Welcome
2017 Faculty Summit Attendees

Faculty Summit 2017
microsoftfacultysummit.com

Microsoft Research
Microsoft.com/research

Facebook
@microsoftresearch

Twitter
@MSFTResearch
#FacSumm
#EdgeofAI
What can AI learn from security

Mike Walker
Mike Walker
“What can AI learn from security”? 
1996

.o0 Phrack 49 Oo.
Volume Seven, Issue Forty-Nine
File 14 of 16
BugTraq, r00t, and Underground.Org bring you

Smashing The Stack For Fun And Profit
by Aleph One
aleph1@underground.org

2011

<table>
<thead>
<tr>
<th>Memory Corruption (19)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defeated by DEP</td>
</tr>
<tr>
<td>Defeated by ASLR</td>
</tr>
<tr>
<td>Defeated by EMET</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logic Flaws (8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Java in Internet Zone</td>
</tr>
<tr>
<td>No EXEs in PDFs</td>
</tr>
<tr>
<td>No Firefox or FoxIt Reader</td>
</tr>
</tbody>
</table>

$114B

Right: Dan Guido, Exploit Intelligence Project
Left: Aleph One, Phrack 49
The Honeymoon Effect

Bugs: Starts fast, then *slows down*

Vulnerabilities: Starts slow, then *speeds up!*

Frei, Clark, Blaze, Smith: Familiarity Breeds Contempt
No Reports of Attacks

Mandiant, APT1 Report
Golden Opportunities in AI Security

• Any software that serves as a gatekeeper to valuable IP, wealth, or life safety must consider the eventual arrival of an expert adversary

• Attack detection is not free; it requires active research & sensors

• No reports of attacks != no attacks

• Techniques to defeat security properties must be discovered & published in the open first (Fun) or be exploited (Profit)
“What can security learn from AI?”
Machine Learning versus Sensors

SandPrint:

“we can use those inherent features to detect sandboxes using supervised machine learning techniques [...] an attacker can reveal characteristics of publicly available sandboxes and use the gathered information to build a classifier that can perfectly distinguish between a user PC and an appliance”

AFL vs. djpeg

Michal Zalewski, Google, on AFL
“Security & AI”
Discussion
“What can AI learn from security”? 
“What can security learn from AI?”
“What does security look like after AI ‘happens’?”
Wrap-up and next steps

• What can AI learn from security?
• What can security learn from AI?
• What does security look like after AI happens?

New techniques, new problems to solve, new collaborations
Find someone to work with today!
Thank you