Defense Innovation Technology Challenge: Tampa, FL, US

Jay Ligatti

- Name of Organization: University of South Florida
- Technology Title: Coauthentication
- Date: October 5, 2017

Organization Information:

- Name: University of South Florida
- Specifically:
  Software-Security Research Lab in the
  Department of Computer Science and Engineering
- Founded: Lab has been running since 2006
- Location: Tampa, Florida
- Website: www.cse.usf.edu/~ligatti
- Employees: 3 faculty + 6 PhD students
- Mission: To improve software security through research and tech-transfer of our research

Technology Information:

- Coauthentication is:
  - A system and method of authenticating
  - No passwords
  - No biometrics
  - => *Single-factor* authentication
  - => Uses the “what-you-have” factor
  - (but can be combined with other factors)

Technology Information:

- What's new about just using the "what-you-have" factor?
  - Surprisingly much, when you *require multiple devices, in order to authenticate*
  - New systems, protocols, designs

Technology Information:

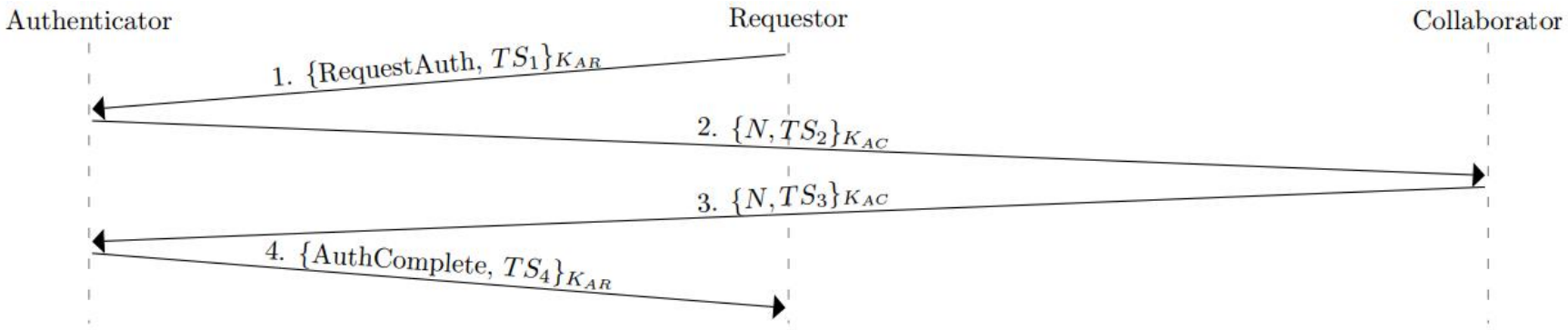
- A key feature of coauthentication—
  - *No new hardware required*
  - *Works with your existing devices*

Technology Information:

- Example application:
- (1) To log in to a web service, both your laptop and your smartphone must participate in a cryptographic challenge-response protocol with the web server

- (or your smartphone and smartwatch,
  or your smartphone and fitbit,
  or your smartphone and smart ID/dog tag,
  etc.)

Technology Information:



Technology Information:

- Benefit: Unlike authentication based on a single what-you-have device, stealing or compromising one of the required devices does not grant access
  - => *To be successful, attackers must steal/compromise multiple devices*

Technology Information:

- Benefit: Unlike authentication based on a single what-you-have device, stealing or compromising one of the required devices does not grant access
  - => *To be successful, attackers must steal/compromise multiple devices*
- *This is the benefit of multi-factor authentication*
- => ***Coauthentication provides mutli-factor protection with single-factor usability***
- *(i.e., the usability of the what-you-have factor)*

Technology Information:

- More example applications:

- (2) To enter a locked/gated area, the smart vehicle and the driver's smart phone must authenticate with the lock/gate

Technology Information:

- More example applications:
- (2) To enter a locked/gated area, the smart vehicle and the driver's smart phone must authenticate with the lock/gate
- (3) Multiple smart devices of authorized users must authenticate use of certain weapons
  - => classic "2-person policy"

Technology Information:

- Stage of Development:
  - 2 patents granted + 2 pending:
    - US Patents Nos. 9,659,160 and 9,380,058
    - US Patent Applications 15/598,974 and 15/644,371

- We've fully implemented coauthentication as Java libraries, so they can be plugged into existing software (not hard to do… <1month)
- Can adapt libraries to plug into other systems
  - E.g., can rewrite these libraries in other languages like C/C++

Technology Information:

- Runtime Performance Analysis
  - Coauthentication is as fast as password verification, *even excluding the time it takes to enter passwords*

- Can *automatically* update the cryptographic keys with every coauthentication
  - provides security benefit analogous to resetting your password on every use

Technology Information:

- We have also modeled our protocols in ProVerif and formally verified the important security properties

Technology Information:

- We have also modeled our protocols in ProVerif, and formally verified the important security properties

- I.e., under explicitly stated assumptions
  - e.g., attacker doesn't obtain all *n* required cryptographic keys
- Coauthentication mechanisms only authenticate legitimate users
  - e.g., no man-in-the-middle attacks, as exist with password and password+SMStext systems

Military Applications:

- *Any use of authentication*
- Authentication happens now whenever
  - passwords are entered,
  - keys are used—physical or digital—or
  - biometrics are scanned

- Coauthentication is particularly amenable to "continuous authentication" (due to usability)

Ask/Funding/Financing/ROI/etc:

- We are part of a state institution
  - More interested in seeing our technology used
  - Want licensing terms to be favorable
- Have licensed coauthentication to StoneVault, LLC
- Seeking more licensees
- More information:
  - Steven Medina, License Manager
  - stevenmedina@usf.edu
  - Tel: 813-974-3085

Thank You!

Jay Ligatti (ligatti@usf.edu) (Tel: 813-974-0908)

Please feel free to contact me.

We've only scratched the surface of coauthentication

For more technical information and documentation:

Do an internet search for "coauthentication", which should bring you to the project homepage:
http://www.cse.usf.edu/~ligatti/projects/coauthentication/