secure by design

- how to think about, design and build secure software

jim rush

PrivSec Consulting

Whānau Mārama
New Zealand International
Film Festival

timely

HOMES.CO.NZ

PRIVSECCONSULTING

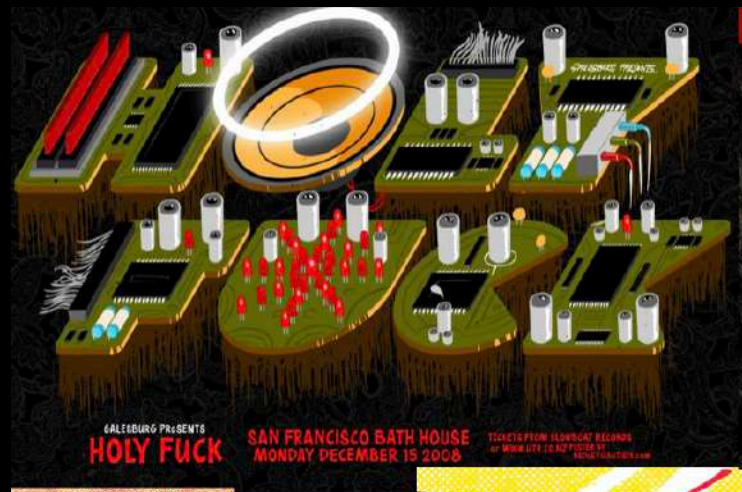
RUSH
MORE

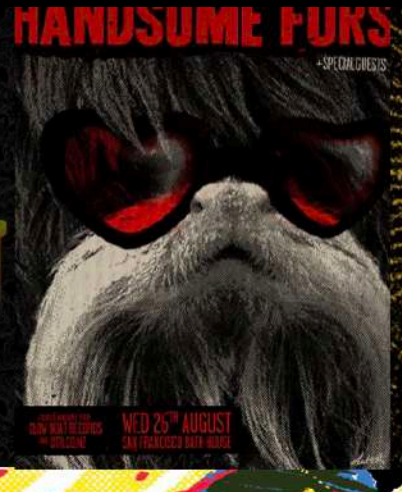
ZX
SECURITY

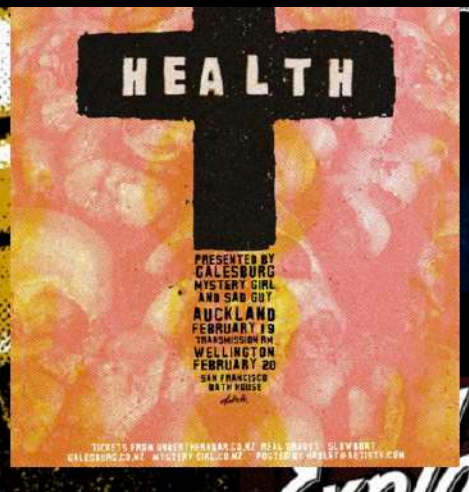
RNZ

about me

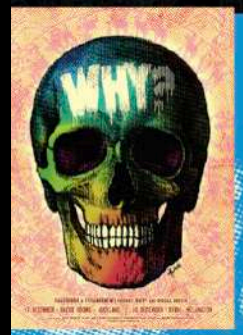
- i was a software developer, once
- DEFCON 32 speaker 2024
- off by one speaker 2025
- MSRC leaderboard Q1 and Q2 2024
- Frequent flyer with CERT (now part of NCSC)


GALESBURG PRESENTS
HOLY FUCK
SAN FRANCISCO BATH HOUSE
MONDAY DECEMBER 15 2008


HANDSOME FURS
+SPECIAL GUESTS
WED 26TH AUGUST
SAN FRANCISCO BATH HOUSE


HEALTH
PRESENTED BY
GALESBURG
MYSTERY GIRL
AND SAD GUY
AUCKLAND
FEBRUARY 19
TRANSMISSION RM
WELLINGTON
FEBRUARY 20
SAN FRANCISCO
BATH HOUSE


DEERHUNTER

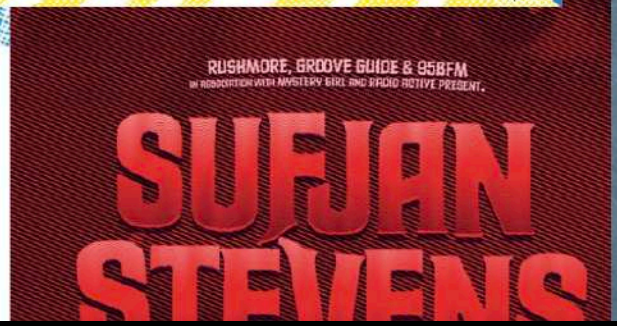

WHY?

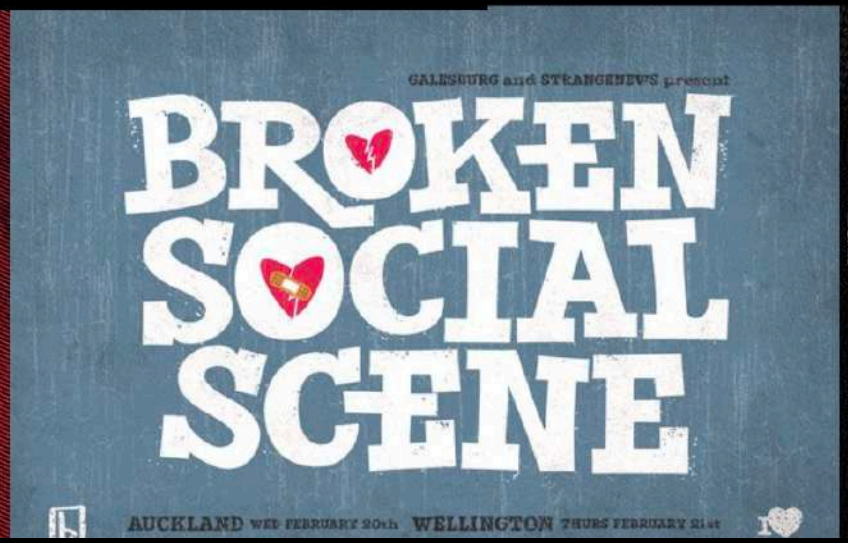

GALESBURG PRESENTS
GIRL TALK
WITH SUPPORT FROM DROPKICK COUSINS
24 JANUARY 2009 SAN FRANCISCO BATH HOUSE
TICKETS FROM SLOWBOAT RECORDS AND UTR.CO.NZ

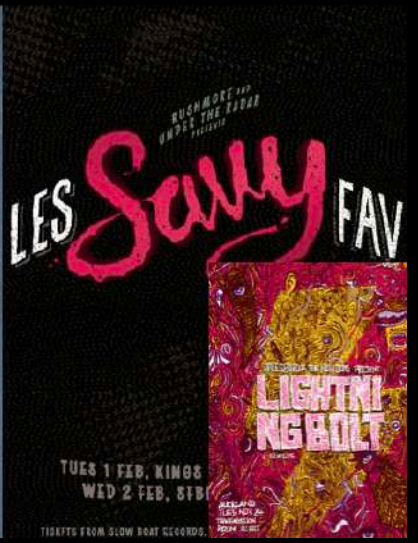

the National
TUE 15 JAN 08 AT THE KINGS ARMS IN AUCKLAND
WITH THE VIETNAM WAR


galesburg and strangenews present
Explosions in the Sky
with Eluvium (usa) and guests
Mon February 11 Auckland Kings Arms
Tues February 12 Wellington San Francisco Bath House

PRESENT
PAVEMENT
1ST MARCH 2010 - AUCKLAND TOWN HALL
TICKETS FROM TICKETEK WWW.TICKETEK.CO.NZ WWW.MYSTERYGIRL.CO.NZ WWW.GALESBURG.CO.NZ


RUSHMORE, GROOVE GUIDE & 95BFM
SUFJAN
STEVENS


GALESBURG and STRANGENEWS present
BROKEN
SOCIAL
SCENE
AUCKLAND WED FEBRUARY 20th WELLINGTON THURS FEBRUARY 21st


LES
Savy
FAV
LIGHTNI
NG BOLT
TUES 1 FEB, KINGS
WED 2 FEB, SIB
TICKETS FROM SLOW BOAT RECORDS

about me (more)

- Security Researcher / bug bounty
  - I find and report things
- Pentester / security consultant (PrivSec)
  - I find and report things for work

disclaimer

- I am a security person who enjoys privacy
- cybersecurity can help protect digital privacy

some things we're going to talk about

- defining some things
- threat modelling
- the CIA triad
- the Software Development Life Cycle (SDLC)
- how insecure design can get you in trouble

some more things we're going to talk about

- some examples of insecure design in the wild
- some byproducts of moving fast
- Microsoft


so you want to build secure software (score 0/600)

some things that can be thought about when making software: the basics

- encryption (at rest, in transit)
- logging & redacting logging
- dev and test environments

some more things to think about when moving pixels

- allowing users to delete their data
- maybe an audit could help
- notifying users when data is collected

it's not always easy

- commercial pressures, various contexts, can lead to less than ideal outcomes
- getting the basics right will get you a long way
- we have to try!

some definitions

- encryption
- hashing
- git
- threat modelling
- security controls

encryption

- sometimes two parties wish to communicate securely and privately
- one of our oldest technologies
  - Caesar cipher

    Plain |A|B|C|D|...

    Cipher|X|Y|A|B|...

encryption in 2025

- Symmetric encryption
  - same key for encryption and decryption
- Asymmetric encryption
  - different key
  - allows for secure key exchange

hashing goes brrr

- a 'one way function'
  - can't get the data back (mostly)
- used to store passwords securely
- plain text -> hash function -> hashed text
  - e234dsdom3k2kmdl3l43iwes9vjro44223m3n32kn5n2ksdo4

git

- version control for software
  - think of it like tracked changes but useful
- nothing really disappears from it

threat modelling

- Defining security requirements.
- Creating an application diagram.
- Identifying threats.
- Mitigating threats.
- Validating that threats have been mitigated.

how this looks in practice

- it depends
- agile is sometimes involved
  - jira even


yay agile

> _

the Software Development LifeCycle (SDLC)

- methodology that helps teams build software
- from planning to eventual deployment

SDLC (generally)

- planning
- requirements gathering
- design
- code
- implement
- test -> deploy


seems fine, we'll just get a
pentest after we're done


oh

threat model early and often

- best done at early stages of design
- sometimes software can be hard to unpick

the CIA triad

- confidentiality
- integrity
- availability

what the CIA triad means

- confidentiality:
  - information access and disclosure
- integrity:
  - information modification or destruction

a framework

- helps us identify risk
- helps us keep data private
- used to classify bugs such as CVE's
  (common vulnerabilities and exposures)

security controls

- password
- warnings in the app (Microsoft)
- MFA
- physical controls, network controls

how insecure design can get you in trouble

- some case studies
  - when the intranet goes inter
  - insecure storage of passwords

the little intranet that could

- a network design issue
- ports 0-65535
  - 80, 443 are the internet ones
- On a pentest, an org had piped their intranet to the world
  - Hundreds of thousands of records


hello world!
Enter search string:
(aaaaaaaaaa_

secure.xml

- we talked about passwords and hashes
- usually they're in a database somewhere
- some servers will show you different file types
- XML -> eXtensible Markup Language

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
▼<users>
  ▼<user>
      <username>alice</username>
      <passwordHash>482c811da5d5b4bc6d497ffa98491e38</passwordHash>
    </user>
  ▼<user>
      <username>bob</username>
      <passwordHash>0d107d09f5bbe40cade3de5c71e9e9b7</passwordHash>
    </user>
  ▼<user>
      <username>charlie</username>
      <passwordHash>5f4dcc3b5aa765d61d8327deb882cf99</passwordHash>
    </user>
  ▼<user>
      <username>diana</username>
      <passwordHash>25d55ad283aa400af464c76d713c07ad</passwordHash>
    </user>
  ▼<user>
      <username>james</username>
      <passwordHash>e99a18c428cb38d5f260853678922e03</passwordHash>
    </user>
```

CERT to the rescue

- with the permission of the client, I disclosed to CERT
- Approximately 220 organisations impacted
- CERT was able to send out a targeted advisory

some byproducts of moving fast

- lots of software ship code several times a day
- sometimes things are 'left over' from this process

are your artifacts getting you in trouble

- deployment pipelines
- write code -> code runs on website
- sometimes things are left over
  - might be written to disk as part of the process


are these.. deployment
artifacts?

several in the wild

- .git/HEAD in web root
  - can download and reconstruct source!
  - like leaving a document with tracked changes just there
- it's ok, people don't put secrets in code
- various xml, json files

encryption (at rest, in transit)

- in transit https:, ftps:
- at rest:
  - things stored in blob storage, s3 buckets, filesystem
  - need a key to decrypt

logging

- logging is a file or a database that logs activities of things that are happening
- sometimes logs can leak personal information!
  - where are they being sent?
  - what is being sent?

scrubbing logging

- both Azure front door and AWS offer 'log scrubbing' to remove personal data
- what about other info making it into logs?


What possible problem could there be!?

Xiaomi S3 Smartwatch

- a standard piece of smartwatch, hacked by Sergei Volokitin
- has lots of sensitive information
- but also has a 6 digit pin protecting it
- was possible to dump memory and logs, but doesn't contain the pin :-(

...but sometimes logs are enough

- how?

The Log

```
[10/23 14:56:13] [46] [ap] [pagemanager] on_ui_destroy: delete view 0x3ced5cb0:{2, 1}
[10/23 14:56:13] [46] [ap] [pagemanager] page_out_anim_ready_cb: page out animation ended
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: down: id 0, x 226, y 436
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: move: id 0, x 226, y 436
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: pressed
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report:  up: id 0, x 226, y 436
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: released
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: down: id 0, x 236, y 413
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: move: id 0, x 236, y 413
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: pressed
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report:  up: id 0, x 236, y 413
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: released
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_verify_pin: succeeded to verify
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_verify_pin: succeeded to verify
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_unlock: screen is unlocked, tag=system_password
```

The Log

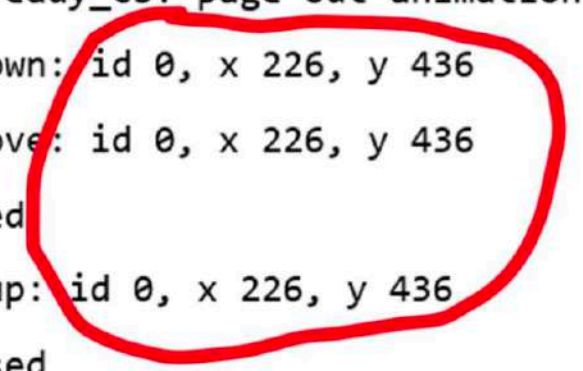
```
[10/23 14:56:13] [46] [ap] [pagemanager] on_ui_destroy: delete view 0x3ced5cb0:{2, 1}
[10/23 14:56:13] [46] [ap] [pagemanager] page_out_anim_ready_cb: page out animation ended
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: down: id 0, x 226, y 436
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: move: id 0, x 226, y 436
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: pressed
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report:  up: id 0, x 226, y 436
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: released
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: down: id 0, x 236, y 413
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: move: id 0, x 236, y 413
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: pressed
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report:  up: id 0, x 236, y 413
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: released
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_verify_pin: succeeded to verify
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_verify_pin: succeeded to verify
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_unlock: screen is unlocked, tag=system_password
```

The Log

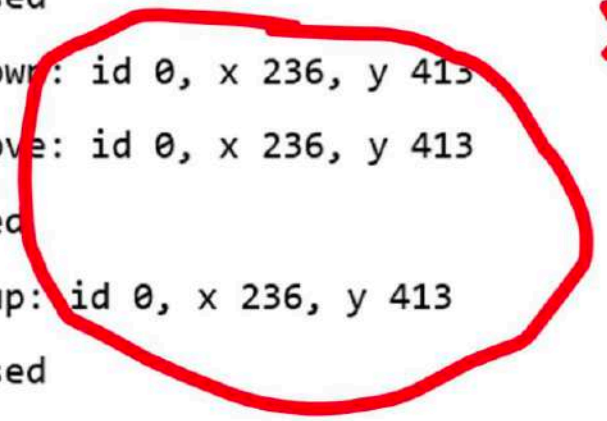
```
[10/23 14:56:13] [46] [ap] [pagemanager] on_ui_destroy: delete view 0x3ced5cb0:{2, 1}
[10/23 14:56:13] [46] [ap] [pagemanager] page_out_anim_ready_cb: page out animation ended
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: down: id 0, x 226, y 436
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: move: id 0, x 226, y 436
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: pressed
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report:  up: id 0, x 226, y 436
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: released
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: down: id 0, x 236, y 413
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: move: id 0, x 236, y 413
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: pressed
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report:  up: id 0, x 236, y 413
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: released
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_verify_pin: succeeded to verify
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_verify_pin: succeeded to verify
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_unlock: screen is unlocked, tag=system_password
```

The Log

```
[10/23 14:56:13] [46] [ap] [pagemanager] on_ui_destroy: delete view 0x3ced5cb0:{2, 1}
[10/23 14:56:13] [46] [ap] [pagemanager] page_out_anim_ready_cb: page out animation ended
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: down: id 0, x 226, y 436
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: move: id 0, x 226, y 436
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: pressed
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report:  up: id 0, x 226, y 436
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: released
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: down: id 0, x 236, y 413
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report: move: id 0, x 236, y 413
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: pressed
[10/23 14:56:13] [ 1] [ap] tma525_parse_touch_report:  up: id 0, x 236, y 413
[10/23 14:56:13] [46] [ap] [touch] touchpad_read: released
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_verify_pin: succeeded to verify
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_verify_pin: succeeded to verify
[10/23 14:56:14] [46] [ap] [LockScreen] lockscreen_manager_unlock: screen is unlocked, tag=system_password
```

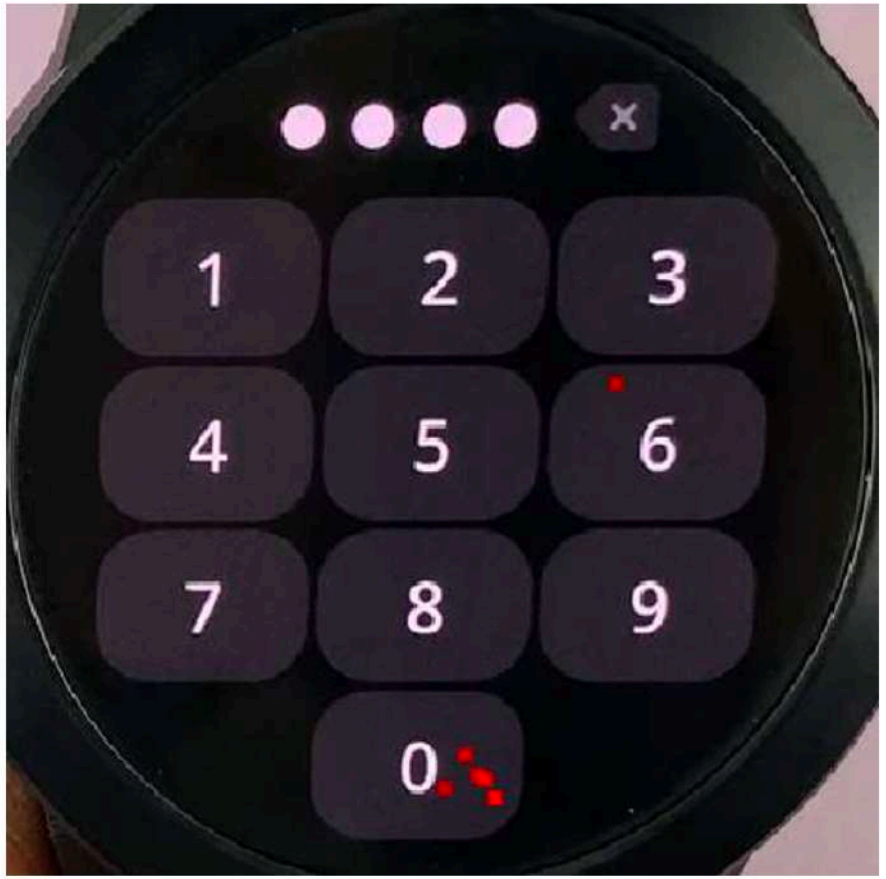


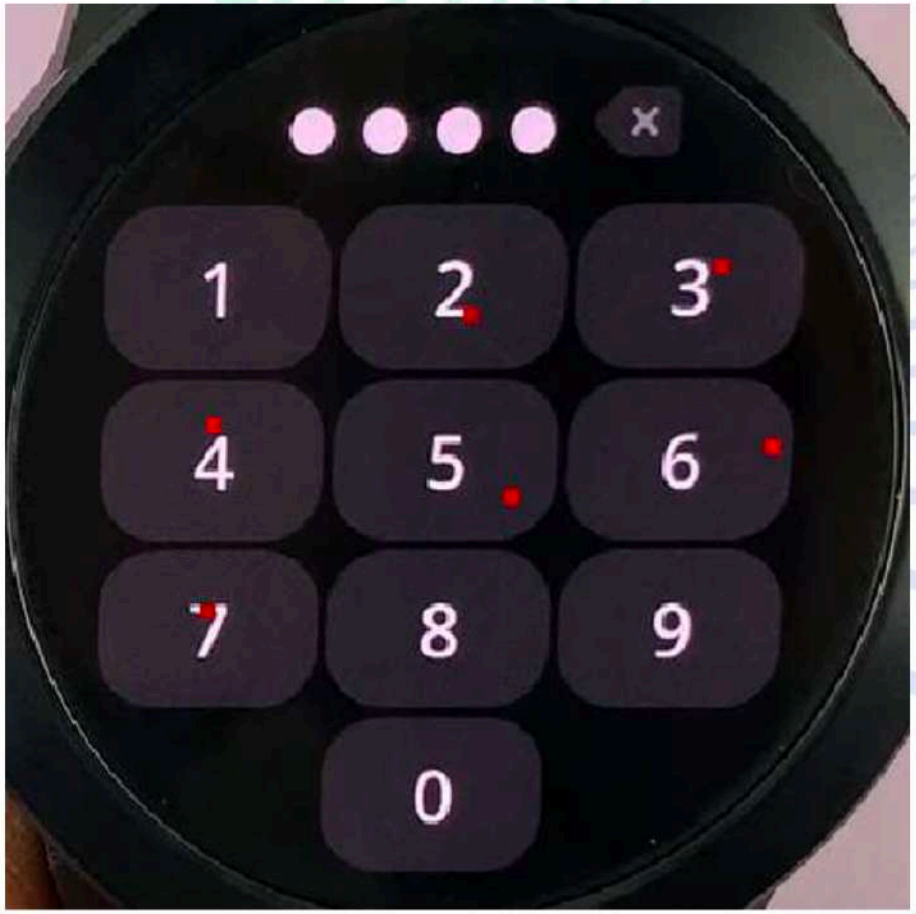
x = 226
y = 436



x = 236
y = 413

Full Pin recovery





dev and test environments

- we use different data, honestly
- demo:demo, test:test
- one of the biggest threats to a lot of organisations
  - prod data exists in test environments
  - security controls are frequently weaker

encourage audits

- Kerckhoffs's principle:
  - 19th century cryptographer
- "a cryptosystem should be secure, even if everything about the system, except the key, is public knowledge"

encourage audits part 2

- similar concepts date back further
- even if everything about the lock is known, it should be secure
- some software tries to obscure itself
- A Very Brief History Of Safecracking: Petra Smith

audits: we're not here to make you feel bad

- privacy and security is a team sport
- we prioritise collaboration over confrontation
- we have the same end goal:
  - a safe and secure NZ digital space

notifying users when data is collected

- the privacy act is reasonably clear on this, as you know
  - "You need to take reasonable steps"
- how many websites have one?

allow users to delete their data

- sometimes not possible, i.e Xero
- what about when you deactivate your account?
  - is it really gone?

it's all about the vibe

- the rise of AI has lead to some ... interesting results
- garbage in, garbage out
- not to mention the blatant disregard the harvesters have for privacy

vibe coding

- using the plagiarsm machine to write code
- let's see how that works

leo @leojr94_ · Mar 14

my saas was built with Cursor, zero hand written code

AI is no longer just an assistant, it's also the builder

Now, you can continue to whine about it or start building.

P.S. Yes, people pay for it

81 38 612 94K

leo
@leojr94_

guys, i'm under attack

ever since I started to share how I built my SaaS using Cursor

random thing are happening, maxed out usage on api keys, people bypassing the subscription, creating random shit on db

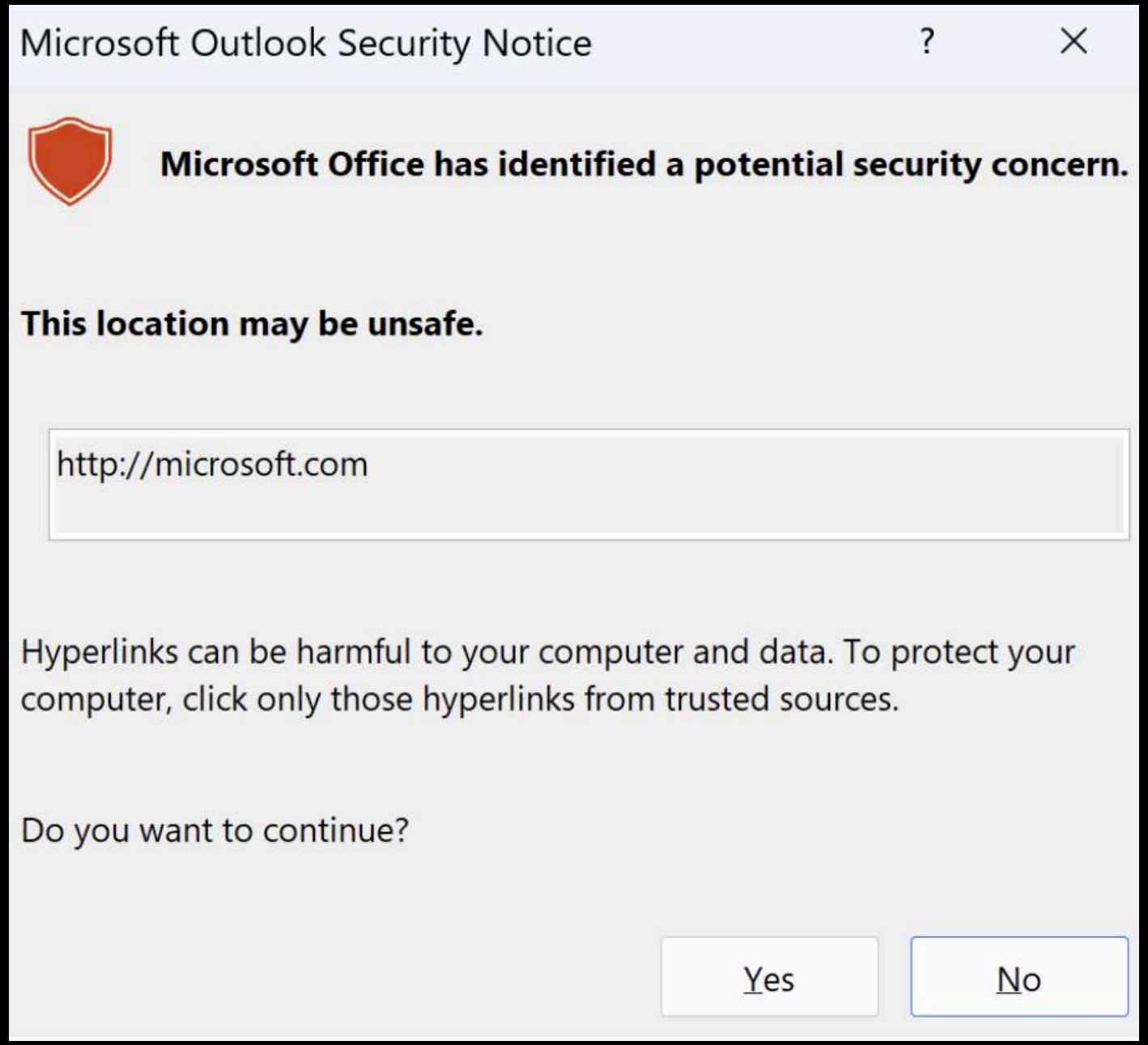
as you know, I'm not technical so this is taking me longer that usual to figure out

for now, I will stop sharing what I do publicly on X

there are just some weird ppl out there

Microsoft

- Microsoft has 'security controls'
- this is their primary 'don't hack me' prevention
- seriously, I wish it wasn't
  - we've all seen them


Microsoft Outlook Security Notice
?
Microsoft Office has identified a potential security concern.
This location may be unsafe.
http://microsoft.com
Hyperlinks can be harmful to your computer and data. To protect your computer, click only those hyperlinks from trusted sources.
Do you want to continue?
Yes
No

we talked a bit about hashes

- microsoft has a VERY special flavour of them
- called the New Technology Lan Manager (NTLM)
  - made in the 90's
- accessing a file share? NTLM is often used

MS has been trying to deprecate this since 2010

- it's not going well
- 'for legacy reasons'
- they're finally turning it off, next year

they're pretty bad

- known and loved by APT (advanced persistent threats)
  - they love to cause data breaches
- can be relayed around an internal domain to impersonate users
- can be cracked offline

so we came up with some techniques to phish for them

- POC or GTFO
- our techniques bypassed all security controls
- bypassed safelinks, MOTW (Mark of the Web), no AV

XXX Demo XXX

we ended up with four of these with MS

- most patched in August/September 2024
- multiple CVEs assigned

so

- we've seen some real world examples of design failures
- we've seen some common techniques to try and create secure software
- what now?

frontload the effort

- trust me
- upfront thinking and planning can save you a tonne of hurt
- design reviews, threat modelling, getting the basics right

questions?

- https://www.linkedin.com/in/jimsrush/
- A Very Brief History Of Safecracking:
  Petra Smith:
  https://www.youtube.com/watch?
  v=pgN7p8mli0A