SYMBIAN FOUNDATION

Mobile Phones, Security and Open Source: Make a Difference

Craig Heath

Chief Security Technologist

1 Boundary Row
London, SE1 8HP
UK

Email: craigh@symbian.org
Mobile: +44 7765 222 659

Web: secblog.symbian.org

UKUUG
Summer Conference
08 Aug 2009

SYMBIAN

Topics

What is the Symbian Foundation?

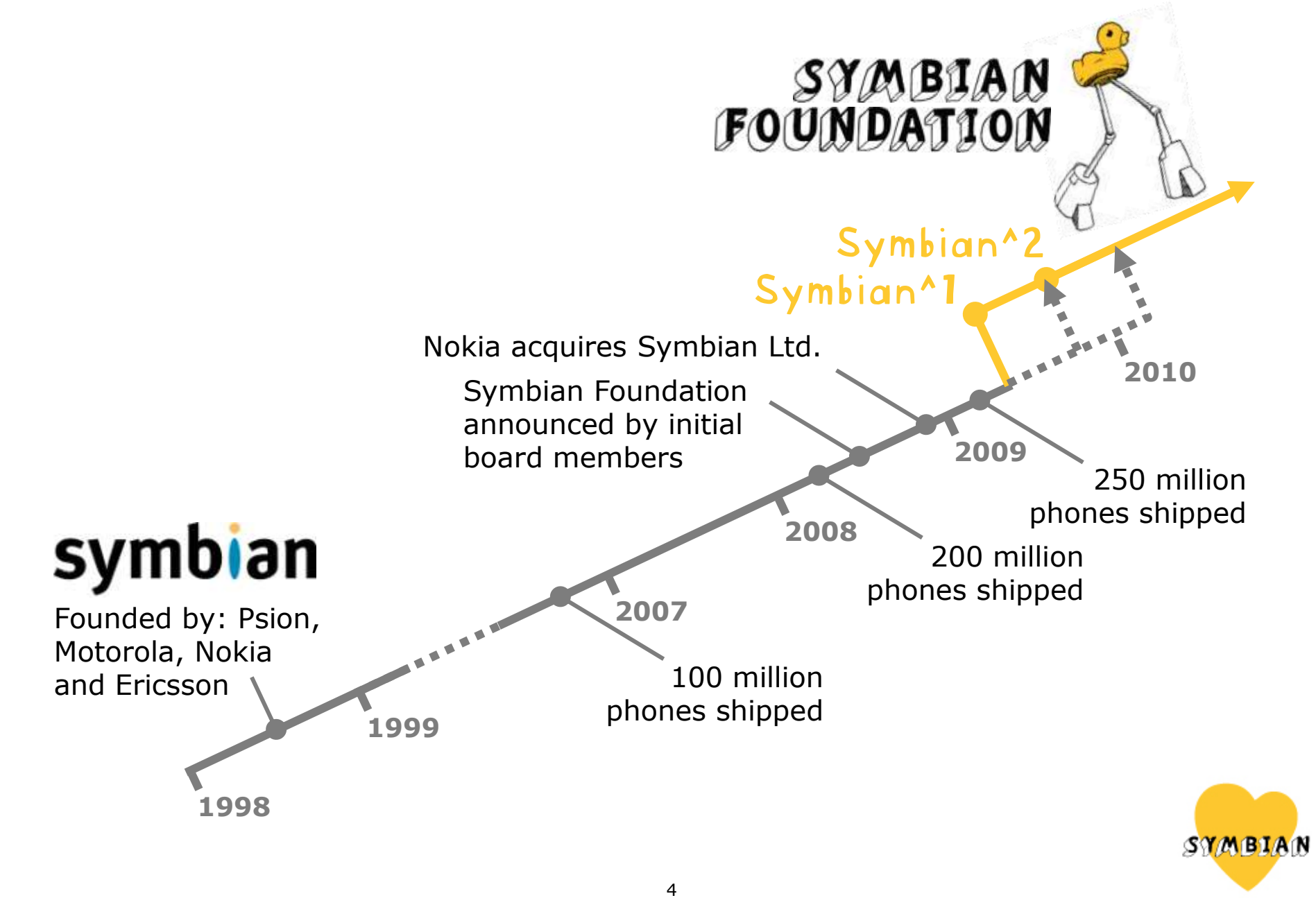
Why Should I Care about the Symbian Platform?

What's so Good about the Security Architecture?

How Can We Make a Difference?

What is the Symbian Foundation?

Symbian Timeline



The Symbian Platform

40 million lines of code (device + tools)

450,000 source files

45,000 source directories

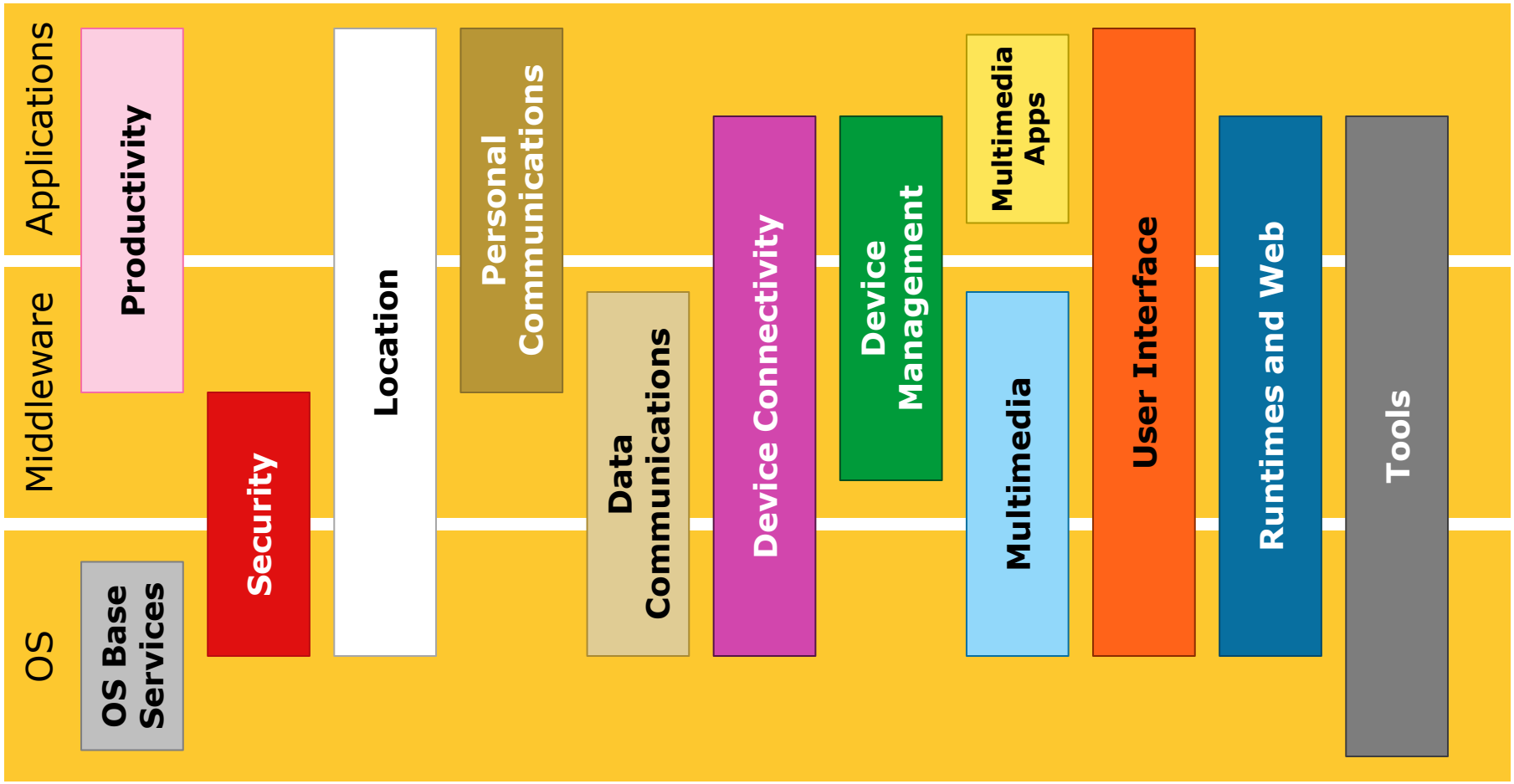
2000 software components

133 packages

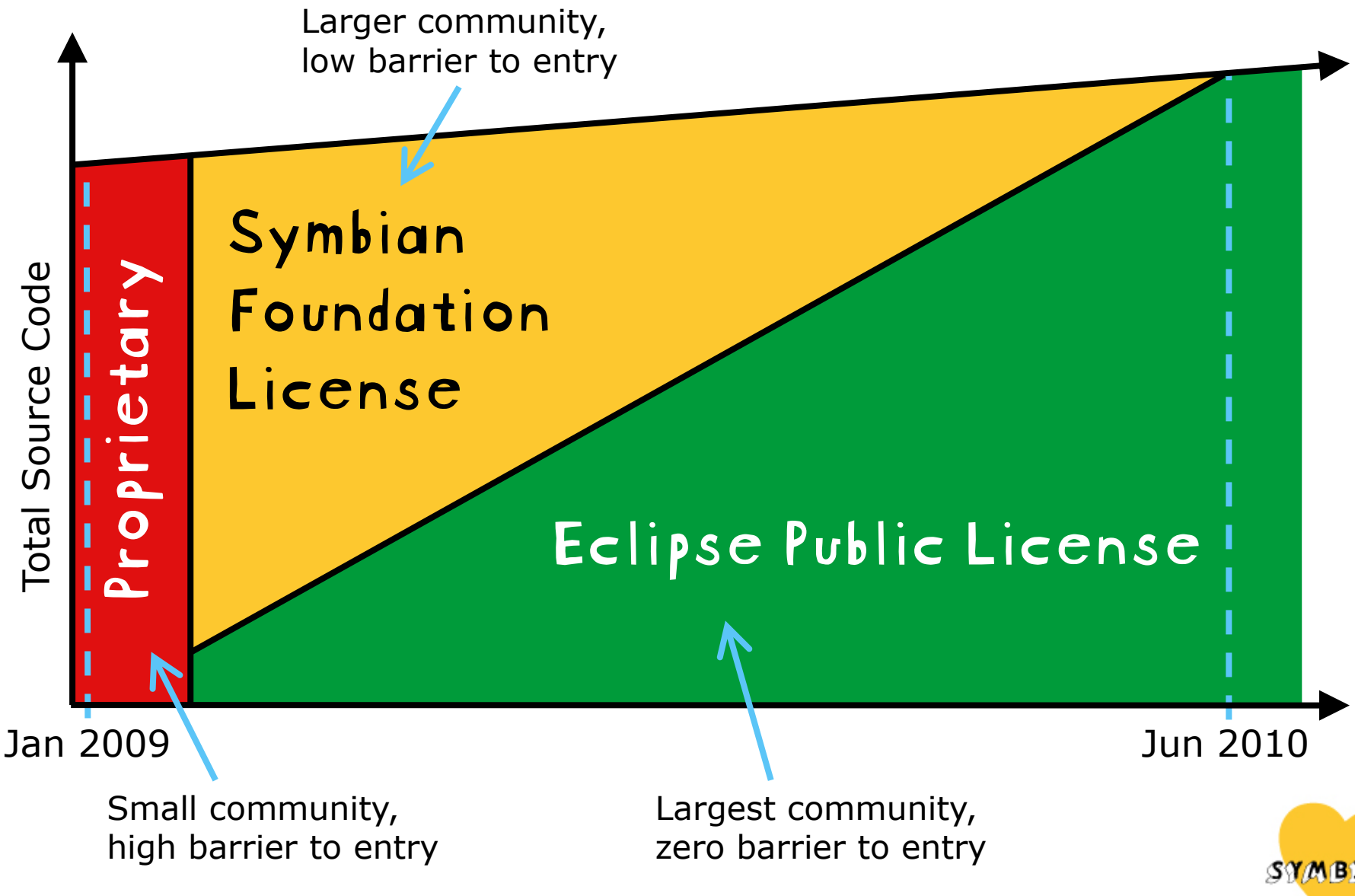
13 technology domains, spanning 3 layers

1 unified mobile operating system

Symbian Platform Technology Domains



Transition to Full Open Source



Why Should I Care about the Symbian Platform?

Phone Software Affects People's Daily Lives

- Opportunities and challenges different to PC or server software
- A mobile phone is a deeply personal item
  - always with you ("don't leave home without it")
  - not typically shared, even with other family members
- A mobile phone can be a payment instrument
  - billing is the "core competency" of mobile network operators
  - e.g. premium rate SMSes for reality TV voting
- A mobile phone is perceived as far more trustworthy than a PC
  - relied on to e.g. make emergency calls
  - not expected to be rebooted daily (if ever)
  - doesn't need anti-virus software
  - your pocket feels like a safe place to keep private information

Smartphone Platform Units Shipped (mid 2009)

- Symbian: > 250 million

- BlackBerry: ~60 million

- Windows Mobile: ~30 million
- iPhone: ~25 million

- Android: < 2 million

If you want your software to get into the pockets of the largest potential number of phone users, the Symbian platform is clearly the best choice!

What's so Good about the Security Architecture?

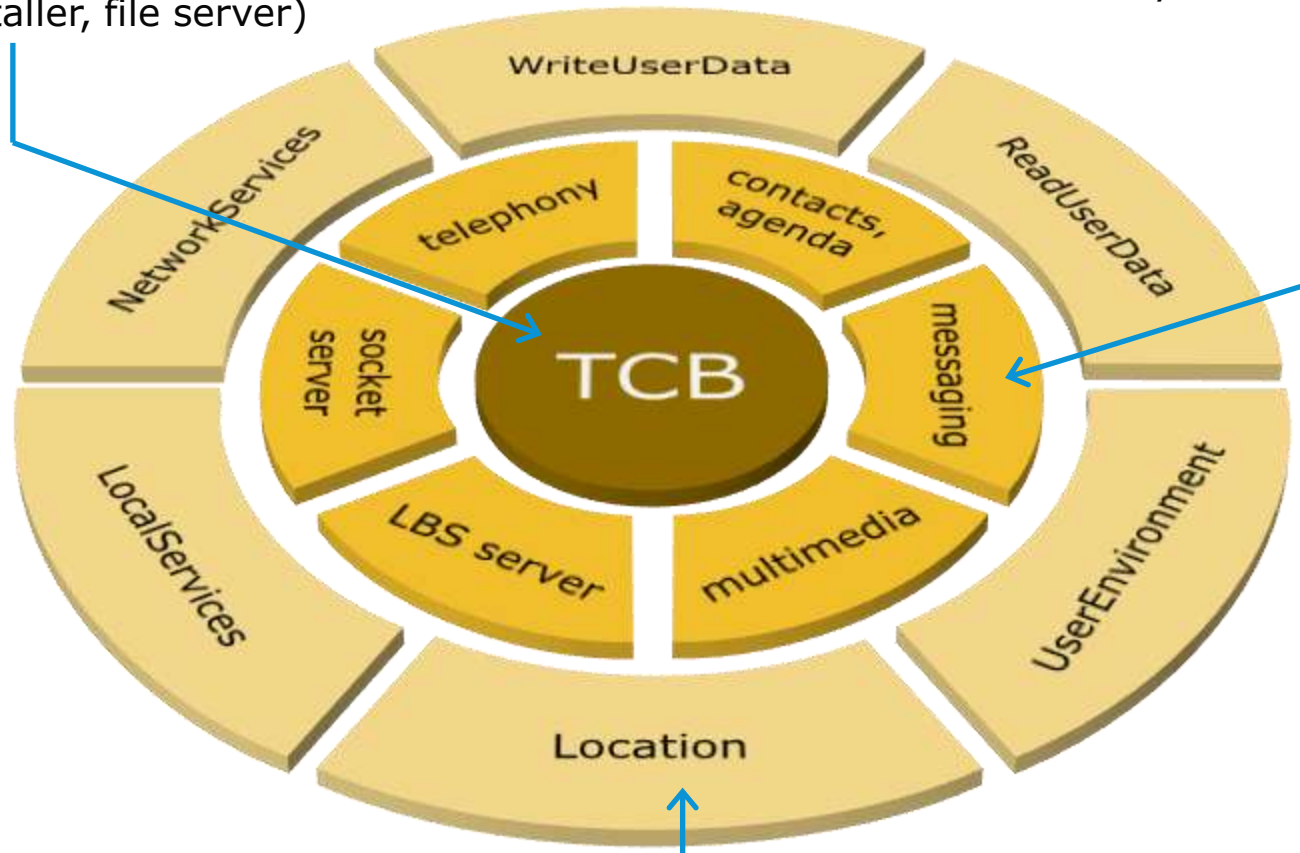
Symbian Platform Security Architecture

- Run-time controls on applications
- Based on long-established security principles
  - e.g. “Trusted Computing Base”, “Least Privilege”
- Designed for mobile device use cases
  - not relying on controls from multi-user timesharing systems
- “Capabilities” determine process privileges
  - checked by APIs which offer security-relevant services
- “Data Caging” protects stored data
  - protected directories for system and for applications
- Secure identifiers (“SIDs”) for applications
  - verified at install-time

Capabilities and the Least-Privilege Principle

Trusted Computing Base (TCB)
full access to all APIs and files
(kernel, installer, file server)

Trusted Computing Environment (TCE)
servers with "system capabilities"



most third-party apps need
only "user capabilities"

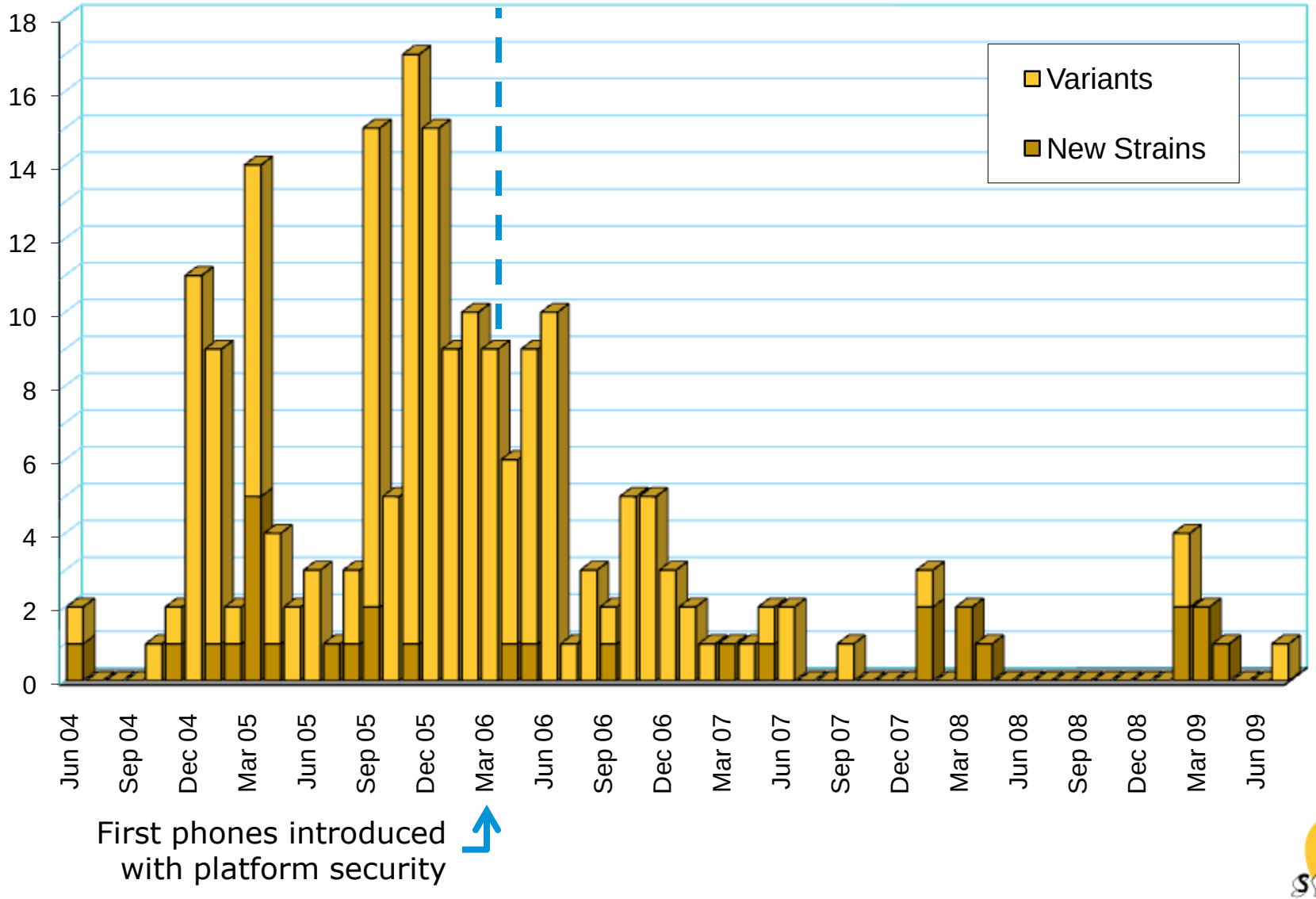
Data Caging and SIDs

- Files protected according to their directory path
- Critical system files are highly protected
  - only the Trusted Computing Base can modify them

directory path	capability to read	capability to write
`\sys`	`AllFiles`	`Tcb`
`\resource`	none	`Tcb`
`\private\`*<mySID>*	none	none
`\private\`*<other>*	`AllFiles`	`AllFiles`
`\`*<other>*	none	none

- Every process identified by a Secure ID (SID)
- ID ranges allocated by Symbian
  - "Protected Range" SIDs only for signed applications
  - SID ownership checked and enforced by signing authority

Symbian Platform Security Effect on Malware



How Can We Make a Difference?

Bringing a Different Perspective

- Open source community can do stuff that has little or no value to the phone companies
  - no need to wait for Nokia (or anyone else) to implement it
- No limitations on distributing "after-market" applications
  - Symbian Signed is being simplified, although it won't go away altogether (we still need to somehow distinguish good freeware from bad malware)
- Contributions to the platform can be included in devices
  - but if you take value away from the manufacturers, it's unlikely to be put in commercial devices
  - taking value away from the network operators could also restrict your user base (it won't get put in subsidised devices)

Roadmap Driven by External Contributors

- Symbian Foundation has no in-house developers
  - similarly to the Eclipse Foundation, staff support the community:
    - collaboration infrastructure (forums, wiki, mailing lists, source code repository, bug tracker, etc.)
    - interface management and testing for device compatibility
    - development kits for devices and after-market applications
    - application security infrastructure (signing, revocation)
- Total commitment to community development, unlike:
  - Android – nearly all development done in-house
  - Mozilla – about 60% of development done in-house

What Community Projects are There?

- The main source of ideas should be the community
- My interests are (obviously!) in the security area:
  - Correcting "information asymmetries" to benefit consumers
  - Better management of personal information
- 4 projects that phone manufacturers are unlikely to do:
  - notarised call recording
    - service providers record your call so why don't you?
  - pre-advice of premium-rate charges
    - data is available, why not present it to the consumer?
  - simple controls on sharing of personal data
    - most social networking services do a bad job on this
  - keeping control of your own identity
    - not having to rely on vendors to "do the right thing"

Notarised Call Recording

- "Reciprocal Surveillance" – who watches the watchers?
- When you call a utility company, do you hear "this call may be recorded"?
  - it's being recorded for their benefit, not yours
- Have you ever been told they will do something, but when you call back: "I'm sorry, I have no record of that"?
  - probably they do, but you can't prove it: information asymmetry
- Even a simple recording would help, along with the call log
  - but unlikely to be good enough evidence to use in court
- Could combine this with a **digital notary**
  - take a hash of the recording (prevents future tampering)
  - have the hash signed by a trusted third party with a time stamp
  - proves that the recording was made at or before that time

Pre-Advice of Premium Rate Charges

- Premium rate voice and SMS service providers in the UK are required by law to advise consumers of their charges in advance
  - but they haven't always done this is the most obvious way
  - malware isn't going to respect this
- Also in the UK, you can find out the charges with a free SMS (76787)
  - also available as a web-based online number checker
  - I doubt many people use this regularly
- It would be much more useful if your phone did this for you
- how about a filter to check the numbers your phone is calling and texting, and warn you before the call is made if it's premium rate?
  - "allow this application to spend 50p?" is far more useful than "allow this application to make phone calls and send text messages?"
  - Could be extended to enforce rules, e.g.
    - allow this application to spend up to £5
    - allow this application to send 2 texts per day

Privacy Labels

- The Symbian platform has the notion of "user data", and the `ReadUserData` and `WriteUserData` capabilities
  - doesn't, however, identify which user data is intended to be shared and which to be kept private
- Could borrow the concept of "sensitivity labels" from the classic MLS (Multi-Level Secure) orange book systems
  - principle is that the sensitivity label is indivisible from the data
- Labels could be set in one application (e.g. the camera app) and then acted upon in another (e.g. a file sharing app)
  - should be preserved even when files are moved or copied

VRM (Vendor Relationship Management)

- Reciprocal of "Customer Relationship Management" (CRM)
  - shouldn't have to rely on vendors to manage your privacy
    - they may "do the right thing" but you shouldn't have to trust them
- projectvrm.org: VRM Principles
  - A manifesto in the form of six principles
  - quick summary:
    - customers should always be in control of their own data
    - customers should be able to set their own "terms of engagement"
- Based on web services standards for identity management
  - "user-driven identity" – OpenID / Information Cards

Over to You! Any Questions?