**Password Managers: Risks, Pitfalls, and Improvements**

David Silver, Suman Jana, Dan Boneh

---

### Types of Autofill

**Automatic Autofill**

- Fits without user interaction
- Enables many attacks

**Manual Autofill**

- Login
- User never visits or logs into site, yet attacker steals password from password manager

---

### Sweep Attacks

**Sync Amplification**

- Force browser to load login page
- Inject malicious JS into login page
- Steal passwords without user knowledge or interaction

**iFrame Attack**

- Secure Home Network
- Cloud Sync
- Passwords can be stolen from any device PM syncs with!

**Window Attack**

- Attacker's Network

**Redirect Attack**

- User requests a.com
- Attacker redirects user to b.com
- Attacker attacks b.com
- Attacker redirects user back to a.com

**Coffee Shop Attacker (2 Stages)**

1. Secure Home Network
   - User logs in to site, saves password in password manager
2. Attacker-controlled Network
   - User never visits or logs into site, yet attacker steals password from password manager

---

### Defense: Secure Filling

- Manual autofill: require user interaction before filling
- Make password field unreadable to JavaScript
- Allow login form to submit only when action matches action when password was saved

---

**Modifying the login page**

- Login Page over HTTP
- Broken HTTPS
- Active Mixed Content
- XSS Injection
- Router admin page HTTPS cert

---

**Stealth Exfiltration**

- Even manually typed passwords can be exfiltrated - a problem password managers can help solve

---

**Cloud Sync**

- 17% of the Alexa Top 500 sites served login pages over HTTP but submitted over HTTPS

---

**Password Managers more secure than manually typing your password!**