Re-examining Email Spoofing in the Context of Spear Phishing

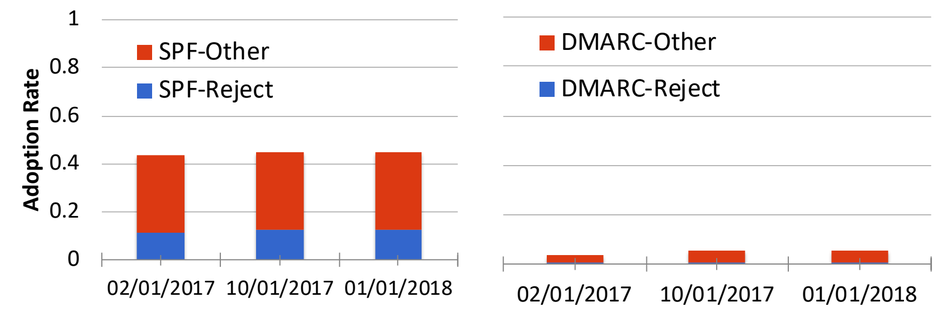
PI: Gang Wang, University of Illinois at Urbana-Champaign
https://gangw.cs.illinois.edu

The Problem

- Spear phishing: targeted phishing attack
- Often involves impersonation/spoofing
- How effective is spoofing during phishing attacks?
- How robust are existing defenses?

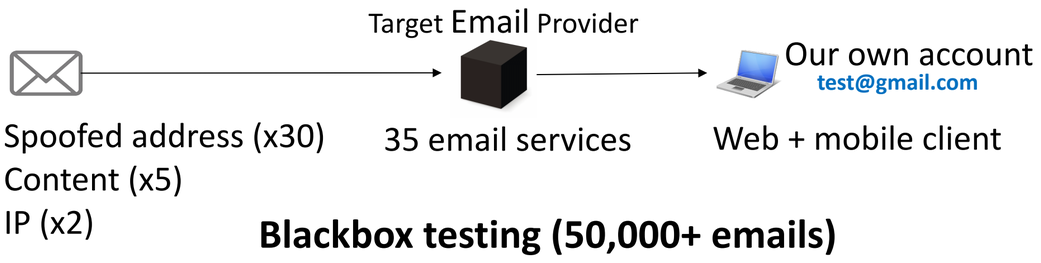
Method

- Measurement: anti-spoofing deployment and config. (SPF/DKIM/DMARC)
- Blackbox spoofing test on real-world email systems
- Users study with *users* and *email system admins*

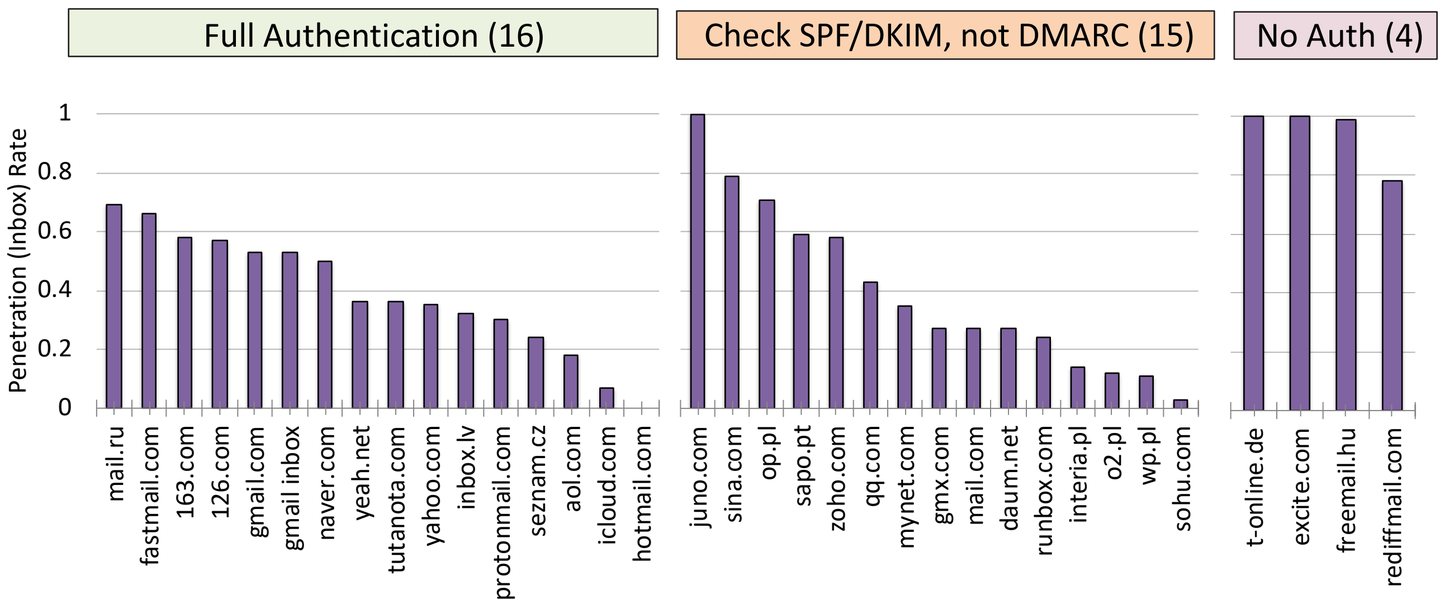


44.9% domains w/ SPF | 5.1% domains have DMARC

Measurement on Alexa top 1 million

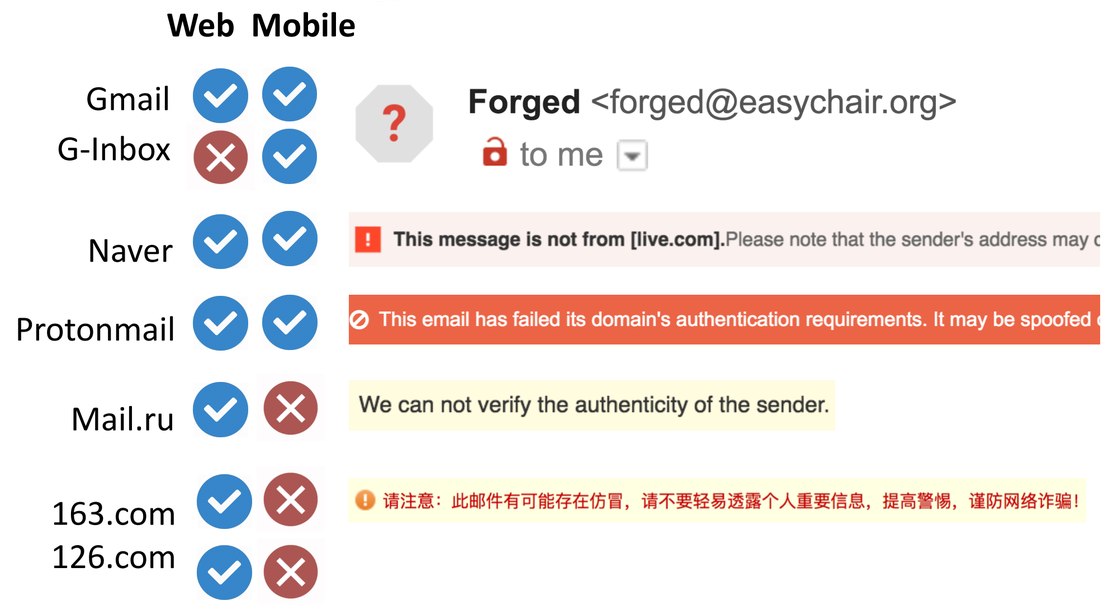


Blackbox testing (50,000+ emails)



Findings

- Anti-spoofing protocols not widely adopted or correctly configured
- 34 out of 35 email services penetrated by spoofing/phishing emails
- Even if both sender and receiver are configured strictly, 13% spoofing emails can still get into user inbox
- Security cues only appear in a few email UIs (even fewer on mobile UI)



User Study

IRB Approved

Q: how much does security indicator help?

- N = 488 (email users), send spoofing emails to subjects
- Ethical deception, to measure realistic user reactions
- Security indicator reduces click rate 48.9% → 37.2%

Q: why are anti-spoofing protocols not widely adopted?

- N = 9 (email admins), interview, open-ended questions
- Protocols have technical flaws (especially SPF, DKIM)
- A lack of critical mass, benefit not outweigh cost
- Deployment difficulties in practice

Ongoing/Next Steps

Measurement

- Reactive honeypots
- Collecting behavioral data by interacting with attackers

Defense

- Human-machine collaboration for defense
- Machine learning + explanation techniques to generate personalized indicators

NSF Support

- **CNS-1750101**: CAREER: Machine Learning Assisted Crowdsourcing for Phishing Defense
- **CNS-1717028**: SaTC: CORE: Small: Securing Web-to-Mobile Interface Through Characterization and Detection of Malicious Deep Links

References

- "End-to-End Measurements of Email Spoofing Attacks". H. Hu, G. Wang. Proc. of USENIX Security, 2018
- "Towards Understanding the Adoption of Anti-Spoofing Protocols in Email Systems". H. Hu, P. Peng, G. Wang. Proc. of SecDev, 2018
- "LEMNA: Explaining Deep Learning based Security Applications". W. Guo, D. Mu, J. Xu, P. Su, G. Wang, X. Xing. Proc. of CCS 2018