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
• What did we do?
  o Examined regulations
  o Understood rules and mandated process
  o Identified potential areas of weaknesses
  o Highlighted potential attacks
  o Suggested possible mitigations
What is Electronic Prescriptions for Controlled Substances (EPCS)?

- Set of rules published by 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

**PHARMACY**

- Verify signature and certificate
- Process prescription

- Sign with digital certificate
- Sign with application
- Sign on receipt and archive

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

Samuel Tan, Rebecca Shapiro, Sean W. Smith, Dartmouth College
• How do we assess EPCS?
  o *Correctness*
  o Integrity
  o Confidentiality
  o Availability

“provide…the ability to use…[electronic] controlled substance prescriptions while maintaining the closed system of controls on controlled substances”
Points of attack

Two-factor Authentication
- Password
- Biometrics
- Hard token

Practitioner System
- Other applications
- Cryptographic module
- Operating System

Pharmacy System
- Other applications
- Cryptographic module
- Operating System

Internet
- Organizational Network

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

Two-factor Authentication
- Password
- Biometrics
- Hard token

Authentication

Practitioner System
- Other applications
- Cryptographic module
- Operating System

Electronic Transmission

Pharmacy System
- Other applications
- Cryptographic module
- Operating System

Organizational Network

Internet

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

Two-factor Authentication
- Password
- Biometrics
- Hard token

Authentication

Practitioner System
- Other applications
- Cryptographic module
- Operating System

Electronic Transmission

Pharmacy System
- Other applications
- Cryptographic module
- Operating System

Organizational Network

Internet

Organizational Network

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

Two-factor Authentication
- Password
- Biometrics
- Hard token

Practitioner System
- Other applications
- Cryptographic module
- Operating System

Pharmacy System
- Other applications
- Cryptographic module
- Operating System

Electronic Transmission

Organizational Network

Internet

Organizational Network

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

Two-factor Authentication
- Password
- Biometrics
- Hard token

Practitioner System
- Other applications
- Cryptographic module
- Operating System

Pharmacy System
- Other applications
- Cryptographic module
- Operating System

Electronic Transmission

Organizational Network

Internet

Organizational Network

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
  o Vulnerability sniffing and delivery of weaponized exploits through open ports
  o Man-in-the-middle attacks
    ➢ E.g. DNS spoofing, ARP cache poisoning

• Possible Mitigation
  o Secure organizational network layout
  o Proper firewall configuration
  o Intrusion detection and prevention systems
Physical (Key) Security

Two-factor Authentication
- Password
- Biometrics
- Hard token

Practitioner System
- Other applications
- Cryptographic module
- Operating System

Pharmacy System
- Other applications
- Cryptographic module
- Operating System

Organizational Network
- Internet

Samuel Tan, Rebecca Shapiro, Sean W. Smith, Dartmouth College
Physical (Key) Security

Two-factor Authentication
- Password
- Biometrics
- Hard token

Practitioner System
- Other applications
- Cryptographic module
- Operating System

Electronic Transmission

Pharmacy System
- Other applications
- Cryptographic module
- Operating System

Organizational Network

Internet

Samuel Tan, Rebecca Shapiro, Sean W. Smith, Dartmouth College
Physical (Key) Security

• What’s in the EPCS standard?
  o Cryptographic signing modules must be FIPS 140-2 Security Level 1
  o 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
  o FIPS 140-2 Security Level 1 requirement too weak
Physical (Key) Security

• Potential Attacks
  o Attacks on the debugging access interface
  o Side-channel attacks (Joye & Oliver)
    ➢ E.g. Power analysis attacks
  o “Cold boot” attacks (Halderman et. al)

• Possible Mitigation
  o FIPS 140-2 Security Level 3 requirement
  o Power analysis attack countermeasures (Joye & Oliver)
    ➢ E.g. blur signal using smoothing techniques, dual-rail logic
  o Regular clearing of private keys from memory
Transmission

Two-factor Authentication
- Password
- Biometrics
- Hard token

Authentication

Practitioner System
- Other applications
- Cryptographic module
- Operating System

Electronic Transmission

Pharmacy System
- Other applications
- Cryptographic module
- Operating System

Internet

Organizational Network

Samuel Tan, Rebecca Shapiro, Sean W. Smith, Dartmouth College
• What’s in the EPCS standard?
  o Protection from modification
• Threat/Potential attack
  o Eavesdropping on unencrypted transmitted electronic prescriptions
• Potential Mitigation
  o 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
  o “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
<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samuel Tan</td>
<td><a href="mailto:samueltan@gmail.com">samueltan@gmail.com</a></td>
</tr>
<tr>
<td>Rebecca Shapiro</td>
<td><a href="mailto:bx@cs.dartmouth.edu">bx@cs.dartmouth.edu</a></td>
</tr>
<tr>
<td>Sean W. Smith</td>
<td><a href="mailto:sws@cs.dartmouth.edu">sws@cs.dartmouth.edu</a></td>
</tr>
</tbody>
</table>