Electronic Prescriptions for Controlled Substances: A Cybersecurity Perspective

Samuel Tan samueltan@gmail.com

Rebecca Shapiro bx@cs.dartmouth.edu

Sean W. Smith sws@cs.dartmouth.edu

Dartmouth

Introduction

- What did we do?
  - Examined regulations
  - Understood rules and mandated process
  - Identified potential areas of weaknesses
  - Highlighted potential attacks
  - Suggested possible mitigations

Introduction

- What is Electronic Prescriptions for Controlled Substances (EPCS)?
  - Set of rules published the DEA
  - "provide…the ability to use…[electronic] controlled substance prescriptions while maintaining the closed system of controls on controlled substances"
  - Regulates process of issuing and receiving electronic prescriptions
  - Applicable to healthcare institutions, practitioners and pharmacies

EPCS-Mandated Process

PRACTITIONER

Write prescription

Two-factor authentication

OR

Sign with digital certificate

Sign with application

PHARMACY

Verify signature and certificate

Sign on receipt and archive

Process prescription

* Clipart from Kootation.com, iPharMD.net, halfelf.org, drabdolkarim.com, 123rf.com, wikipedia.com, sweetclipart.com, todaysseniorsnetwork.com

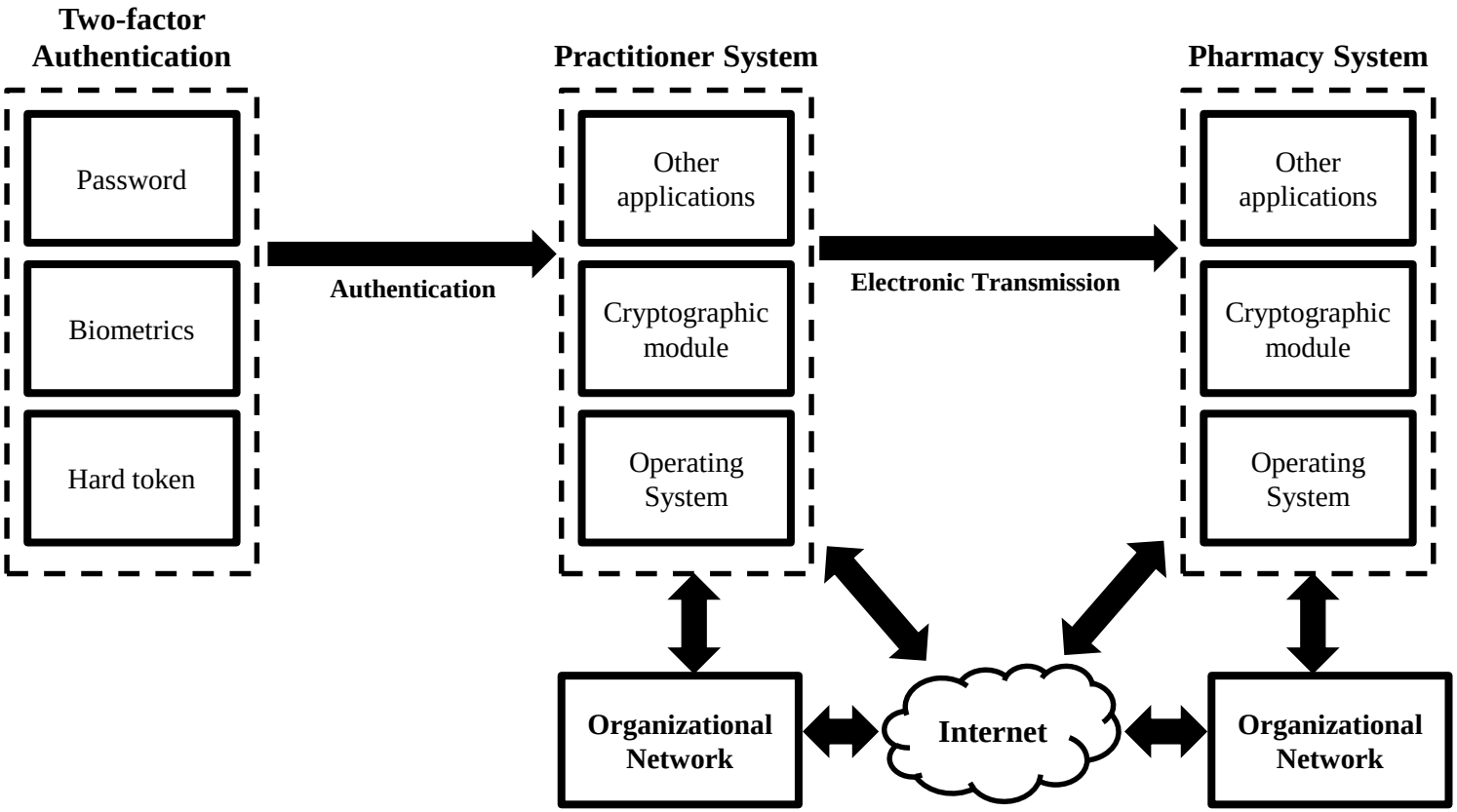
Samuel Tan, Rebecca Shapiro, Sean W. Smith, Dartmouth College

Security Metrics

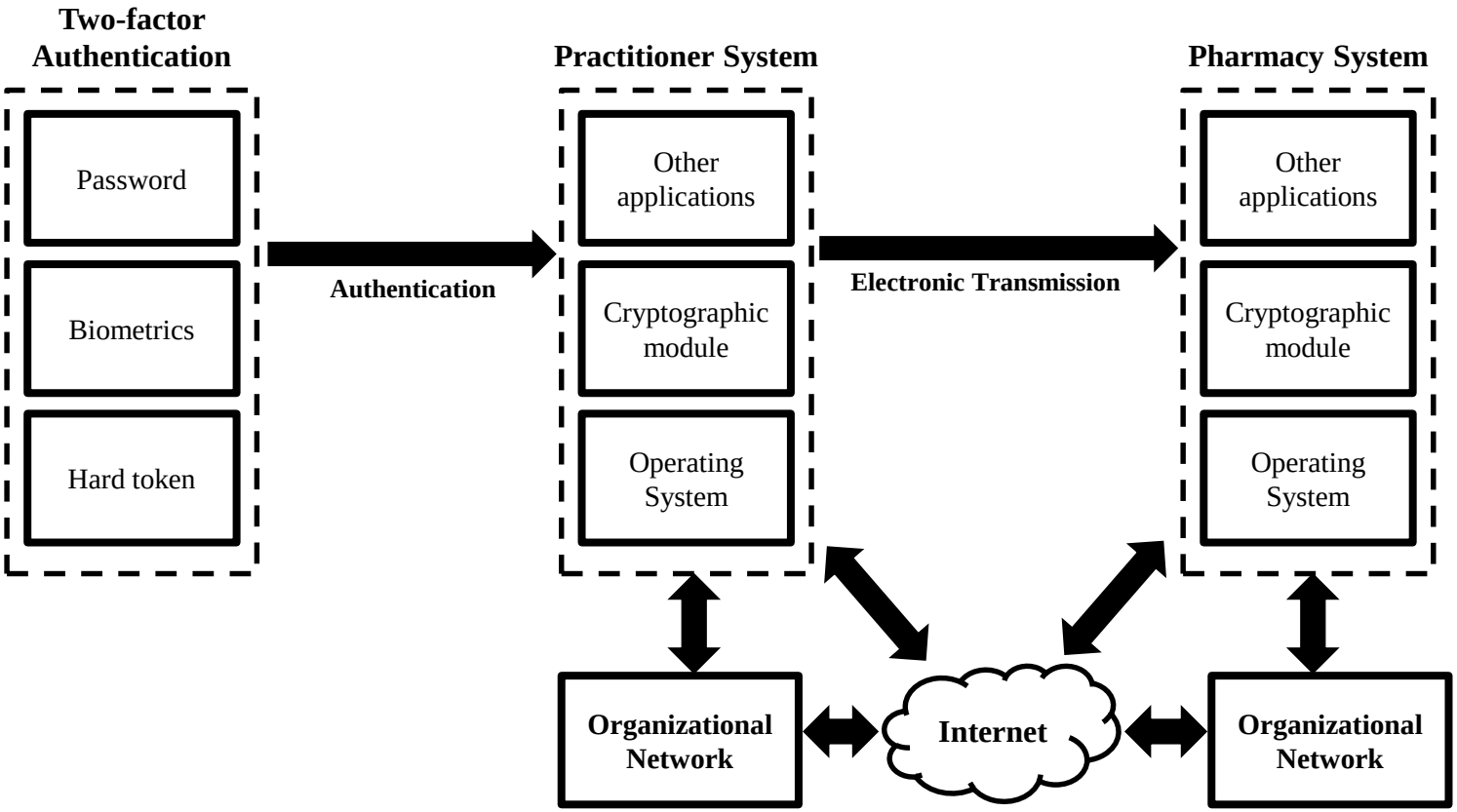
- How do we assess EPCS?
  - *Correctness*
  - Integrity
  - Confidentiality
  - Availability

> "provide…the ability to use…[electronic] controlled substance prescriptions while maintaining the closed system of controls on controlled substances"

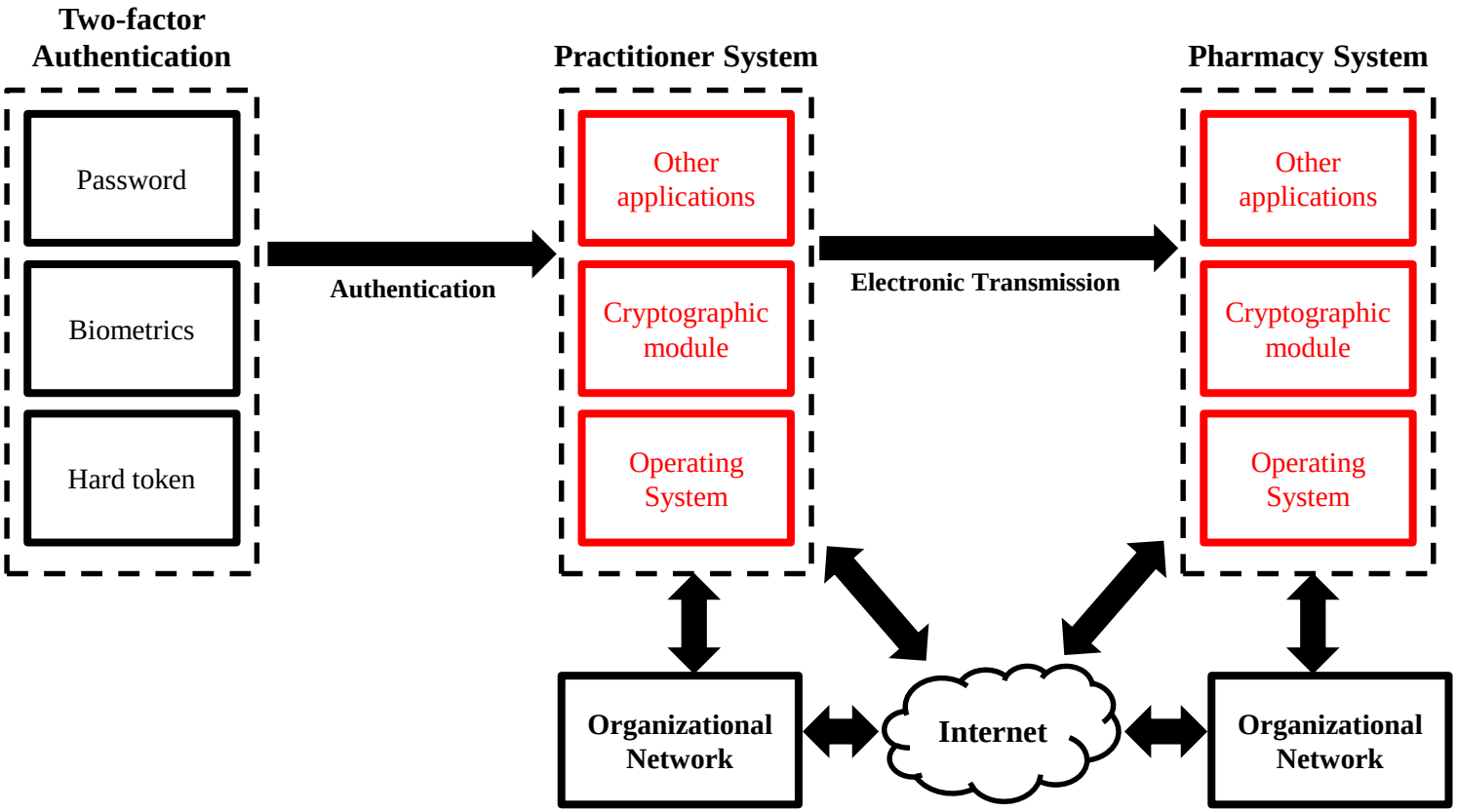
Points of attack



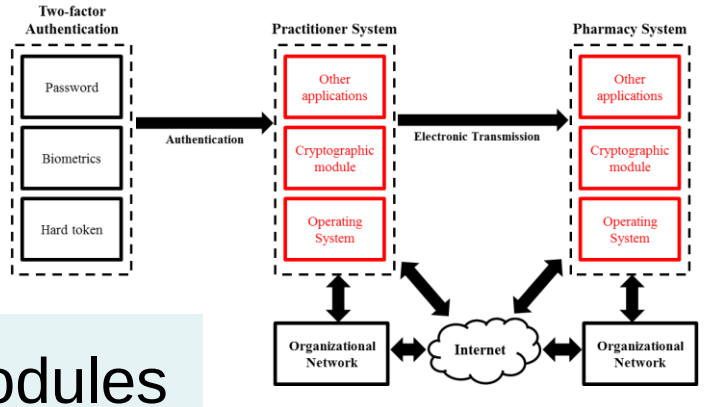
Software Security



Software Security

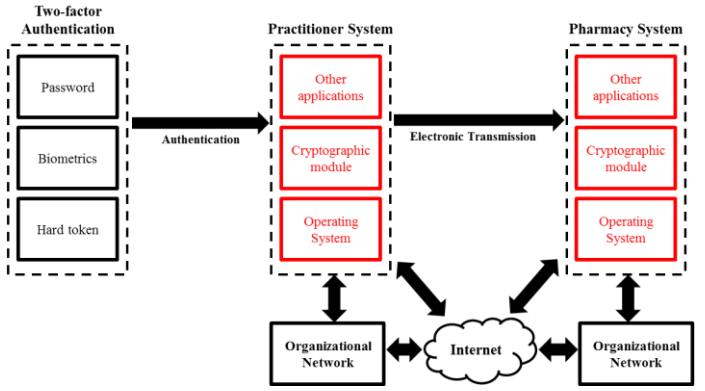


Software Security



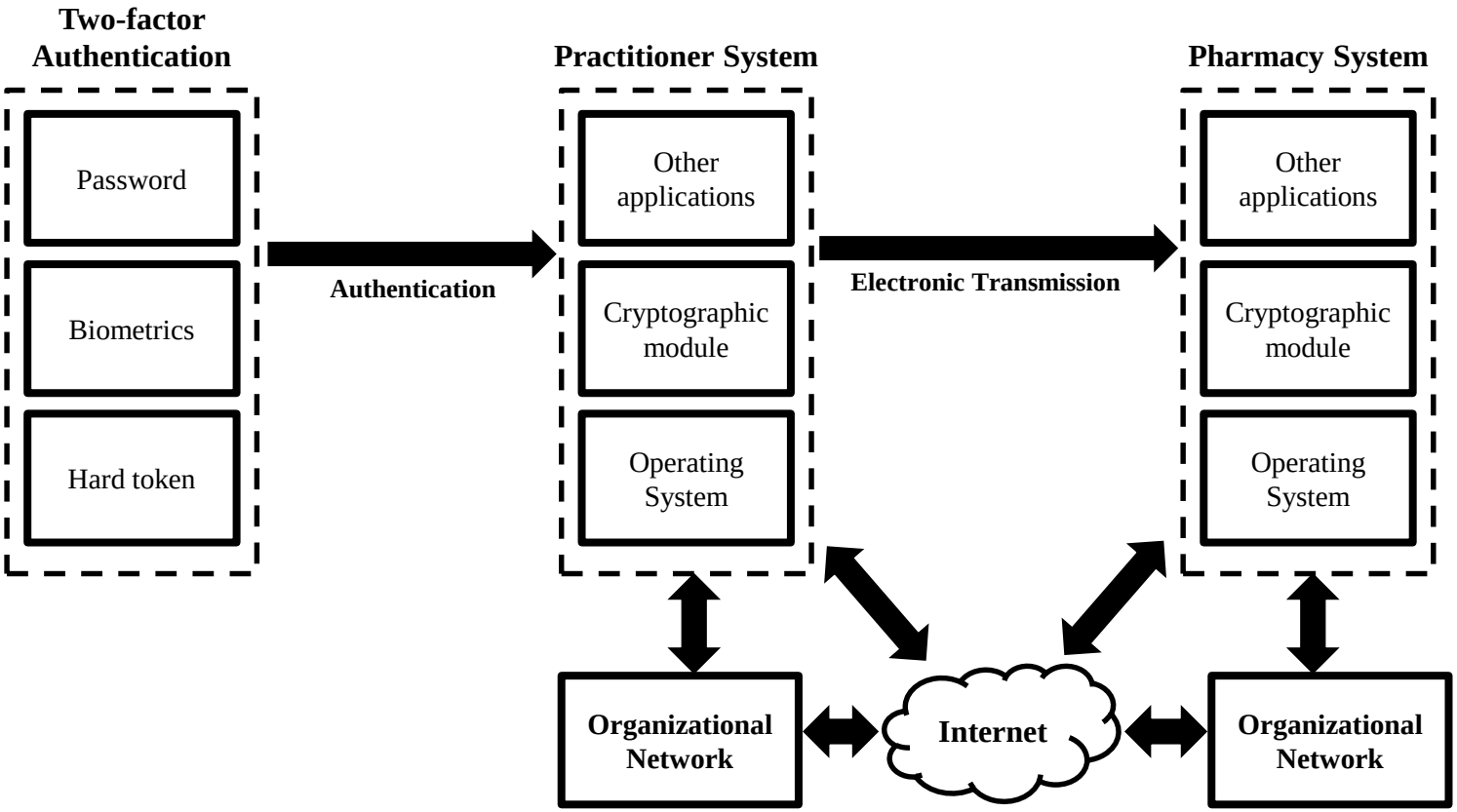
- What's in the EPCS standard?
  - Logical access controls
  - FIPS 140-2 Security Level 1 validated cryptographic signing modules
    - OS restricted to "single operator" mode of operation
    - OS protects private keys from other processes
    - OS source code and binaries cannot be viewed or changed
- Threats
  - FIPS 140-2 Security Level 1 an inadequate guarantee
  - No other requirements!
  - Compromise of other services
  - Compromise of operating system itself

Software Security

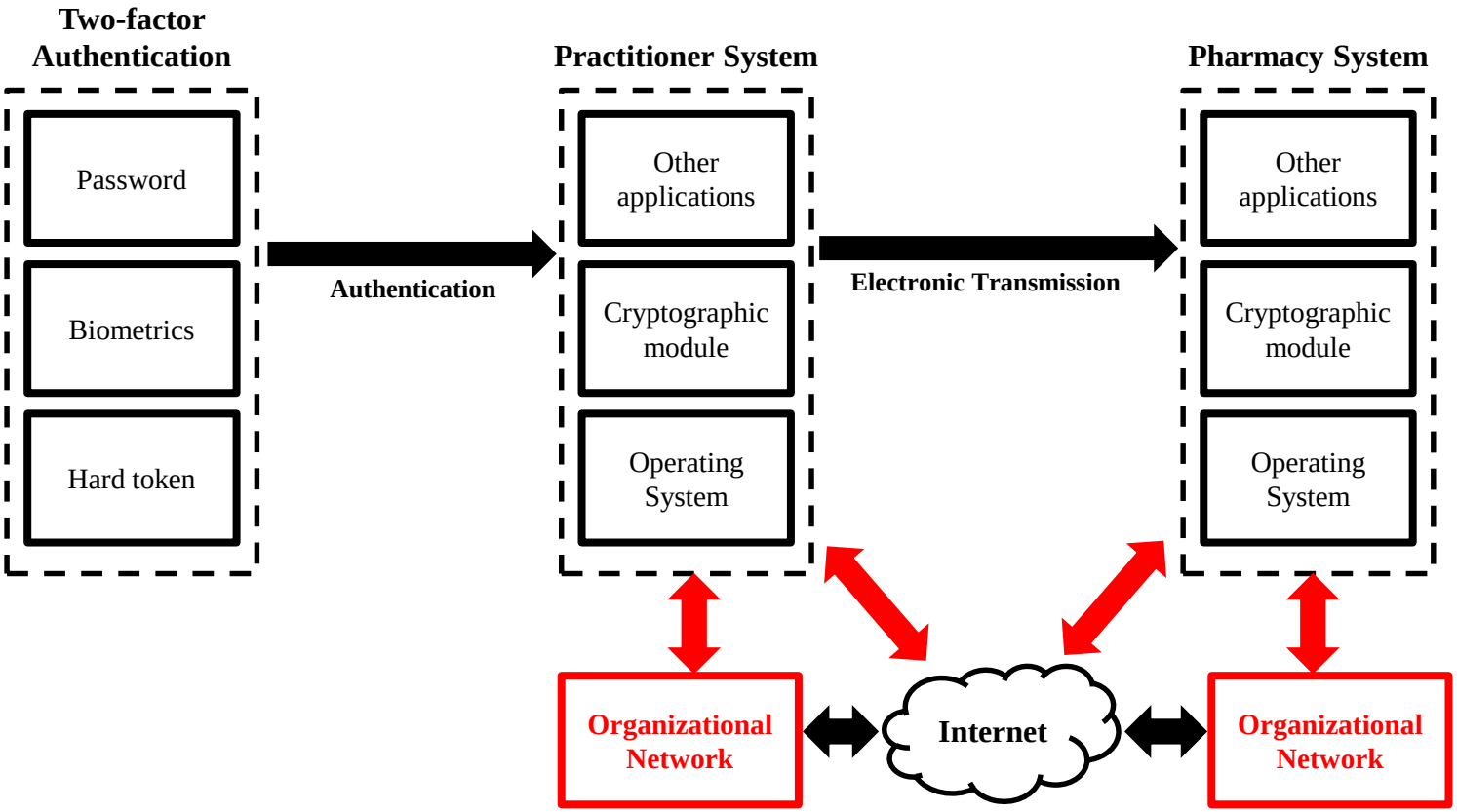


- Potential Attacks
  - Detect OS/software vulnerabilities using remote security scanners, port scanners or packet sniffers
  - Weaponize vulnerabilities (e.g. using Metasploit)
- Possible Mitigation
  - Disable unnecessary applications
  - Frequent patching of OS and applications
  - Configuring user permissions and access privileges
  - Frequent security audits

Network Security



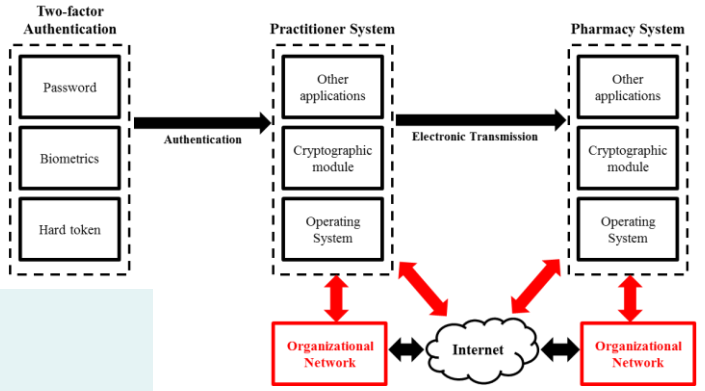
Network Security



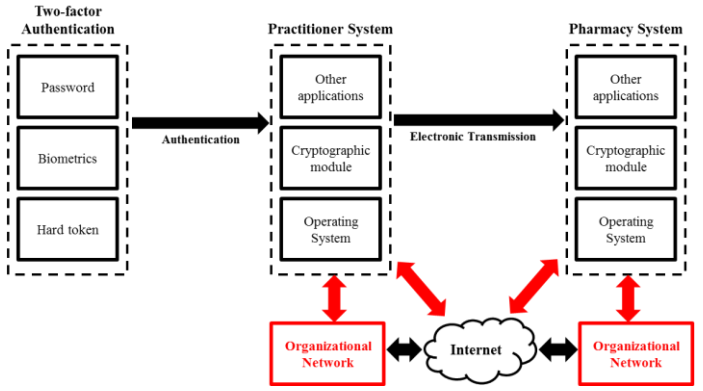
Samuel Tan, Rebecca Shapiro, Sean W. Smith, Dartmouth College

Network Security

- What's in the EPCS standard?
  - No requirements for practitioner or pharmacy system
  - No requirements for networks either is connected to
- Second-order problem
- Threats
  - Attacks via networks
  - Attacks on networks themselves

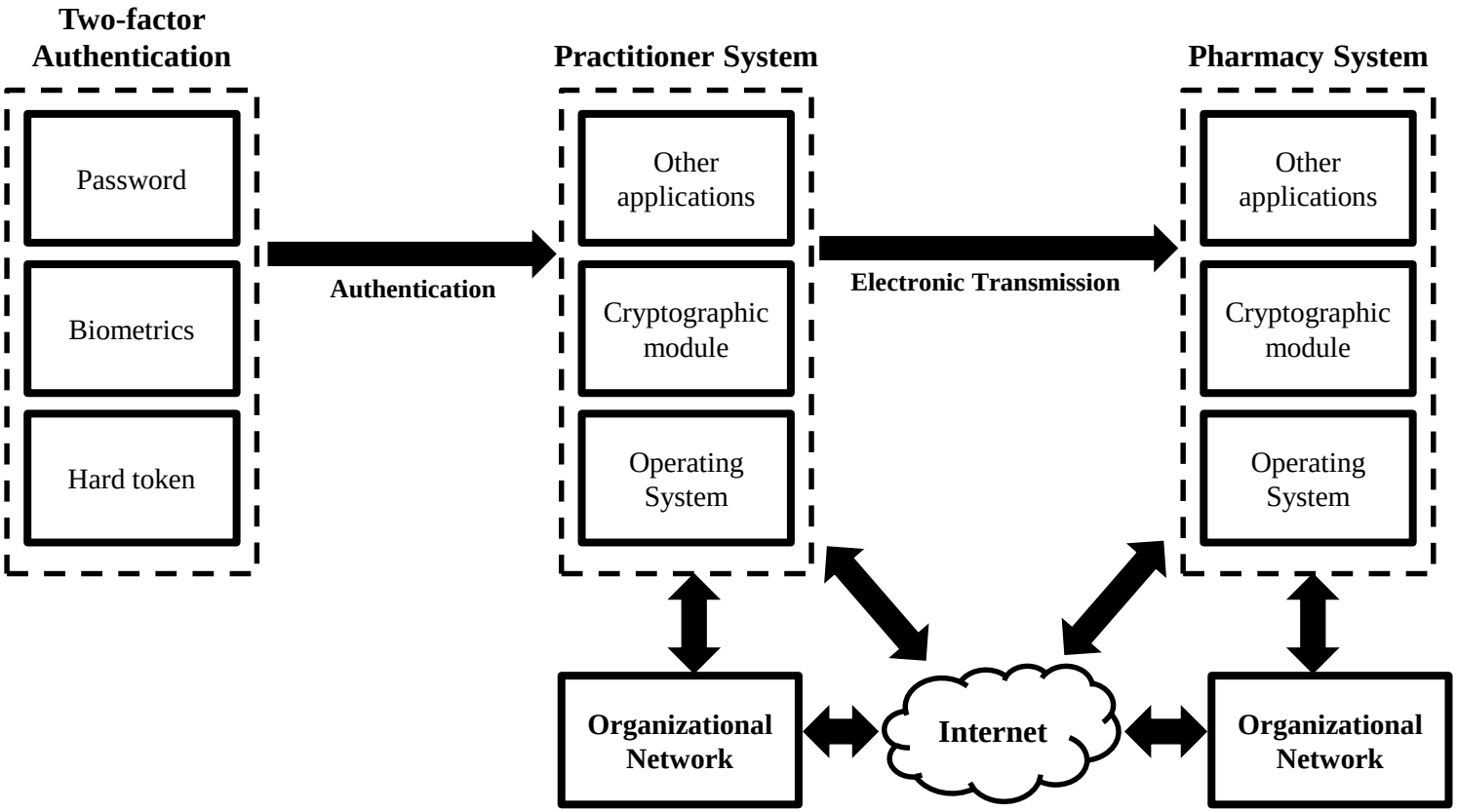


Network Security

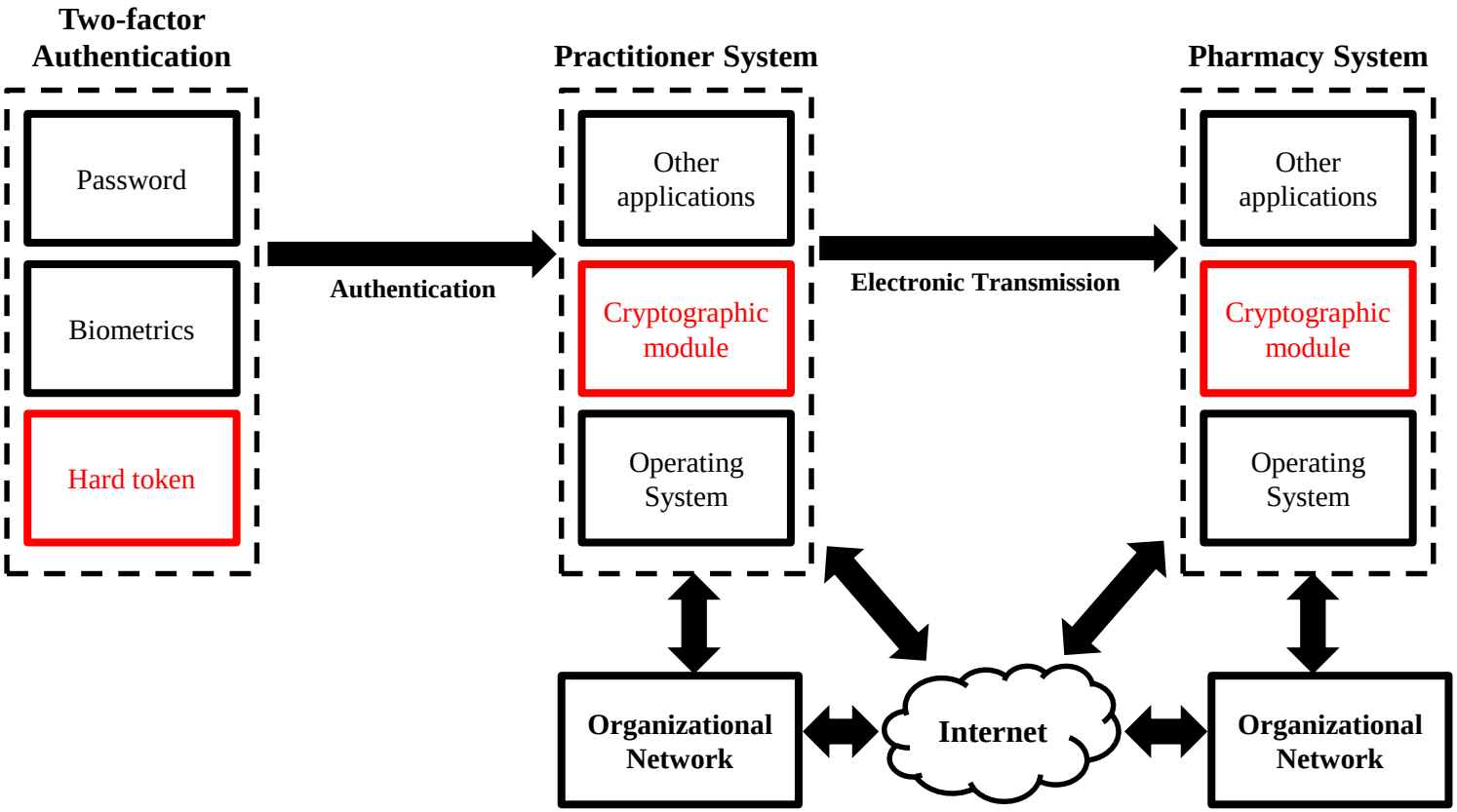


- Potential attacks
  - Vulnerability sniffing and delivery of weaponized exploits through open ports
  - Man-in-the-middle attacks
    - E.g. DNS spoofing, ARP cache poisoning
- Possible Mitigation
  - Secure organizational network layout
  - Proper firewall configuration
  - Intrusion detection and prevention systems

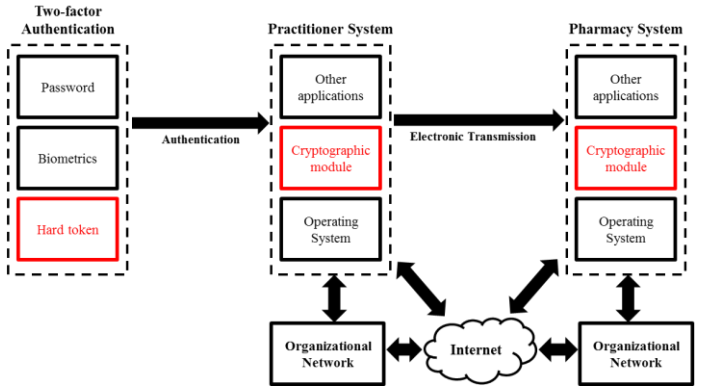
Physical (Key) Security



Physical (Key) Security

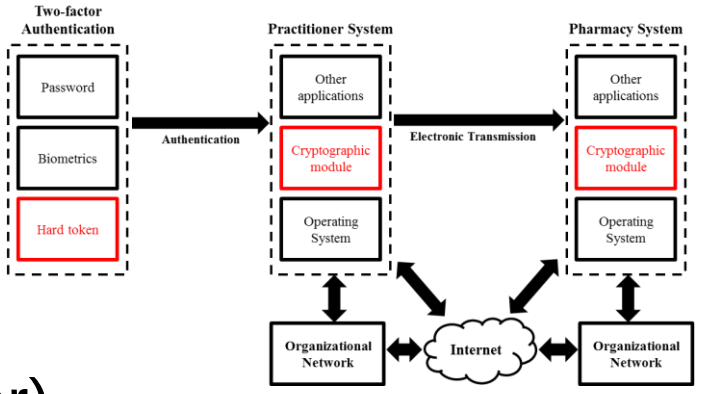


Physical (Key) Security



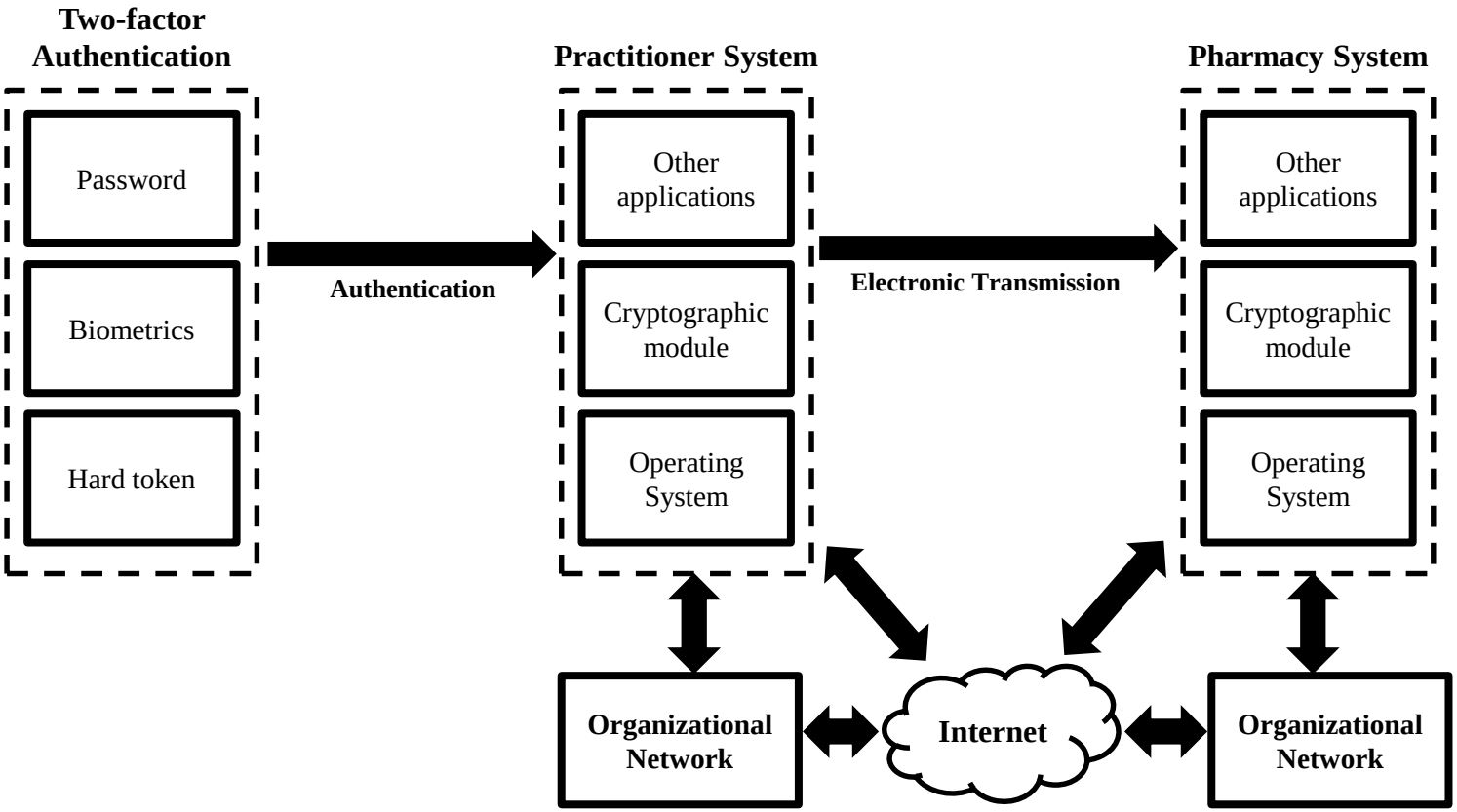
- What's in the EPCS standard?
  - Cryptographic signing modules must be FIPS 140-2 Security Level 1
  - Hard token (if used) must be separate and FIPS 140-2 Security Level 1
    - Made of "Production grade equipment"
    - Zeroize keys if maintenance/debugging mode is accessed
- Threats
  - FIPS 140-2 Security Level 1 requirement too weak

Physical (Key) Security

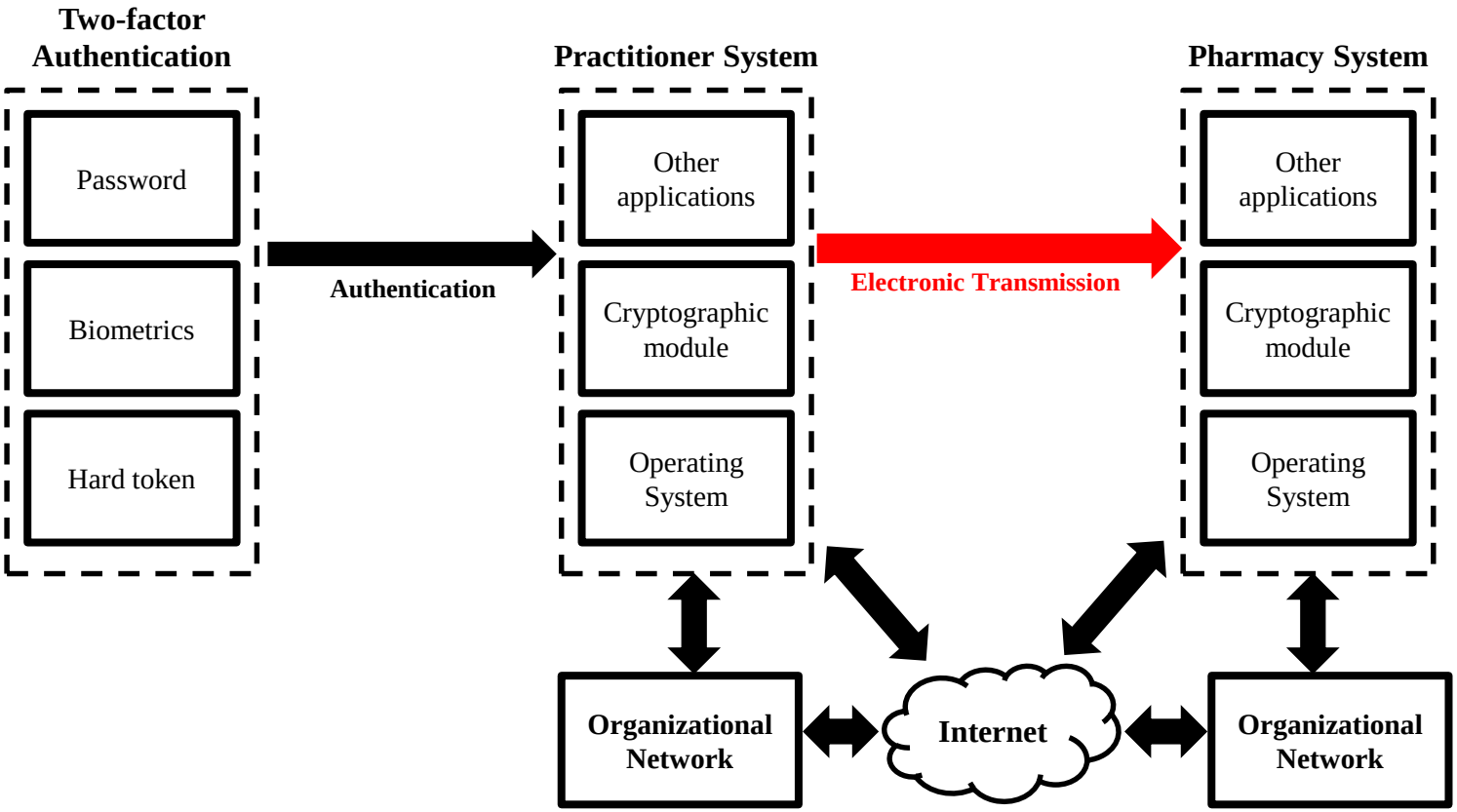


- Potential Attacks
  - Attacks on the debugging access interface
  - Side-channel attacks (Joye & Oliver)
    - E.g. Power analysis attacks
  - "Cold boot" attacks (Halderman et. al)
- Possible Mitigation
  - FIPS 140-2 Security Level 3 requirement
  - Power analysis attack countermeasures (Joye & Oliver)
    - E.g. blur signal using smoothing techniques, dual-rail logic
  - Regular clearing of private keys from memory

Transmission

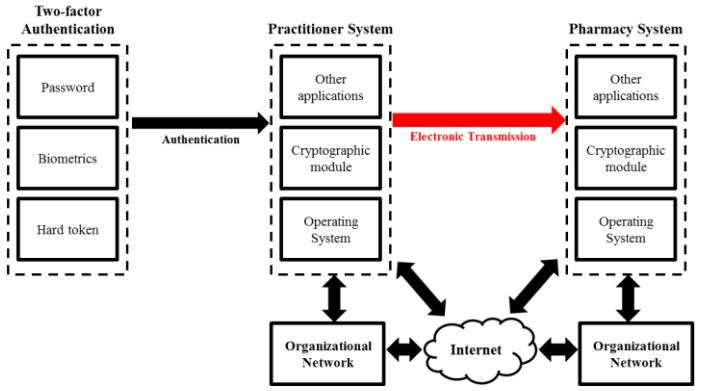


Transmission



Transmission

- What's in the EPCS standard?
  - Protection from modification
- Threat/Potential attack
  - Eavesdropping on unencrypted transmitted electronic prescriptions
- Potential Mitigation
  - Use TLS protocol during transmission



Other Security Weaknesses

- Biometric subsystem
- Password policy
  - Read paper for in-depth discussions

Conclusions

- Current regulations insufficient
- Many easy fixes
- Increase attacker cost for attacks that are harder to defend against
- Tradeoff between cost and security

Lessons Learnt

- Establish security goals from the start
  - "provide…the ability to use…[electronic] controlled substance prescriptions while maintaining the closed system of controls on controlled substances"
- Accepted standards ≠> secure system
- Regulations should be conservative
- Be specific where it counts

Q&A

Samuel Tan samueltan@gmail.com

Rebecca Shapiro bx@cs.dartmouth.edu

Sean W. Smith sws@cs.dartmouth.edu