CE0973a - Issues in Network Security
8: Email Security

James A Sutherland

Abertay University

Monday, 29th February 2016

E-mail Security

As well as the general security issues of any service, email presents particular risks:

- Spam
- Phishing
- Interception
- Impersonation

Spam

No doubt we've all received spam in the past, but there are a lot of measures to block or mitigate it:

- SPF
- DKIM/DomainKeys
- DMARC
- Signed Envelope Sender
- Filters

SPF

Sender Policy Framework – RFC7208

`"v=spf1 ip4:192.0.2.0/24 a -all"`

- Version SPF1
- Mail from that IPv4 address block
- Any host matching this domain name
- Anything else is *definitely* fake, discard it
- (Alternatively, ~would imply *probably* fake)

SPF Results

- Prevents direct impersonation of `microsoft.com`
- Doesn't stop `m1crosOft.com` though
- Also causes problems with forwarding

DKIM/DomainKeys

- Started as DomainKeys and Identified Internet Mail
- Used by Gmail, Yahoo, AOL, FastMail
- Add cryptographic signature to outgoing mail
- Anything not signed is *probably* fake

DMARC

Domain-based Message Authentication, Reporting & Conformance – `https://dmarc.org/`

- Feedback/reporting mechanism
- "Report statistics to https://blah.com/dmarc/"
- Gives victims some feedback on impersonation/problems
- Otherwise, complaints someone is impersonating me never reach me

Signed Envelope Sender

- Bounce addresses are trivial to fake, so a spammer can cause a lot of backscatter.
- To avoid this, use dynamic senders on real mail – a timestamp or short signature.
- For example, fred-4371438748@example.com and treat any bounce to fred@ as junk.
- Clever, but needs *all* mail to go through such a server.

Filters

- Simple idea, hard to get right!
- Keywords easy to trick - \/1agr4, “blue pill”...
- More elaborate schemes: Bayes filters, IP reputation
- Always some false negatives, false positives, both bad

Attribution

Hard to identify real origin, but `http://www.spamcop.net/` does for free.

- Cisco owned
- Tracks spam to origin
- Sends complaints
- Also shares real-time intelligence for filtering

Phishing

- Common problem on low end
- Serious threat at high end: "spear-phishing"
- NSA tried at West Point: 80% click rate![1]
- Serious threat, average $\$1.6m$[2]
- Big business for pen testers

[1] http://searchsecurity.techtarget.com/definition/spear-phishing

[2] http://business-reporter.co.uk/2016/01/14/spear-phishing-incidents-cost-firms-an-average-of-1-6m/

Email interception

- Obvious issue: you have no control over senders
- Nor recipients
- If *both* ends support it, STARTTLS helps[3]
- End-to-end: PGP, S/MIME, policy e.g. sgov.gov
- Easy on recipient end: HTTPS, IMAPS, POP3S
- SMTPS (port 587) for sending with authentication

[3] `https://starttls.info/check/sutherland.pw`

End to end email security

- Sign and encrypt using S/MIME or PGP
- Problem: what is fred's key?
- Tricky (PKI v webs of trust)
- Proprietary systems – GroupWise, Notes – solve *internally*, mostly

Encryption at rest

- Amazon's new SMTP service can encrypt incoming mail on arrival using a public key you supply.
- Some proprietary systems do too, but difficult to achieve with IMAP or POP3.

Destination protection

- DNS spoofing: "I'm mail.example.com"
- Typos: exmaple.org
- Wrong TLD: microsoft.net
- Username on public systems: billgates v bill.gates

CIA view

- Confidentiality: encrypt in transit and at rest, protect destination
- Integrity: sign email, DKIM, verify origins
- Availability: DoS protection, spam precautions

Lab Work

- Find DKIM protected domain, study headers
- Find spam, study origins, run through Spamcop
- Investigate: was it detected? Was the origin protected?