Ecosystem Overview

Most Common Threats and Attacks

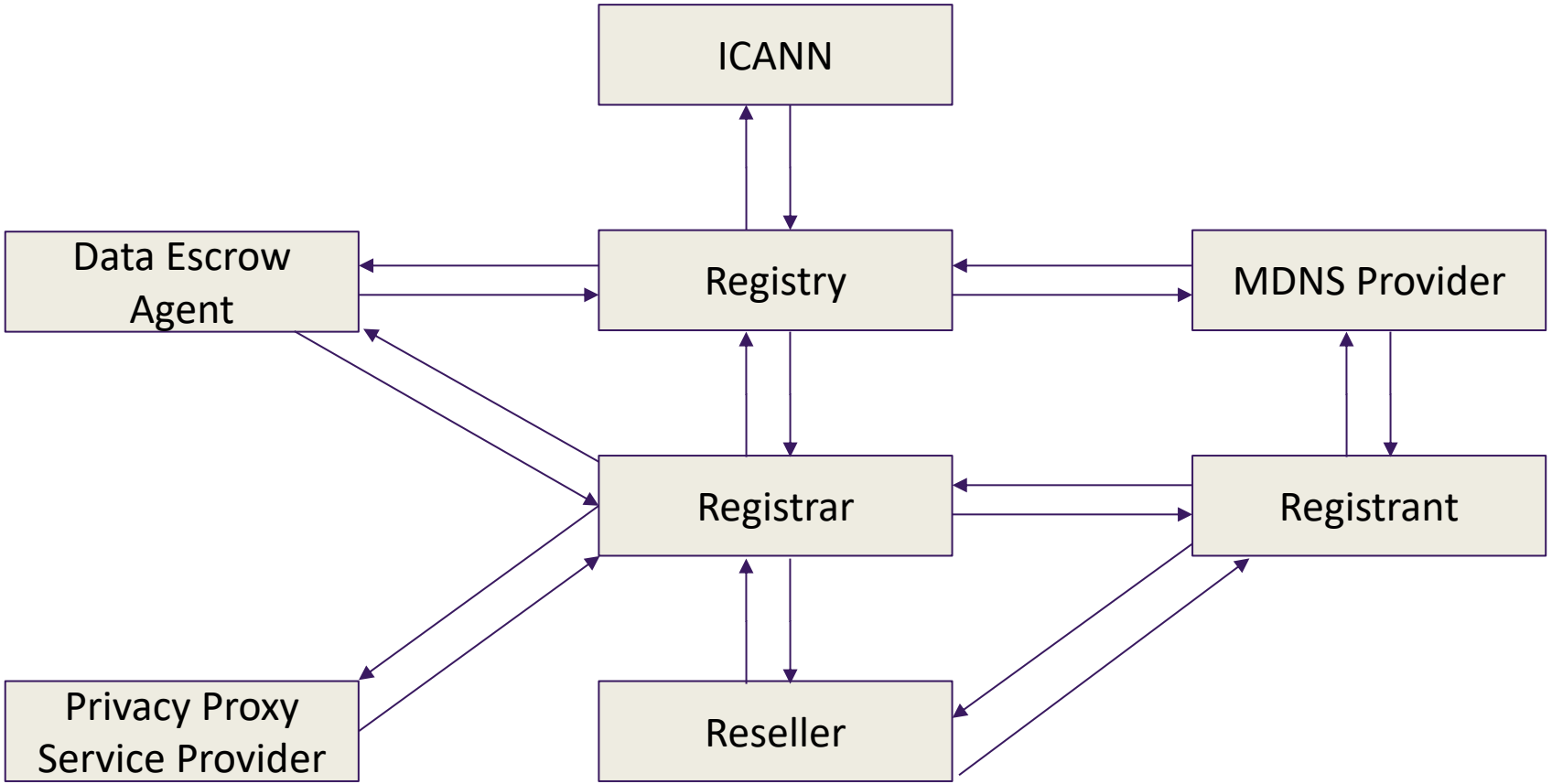
- Unauthorized access
  - Thru insecure hosts or password cracking
- Eavesdropping
  - Looking for passwords, credit card numbers, or business secrets
- Hijacking (i.e. taking over communications)
  - Inspect and modify any data being transmitted
- IP spoofing (i.e. faking network addresses)
  - Impersonate to fool access control mechanisms
  - Redirect connections to a fake server
- DOS attacks
  - Interruption of service due to system destruction or using up all available system resources for the service (CPU, memory, bandwidth)

DNS Abuse Is Rising

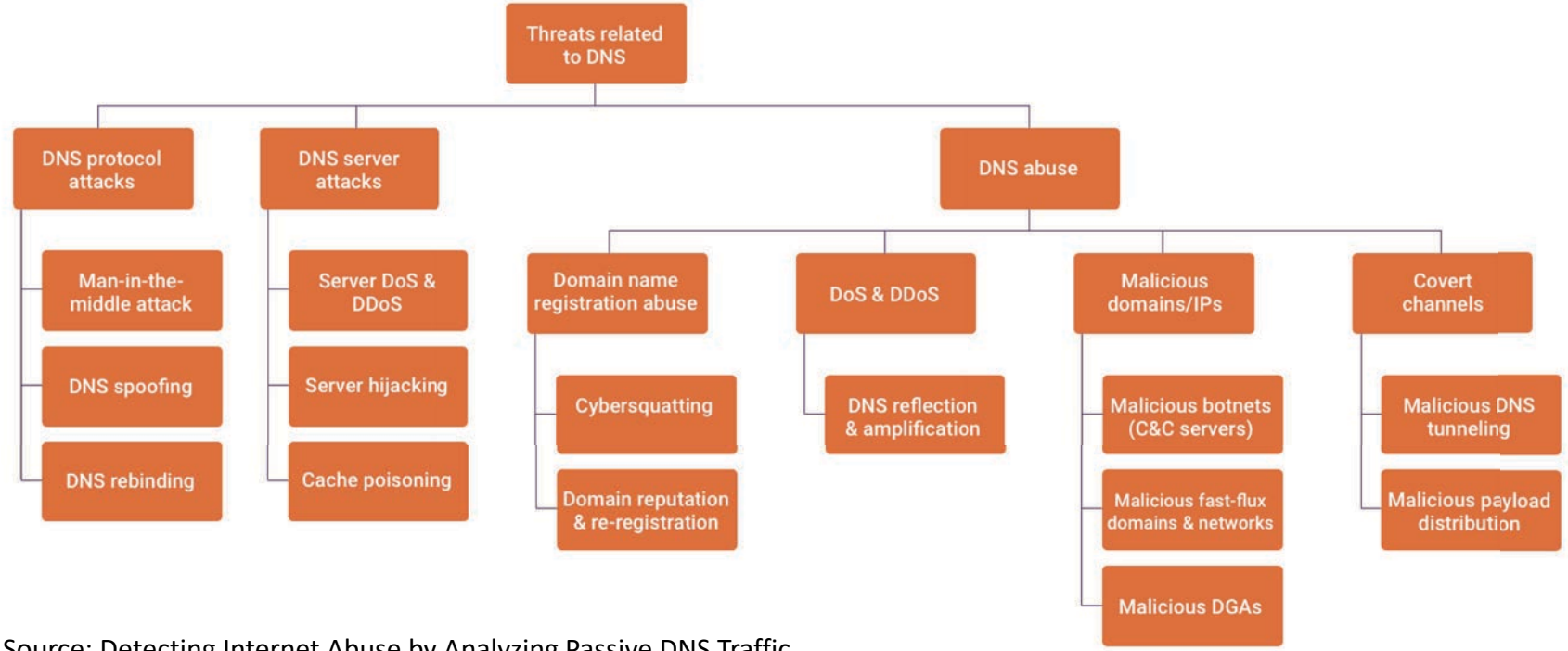
What Is Changing ?

- Same Fundamental Security Controls
  - User/Device Authentication
  - User/Device Authorization
  - Data Integrity
  - Data Confidentiality
  - Auditing/Logging
  - DoS/DDoS Mitigation
- What Is Different
  - Scale
  - Automation
  - Sophistication
  - Impact

DNS Ecosystem (People & Process)

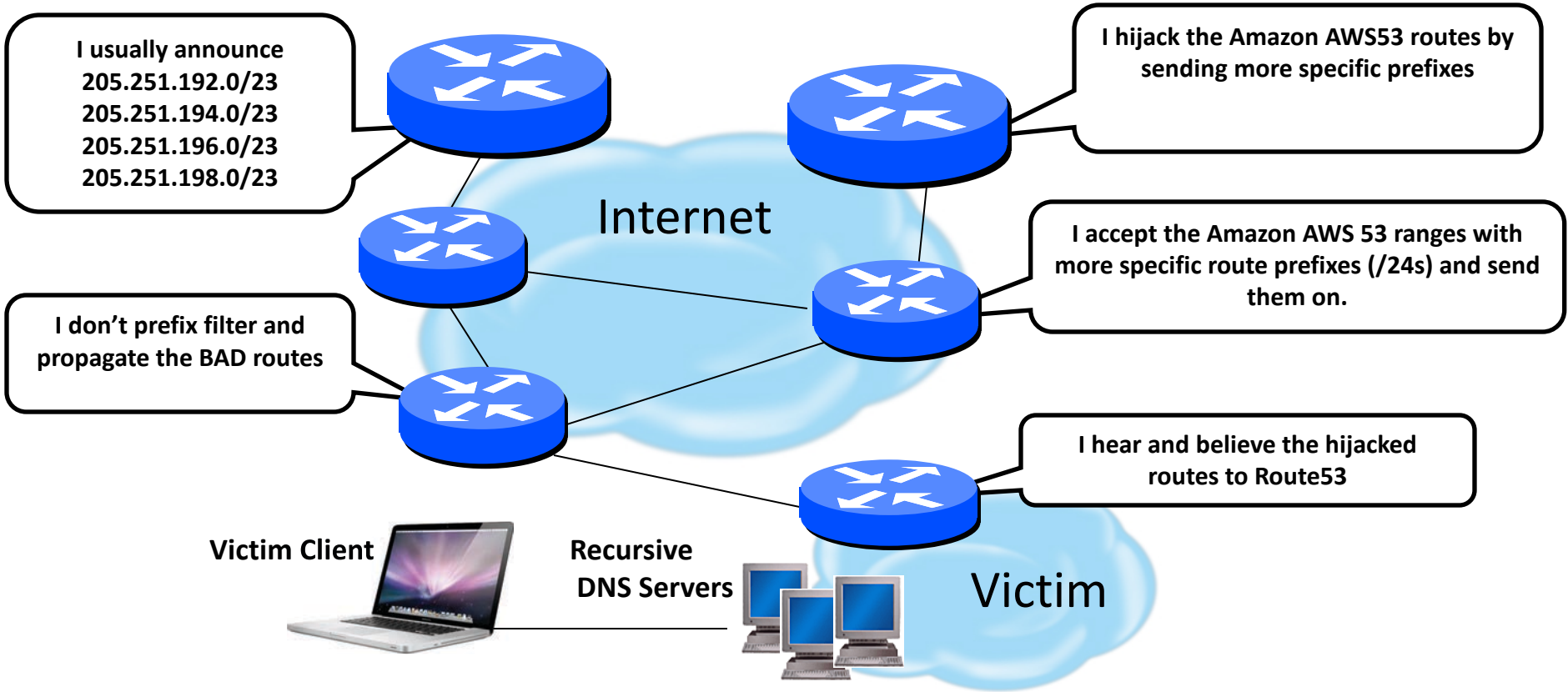


DNS Ecosystem Technical Threats

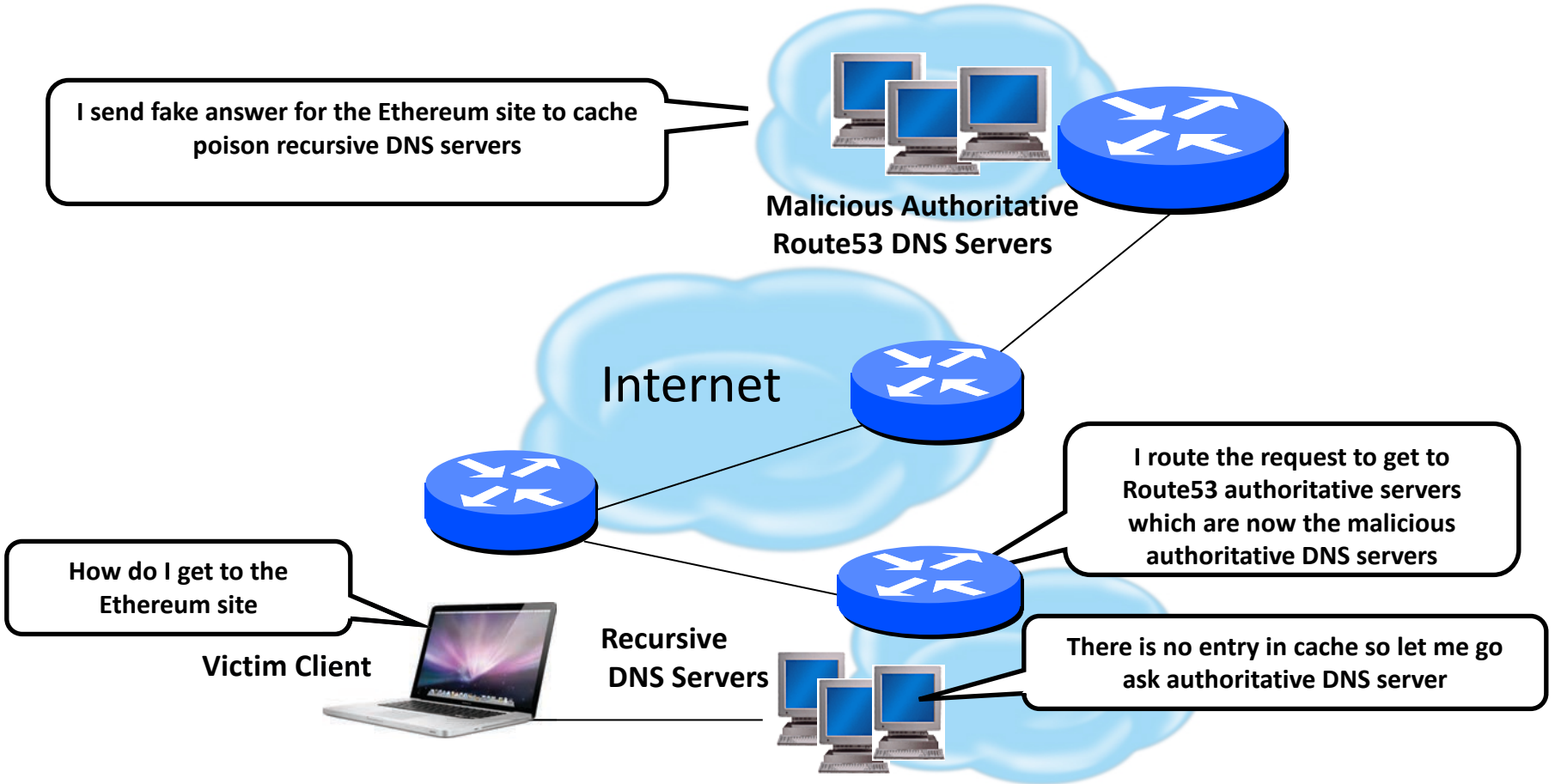


Source: Detecting Internet Abuse by Analyzing Passive DNS Traffic
(Sadegh Torabi, Amine Boukhtouta, Chad Assi, and Mourad Debbabi)

Using Routing to Poison DNS Cache



Using Routing to Poison DNS Cache



Exploiting CPEs to Change Resolver DNS

scan → Find vulnerable CPE → Change password (PW=0Wn3D) → Change CPE DNS Servers (DNS=bad server)

Change CPE DNS Servers → DNS incorrectly resolves names for high profile sites

DNS incorrectly resolves names for high profile sites → redirected to a page with links to a malware that disables banking protections

redirected to a page with links to a malware that disables banking protections → Once the protection is disabled, DNS incorrectly resolves names for several banks (for short periods of time)

Mitigation – Basic Cyber Hygiene (NOT JUST DNS)

- Keep up with vulnerabilities
- Review and apply all system security patches
- Review log files for unauthorized access to systems, especially administrator access
- Enforce good credential management lifecycle practices
- Ideally ensure multi-factor authentication is enabled to all systems, especially for administrator access

Mitigation – DNS Basic Hygiene

- Use physically different machines for authoritative and recursive functions
- Use multiple authoritative servers to distribute load and risk:
- Put your name servers geographically apart from each other
- Utilize caches to reduce load to authoritative servers and reduce response times

Mitigation – DNS Basic Hygiene (cont.)

- Limiting views to control what data systems can be known
- Restrict resolution to specific address ranges if needed
- Be wary of incorrect use and monitor authoritative name servers to ensure correct behavior
- Use techniques to assure authoritative answers come from expected source and that noone has been able to modify the answer in transit

SSAC Advisories

- SAC004 – Securing The Edge
- SAC007 - Domain Name Hijacking Report [speaks to Registrar-Lock and appropriate authentication controls]
- SAC008 – DNS Distributed Denial of Service (DDoS) Attacks
- SAC010 - Renewal Considerations for Domain Name Registrants
- SAC011 - Problems cause by non-renewal of a domain name associated with a DNS Name Server
- SAC015 - Why Top Level Domains Should Not Use Wildcards
- SAC025 - SSAC Advisory on FastFlux Hosting and DNS
- SAC028 - SSAC Advisory on Registrar Impersonation Phishing Attacks
- SAC032 - Preliminary Report on DNS Response Modification [NXDomain redirect]

SSAC Advisories

- SAC040 - Measures to Protect Domain Registration Services Against Exploitation or Misuse
- SAC041 - Recommendation to prohibit use of redirection and synthesized responses by new TLDs
- SAC044 - A Registrants Guide to Protecting Domain Name Registration Accounts
- SAC049 – SSC Report on DNS Zone Risk Assessment and Management
- SAC057 - SSAC Advisory on Internal Name Certificates
- SAC074 - SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle

Best Practices for Credential Management (one version)

Types of Credentials

- Passwords/Passphrases
- Digital Certificate
  - Used in public key and private key scenarios that enable encryption, authentication and digital signatures.
- Security tokens
  - Typically one-time-passwords or PINs generated via a physical device (e.g. hardware token) or via a program running on a computer (e.g. software token).
- Biometric attributes
  - Identify a user by a feature of their biology, including fingerprints or iris scans.

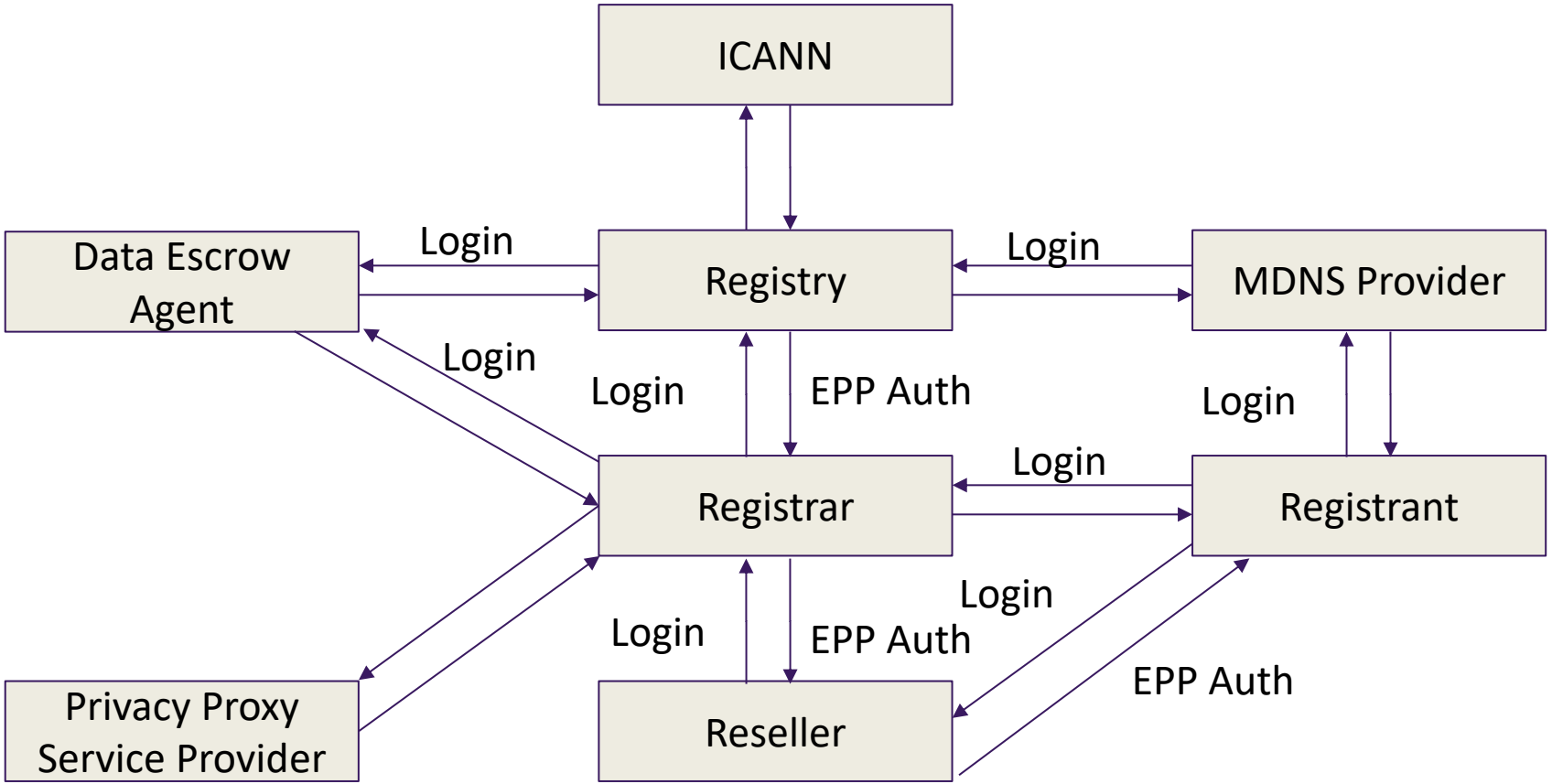
DNS Ecosystem Credential Types and Purpose

Credential	Purpose of Credential	Entity Using Credential	Entity Validating Credential
EPP AuthInfo code	Initiate registrar-to-registrar transfer	Registrant, Registrar/Reseller	Registry
Registrant username and password at registrar/reseller	Access to domains, DNS settings, payment methods, etc.	Registrant	Registrar/reseller
Username/password and certificate for registry access	Gives registrar access to TLD registry. SSL certificate and encryption required for communication between the Registrar's client system and the registry; authentication by user/pass required for session establishment.	Registrar	Registry
IP Addresses	Controls access to registry; access is restricted from known registrar IPs via address filter.	Registrar	Registry
Payment credentials (credit card number and CVV code, etc.)	Pay for services	Registrant	Registrar/Reseller, payment processor
Privacy/proxy account	Privacy/proxy services are designed to mask data about the registrant and other domain contacts so that it is not published in WHOIS. Data about the underlying contact is stored at the service provider, which may or may not be associated with the domain registrar.	Registrant, Registrar, Privacy/proxy service provider	Registrant, Privacy/proxy service provider

DNS Ecosystem Credential Types and Purpose(2)

Credential	Purpose of Credential	Entity Using Credential	Entity Validating Credential
Registrar account funding credentials. May involve bank account numbers, credit card account details, etc.	Transaction accounts at registries; each time the registrar performs a billable transaction.	Registrar, Registry	Registry, bank
Registry-registrar security passphrases and service usernames and passwords.	Authenticate the registrar's requests to tech support, finance department, etc.	Registrar	Registry
Registrar-registrant - security passphrases, PIN numbers, and service usernames and passwords.	Authenticate the registrant's requests to the registrar.	Registrant	Registrar
Credentials for access to registry's or registrar's internal systems or hardware	May involve usernames/passwords; firewalls and VPNs; and/or two-factor methods such as security tokens, biometrics, ID documents, etc.	Registrar or Registry	Registrar or Registry
DNSSEC Key-Signing Key (KSK)	A key that signs the set of all keys for a given zone, including itself	Registrants, Registrars and Registries	Registrants, Registrars, and Registries
DNSSEC Zone-Signing Key (ZSK)	A key hat signs data within a given zone	Registrants, Registrars and Registries	Registrants, Registrars, and Registries

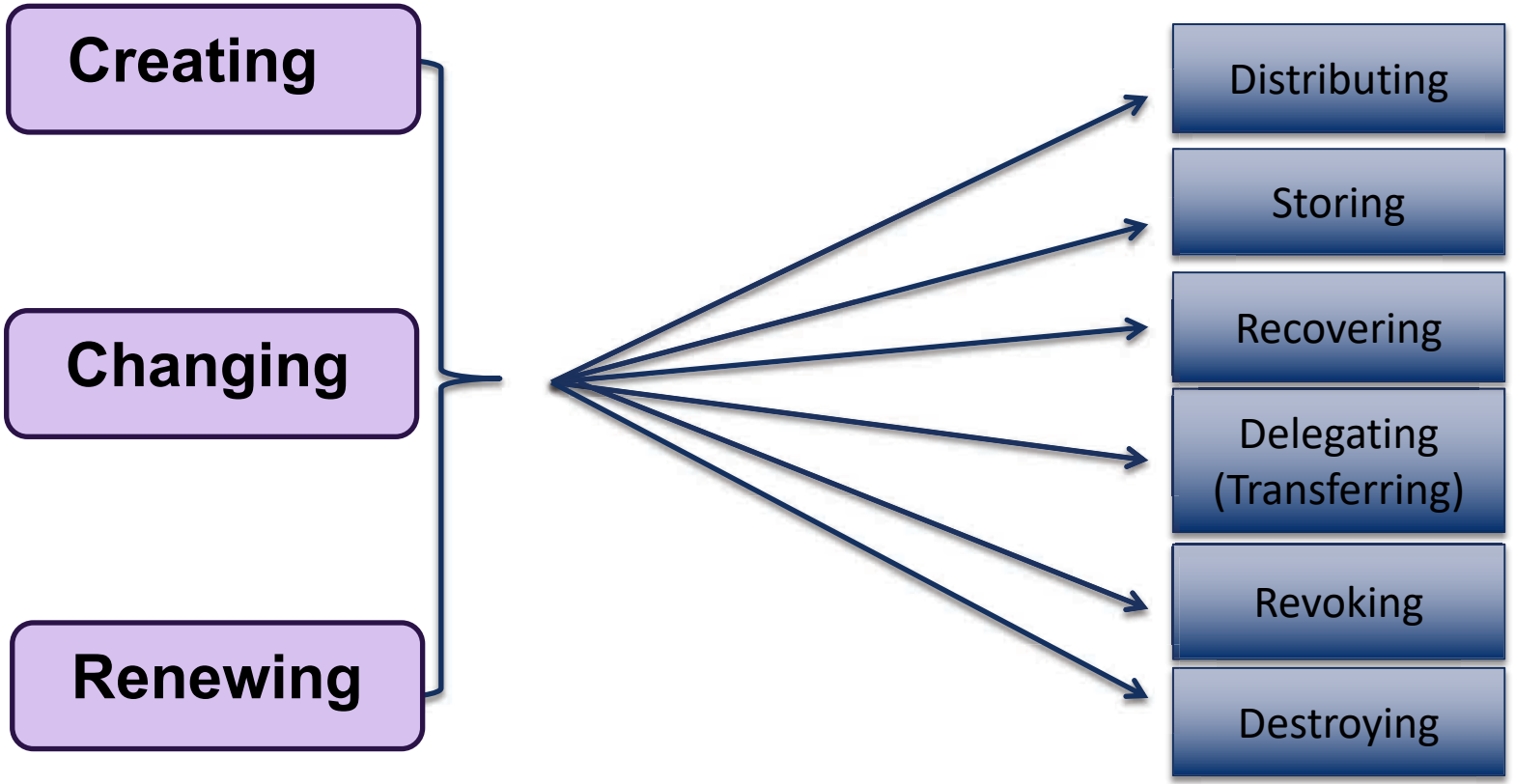
DNS Ecosystem Credentials



How Credentials Get Compromised

- Being victim of a phishing attack
- Laptop gets stolen
- Sharing your password with another person
- Re-using same password on many systems
- Spyware on your computer installed a keylogger
- Storing your private key in an easily accessed file
- Sending credentials in cleartext emails
- Unpatched security vulnerabilities are exploited

Credential Management Lifecycle



Avoiding Surprises

- Check to see whether systems log passwords in clear text on authentication attempts
- Some systems may have configuration files that store passwords and/or shared secrets in cleartext
- Make sure you know how backups are done and how credentials stored for backups
  - Cloud storage specifically important
  - If you use mobile devices know what is backed up, where, and how.

Questions to Consider

- Do you do multi-factor authentication and if not why not?
- How do you store credentials and how/where do you perform your backups?
- What do you do with credential of users who aren't customers any more?
- Do you rotate credentials and if not why not?
- Do you force customers to change their passwords?
- What do you consider adequate for password strength and username types?

Questions to Consider (2)

- What type of system are you using for password recovery? What are the options to authenticate the entity?
- How do you ensure customer compliance?
- What kind of know-your-customer programs do you have to review credentials and make sure everything is up to date?
- What kind of measures do you employ to detect compromised credentials, or attempts to compromise them (e.g. brute-force attacks)?

Credential Management Best Practices

- Know ALL Credentials That Are Utilized
- Limit Fate Sharing
- Encourage Use of Multifactor Authentication
- Do NOT Send/Store Credentials In Cleartext
- Create Processes For Credential Changes
  - Identity Verification Is Critical Component
- Know Where You Are Storing Credentials

Multi-Factor Authentication

- Multi-factor authentication provides added layer of protection
- Varying types of MFA
  - Universal 2nd Factor (U2F)
  - Time based onetime passwords (TOTP)
  - HMAC-based onetime passwords (HOTP)
  - SMS Passcode
  - Phone Based Verification
- One good registry study is from Brazil
  - https://community.icann.org/display/CMTP/How+to+Guides

Registry Lock

- Enable registry lock when available
- Registry locks must be disabled to make changes to records
- Not all registries or registrars support registry locks
  - Often comes at an extra charge
- Area for future work: registry lock process standardization

Audit and Monitor

- Monitor for unauthorized access attempts
- Monitor unauthorized infrastructure changes
  - Authoritative servers
  - Recursive resolvers
- Monitor DNS data
  - Name server records
- Monitor TLS certificate transparency logs
- Monitor DNSSEC validation failures