[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Human decision making in cybersecurity

Dr. Jonathan M. Spring

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2019 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-1190

Approach

Qualitative understanding of how humans reason about complex systems

Apply that reasoning structure specifically to the cyber context

Focus on forensics and incident response

- That is, figuring out what happened in the past

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Purpose

Human

- Help experts reflect on their processes
- Identify the skills and techniques we should teach new analysts and investigators

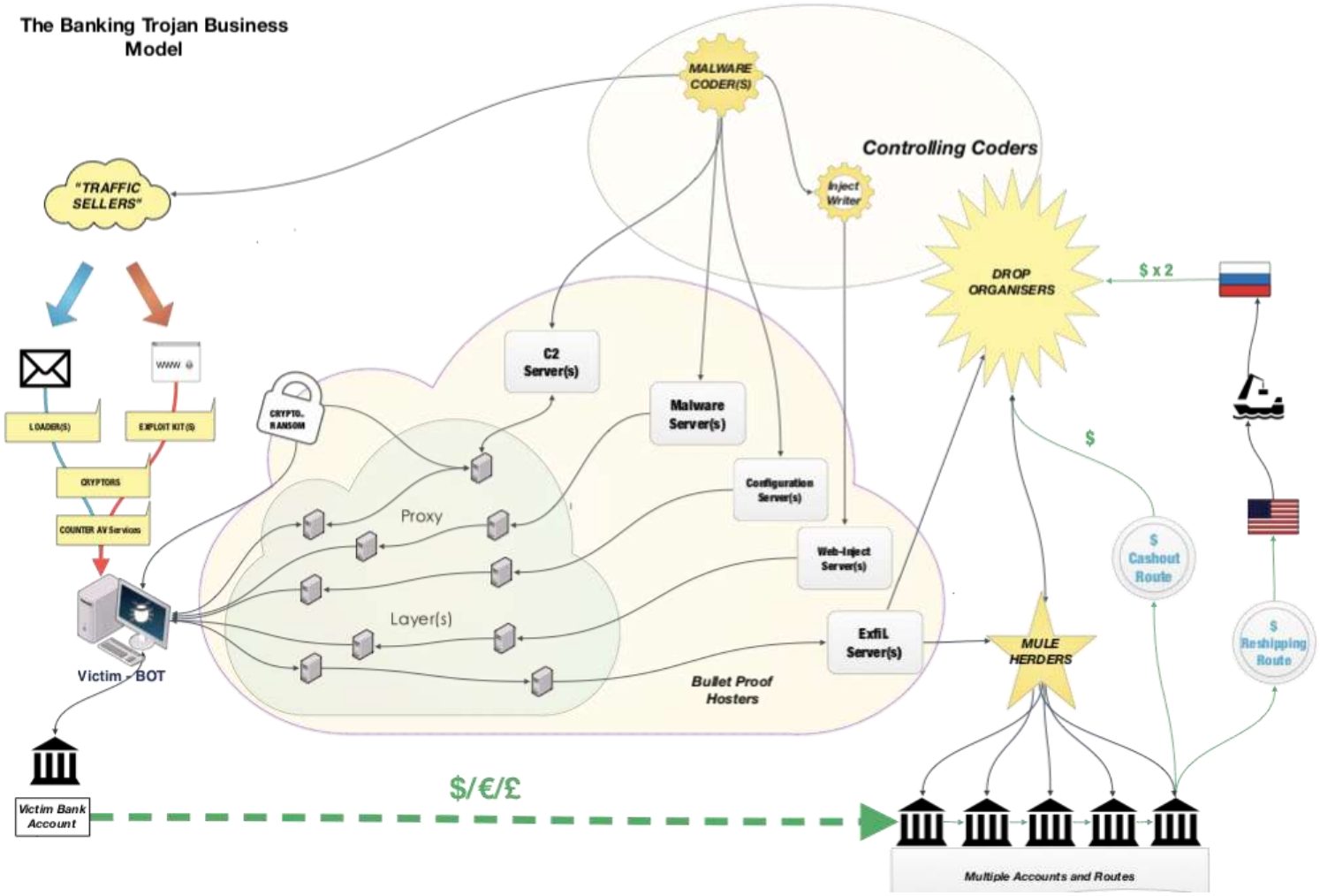
Machine

- You cannot (easily) automate what you don’t understand

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Motivating example from eCrime



Addis and Garrick, Botnet Takedowns - Our GameOver Zeus Experience. BotConf 2014. Imaged used with permission from the author.
https://www.botconf.eu/wp-content/uploads/2014/12/2014-1.2-Keynote-United-Kingdom%E2%80%99s-National-crime-agency-on-botnet-takedowns.pdf

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Scope

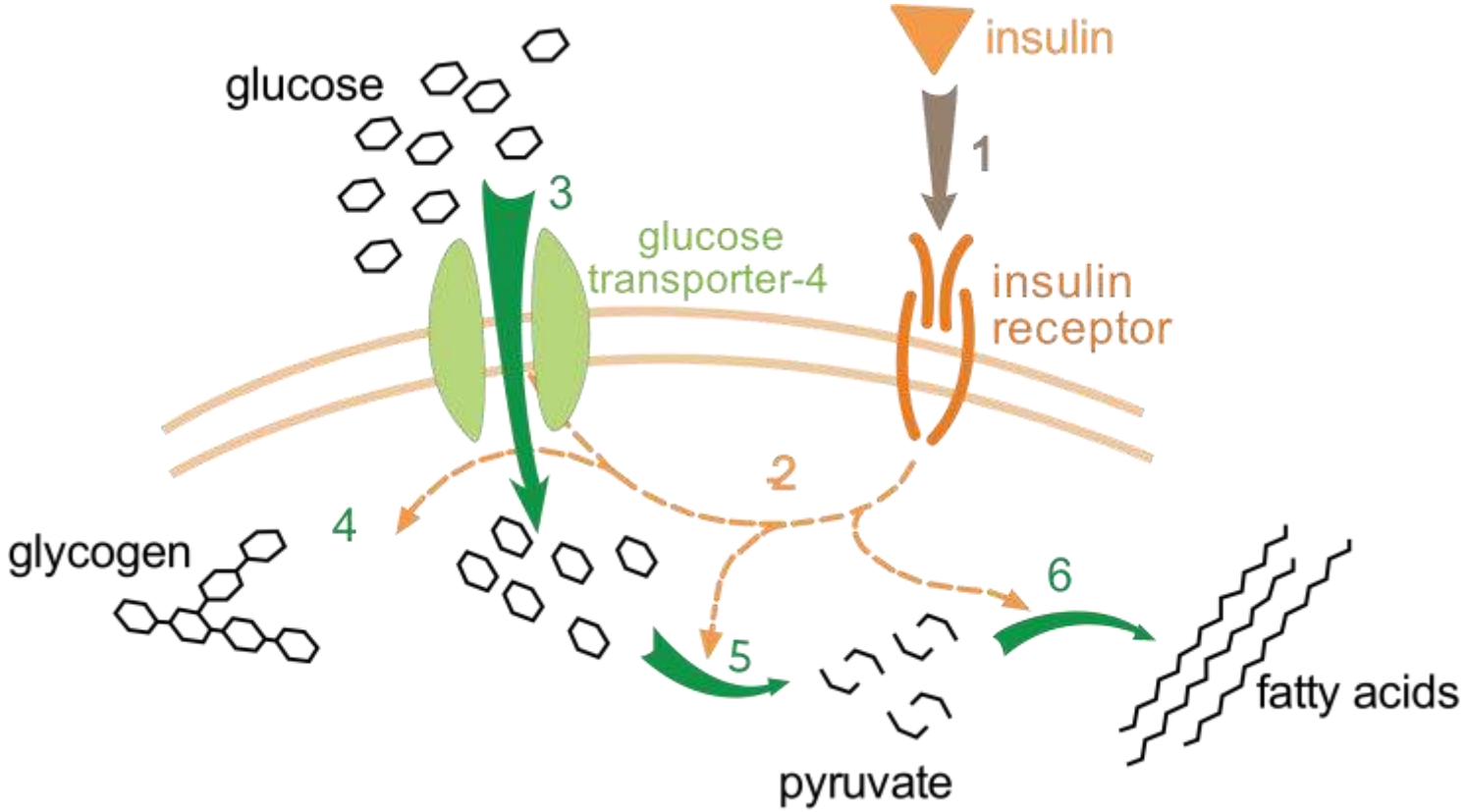
Concept goes by different names

- Incident analysis, digital forensic investigation, root cause analysis, triage, etc.
- These all mean slightly different things to different people, but for all of them we need to be able to do three things:
  - Collect evidence
  - Analyze evidence and make connections
  - Report results

© 2019 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Summary intuition

The Zeus diagram looks like life science explanations



I do not believe that is an accident

By XcepticZP at en.wikipedia - Transferred from en.wikipedia to Commons by User:Shizhao using CommonsHelper, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4436369

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Insights

To stop a botnet like GameOver Zeus, it helps to understand how it was working.

- However, mechanism of action != mechanism of cure
- Breaking stable / homeostatic / self regulating systems is hard
  - This is true of viruses and of viruses

The life science have a wide variety of methods for understanding complex, resilient systems that we can adapt

- There are some distinct challenges
- The Zeus example is one of many that shows how they are being overcome

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Goal – adequate explanations

Should contain / explain:

- Clusters of related multifield mechanism schemas

Relationships should be built, investigated, and discovered along four dimensions of variation:

- Activities and entities
- Phenomena
- Organization
- Etiology

Jonathan M Spring and Phyllis Illari (2018). 'Building General Knowledge of Mechanisms in Information Security'. In: *Philosophy & Technology*. doi: 10.1007/s13347-018-0329-z.

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Barriers

- The immediate object of study, namely software, can change behavior during or between observations
- Active adversaries respond to, and try to confound, observations
- There is often justified secrecy among friendly parties

© 2019 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Some mitigations

These are generally familiar. But let's emphasize that they are all necessary for interlocking support.

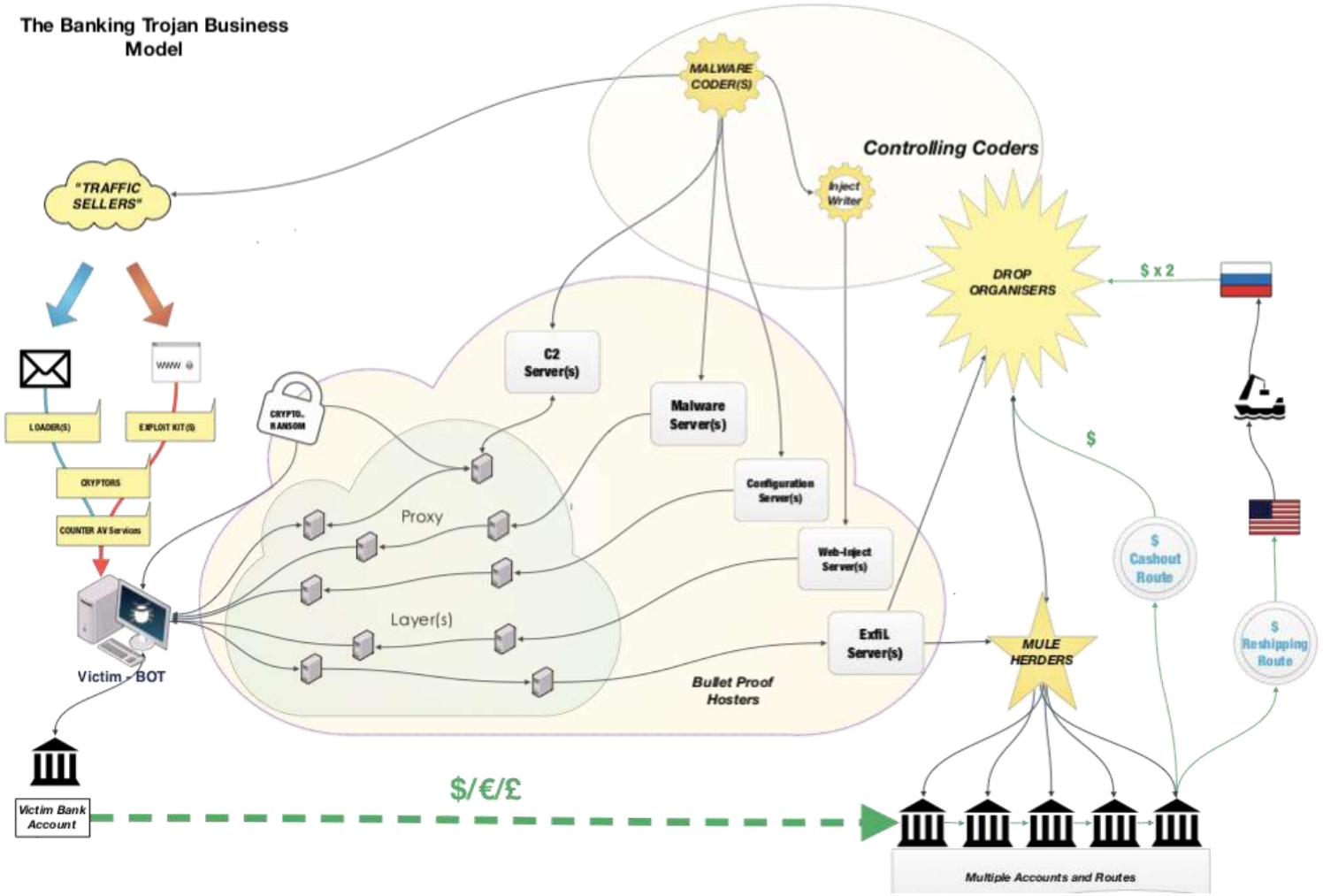
A kind of epistemic defense in depth

- Software is changeable, so analyze it from different view points
  - RE will need static decompilation, dynamic analysis, deep analysis of single executables and surveys for context
- Adversaries learn from us, but they are human
  - Understand their goal, and try to observe / measure / protect what they are actually after
- Share explanations at the appropriate level of detail
  - More general knowledge is harder to produce, but it is more stable and so safer to share

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Like this, for example



Addis and Garrick, Botnet Takedowns - Our GameOver Zeus Experience. BotConf 2014. Imaged used with permission from the author.
https://www.botconf.eu/wp-content/uploads/2014/12/2014-1.2-Keynote-United-Kingdom%E2%80%99s-National-crime-agency-on-botnet-takedowns.pdf

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Current plans

We're current apply these principles to improve how vulnerabilities are explained and prioritized

- Towards Improving CVSS https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=538368

Evidence collection can probably be automated to support this rich idea of analysis and adequate explanations

- Jonathan M Spring and David Pym (31st Oct. 2018). 'Towards Scientific Incident Response'. In: *GameSec*. LNCS 11199. Seattle, WA: Springer.

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Thanks for your time!

Questions?

jspring----cert. org

© 2019 Carnegie Mellon University
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.