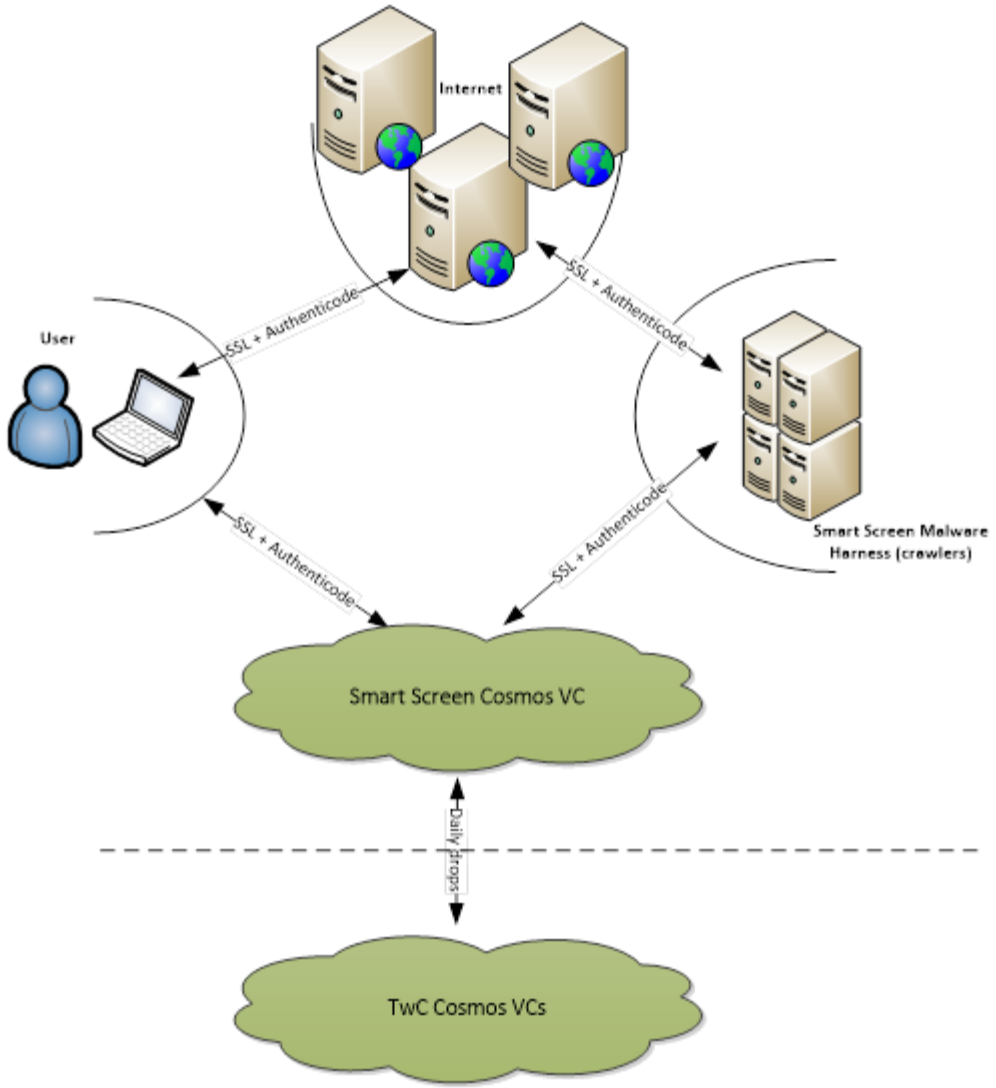
Certificate Reputation

Data Collection



Certificate Reputation
Detecting Fraudulent Certificates

- Find independent DNS names associated with the same public key
- Find different certs with the same signature hash
- Existence of two certificates for the same DNS but the certificate is renewed “too early”
- Existence of two (or more) certificates for the same DNS name where the frequency of at least one of the chain is very small compared to the other one(s).

- …

Certificate Reputation
Certificate Hygiene Analysis

- Find end entity SSL certificates with basic constraints cAType=True or CA certificate without path constraints
- Find all CAs that do not use enough entropy (8 bytes) in the serial number in the issued certificate.
- Find end entity SSL certs issued directly under root
- …

Certificate Reputation
Analysis of Weak Crypto

- Analyzed 415K+ signed binaries which used 6500+ signer certificates

Certificate Type	Results
End-entity code signing certificate	No MD5 certificate was used after 2010
CA certificate	2 certificates were used after 2010 (GeoTrust and Equifax)
Time stamping certificates	Found 4 VeriSign certificates

Certificate Reputation
Mitigations

- Upon finding suspicious/non-hygiene certificates, we may choose to do two things:
  - Contact CAs
  - Notifications sent to site owners
- If certificate is confirmed to be fraudulent, we will revoke it using black list feature in Windows. We will also notify other browsers about it.

Certificate Reputation

Summary

- Detecting fraudulent SSL certs
- Enable hygiene analysis
- Analysis of “weak” cryptographic algorithms used in certificates