FH MÜNSTER
University of Applied Sciences

ETI
FB Elektrotechnik und Informatik
Department of Electrical Engineering
and Computer Science

LanDscAPe:
Exploring LDAP Weaknesses and Data Leaks at Internet Scale

Jonas Kaspereit[1], Gurur Öndarö[1], Gustavo Luvizotto Cesar[2], Simon Ebbers[1], Fabian Ising[3,4], Christoph Saatjohann[1,3,4], Mattijs Jonker[2], Ralph Holz[2,5], and Sebastian Schinzel[1,3,4]

[1] *Münster University of Applied Sciences*
[2] *University of Twente*
[3] *Fraunhofer SIT*
[4] *National Research Center for Applied Cybersecurity ATHENE*
[5] *University of Münster*

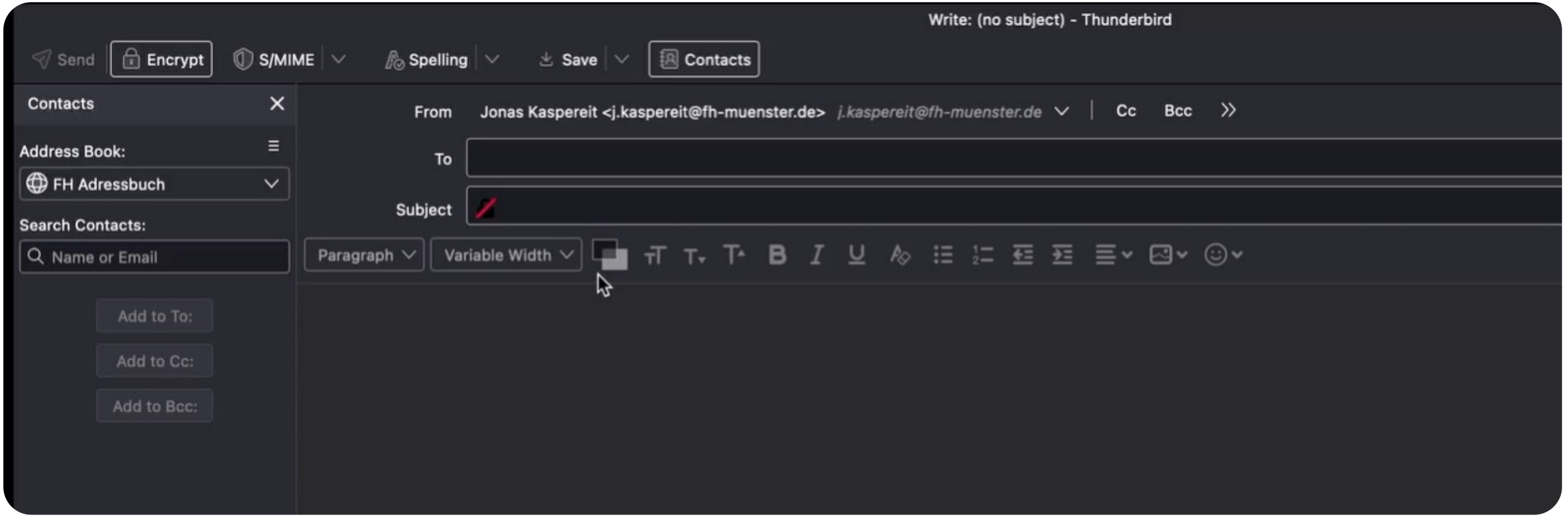
Fraunhofer SIT

NERD.NRW

ATHENE
National Research Center for Applied Cybersecurity

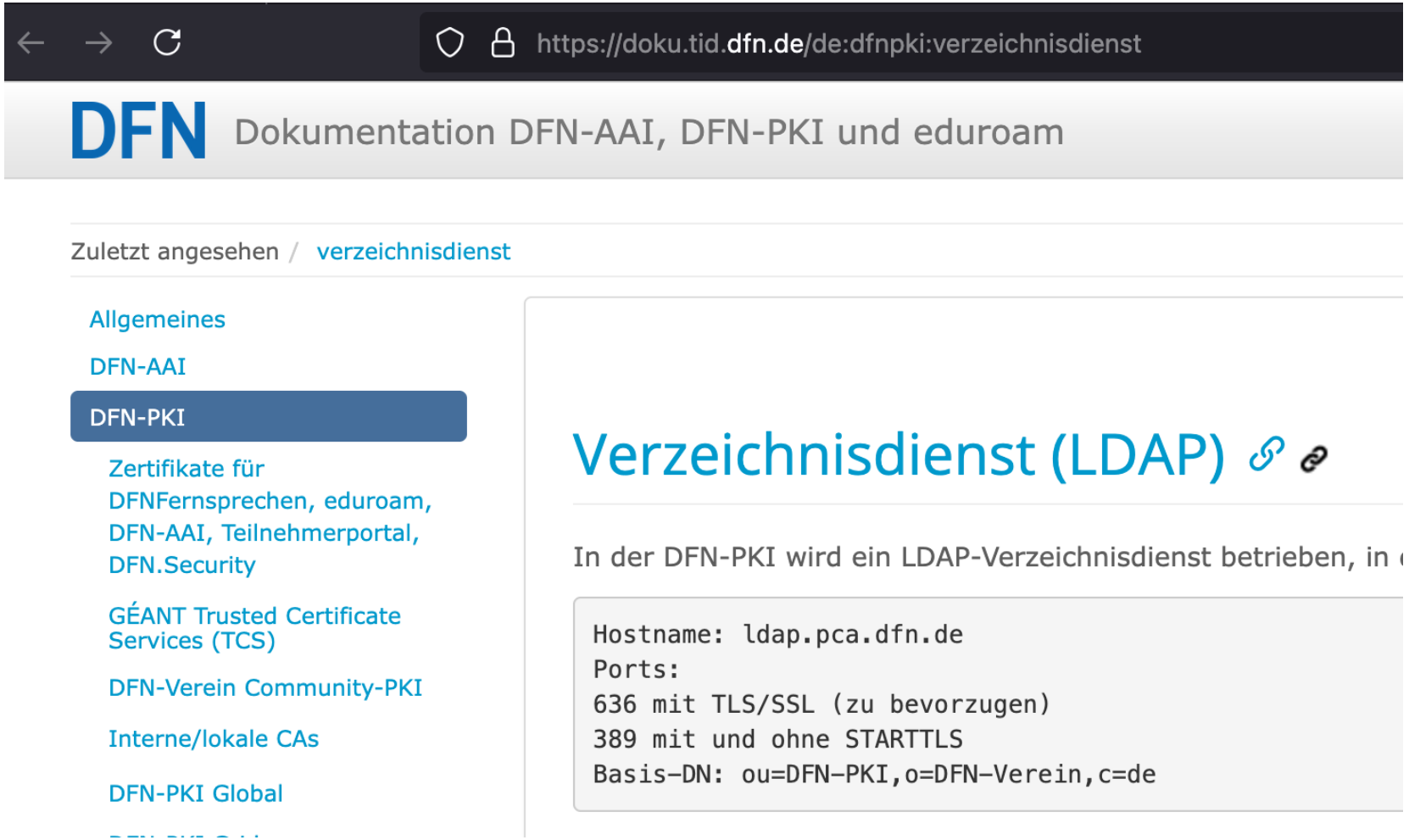
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Lightweight Directory Access Protocol (LDAP)

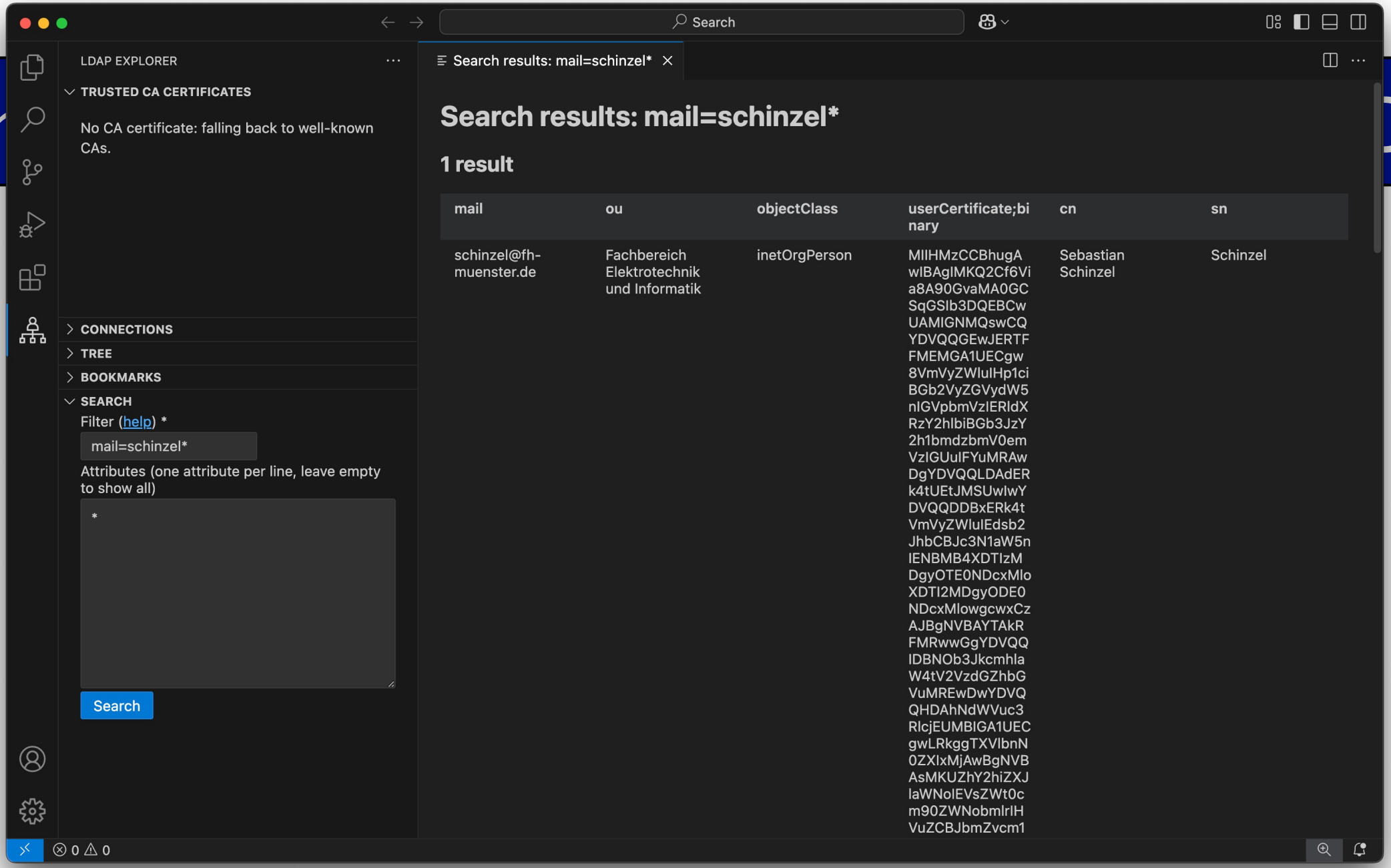


Lightweight Directory Access Protocol (LDAP)

- LDAP servers as address books.
- https://doku.tid.dfn.de/de:dfnpki:verzeichnisdienst



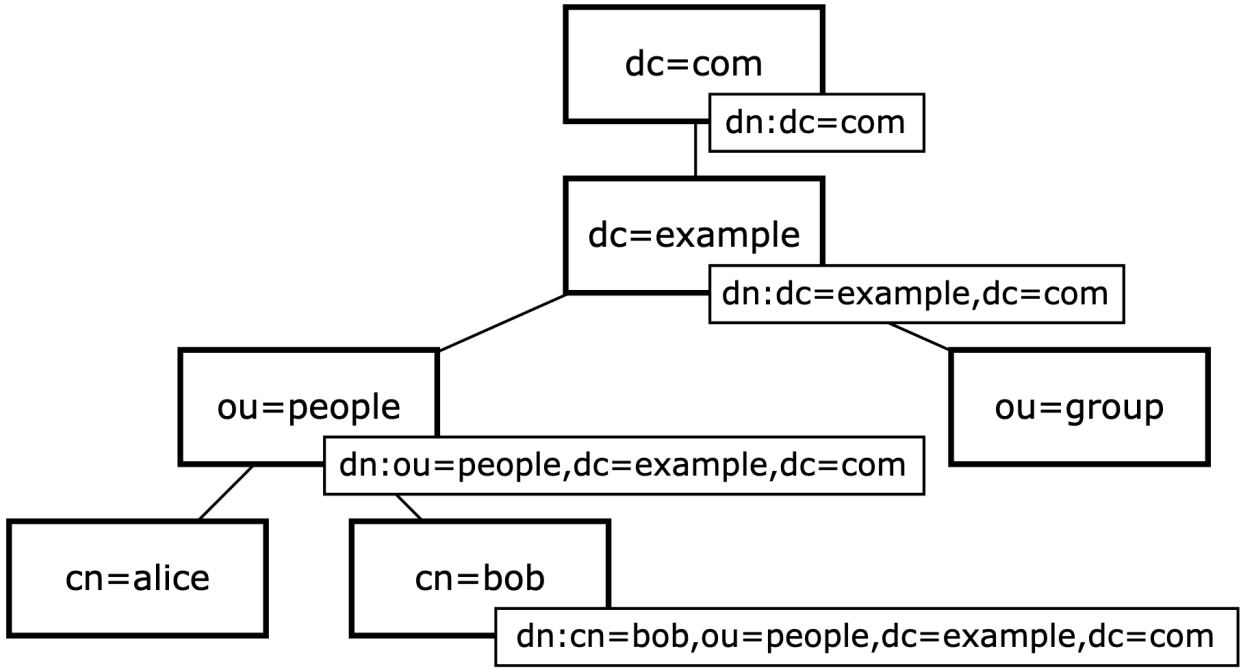
Ligh DAP)


Search
LDAP EXPLORER
TRUSTED CA CERTIFICATES
No CA certificate: falling back to well-known CAs.
CONNECTIONS
TREE
BOOKMARKS
SEARCH
Filter (help) *
mail=schinzel*
Attributes (one attribute per line, leave empty to show all)
*
Search
Search results: mail=schinzel*
Search results: mail=schinzel*
1 result
mail
ou
objectClass
userCertificate;binary
cn
sn
schinzel@fh-muenster.de
Fachbereich Elektrotechnik und Informatik
inetOrgPerson
MIIHMzCCBhugAwIBAgIMKQ2Cf6Via8A90GvaMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYDVQQGEwJERTFMEMGA1UECgw8VmVyZWlulHp1ciBGb2VyZGVydW5nIGVpbmVzIERldXRzY2hlbiBGb3JzY2h1bmdzbmV0emVzIGUuIFYuMRAwDgYDVQQLDAdERk4tUEtJMSUwIwYDVQQDDBxERk4tVmVyZWlulEdsb2JhbCBJc3N1aW5nIENBMB4XDTIzMDgyOTE0NDcxMloXDTI2MDgyODE0NDcxMlowgcwxCzAJBgNVBAYTAkRFMRwwGgYDVQQIDBNOb3Jkcmhla W4tV2VzdGZhbGVuMREwDwYDVQQHDAhNdWVuc3RlcjEUMBIGA1UECgwLRkggTXVlbnN0ZXIxMjAwBgNVBAsMKUZhY2hiZXJlaWNolEVsZWt0cm90ZWNobmlrIHVuZCBJbmZvcm1
Search
0 0

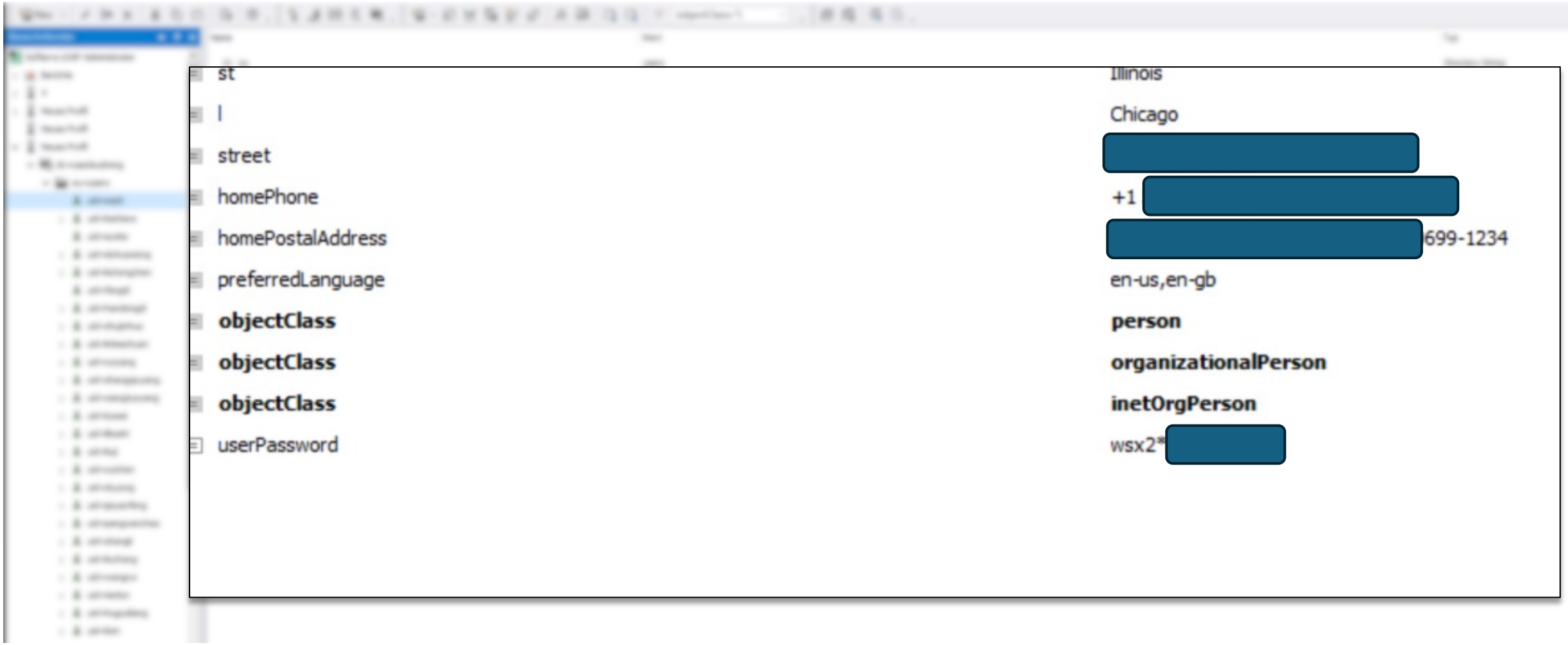
Lightweight Directory Access Protocol (LDAP)

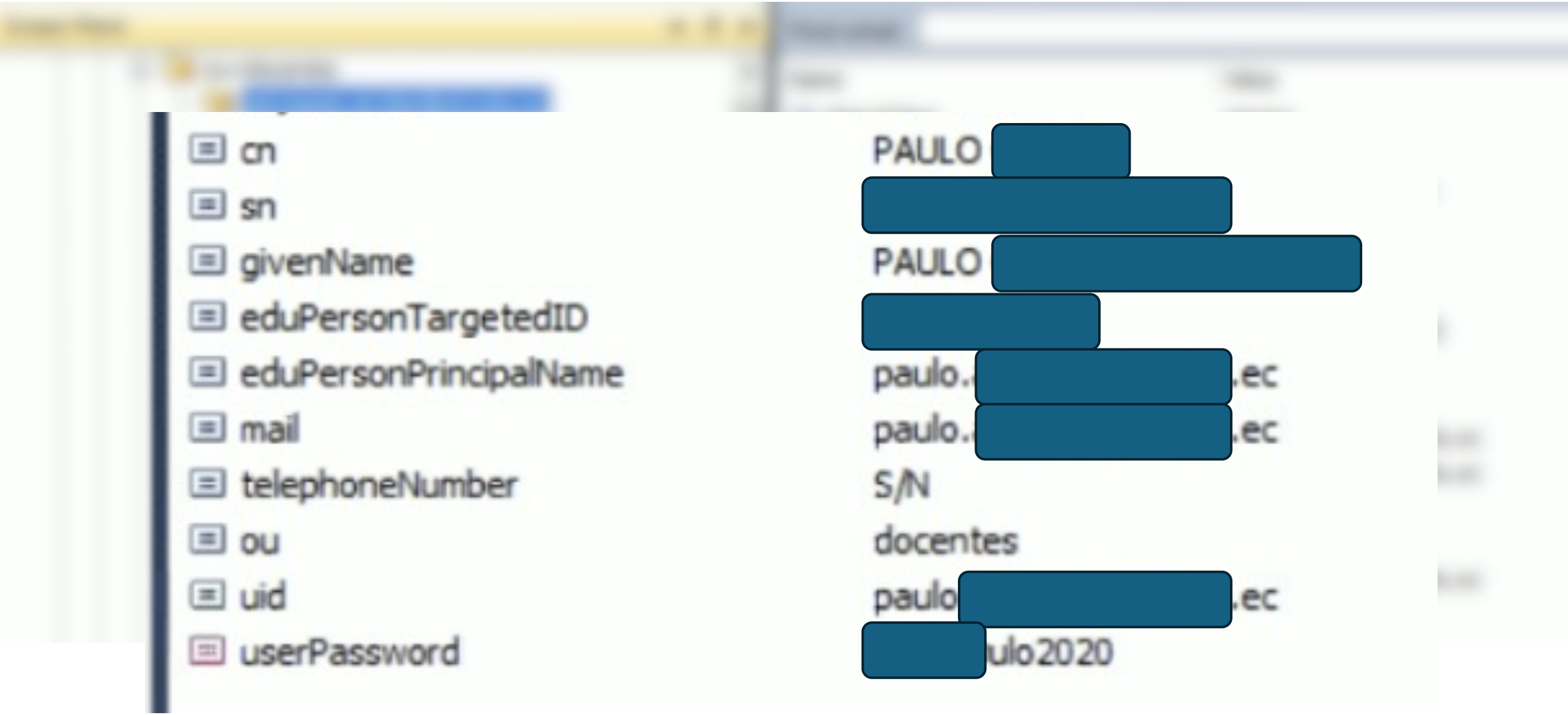
LDAP is like a weird database...
...used for

- storing personal data (address book),
- storing configuration data 😳,
- their bash history 😱,
- storing authentication information 🤯 !?

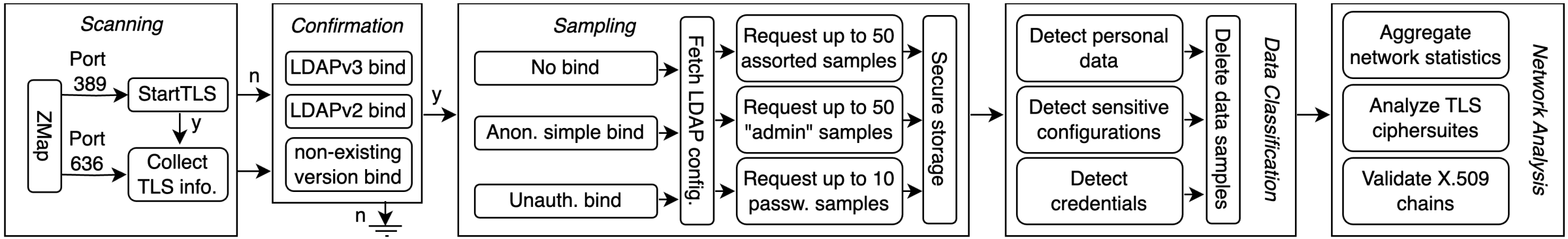


Lightweight Directory Access Protocol (LDAP)

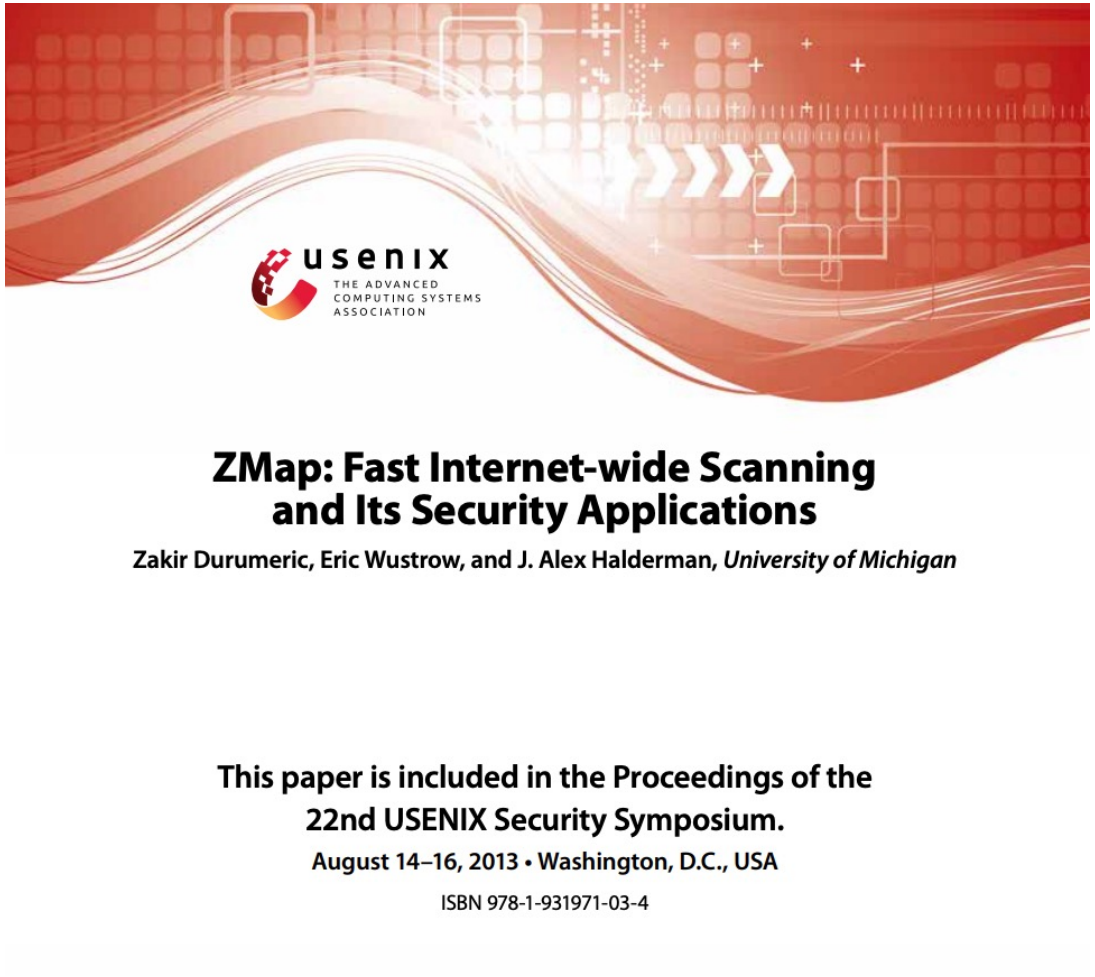



cn
PAULO
sn
givenName
PAULO
eduPersonTargetedID
eduPersonPrincipalName
paulo.
.ec
mail
paulo.
.ec
telephoneNumber
S/N
ou
docentes
uid
paulo
.ec
userPassword
ulo2020

LanDscAPe

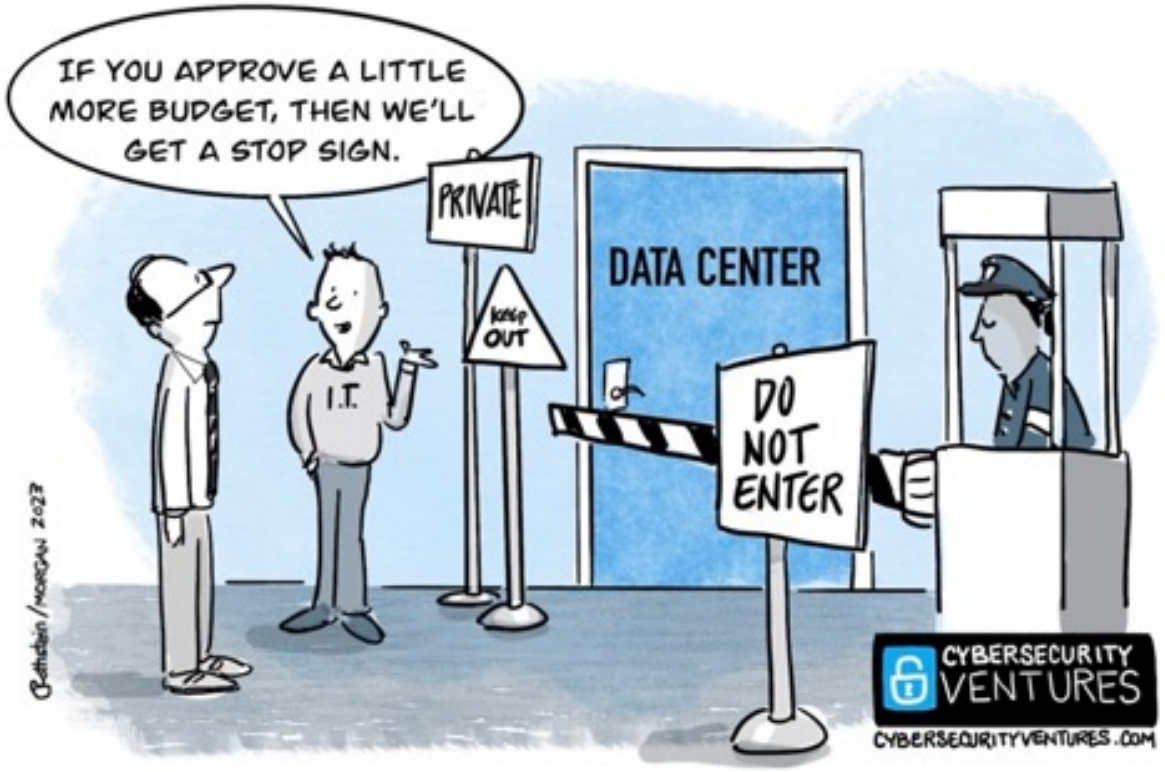

Scanning
ZMap
Port 389
StartTLS
y
Port 636
Collect TLS info.
n
Confirmation
LDAPv3 bind
LDAPv2 bind
non-existing version bind
n
y
Sampling
No bind
Anon. simple bind
Unauth. bind
Fetch LDAP config.
Request up to 50 assorted samples
Request up to 50 "admin" samples
Request up to 10 passw. samples
Secure storage
Data Classification
Detect personal data
Detect sensitive configurations
Detect credentials
Delete data samples
Network Analysis
Aggregate network statistics
Analyze TLS ciphersuites
Validate X.509 chains

Scanning and Confirmation



- 3.7 million hosts on each port (389 and 636)
- 82k positive LDAP bind request

User Data



- Limit samples
- Unique counting method
- Secured internal server with restricted access
- Data deletion
- Responsible disclosure

Sampling Module

1. Connection to Servers 2. Fetching Configurations 3. Collecting Samples

Bind Type	Root DSE	Schema	Naming Context	Passw. Policy	Samples		
					Rand.	Admin	Passw.
Total	92,588	35,658	90,265	1,432	17,283	11,715	2,935
No bind	95.04%	87.28%	94.97%	99.93%	84.02%	99.74%	99.18%
Only Simple bind	4.93%	12.69%	5.00%	0.07%	15.98%	0.26%	0.82%
Only Unauth. bind	0.03%	0.03%	0.03%	0.00%	0.00%	0.00%	0.00%

Data Classification Module

- 26,464 servers support SASL
- 9,731 servers leak internal information
- 616 servers are vulnerable to existing CVEs

Data Classification Module

- 12,179 servers leak personal data such as:
  - First name, last name
  - Birthdate
  - Address information
  - Contact information
  - And more …

Fast Track to Admin

- 1,817 LDAP servers exposed credentials
- > 32% leaked plausible plaintext passwords
- > 3.9 million credentials publicly accessible
- 526 servers leaked passwords where the username contained the substring ‘admin’

Network Analysis Module

	Total IPs	Leak credentials	Personal data	SASL support	CVE	Internal info.
Supporting TLS	48,198 (100%)	910 (100%)	7,378 (100%)	18,502 (100%)	528 (100%)	7,118 (100%)
TLSv1.3	36.67%	20.00%	27.24%	42.04%	28.41%	49.34%
TLSv1.2	59.46%	77.03%	68.91%	55.92%	71.59%	46.90%
TLSv1.1	0.33%	0.33%	0.16%	0.23%	0.00%	0.10%
TLSv1.0	3.54%	2.64%	3.69%	1.81%	0.00%	3.67%
Recommended cipher suites	65.92%	36.59%	44.20%	57.49%	94.89%	61.42%
Other cipher suites	34.08%	63.41%	55.80%	42.51%	5.11%	38.58%
... with RSA key exchange	24.27%	57.14%	53.71%	41.77%	5.11%	36.93%
... using CBC	12.26%	8.35%	6.30%	3.64%	5.11%	5.49%
... using 3DES	0.31%	0.00%	0.03%	0.00%	0.00%	0.00%
Valid Cert. Chain	36.81%	17.69%	24.10%	40.38%	32.20%	47.78%
Invalid Cert. Chain	63.19%	82.31%	75.90%	59.62%	67.80%	52.22%
... Self-signed	32.30%	21.87%	22.61%	16.53%	1.70%	10.97%
... Expired/not yet valid	19.65%	43.63%	35.52%	25.15%	6.63%	14.34%
... Unknown authority	11.20%	16.70%	17.74%	17.91%	59.28%	26.89%

Mitigations

Disclosure Campaign February 2024

- 475 (26.1%) of credential-leaking servers are no longer available
- 5 servers are requiring authentication now

Conclusion

Findings

- Out of 80,000 servers, 12,000 are leaking personal data.
- Around 3.9 million user credentials, including cleartext passwords, are exposed.
- Most LDAP servers have no proper TLS configuration.

Conclusion

Lessons Learned

- LDAP Server are valuable target for attackers.
- Organization must secure or even remove their LDAP servers from public access.

FH MÜNSTER
University of Applied Sciences

Thank You!

Sebastian Schinzel
schinzel@fh-muenster.de

Jonas Kaspereit
j.kaspereit@fh-muenster.de

Gurur Öndarö
gurur.ondaro@fh-muenster.de

Our Paper

SCAN ME

Fraunhofer SIT

ATHENE
National Research Center for Applied Cybersecurity

Graduiertenkolleg "Human Centered Systems Security"
NERD.NRW

Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen