PKI That Works: Advancing Usability While Expanding Use

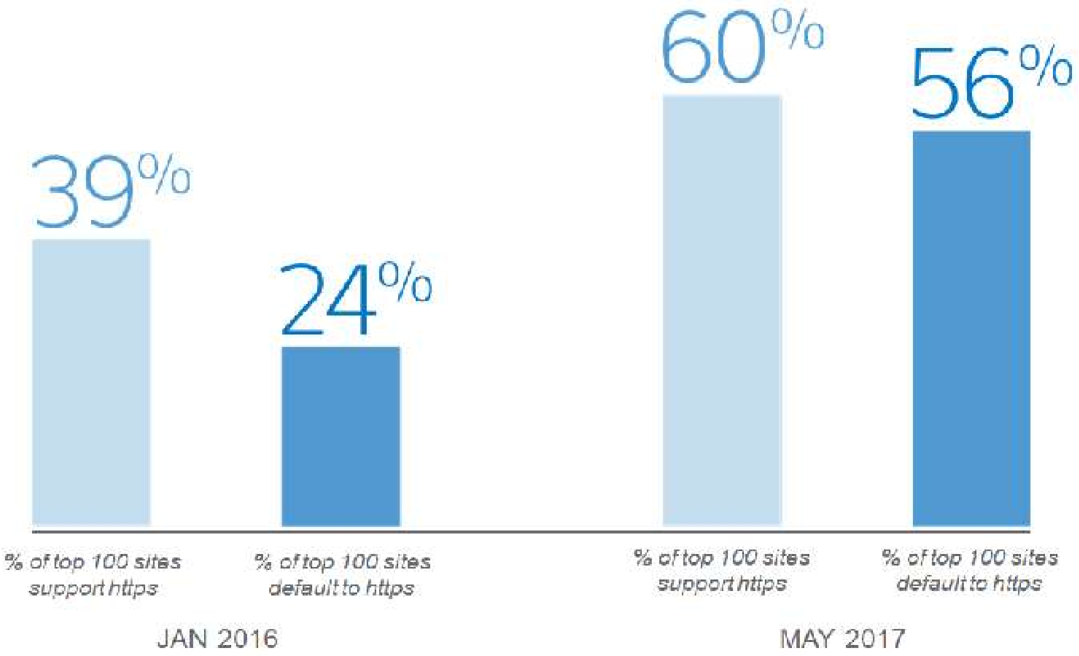
digicert® | Symantec™ Website Security

Sad IT Man

- Individual server configs
- Unprotected devices
- Random devices
- Rogue staff
- Remote devices
- Disparate policies

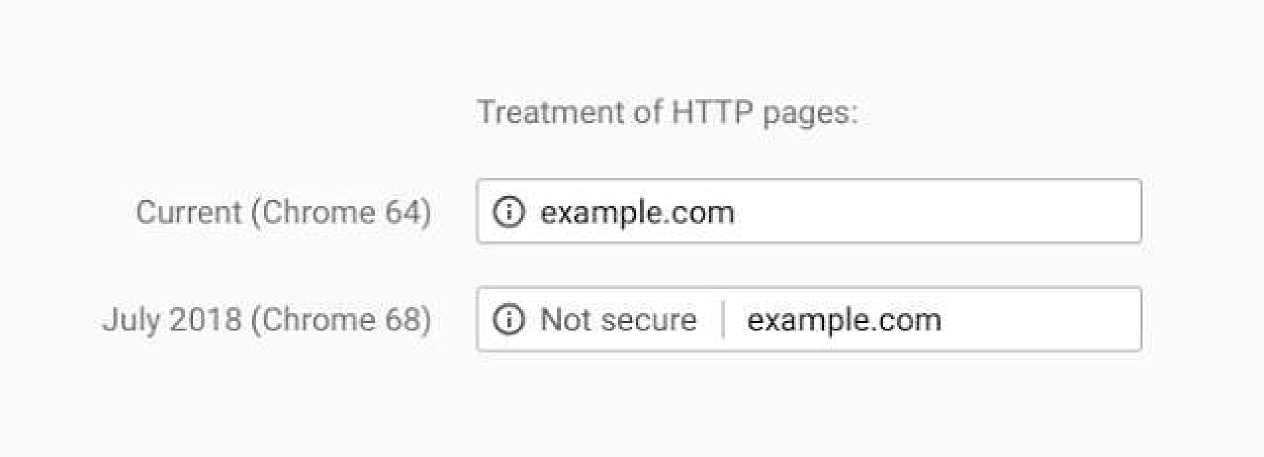
A Changing Landscape

- HTTPS – the norm
  - Traffic has increased by 75% over the last two years.
  - 3/4 page loads are now performed over HTTPS.



A Changing Landscape

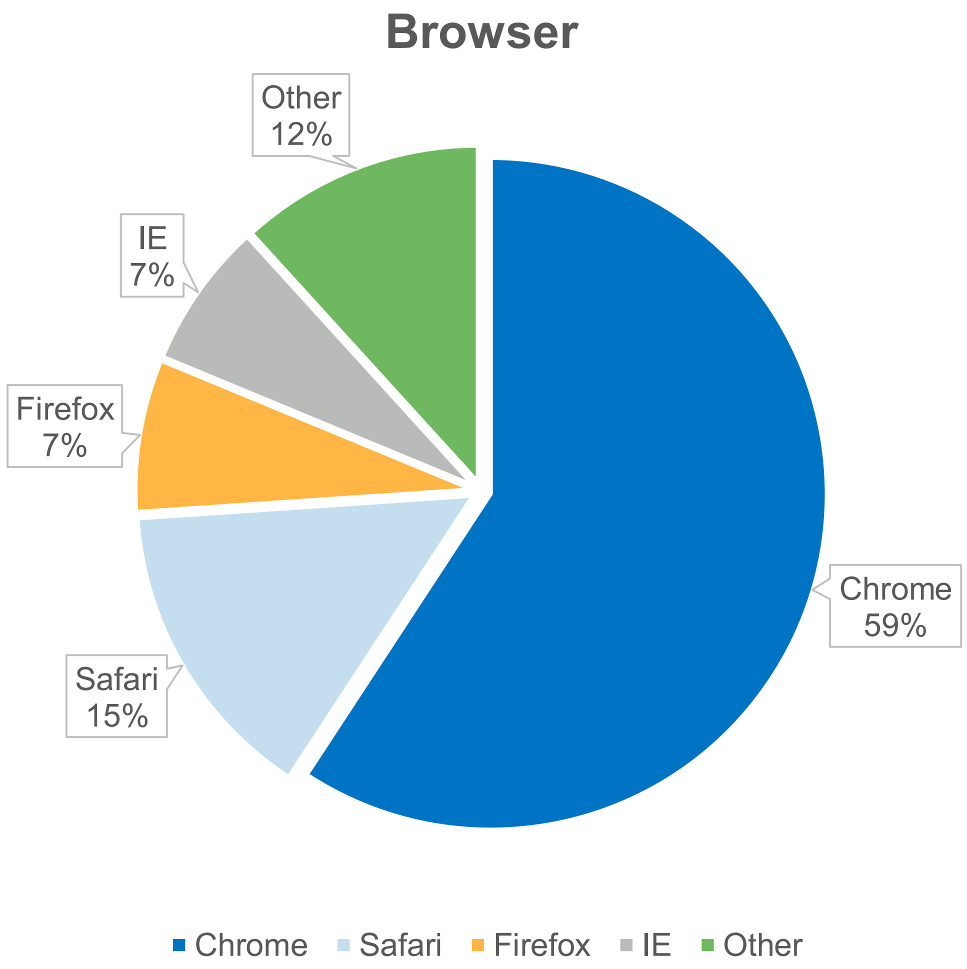
- Firefox will require HTTPS for all new features added to the browser. HTTP/2 requires HTTPS.
- Later this year, in July, Google is going to mark all HTTP pages as “Not Secure”.



Treatment of HTTP pages:

Current (Chrome 64)	ⓘ example.com
July 2018 (Chrome 68)	ⓘ Not secure | example.com

A Changing Landscape



The Rise of the Machines

- Everything is connected
- By 2020, an estimated 25 billion devices will be connected to the internet.
- Communication process varies
- IoT can be the target or the tool
- Threats
  - Over-the-air updates
  - Secure patch management
  - Secure boot
  - Authenticating devices
  - Stolen data

The Meaning of Life

- More work
- Less resources
- More attacks
- Less control
- More sadness

Turn Tears into Profits!

- 1. Secure all the things
- 2. ???
- 3. Profit!

Reality

- Make PKI Great Again
  - Simplify creation
  - Simplify provisioning
  - Simplify management
  - Simplify control

Simplify Creation

- Get rid of the muck
  - Need a key
  - Need a server
  - Need a cert
- Scaling to Billions
- Discovery
- Bulk replace

Simplify Provisioning

- CSR/SCHMEE-SR
    - Auto-replace
    - Auto-install
    - Auto-manage
- Remove the human-error in deployment
    - Simplify support

Provisioning

- Homegrown tools
  - Automate the verification and issuance of certificates
- ACME
  - IETF standard for a homegrown tool
  - Automating the verification and issuance of certificates
- Integration with third parties

Tools

- SCEP
- EST
- API

Improving Usability

- System integration

  - Get all the benefits of strongly vetted, publicly-trusted certificates directly within the environments you already use.

  - Microsoft Azure’s Key Vault can directly connect to DigiCert via API, allowing Key Vault to seamlessly handle key storage, certificate requests, and automated renewal.

Simplify Management

- Manage by exception
- Manage by profile
- Manage by delegation
- Manage by not managing

Certificate Transparency (CT)

- All publicly-issued certificates are published to online logs.
- Protects the entire ecosystem by creating an auditable log of what certificates a CA is issuing.
- Detection method for mis-issued certs, as well as a way to monitor certificate inventory.
- Required for all publicly-trusted certs in April. DigiCert started in February

Simplify Control

- Restrict use
- Restrict access
- Distribute policies

Certificate Authority Authorization (CAA)

- Control over issuing authority
  - Control over issuing account
  - Control over certificate type
  - Control over validation method
- Restrict outside purchases
- Policy communication on an FQDN level

Simplify Security

- Automated
- Regularly updated
- Distributed
- Reliable
- Effective

Short-Lived Certificates

- Reduced validity for publicly-trusted SSL certificates to 825 days
  - Frequent key rotation
  - Faster evolving standards
  - Short-lived permit frequent key rotation
- Validity measured in days, not years
  - 90 day certs
  - 8 hour certs
  - 15 min certs

PKI for All the Things

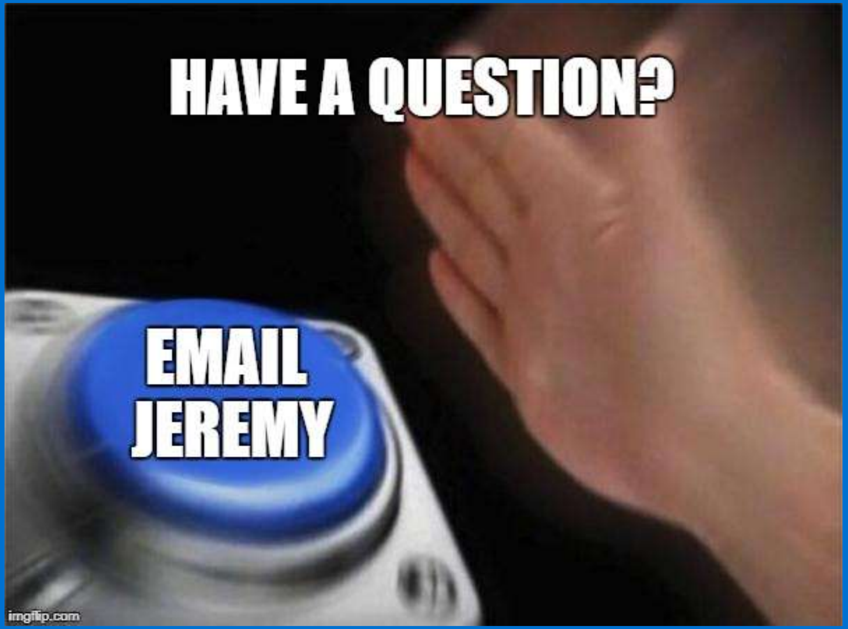
- Authentication
- Identification
- Encryption

Conclusion

- Simplify PKI so it’s always there
- Scale the systems to meet the global need
- Extend PKI to the evolving landscape

ConJeremclusion

digicert® | Symantec™ Website Security



Jeremy Rowley
jeremy.rowley@digicert.com
C: 801-633-8482

digicert® | Symantec™ Website Security