

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

...AND THEN ONE GOT CALLED TODAY, IT'S ALL OVER THE NEWS. "TEENAGER
ARRESTED IN COMPUTER CRIME SCANDAL", "HACKER ARRESTED AFTER BANK TELLERING
...THEY'RE ALL ALIKE...
...I AM A HACKER, ENTER MY WORLD...
...MINE IS A WORLD THAT BEGINS WITH SCHOOL... I'M SMARTER THAN MOST OF
THE OTHER KIDS... I DRAFT THE TEACHERS BORES ME...
DAMN UNDERSTANDING...
...I'M IN JUNIOR HIGH SCHOOL... I COULDN'T...
FOR THE FIFTEEN...
SMITH, I DIDN'T SHOW MY WORK, I DID IT IN MY HEAD...
DAMN KID, PROBABLY COPIED IT. THEY'RE ALL ALIKE.

...I MADE A DISCOVERY TODAY, I FOUND A COMPUTER...
COOL... IT DOES WHAT I WANT IT TO, IF IT MAKES A MISTAKE BECAUSE
SCREAMED IT UP, NOT BECAUSE IT DOESN'T LIKE ME...
OR FEELS THREATENED BY ME...
OR THINKS I'M A SMART ASS...
OR DOESN'T LIKE TEACHING AND...
DAMN KID, ALL HE DOES IS PLAY GAM...

...AND THEN IT HAPPENED... A DOOR OPENED...
THE PHONE LINE HEARDIN' THROUGH AN ADDICT'S...
SENT OUT, A REFUGE FROM THE DAY-TO-DAY INCOMPLETE...
FOUND...
"THIS IS IT... THIS IS WHERE I BELONG..."
I KNOW EVERYONE HERE... EVEN IF I'VE NEVER MET THEM...
THEY MAY NEVER HEAR FROM THEM AGAIN... I KNOW YOU ALL...
DAMN KID, TYING UP THE PHONE LINE AGAIN, THEY'RE ALL...

...YOU SET YOUR ASS WHERE ALL ALIKE... WE'VE BEEN SPOON-
SCHOOL WHEN WE HUNGRED FOR STEAK... THE BITS OF MEAT THAT
THROUGH WE'RE PRE-CHEWED AND TASTELESS... WE'VE BEEN DOMIN-
IGNORED BY THE APATHETIC... THE FEW THAT HAD SOMETHING TO
ING PUPILS, BUT THOSE FEW ARE LIKE DROPS OF WATER IN THE...

...THIS IS OUR WORLD NOW... THE WORLD OF THE ELECTRIC
BEAUTY OF THE BAD... WE MAKE USE OF A SERVICE ALREADY
FOR WHAT COULD BE DIRT-CHEAP IF IT WASN'T RUN BY...
YOU CALL US CRIMINALS... WE EXPLORE...
AFTER KNOWLEDGE... AND YOU CALL US...
WITHOUT NATIONALITY, WITHOUT REL...
YOU BUILD ATOMIC BOMBS, YOU WAGE...
AND TRY TO MAKE US BELIEVE IT'S A...

...YES, I AM A CRIMINAL... MY CRIME...
THAT OF JUDGING PEOPLE BY WHAT THEY...
MY CRIME IS THAT OF OUTSHATING YOU...
FOR...
...I AM A HACKER, AND THIS...
BUT YOU CAN'T STOP US ALL...
...THE MENTOR...

...THIS INDIVIDUAL...
...I AM A HACKER, AND THIS...
BUT YOU CAN'T STOP US ALL...
...THE MENTOR...

...I AM A HACKER, AND THIS...
BUT YOU CAN'T STOP US ALL...
...THE MENTOR...

Jon McCoy

www.DigitalBodyGuard.com





OWASP

The Open Web Application Security Project

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



OWASP

The Open Web Application Security Project

THIS TALK

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

Intellectual Property Licensing Security



Red Gate Software 

@redgate

Software: the foundry of ingeniously simple things
for .NET, Oracle and the Cloud

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



Licensing



Red Gate Software 

@redgate

Software: the foundry of ingeniously simple tools
for .NET, Oracle and the Cloud

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





OWASP

The Open Web Application Security Project



630,000 users

rely on Red Gate's software
to deploy their databases,
manage their data, and improve their code


Check out our products





OWASP

The Open Web Application Security Project



1630,000 users
rely on Red Gate's software
to deploy their databases,
manage their data, and improve their code

[Check out our products](#)



OWASP

The Open Web Application Security Project

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

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



OWASP

The Open Web Application Security Project

HACKER OR ATTACKER





OWASP

The Open Web Application Security Project

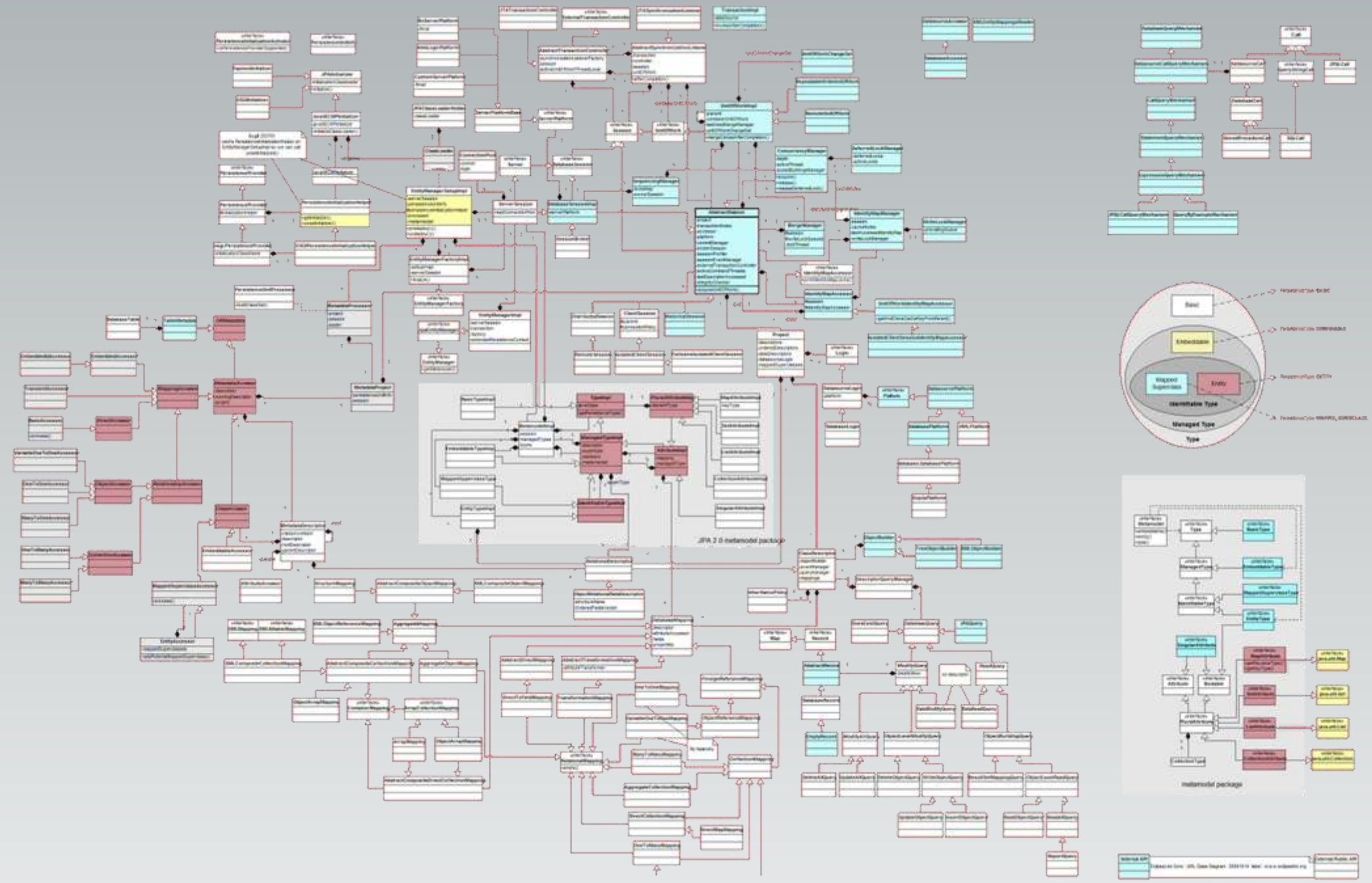
- ◆ Who should have stopped this
- ◆ What did they/we do wrong
- ◆ How do we change

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

Intellectual Property



PRODUCT DEV





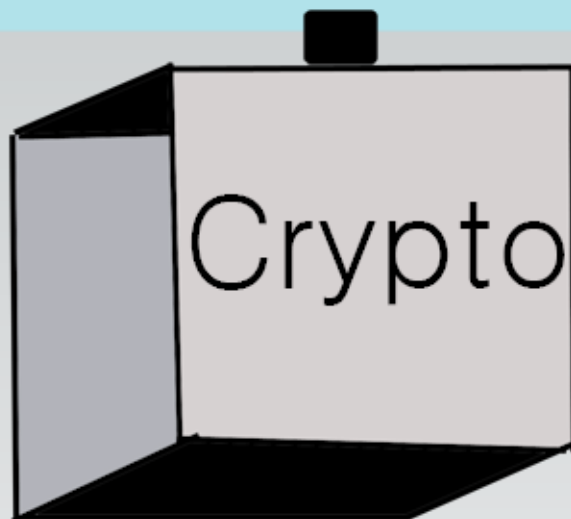
Phone Home
Reg Check
API

Update
DB Call
Twitter

Secure App



Secure USB
Dongle



Application hardening

Effective Risk Mitigation





Phone Home
Reg Check
API

Update
DB Call
Twitter



Secure USB
Dongle

PROTECTION ON DISK

Obfuscated



Security





Phone Home
Reg Check
API

Update
DB Call
Twitter



Secure USB
Dongle

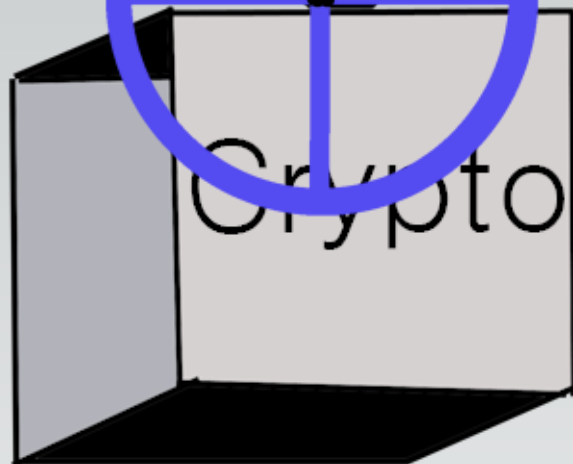


Phone Upgrade
Rec & LeakData
AF BackDoor
Update DB Call
Twitter

Secure App



Secure USB
Dongle



Return True;



Phone Home
Reg Check
API

Update
DB Call
Twitter



Secure USB
Dongle





OWASP

The Open Web Application Security Project

FIN





OWASP

The Open Web Application Security Project

MORE INFO@:

DigitalBodyGuard.com

FIN = 1

