

Defensive Exploitation

How to Pwn Your Attacker's Decision-making

Kelly Shortridge (@swagitda_)

ZeroNights 2017

A tiger with orange and black stripes is walking through a snowy, hazy environment. The tiger is looking directly at the camera with a serious expression. The background is a soft, out-of-focus white and grey, suggesting a winter or high-altitude setting.

Привет, я Келли



SecurityScorecard

A close-up photograph of a hand holding a glowing lightbulb. Inside the lightbulb, a human brain is visible, illuminated with a blue and white glow. The background is dark, and the lighting is warm and focused on the hand and lightbulb.

**Attackers are human.
Their brains have vulns.**

**Today you'll learn how to
exploit these vulns for defense**



**We'll liberate exploitation
from the clutches of the few...**

A crowd of people is shown from the chest up, with their arms raised in the air. The scene is dimly lit, with a strong red glow that highlights the silhouettes of the hands and arms against a dark background. The overall atmosphere is one of collective participation or celebration.

...into the hands of the many

A woman with dark skin and braided hair is shown from the chest up, looking upwards and to the right. Her right hand is resting under her chin, suggesting a state of deep thought or contemplation. The background is a plain, light-colored wall. The overall mood is one of intellectual pursuit and reflection.

How do humans think?

People predict their opponent's moves
by either “**thinking**” or “**learning**”

Thinking = modeling how opponents
are likely to respond

Our brains work like **volatile memory**

Learning = predicting how players
will act based on prior games / rounds

A skateboarder with dreadlocks is captured in mid-air, performing a trick. He is wearing a light-colored t-shirt and dark pants. His skateboard is positioned vertically below him, with the wheels pointing upwards. The background is a dark, clear sky. The text "Humans learn through 'error-reinforcement learning' (trial & error)" is overlaid on the image in white and teal colors.

Humans learn through
“error-reinforcement learning” (trial &
error)

“Learning rates” = how much
experiences factor into one’s decisions

Veksler & Buchler case study:
200 “security games” to test the # of
prevented attacks across 4 strategies

Fixed strategy: 10% - 25% of attacks prevented

Game Theory strategy: 50% of attacks prevented

Random strategy: 49.6% of attacks prevented

Cognitive Modelling strategy: 61% -
77% of attacks prevented



Don't be replaced by a random
SecurityStrategy™ algorithm

A photograph of two tigers in a natural, grassy environment. One tiger is on the left, leaning forward with its right paw extended towards the other tiger. The second tiger is on the right, looking towards the first. The background is a soft-focus green landscape with a body of water visible. The overall tone is natural and somewhat somber due to the muted colors.

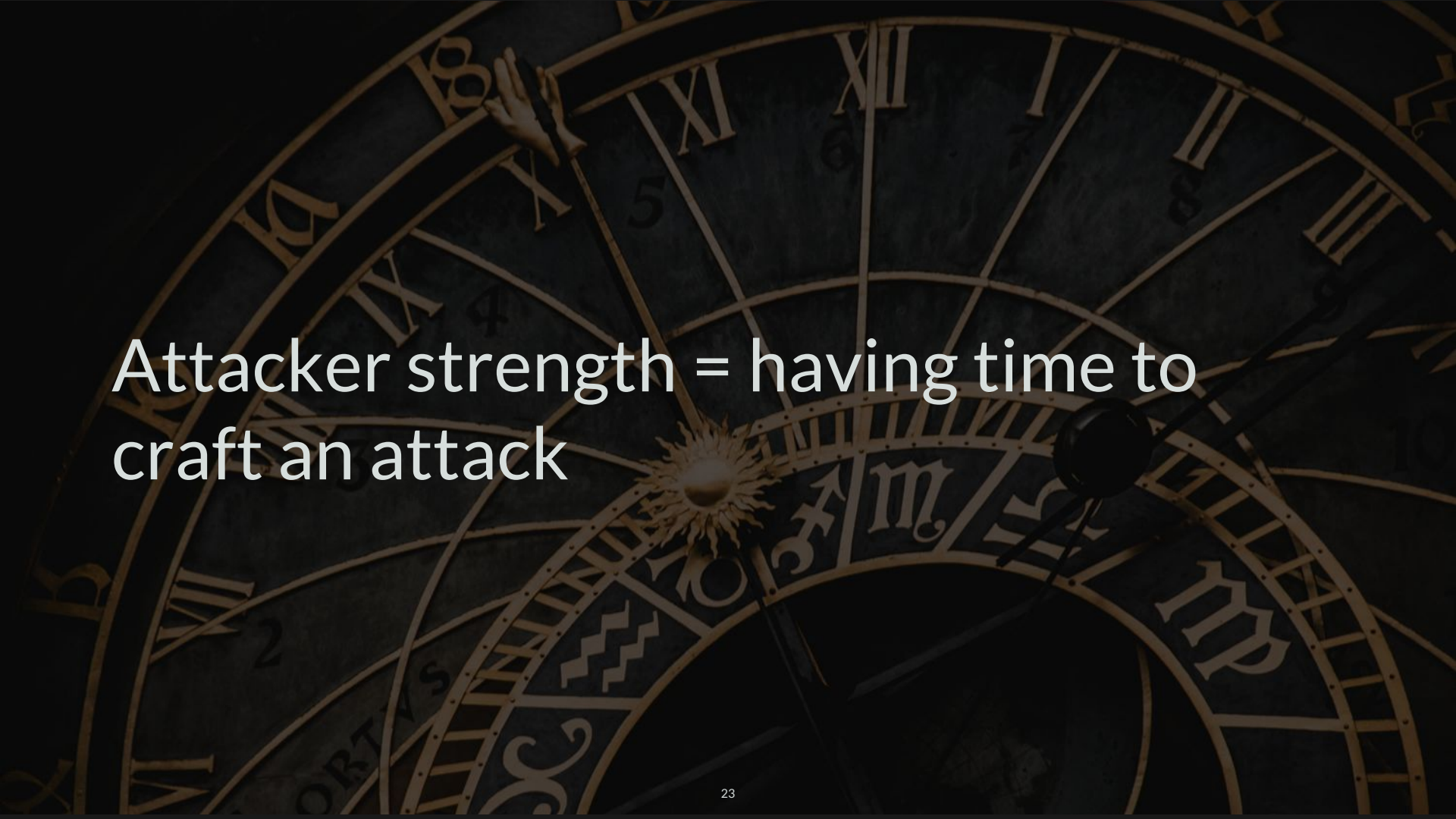
How to Pwn Attackers

A photograph of a woman's muscular back, seen from behind, wearing a black sports bra. The background is dark and out of focus, suggesting a gym environment. The lighting highlights the contours of her muscles.

Perceptual SWOT Analysis

How can strengths be weaknesses?

How can weaknesses be strengths?



Attacker strength = having time to craft an attack

A white rabbit with black ears and markings is sitting in a field of brown autumn leaves. The rabbit is looking to the right. The background is a soft-focus field of similar leaves.

Leverage that “strength” with
strategies leading down rabbit holes



Attacker strength = access to known
vulns



Confuse them with fake architecture
for uncertainty around your systems

A brown bear cub is lying on its back in a grassy field. The cub's front paws are raised towards its face, and its hind legs are also raised. The cub is looking directly at the camera with a neutral expression. The background is a dense field of green and brown grass.

Learning Exploitation

Info asymmetry exploitation:

Disrupt the attacker's learning process

Learning rate exploitation:

Introduce unreliability and pre-empt attacker moves

Exploit the fact that
you understand the local environment
better than attackers

A close-up photograph of a dog's face, likely a Border Collie, wearing a black wig, black-rimmed glasses, and a large, light-colored, bulbous nose. The dog's eyes are visible through the glasses. The background is a plain, light-colored wall with some small dark spots.

Дезинформация (disinformation)

Defenders have information their adversaries need to intercept

Hide or falsify data on the legitimate system side

Remove the attacker's **scientific method** so they can't test hypotheses



Create honeytokens that look legit & would be useful in attacker recon

Example: Create custom email rejection messages

Then, create a **honeypoc** for violation of the “Rivia Policy”

Respond to suspicious emails with,
“You’ve violated the Rivia policy 21a”



Track when the honeydoc is accessed



Маскировка (deception)

Non-determinism: different behaviors at different times

A silhouette of a quadcopter drone with a camera attached, flying against a solid brown background. The drone is positioned in the upper left quadrant of the frame, with its arms extending horizontally. The text is overlaid on the drone's body and the background.

Raise costs at the 1st step of the attack:
Reconnaissance

Make the attacker **uncertain** of your defensive profile and environment

Attackers now design malware to be VM-aware



Good: Make everything look like a malware analyst's sandbox

Better: Look like a **different** malware analyst's sandbox each time



Put wolfskins on the sheep

Mix & match superficially
sketchy-looking artifacts on normal
systems

Emulate virtual artifacts onto physical machines

<https://github.com/fr0gger/RocProtect-V1>

VMwareServices.exe

VBoxService.exe

Vmwaretray.exe

VMSvc.exe

vboxtray.exe

ollydbg.exe

wireshark.exe

fiddler.exe

\\\\.\\pipe\\cuckoo

cuckoomon.dll

dbghelp.dll

Mac addresses:

"00:0C:29", "00:1C:14",

"00:50:56", "00:05:69"

system32\drivers\VBBoxGuest.sys
system32\drivers\VBBoxMouse.sys

HKLM\SOFTWARE\Oracle\VirtualBox Guest
Additions

C:\cuckoo, C:\IDA
Program Files\Vmware

Make the IsDebuggerPresent function call always return non-zero

Create fake versions of driver objects like \\.\NTICE and \\.\SyserDbgMsg

Set KdDebuggerEnabled to 0x03

Load DLLs from AV engines using a Windows loader with a forwarder DLL

ex64.sys (Symantec)

McAVSCV.DLL (McAfee)

SAUConfigDLL.dll (Sophos)

cbk7.sys (Carbon Black)

cymemdef.dll (Cylance)

CSAgent.sys (Crowdstrike)

Deploy lightest weight hypervisor possible for added “wolfskin”

<https://github.com/asamy/ksm>

<https://github.com/ionescu007/SimpleVisor>

<https://github.com/Bareflank/hypervisor>

A woman with long dark hair is wearing a white, stylized mask that covers her eyes and nose. She is dressed in a red lace-trimmed bra and black pants. She stands in a dark, wooded area. Behind her is a large, billowing cloud of red smoke or fog. The word "Conclusion" is written in large, white, bold, sans-serif font across the center of the image.

Conclusion

**Start with a perceptive SWOT
analysis to gain perspective**

**Use info asymmetry & learning
rate exploitation to beleaguer
your adversaries**

Дезинформация и маскировка

**Worst case, random strategies
are just as good as game theory**



**Клин клином вышибают
(fight fire with fire)**



@swagitda_



/in/kellyshortridge



kelly@greywire.net

Suggested reading

- “Know Your Enemy: Applying Cognitive Modeling in the Security Domain,” Veksler, Buchler
- “Know Your Adversary: Insights for a Better Adversarial Behavioral Model,” Abbasi, et al.
- “Deterrence and Risk Preferences in Sequential Attacker–Defender Games with Continuous Efforts,” Payappalli, Zhuang, Jose
- “Improving Learning and Adaptation in Security Games by Exploiting Information Asymmetry,” He, Dai, Ning
- “Behavioral theories and the neurophysiology of reward,” Schultz
- “Evolutionary Security,” and “Measuring Security,” Dan Geer