OARC TAR Panel

SECURE 64

SOFTWARE CORPORATION

La Brea Tar Pit

- What was originally intended to expedite the roll-out of DNSSEC seems to be bogging it down instead
- People who read press articles or attend conferences where they get the impression that “DNSSEC won’t “really be ready for N years” (e.g. RSA conference in San Francisco) or “TARs don’t work” will naturally delay action on their own part to deploy DNSSEC, sign zones or enable validation.

Can we Simplify the Task for Administrators?

Yes, I manage trust anchors

Tar Paper

- If we roll this out a bit at a time, people will start to use it
- Constructive “baby steps”

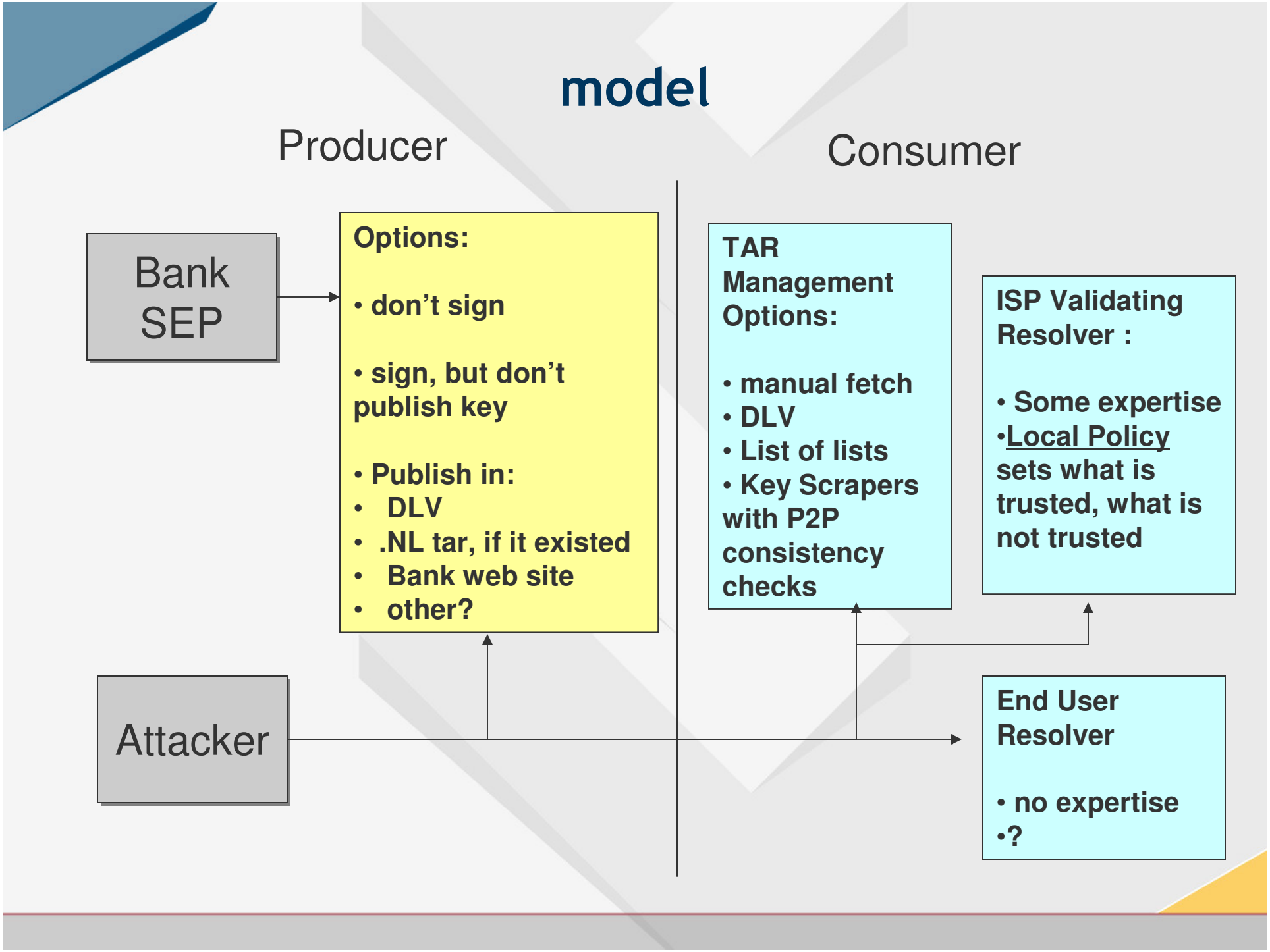
Pragmatic First Steps

- ITAR for TLD's solves first level of problem.
- But it would be helpful to automate the work for the administrator (who may have DNSSEC expertise from "none" to "some" to "expert")
  - Minimum: publish a cookbook to explain how to set up validation
  - Or -- TAR "fetcher" program, coupled with TAR "updater" program
    - Distribute TAR list with system/products
    - 3-file approach
      - Distribution defaults
      - Local over-rides to defaults (delete, modify)
      - Local trust anchors
    - Auto-trust and/or TrustMan to automate RFC 5011 changes to keys
    - Set and forget

Next Level Down

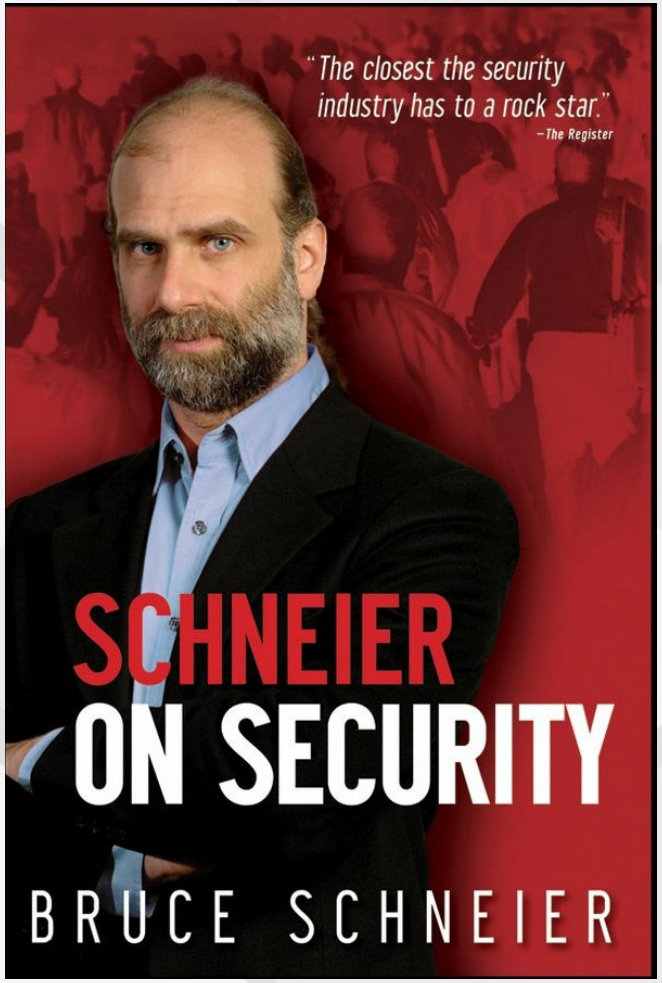
- Example:
  - MyBank.NL wants to sign with DNSSEC after hearing about Brazil's Banco Bradesco cache-poisoning attack
  - But .NL is not signed, so:
    - Do nothing
    - There are benefits to signing, but what do I do with my SEP Key?

model


Producer
Consumer
Bank SEP
Options:
• don't sign
• sign, but don't publish key
• Publish in:
• DLV
• .NL tar, if it existed
• Bank web site
• other?
TAR Management Options:
• manual fetch
• DLV
• List of lists
• Key Scrapers with P2P consistency checks
ISP Validating Resolver :
• Some expertise
•Local Policy sets what is trusted, what is not trusted
Attacker
End User Resolver
• no expertise
•?

Local Policy Example: The X-(Tar) Files

Local Policy 2: Security is a Trade-Off
"Trust, but Verify"



Peer 2 Peer

- Local Policy can turn on/off or set how many friends must agree from how many places before trust begins to grow
  - Policy could be set to
    - None
    - Check, but don't set AD
    - Set AD if everybody agrees
      - Would anyone do this?
- More interestingly, "negative trust" can be inferred if a zone shows up with no key when a key is expected, or a different key than friends found earlier (but that doublecheck because a rollover may be happening)

Summary

- Don’t Shoot Ourselves in the foot; if you have something to say to the outside world, do it constructively
- Baby Steps
- Simplify & Automate
- Local Policy