Common Flaws of Distributed Authentication and Identity Systems

Brad Hill

Me

- iSEC Partners: 2005 – Mid-April 2011
- PayPal ISG: Mid-May 2011 - ???

- Reminder: This workshop's RFP close: Early April 2011

My position paper does not necessarily reflect the views of my current or former employer.

What I used to do:

- Break things (application security consulting)
- Looked at lots of authentication systems
  - For hire
  - For fun
  - As historical background to the above
- Found lots of bugs and flaws
  - WS-*, Public Key Kerberos, many more under NDA

Lots of the same flaws

- Or flaws that rhyme
- Pentesters develop an intuition about such things
- A bit different than an academic researcher might

My project: Make that intuition useful to others

- Train other security testers
- Educate developers and designers to reduce avoidable mistakes
- Risk management targets for ecosystem participants

“Common Flaws and Failures of Distributed Authentication and Identity Systems”

- An “OWASP Top 10” for enterprise and federated authN systems

- Presented at RSA 2011
- Whitepaper at:

  https://www.isecpartners.com/

  Research -> White Papers

The Top Flaws and Attacks

1. Unconstrained Delegation
2. Unbound Composition of Transport and Message Security
3. Un-Scoped or Over-Scoped Authority
4. PKI, PKIX and SSL/TLS Dependencies
5. Impedance Mismatch in Identity Contexts
6. False Dilemmas in Adoption vs. Assurance
7. Confused Deputy and DoS Attacks against Key Discovery and Revocation Checking
8. Crypto Implementation Foibles

ID in the Browser context:

1. Unconstrained Delegation = OAuth 2 token leaks
2. Unbound Composition of Transport and Message Security = TLS Renego, WWW-Auth forwarding attacks
3. Un-Scoped or Over-Scoped Authority = Compromised and/or incompetent CAs
4. PKI, PKIX and SSL/TLS Dependencies = All of the above
5. Impedance Mismatch in Identity Contexts = ID in the Browser is inherently cross-contextal
6. False Dilemmas in Adoption vs. Assurance = No signatures in OAuth2
7. Confused Deputy and DoS Attacks against Key Discovery and Revocation Checking = *K.I.S.S.*
8. Crypto Implementation Foibles = *Not quite there yet today…*

What I will be doing:

- Now at PayPal's Internet Standards and Governance group (with Jeff Hodges, Andy Steingruebl, et al.)

- Work in the context of W3C and other orgs to develop, improve and promote new and existing security standards for the web

What I'm here to do:

- Officially unaffliated
- Here as an interested "expert" to help work towards the ambitions of my paper and contribute a perspective on WCPGW.

  (What Could Possibly Go Wrong?!?)

- Unofficially acquire context and connections for my new role and goals

Thanks!

Brad Hill

hillbrad@gmail.com
bhill@paypal.com

skype + twitter: hillbrad