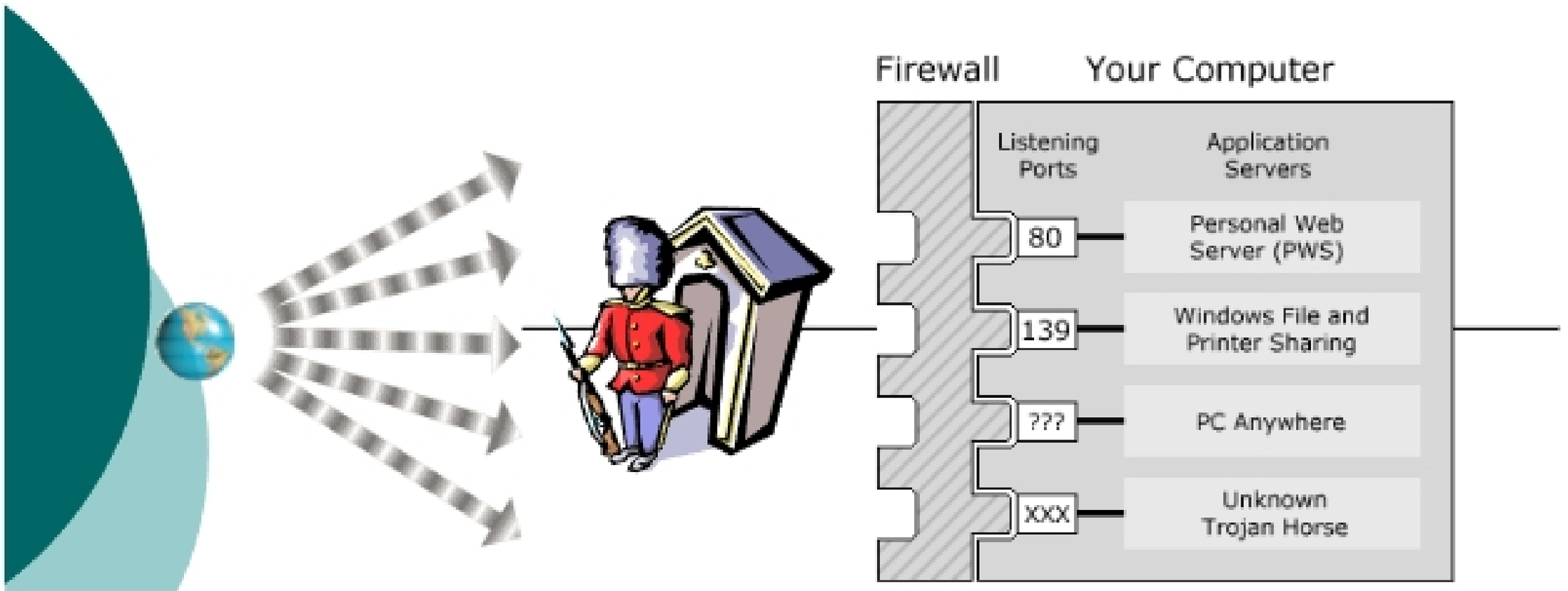

Presented by Joshua Schiffman & Archana Viswanath

Ten Risks of PKI : What You're not Being Told about Public Key Infrastructure – By Carl Ellison and Bruce Schneier

Trust Models

Rooted Trust Model

- In a rooted trust model, the root CA is the trust anchor and has a self-signed certificate.
- The root CA issues a certificate to all direct subordinate CAs, if needed, which, in turn issue certificates to their subordinate CAs. A subordinate CA is trusted cryptographically, based on the signature of its parent.

Network Trust Model

- In a network trust model, all CAs are self-signed and trust relationships between CAs are based on cross-certificates. Cross-certificates establish trust between unrelated CAs.

Hybrid Trust Model

- It is a combination of the above two models.
- Certain CAs are cross certified and certain others are rooted trust models.

Keys

Risk – "Who is using my key?"

- Safety of Private Key at user end
  - Is the key encrypted?
  - Is the user computer protected?
  - Is the computer virus-free?
- Basis of PKI – Non – Repudiation
  - The user is held responsible for all transactions executed with his key.