

Internet banking is dead!

Long live Internet banking

or

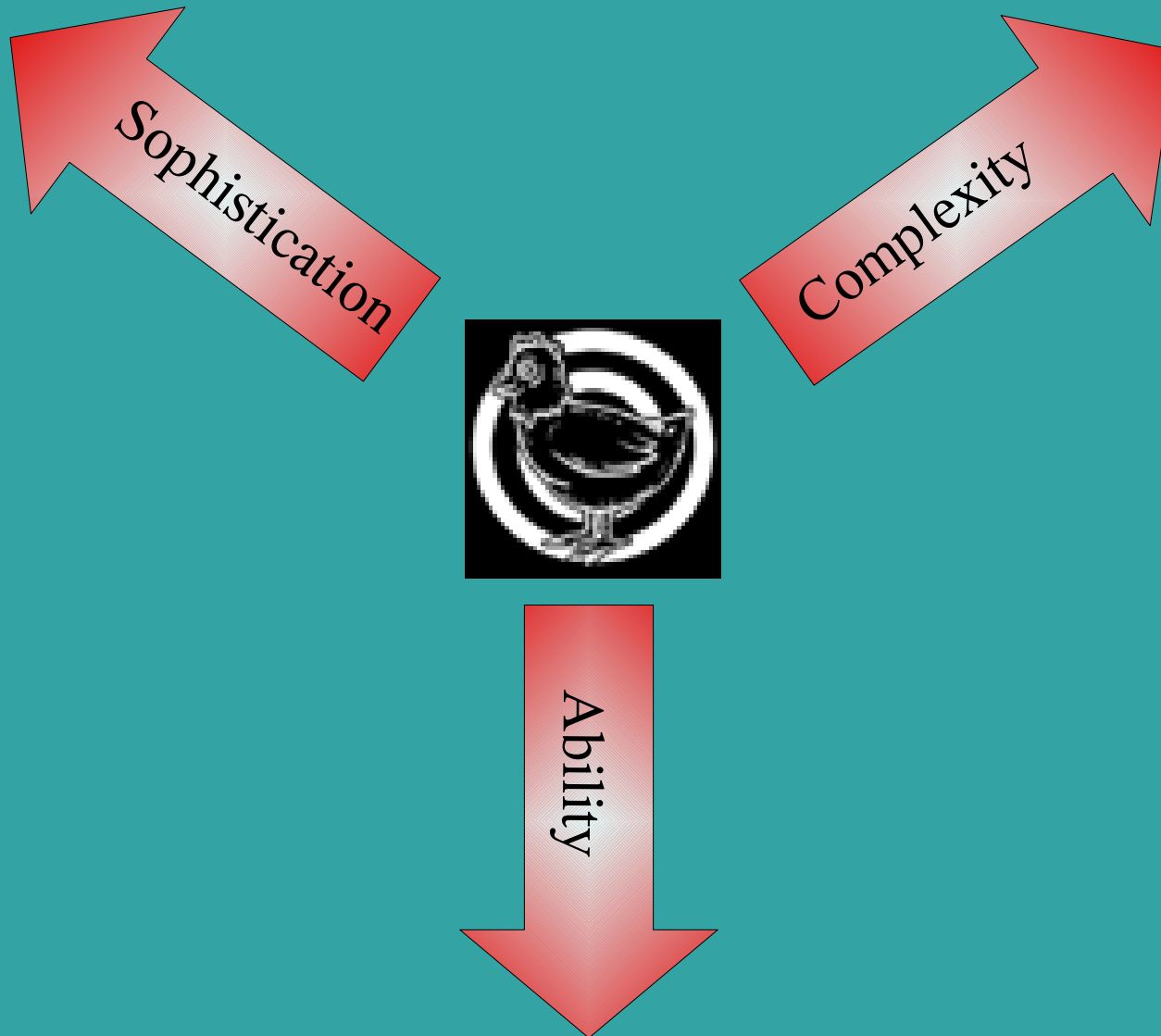
How diverging forces combine to pull apart a hopefully-secure on-line business



Dr Tim Redhead
DotSec Pty Ltd
www.dotsec.com

Brief introductions

- DotSec – Information security specialists
- Secure information-systems
 - Design, implementation, maintenance and testing
 - Legal, financial, utilities and government
- Application security
 - Make it or break it
- Despite the tongue-in-cheek title
 - Broader trends lead to concerns



Force #1

Sophistication of attack

Force 1 - Sophistication of attack

- Ah, the good old days...
- The reality now
 - Established services-oriented industry
- Customizable, software packages and kits
 - Why buy when you can rent?
- Specific targets and flexible clients
 - Mother knows best... about targeted attacks!



What's on the menu?

- Social-engineering attacks
 - Phishing for plug-ins from my virtual wall
- Scripting attacks
 - But its OK, its [whatever] site
- HTML injection attacks
 - Undetectable and SSL-immune
- I'll have the works!



Demo 1

- Install a codec, become one with the borg.
 - Watch for target behaviour
 - Capture anything
 - Key clicks, mouse movements, screen dumps
 - Report back to HQ and await further orders

Force #2

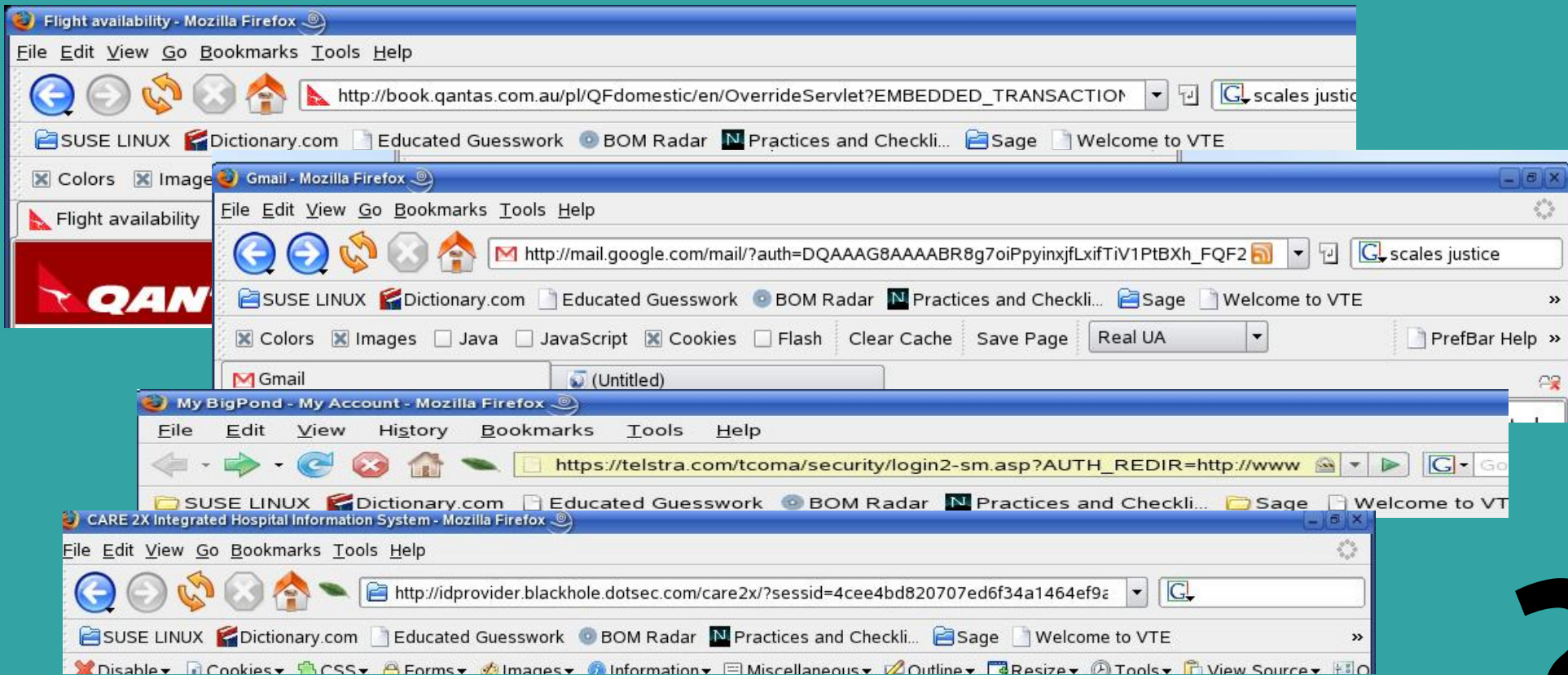
Inability of users

Force 2 - (In)Ability of users

- How many studies do we need?
 - Ask and ye shall receive (1996) UQ
 - Why can't Johnny encrypt? PGP usability study (1999)
 - Failure to Recognize Fake Internet Popup Warning Msgs (2008)
- What are we asking them to do?
 - Identify, refuse, patch, alert, disable...
- Its not going to happen!



And just for example...



Demo 2

- Its a feature, not a bug!
- Users forced to use complex applications
 - Trained in bad practices
 - Given buggy services to use
- Attacker can take advantage of both
 - Is that credit card-request supposed to be there?
 - Are those my login details on gmail?
 - Or, in this case, has my session really expired?

Force #3

Complexity of services

Force 3 - Complexity of services

- Common client platform requirements
 - Javascript, ActiveX, even Flash!
- Service complexity
 - “Rich access-control matrix”
 - “Dynamic user roles”
- Current discussions
 - Shameless marketing FUD?
 - Our experience



Complexity of services

- Applications becoming more complex
 - Underlying policies also
- Many difficulties
 - Describing and enforcing complex policies
 - Understand the consequences of an attack
- Risk and requirements-based design
 - Threat and risk assessment, modelling and testing.
 - Secure application development framework

Demo 3

- But they can't change anything, right?
 - Under-estimation of the risk

So, what does the future hold?

- Is the sky really going to fall down?
- Only two options?
 - Pack up and go home?
 - Continue as before?
- The customer is the key
 - Will they accept liability tricks?
 - Will they accept multiple high-profile failings?
 - Then where will they seek shelter?



And that's the opportunity!

- Defer the apocalypse! Third option found!
- The sky won't fall
 - But chunks of the status quo might!
 - No slackening. No more-of-the-same
- Opportunity for the proactive and prepared
 - And avoid hoping for silver bullets
 - Business modelling, SSDLC, holistic approach
- Answers are there to be found

