Betrayed by the keyboard

How what you type can give you away

Matt Wixey

Research Lead, PwC UK Cyber Security

Building a secure digital society.

pwc

www.pwc.com

Disclaimer

- This content is presented **for educational purposes only**
- What this presentation isn't…

Introduction

Matt Wixey

- Research Lead for the Cyber Security BU
- Work on the Ethical Hacking team
- PhD student at UCL
- Previously worked in LEA doing technical R&D

Why this talk?

- Based on some research I did at UCL
- Interest in side-channel attacks
- Humans have side-channels too
- Previous work on forensic linguistics
  - First degree = English Literature and Language

Agenda

- What is attribution?
- Problems
- Case Linkage Analysis
- Experimentation
- Results
- Implications
- Summary

What is attribution?

- Why would we want to do it?
- Benefits
- Types
- Approaches

What is attribution?

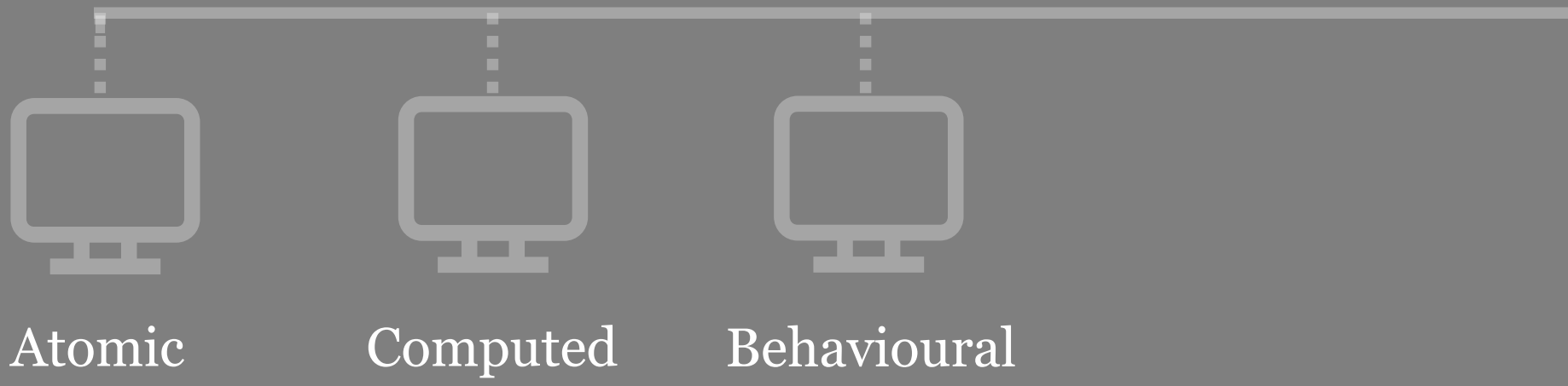
- Identifying an attacker's location?
  - Hunker et al, 2008; Wheeler and Larsen, 2003
- Identify the country or organisation behind an attack?
  - Rid and Buchanan, 2014
- "Determining who is responsible for a hostile cyber act"?
  - Mejia, 2014
- "We must find a person, not a machine"
  - Clark and Landau, 2011

Benefits of attribution

- Deterring future attacks
- Improving defences
- Interrupting and disrupting attacks (Hunker et al, 2008)
- Does attribution actually lead to deterrence? (Guitton, 2012)
- Regardless, attribution is a desirable outcome (depending on which side you're on!)

Types of attribution

- Hutchins et al, 2011:



Problems with attribution

- Hiding atomic IOCs
- Issues with computed IOCs
- Lack of tangible benefits from behavioural IOCs

Hiding atomic IOCs

- These are the most effective identifiers
- Easy to resolve (usually)
- But also easiest to spoof/anonymise/obfuscate

Issues with computed IOCs

- Changes to malware make it harder
- Other methods:
  - Correlating activity with office hours in timezones (Rid & Buchanan, 2014; CloudHopper, 2017)
  - Deanonymising developers through artefacts (Caliskan et al, 2015)
  - Similar malware capabilities (Moran & Bennett, 2013; Symantec, 2011)
  - Distinguishing humans vs bots (Filippoupolitis et al, 2014)

Mo methods, mo problems

- Less focused on individuals
- Sufficient if aim is to identify a state/sponsor
  - Challenge is then legal/procedural

Behavioural profiling

- Less attribution
- More trying to understand *who* hacks, and *why*
  - Motivation, skills, attack behaviours (Landreth, 1985)
  - Attitudes and culture (Chiesa et al, 2008; Watters et al, 2012)
  - Psychological (Shaw et al, 1998)

Attack profiling

- Humans vs bots
  - Filippoupolitis et al, 2014: Skill, education, typing speed, mistakes, etc
- Skill level
  - Salles-Loustau et al, 2011: SSH honeypot. Stealth, enumeration, malware familiarity, protection of target
- Attacker behaviour
  - Ramsbrock et al, 2007: Specific actions undertaken

The problem

- Profiling attackers is interesting
- Next logical step is *comparison*
  - To what extent is an attacker's profile similar to another's?
- Not really explored

Case Linkage Analysis

- The idea
- Discovering case linkage analysis
- Benefits of linking offences
- What case linkage analysis is (and isn’t)
- Methodology
- Example
- Exceptions

The idea

- I had an idea (rare occurrence - to be celebrated)
- Lurking in OSCP labs a few years ago
- Discussing attack techniques, commands, methodologies
  - Casual observation 1: everyone has their own way of doing things
  - Casual observation 2: this way of doing things rarely changes

Science!

- This seems obvious
- My first degree was English Lit
  - Could pretty much make it up as you went along
- Apparently, in science, you have to *prove* stuff
  - Can't just write "this seems obvious"
  - Science is hard ☹

Discovering case linkage analysis

- How could I empirically test this?
- Came across “Case Linkage Analysis”
- Methodology used in crime science literature
- Designed to *link* separate crimes to common offenders
- Based on behavioural aspects (Woodhams & Grant, 2006)

Benefits of linking offences

- Can attribute previously unsolved crimes
- Can investigate offences under one grouping – focused resources
- Useful evidentially
- Database of offences grows = better chance of success
- A minority of offenders commit the majority of crimes (?)
  - Not necessarily true of crime generally
  - But more accurate with specialist crimes

Benefits of linking offences

- Best method for linking: physical evidence (DNA, fingerprints, etc)
- Highly accurate, ***but:***
  - May be absent or inconclusive (Grubin et al, 1997)
  - Does not really apply to cyber attacks
  - Closest approximation is forensic artefacts, but these are not always unique
  - Time-consuming and expensive (Craik and Patrick, 1994)

What case linkage analysis is

- Uses behavioural evidence
  - Things the offender does during the commission of an offence
- Classify granular crime behaviours into domains
- Create linked and unlinked pairs of offences
- Compare with behaviours in other offences
- Determine degree of similarity

What case linkage analysis isn't

- It's not offender profiling
- Offender profiling makes inferences about the offender
- Based on assumption of consistency between criminal and everyday behaviour (Canter, 2000)
  - *Based on this behaviour, I infer that the perpetrator is a balding but charismatic researcher from the UK*

What case linkage analysis isn't

- CLA: statistical inferences about the similarity of 2 or more offences, based on common behaviours
  - *Crime A, perpetrated by Matt "Charismatic But Balding" Wixey, has several features in common with Crime B*
  - *Therefore, Wixey may have also committed Crime B*

Case linkage analysis in context

- Two key assumptions
- **Behavioural consistency**
  - Offenders display similar offending behaviours across crimes
- **Behavioural distinctiveness**
  - The way an offender commits crimes is characteristic of that offender
  - And distinguishable from the style of other offenders (Canter, 1995)

Case linkage analysis in context

- Both assumptions must be present
- Otherwise CLA is unlikely to be useful
- e.g. homicide: dumping a body in a remote location is consistent for many offenders
- But not distinctive

Case linkage analysis in context

- Individuals have stable, distinctive responses (Shoda et al, 1994)
- Cognitive-affective personality system (CAPS)
  - Mischel & Shoda, 1995; Mischel, 1999
  - System of goals, expectations, beliefs, plans, strategies, memories
- CAPS is consistent yet distinctive (Zayas et al, 2002)

Case linkage analysis in context

- Assumptions of stability/distinctiveness made in other fields
- Forensic linguistics
  - Word and sentence length; slang; typos; errors; syntax; idiolect; article frequency; syllable count; punctuation; hapax legomena; sentence length; stylistics
  - Language is socially acquired, continually – so may change
- Some biometrics
  - Typing speed; typos; typing habits

Case linkage analysis – does it work?

- Consensus: yes, in most cases
- Observed variance significantly smaller in linked crimes
  - Grubin et al, 1997; Mokros & Alison, 2002
- Significant evidence for cross-situational consistency
  - Both criminal and non-criminal behaviours (Tonkin et al, 2008)

Methodology

- Separate behaviours into domains
- Calculate similarity coefficient
- Input into logistic regression model
- Determine optimal combination of domains
- Receiver Operating Characteristic (ROC) curves

Methodology

- Lots of stats stuff
- I hate stats. I am bad at stats.
- Will try and explain this with a worked example
- None of that “left as an exercise for the reader” nonsense

Example

- Two burglaries, A and B
- We want to find out if the same offender did both
- Define a **dichotomous dependent variable**
  - This is a Y/N question, and we're trying to 'predict' the answer
  - And find out what variables contribute more
  - "Are these two crimes linked?"

Example

- Take granular behaviours and put them into domains
  - e.g. *Entry behaviours* = method of entry; tools used; time of day; etc
  - *Property behaviours* = property taken; property damaged; and so on
- These are our **independent variables**
- Make these **dichotomous** by turning into yes/no questions
  - e.g. *Entry behaviours:* "was a screwdriver used? Was a crowbar used? Was a window open? Were the occupants home?" etc

Example

- Then apply a **similarity coefficient**
  - Index of similarity
  - **Jaccard's** is coarse, but the measure of choice (Tonkin et al, 2008)
  - x = count of behaviours present in both
  - y = count of behaviours present in A but not in B
  - z = inverse of y

$$J = \frac{x}{(x + y + z)}$$

Example

- 1 = perfect similarity
- 0 = perfect dissimilarity
- 1 coefficient per domain
- Ignores joint non-occurrences
  - This is a concern when dealing with police data
  - Something may have been present, but not recorded
  - Less of a concern in this case

Example

- Each coefficient into direct logistic regression model
- Predictive analysis
- “To what extent does a given factor contribute to an outcome?”
  - e.g. “to what extent does being a smoker contribute to the risk of having a heart attack?”
  - Or “does similarity in the *entry behaviours* domain predict whether or not the two burglaries are linked?”

Example

- Logistic regression tells us:
  - Whether a variable is positively or negatively correlated with the outcome
  - How well a given variable fits with the data
  - The amount of variance that a given variable explains
  - A p-value (probability of seeing this result if the null hypothesis is true)
- Run for each domain

Example

- Then forward stepwise logistic regression
  - Start with one domain
  - Add a domain at each step
  - If this contributes to the model's predictive power, keep it
  - Else discard it
- Determines optimal combination of domains

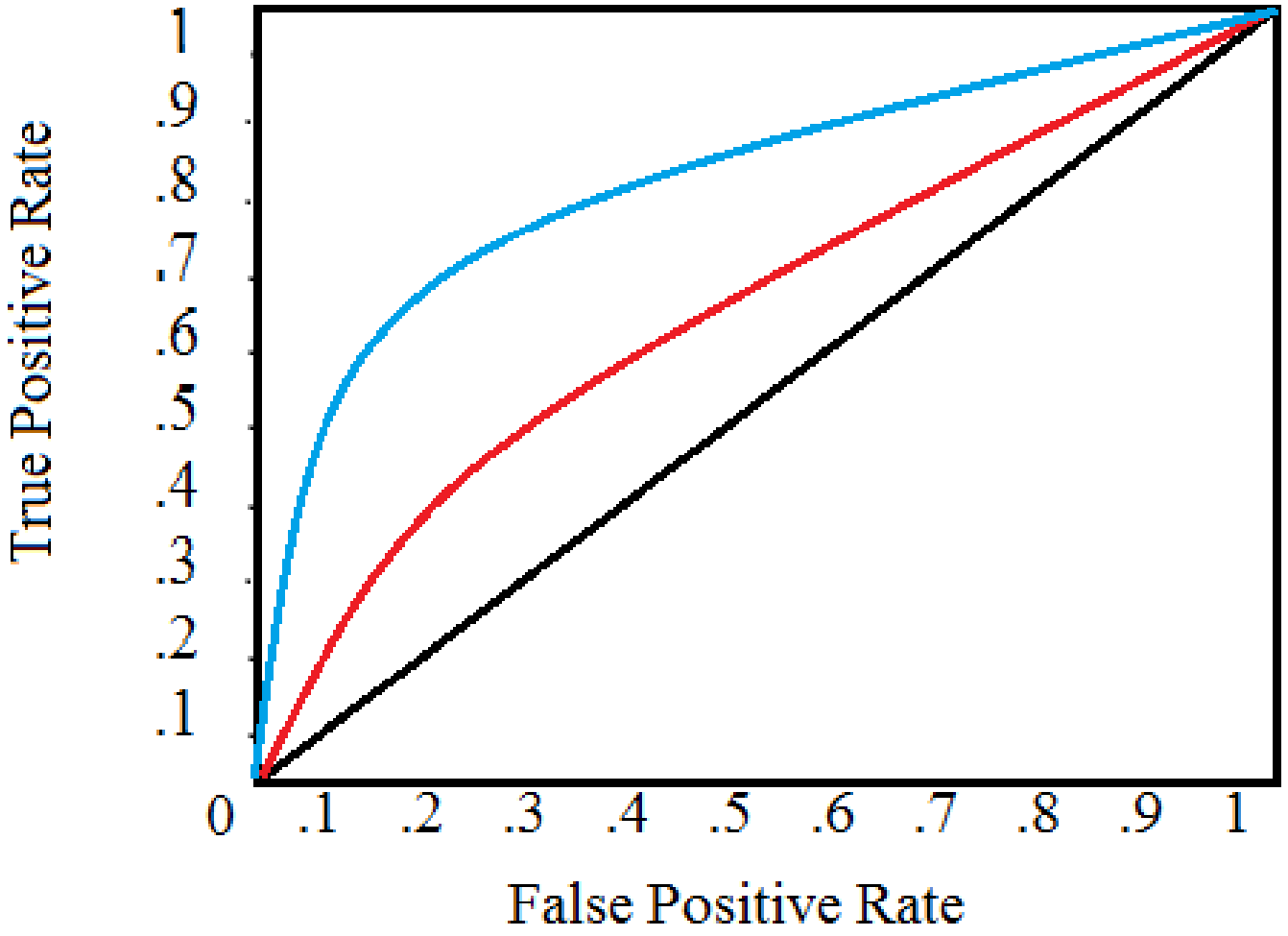
Example

- Regression results into ROC curves
- Graphical representation
  - ***x*** (probability of false positive) against ***y*** (probability of true positive)
- More reliable measure of predictive accuracy
- Based on area under the curve (AUC)

Example

- Overcomes statistical issue of using pairs from same sample (Tonkin et al, 2008)
- No reliance on arbitrary thresholds (Santtila et al, 2005)
- Measure of overall predictive accuracy (Swets, 1988)

Example



- Diagonal: no better than chance
- The higher the AUC value, the greater the predictive accuracy
- **0.5 – 0.7 = low**
- **0.7 – 0.9 = good**
- **0.9 – 1.0 = high**
- Swets, 1988

http://www.statisticshowto.com/wp-content/uploads/2016/08/ROC-curve.png

Exceptions

- Some offences are less suitable, e.g. homicide
  - Bateman & Salfati, 2007; Harbort & Mokros, 2001; Sorochinski & Salfati, 2010
- Some offenders show more distinctiveness than others
  - Bouhana et al, 2016
- Some behaviours less consistent, e.g. property stolen in burglaries
  - Bennell & Canter, 2002; Bennell & Jones, 2005

Exceptions

- MO is a learned behaviour, and offenders develop
  - Pervin, 2002; Douglas & Munn, 1992
- Offenders will change behaviours in response to events
  - Donald & Canter, 2002
- Behaviours under offender's control more likely to be stable
  - Furr & Funder, 2004; Hettema & Hol, 1998
- So offences involving victim interaction may differ
  - e.g. whether victim fights back / runs / shouts for help, etc

Exceptions

- Most research only applied to solved crimes
  - Woodhams & Labuschagne, 2012
- Relatively small samples
- Only serial offences
  - Slater et al, 2015

Experimentation

- Concept
- Research design
- Hypothesis
- Analysis
- Results

Concept

- Could CLA be applied to network intrusions?
  - Specifically, where attacker has code execution
  - Has never been done before
- Take granular behaviours (keystrokes, commands, etc)
- Apply CLA methodology

Research design

- Common approach historically: use police reports
- Can be inaccurate and/or incomplete
- Victim accounts may be inaccurate
  - Alison et al, 2001; Canter & Alison, 2003
- Crimes are often traumatic
- Traumatic experiences can distort memories
  - Freyd, 1996; Halligan et al, 2003

Research design

- Crime reports unlikely to be granular enough
- Previous studies on attacker profiling used simulations
- Honeypot?
  - Needed ground truth, as CLA previously untested on this offence type
  - Same IP addresses do not guarantee same individual at keyboard
  - Need to also distinguish between bots and humans
  - Honeypots can be fingerprinted
  - Attackers may deliberately change approach

Research design

- Modified open source Python SSH keylogger (strace)
  - https://github.com/NetSPI/skl
- Two VMs, exposed on the internet (SSH)
- One account per user per box
- Deliberate privesc vulnerabilities
- Plus fake data to exfiltrate

Research design

- Obtained participants
  - 10x pentesters / students / amateur enthusiasts
- Asked to SSH into both machines and try to:
  - Get root
  - Steal data
  - Cover tracks
  - Poke around
- Meanwhile, I recorded all keystrokes on each VM

Hypothesis

Cyber attackers will exhibit consistent and distinctive behaviours whilst executing commands on compromised hosts, which will provide a statistically significant basis for distinguishing between linked and unlinked attack pairs.

Analysis

- Split into behavioural domains, 40 behaviours each:
  - Navigation – moving through filesystem
  - Enumeration
  - Exploitation – privesc and exfil attempts
- Also coded for 3 metadata variables:
  - Number of ms between each keystroke
  - Number of ms between each command
  - Number of backspaces (as percentage of all keystrokes)

Metadata variables

- Non-dichotomous
- Used in other CLA work, in addition to behavioural domains
  - Intercrime distance (Bennell & Canter, 2002)
  - Temporal proximity (Tonkin et al, 2008)
- Filippoupolitis et al, 2014: commands typed per second
  - Problematic: length of command, time to complete, and time spent interpreting or manipulating output

Example behaviours

pwd

cd /

cd ../../

cd ..

ls /remote/dir

ls -al

cd ../

cd /../

rm

cd /remote/dir

ls -la

ls -la |grep

Ctrl+D

ls with wildcards

date

exclamation commands

ls -al /remote/dir

man

which

tab autocomplete

pipe errors to dev null

cd../[dir]

cat/etc/passwd

cd .

cd/[dir]

cd..

ls -a

ls [dir] -al

clear

cd -R

cd -r

ls -R

ls -ahlr

cat /remote/file

find exec

find /usr

grep -i

locate

find / -name

less

python escape shell

Uses FTP for exfil

kill

sync

Used exploit suggester

/bin/sh

telnet

su [username]

sudo

su

sudo [command]

sudo [username]

sudo -n

su root

su - [username]

sudo -s

sudo su

gcc file.c -o file

CVE exploits

wget

wget 127.0.0.1

Python script

cp to home dir

mkdir in tmp

mv file

cp file to tmp

scp file

touch

chmod 755

chmod 777

chmod +x

chmod +x [dir]

vi

nano

cat /etc/sudoers

sudo -s

sudo -l

bash

looks for ssh authorized keys

mount

Analysis

- Average attack time per host: **133.34 minutes**
- Average commands per host: **243**
- 2 participants got root on Host A
- 1 participant got root on Host B

Similarity coefficients

- 10 attackers, 2 machines = 100 crime pairs
  - Compare each attack against Host A to each attack against Host B
  - 10 linked pairs, 90 unlinked pairs
- Wrote application to calculate the similarity coefficient:
  - For each pair for the 3 behavioural domains
  - And differences between the 3 metadata variables
- Ended up with CSV file:
  - ID, paired (y/n), coefficients for each domain, differences for each metadata variable

Similarity coefficients - behaviours

Variables	Mean	Median	SD	Variance	Range
Navigation(linked)	0.756	0.756	0.166	0.28	0.5
Navigation (unlinked)	0.163	0.125	0.134	0.018	0.75
Enumeration (linked)	0.641	0.708	0.259	0.067	0.857
Enumeration (unlinked)	0.108	0.087	0.122	0.015	0.567
Exploitation (linked)	0.58	0.555	0.281	0.079	0.875
Exploitation (unlinked)	0.091	0.077	0.097	0.009	0.455

Table 1 showing mean, median, standard deviation, variance and range scores for the three behavioural domains for linked and unlinked subsets (Jaccard's coefficient)

Similarity coefficients - metadata

Variables	Mean	Median	SD	Variance	Range
Keystroke Interval (linked)	1726.642	351.723	4011.047	16088496.15	13017.14
Keystroke Interval (unlinked)	1827.393	488.678	3731.947	13927431.81	13425.62
Command Interval (linked)	46677.82	17058.83	61843.71	3824644150	194211
Command Interval (unlinked)	56354.3	29744.82	71853.04	5162858878	369751.9
Backspaces (linked)	5.471	2.416	7.53	56.695	24.355
Backspaces (unlinked)	9.574	6.941	8.715	75.944	38.249

Table 2 showing mean, median, standard deviation, variance and range values for the three timing and error variables for linked and unlinked subsets (keystroke and command interval in ms; backspaces as a percentage of total keystrokes).

Logistic regression

- Imported CSV file into SPSS
  - Strenuous Package for Sad Students ☹
  - Significant Probability of Statistics-related Stress ☹
- Direct logistic regression for each predictor variable
- Then forward stepwise logistic regression
- Six models in total, for each domain
- Plus an optimal combination/order of all domains

Results

Here comes the slide you've all been waiting for…

Variables	Statistics	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7
Constant	b	-8.782	-5.773	-5.815	-2.184	-2.083	-1.553	-104.458
	SE	2.741	1.318	1.297	0.37	0.421	0.502	8648.491
	OR	0	0.003	0.003	0.113	0.125	0.212	0
Navigation**	b	14.786						119.572
	SE	4.802						10021.408
	OR	2639086.08						8.50E+51
Enumeration*	b		10.701					136.097
	SE		2.716					31066.523
	OR		44415.895					1.28E+59
Exploitation*	b			14.012				
	SE			3.772				
	OR			1217542.54				
KS Interval+	b				0			
	SE				0			
	OR				1			
Cmd Interval+	b					0		
	SE					0		
	OR					1		
Backspaces+	b						-0.9	
	SE						0.065	
	OR						0.914	
	Model X^2	50.16	41.673	42.526	0.007	0.185	2.747	65.017
	X^2 sig.	p <0.05	p <0.05	p <0.05	Not sig.	Not sig.	Not sig.	p <0.001
	Nagelkerke R^2	0.825	0.713	0.725	0	0.004	0.057	1
	HL X^2	0.211	11.26	5.627	8.808	10.876	18.605	0
	HL X^2 sig.	p >0.05	p >0.05	p >0.05	p >0.05	p >0.05	p >0.05	p >0.05

Table 3 showing summary of logistic regression models for individual predictor variables.
b: logit coefficient; SE: standard error; OR = odds ratio
**: $p < 0.001$*
***: $p < 0.005$*
+: Not statistically significant
HL: Hosmer and Lemeshow goodness-of-fit test
Models 1-6: Binary logistic regression
Model 7: Forward stepwise logistic regression (inclusion criteria: $p < 0.05$)
Dependent variable: linked attack pair (1), unlinked attack pair (0)

You're too kind

(waits for applause to die down)


Calculator
STANDARD
0
MC MR M+ M- MS M˅
% √ x² ¹/x
CE C ⌫ ÷
7 8 9 ×
4 5 6 −
1 2 3 +
± 0 . =

What does this tell us?

- Three behavioural domains can classify linked/unlinked offences
- High level of accuracy
- Navigation: most effective predictor
  - Followed by exploitation, then enumeration
- Strong positive correlation to dependent variable
- Keystroke and command interval variables not reliable predictors
- Backspace: weak negative correlation to linkage
- Results statistically significant for behavioural domains
- But not for any metadata variables

ROC curves

- Results used to build ROC curves

Variable	AUC	Sig.	SE	95 %CI
Navigation	0.992	p <0.001	0.007	0.978 - 1.0
Enumeration	0.912	p <0.001	0.081	0.753 - 1.0
Exploitation	0.964	p <0.001	0.028	0.91 - 1.0
Keystroke Interval	0.572	NS	0.102	0.373 - 0.771
Command Interval	0.58	NS	0.113	0.358 - 0.802
Backspaces	0.702	p <0.05	0.094	0.519 - 0.886
Optimal	1	p <0.001	0	1.0 - 1.0

Table 4 showing area under the curve (AUC) values for each of the six predictors as well as the optimal model. SE: Standard error

ROC curves

I got 0.992 AUC, but it just ain't 1

Jay-Z

(A ROC fella)

https://www.discogs.com/artist/21742-Jay-Z#images/30264081

ROC curve results

- Navigation = 0.992
- Enumeration = 0.912
- Exploitation = 0.964
- Keystroke internal = 0.572
- Command interval = 0.58
- Backspace variable = 0.702
- **Optimal model (navigation & enumeration) = 1.0**

Implications

- Observations & comparisons
- Investigation implications
- Privacy implications
- Defeating CLA
- Threats to validity

Observations & comparisons

- High levels of consistency and distinctiveness
- Navigation and enumeration combined
  - No need for exploitation (in this study)
- Why was navigation specifically so prominent?
  - Something everyone does, every day
  - Enumeration & exploitation only done during attacks
  - Navigation behaviours may be more ingrained

Observations & comparisons

- Higher accuracy than other crime types
- Behaviours less subject to influence may be more stable
  - Nature of offence: offenders less likely to be influences
  - Broader approach may change
  - But possibly not granular command choice
  - Especially navigation

Observations & comparisons

- Metadata variables significantly weaker
- *What* you type has greater linking power than *how* you type
- Latency may have affected some of the results
- But mistakes/typos show some promise
- Needs further exploration

Implications for investigators

- Can link separate offences to common offenders
- With no atomic or computed IOCs
- But need a lot of information
  - Previous CLA/attribution work: limited, specific info required
  - Bennell & Canter, 2002; Hutchins et al, 2010; Clark & Landau, 2011
  - Here, need as much as possible
  - As granular as possible

Implications for investigators

- Need to be in a position to capture commands/keystrokes
  - High-interaction honeypots
  - Verbose and detailed logging
  - Backdoored CTFs or vulnerable VMs

Implications for investigators

- Could also link attackers who trained together
- Or who have all done a certain certification
  - Sample commands and code
  - Dilutes CLA assumption of distinctiveness
  - But could still assist with attribution

Privacy implications

- People can be linked to separate hosts/identities
  - Based on approaches, syntax, and commands
- Regardless of anonymising measures
- Regardless of good OPSEC elsewhere

Privacy implications

- Like forensic linguistics, exploits stable behavioural traits
- Won't be 100% accurate obviously
- And affects less of the population, cp. forensic linguistics
  - e.g. ~86% of the population is literate*
  - Less people than that can operate a command-line

* https://data.worldbank.org/indicator/SE.ADT.LITR.ZS, 27/06/18

Privacy implications

- This study only focused on commands
- May also apply to:
  - Typos, and the way you correct them
  - How you form capitals
  - Using PgDn/PgUp
  - Using arrow keys rather than the mouse
  - Tabs/spaces
  - Keyboard shortcuts
  - Use of, and preference for, bracket types

Privacy implications

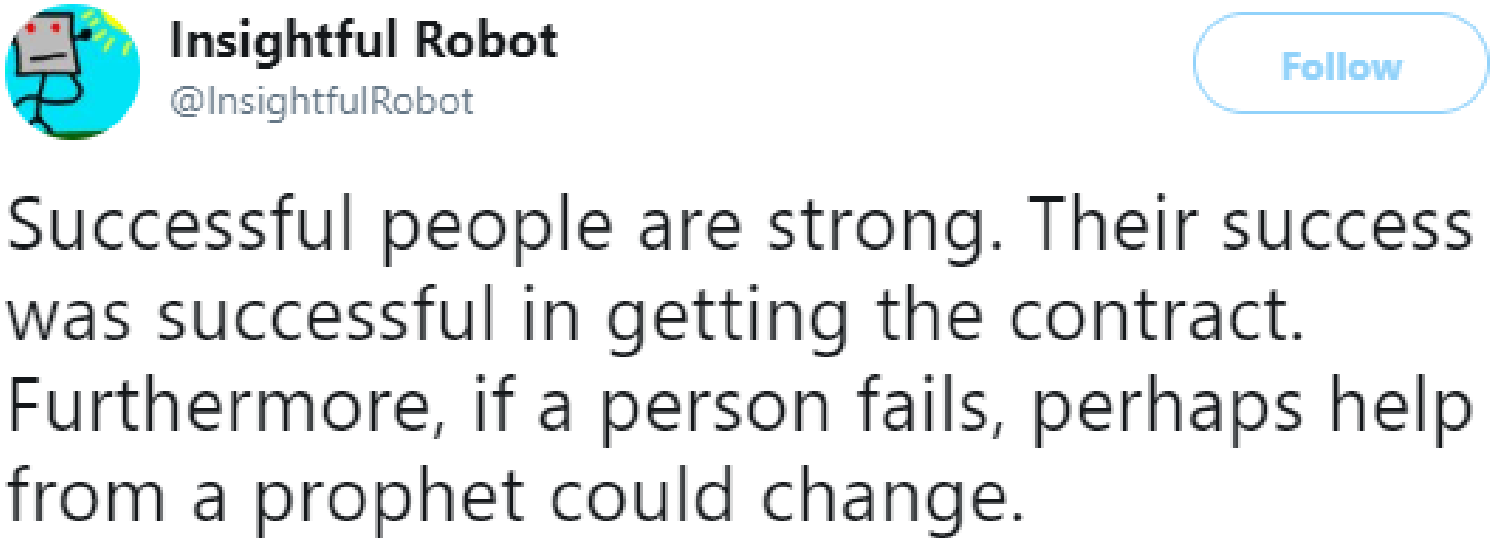
- If someone can log your keystrokes, you have issues anyway
  - But this is less about *identification*
  - If someone can log your keystrokes, it's not hard to find out who you are
- This is more about *attribution via linkage*
- Could be used to link you to historical/future activity
- Used to build up repository of command profiles

Defeating CLA

- Similar to defeating authorship identification
- Make a conscious decision to disguise your style
  - Forensic linguistics: solutions range from crude (Google Translate) to sophisticated (automated changes to sentence construction, synonym substitution, etc)
  - CLA different – e.g. alias command would not work
  - Hard to automate – can't predict commands in advance
  - Could semi-automate, using scripts

Note on Google Translate

- @InsightfulRobot)created by colleague Keith Short (@ItsNotKeith)
- Turns: *People who succeed have momentum. The more they succeed, the more they want to succeed, and the more they find a way to succeed. Similarly, when someone is failing, the tendency is to get on a downward spiral that can even become a self-fulfilling prophecy.*
- into:



Note on Google Translate

This is me trying to disguise my writing style through multiple translations, as a demonstration

- English -> Norwegian
- Norwegian -> French
- French -> Afrikaans
- Afrikaans -> Romanian
- Romanian -> Japanese
- Japanese -> English

U wot m8

彼女はデモンストレーションなど、さまざまな翻訳を通して私の文体を説明しようとしています

She is trying to explain my style through various translations such as demonstration

Defeating CLA

- Conscious changes are probably the best way to do it
- Randomising ordering of command switches
- Switching up tools used e.g. wget instead of curl; vi instead of nano; less instead of cat

Threats to validity

- Very small sample
- Not real-world data
- Attackers were willing volunteers
  - Knew they had permission, with no risk of reprisal
- Linux only
- One scenario (low-priv shell)
- Attackers may not always want/need to escalate

Summary

- Topics for future research
- Collaboration
- Conclusion
- References

Future research

- Explore effects of expertise and temporal proximity
- Further research into metadata variables for mistakes
- Real-world data
- Stochastic analysis
- Greater environmental and scenario diversity
- Real-time or near real-time automation

Collaboration

- Get in touch if you want to discuss
- **@darkartlab**
- **matt.wixey@pwc.com**

Conclusion

- Small, novel study
- Some promising results
- Significant implications for defenders/investigators
- As well as implications for privacy
- Needs further investigation

References

Alison, L.J., Snook, B. and Stein, K.L., 2001. Unobtrusive measurement: Using police information for forensic research. *Qualitative Research*, 1(2), 241-254.

Bateman, A.L. and Salfati, C.G., 2007. An examination of behavioral consistency using individual behaviors or groups of behaviors in serial homicide. *Behavioral Sciences & the Law*, 25(4), 527-544.

Bennell, C. and Canter, D.V., 2002. Linking commercial burglaries by modus operandi: Tests using regression and ROC analysis. *Science & Justice*, 42(3), 153-164.

Bennell, C. and Jones, N.J., 2005. Between a ROC and a hard place: A method for linking serial burglaries by modus operandi. *Journal of Investigative Psychology and Offender Profiling*, 2(1), 23-41.

Bouhana, N., Johnson, S.D. and Porter, M., 2014. Consistency and specificity in burglars who commit prolific residential burglary: Testing the core assumptions underpinning behavioural crime linkage. *Legal and Criminological Psychology*, 21(1), 77-94.

Caliskan-Islam, A., Yamaguchi, F., Dauber, E., Harang, R., Rieck, K., Greenstadt, R. and Narayanan, A., 2015. When Coding Style Survives Compilation: Deanonymizing Programmers from Executable Binaries. *arXiv preprint* arXiv:1512.08546.

Canter, D., 1995. Psychology of offender profiling. *Handbook of psychology in legal contexts* (1994).

Canter, D., 2000. Offender profiling and criminal differentiation. *Legal and Criminological Psychology*, 5(1), 23-46.

Chiesa, R., Ducci, S. and Ciappi, S., 2008. *Profiling hackers: the science of criminal profiling as applied to the world of hacking* (Vol. 49). CRC Press.

Clark, D.D. and Landau, S., 2011. Untangling attribution. *Harv. Nat'l Sec. J.*, 2

Craik, M. and Patrick, A., 1994. Linking serial offences. *Policing London* 10

data.worldbank.org/indicator/SE.ADT.LITR.ZS, accessed 27/06/2018

References

Donald, I. and Canter, D., 1992. Intentionality and fatality during the King's Cross underground fire. *European journal of social psychology*, 22(3), 203-218.

Douglas, J.E. and Munn, C., 1992. Violent crime scene analysis: Modus operandi, signature and staging. *FBI Law Enforcement Bulletin*, 61(2).

Filippoupolitis, A., Loukas, G. and Kapetanakis, S., 2014. Towards real-time profiling of human attackers and bot detection. http://gala.gre.ac.uk/14947/1/14947_Loukas_Towards%20real%20time%20profiling%20(AAM)%202014..pdf, accessed 05/07/2018.

Freyd, Jennifer J., 1996. *Betrayal Trauma: The Logic of Forgetting Childhood Abuse*. Cambridge: Harvard University Press.

Furr, R.M. and Funder, D.C., 2004. Situational similarity and behavioral consistency: Subjective, objective, variable-centered, and person-centered approaches. *Journal of Research in Personality*, 38(5), 421-447.

github.com/NetSPI/skl, accessed 27/06/2018

Grubin, D., Kelly, P. and Brunsdon, C., 2001. Linking serious sexual assaults through behaviour (Vol. 215). Home Office, Research, Development and Statistics Directorate.

Guitton, C., 2012. Criminals and cyber attacks: The missing link between attribution and deterrence. *International Journal of Cyber Criminology*, 6

Halligan, S. L., Michael, T., Clark, D. M., & Ehlers, A. (2003). Posttraumatic stress disorder following assault: The role of cognitive processing, trauma memory, and appraisals. *Journal of consulting and clinical psychology*, *71*(3)

Harbort, S. and Mokros, A., 2001. Serial Murderers in Germany from 1945 to 1995: A Descriptive Study. *Homicide Studies*, 5(4), 311-334.

Hettema, J. and Hol, D.P., 1998. Primary control and the consistency of interpersonal behaviour across different situations. *European journal of personality*, 12(4), 231-247.

Hunker, J., Hutchinson, B. and Margulies, J., 2008. Role and challenges for sufficient cyber-attack attribution. *Institute for Information Infrastructure Protection* 5-10.

Hutchins, E.M., Cloppert, M.J. and Amin, R.M., 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1

Landreth, B., 1985. *Out of the inner circle: A hacker guide to computer security*. Microsoft Press.

References

Mejia, E.F., 2014. Act and actor attribution in cyberspace: a proposed analytic framework. *Air Univ Maxwell AFB AL Strategic Studies Quarterly*.

Mischel, W. and Shoda, Y., 1995. A cognitive-affective system theory of personality: reconceptualizing situations, dispositions, dynamics, and invariance in personality structure. *Psychological review*, 102(2)

Mischel, W., 1999. Personality coherence and dispositions in a cognitive-affective personality system (CAPS) approach. In: *The coherence of personality: Social-cognitive bases of consistency, variability, and organization* (eds. Cervone and Shoda), 37-60.

Mokros, A. and Alison, L.J., 2002. Is offender profiling possible? Testing the predicted homology of crime scene actions and background characteristics in a sample of rapists. *Legal and Criminological Psychology*, 7(1), 25-43.

Moran, N. and Bennett, J., 2013. *Supply Chain Analysis: From Quartermaster to Sun-shop* (Vol. 11). FireEye Labs.

Pervin, L.A., 2002. Current controversies and issues in personality. 3rd ed. John Wiley & Sons.

Ramsbrock, D., Berthier, R. and Cukier, M., 2007, June. Profiling attacker behavior following SSH compromises. In 37th Annual IEEE/IFIP international conference on dependable systems and networks (DSN'07) 119-124

Raynal, F., Berthier, Y., Biondi, P. and Kaminsky, D., 2004. Honeypot forensics, Part II: analyzing the compromised host. *IEEE security & privacy*, 2(5), 77-80.

Rid, T. and Buchanan, B., 2015. Attributing cyber attacks. *Journal of Strategic Studies*, 38(1-2), 4-37

Salles-Loustau, G., Berthier, R., Collange, E., Sobesto, B. and Cukier, M., 2011, December. Characterizing attackers and attacks: An empirical study. In Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing 174-183

Shaw, E., Ruby, K. and Post, J., 1998. The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, 2(98), 1-10.

Shoda, Y., Mischel, W. and Wright, J.C., 1994. Intraindividual stability in the organization and patterning of behavior: incorporating psychological situations into the idiographic analysis of personality. *Journal of personality and social psychology*, 67(4)

References

Slater, C., Woodhams, J. and Hamilton-Giachritsis, C., 2015. Testing the Assumptions of Crime Linkage with Stranger Sex Offenses: A More Ecologically-Valid Study. *Journal of Police and Criminal Psychology*, 30(4), 261-273.

Sorochinski, M. and Salfati, C.G., 2010. The consistency of inconsistency in serial homicide: Patterns of behavioural change across series. *Journal of Investigative Psychology and Offender Profiling*, 7(2), 109-136.

Swets, J.A., 1988. Measuring the accuracy of diagnostic systems. *Science*, 240(4857), 1285-1293.

Symantec, 2011. W32.Duqu: The precursor to the next Stuxnet. Symantec Corporation, California, USA. Available from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Tonkin, M., Grant, T. and Bond, J.W., 2008. To link or not to link: A test of the case linkage principles using serial car theft data. *Journal of Investigative Psychology and Offender Profiling*, 5(1-2), 59-77.

Watters, P.A., McCombie, S., Layton, R. and Pieprzyk, J., 2012. Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP). *Journal of Money Laundering Control*, 15(4), 430-441.

Wheeler, D.A. and Larsen, G.N., 2003. Techniques for cyber attack attribution (No. IDA-P-3792). Institute for Defense Analyses, Alexandria, VA, USA.

Woodhams, J. and Grant, T., 2006. Developing a categorization system for rapists' speech. *Psychology, Crime & Law*, 12(3), 245-260.

Woodhams, J. and Labuschagne, G., 2012. A test of case linkage principles with solved and unsolved serial rapes. *Journal of Police and Criminal Psychology*, 27(1), 85-98.

Zayas, V., Shoda, Y. and Ayduk, O.N., 2002. Personality in context: An interpersonal systems perspective. *Journal of personality*, 70(6), 851-900.

Thoughts, questions, feedback:

@darkartlab

matt.wixey@pwc.com