New IETF Working Group to address 'Email Security' issues? Discussion & Justification

Email is still the number one used service on the Internet

Business Email Compromise 23% Cyber-Insurance Claims

No current Working Group with the mandate to cross protocols

Data Leaks reaching all times high, Mass Authentication Botnets

Large percentage of people still using insecure POP/SMTP

Should Methods that allow for compromise still be in RFC's

Promoting Transparent Methods of Security like CLIENTID Drafts

Acknowledging the Problem
Developing a takeaway Problem Statement

Email Compromise is a Real Threat
- Compromised Email is no longer just for spamming
- Date Exfiltration, Personal Information, Contacts
  - Banking Information
  - Tools for Spear Phishing
  - Ransomware opportunities
- Access to Email allows take over of online services
  - Banking Information
  - Domain Name Ownership
  - Password Resets

Top Three Methods of compromising Email Accounts
- Data Breaches, re-used credentials
- Plain Text Transmission of credentials (sniffing)
- Brute Force attacks and easy to guess passwords

Identifying Key Problems
Developing a Mandate for a Working Group

Reviewing Current RFC's that encourage/support the use of insecure Authentication/access methods, across POP/SMPT/IMAP etc

Looking at other areas where RFC's and BCP's could be developed to Prevent Email compromises, and protect end users.

Examining CLIENTID RFC drafts for suitability and standards

Reviewing existing RFC's pertaining to email communication protocols

Other considerations for transparent 2FA that are easily adoptable by Community, and transparent to the end user.

Other Mandates? Stopping IoT Bots from performing Wide Spread email hacking?? TLS methods? Webmail Issues?

Why existing WG's are not suitable

An example was our own CLIENTID RFC Drafts which could not find a home in existing working groups for over a year, which only focused on single protocols (eg the 'extra' working group for SMTP)

Cross Protocol RFC's which are not suitable for generic 'security' WG's

Email represents a larger critical set of services which are embodied

Requires a different set of skills and experience for WG members

Requires understanding of Real World impediments to adoption of various recommendations.

Discussion on this point.. Are Alternative suggestions viable

Talking Points
Why do these common email risks exist?

Without a mandate of IETF RFC's and BCP's ISP's have no motivation to change, and are adverse to wholesale changes unless required.

Many ISP's still allow POP/SMTP Clear Text Authentication.

Email Clients still will allow connection via insecure protocols

Customers don't understand the implications (should not have to)

Customer's don't want to change their behavior

Customers don't want to use long complex passwords, hardware dongles, or complex setups or configuration.

Up to the vendors of Email Servers and Clients to change, but need support from RFC's in order to affect change.

Email Protocol Specification
Using CLIENTID as an example

POP/IMAP/SMTP protocol specifications from an earlier era.

Authentication over unencrypted channels not acceptable in the current internet environment. Users want it simple, so technology has to change. Modern email requirements not supported by legacy protocols. The ability to apply ACL's to who/what can access a resource. The ability to limit authentication attempts to authorized devices transparently. The ability to alert users/administrators when attacks or un-authorized attempts are made.

Several Email Clients already support initial DRAFT specifications
Several Server Vendors expressed interest in supporting it

Requires a change to cross protocol specifications to allow support.
What is the best forum/mechanism to move these DRAFTS forward?

Simple, Transparent 2FA for everyone
What we would like to achieve

Hello,

This is an auto-generated system alert.

Your account (michael@wizard.ca) had an access attempt rejected.

Device Signature:	IMAP Client, Linux (Unknown Mail Software)
Authentication:	Failure
IP Address:	208.53.45.68 (208-53-45-68.c7dc.com)
Country Code:	US
Date:	Mon, 23 Mar 2020 10:40:34 -0700

Don't recognize this activity?

If this WAS you, or one of your devices and you are traveling, or have a new device, visit the 'Security Settings' i and/or permitted devices accordingly.

Review your recently used devices now and update the status of your known devices, by following the link https://mail.cityemail.com/portal/communication/email/preferences/cid

-- Automated Security Notification System --

Note: The location is approximate and determined by the source IP address of the attempted login.
DO NOT REPLY TO THIS EMAIL.

You only check your email from a few devices, should any other devices in the world be using your email address and password?
Stops Brute force attacks, Password Reuse Problems, Insecure Auth