Unmasking Data Leaks

A Guide to Finding, Fixing, and Preventing

DUO LABS

Duo Security is now part of Cisco. cisco.

Hi there, I’m Jordan.

- Tech lead for Duo Labs
- Open-Source software author

@jw_sec

jordan-wright

DUO LABS

Duo Security is now part of Cisco. cisco

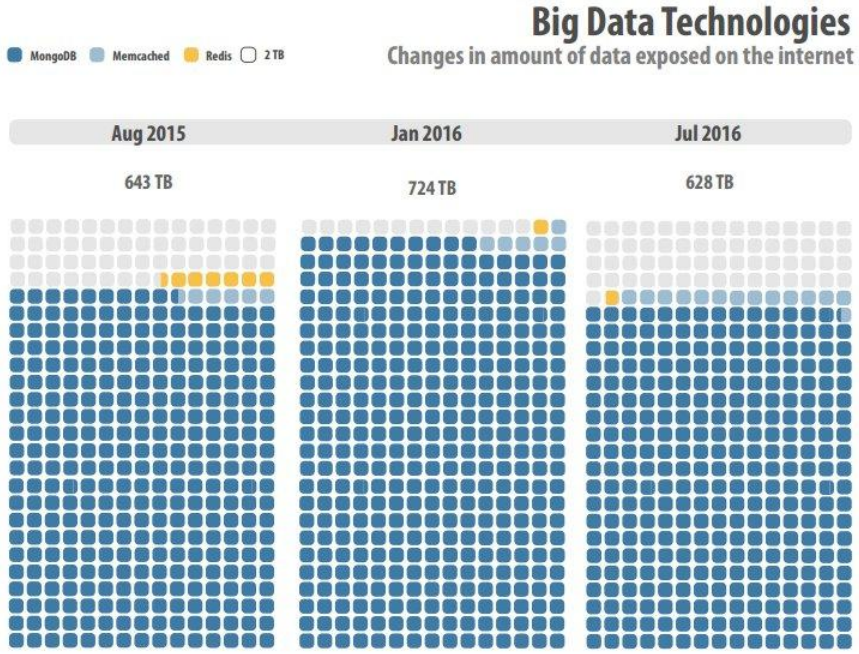
Today, we're going to talk about **research.**

A Flashback

- Presented at LASCON 2016 about data leaks

A Flashback

- Presented at LASCON 2016 about data leaks
- Discussed the results of research exploring data leaks
  - What types of databases are available
  - How much data is exposed
  - What types of data are exposed



Source: BinaryEdge Internet Security Exposure Report

Agenda

- The security research process
- Identifying a problem: data leaks
- How to find data leaks
- Live coding a scanner
- Preventing data leaks

Disrupt.
Derisk.
Democratise.

What is Security Research?

Identifying a problem

Home > News > Security > Over 275 Million Records Exposed by Unsecured MongoDB Database

Over 275 Million Records Exposed by Unsecured MongoDB Database

By Sergiu Gatlan

May 8, 2019 06:35 PM

14 DEC 15

13 Million MacKeeper Users Exposed

ElasticSearch server exposed the personal data of over 57 million US citizens

Leaky database taken offline, but not after leaking user details for nearly two weeks.

By Catalin Cimpanu for Zero Day | November 28, 2018 -- 15:00 GMT (07:00 PST) | Topic: Security

January 24, 2019

24 million credit and mortgage records exposed on Elasticsearch database

Doug Olenick

798M email addresses found exposed on misconfigured MongoDB database

BY DUNCAN RILEY

Data of nearly 700,000 Amex India customers exposed via unsecured MongoDB server

Over 2.3 million user records were encrypted, but data for 700,000 customers was not.

By Catalin Cimpanu for Zero Day | November 7, 2018 -- 14:00 GMT (06:00 PST) | Topic: Security

NEWS

MongoDB configuration error exposed 93 million Mexican voter records

According to Mexican law, it's illegal to use voter records for personal gain

Rapid7 Blog

Rsunk your Battleship: An Ocean of Data Exposed through Rsync

Thousands of Unprotected Kibana Instances Exposing Elasticsearch Databases

April 01, 2019 Wang Wei

Fortune 500 company leaked 264GB in client, payment data

Updated: The data leak impacted [redacted] client servers, SAP systems, and more.

By Charlie Osborne for Zero Day | June 7, 2019 -- 10:39 GMT (03:39 PDT) | Topic: Security

Fortune 500 company leaked 264GB in client, payment data

Updated: The data leak impacted client servers, SAP systems, and more.

By Charlie Osborne for Zero Day | June 7, 2019 -- 10:39 GMT (03:39 PDT) | Topic: Security

June 7, 2019 -- 10:39 GMT

DUO LABS

Duo Security is now part of Cisco. cisco

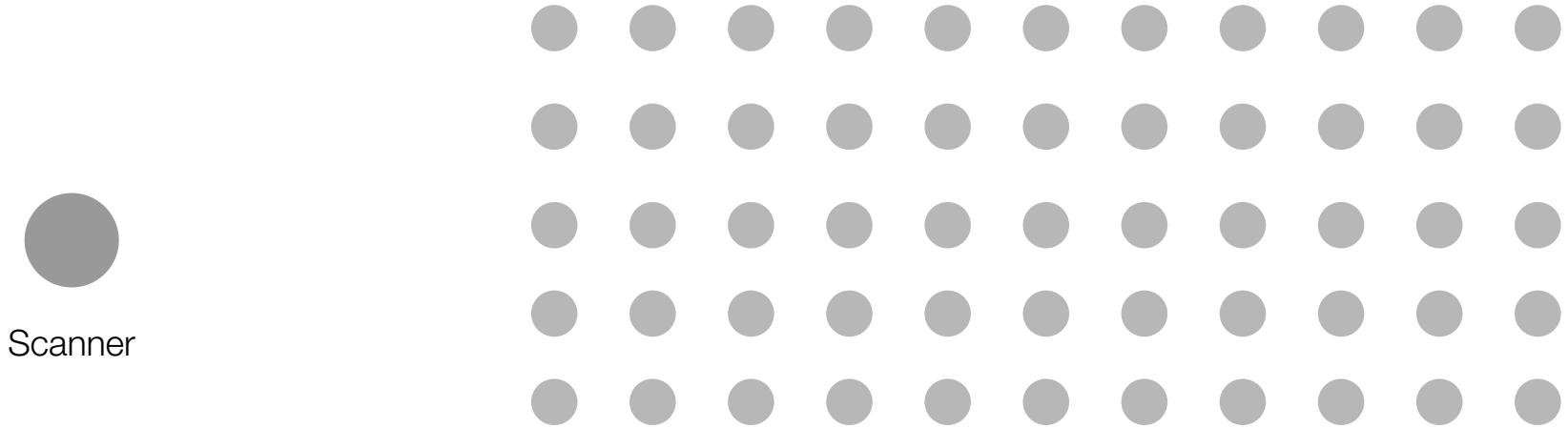
Potential Open “Databases”

- MongoDB
- Elasticsearch (and Kibana)
- CouchDB
- Rsync
- S3 buckets
- Redis
- Memcached
- Cassandra
- Graylog

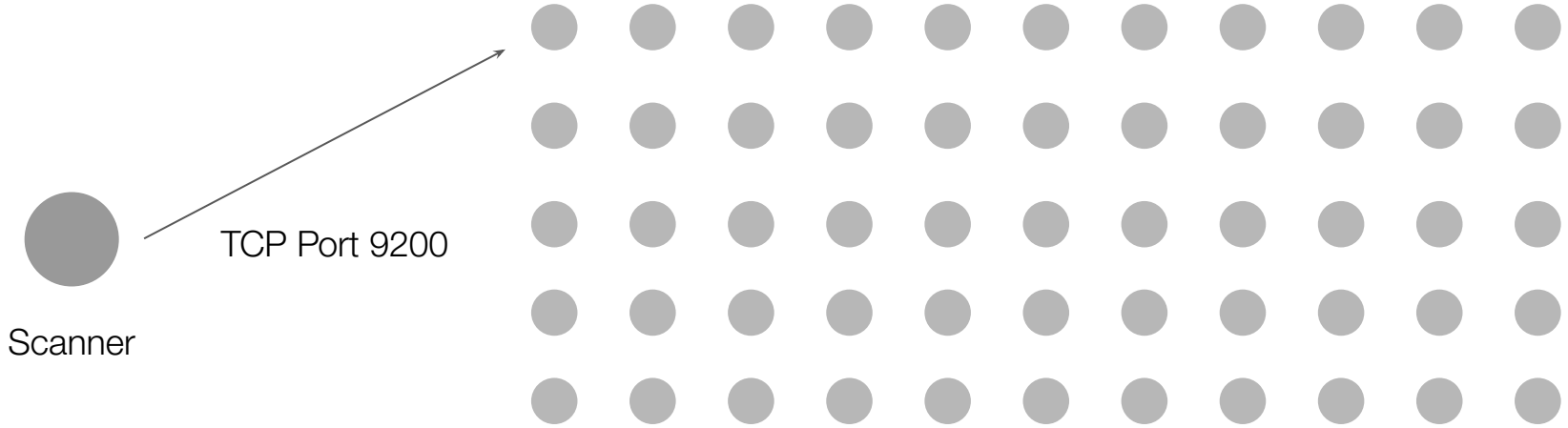
Exploring a problem

Remember:
The goal of our research is remediation.

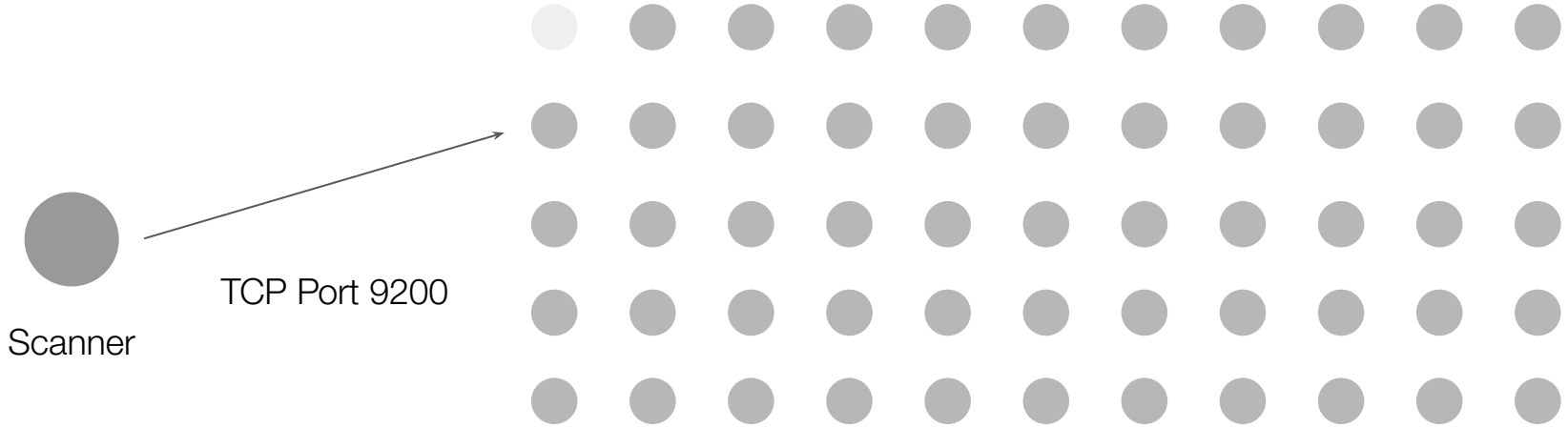
How to Find Data Leaks



How to Find Data Leaks



How to Find Data Leaks

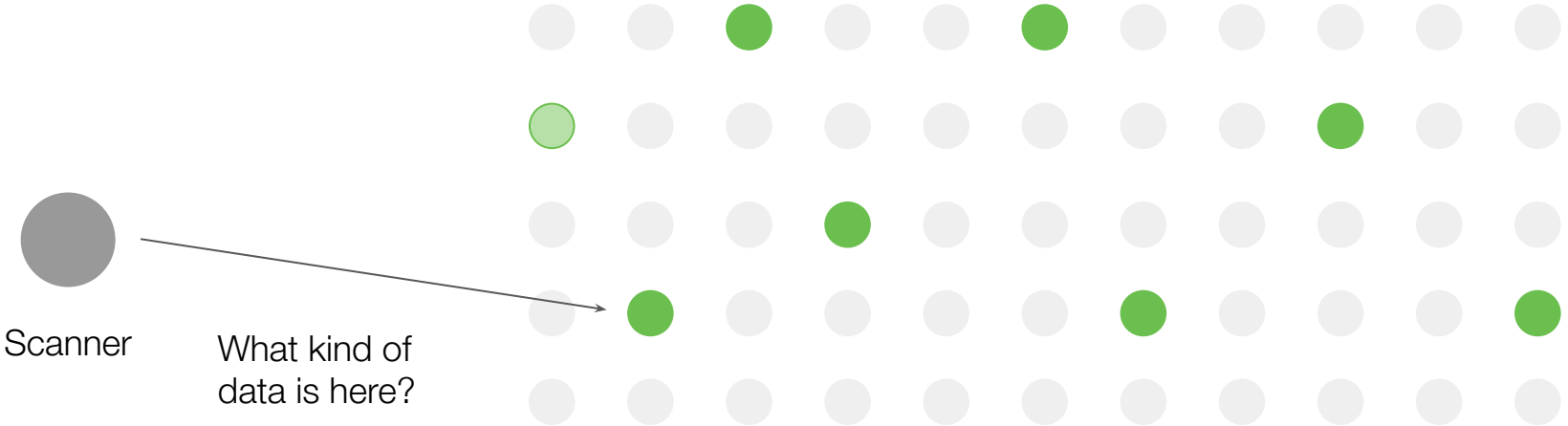


How to Find Data Leaks

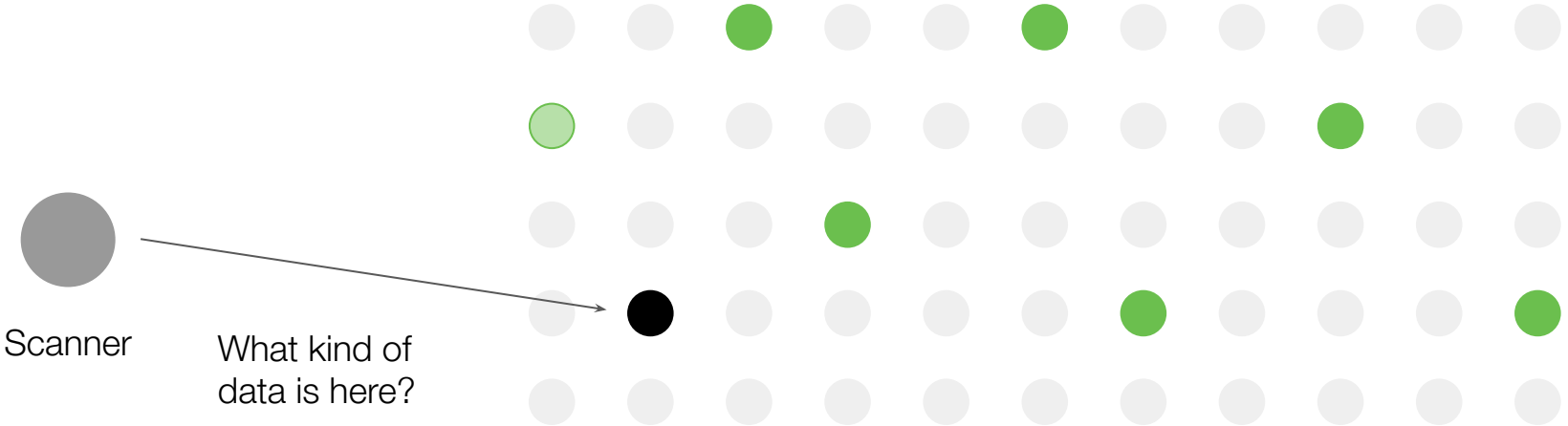
How to Find Data Leaks

How to Find Data Leaks

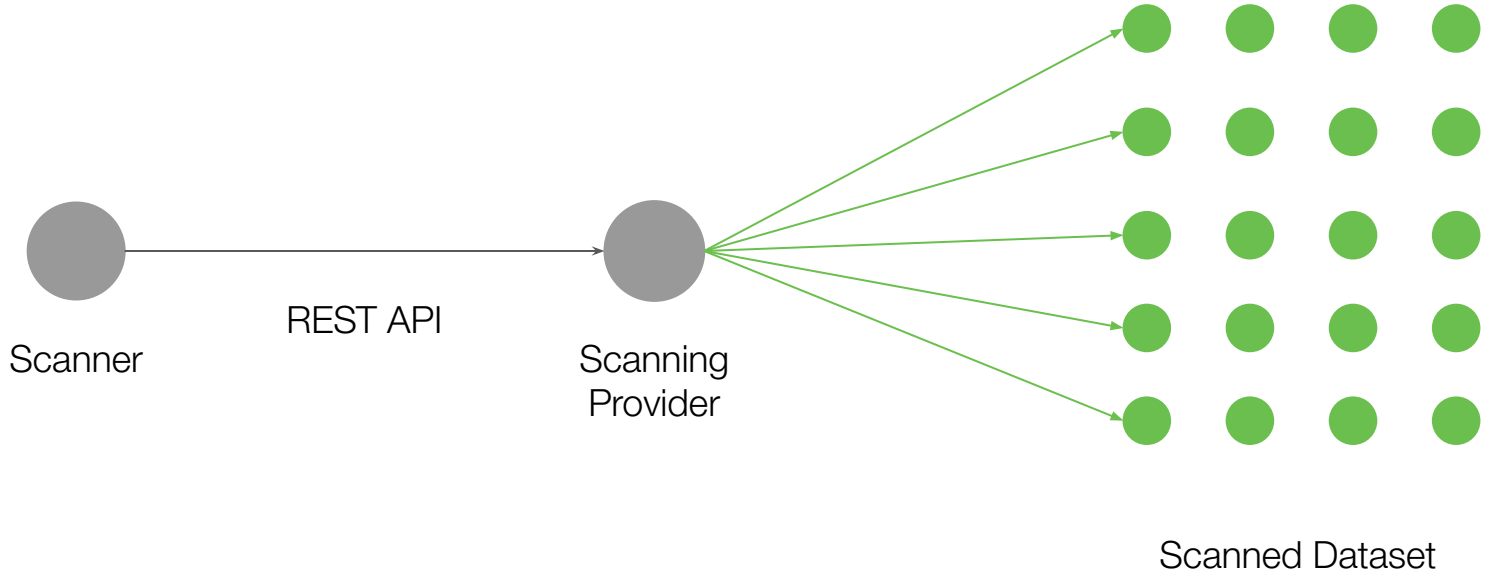
How to Find Data Leaks



How to Find Data Leaks



How to Find Data Leaks: Another Approach



There are quite a few scanning providers to choose from.

The Game Plan

- Get a list of hosts with open databases
- For every host:
  - Determine if there's potentially sensitive information exposed
  - If so:
    - Keep a record of the host
    - **(Manual)** Try and contact the owner for remediation

...I really hope this works

Let’s Code.

Next Steps

- Limited querying to determine sensitive information
- Add new data sources
- Set up daily alerts to see new hits
- When sensitive information is found, we can alert the owner
- Create regular reports on the state of the problem

Recommending solutions

Preventing Data Leaks

- Only accept connections from authorized hosts
- Enable authentication, where possible
  - Plus RBAC
- Disable unused features

Security Guides

- MongoDB
- CouchDB
- Elasticsearch (and Kibana!)
- Rsync
- S3 (and don't forget other storage services!)
- Redis

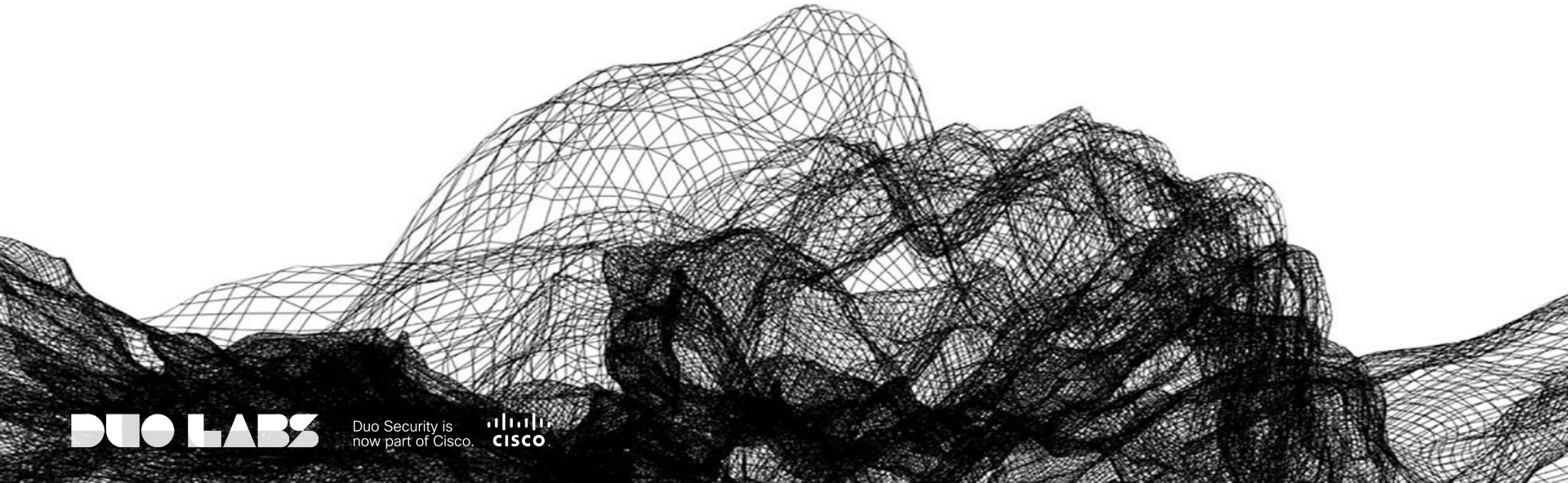
More Tools

Database	Tool Name	URL
S3	S3Scanner	https://github.com/sa7mon/S3Scanner
S3	Bucket Stream	https://github.com/eth0izzle/bucket-stream
S3 (Dataset)	N/A	https://buckets.grayhatwarfare.com/
Elasticsearch, CouchDB, RSync, and more	Leak Looker	https://github.com/woj-ciech/LeakLooker
Elasticsearch	Stretcher	https://github.com/6IX7ine/stretcher
Redis	Redis Key Analysis	https://github.com/achillean/redis-keys

Conclusion

- **You can do impactful security research**
- Open databases still exist today
- Measuring the problem gives insight into the scale of the issue
- Remediation and prevention are the goals of our work

Questions?



DUO LABS

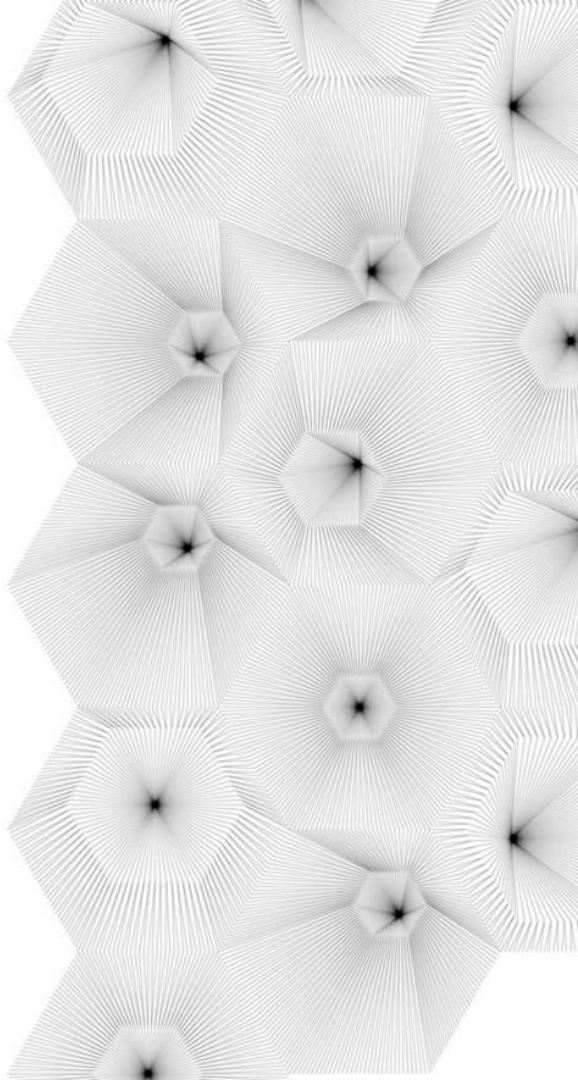
Duo Security is
now part of Cisco.

cisco

Thank you!

jwright@duo.com

@jw_sec



DUO LABS

Duo Security is now part of Cisco. cisco