Messy States of Wiring: Vulnerabilities in Emerging Personal Payment Systems

Jiadong Lou*, Xu Yuan*, and Ning Zhang†

* University of Louisiana at Lafayette

† Washington University in St. Louis

Online Payment Service

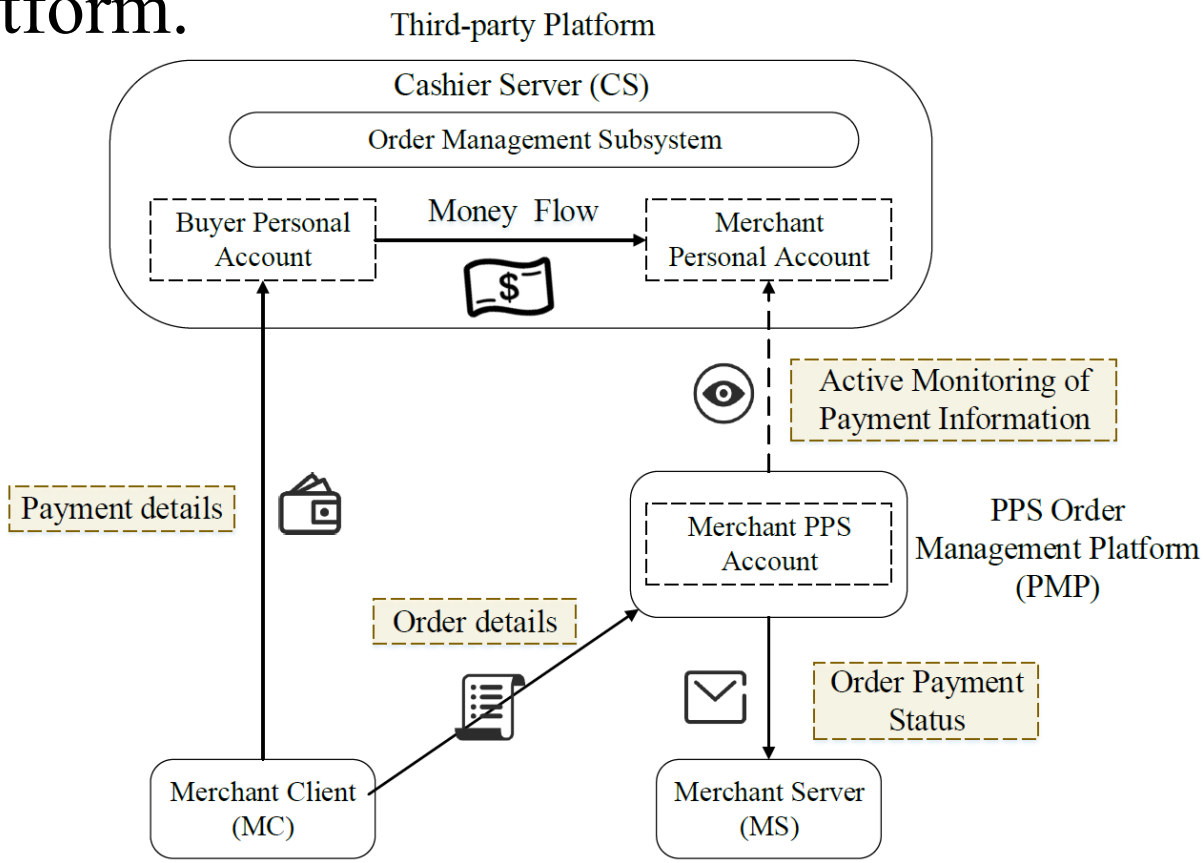
- The online payment services become ubiquitous in our daily life.

- However, there is non-trivial barrier of entry
  - Individual payment accounts are not designed to handle large volumes of transactions.
  - Some regions require a government license to sign up for commercial services incurring delays in application.
  - A non-trivial upfront cost commitment to getting started.

Personal Payment System

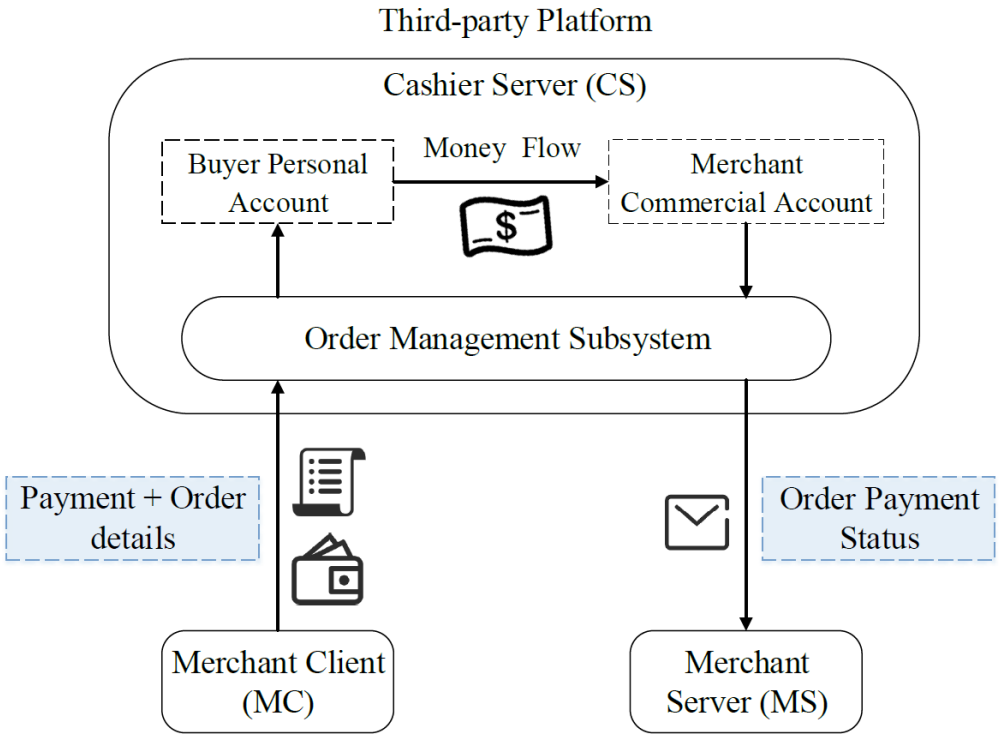
- A new paradigm couples personal money transfer with an independent order management platform.

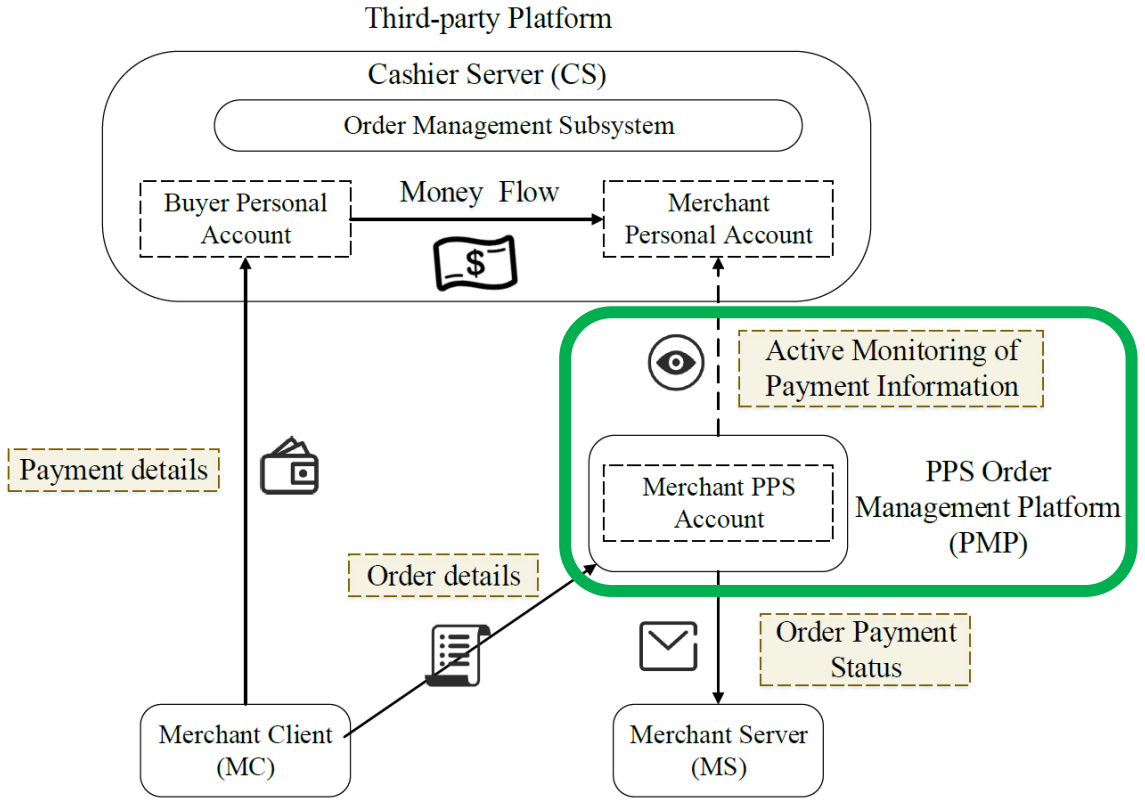
  - MC: merchant client where users browse merchandise and make orders.
  - MS: the merchant server that hosts the client content.
  - CS: a third-party platform manages money transactions between different accounts.
  - PMP: PPS order management platform offers the commercial payment functionalities



The Rise of Personal Payment System (PPS)

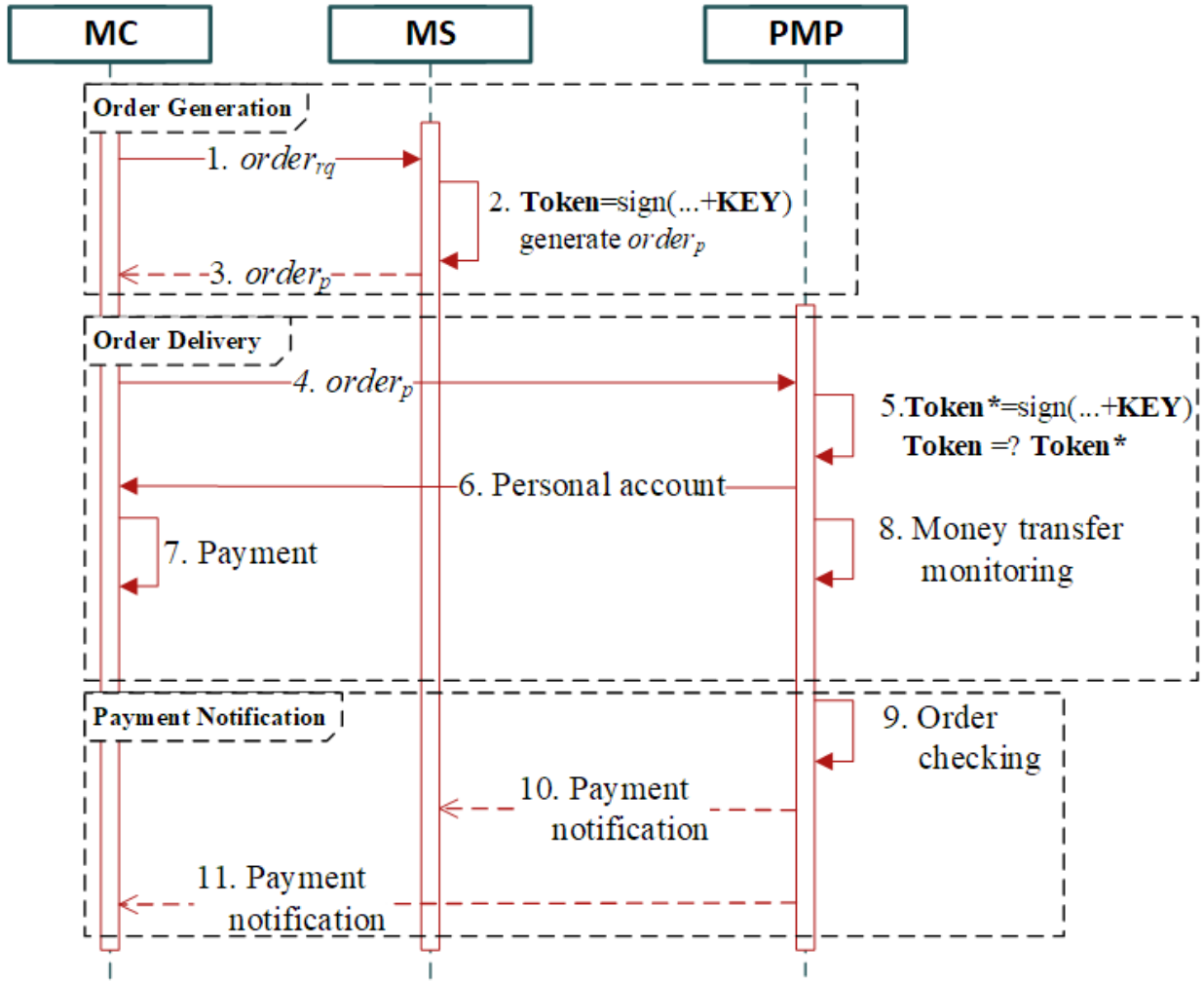
- Commercial Payment System vs Personal Payment System





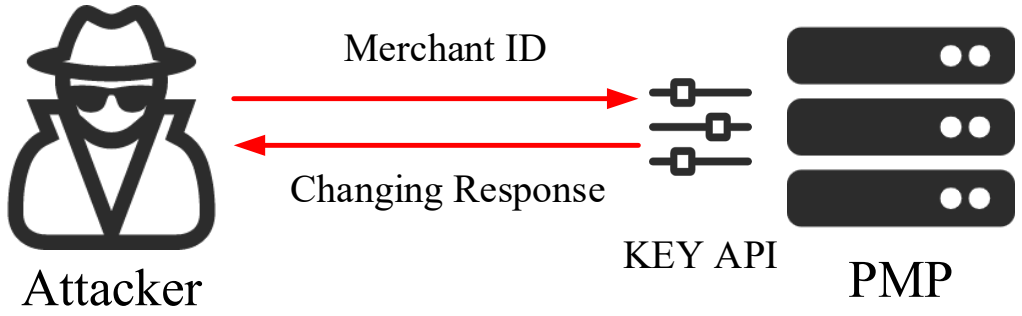
High Level Workflow of PPS

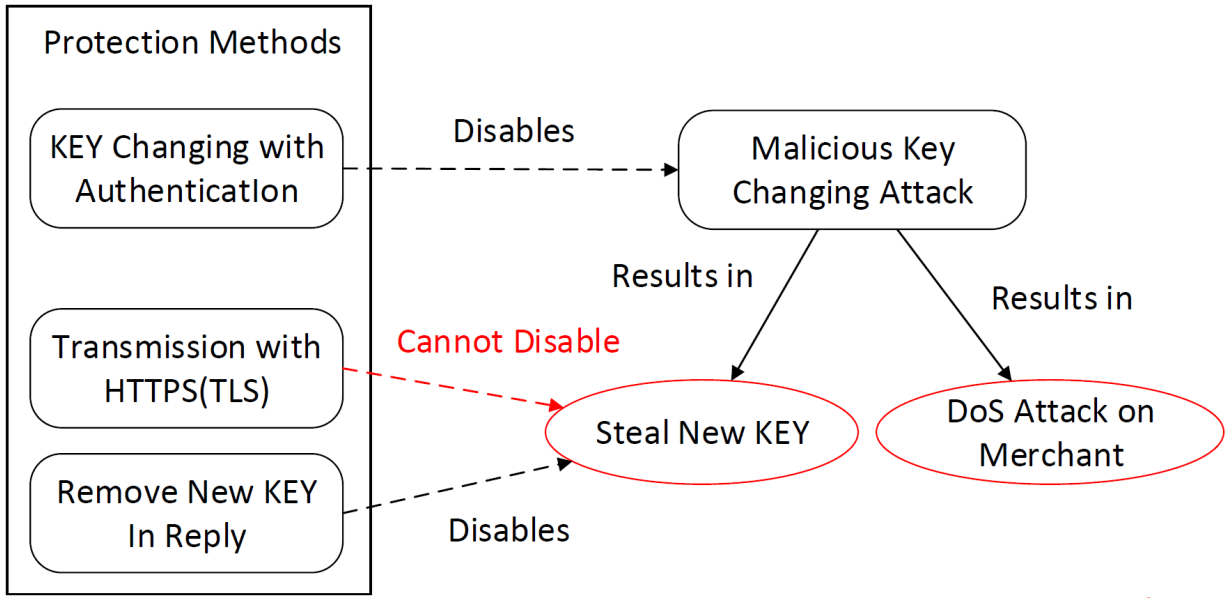
- The transaction flow
  - **Key Distribution (PPS service sign up)**
  - **Order Generation (upon selection of item)**
  - **Order Payment (user pays for the item)**
  - **Payment Notification (ready to ship)**



Security Analysis

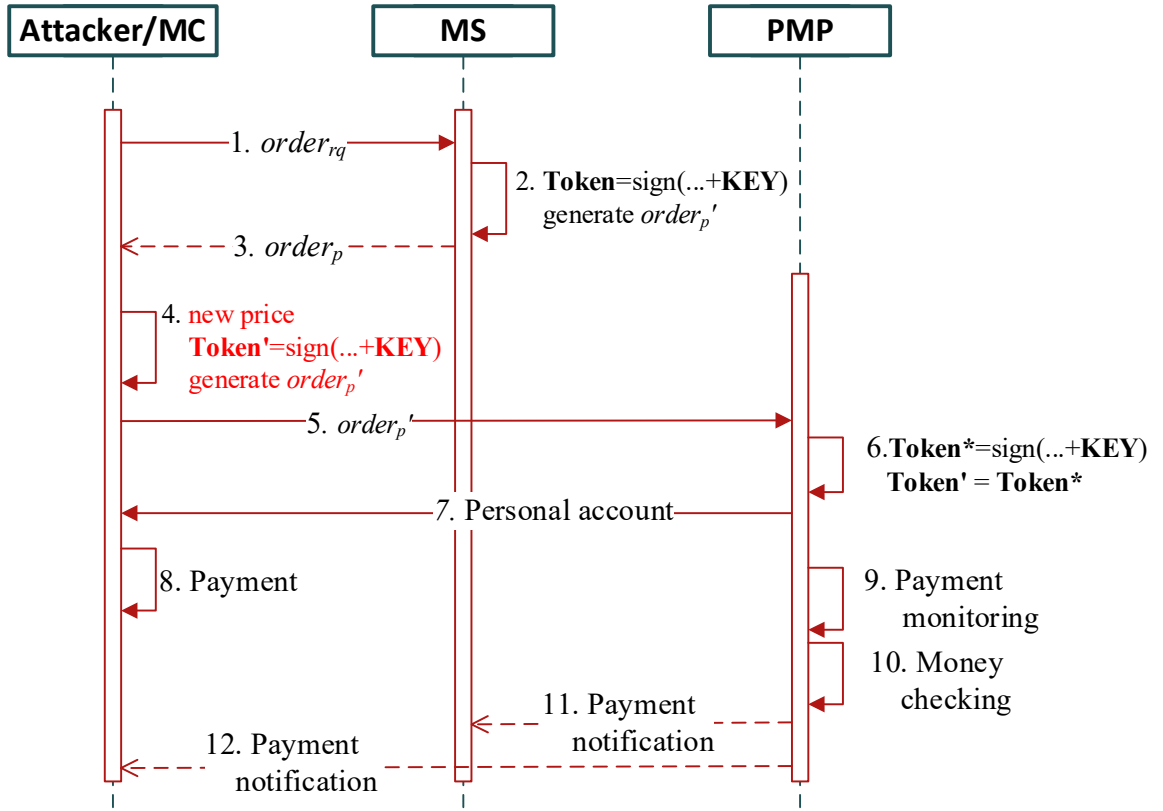
- Unprotected key changing API allows unauthorized key change
  - API allows pre-authenticated requests to change KEY.
  - API only requires merchant ID.
  - Merchant ID can be obtained by examining the order packet.





Security Analysis

- Vulnerable order generation allows modification of order content
  - Local Order Generation
    - Attackers can tamper with some fields of a locally stored order.
  - Local KEY Storage
    - Some MC implementations store KEY in MC for calculation convenience.



Security Analysis

- Vulnerable Signature allows order tampering without KEY
  - String Concatenation in Token Generation

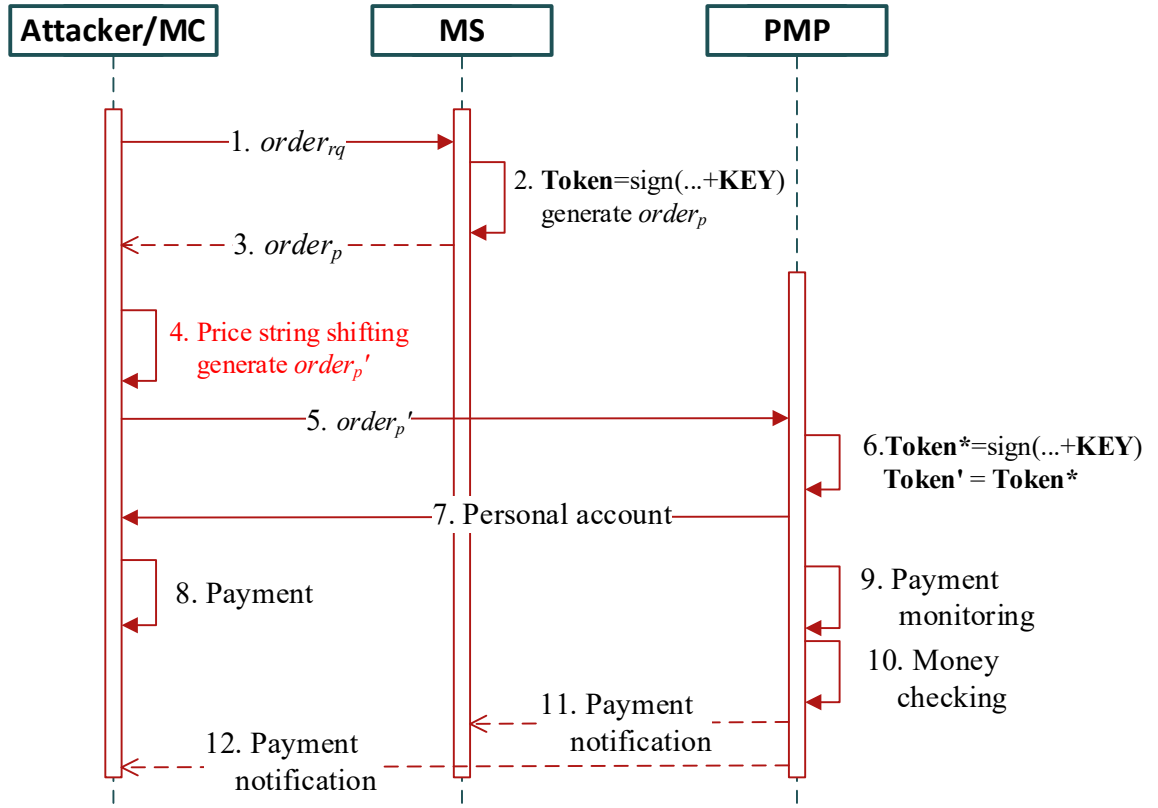
Token=MD5 (order parameter Concatenation +**KEY**)

… 100 www.xxxx.com …
price Notify URL

… 10 0www.xxxx.com …
price Notify URL

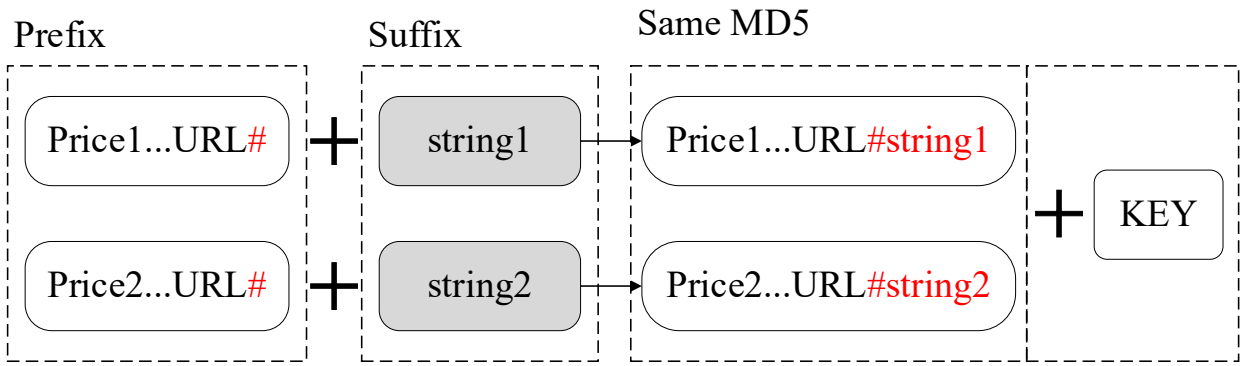
Same in calculating Token

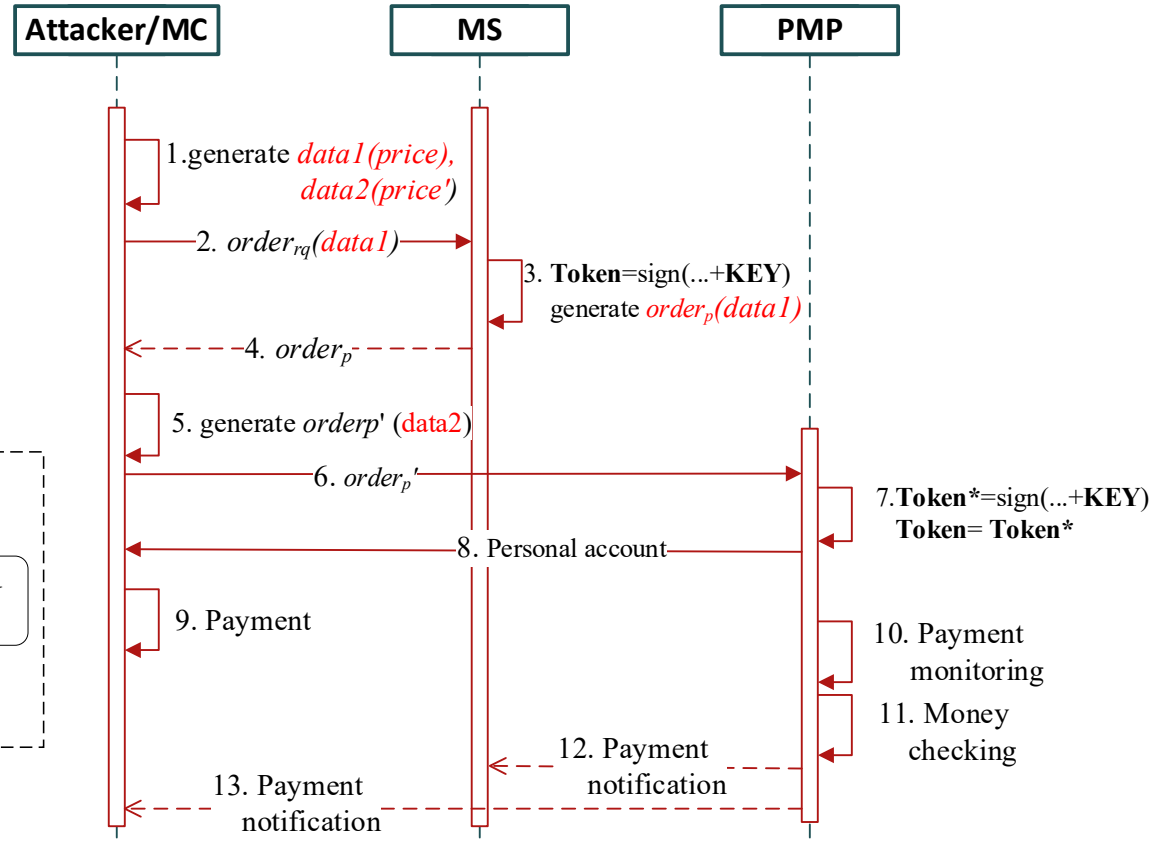
…100www.xxxx.com…KEY



Security Analysis

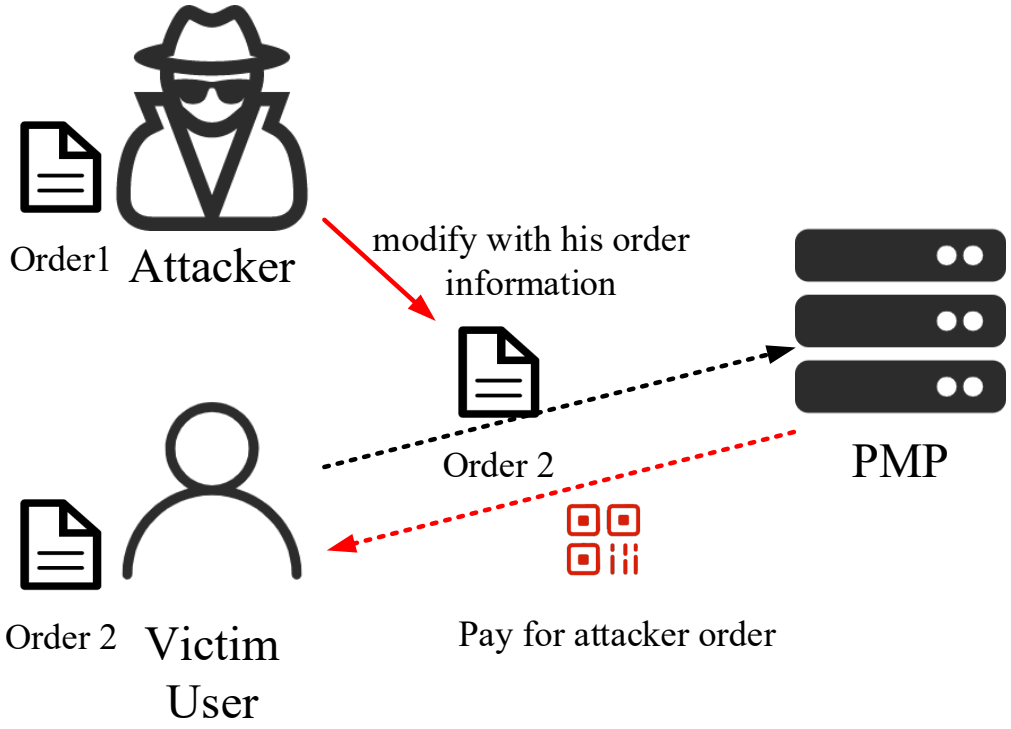
- Vulnerable Signature allows Order tampering without KEY
  - MD5-based Token Generation
    - Suffer from the chosen-prefix collision attack





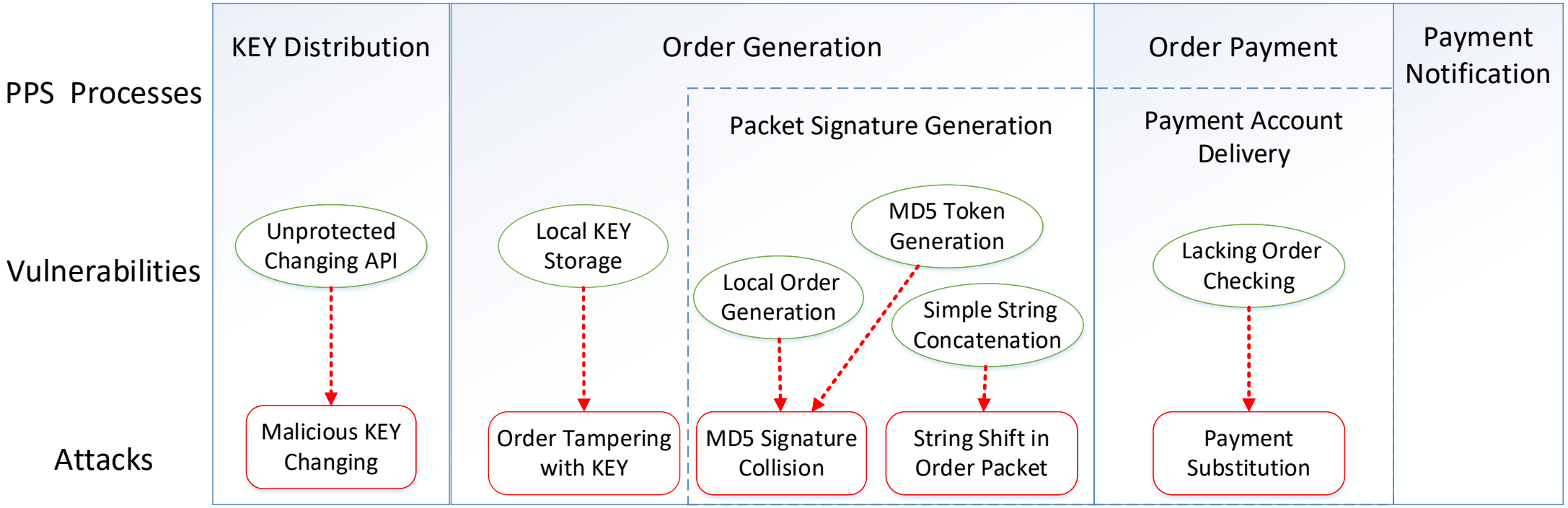
Security Analysis

- Vulnerable account delivery allows payment substitution (making others pay for my purchases)
  - PPS only displays the price, order ID, and QR code to the MC.
  - Order ID is the only clue a buyer can use to associate the payment with his item.
  - Man-in-the-middle attack to swap a buyer's order payment with attackers' order without the victim being aware.



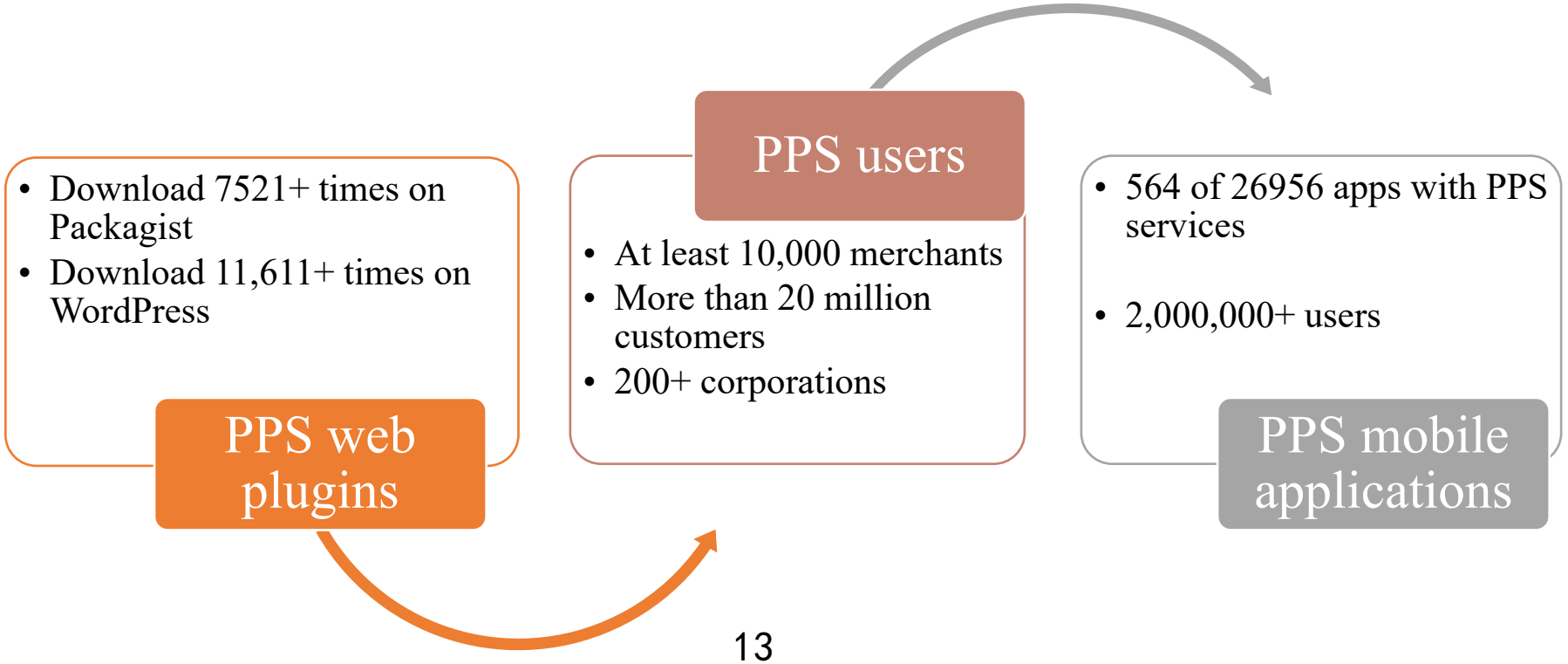
Security Analysis

- Six vulnerable patterns and five proof-of-concept attacks



Empirical Study

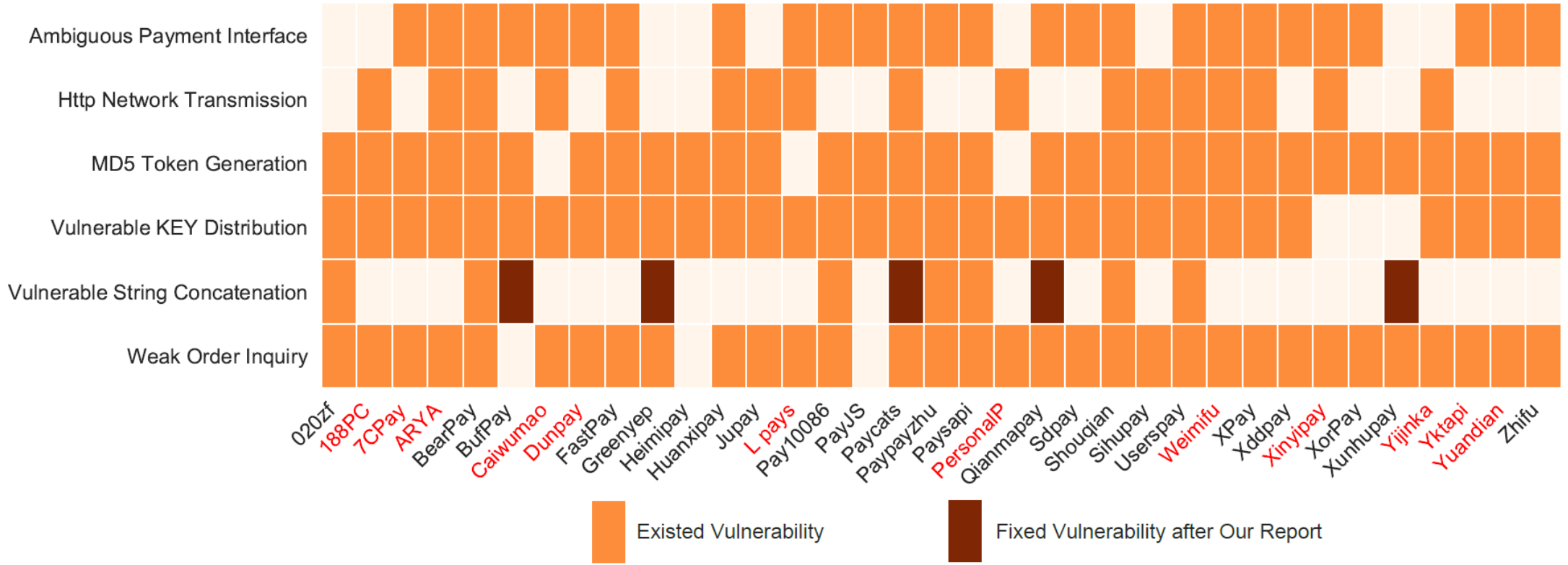
- PPS Ecosystem and Usage Statistics
  - PPSs are currently used in both websites and mobile apps, while the web application is the recommended method of deployment



Empirical Study

- PPS Vulnerability Analysis

35 PPSs and their vulnerabilities distributions



Empirical Study

- Cases for Real-world Attacks
  - String Shifting Attack
    - Recharge 30 ¥ amount to our registered account on *Paysapi* website but pay less than the amount, which only 3 ¥ .
  - Key Changing Attack
    - Disabling the merchant's service on *Paysapi* website.
    - Stealing the new KEY on *Xunhupay* website.

Empirical Study

- Cases for Real-world Attacks
  - Payment Substitution Attack
    - Let the victim pay 10 ¥ on a resource website for the attackers' order.
  - MD5 Collision Attack.
    - Only pay 0.01 ¥ donation amount on a PPS employed blog with expected 0.02 ¥ amount.
    - The calculation was processed on a computer with CPU: Intel i7-8700k, GPU: NVIDIA GeForce GTX1080Ti, and RAM: 64G, where the CUDA was employed.
    - 7 days to find a collision

Empirical Study

- Ethical Consideration in Vulnerability Verification
  - We made use of our test accounts created solely for demonstrating the attacks
  - We always let the authority know the detailed procedures and results so that they can correct at the back end.
- Responsible Disclosure
  - We reported all our findings to the PPS providers in January 2020. 12 of 35 PPSs which possess multiple vulnerabilities stopped providing payment services after our report.
  - We reported the vulnerable PPS list and the security issues to the Security Response Center of Tencent (WeChat Pay) and the Alibaba Security Response Center (AliPay).

Thank you!

Questions?

For any questions, you could send an email to C00413657@louisiana.edu