

Towards Improving the Security of the Internet

Vint Cerf
Google

Strong Authentication

- Edge Devices
- Active Processes (persistence)
- Users
- Digital Objects
- Implications
 - Certificates(?) and Identification Processes
 - Access controls and authorization
- Two-part authenticators (devices)

Vulnerabilities

- Browsers (xss, etc.)
- Operating Systems
- Routing
- Domain Name resolution
- DPI-based attacks (e.g. Against TCP)
- MANETs (autoconfiguration and overrun conditions)

More Vulnerabilities

- Zombies
- Botnets
- DOS/DDOS/Amplified DDOS
- Drive-by downloads
- Zero Day attacks

Obvious Responses

- IPSEC, TLS, SSL, SSH, etc.
- DNSSEC
- IP address filtering
- Routing Arbiters/Servers/Registries
- RIR AS validations
- Embedded end-point authentication (hosts, routers, etc.)
- Mobile IP revalidation (challenge/response)

Things That Sorta Worked

- Certificates for the general public
 - Expense of validation
- Trusted Computing Base
- Open Source
 - How do you know the object code is ok? The source code?
- Web Crawl for badware identification

Hare-brained Ideas

- Incremental trust model
 - Begins with exchange and verification of public keys. (challenge/response)
 - Demand certification for transactions requiring same (“loan” anecdote)
 - Trusted Third Party Validation
- Others?

**For those viewing
via webcast,
please submit questions
for this presentation to
kmwquestions@nist.gov**