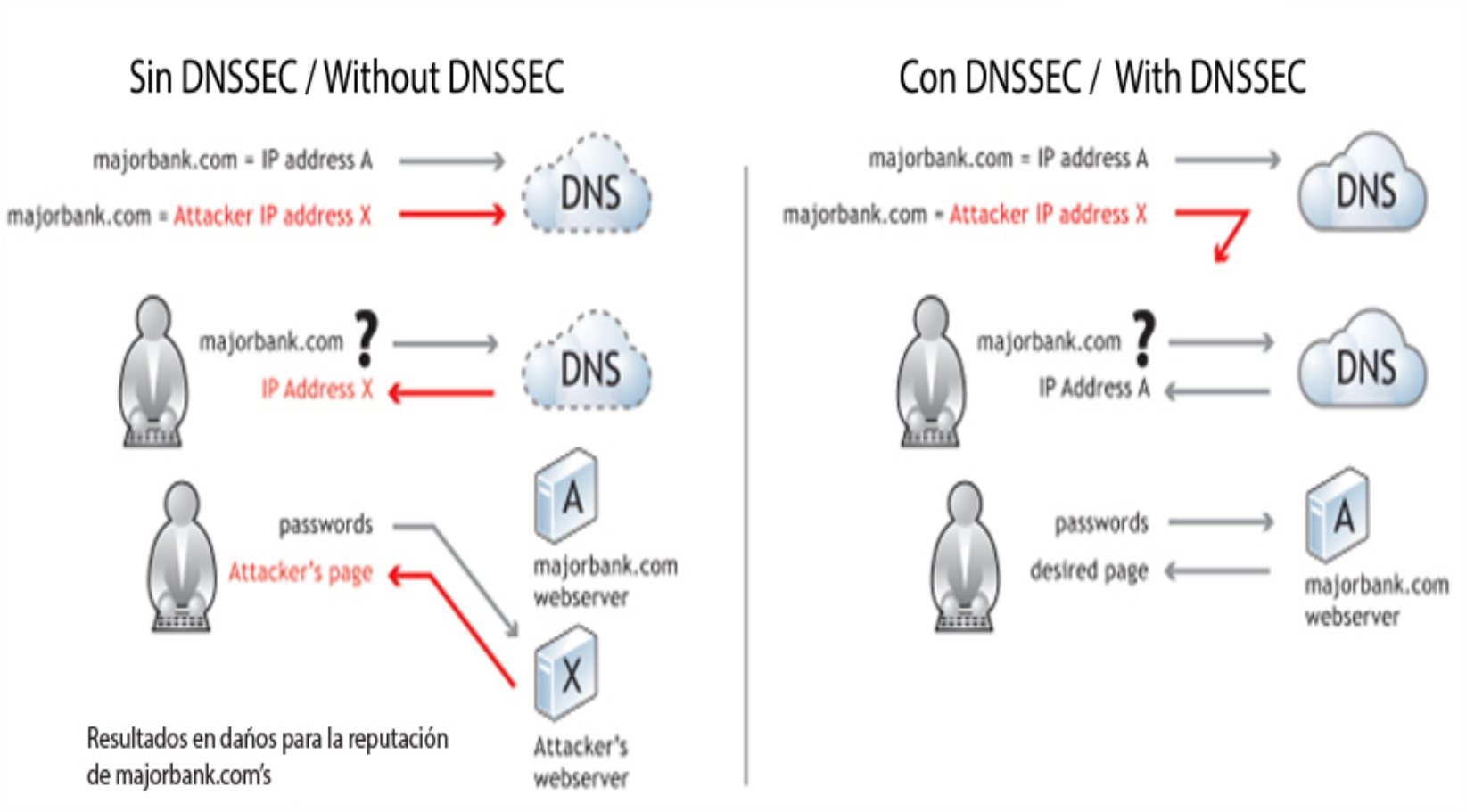
DNSSEC is protocol that strengthens authentication in DNS using *digital signatures* based on *public key cryptography*. With DNSSEC, it's not DNS queries and responses themselves that are cryptographically signed, but rather DNS data itself is signed by the owner of the data.

# Características Importantes de DNSSEC
# DNSSEC important features

- La autenticación del origen de los datos permite que un resolutor verifique criptográficamente que los datos que recibió realmente provienen de la zona donde cree que se originaron.
- La protección de la integridad de los datos permite al solucionador saber que los datos no se han modificado en tránsito desde que el propietario de la zona los firmó originalmente con la clave privada de la zona.

- Data origin authentication allows a resolver to cryptographically verify that the data it received actually came from the zone where it believes the data originated.
- Data integrity protection allows the resolver to know that the data hasn't been modified in transit since it was originally signed by the zone owner with the zone's private key.

# DNSSEC reduce las vulnerabilidades a los ataques
# DNSSEC decreases vulnerabilities to attacks



# DNSSEC promueve la innovación
# DNSSEC fosters innovation

- Se han desarrollado nuevos protocolos que se basan en DNSSEC
- Solo funcionan en zonas que están firmadas
- Dane es un ejemplo de ello, permite la publicación de claves de seguridad de la capa de transporte (TLS) en zonas para aplicaciones como el transporte de correo.
- DANE proporciona una forma de verificar la autenticidad de las claves públicas que no depende de las autoridades de certificación.
- Las nuevas formas de agregar privacidad a las consultas de DNS también podrán usar DANE en el futuro.

- New protocols have been developed that are based on DNSSEC
- They only work in areas that are signed
- Dane is an example of this, it allows the publication of transport layer security (TLS) keys in zones for applications such as mail transport.
- DANE provides a way to verify the authenticity of public keys that does not depend on the certificate authorities.
- New ways to add privacy to DNS queries will also be able to use DANE in the future.

# Lo que no hace DNSSEC
# What DNSSEC Doesn't Do

DNSSEC **No**:

- Previene ataques DDoS
- Mantener confidencialidad
- Protege todo el servidor

DNSSEC **does not**:

- Prevent DDoS attacks
- Maintain confidentiality
- Protect the entire server

# Retos
# Challenges

- La adopción e implementación de DNSSEC por ccTLDs, ISPs, y otras instituciones es muy lenta en LAC y África
- Estudios identifican retos financieros asociados a la contratación y capacitación de personal
- La implementación de DNSSEC añade una capa de complejidad adicional a los operadores de redes
- El desconocimiento de sucesos locales fomenta la resistencia de implementar DNSSEC
- No existen mecanismos en los buscadores que avisan que una pagina web no tiene DNSSEC como es el caso de los SSLs

- The adoption and implementation of DNSSEC by ccTLDs, ISPs, and other institutions is very slow in LAC and Africa
- Studies identify financial challenges associated with the hiring and training of personnel
- Implementing DNSSEC adds an additional layer of complexity to network operators
- Ignorance of local events fosters resistance to implementing DNSSEC
- There are no mechanisms in search engines that warn that a web page does not have DNSSEC as is the case with SSLs

# Aprenda a identificar si una página web tiene DNSSEC
# Learn to identify if a web page has DNSSEC

Use está herramienta para ver si una página web tiene DNSSEC

- www.dnsviz.net
- https://dnssec-debugger.verisignlabs.com

Use this tool to see if a web page has DNSSEC

- www.dnsviz.net
- https://dnssec-debugger.verisignlabs.com

# Protejase adoptando buenas medidas de seguridad
# Protect yourself adopting good security measures

- No use computadoras públicas o no seguras.
- Identifique quien le envía un email antes de responder
- Instale software antivirus y de detección de *spyware* en todos sus sistemas de computadora.

- Don't use public or unsecured computers.
- Identify who sends you an email before responding
- Install antivirus and spyware detection software on all your computer systems.

# Protejase adoptando buenas medidas de seguridad
# Protect yourself adopting good security measures

- Asegurese de quien es que le escribe:
  - popular.com ≠ p0pular.com

  Caracteres usados para confundir
  - 0 ≠ o
  - 1 ≠ l
- Don't use public or unsecured computers.
- Identify who sends you an email before responding
- Install antivirus and spyware detection software on all your computer systems.

# THANK YOU!