Email from a DNS perspective

Tony Finch ⟨fanf2@cam.ac.uk⟩

Hostmaster
University Information Services
⟨https://www.dns.cam.ac.uk/⟩

May 2019 [*]

0 Overview

I am responsible for the University of Cambridge's DNS services. Until 2014 I was one of the maintainers of our central email services.

I discuss two issues below:

- The security of email affects the security of our DNS and other services (section 1). Because the DNS is a foundational service, its security affects everything else.

  We must maintain careful control over security-critical email addresses such as ⟨hostmaster@cam.ac.uk⟩ to avoid mayhem.

- Poorly-configured off-site email-related services cause a number of risks and problems (section 2).

  We should thoroughly revise our email policies so they provide up-to-date guidance both for UIS staff and IT staff around the University.

1 Security of email

I handle a number of information security processes related to authenticating ownership of domain names and the computing resources that they refer to. These processes rely heavily on secret tokens transferred by email, so the security of the University's domain names and other computer systems is critically dependent on the security of our email services.

For instance,

[*] Document source ⟨https://git.uis.cam.ac.uk/x/uis/u/fanf2/2019-05-email-review.git⟩
version 1.1 commit 4768401 date 2019-05-30 00:03:17 +0100

- Transferring ownership of non-cam.ac.uk domain names to or from other organizations;
- Authorizing web site TLS certificates that are not issued by our usual certificate providers;
- Proving to a third party that we control a domain and we permit them to set up an off-site service.

1.1 Trustworthiness of email

I am concerned that we should maintain high standards of reliability and debugability in our email service.

When handling sensitive email workflows I am confident that Hermes and PPSW will deliver messages with a very high degree of reliability.

On the rare occasions when things go wrong I am confident it is possible to for our email admins to help me with troubleshooting, and help work out what needs to be done to fix it. This is important when an authentication request does not arrive as expected.

1.2 Example: DNS-related email addresses

Putting these security and trustworthiness concerns into practice, a couple of years ago I reorganized our DNS support email addresses to separate internal support requests from external communications.

Internal support requests via ⟨ip-register@uis.cam.ac.uk⟩ may pass through less secure or trustworthy systems such as HEAT. Most of the risky communication is with external organizations via ⟨hostmaster@cam.ac.uk⟩; my aim is to keep this as safe as possible.

1.3 Implications for the cam.ac.uk mail domain

The choice of email address ⟨hostmaster@cam.ac.uk⟩ is largely not under our control: it is common for external organizations to construct this address given a domain name and speculatively send security-critical messages to it. For example this is one of the authentication mechanisms for issuing TLS certificates in the CA/Browser Forum baseline requirements [1] (section 3.2.2.4.4).

So the cam.ac.uk mail domain must be configured to allow us to implement any security policy that we decide is necessary for crucial email addresses such as ⟨hostmaster@cam.ac.uk⟩.

[1] ⟨https://cabforum.org/baseline-requirements-documents/⟩

2 Ancillary email services

Many University institutions use multiple off-site services that send email on their behalf, including:

- Full-feature mail services, primarily Microsoft Exchange Online;
- Mail security providers, such as Mimecast or Barracuda, used by a few institutions in preference to PPSW;
- Bulk mail services for newsletters, mailshots, and so forth;
- Other services that send email as part of their workflow, such as helpdesk systems.

I work with the email team and others to help set these up.

2.1 Segregating providers

We draw a distinction between an institution's primary mail service and the various ancillary services such as mailshots and helpdesks. In common with many other universities, we strongly prefer to set up ancillary mail services on subdomains, to avoid problems:

- A compromised account on a third-party provider can cause security and reputational problems for other mail from the same domain, leading to messages being blocked or discarded. The more services using the same mail domain, the greater the risk.
- The SPF mail authentication protocol [2] has very tight limits which prevent more than 3 or 4 off-site services on the same domain; if that limit is reached the domain can't use SPF, which will make it hard to reliably deliver mail to strict providers such as Google and Microsoft.

It is vexingly hard to follow this policy.

Typically, the documentation from third-party providers encourages their customers to set up the service on the primary domain. When our colleagues follow this documentation before contacting the UIS or consulting our documentation, we have to advise them to re-do the setup work.

Choosing names for these subdomains can be tricky, and sometimes involves lengthy discussions between various interested parties.

[2] ⟨https://en.wikipedia.org/wiki/Sender_Policy_Framework⟩

2.2 University branding

Ideally, newsletter, helpdesk, and similar services should be set up using University branding, including University domain names. This does not always happen.

- The University Reporter is a good example of this done well: the announcement messages use the `admin.cam.ac.uk` domain almost entirely consistently.
- The UIS HEAT helpdesk system uses the provider's domain name, because the provider does not allow us to use our domain.
- The UIS comms team use a number of off-site mailing lists with un-branded / obscured URLs.

In cases where University branding is not used even though it is possible, I get the impression that our colleagues find the setup process too difficult, even when help is available.

But unclear and inconsistent branding makes it easier for fraudulent messages to appear legitimate.

2.3 Wider implications

I regret that we have not always managed to find the right balance between getting the job done and not creating an unholy mess. To a large extent this is a matter of providing expert support and documentation; but the email policy-related documentation has been problematic for a very long time.

It is easier for us to require best practices if there is a clear policy that we can apply fairly and consistently. But the policy also needs to adapt to changing circumstances – preferably using a process with a bit more legitimacy than “the postmasters and hostmasters think it makes sense”.

I hope that this strategic review, and better policy documentation, will help raise awareness amongst University IT staff of email-related risks and best practice mitigations.

3 Coda

I welcome this long-overdue strategic review. Thank you for the opportunity to submit our thoughts, and thank you for reading them. I have only addressed a couple of tangential points; regarding the central questions of the review I largely agree with Dr David McBride.

I look forward to reading the report with great interest.