"Protecting Your Email"
MagicMail®

LinuxMagic
"Catch the Magic of Linux..."

Home | Features | Demo | Purchase | Support

Overview | News | Why Buy? | Clients | Partners

An Argument for CID adoption

Why Email Authentication Methods protocols need a more universal way to accept device identifiers (Informal Discussion)

https://tools.ietf.org/html/draft-yu-imap-client-id-00
https://tools.ietf.org/html/draft-storey-smtp-client-id-05

Speaker: Michael Peddemors
President/CEO of LinuxMagic
Audience: IETF - Extra

"Protecting Your Email"
MagicMail®

LinuxMagic
"Catch the Magic of Linux..."

Home | Features | Demo | Purchase | Support

Overview | News | Why Buy? | Clients | Partners

Background Information

- Developers of the MagicMail Email Platform
- Operated by 238 ISP's, Telco's and Cable companies
- Representing Millions of End User customers
- Over 20 years in the Email and Email Security space
- Supported many OpenSource and Proprietary IMAP
- Automated Feedback Systems and Analytics
- Intimate knowledge of real world industry issues
  - Allowing us to look at it from a different angle
- Working on a new approach to old problems for 2 yrs

The Problem CID wants to solve

- Making email security EASY to implement everywhere
- In spite of all previous recommendations..
- 70 Percent of Users Admit to Re-Using email/password
- Large Database Hacks in the news
  - Even an encrypted password can be broken in seconds
- Over 35% of ISP's still use default open source
  - Struggle with engineering skills/talent
  - If it isn't broke, don't fix it mentality, plain text still common
  - Enforcing TLS/SSL still a scary option to ISP's
    - Change means support calls or customer loss
- Compromised Email, it's not just to spam anymore

How the Industry Views Security

- More open to change than ever before
- Compromised Email accounts are expensive
  - Support Calls, Engineering expense, removal from blacklists
  - Increases Customer Churn from customer trust issues
- Issues with implementing stronger AUTH mechanisms
- TWO factor hard to implement
- Trust factors with 3rd parties more than ever
- First impulse is to 'give up email' or outsource
- That option doesn't make good business sense

What are we really trying to do?

- Allow customers to 'lock' their mailbox
- Where do you check your email from?
  - Home Computer, Office, Cel and Tablet..
  - Restrict ANY authentication type to permitted devices
  - While the holy grail is to restrict to 'people', not there yet
- ISP's afraid to 'enforce' modern security globally
  - 20 years history, and major percentage still don't
- Empower this at the domain and customer level
- Not everyone is Google/Apple/Microsoft
- Existing two factor methods are not.. easy for all
- Which leads us to offering an alternative..

Two and a Half Factor Authentication

- Jokingly call it, as CID is more that just two factor
- Universal adoption, means creating a 'standard'
- However, 'incremental' adoption is the only way
- Should help prevent Dictionary Attacks
  - Legacy Protocols reveal information used to facilitate
  - Currently a Large Scale BotNet used to dictionary attack
  - Identifies email addresses, targets, and data for sale
- Should help stop Brute Force attacks in protocol
  - ISP's still usually don't enforce tough passwords
  - Distributed attacks, hard for ISP's to stop without problems
  - Fail2Ban methods still most common, and not sufficient

CID Implementation overview

- Email/User and Password Problem..
  - Database Compromises and Password Reuse
- Brute Force/Password Guessing.. CID + password
  - Many more factors of difficulty for distributed bots
- Information only over Encrypted Channels
- Ability to limit to approved 'device types' / devices
- However, 'incremental' adoption is the only way
- Should help prevent Dictionary Attacks
  - Legacy Protocols reveal information used to facilitate
  - Currently a Large Scale BotNet used to dictionary attack
  - Identifies email addresses, targets, and data for sale

Arguments Against CID?

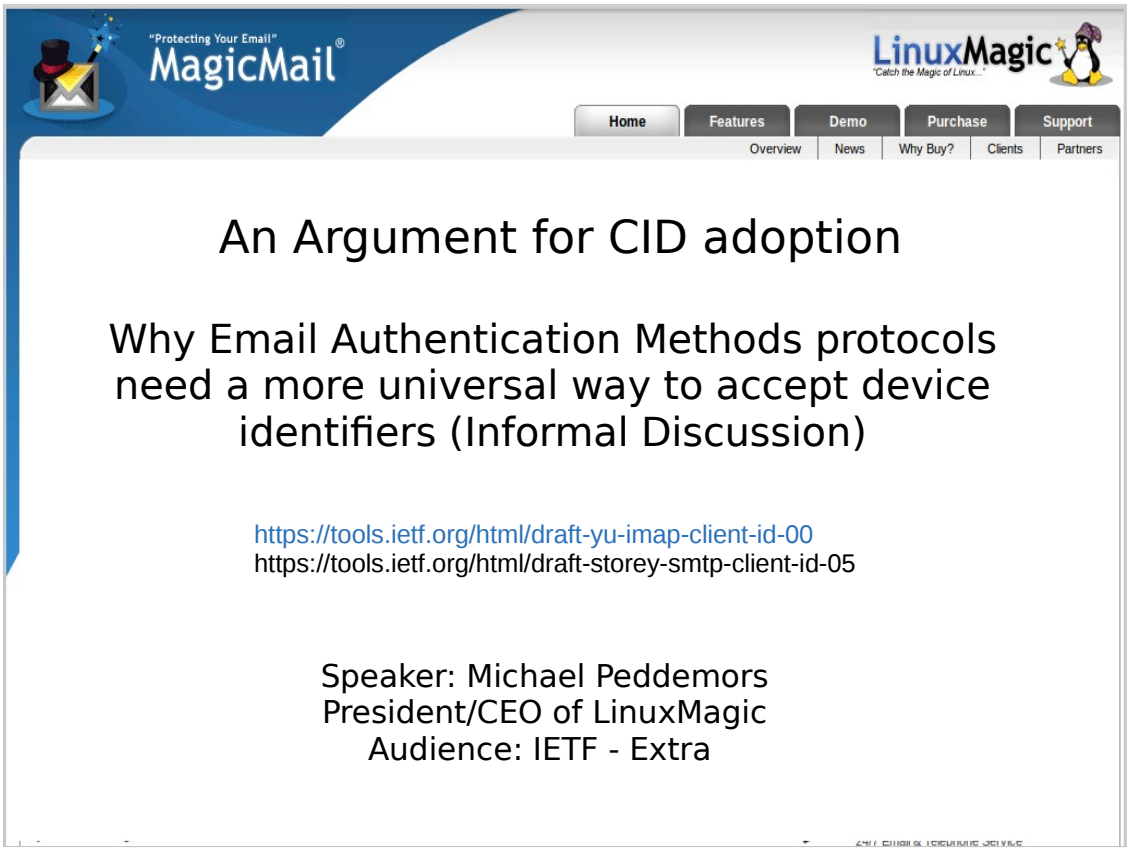
- Over two years examining the problem..
  - It isn't a technical problem, it is a real world problem
- Consulted with peers, partners..
  - Several other vendors support the concept..
- Suggestion that it should be stand alone SASL?
  - That's only two factors.. adoption problems, data leakage
- Suggestion that it be part of other implementations
  - Identifies email addresses, targets, and data for sale
- Consulting with industry experts..
  - This is why we are here.. implemented already but..
- 100% Backwards compatible, allowing easy adoption

And of Course Feedback..

- The Floor is yours.... Questions please..
  - Next steps.. for IETF RFC track..
  - Improvements on the Draft suggestions..

Question Period

https://tools.ietf.org/html/draft-yu-imap-client-id-00
https://tools.ietf.org/html/draft-storey-smtp-client-id-05

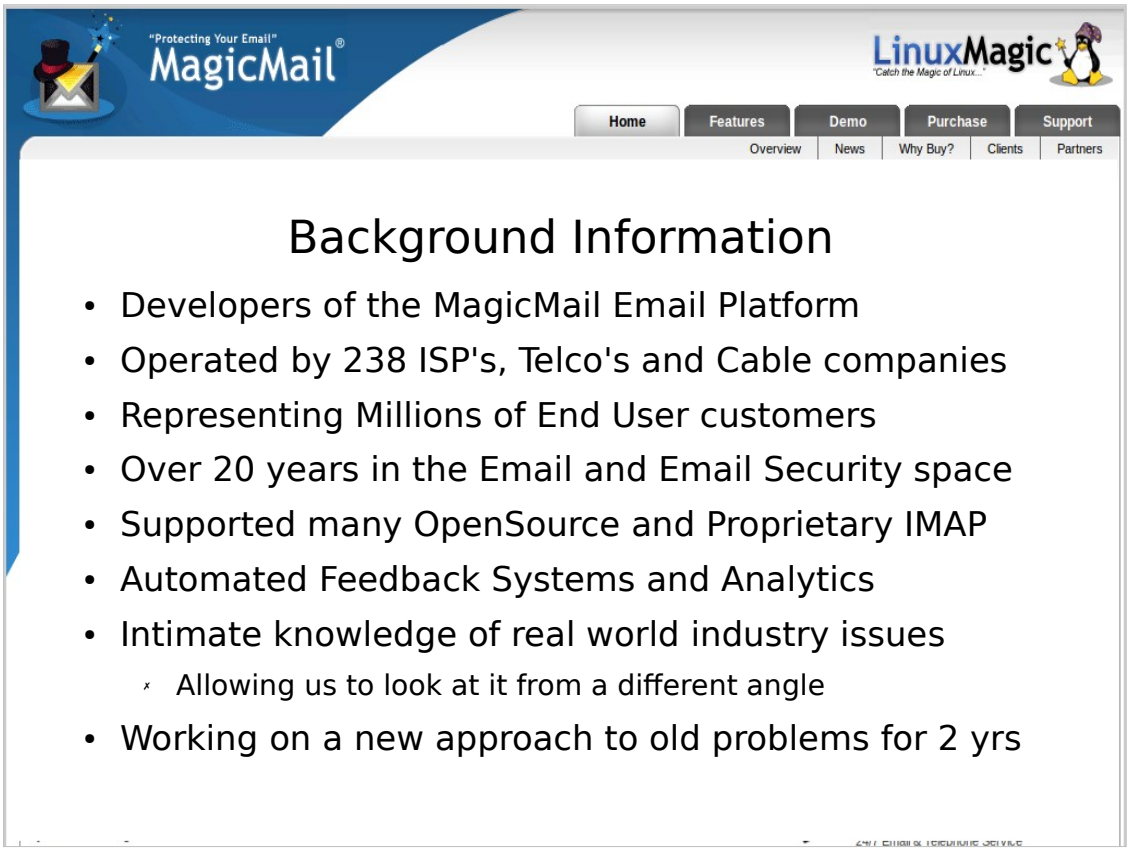


Hi, my name is Michael Peddemors, I'd like to first of all, thank my peers and the industry experts here today for being gracious enough to allow me to speak.

The conversation I would like to have here is the introduction of our RFC proposal for adding a new IMAP extension called 'Client ID', to help have it represented as part of the IMAP standards.

And I should beg your indulgence; while over the years as a company we have given back to the community in many ways, this is our first attempt at an RFC, and we are hoping that we can learn, gain feedback, and support from those of you with more experience.

And I hope you don't mind that I start off by spending a few minutes providing a little background for those of you who may not be familiar with me, our company, and of course the decisions leading up to this RFC proposal.



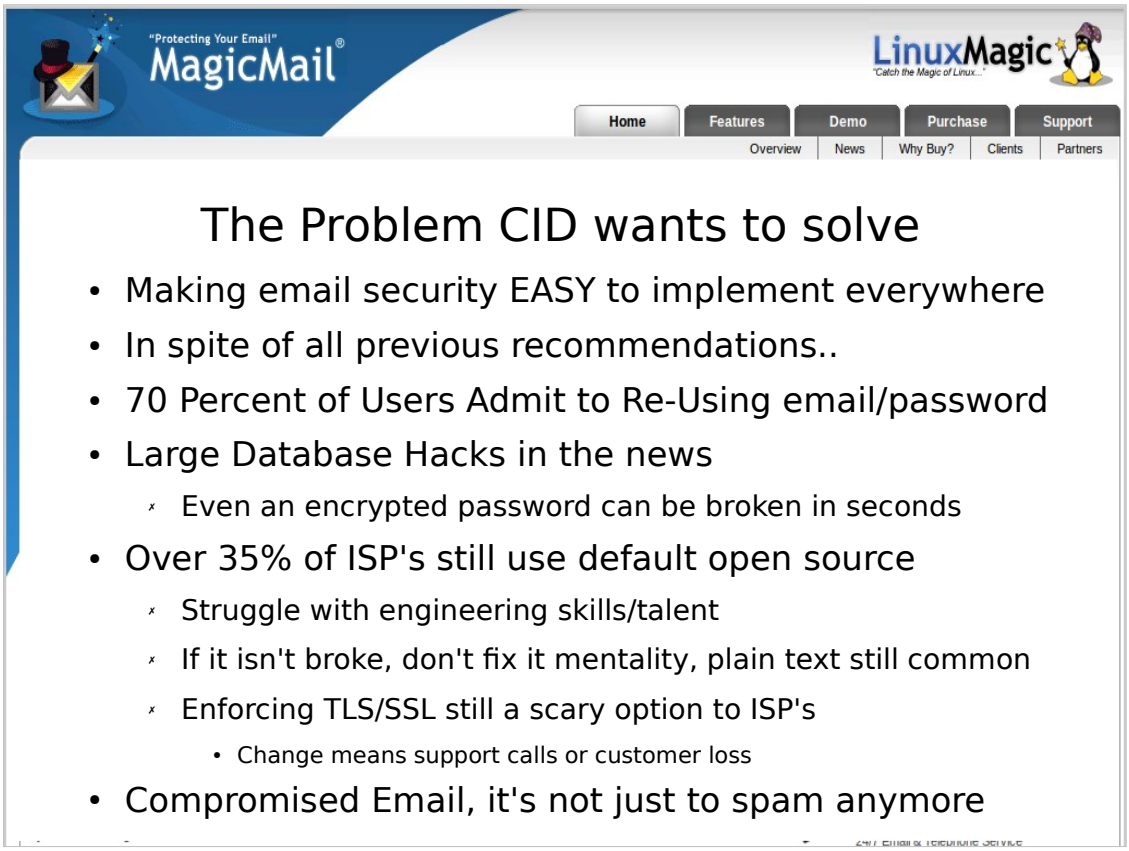
First of all LinuxMagic is our company, and we are the developers of many products and technologies in the email space, with our core product being 'MagicMail', a Carrier Grade On-Premise email platform for the ISP and Telco space.

And we are proud to say, that over the last 10 years, MagicMail has grown to be the number one on premise email platform in North America, with over 238 Internet providers relying on MagicMail for their customer's email, and representing millions of individual email accounts. We have been doing email development, support and services for more than 20 years, not only for our own products, but for both opensource and commercial platforms as well.

The trust relationships we have developed ISP's, the advanced automated feedback systems that we have developed, and the close relationships our support teams have with our partners, we see on a daily basis not only the industry pains, the problems that they face, but also the real world challenges in creating solutions to solve these problems.

And the challenge surrounding security and access to email accounts has been a problem we've been working on for quite some time.

Over the last two years, we have have applied considerable time, energy and thought on the concepts of how to address the situation in a way that is both easy for ISP's to adopt, while improving the user experience of the most used service in the world.



So lets just quickly review the world today, because I am sure most of you here have an understanding of the underlying issues, just so that you can better understand how 'our' experiences have led us to this RFC proposal.

Working with ISP's one of the things that becomes quickly apparent, is that implementing even the most simplest 'Best Practices' are, in the real world not as simple as the experts would make them out to believe.

New solutions HAVE to be very simple to implement, very flexible, and understanding of industry climate. And while security concerns have never been higher in the public's mind, in practice, the majority are NOT as tech savvy as we like to think, even for the simplest things we consider obvious. It was recently reported, that in a survey, 70% of all respondents admit to re-using the same email, and the same password at multiple different sites.

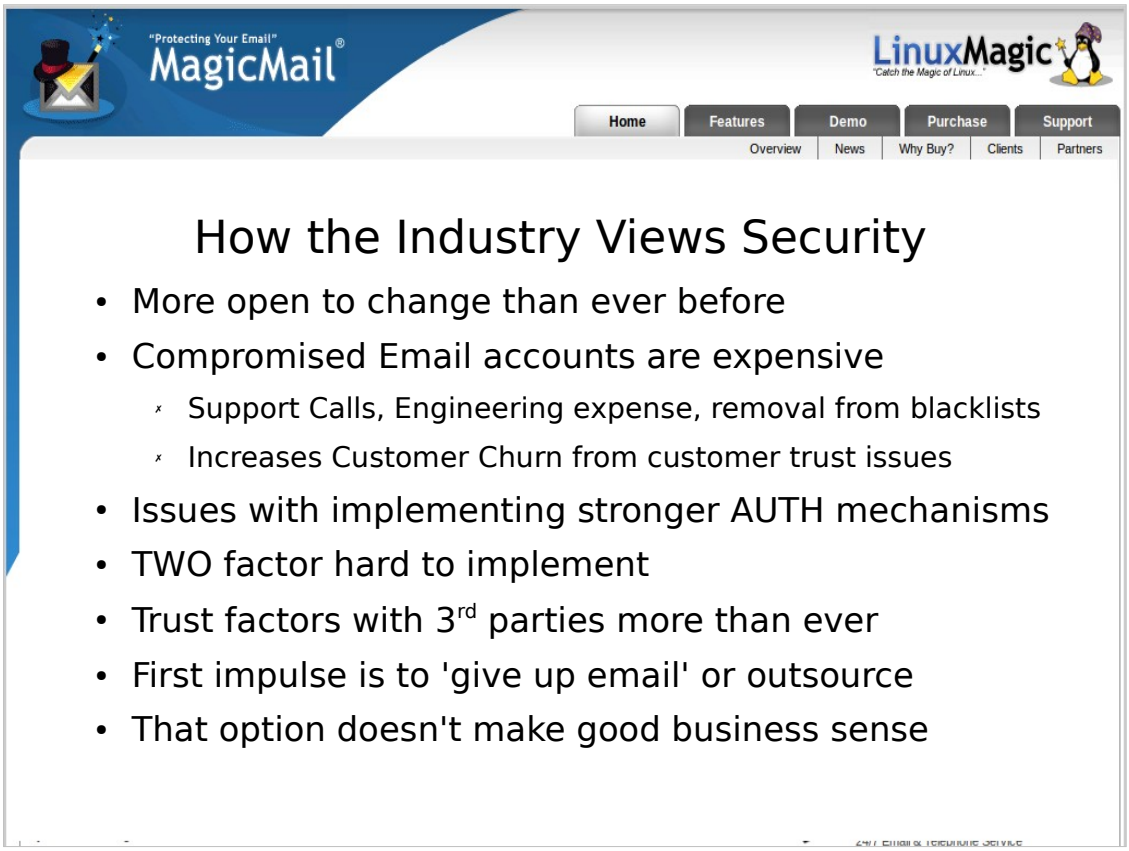
Simplicity and convenience seem to thwart security at every turn.

And we all know what that can lead to, a simple visit to any online database of compromised sites gives access to literally millions of authentication credentials. Even if encrypted, we know that it takes literally only seconds for a typical MD5 password to be cracked.

But it isn't just end users.. the email providers themselves have a part to play in this. But its not as simple as blaming them for poor email practices. While it is fairly easy to offer email as a service, to be an email security expert is difficult, and there are not enough of us to go around, and skills are getting expensive.

So what happens? ISP's are scared to change things.. in case it affects a customer adversely. Or, in general, they are just afraid of change and the complexity that may be involved. But on the other hand, they KNOW that they can't keep operating the way they have been.

A compromised account now means a LOT more than a little bit of spam leakage



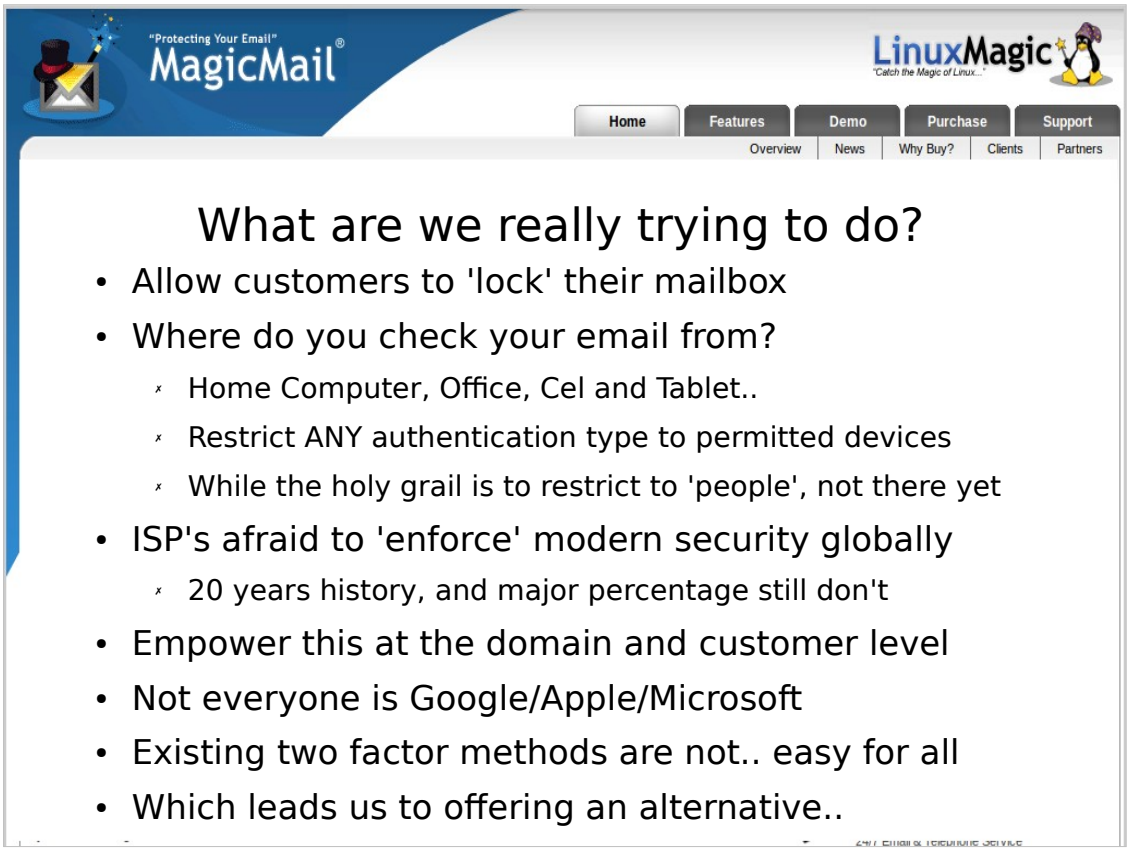
So, ISP's KNOW they have to change. They see it in the support costs, customer loss, and even more, they see it in the news every day. Hillary Clinton's hack was the start of this conversation, but not the end of it. But STILL, actually doing anything about it still scares the heck out of them as well. Change is Chaos. And frankly, they see that change as not only a threat, but very hard to do as well. So most operate email the same way they did 10 years ago.. Default loose configurations that 'work'..

ISP's still allow plain text logins over unencrypted connections, they can fix that with a click of a button, but they don't. Often, their idea of 'fixing' email security is simply to install a default installation of 'fail2ban'.

But it is reaching the point where the ISP's feel they are between a rock and a hard place when it comes to email.. so much, that 20% of tradition ISP's simply gave up trying to do email, and a further 30% have outsourced it, often because they can't keep up to the latest trends. But they ALSO know, giving up on email, is not the best business decision either..

So, we think we have a responsibility.. to make email security simpler, available to everyone, and flexible enough that it can be rolled out, without the fear and uncertainty of it breaking existing customers experience.

And one way to do this, is change the equation. And this ultimately comes back to ... the person who is accessing the email.

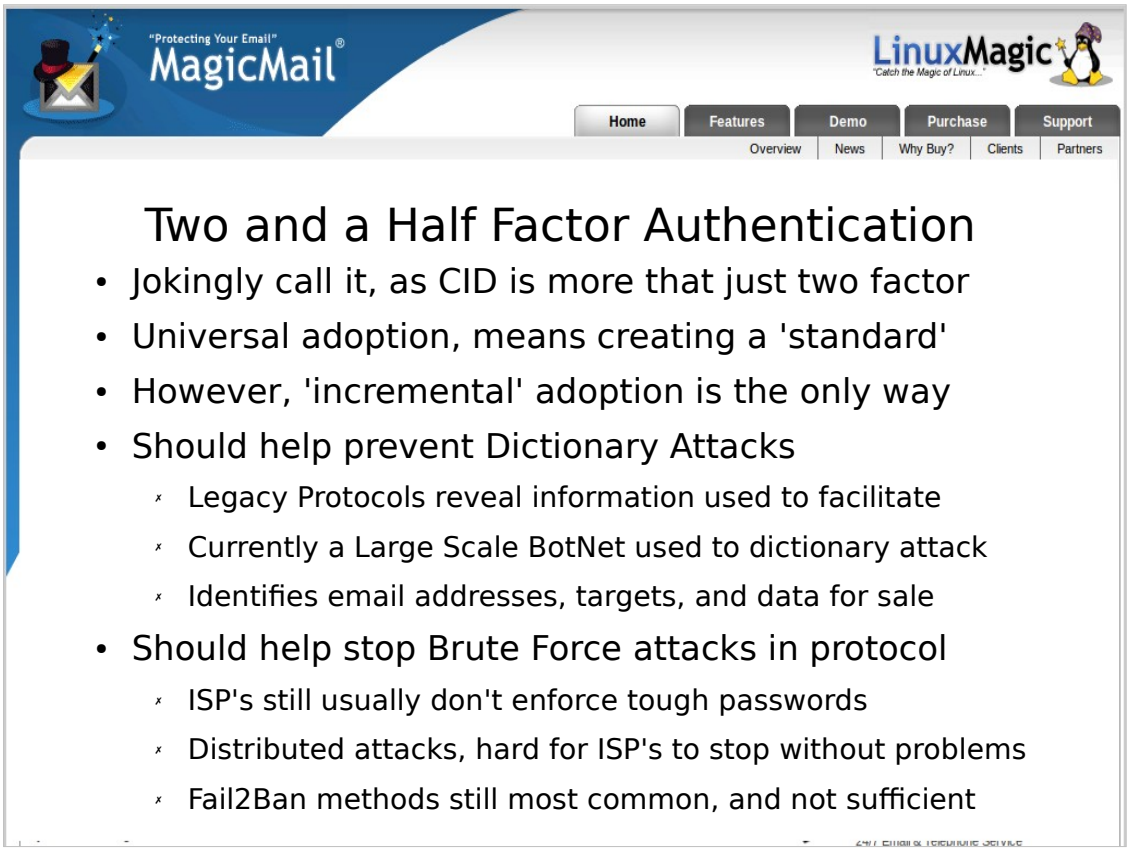


Well, to over simplify it.. We just want to make it so that users, companies, ISP's can simply 'lock' the mail box, so that only the authorized person can 'authenticate' to their mailbox, or for that matter to access it.

(Where do you check your email from?)

Now, we all know the holy grail is to make it so that only the 'person' or 'individual' who owns something, can access it.. But IMAP and other email protocols were never designed for that. Instead, it was designed so that a person can 'provide' authentication credentials and methods, in the theory that only the approved person would have or know those credentials.. Historically this was via simple ways like user name and password, and now many new and inventive ways have been introduced, especially amongst industry giants to make the 'authentication' more accurate, but still, the need for backwards compatibility have precluded the actual protocols from moving in the right direction, and many alternatives are still either too expensive or two difficult to implement for the average email system operator.

But, until we make it so that the 'individual' becomes the only person who can even use or 'present' their authentication credentials, in the mean time, maybe we can lock access to the 'devices' the person specifies as BELONGING to them.



And to be clear, this isn't about a 'better' authentication method, it is about how access and authentication in traditional protocols are handled.. it is about 'who' can even 'present' authentication credentials.. And while the 'identity' of the device can be thought of as 'two factor', it actually is more than that..

And while we believe strongly in this, and have now developed it for use in our own products and it already shows many advantages, we want to work towards universal adoption; and while we are planning to work/develop for other open source products and other industry partners, it is a lot easier when a standard can be agreed on first.

But given the lack of adoption at ISP's of even the current 'best practices', we see it can't be simply an on/off adoption model, it has to be something that can be 'incrementally' adopted, whether that is on an end user by end user basis, or by the email operators themselves, even the ability to do a little of this at a time has immediate gains, and that is part of what led us to this model.

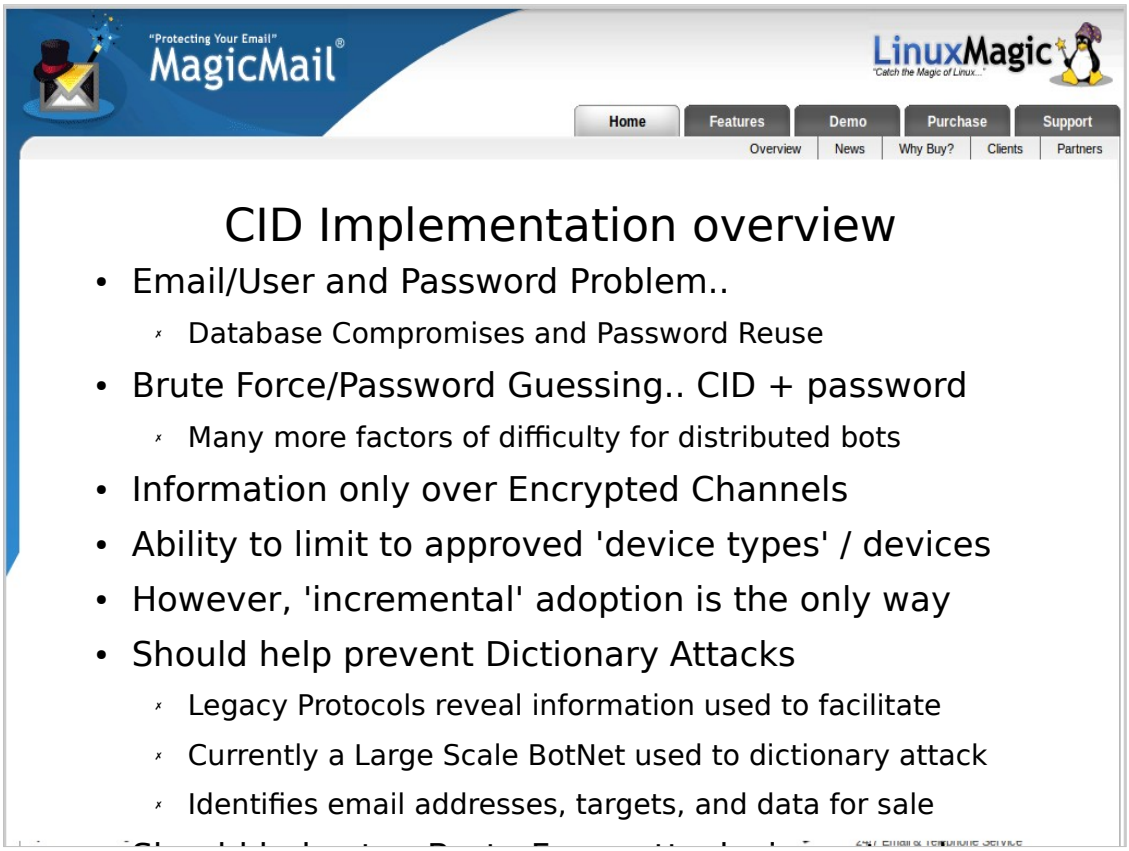
We say two and 1/2 factor, but it isn't all jokingly.. by changing the way we allow access, we address real world problems other than simply authentication, we address things like the ability to prevent dictionary attacks, which can reveal the existence of 'targets'. And given an attack, we can prevent even revealing if an attacker has learnt the actual authentication credentials via brute force. It even allows for new attack detection abilities.

Think about your typical home device alarm system with it's alarm code.

You can use a 'fail2ban' type method to prevent the number of guesses before being locked out, but you have to allow access again, so the real person can get it, so technically a person hiding in the bush can eventually guess your pass code, and he can present that, and gets access.

Of course if you added a camera that could tell it is you, before even allowing a person to guess, that person would never get a success/failure determination.. To fool both systems is much more difficult, but you can also tell if anyone who wasn't you tried to access the keypad at all.

Or you can have a 'class' of individuals that can use the keypad, the person trying the keypad would have no idea that you have to be over 6' to even use the keypad.

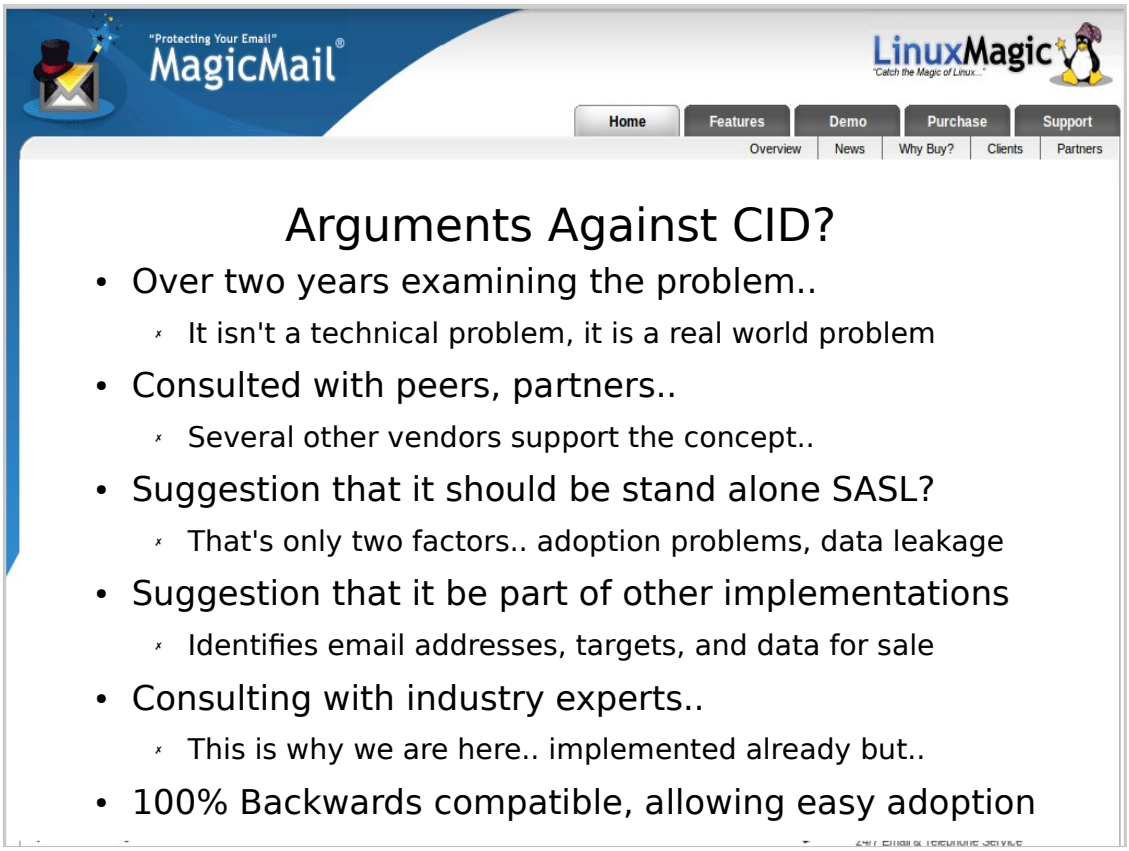


CID is our concept to address these problems, and it is especially important since we know how wide spread the problem is in the real world with authentication credentials becoming available/discoverable to person's other than the person who should have it. We can no longer be assured that the person who has it is the 'privileged' person with traditional protocols and methods, simply based on possession of those credentials alone. Other methods available in traditional protocols aren't sufficient, eg the IP Address, or the country.. Albeit they are helpful, they usually arent' enough to identify a 'person' in any form of semi-unique method.

CID will even 'help' traditional authentication methods be a matter of many factors more difficult. And since the identifier is NOT part of the authentication, and will ONLY be able to be transmitted across encrypted channels, and it will NOT be stored with the authentication systems themselves, helps preserve the integrity of the extra factor.

And it also allows for the added factor of systems being able to use traditional protocols, but limiting them to 'devices' they deem more .. well be it secure, approved, vetted.. be it at the server level, the domain level, or the user..

Given that at ISP's 25% of users might ONLY use web mail, eg your grandmother, wouldn't it be nice to ensure that some script kiddie hitting the POP or IMAP or SMTP layer doesn't have a chance to guess/sniff her simple to use password? But in a way that the ISP doesn't have to worry about breaking email for that one person using “Eudora 1.0” email client still.



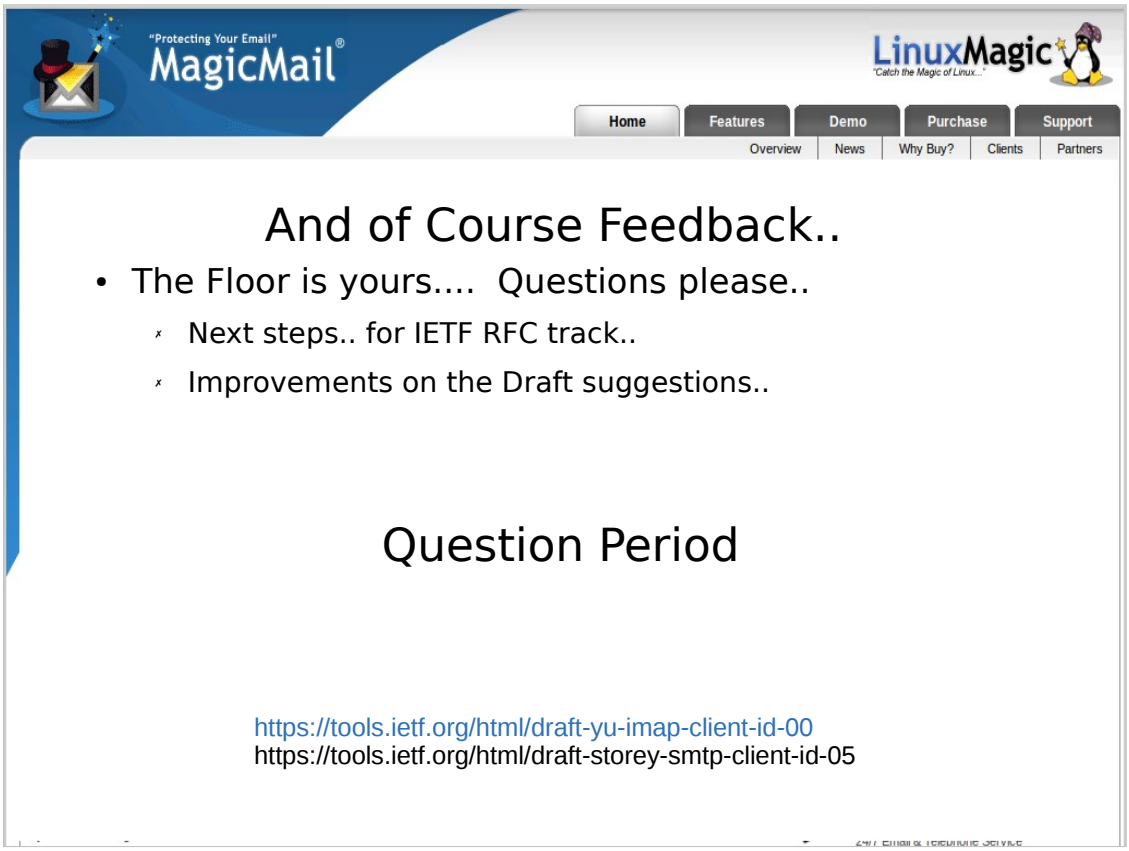
Now yes, we are strongly committed to the ideals behind this initiative, because our experience and expertise tells us this can and will be adopted, and our customers see it as a solution. Insofar as better 'authentication' methods are concerned, admittedly there are far brighter minds than just us working on those problems. But not all 'better' solutions are easy to implement/adopt, roll out, or use at the ISP level, or at the individual level.

We have spent considerable time on this problem, and have discussed it with peers and competitors alike.. but we recognize the IETF members and experts here might have both insight, recommendations, and even arguments against why our approach should be taken, and we would be foolish not to listen to your opinions.

Some have suggested it be part of a standalone SASL.. we considered that, but that model ended up with not only limitations, but we see it could also hamper adoption.. it requires change, as well as presents other technical and real world risks.

This should be available to all authentication implementations.. as well as the protocol levels themselves.

But here we have an opportunity to hear any arguments, but we are hoping to get consensus that this RFC should move forward to the discussion phase, and we are looking forward to help on perfecting the RFC with the advice and consultation that would result.



Everyone, I thank you for the time, and hopefully everyone has had an opportunity to review the concepts and the draft itself.. I can bring it up now, if it will help the discussions, or we can first discuss this in general terms.