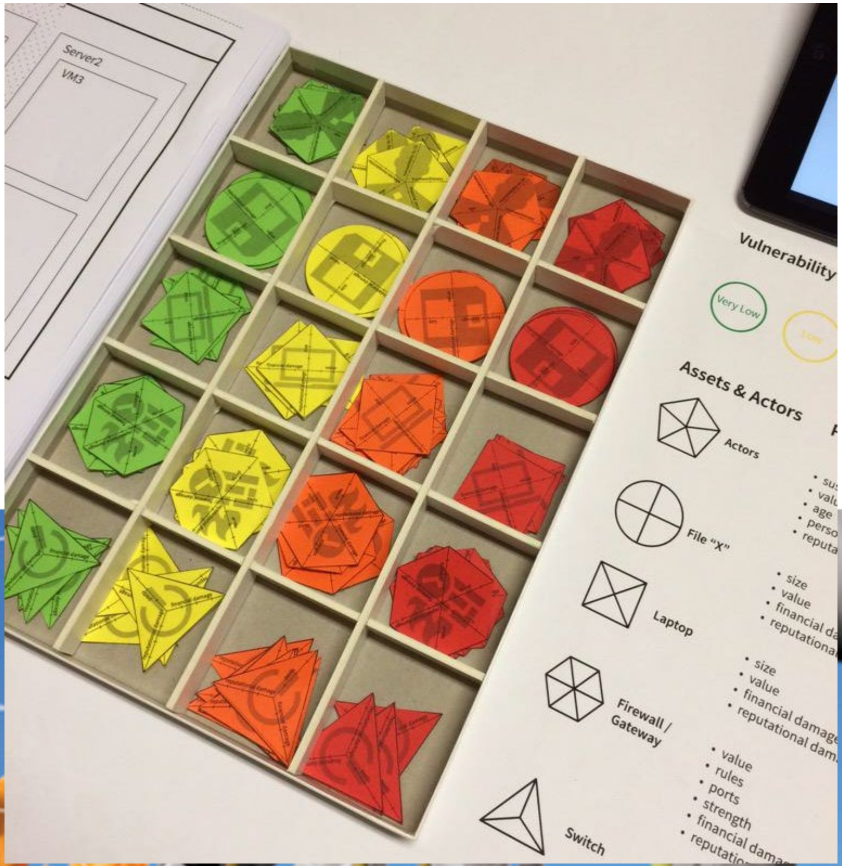
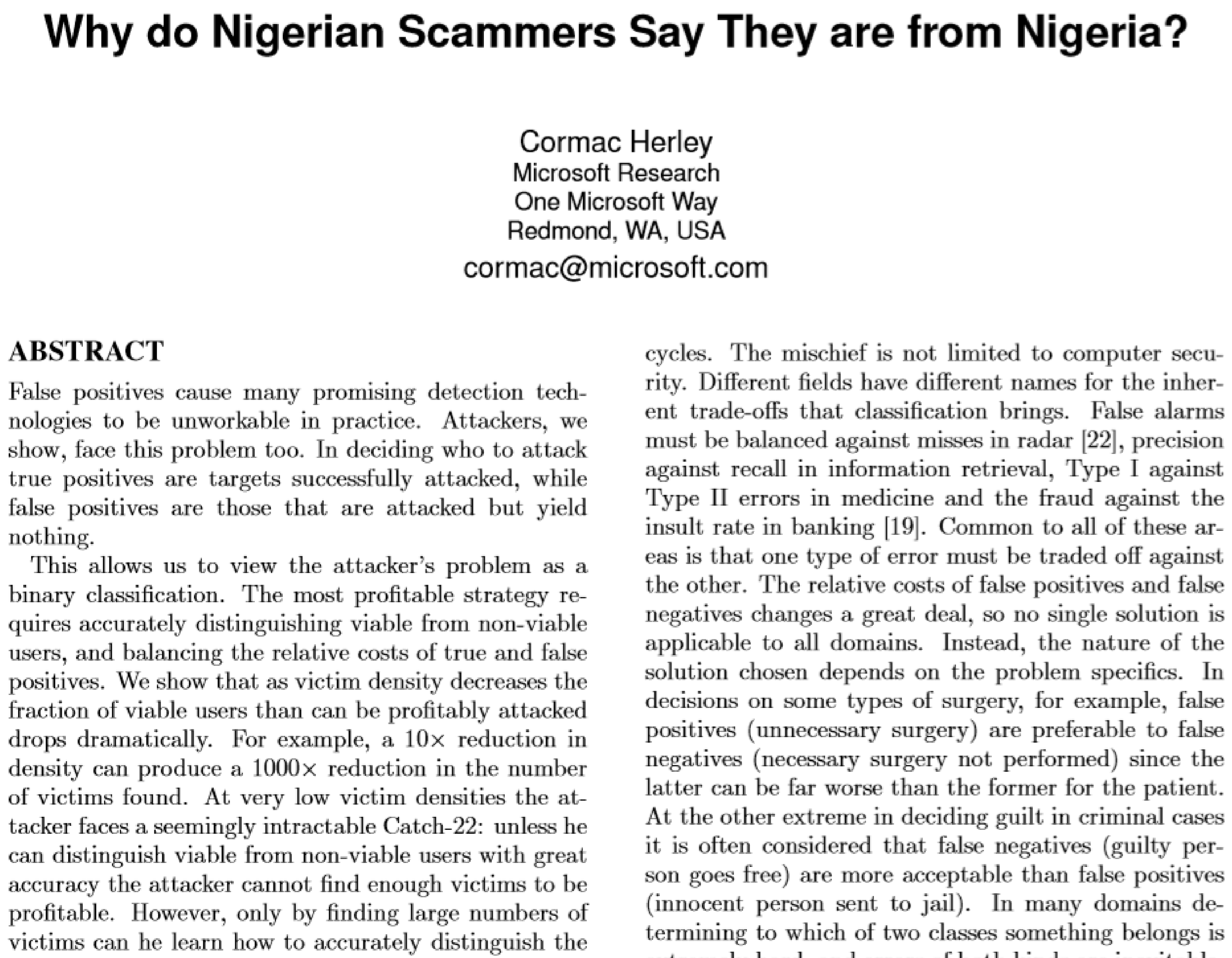
Economics of Cybersecurity

Wolter Pieters (TUD)

4TU cyber security kickoff





Why do Nigerian Scammers Say They are from Nigeria?

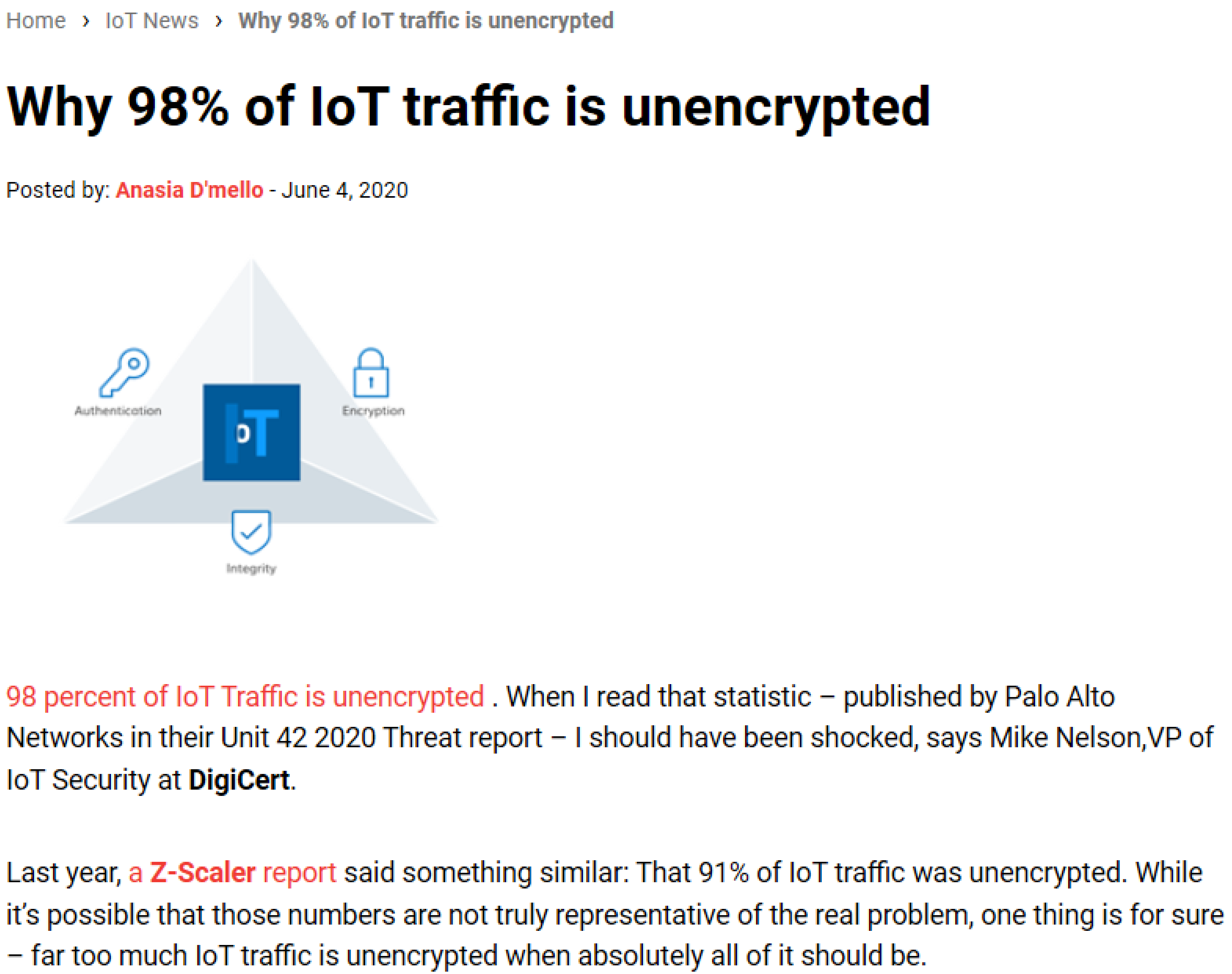
Cormac Herley
Microsoft Research
One Microsoft Way
Redmond, WA, USA
cormac@microsoft.com

ABSTRACT

False positives cause many promising detection technologies to be unworkable in practice. Attackers, we show, face this problem too. In deciding who to attack true positives are targets successfully attacked, while false positives are those that are attacked but yield nothing.

This allows us to view the attacker's problem as a binary classification. The most profitable strategy requires accurately distinguishing viable from non-viable users, and balancing the relative costs of true and false positives. We show that as victim density decreases the fraction of viable users than can be profitably attacked drops dramatically. For example, a 10× reduction in density can produce a 1000× reduction in the number of victims found. At very low victim densities the attacker faces a seemingly intractable Catch-22: unless he can distinguish viable from non-viable users with great accuracy the attacker cannot find enough victims to be profitable. However, only by finding large numbers of victims can he learn how to accurately distinguish the

cycles. The mischief is not limited to computer security. Different fields have different names for the inherent trade-offs that classification brings. False alarms must be balanced against misses in radar [22], precision against recall in information retrieval, Type I against Type II errors in medicine and the fraud against the insult rate in banking [19]. Common to all of these areas is that one type of error must be traded off against the other. The relative costs of false positives and false negatives changes a great deal, so no single solution is applicable to all domains. Instead, the nature of the solution chosen depends on the problem specifics. In decisions on some types of surgery, for example, false positives (unnecessary surgery) are preferable to false negatives (necessary surgery not performed) since the latter can be far worse than the former for the patient. At the other extreme in deciding guilt in criminal cases it is often considered that false negatives (guilty person goes free) are more acceptable than false positives (innocent person sent to jail). In many domains determining to which of two classes something belongs is



Home › IoT News › Why 98% of IoT traffic is unencrypted

Why 98% of IoT traffic is unencrypted

Posted by: Anasia D'mello - June 4, 2020

98 percent of IoT Traffic is unencrypted . When I read that statistic – published by Palo Alto Networks in their Unit 42 2020 Threat report – I should have been shocked, says Mike Nelson,VP of IoT Security at **DigiCert**.

Last year, a **Z-Scaler** report said something similar: That 91% of IoT traffic was unencrypted. While it's possible that those numbers are not truly representative of the real problem, one thing is for sure – far too much IoT traffic is unencrypted when absolutely all of it should be.

Course setup

Aim:

- provide economic concepts, measurement approaches and data analytics to make better security decisions

Contents:

- measuring cybersecurity
- security strategies and investment
- market failures and policy interventions

Format

- Period: Q1, access via TUD Brightspace

- Theory (clips/papers/quizzes)
- Assignments related to dataset (with supervisor)
  - Small group assignments (40%)
  - Large group assignment (research paper) + individual reflection (60%)

- https://studiegids.tudelft.nl/a101_displayCourse.do?course_id=54770