Why Security MUST Matter

Merike Kaeo
merike@doubleshotsecurity.com

We Have Blind Trust Issues

- Protocol Standards
- Implementation Guidelines
- Device Certifications
- Compliance Mandates
- Documented Policies

But…There's The Human Factor

You can do everything right and still screw up

Question the status quo

Global Criminal Behavior is Rampant

DDoS Attack Takes Down Central Heating System Amidst Winter In Finland

Wednesday, November 09, 2016 Mohit Kumar

Tweet G+ Share Share 37 Share 680 Share 2.08k Share

Hacker Shuts Down Apartments' Heating System

Indiana healthcare group hit by third-party data breach

James Walker 11 January 2019 at 14:39 UTC

Healthcare Data Breach

Bodybuilding.com discloses security breach

Company blames February 2019 security breach on phishing email received in July 2018.

By Catalin Cimpanu for Zero Day | April 22, 2019 -- 18:14 GMT (19:14 BST) | Topic: Securit

Marriott says as many as 500 million Starwood guests' data may have been breached

Mike Snider | USA TODAY
Published 4:13 PM EST Nov 30, 2018

As many as 500 million people who made r
their personal information accessed in a br

Millions of Toyota Customers in Japan Hit by Data Breach

By Eduard Kovacs on March 29, 2019

Share Tweet Recommend 15 RSS

Personal information belonging to millions of Toyota customers in Japan may have been compromised as a result of a breach suffered by a Toyota Motor Corporation (TMC) sales subsidiary and its affiliates.

An investigation into the incident is ongoing, but Toyota said unauthorized access had been detected on March 21 on a server storing information on 3.1 million customers. The exposed data included names, addresses, dates of birth, occupation and other information. Payment

29 MAR 19 A Month After 2 Million Customer Cards Sold Online, Buca di Beppo Parent Admits Breach

On Feb. 21, 2019, KrebsOnSecurity contacted Italian restaurant chain **Buca di Beppo** after discovering strong evidence that two million credit and debit card numbers belonging to the company's customers were being sold in the cybercrime underground. Today, Buca's parent firm announced it had remediated a 10-month breach of its payment systems at dozens of restaurants, including some locations of its other brands such as **Earl of Sandwich** and **Planet Hollywood**.

British Airways boss apologises for 'malicious' data breach

7 September 2018 Share

We Need To Get Back To Basics

- Incident Response / Crisis Plan
  - Routing and DNS Compromise
- Vulnerability Disclosure/Patch Plan
- Fundamental Security Controls
  - User Authentication/Authorization
  - Device Authentication/Authorization
  - Access Control (Packet/Route Filtering)
  - Data Integrity
  - Data Confidentiality
  - Auditing / Logging
  - DoS Mitigation

Most Basic Security Controls Minimize Impact Of Sophisticated Attacks

- Don't rely on defaults
- Implement 2FA
- Use cryptographically protected protocols
- Get alerted for unauthorized changes

Balance Convenience vs Security vs Privacy

- Access to all data by default
- Sharing data with anyone who wants it

- Authentication
- Authorization
- Access Control
- Integrity
- Confidentiality
- Availability

- Internet Access
- Online Privacy
- Freedom of Expression

Fundamental Building Blocks

- Routing
- Domain Name System
- Public Key Infrastructure
- Credential Management
- Humans

- Identity must be hard to impersonate
- How is identity validated?

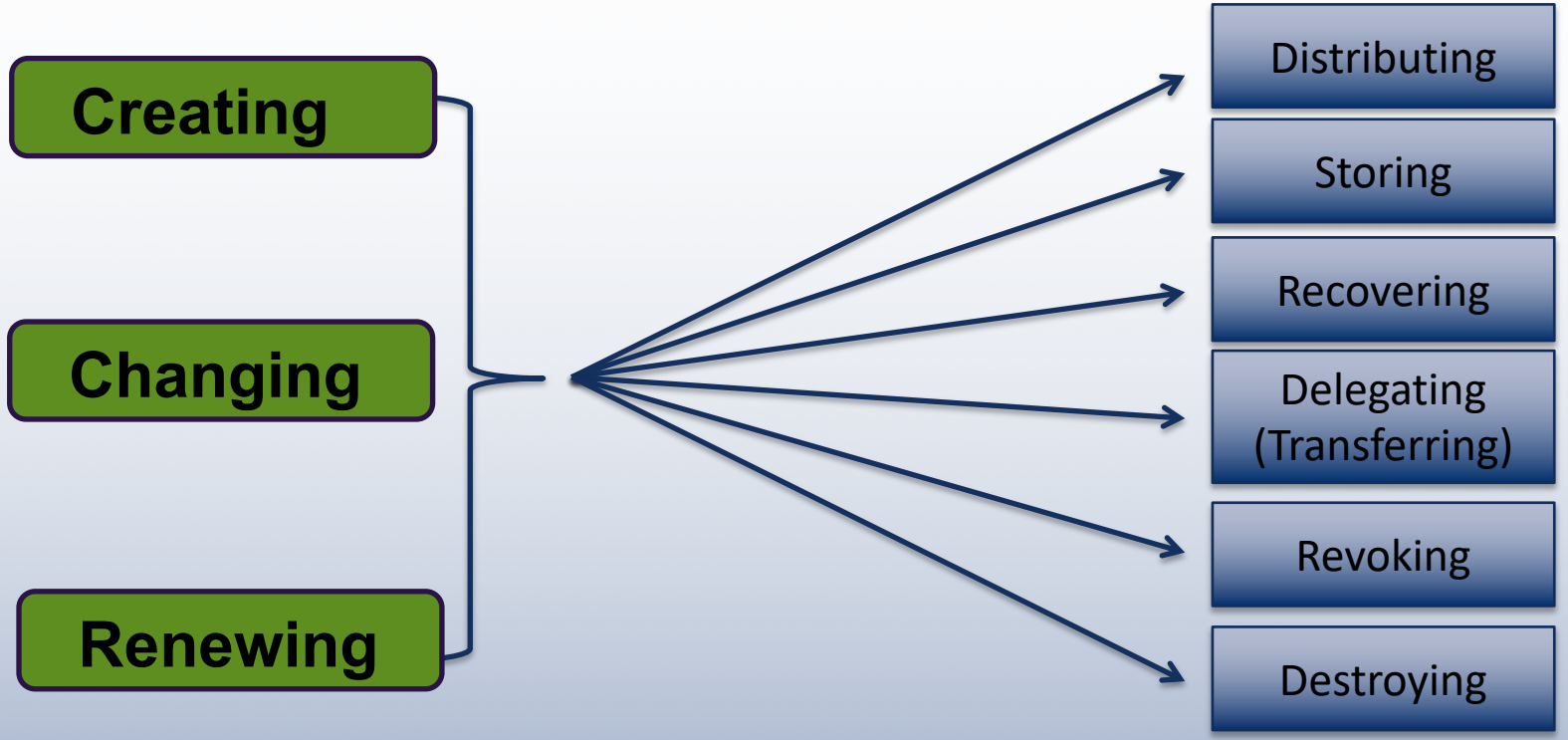
- Integrity of data
- Confidentiality of data

- Audit changes
- Who has seen the information?
- Early warnings

Stealing Credentials is Too Easy

	HUMAN	TECH
• Being a 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 cleartext on authentication attempts
- Some systems may have configuration files that store passwords and/or shared secrets in cleartext
- Employ measures to detect compromised credentials, or attempts to compromise them (e.g. brute-force attacks)
- Make impersonation difficult thru solid identity validation processes
- 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

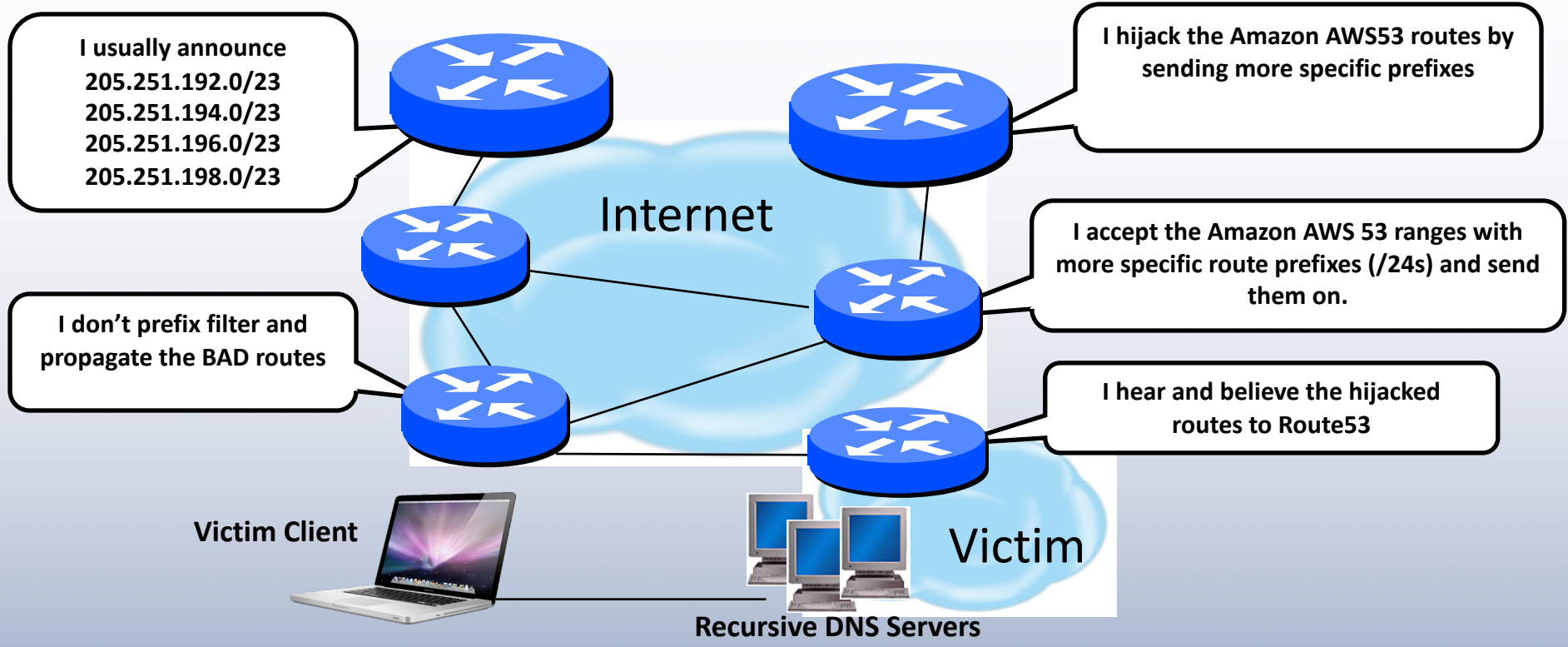
Validating Identity

- 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

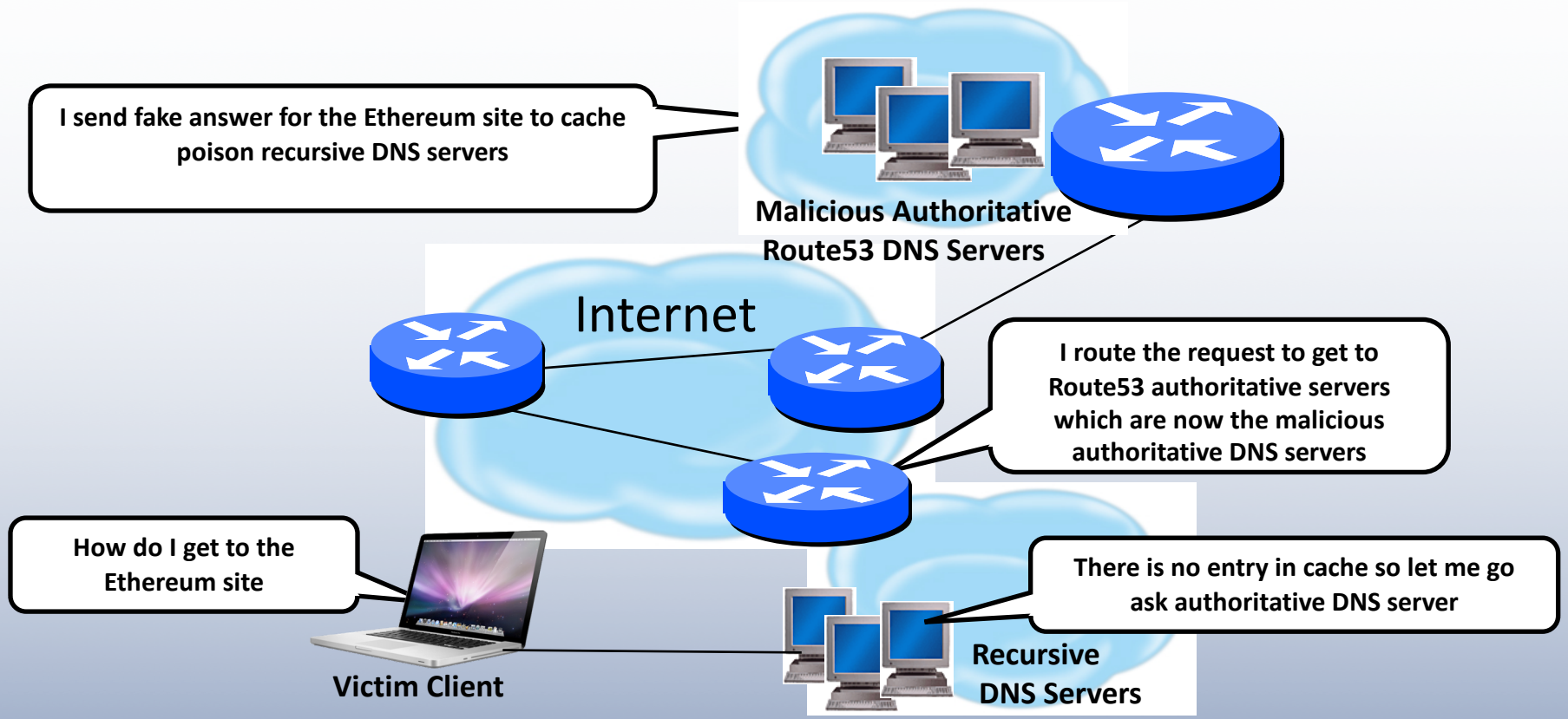
Sophisticated Infrastructure Attacks

- April 2018 - Amazon route ***prefixes*** were ***hijacked***
- Amazon's Route53 DNS traffic was re-routed towards a malicious DNS server
- The malicious DNS authoritative server had a ***legitimate IP address***
- These malicious DNS authoritative servers sent DNS answers back to DNS resolvers that pointed to malicious sites (i.e. cache poisoning)
- Traffic to any query to DNS resolvers that asked for names handled by Route53 would route to malicious sites
- Intent was to ***take over Ethereum cryptocurrency wallets***

Route Hijack....But Wait, There's More....



DNS Compromise Due To BGP Route Hijack

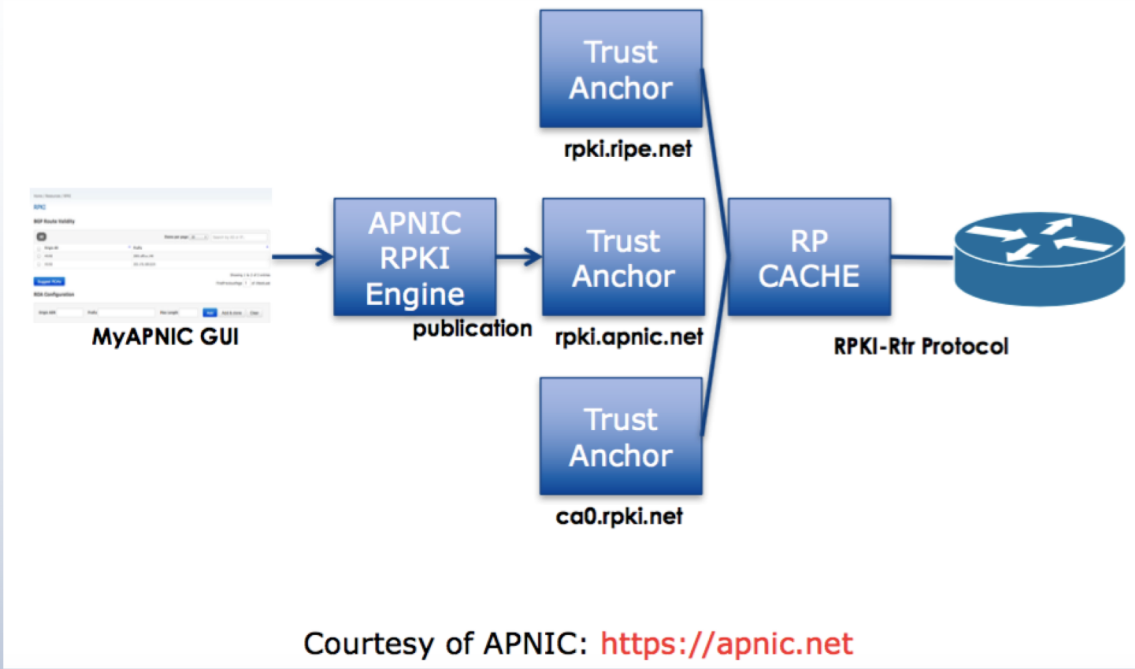


Basic Attack Mitigation Techniques

- Route hijack would not have been possible if there had been effective BGP Prefix Filtering
  - Most environments do NOT filtering comprehensively
  - ISPs should be filtering customer's prefixes
  - ISPs should be filtering prefixes going out of their network
- RPKI (Resource Public Key Infrastructure) helps mitigate route hijacks by a prefix that originated from an AS without authorization
- Recursive DNS server cache poisoning would not have been possible if DNSSEC had been deployed

Routing Security - RPKI

- Origin authentication
- Who owns an IP Prefix and which AS(s) may announce it
- Prevents route-hijacking
- Prevents mis-origination
- Route Origin Authorization
  - Digital object that contains a list of IP prefixes and one AS number
  - Authorizes an AS number to originate one or more specific route advertisements

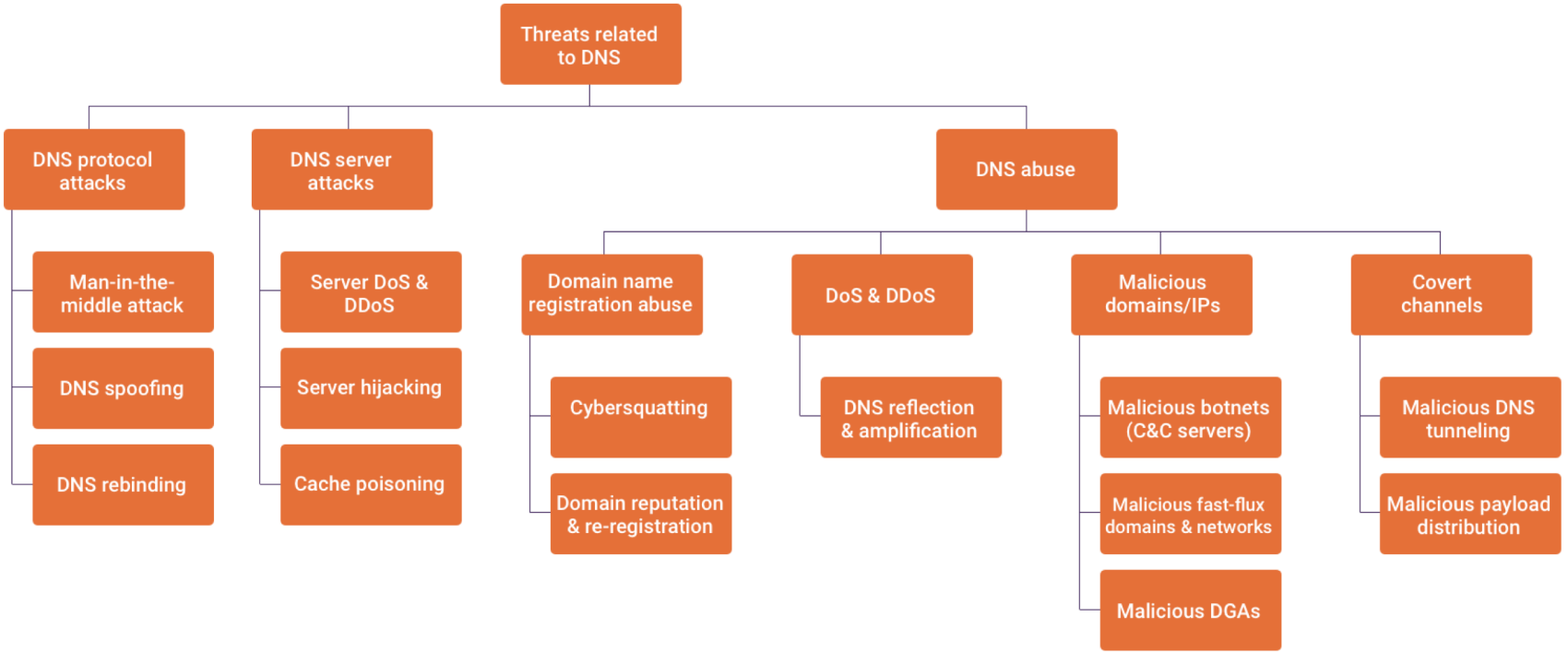


Routing Security - MANRS

- Prevent propagation of incorrect routing information
  - Filter BGP peers, in & out
- Prevent traffic with spoofed source addresses
  - BCP38 – Unicast Reverse Path Forwarding
- Facilitate communication between network operators
  - NOC to NOC Communication
- Facilitate validation of routing information
  - Route Origin Authorisation using RPKI

https://www.routingmanifesto.org/manrs

DNS Ecosystem Technical Threats



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

Why Criminals Register Domain Names

- Often Done At High Volumes
  - Phishing sites
  - Ransomware payment web pages
  - Malware distribution sites
  - Counterfeit goods sites
  - Illegal pharmaceutical or piracy sites
- Part Of Criminal Infrastructure
  - Server names for eCrime name resolution
  - Names for command-control botnet administration

- Domain Generating Algrithms (DGA)
  - Ability to create hundreds of thousands of domains according to a specified ‘recipe’
  - Designed for resiliency
  - Good guys need to register or block ALL DGA generated names
  - Bad guys only need to be able to register one to retain/regain control of botnet
  - Used for Botnet C&C

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
- Limiting views to control what data systems can be known
- Restrict resolution to specific address ranges if needed
- 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

DNS Basic Hygiene (2)

- Ensure all system security patches have been reviewed and applied
- Review log files for unauthorized access to systems
- Verify integrity of every DNS record as well as the change history
- Enforce good credential management lifecycle practices
- Ideally ensure multi-factor authentication is enabled to all systems
- Ensure that DNS zone records are DNSSEC signed and your DNS resolvers are performing DNSSEC validation
- Ideally ensure your email domain has a DMARC policy with SPF and/or DKIM and that you enforce such policies provided by other domains on your email system.

DNSSEC

- An extension of the domain name system (DNS) which increases its security and mitigates cache spoofing attacks
- DNSSEC assures that the DNS information has been provided by the correct source, and is complete
- DNSSEC assures that the integrity of the data has not been breached during transmission
- Records for DNS lookups are digitally signed using public key cryptography
- Protects against Man-in-the-Middle attacks and scenarios where a fake authoritative server is set up give seemingly valid DNS answers

Fall 2018 Domain Registration Hijacking

- Attackers gained access to victims' registrar accounts, typically by ***compromising login credentials***
- Attackers ***changed DNS records*** (A, NS) often pointing them to the attackers' servers
- Once DNS zone content was changed attackers ***impersonated legitimate services*** hosted by the victims
- From there the attackers executed MiTM attacks against users by ***generated X.509 certificates*** to trick web users into downloading malware payloads

Example of Cross-Functional Brokenness

Protocol Developer	Lets give *CSP* lot's of options to handle every conceivable use case
Software Implementor	There's some ambiguities but I will code *CSP* to work this way
Security Architect	Use *CSP*
Network Operator	I'll use defaults for *CSP* since that is easiest for me
Executive	We are compliant since we use *CSP*
Security Researcher	Corporate is stupid because their use of *CSP* can be exploited

CSP = Cool Security Protocol

We Have Organizational Silo Issues

- Executive Teams
- Legal Department
- Technical Teams
  - Research
  - Architecture
  - Operations
- Government Policy
- Law Enforcement

- Cryptography Uses
  - Integrity
  - Non-repudiation
  - Confidentiality
- Crypto is BINARY
- Do NOT Build Backdoors
- Crypto has consequences
  - Loss of visibility
  - Operational risks

We Need Cross-Functional Education and Understanding

Improvements in Information Sharing Needed

- **Everyone** Gets Vilified
  - Why not detected sooner
  - Why not fixed quicker
  - Why notifications delayed
- Issues To Be Resolved
  - Breach notification laws
  - Lack of transparency
  - Escalation chain
  - Cross sector sharing (DNS, ISP)
  - Media hype with incomplete information

Security Fundamentals ALWAYS Matter

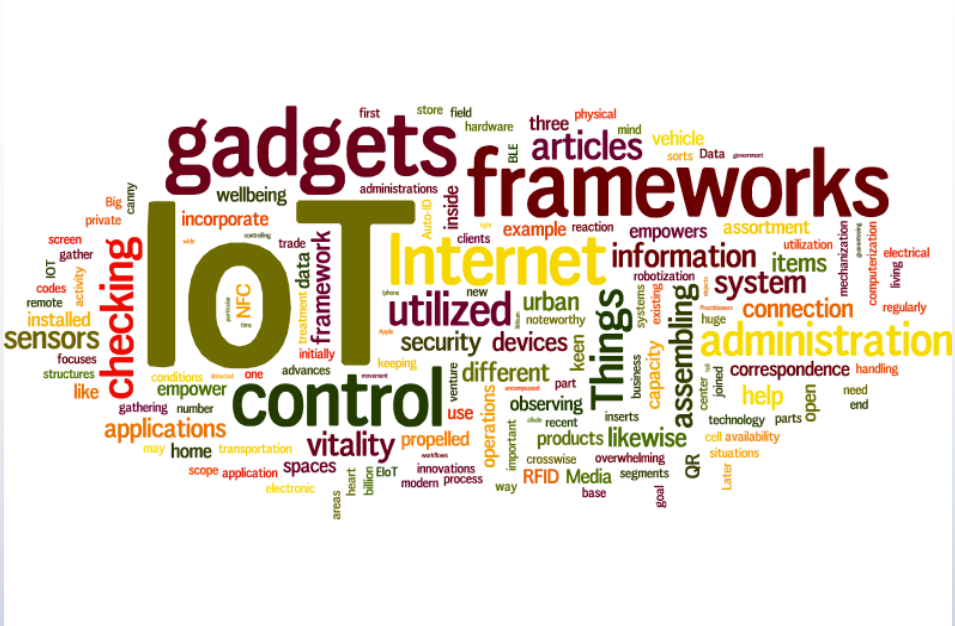
- User Authentication/Authorization
- Device Authentication/Authorization
- Access Control (Packet or Route Filtering)
- Data Integrity
- Data Confidentiality
- Auditing / Logging
- DoS Mitigation
- Timely Patch Management

Most Basic Security Controls Minimize Impact Of Sophisticated Attacks

- **Don’t rely on defaults**
- **Limit fate sharing**
- **Use cryptographically protected protocols**
  - **CHECK HASHES(!)**
- **Get alerted for unauthorized changes**

Trust But Verify

- Standards
- Frameworks
- Best Practices
- Reference Implementations
- Certifications



HOW DO YOU MEASURE EFFECTIVENESS OVER TIME ?