DNSSEC and Web Security

Phillip Hallam-Baker
Comodo Group Inc.
The Biggest Problem in Web Security
Security is Optional

NOW!
With Added Safety!
WEB SECURITY NEEDS YOU
Two Approaches

• Security Upgrade in HTTP
  – Always retrospective
  – Only Applies to HTTP
  – No dependencies

• Security Upgrade in Discovery (DNS)
  – Infrastructure: Applies to any protocol
  – Depends on DNSSEC
Proposal: BOTH
Why DNS?
It is what the DNS is for.
DNS Development

1980s: Name → Host
1990s: Name → Host(s)
2000s: Name → Internet Service
2010s: Name → Internet Service + Properties
How?

- Some Design Choices
  - Support DNS CNAMEs, DNAMEs
  - Support DNS Wildcards
  - Support enhanced discovery (SRV, URI)
  - Granularity: Domain, Service Host
  - Number of DNS round trips
One Approach ESRV-01

$origin example.com
.
.
www
.
_http._tcp
A
CNAME
ESRV
ESRV
ESRV
ESRV
10.1.2.3
example.com.
dcert <CA Cert Digest>
disc prefix
tls required
ESRV with SRV

$origin example.com
.
A 10.1.2.3
www CNAME example.com.
.
ESRV disc SRV
$http._tcp SRV 1 1 80 host1.example.com
$http._tcp SRV 1 1 80 host2.example.com
host1 ESRV tls required
host1 ESRV dcert <EE Cert Digest>
host2 ESRV tls required
host2 ESRV dcert <EE Cert Digest>
Performance?

No impact unless you use features
Next Steps

• Constraints
  – Using DNS is the right way
  – But needs to be done right

• Approach
  – Continue with HTTP based Strict Security
  – Develop DNSSEC based approach as EXPERIMENTAL

• Will require multiple groups
  – DNS framework
  – Leveraging framework