Using Covert Communication to Enhance Security

Presented By:
Mohammed Almeshekah

September 7th, 2013
Motivations
Motivations

Traditional security focuses on preventive techniques.

However, vulnerabilities always exist!

We mainly focus on the aftermath.

Can we be preemptive in security?

Adversaries view of the attack result in binary.

Can we change that?

There are no risks on the attacking side to probe a system with particular exploits.
Authentication and Phishing Challenge

- Servers traditionally provide “all-or-nothing” access.
- If someone gets your username/password, you’re done.
- Adversaries can try all the credentials to see which “works”.
- When user account is compromised we know when the user complains.
Can we do better?

Username/passwords not always work (at least not for everything).

Phishers can get in, but not to the real accounts.

Know that the user’s account is compromise the moment attackers try to login.
Preliminary Solution

Based on password-based authentication.

Goals:

- Same interfaces.
- Simple for users to remember.
- Alleviate the damage of password compromise.

The user needs to choose one word from a dictionary of words.

No randomness requirement!
User enters her normal username and password.

Following the password the user enters a space and either:

- His choice of word → Normal login from trusted machine/network.
- Any other word from the dictionary → Whenever there is doubt.

Username : Alice
Password : pass<sp>wi
Beyond Passwords

Biometrics - e.g., the choice of which finger to use, the angle, and the pressure can be used to express some information.

Multi-factor authentication:

- Two-factor and active man-in-the-middle attacks.
- The multiplicity of factors provides a new communication channel.
Stored Credentials Challenges

In password DBs leakage, all what the adversary need is to crack it.

The retrieved credentials work by definition.

Such incident are not easily detected.
Can we do better?

A solution presented by Jules and Rivest.

Add \((N-1)\) saved credentials to the DB.

The adversary has to crack \((N)\) instead of \((1)\).

\((N-1)\) of them are beaoning credentials to alert system admins that DB has been cracked whenever used.
Final Remarks

- Interesting applications.
- Creating doubts and risk at the adversary side.
- The grand vision of authentication.
- Risk analysis and economics.
Acknowledgment:

This work was done in collaboration with Prof. Mikhail Atallah and Prof. Eugene Spafford.

Thanks to Prof. Marina Blanton and the NSF.

Portions of this work were supported by National Science Foundation Grants, Science and Technology Center, King Saud University, Qatar National Research, and by sponsors of CERIAS.

References:


Ari Juels and Ronald L. Rivest, “Honeywords: Making Password-Cracking Detectable”. 

Students Knowledge Exchange                         Using Covert Communication to Enhance Systems Security and User Authentication                         Sept 7th, 2013
Questions?

Mohammed Almeshekah
email: malmeshe@purdue.edu
twitter: @meshekah
presentation: