OWASP
The Open Web Application Security Project

Defending Desktop Applications: Mitigating in the Dark

AppSec 2013

Jon McCoy
www.DigitalBodyGuard.com

OWASP
The Open Web Application Security Project

Defending Desktop Applications: Mitigating in the Dark

McCoy

www.DigitalBodyGuard.com

Defending Desktop Applications: Mitigating in the Dark

Jon McCoy

www.DigitalBodyGuard.com

- Training
- Malware Analysis
- Code Review
- Application Penetration Testing
- Custom Security Modification
- Research

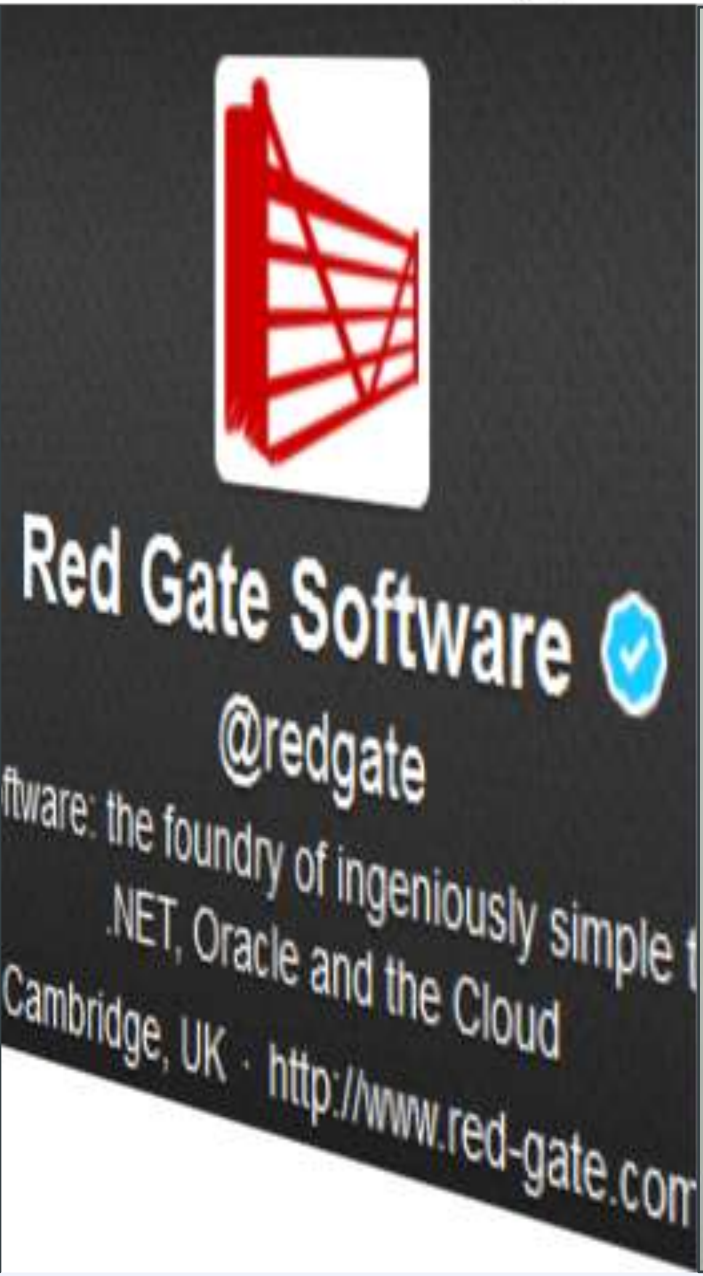
THIS TALK

- An attack what is it
- Who and what is attacked
- How does the attack start
- What do people do in response
- ...

Licensing

Intellectual Property

Security



Red Gate Software

@redgate

ftware: the foundry of ingeniously simple t
.NET, Oracle and the Cloud

Cambridge, UK · http://www.red-gate.com

Licensing

Red Gate Software

@redgate

ftware: the foundry of ingeniously simple t
.NET, Oracle and the Cloud

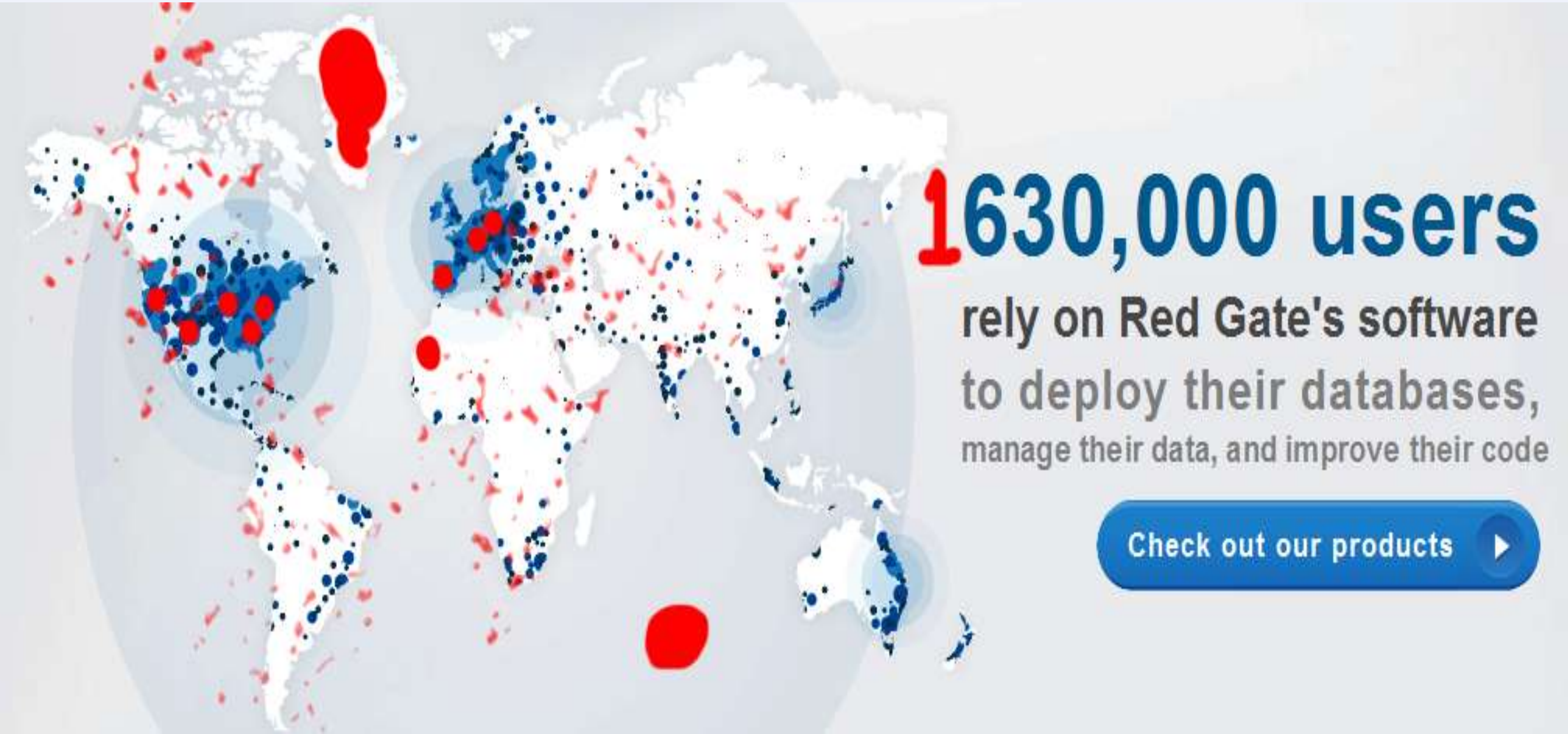
Cambridge, UK · http://www.red-gate.com

630,000 users

rely on Red Gate's software

to deploy their databases,

manage their data, and improve their code



1630,000 users

rely on Red Gate's software

to deploy their databases,

manage their data, and improve their code

- Who attacked
- What did they do
- How did they attack

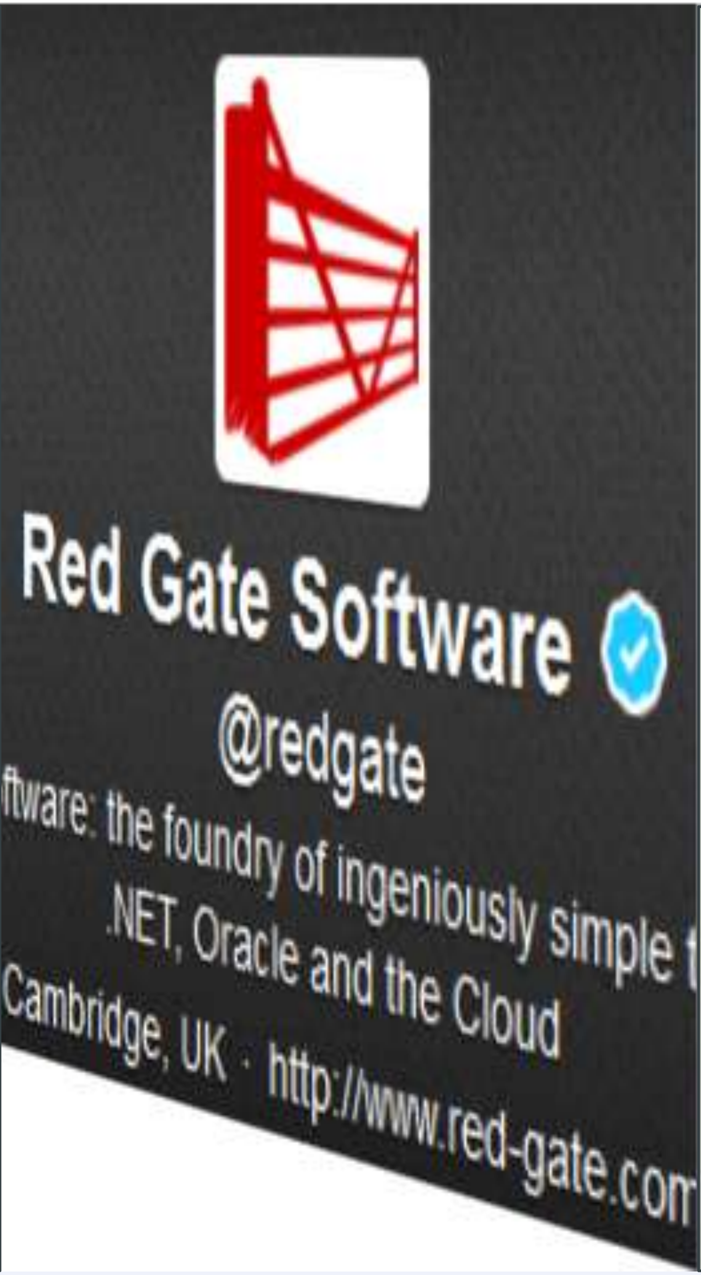
- How do we respond
- What should be done
- Who should be working on it

HACKER OR ATTACKER

- Who should have stopped this
- What did they/we do wrong
- How do we change

- How do we move forward
- What is critical for security
- Who will implament security

Intellectual Property



Red Gate Software

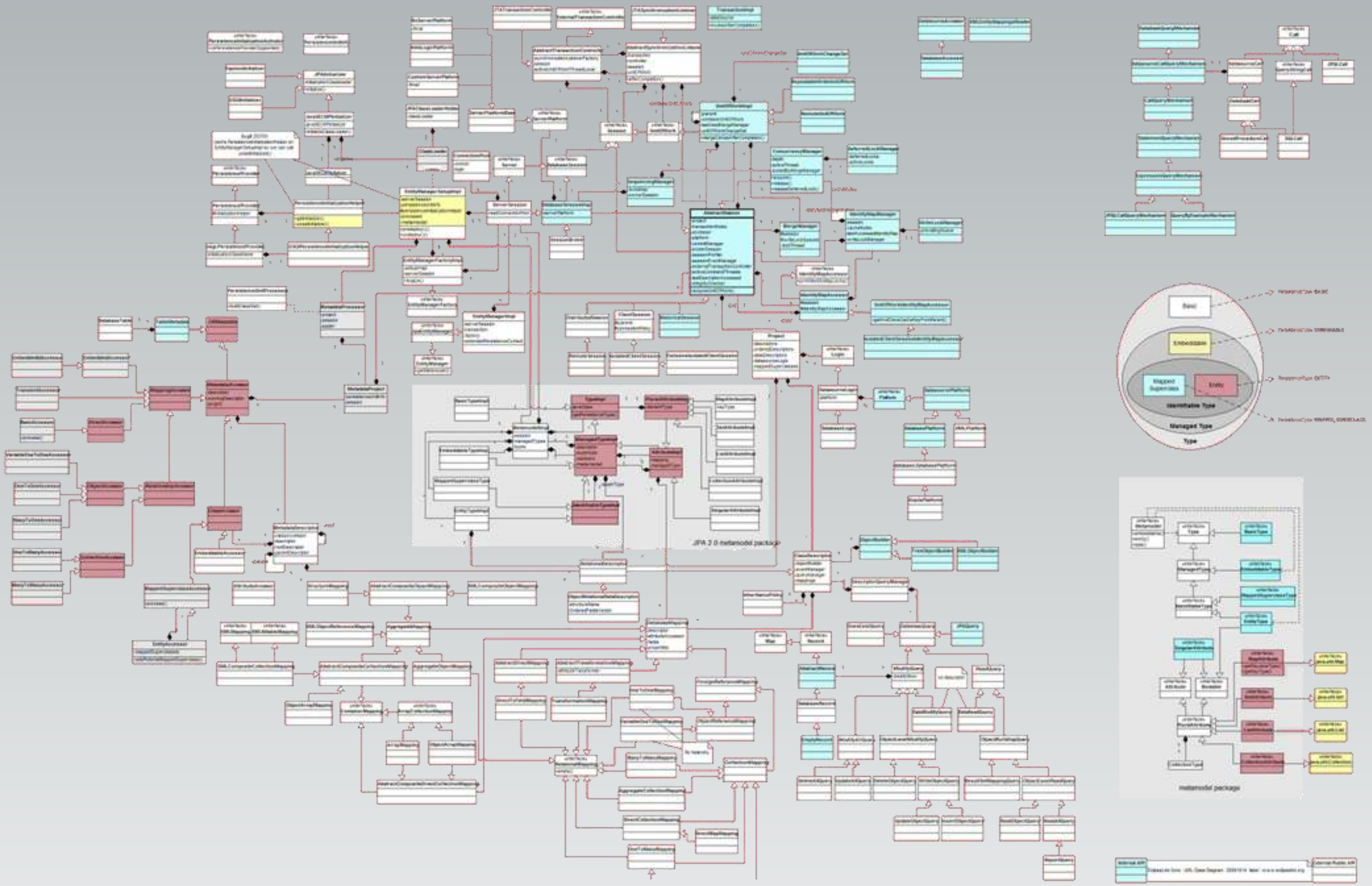
@redgate

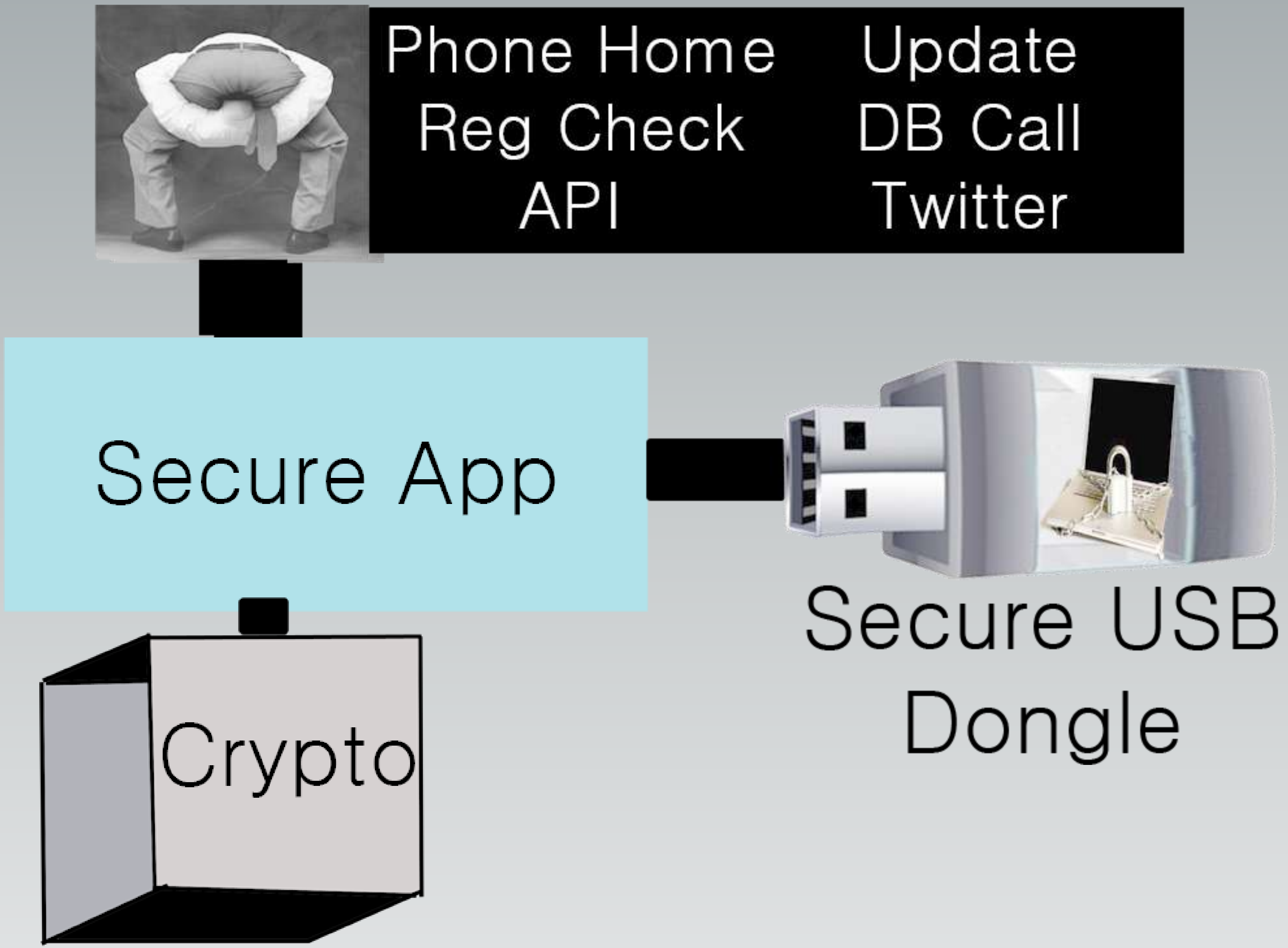
ftware: the foundry of ingeniously simple t

.NET, Oracle and the Cloud

Cambridge, UK · http://www.red-gate.com

PRODUCT DEV


JPA 2.0 metamodel package
Basic
Embeddable
Mapped Superclass
Entity
Identifiable Type
Managed Type
Type
metamodel package



Phone Home Update

Reg Check DB Call

API Twitter

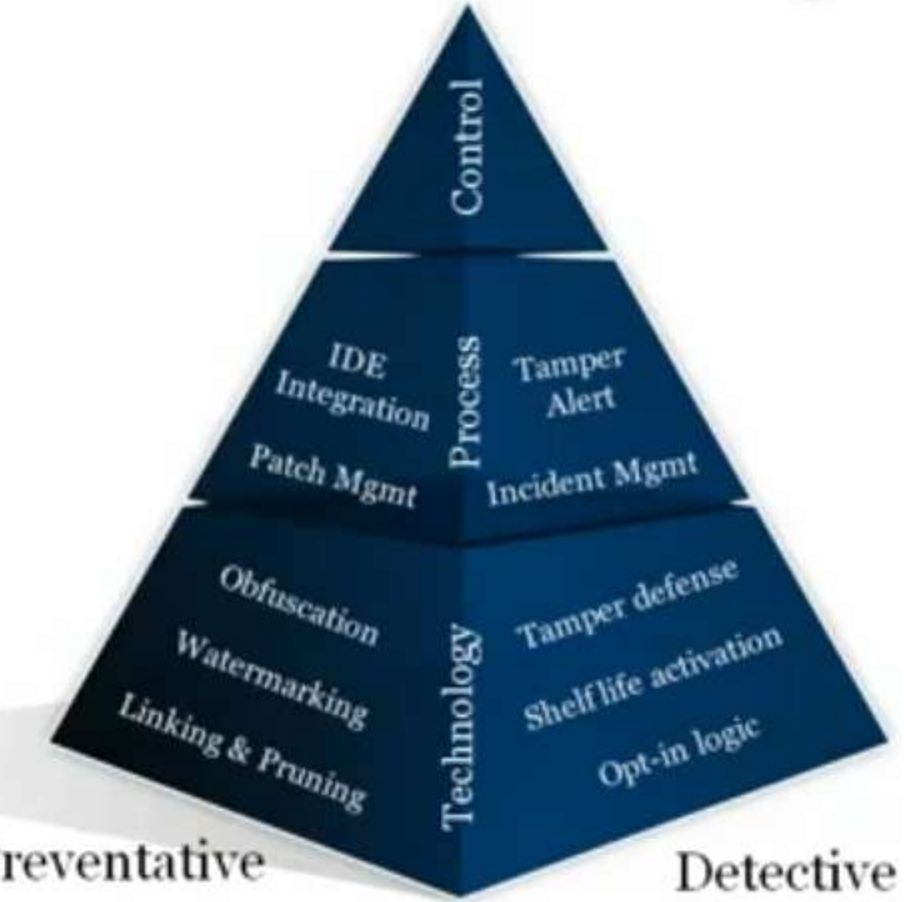
Secure App

Secure USB Dongle

Crypto

Application hardening

Effective Risk Mitigation



Phone Home
Reg Check
API

Update
DB Call
Twitter

Secure USB Dongle

PROTECTION ON DISK

0bfu$ca7ed

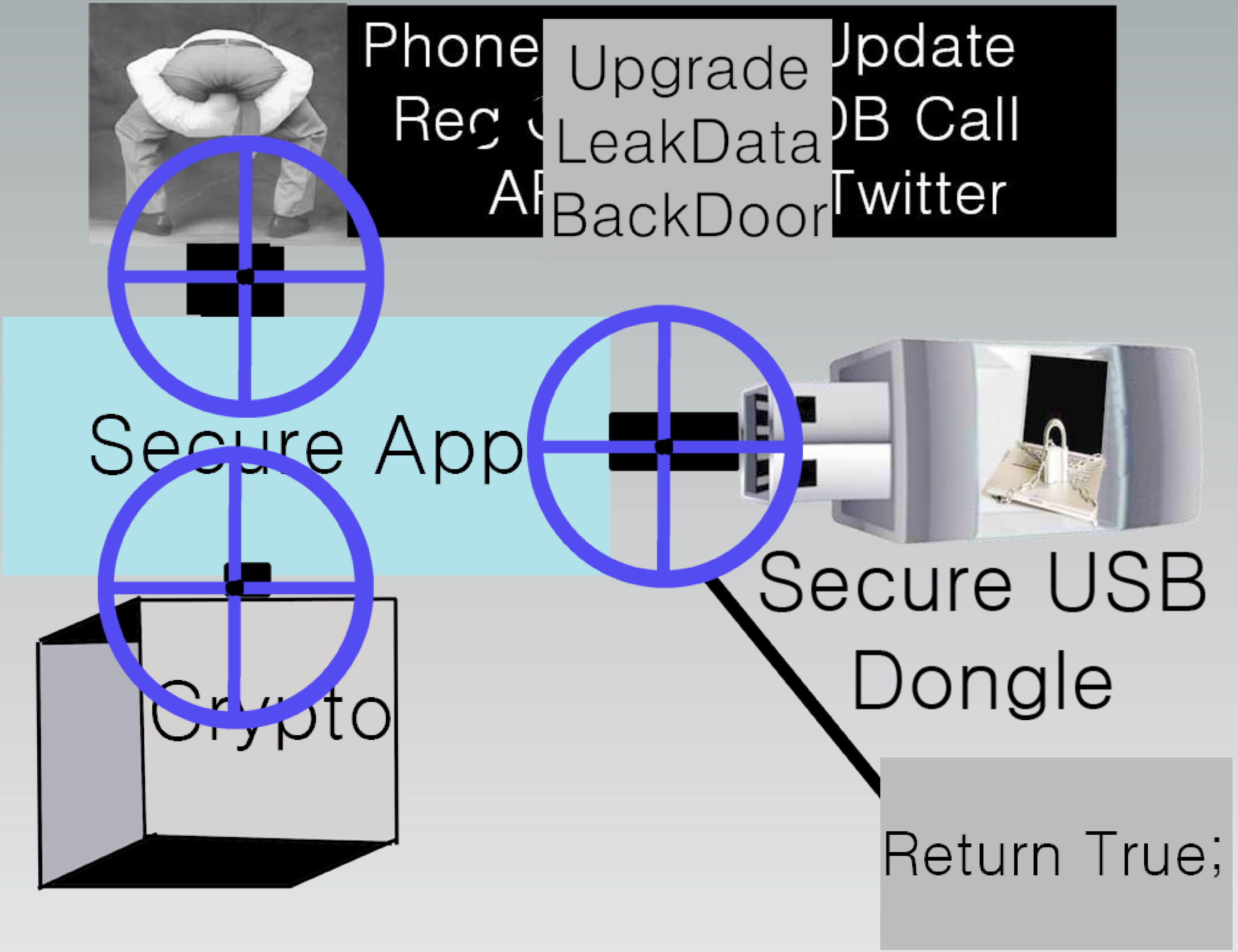
Security

Red Gate Software
@redgate
ftware: the foundry of ingeniously simple t
.NET, Oracle and the Cloud
Cambridge, UK · http://www.red-gate.com

Phone Home
Reg Check
API

Update
DB Call
Twitter

Secure USB Dongle



Phone Update

Req DB Call

AP Twitter

Upgrade

LeakData

BackDoor

Secure App

Secure USB Dongle

Crypto

Return True;

Phone Home
Reg Check
API

Update
DB Call
Twitter

Secure USB Dongle

Crypto

FIN

MORE INFO@:
DigitalBodyGuard.com

FIN = 1