Secure Systems Group, Aalto University

Thanh Bui, Siddharth Prakash Rao, Markku Antikainen and Tuomas Aura

Man-in-the-Machine: Exploiting Ill-Secured Communication Inside the Computer

MitMa attacks

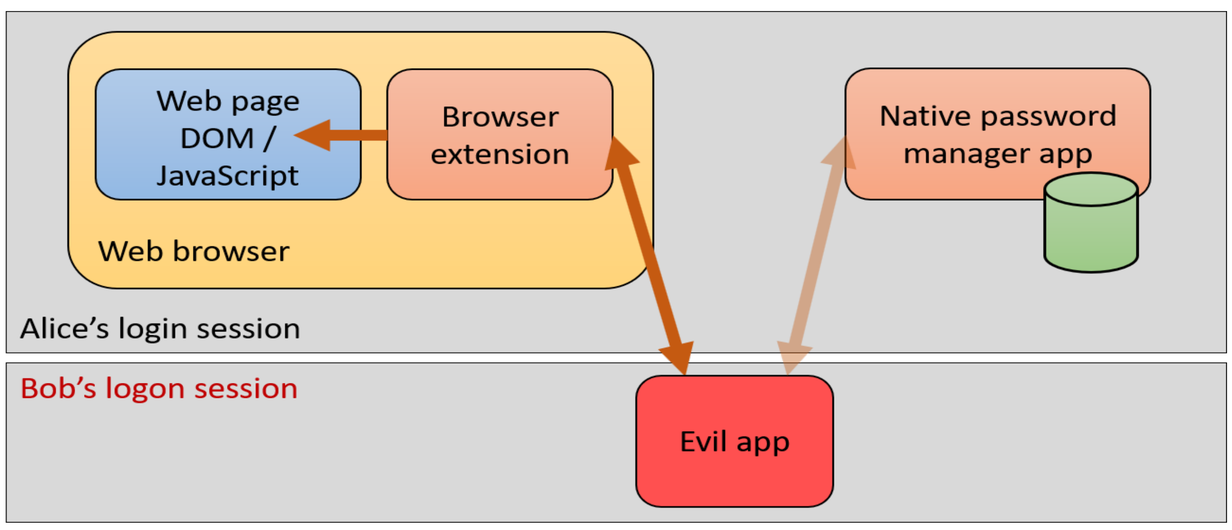
- Attack by unprivileged user against inter-process communication of another user on the same computer
- Attacker: background login session or process on a multi-user computer, e.g. guest user after fast user switching
- Target: software with frontend and backend components

Attack vectors

Channel	Attacks
Network sockets	- Client impersonation - Server impersonation - Man-in-the-middle
Windows named pipe	
USB HID	Unauthorized access

Case study 1: Password manager

- Desktop app communicates passwords with browser extension over network socket or named pipes
- MitMa attacker hijacks the port or the named pipe to impersonate the app to steal the passwords



Results

Application	Communication channel	Attacks
Roboform	Network Socket	Client impersonation
Dashlane	Network Socket	Server impersonation
1password	Network Socket	Server impersonation
F-Secure Key	Network Socket	Client impersonation Server impersonation
Password Boss	Named pipe	Man-in-the-middle
Sticky Password	Network Socket	Client impersonation Server impersonation
FIDO U2F Key	USB	Unauthorized access
DigiSign	Network Socket	Client impersonation
Blizzard	Network Socket	Client impersonation
Transmission	Network Socket	Client impersonation
Spotify	Network Socket	Client impersonation
MySQL	Named pipe	Man-in-the-middle
Keybase	Named pipe	Server impersonation

Password managers · USB hardware tokens · Backends with HTTP API · Others

Case study 2: FIDO U2F Key

- Web browser obtains 2nd authentication factor from FIDO U2F key over USB HID
- MitMa attacker impersonates the browser to steal the factor

Mitigation

- Spatial and temporal separation
- Proper access control
- Secure key exchange
- Avoiding named IPC mechanism
- Architectural changes

Aalto University · HELSINGIN YLIOPISTO

Full paper
Bui, T., Rao, S. P., Antikainen, M., Bojan, V. M., & Aura, T. (2018, August). *Man-in-the-Machine: Exploiting Ill-Secured Communication Inside the Computer*. In 27th USENIX Security Symposium (USENIX Security 18). USENIX Association.

Contact: siddharth.rao@aalto.fi, markku.antikainen@helsinki.fi