SiVenture

Building Technical Attacks into Common Criteria Evaluations

Tony Boswell

CLEF Technical Manager

SiVenture

ECRYPT II

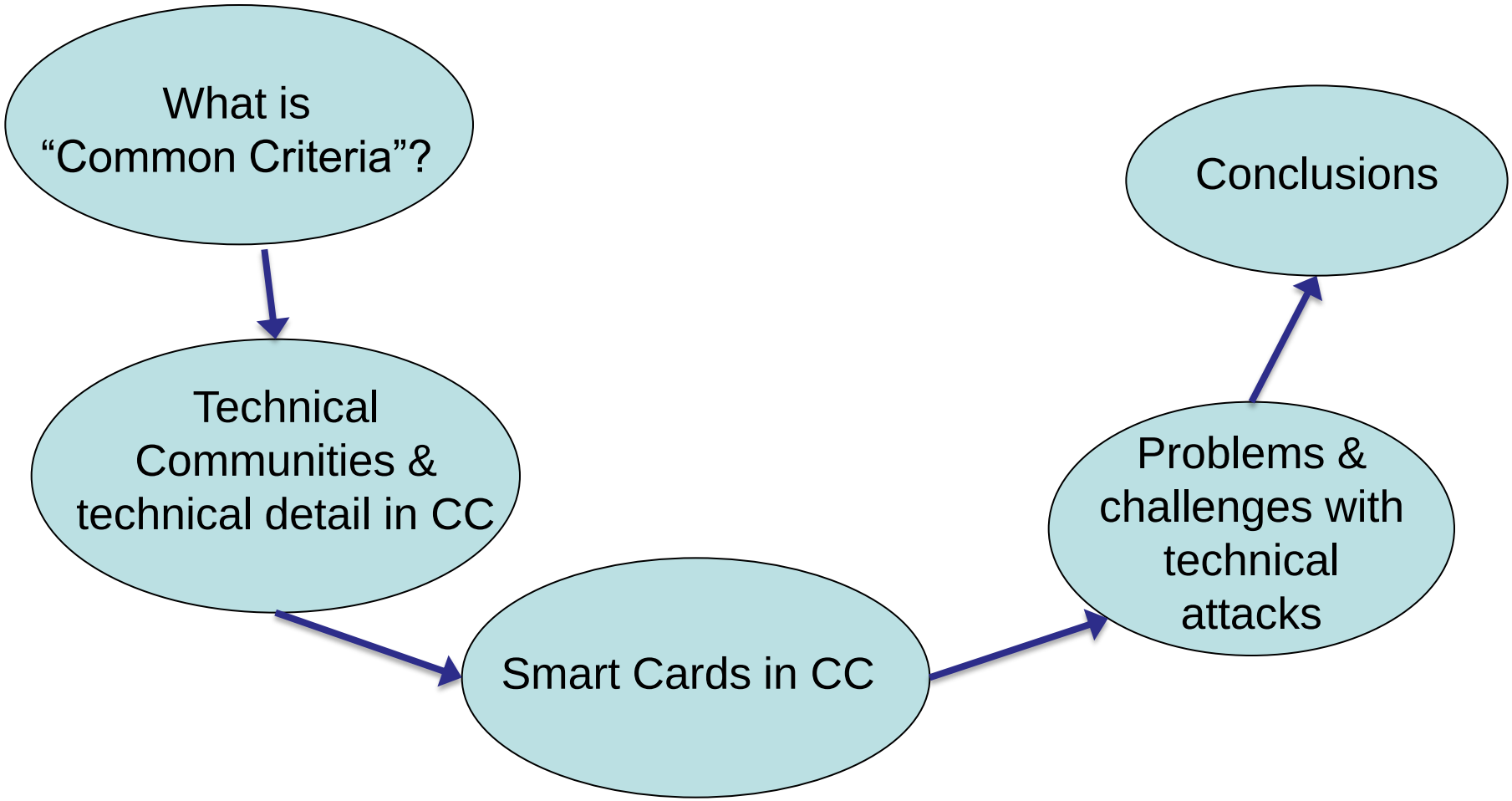
Physical Attacks

November 2012

SiVenture is now part of Cisco.

cisco

Overview

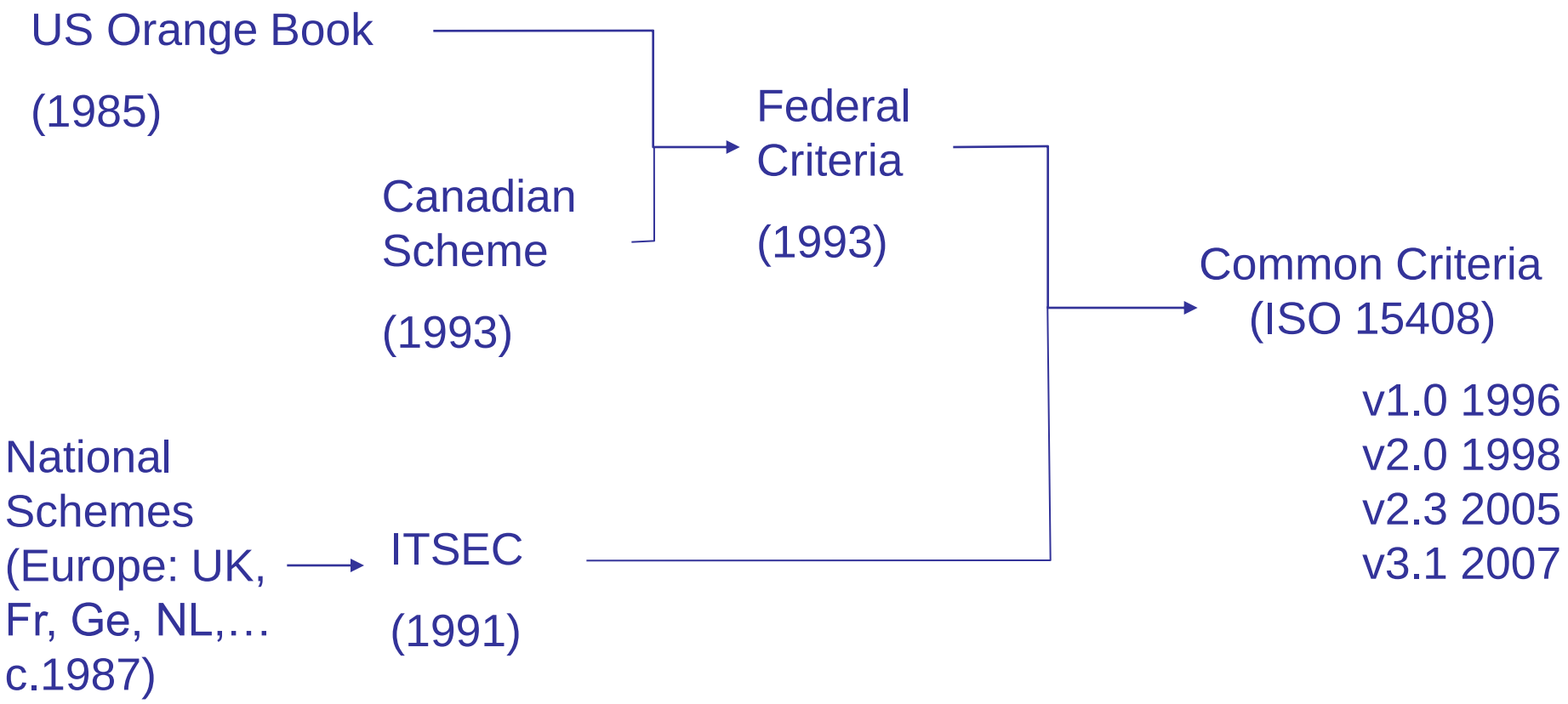

What is "Common Criteria"?
Technical Communities & technical detail in CC
Smart Cards in CC
Problems & challenges with technical attacks
Conclusions

Common Criteria – what is it?

- A method of *evaluating* (some of) a product's (or system's) security (features)
- Aimed at establishing *assurance* (="grounds for confidence")
- Evaluations are performed by approved organisations
- Certification is by national certification bodies (CBs)
- Something you choose (or are forced) to do

- Internationally recognised under CCRA and SOG-IS

Roots of Common Criteria



Common Criteria – Aims

- *Comparable* evaluations
- "Evaluation should lead to objective and repeatable results that can be cited as evidence, even if there is no absolute objective scale for representing the results of a security evaluation. The existence of a set of evaluation criteria is a necessary pre-condition for evaluation to lead to a meaningful result and provides a technical basis for mutual recognition of evaluation results between evaluation authorities."

(Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012)

Common Criteria – Structure

- 3 Main parts:
  - 1: Introduction & General Model
  - 2: Security functional components
  - 3: Security assurance components
- …plus Common Evaluation Methodology (CEM)
- …plus (mandatory) supporting documents
- …plus national scheme requirements

See www.commoncriteriaportal.org

Smart Cards and CC

- Smart card evaluation started under ITSEC
- Smart cards were a natural fit for early CC because of the evaluation structure and international recognition…

  …but it took a while to make this really work internationally
- Smart cards are still by far the largest product category for CC certificates (over 500 certificates)

CC Limitations (1)

- “The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using the CC in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.”

(*Ibid*)

CC Limitations (2)

- "The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area."

(*Ibid*)

Generic CC challenges

- Consistency
  - Between national schemes (CBs), labs, evaluations
  - Especially important as more countries issue certificates
- Building state-of-the-art attacks into evaluations…for every technology type
  - Cf. Tracking and applying CVEs?
  - Lists and databases specific to technologies
- Maintaining relevance to stakeholders
  - Government and commercial use
- Time and cost of evaluations
  - In practice this has to matter!

Current CC trajectory…

- Realisation that EAL4 may not mean quite the same thing for a smart card product and a larger-scale product…
- 'Retreat to EAL2' for most product types (except smart cards and POI)
  - See the recent CCRA Management Committee vision statement at http://www.commoncriteriaportal.org/files/ccfiles/2012-09-001_Vision_statement_of_the_CC_and_the_CCRAv2.pdf
- This sets out a new direction to improve evaluation through the use of Technical Communities, based on the smart card model (ISCI & JHAS)

Technical Communities?

- Looking to deal with what happens when CC abstraction meets reality!
- Gather together a wide-ranging group of stakeholders
- Interpret CC for a particular technology domain, and provide a foundation for *acceptance* and *use* of that interpretation

(For more, see:

- Boswell T, Smart card security evaluation: Community solutions to intractable problems, Information Security Technical Report, Volume 14 issue 2, May 2009, pp57-69
- Building Successful Communities to Interpret and Apply CC, 10th ICCC, at http://www.yourcreativesolutions.nl/ICCC10/proceedings/doc/pp/Building_successful.pdf

Community Characteristics (1)

- Relevant: identifies and solves real problems
  - therefore has to involve all the players, and especially the problem-owners
- Representative: no gaps in the stakeholder web
  - both problems and solutions should benefit from the views of all the stakeholders
- Inclusive: not just the people we may *prefer* to talk to
  - and of course this means the Community will include competitors
- Engaged: caring about the solutions
  - experience and expertise
  - regular attendance (by the same person); tangible contributions

Community Characteristics (2)

- Connected: works with other communities
  - e.g. CBs, evaluators, industry/vendor groups, deployment schemes (e.g. payment schemes)
  - ‘sub-communities’ enable better consensus within the main Community
- Output-oriented: produces specific deliverables
  - obviously related to the problems!
- Authoritative: can determine acceptance as well as definition
  - avoid ‘solutions in principle’ or ideas that face further hurdles to get adopted
  - avoid ‘not invented here’
  - channel to formal adoption of outputs

What do communities produce?

Examples of what CC Technical Communities may produce:

- protection profiles
  - containing interpretations, refined/extended assurance components, etc.
- methodology
  - e.g. applying composition (and maybe ALC requirements) in the situations typical of the technology type or usage domain
- catalogues of attack methods
  - to establish evaluation content and improve consistency between evaluations
- qualification/competence processes
  - initial qualification of a lab for a domain
  - updating for consistency at (or close to) state-of-the-art

Smart Card CC Interpretation

- We map the general CC methodology (e.g. what is CC's "Functional Specification" for an IC?)
- We identify requirements for CC laboratories undertaking this work
- We write general standard requirement sets in Protection Profiles
- But some of the most important work is in identifying what vulnerability analysis should mean in an evaluation:
  - what attacks to try
  - how to interpret results

Smart Card Attack Potential Model

- Rate the difficulty of ‘Identification’ and ‘Exploitation’ phases of an attack in terms of:
  - Elapsed time
  - Expertise
  - Design knowledge
  - Number of samples required
  - Equipment
  - Open Samples

For more details see:

Application of Attack Potential to Smartcards, v2.7 Revision 1, March 2009, CCDB-2009-03-001

Attack Potential Example

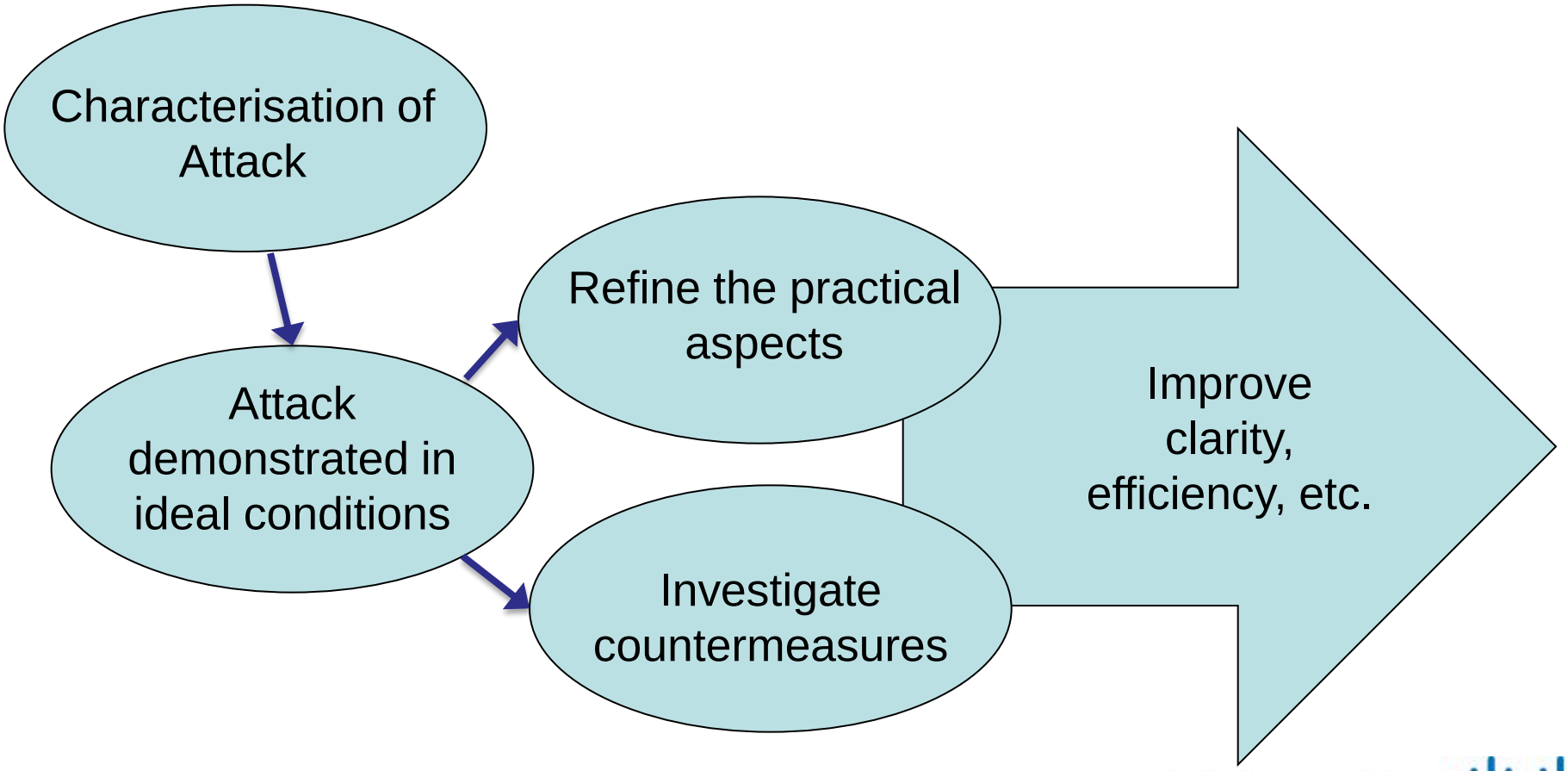
Factor	Comment	Ident'n	Exploit'n
Elapsed Time	We assume the deprocessing and initial testing to identify the failure combined with demonstrating the vulnerability takes less than 1 month using open samples to find the right combination of trigger and location (assuming the restricted command information is available). We assume exploitation based on a description of the attack and the commands to use.	< 1 month (3)	< 1 week (4)
Expertise	To find the right combination of trigger and location the attacker needs expert knowledge. He has to analyse the power traces and define the pattern recognition. A Proficient rating is required for exploitation, because of the deprocessing techniques and equipment operation required.	Expert (5)	Proficient (2)
Knowledge of TOE	The attack requires Restricted information to identify exploitable commands, but the command is assumed to be scripted for the exploitation phase (hence Public).	Sensitive (4)	Public (0)
Access to TOE	More than one sample may be necessary, but less than ten.	<10 samples (0)	< 10 samples (0)
Open Sample / Known Key	It is assumed that open samples are managed accordingly.	Sensitive (4)	NA
Equipment	Minimum requirement is equipment to deprocess the chip, bond out the pads, and then to generate and analyse the required commands to drive the IC. A laser and optical microscope are required to generate the perturbations, and a digital oscilloscope is used to identify and repeat the attack timing.	Specialized (3)	Specialized (4)
Sub Total		**19**	**10**
Total		**29**	

Why we need technical detail for CC

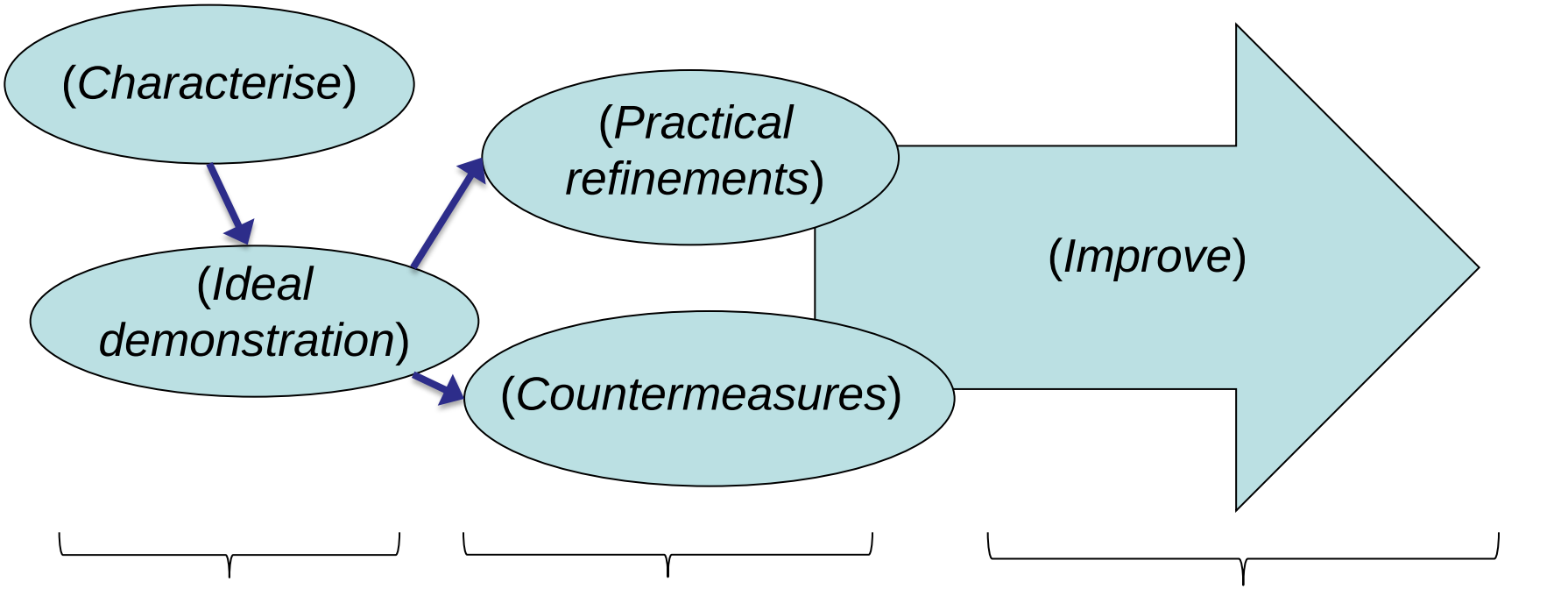
- Adding technical detail in CC documents *and community discussions* helps to get consistent attack potential ratings
- And of course it helps to establish the expectations for an evaluation (for developer, lab and certificate-user)
- Makes useful links to risk-owners
- But it also imposes a maintenance burden
  - we have to review ratings regularly
  - we get an ever-increasing number of attacks to squeeze in

How do we bring attacks into CC? (1)

I think it's something like this:



How do we bring attacks into CC? (2)



An ideal CC attack?

What might an ‘ideal’ attack look like, from the point of view of applying it in a CC evaluation?

- Clearly defined attack method and result
- Clearly defined conditions of applicability
- Clearly defined countermeasures

This doesn’t turn out to be the naturally-occurring form of most attacks!

Some example attack types in CC

Below are some example attack types that changed expectations for evaluators and developers in CC:

- Early physical (e.g. FIB edits, probing)
- Early power analysis
- Light attacks
- EM analysis
- Backside laser
- Double laser
- 'New' physical (reverse engineering, backside edit)

Along the way we moved from lab-focussed to criteria-focussed

Challenges

- Repeatability, repeatability, repeatability,…
- How to collaborate most effectively?
  - Without killing ideas too early, ‘stealing’ ideas and/or people, or risking reputations
- How to control the explosion of potential tests (so many attacks, so little time)?
- How to encourage research without becoming unrealistic about real applications?

In Conclusion…

- Technical Communities are raising the expectation for collaborative work on attacks (and countermeasures) and for more technical definition of attacks
- For CC, we want to build in new attacks and improved attacks, but also to address the challenges of time and repeatability, so we would very much like:
  - Better tests for susceptibility
  - Better techniques for managing the number of potential attacks
  - Better ‘relevance criteria’ ☺
  - And of course better, *recognisable* countermeasures!

Tony Boswell
tony.boswell@siventure.com
tel: +44 1628 651 361