

The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

Chih-Hsuan Yang

National Sun Yat-sen University

Advisor: Chun-I Fan

May 13, 2021

Outline

- 1 Background
- 2 EEC & EMR
- 3 Linux source code
- 4 Formal verification
- 5 Privacy
- 6 References

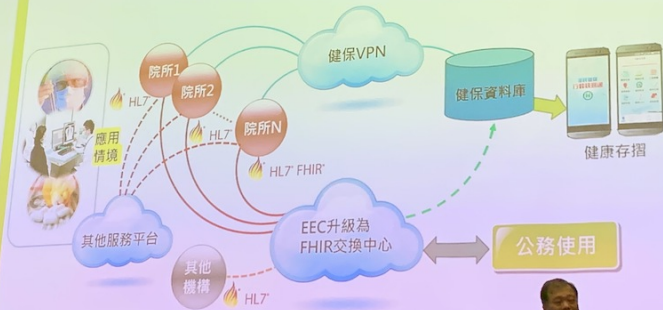
Background

Backgriund

Researching takes time.



電子病歷交換架構及平台的改革



EEC & EMR

2017衛生福利部電子病歷資訊安全檢查表

Change password?

19	具特殊權限公用程式之使用	<p>目的： 應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。</p> <p>合格項目： 特權的公用程式應造冊，每次抽查時，未限制不得超過3件。</p> <p>[註]未有使用特權的公用程式者，可自選本條免評。</p>	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格
----	--------------	--	--	--

Parallel permission

19	具特殊權限公用程式之使用	<p>目的： 應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。</p> <p>合格項目： 特權的公用程式應造冊，每次抽查時，未限制不得超過3件。</p> <p>[註]未有使用特權的公用程式者，可自選本條免評。</p>	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格
----	--------------	--	--	--

Without encryption?

六、密碼學				
21	密碼控制措施	<p>目的： 資訊系統設定加解密演算機制有否符合院內規定，且機密資訊應加密儲存。</p> <p>合格項目： 訂有加解密機制之規範與落實執行。</p> <p>[註]醫院之資訊系統若無設定加解密機制，可自選本條免評。</p>	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格

2017衛生福利部電子病歷資訊安全檢查表

FTP? SFTP?

36	資訊傳送政策 /程序與協議	<p>目的： 應訂有資訊傳送協議(內外部)、政策、程序及控制措施，以保護經由使用所有型式通訊設施或電子(例如電子郵件、即時通訊或FTP資料傳輸等)等資訊傳送。</p> <p>合格項目 訂有相關規範與落實執行。</p>	<input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 合格 <input type="checkbox"/> 不合格
----	------------------	--	---	---

Without certificate?

項次	項目	必要	評量項目	自評結果	檢查結果
22	金鑰		<p>目的： 金鑰管理(如軟體憑證等)須符合院內規定。</p> <p>合格項目： 訂有金鑰管理之規範與落實執行。</p> <p>[註]醫院若無軟體憑證等金鑰，可自選本條免評。</p>	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	<input type="checkbox"/> 免評 <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格

嚴重懷疑沒有經過資安專家審核

Linux source code

`static __latent_entropy struct task_struct *copy_process`

- `fork.c` L1851-2399
- 549

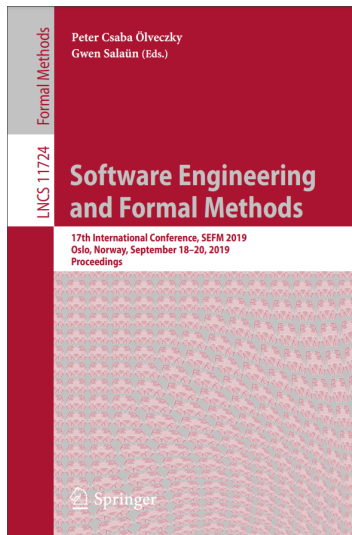
`task_struct`

- `sched.h` L649-1401
- 753

Formal verification

Formal verification

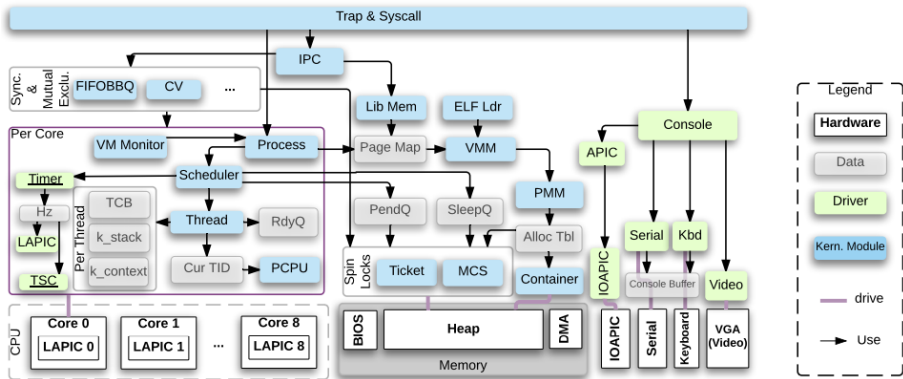
- Abstract Interpretation
- Formal Model Checking
- Theory Prover



[1]

Formal verification

System architecture for the sample kernel [2]



Formal verification

The contextual refinement property about the s kernel can be stated as:

$$\forall P, [[K \& P]]_{x86mc} \subseteq [[P]]_s$$

Formal verification

L : each layer interface

A : an active thread set

$EC(L, A)$: set of valid environment contexts

$\prod_{L(A)}(P, \epsilon)$: thread-modular machine

The semantics for a concurrent layer machine L is then:

$$[[P]]_{L(A)} = \{ \prod_{L(A)}(P, \epsilon) \mid \epsilon \in EC(L, A) \}$$

λ -calculus

Formal Small-step Verification of a Call-by-value Lambda Calculus Machine [3]

Stack

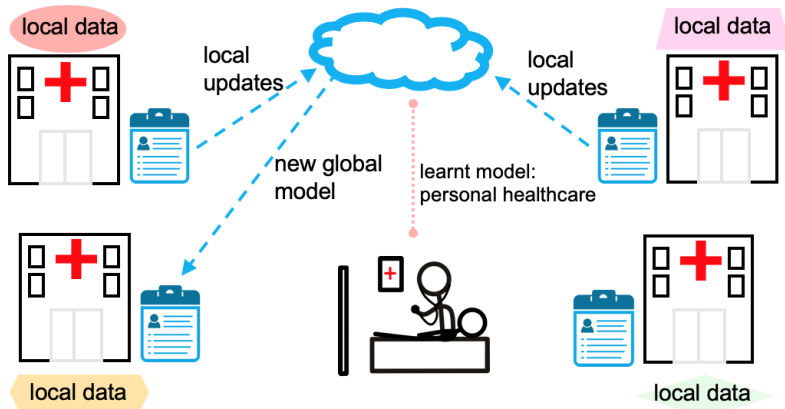
$$(T, V) \gg \sigma := \text{closed}(T, V) \wedge (\delta_0 @ T, \delta_1 @ V) = \sigma$$

Heap

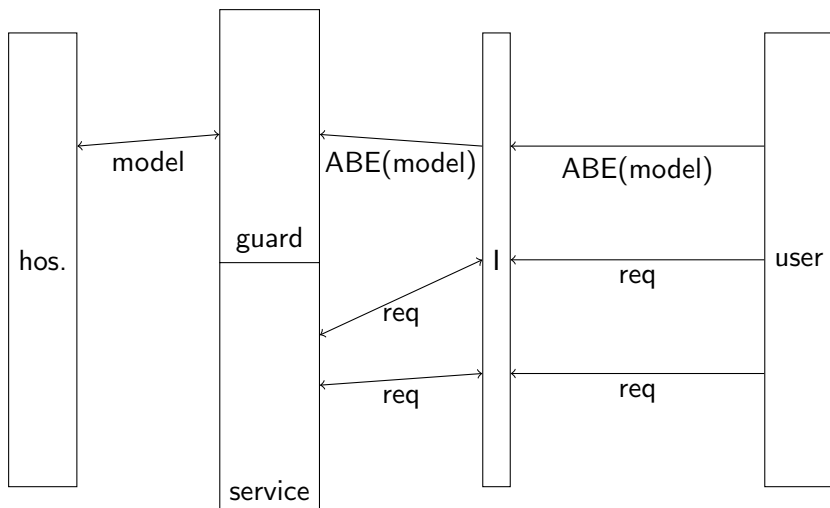
$$(T, V, H) \gg (\dot{T}, \dot{V}) = T \gg_H \dot{T} \wedge V \gg_H \dot{V}$$

Privacy

Privacy is not only federated learning



Attribute Based Homomorphic Encryption



References

References I

- [1] Marjan Sirjani Alessandro Cimatti, ed. *Software Engineering and Formal Methods*. Springer, Cham, 2017. DOI: <https://doi.org/10.1007/978-3-319-66197-1>.
- [2] Ronghui Gu et al. “CertiKOS: An Extensible Architecture for Building Certified Concurrent OS Kernels”. In: *Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation*. OSDI'16. Savannah, GA, USA: USENIX Association, 2016, 653–669. ISBN: 9781931971331.
- [3] Fabian Kunze, Gert Smolka, and Yannick Forster. “Formal Small-Step Verification of a Call-by-Value Lambda Calculus Machine”. In: *Lecture Notes in Computer Science* (2018), 264–283. ISSN: 1611-3349. DOI: 10.1007/978-3-030-02768-1_15. URL: http://dx.doi.org/10.1007/978-3-030-02768-1_15.