



Nytt liv i säkerhetsforskningen på SICS - pågående aktiviteter och framtidsutsikt

Christian Gehrman



Säkerhet idag och igår...

- Den klassiska (andra världskriget) kommunikationssäkerhetsmodellen

Sändare



Kanal

Mottagare



Hej Klas!
Här kommer
de preliminära
bokslutssiffrorna
för er kontroll....

Kryptering



!XjkddjJKediek"

D93nc982^<j34k
fsf>Skjf9s0u9jljs
dfsdf94n45!90?g
"de...

!XjkddjJKediek"

D93nc982^<j34k
fsf>Skjf9s0u9jljs
dfsdf94n45!90?g
"de....

Avkryptering

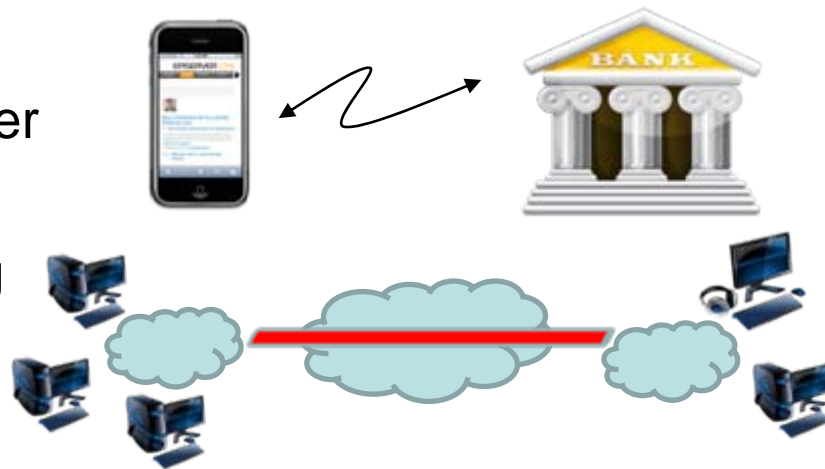


Hej Klas!
Här kommer
de preliminära
bokslutssiffrorna
för er kontroll....

Behovet av informationsskydd

- Skydd av information med hjälp av kryptering och eller speciell hårdvara har idag för länge sedan lämnat de rena militära tillämpningarna och är en del av vår vardag

- Banktransaktioner
- Access system
- Skydd av lagring
- VPNs
- Etc.



- Metoder för kryptering, protokoll, intrångsdetektering och nyckelhantering har nått en hög mognadsgrad

Var finns den svagaste länken?

Kan vi lita på våra enheter!?

Sändare



Hej Klas!
Här kommer
de preliminära
bokslutssiffrorna
för er kontroll....



Kanal

Mottagare



Hej Klas!
Här kommer
de preliminära
bokslutssiffrorna
för er kontroll....

Kryptering



!XjkddjJKediek"

D93nc982^<j34k
fsf>Skjf9s0u9jljs
dfsdf94n45!90?g
"de...

!XjkddjJKediek"

D93nc982^<j34k
fsf>Skjf9s0u9jljs
dfsdf94n45!90?g
"de....

Avkrypterin
g



Hej Klas!
Här kommer
de preliminära
bokslutssiffrorna
för er kontroll....

Ny inriktning - plattformssäkerhet

- Plattformssäkerhet – en definition
 - En säkerhetsmodell som används för att skydda all eller den mest säkerhetskritiska delen av mjukvaran och/eller exekveringsmiljön på en plattform, dvs. en väldefinierad beräkningsenhet.
- Ron Rivest på RSA 2010
 - ” ...platform security is getting critical – keep secrets secret and use them securely”

Vad innebär plattformssäkerhet?

- Metoder för att "mäta" om ett system är i ett pålitligt tillstånd eller ej (beräkning och jämförelse av hash värden, loggar, verifikation av hårdvaru-identitet, identifikation av plattformens "ägare" etc.)
- Metoder för att separera säkerhetskritiska funktioner från icke-säkerhetskritiska på en och samma plattform
- Metoder för att förhindra att skadlig mjukvara tillåts att exekvera på en plattform
- Skydd av exekveringsmiljö från intrång och avlyssning
- Övervakning/monitorering av en exekveringsmiljö

Plattformssäkerhet berör allt från högpresentanda plattformar så som serverar till inbyggda system och sensornoder!

Plattformssäkerhetsprojekt på SICS

- Secure Virtualization and Multicore Platforms (SVaMP)



- <http://www.sics.se/projects/svamp>

- Secure Management of Trusted Virtualized Platforms (SMTVP)

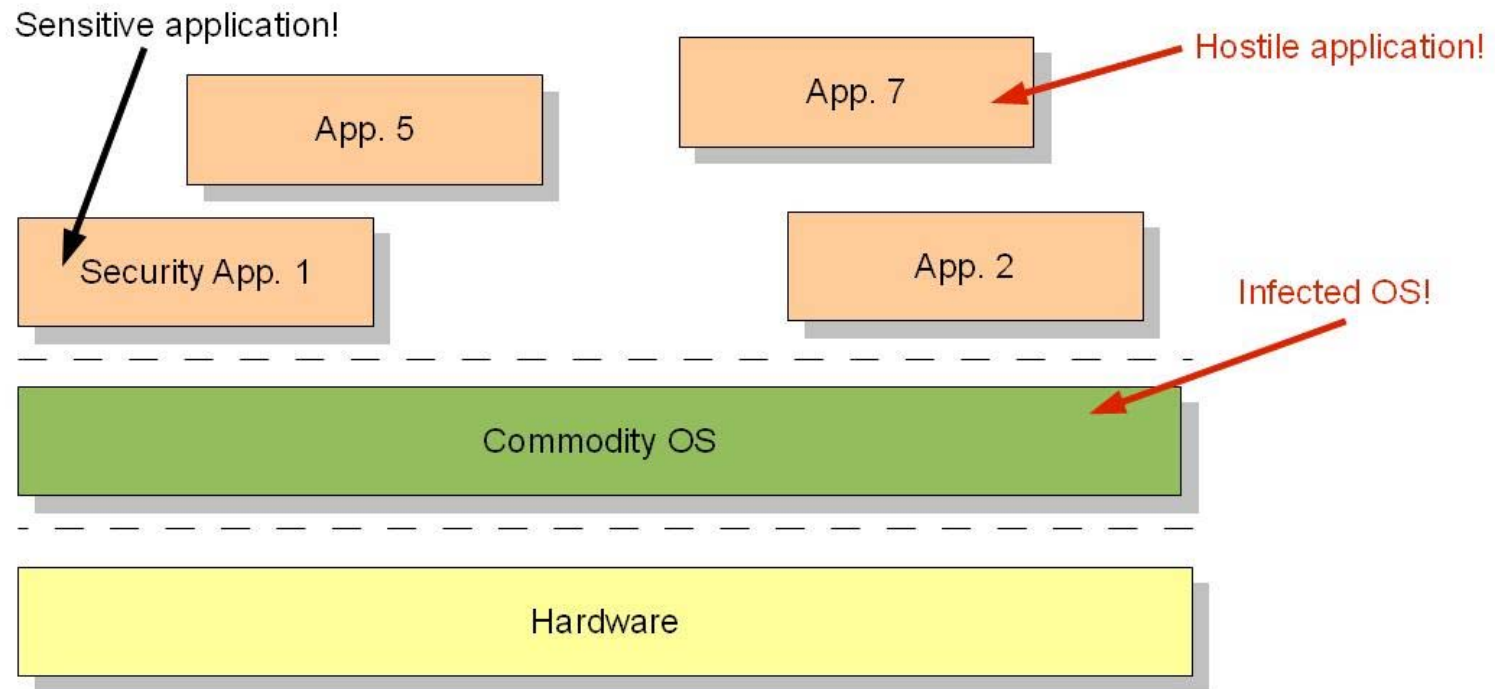


- <http://www.sics.se/projects/smtvp>

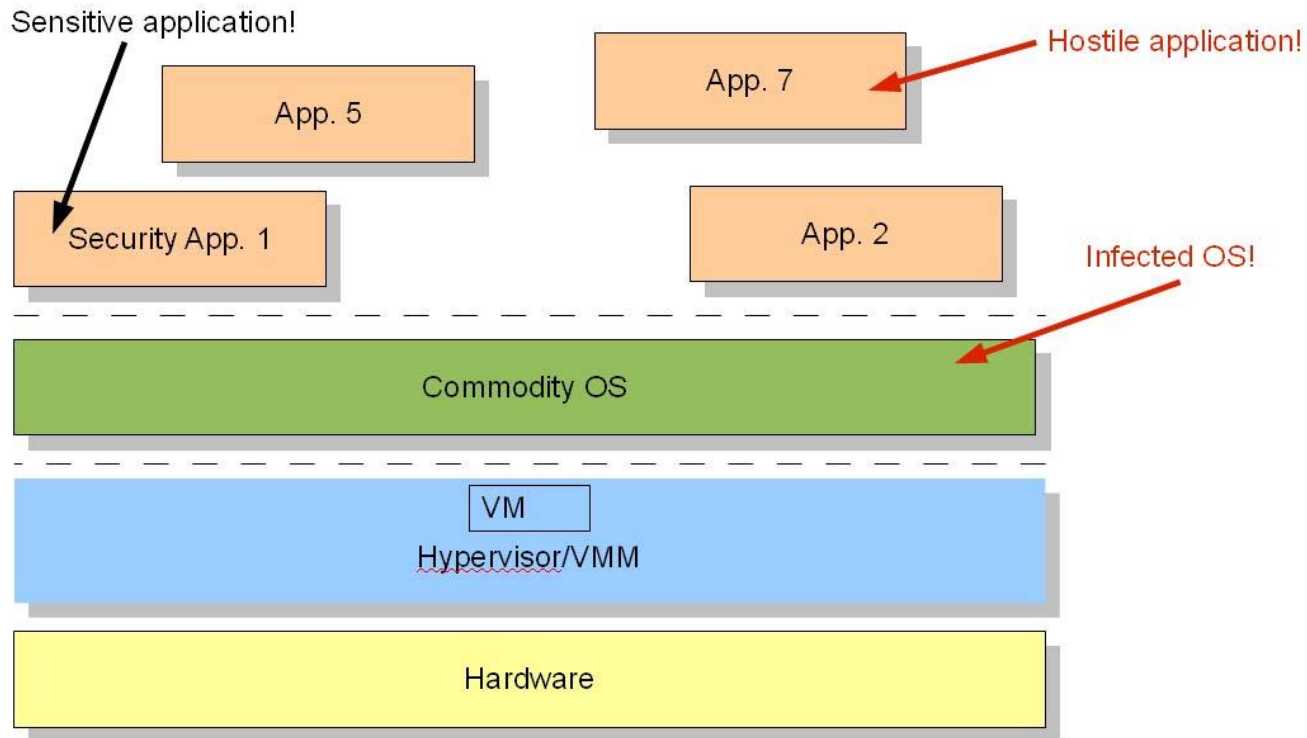
- Secure Virtualization for Embedded Systems (with KTH)

- <https://www.sics.se/projects/tngsecurity>

Typiskt hotscenario

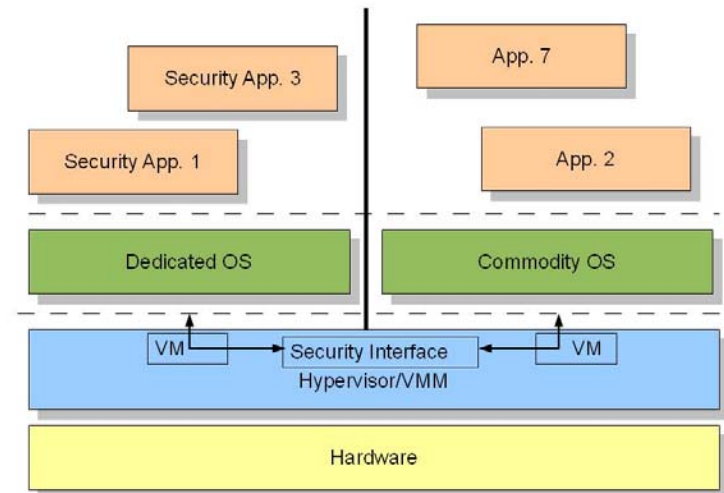


Systemvirtualisering

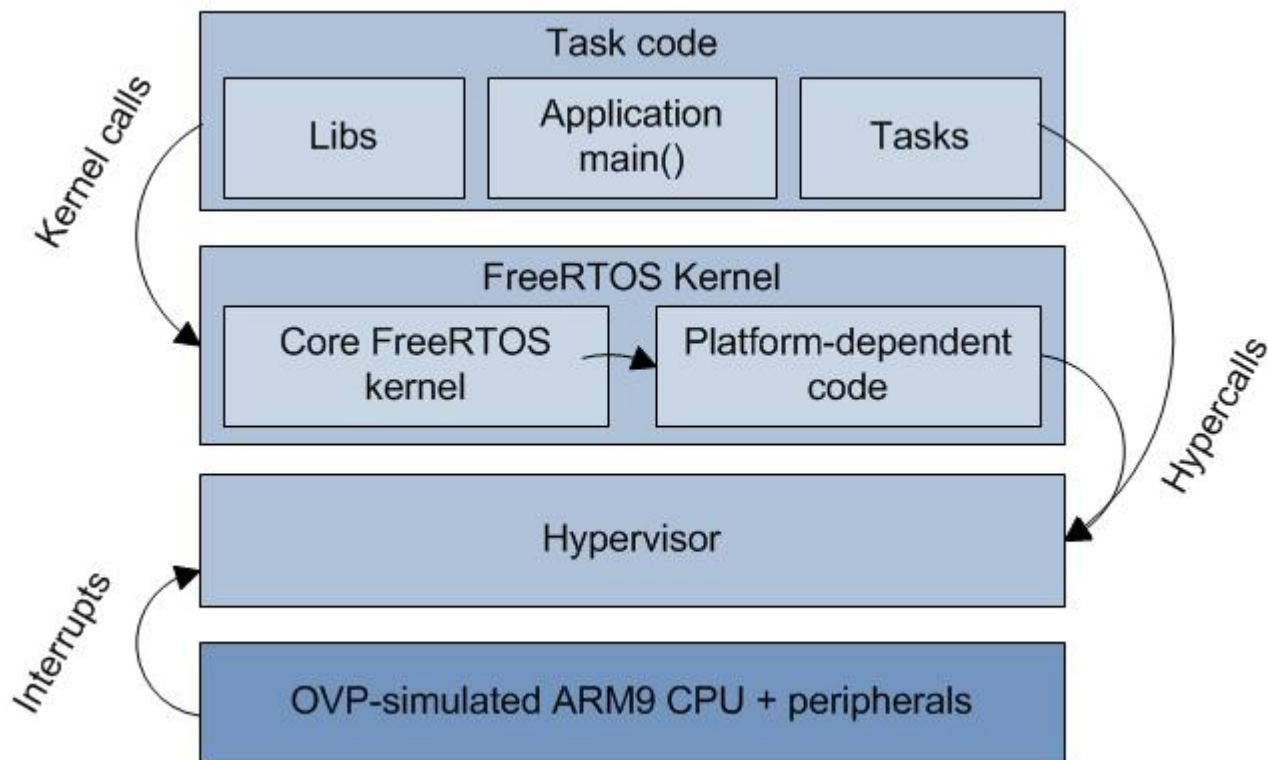


Säker isolering

- Partitionering av systemet där säkerhetskritiska komponenter isoleras från icke-säkerhetskritiska eller potentiellt fientliga komponenter
- En kombination av hårdvaru och mjukvarufunktioner där prestandan till stor del bestäms av stödet i hårdvaruplattformen
- Några forskningsfrågor:
 - Lösningar för resursbegränsade plattformar
 - Prestanda!
 - Formellt bevis av säkerheten



En SICS utvecklad liten hypervisor för ARM och FreeRTOS



Några testresultat

Test	Hypervisor instructions	Normal instructions	Overhead %
<i>MathTest, Preemptive</i>	10,766,931	10,472,960	2.81
<i>MathTest, Non-preemptive</i>	10,762,865	10,469,648	2.80
<i>YieldingMathTest, Preemptive</i>	11,902,174	11,109,395	7.14
<i>YieldingMathTest, Non-preemptive</i>	11,897,357	11,105,748	7.13
<i>FlashTest, Preemptive</i>	163,411,107	163,406,633	0.003
<i>FlashTest, Non-preemptive</i>	163,411,584	163,406,780	0.003

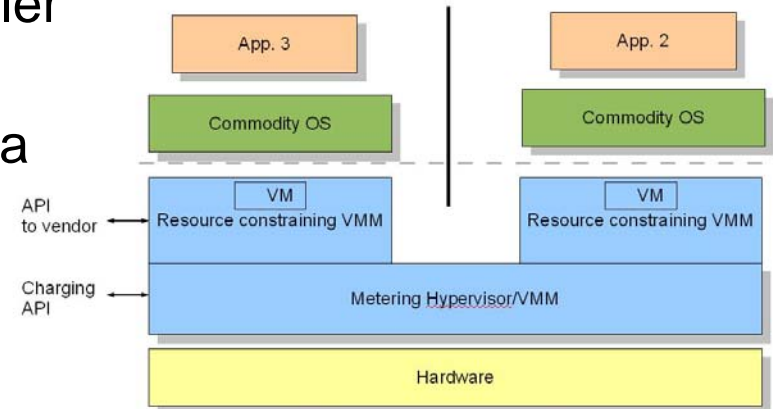
SICS hypervisor – nästa steg

- Stöd av minst två parallella virtuella maskiner
- Stöd för ARM v6 instruktionsuppsättning
- Undersöka olika metoder för att formellt bevisa säkerheten av olika implementeringar
- Stöd för multiprocessor system
- Andra CPU arkitekturer
- Etc.

Virtualiserade telekommunikationssystem

- Scenario

- Flera teleoperatörer på gemensam infrastruktur
- Virtualiseringslager ansvarar för att tilldela resurser enl. licensavtal och/eller *mäta verklig resursförbrukning*
- Operatörers resurser i form av virtuella maskiner kan flyttas mellan fysiska plattformar efter behov

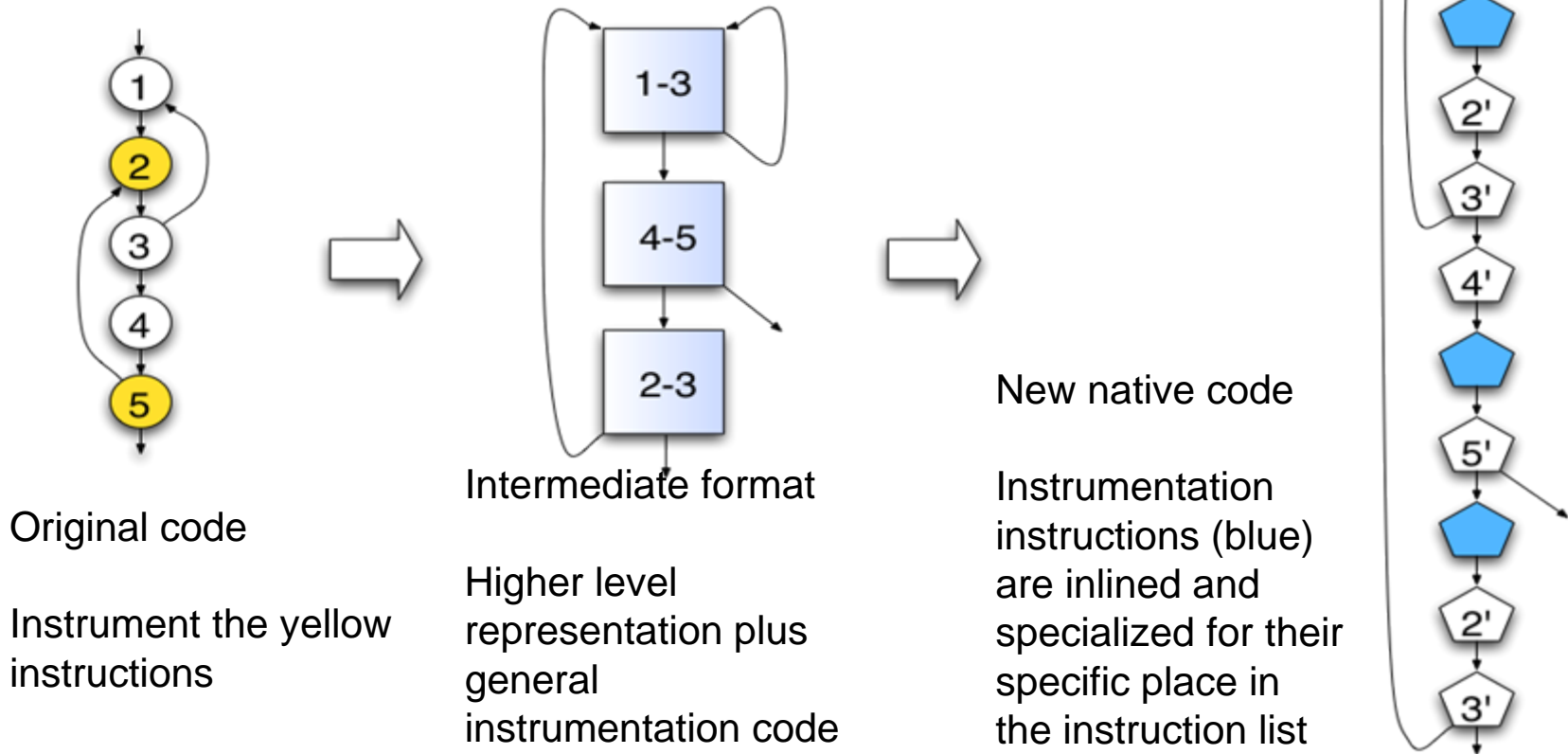


Säker resurshantering i virtuella system – några forskningsfrågor

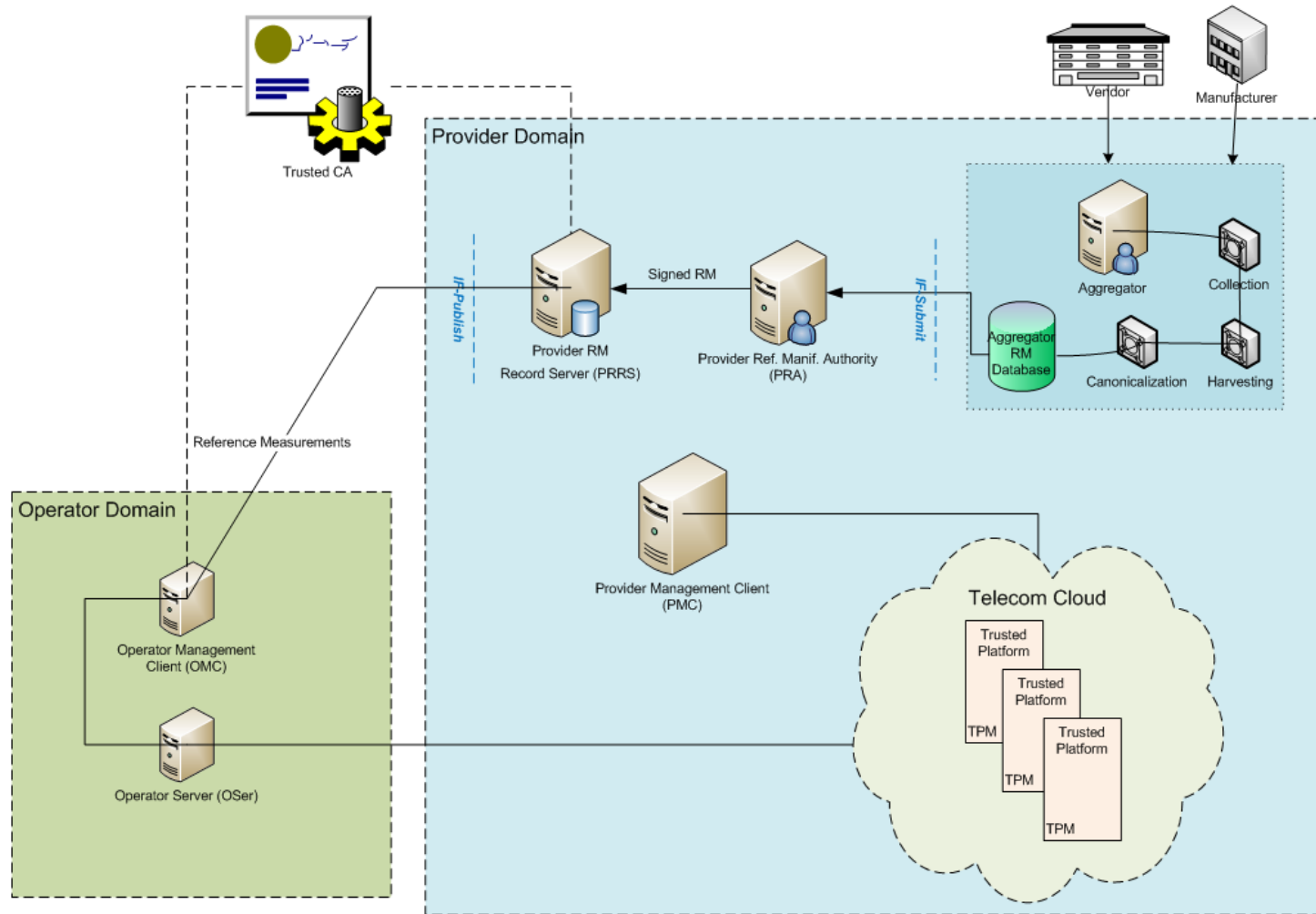
- Design av hypervisor för säker mätning av resurser och/eller kontroll av resurstilldelning
- Säker konfigurering och migrering av operatörskontrollerade virtuella maskiner
- Hot:
 - Operatör rapporterar ej korrekt resursmängd eller försöker tillskansa sig större resursmängder än de tilldelade
 - En operatör får tillgång till information från annan operatörs nät (informationsläckage mellan virtuella maskiner)
 - Operatörer lägger ut ”jobb” på osäkra eller komprometterande plattformar som göra att känslig information läcker ut

Finkornig mätning av resursförbrukning och resurskontroll (Lars Rasmusson)

- Ny SICS metod: "Re-assembling code with intrumentations"



Förslag på TCG baserad arkitektur (Mudassar Aslam)



Virtualiserade telekommunikations-system – nästa steg

- Fullständigt design av en TCG baserad arkitektur för skydd av virtualiserade telekomresurser
- Färdigutvecklad prototyp för resursmätning och kontroll
 - Formell verifikation av säkerheten av implementationen/modellen
- Utveckling av ett komplett testsystem

Personer på SICS

- Christian Gehrman
- Lars Rasmusson
- Mudassar Aslam
- Oliver Schwarz
- (Dennis Nilsson)