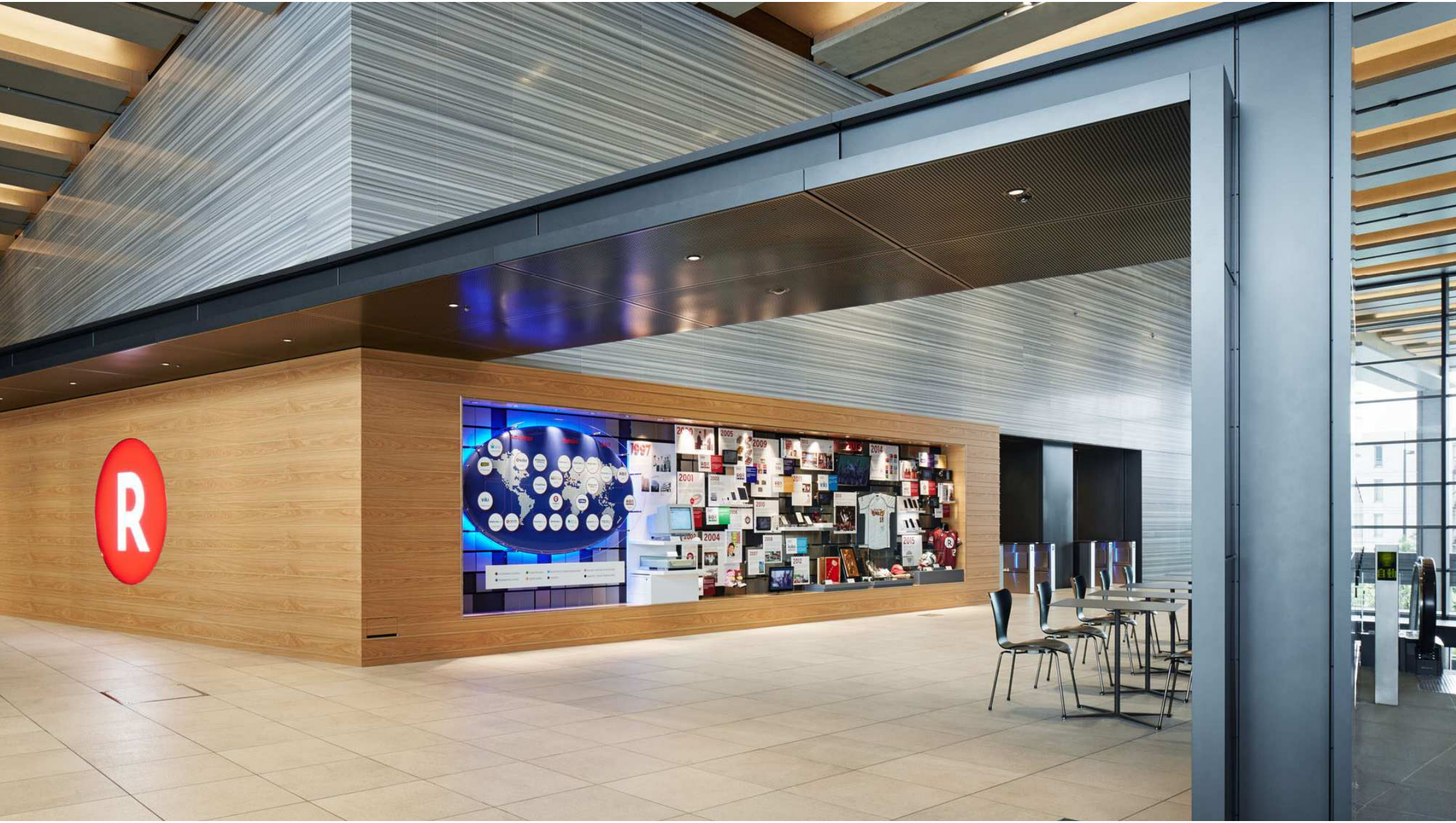
Virtual DMARC
DMARC verification without record definitions

Genki YASUTAKA

Rakuten, Inc.

Rakuten


R
1997
2001
2004
2005
2009
2014
2015

Outline

- What is Virtual DMARC?
- Why Virtual DMARC?
- How it's done?
- Why now?
- What have done?
- What's next?

What is Virtual DMARC?

- There are cases where DMARC evaluates to “pass” even without DMARC record published by the sender, assuming as if there is one. Receivers can utilize such results to find non-malicious messages.
- Why should we not treat these kinds of emails as "DMARC PASS"?
- We name this practice as “Virtual DMARC”.

Quick glance at Virtual DMARC

- Domains are strict align as bellow.
  - SPF PASS and RFC5321.From domain strictly matches RFC5322.From one
    - Ex) Both of RFC5321.From and RFC5322.From are local-part@example.com
  - DKIM PASS by Author signature
    - Ex) d=example.com and RFC5322.From is example.com

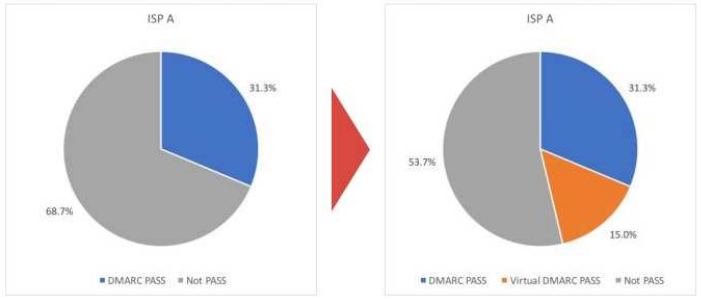
- Scope

		SPF or DKIM	
		Align	Not Align
DMARC record	Yes	dmarc=pass	None (p=none)
	No	None ↓ **Pass**	None

Effect of Virtual DMARC

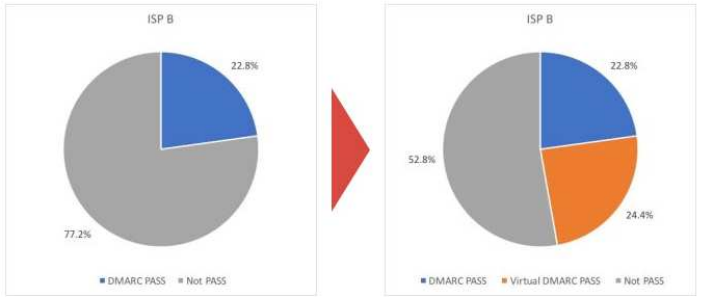
We simulated how “Virtual DMARC” would be effective, in cooperation with some Japanese ISPs.

- DMARC PASS -Blue zone on graphs.
- Virtual DMARC PASS -Orange zone on graphs.
- ISP A
  - Blue: 31.3%
  - **Orange: 15.0%**
- ISP B
  - Blue: 22.8%
  - **Orange: 24.4%**



The orange group shows the effect of Virtual DMARC. On the first chart, “DMARC PASS” is 33% of all traffic. When we apply
goes to 48%, which is 15 point increase.

Let’s move on to statistics from ISP B.



Quoted from https://www.vdmarc.dmarc.jp/?p=122

Why Virtual DMARC?

- The value of DMARC (very roughly speaking)
  1. Deliver legitimate (not spoofing) emails
  2. Do not deliver spoofing emails

- The value of virtual DMARC
  - **Contribute for purpose 1**
    - Receivers side get chance to increase the target emails for Domain reputation
    - While expanding DMARC adoption in the Receivers side, enhancing opportunities for DMARC declare in senders side. (maybe)

Why document now?

- As a similar standard, Microsoft adopts BestGuessPass (equivalent to relax)
  - This draft adopts only a case that it is absolutely pass (equivalent to strict) at the present time.

- Discrepancy between Virtual DMARC and DMARC
  - In case of no DMARC record, the Authentication-results code should be "none".
    - RFC 7489: DMARC does not evaluate if there is no record, and "dmarc=none" is inserted in Authentication-results
  - We'd like to define PASS (or BestGuessPass, SoftPass) in Virtual DMARC
  - **This is just discussion points on Phase III in DMARC WG.**
    - In fact, technically is pass

How it's done?

- Past practices documented in:
  - https://tools.ietf.org/html/draft-akagiri-dmarc-virtual-verification-02

- **Virtual DMARC is implementing and testing on yenma** (a milter program: http://enma.sourceforge.net/)
  - https://github.com/iij/yenma
- Investigating on Open DMARC

What have done?

- Past discussion
  - Out of scope in Phase II but possibility to include scope in Phase III on ML

  In previous discussion, Chair(Ned) made the following comment:
  https://mailarchive.ietf.org/arch/msg/dmarc/l8wd2wmO1mnoE3HRLB1sU8WW00c
- Past issue and how to solve
  - Added focus of document to Introduction and Problem Statement
  - Added Use cases section

  etc.

- Issues
  - Name(DMARC-Lite?)
  - Authentication-Result Code
  - Opt-in
  - Reporting part(rua/ruf)

  etc.

Rakuten

What’s next

- Implementation of Virtual DMARC to open source other than yenma
- Deployment of virtual DAMRC on receivers other than Microsoft (MS is BestGuessPass)
- Acquire the latest information on the effects of Virtual DMARC
- Discussion on ML
  - When there is no DMARC Record in RFC 7489, it is written as “None”, but I do not want to be “None”
    - We believe this is one of points in Phase III

- Is there any possibility to treat an WG item in Phase III?
- Can we do this together?

THANK YOU