Requirements for Secure Device Authentication

"Identity in the browser" workshop, 24-25 May 2011, Mountain View

Mark Watson, Mitch Zollinger, Wesley Miaw

NETFLIX

Contents

- What is the problem ?
- What is “secure device authentication” ?
- How do we use it ?
- What do we mean by “secure” ?
- What about privacy ?
- Conclusion

NETFLIX

What is the problem ?

- Several interesting services rely on *guarantees of device behavior*
  - Example: HD content that can only be provided to devices with media protection capabilities
  - Example: Sensitive financial data that can only be provided to certain tamper-proof devices
  - No concept like this on the web today
- How does a service determine whether a device has the required properties ?
- Some services have restrictions on the number of devices that can be used with one user account

NETFLIX

What is device authentication ?

- A means for a service to securely determine
  - The type of device accessing the service
  - A unique identifier for the particular device that remains constant over time
- But not …
  - A common device identifier across multiple services

NETFLIX

How do we use it ?

- To make authorization decisions
  - Example: HD content only allowed to devices with certain special security properties
- Enforce service restrictions
  - Example: number of active devices on one account
- Revoking service access for compromised devices

NETFLIX

What do we mean by "secure"?

- Only that we can determine the security properties with known reliability
- Some devices may provide very limited assurances
  - Identity protected by software techniques: obfuscation, IBX etc.
- Other devices may provide stronger guarantees
  - Trusted Hardware Security Module
- *The strength is implicit in the identity*
  - Need out-of-band information to interpret it
  - Example: device identity provisioned by device manufacturer and signed with manufacturer public key: Need to ask the manufacturer about the properties of the device
  - Services that care have sufficient incentive to obtain the necessary information

NETFLIX

What about privacy ?

- A device identifier is Personally Identifiable Information
  - Even if the identifier is different for each service
- User consent is required to transmit it to a given destination
- Even with consent, we must ensure it is only sent to the user-approved destination
  - *services must be authenticated to the user's satisfaction*

NETFLIX

Possible approach

- JS API for service device authentication
  - Separate identity per origin
  - Only available to authenticated JS code (e.g. code received over https)
  - Key agreement for temporary keys
  - Functions for encrypt/decrypt using device and temporary keys
  - Functions to create/verify MACs using device and temporary keys

NETFLIX

Conclusion

- Some services not possible on the web today due to
  - Lack of guarantees on device behaviour
  - Lack of ability to count devices on one account
- Secure device authentication can solve this
  - With generally-applicable capabilities
  - Without compromising privacy
  - Without standardizing device properties (implicit in identity)
- *Interest in working on solutions ?*

NETFLIX