Waking Up The Guards

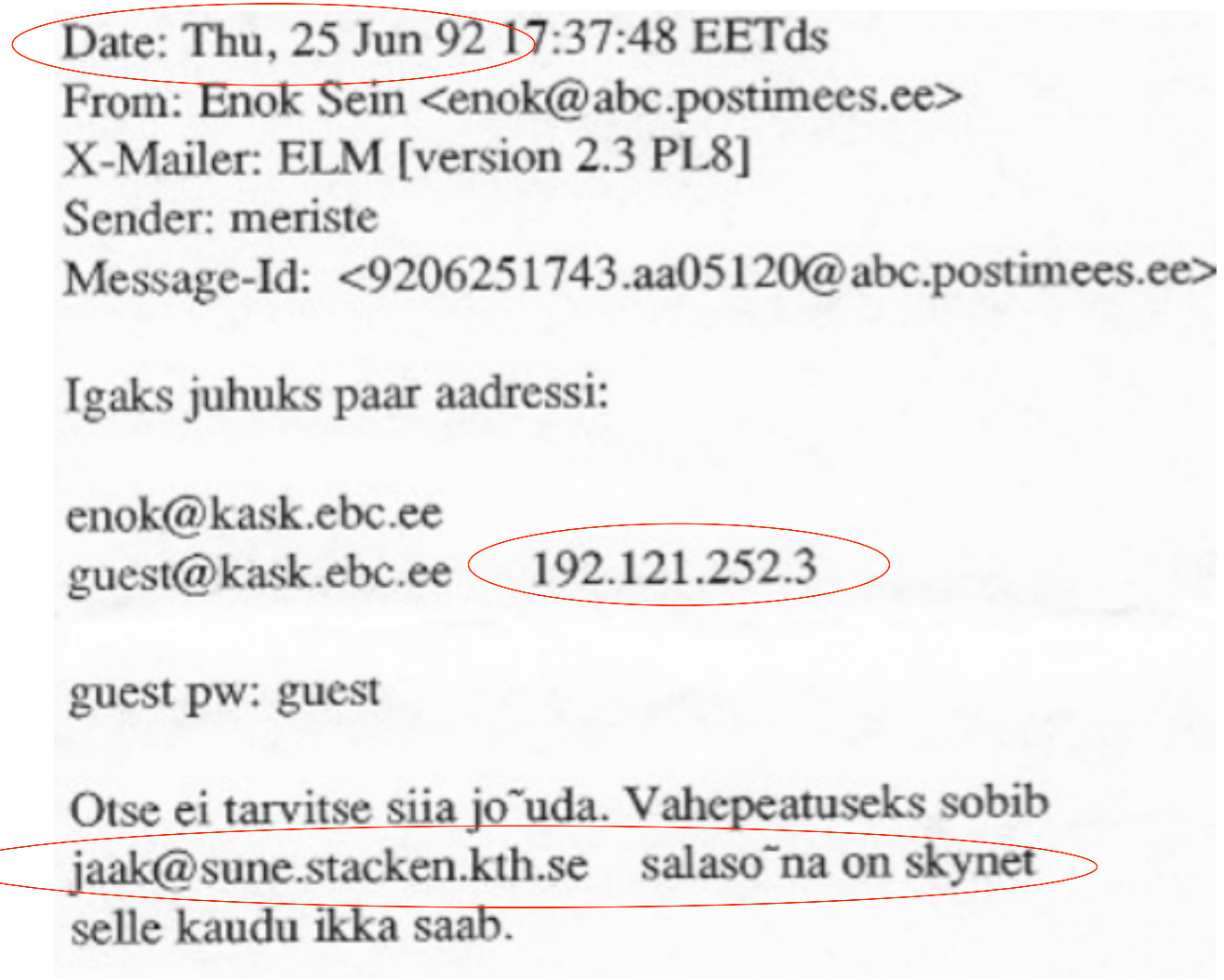
Renewed Vigilance Needed To Regain Trust In Fundamental Building Blocks

Merike Kaeo

merike@doubleshotsecurity.com

IN THE BEGINNING TRUST WAS INHERENT

- Trust established thru personal relationships
- Access control existed but credentials shared with trusted individuals
- Focus was on getting connectivity to work
- Privacy and online safety was not yet a [big] concern



Date: Thu, 25 Jun 92 17:37:48 EETds
From: Enok Sein <enok@abc.postimees.ee>
X-Mailer: ELM [version 2.3 PL8]
Sender: meriste
Message-Id: <9206251743.aa05120@abc.postimees.ee>

Igaks juhuks paar aadressi:

enok@kask.ebc.ee
guest@kask.ebc.ee 192.121.252.3

guest pw: guest

Otse ei tarvitse siia jo˜uda. Vahepeatuseks sobib
jaak@sune.stacken.kth.se salaso˜na on skynet
selle kaudu ikka saab.

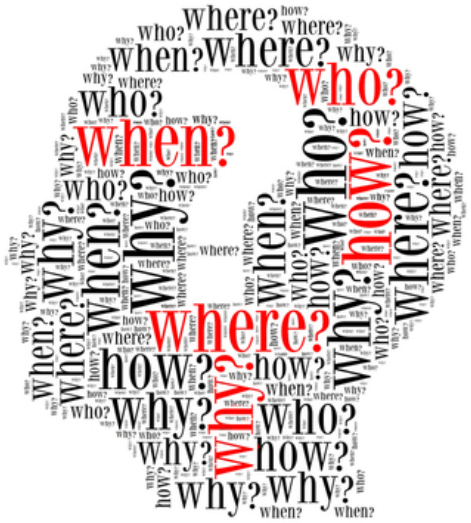
WE HAVE BLIND TRUST ISSUES

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

You can do everything right and still screw up

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

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

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

EVERYTHING IS BROKEN

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BIZ & IT —

Critical Tor flaw leaks users' real IP address—update now

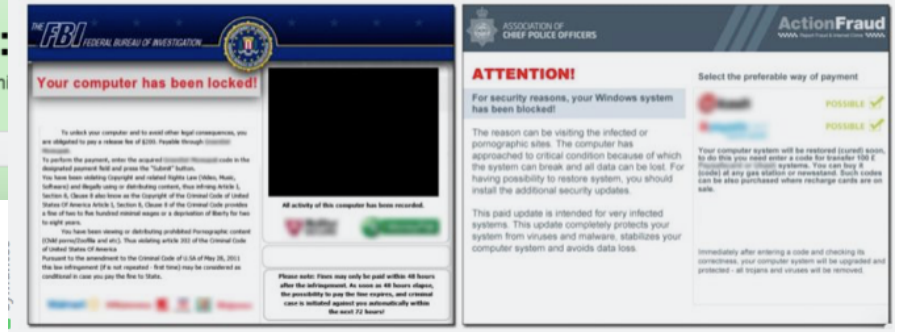
TorMoil threatens Mac and Linux versions of Tor browser; Windows and Tails not affected.

DAN GOODIN - 11/3/2017, 3:30 PM

Legal raids in five countries seize botnet servers, sinkhole 800,000+ domains

At one point, Avalanche network was responsible for two-thirds of all phishing attacks.

SEAN GALLAGHER - 12/1/2016, 10:55 AM



JUL 7, 2014 @ 12:46 PM 5,018

The Little Black Book of Billionaire Secrets

Data Breach Bulletin: Brazilian Banks Lose $3.75 Billion Because Of Boleto Malware

Kat
FULI

Let's Encrypt's free HTTPS certificates are already being used to distribute malware

by ABHIMANYU GHOSHAL — Jan 7, 2016 in INSIDER

Security experts say the attack on Juniper firewalls underscores precisely why they have been saying for a long time that government backdoors in systems are a bad idea—because they can be hijacked and repurposed by other parties.

Security

'Amnesia' IoT botnet feasts on year-old unpatched vulnerability

New variant of 'Tsunami' is a disaster waiting to happen

By John Leyden 7 Apr 2017 at 15:01 13 SHARE ▼

WHY ARE THINGS SO BROKEN?

- Scale
  - Billions of new devices
  - Large amounts of bandwidth
- Criminal Sophistication
  - Network architecture clue
  - Prevalent use of tunneling
  - More use of encryption
  - Social media ‘weaponization’
- Automation
  - Trusting outsourced infrastructures (i.e the ‘Cloud’)
  - Persistent continuous attacks on targets

DATA SHARING HAS OPPORTUNITIES and RISKS

Opportunities of Sharing Data

- Social media simplifies sharing
- Digitalization enables sharing
- Time and cost savings
- Instant gratification

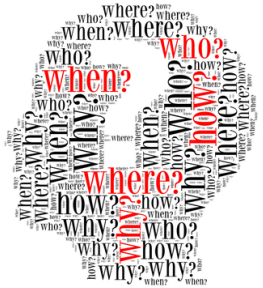
Risks Introduced

- Who has the data?
- Where is data going?
- What is done to protect the data?
- How is our data being abused?

FUNDAMENTAL BUILDING BLOCKS

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

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



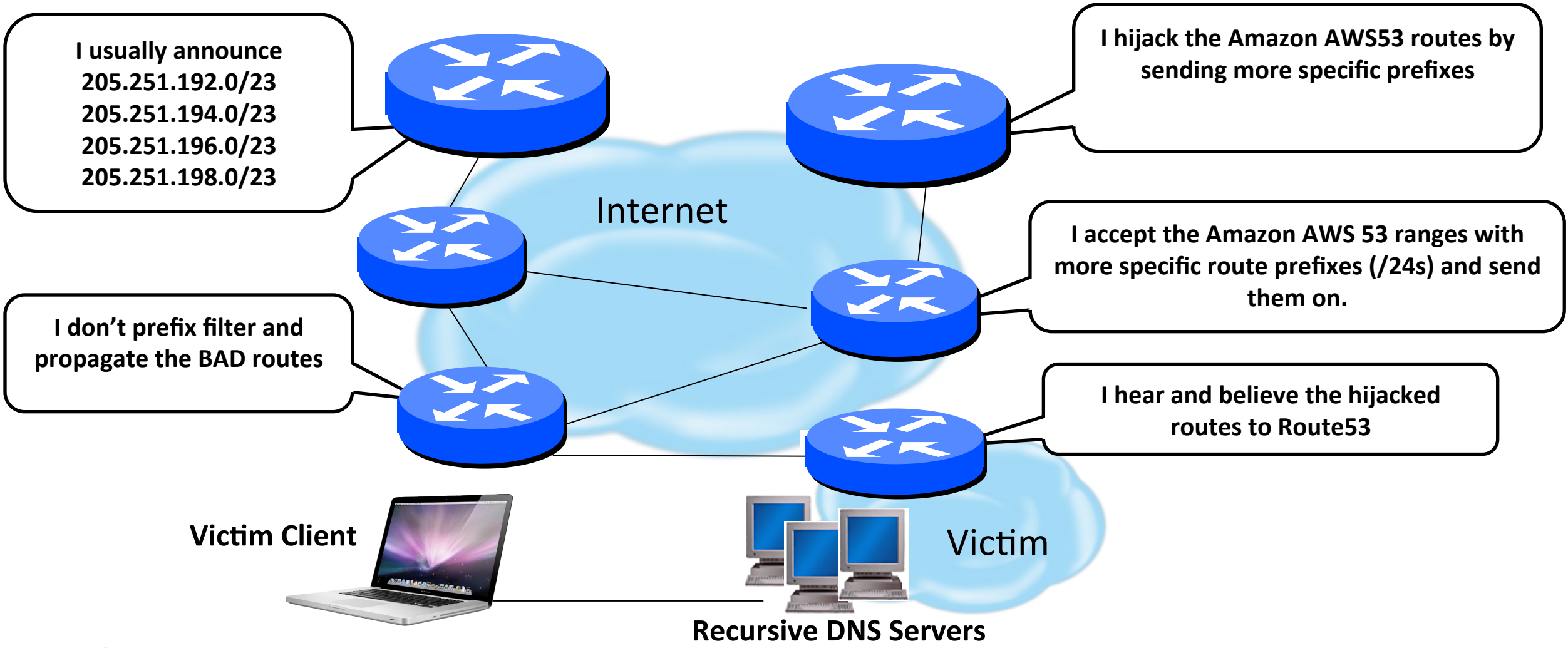
- Integrity of data
- Confidentiality of data

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

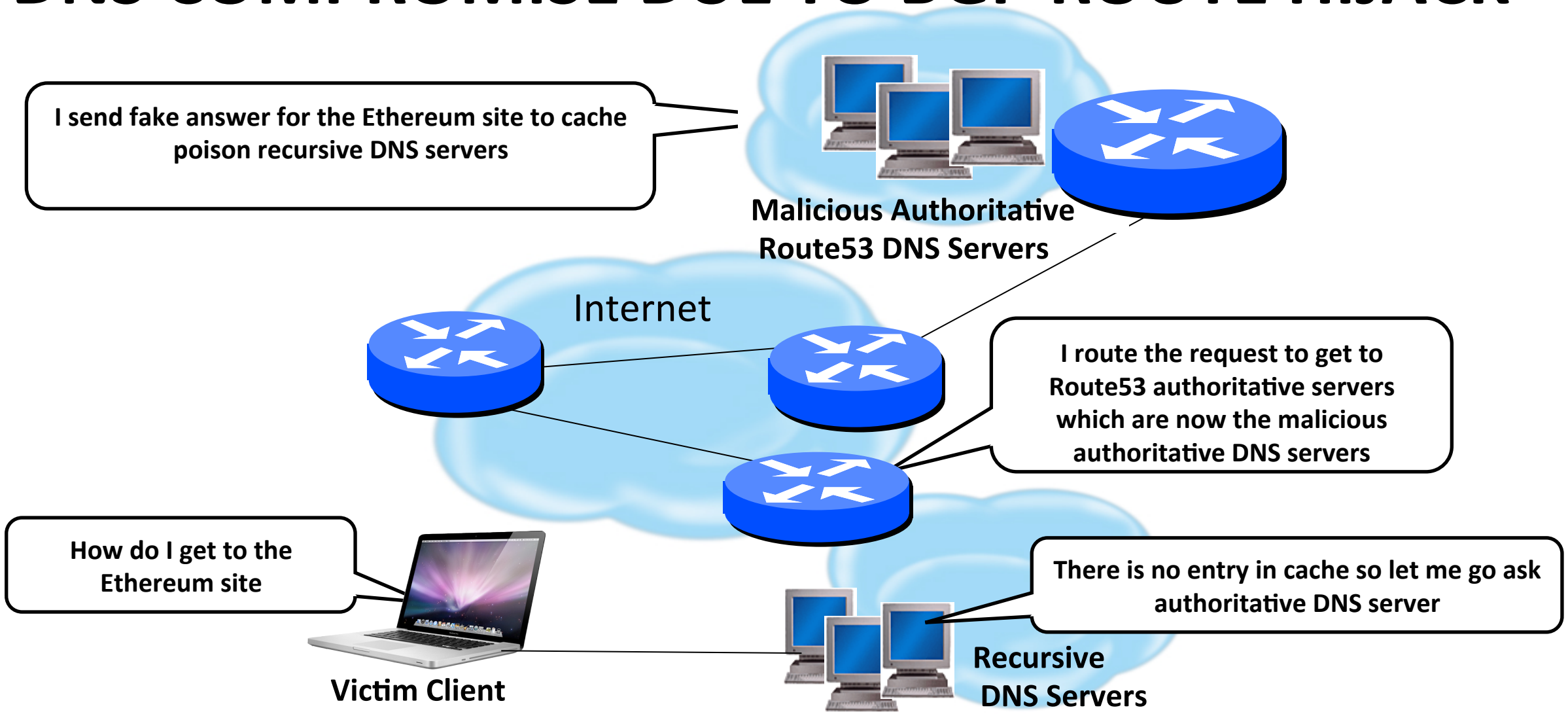
SOPHISTICATED INFRASTRUCTURE ATTACKS

- 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

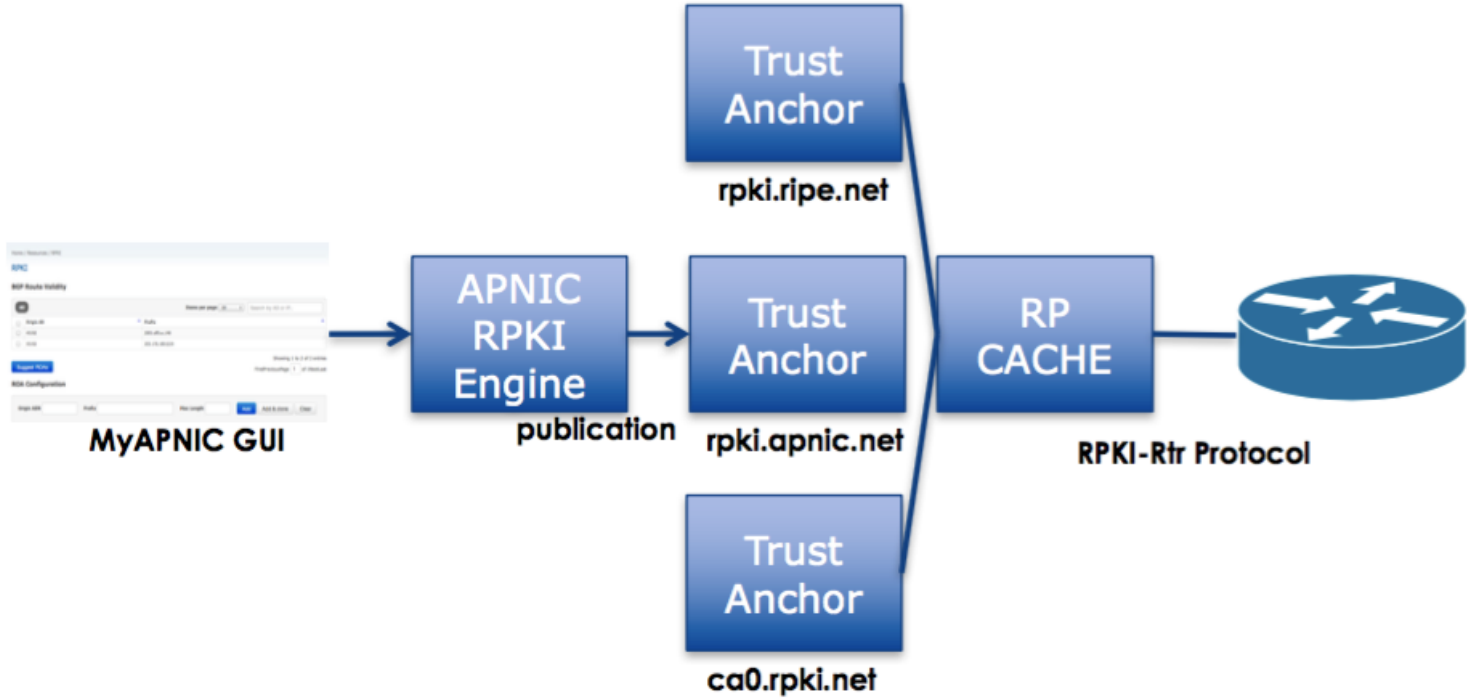


BASIC ATTACK MITIGATION TECHNIQUES

- 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



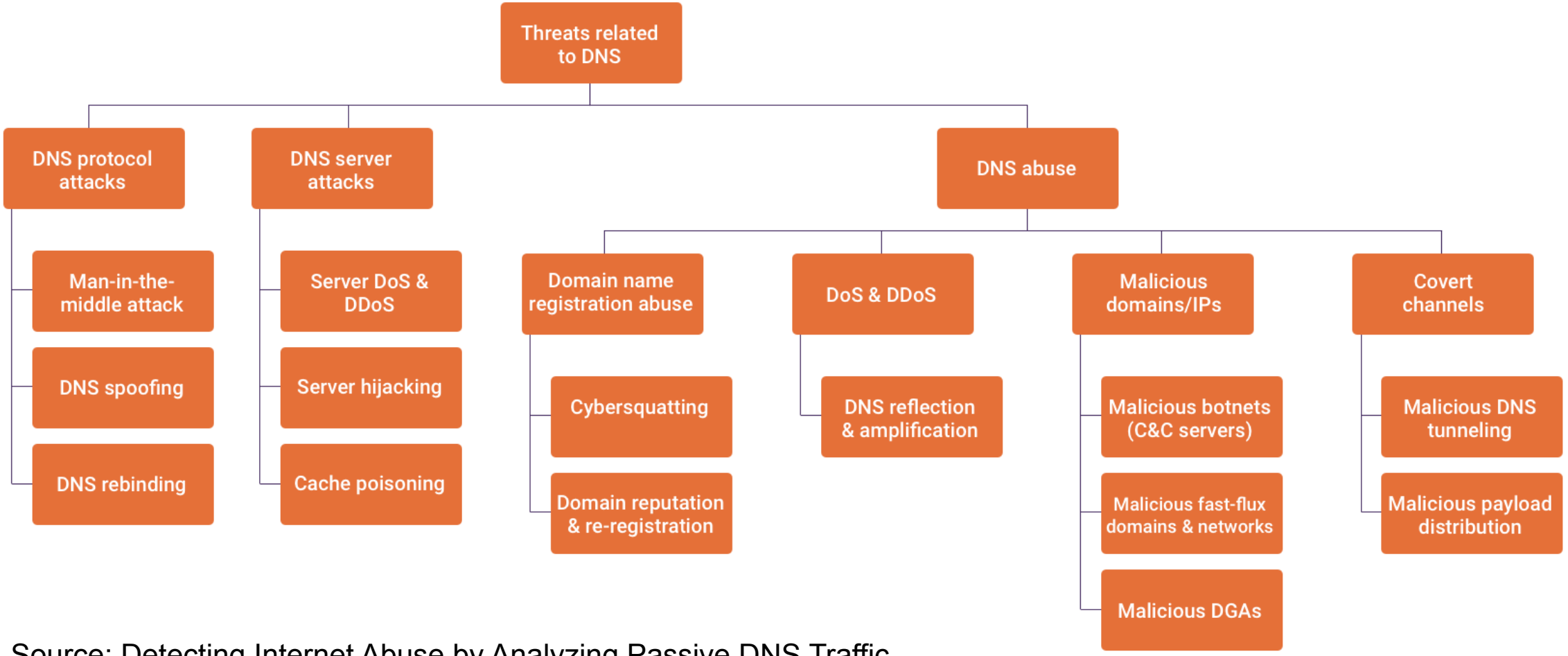
Courtesy of APNIC: https://apnic.net

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 CRIMINAL 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 Algorithms (DGA
  - Ability to create hundreds or thousands of domains according to a specified "recipe”
  - Designed for resiliency
  - Good guys need to register or block ALL DGA generated names
  - Bad guy only needs 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

WHAT IS IT CRIMINALS ARE AFTER?

- Name(s)
- Username
- Password
- Phone #
- Email
- Date Of Birth
- Home Address
- Mother's Maiden Name

- Medical Insurance Provider
- Insurance Account Number
- Primary Physician
- Hospital Affiliated With Physician

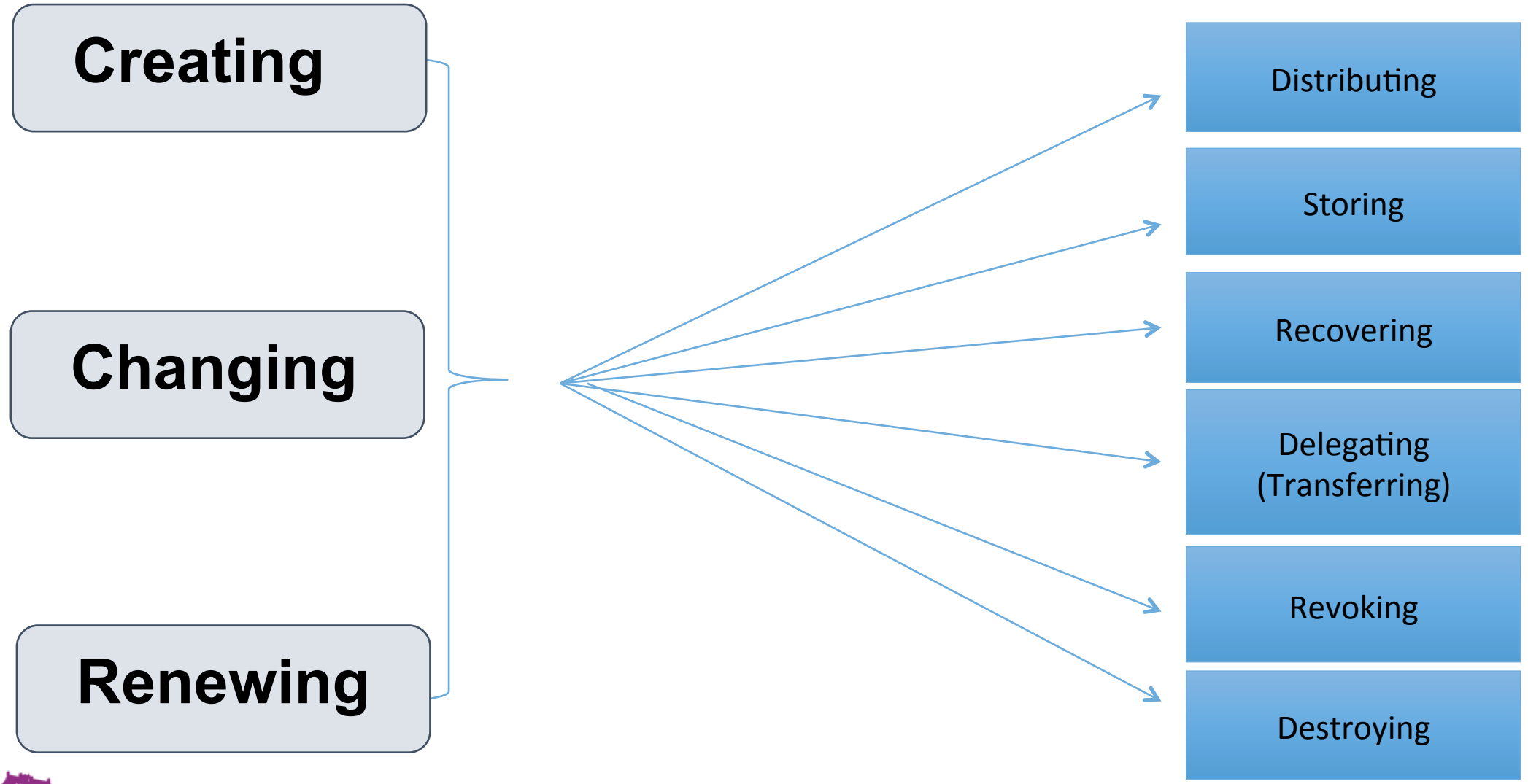
- Bank Account
- Bank Routing Number
- Income Tax Number
- Credit Card Number
- Mortgage Information

- Social Security Number
- National ID Number
- Passport Number
- Drivers License Number

IT STARTS WITH GETTING CREDENTIALS

- 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 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

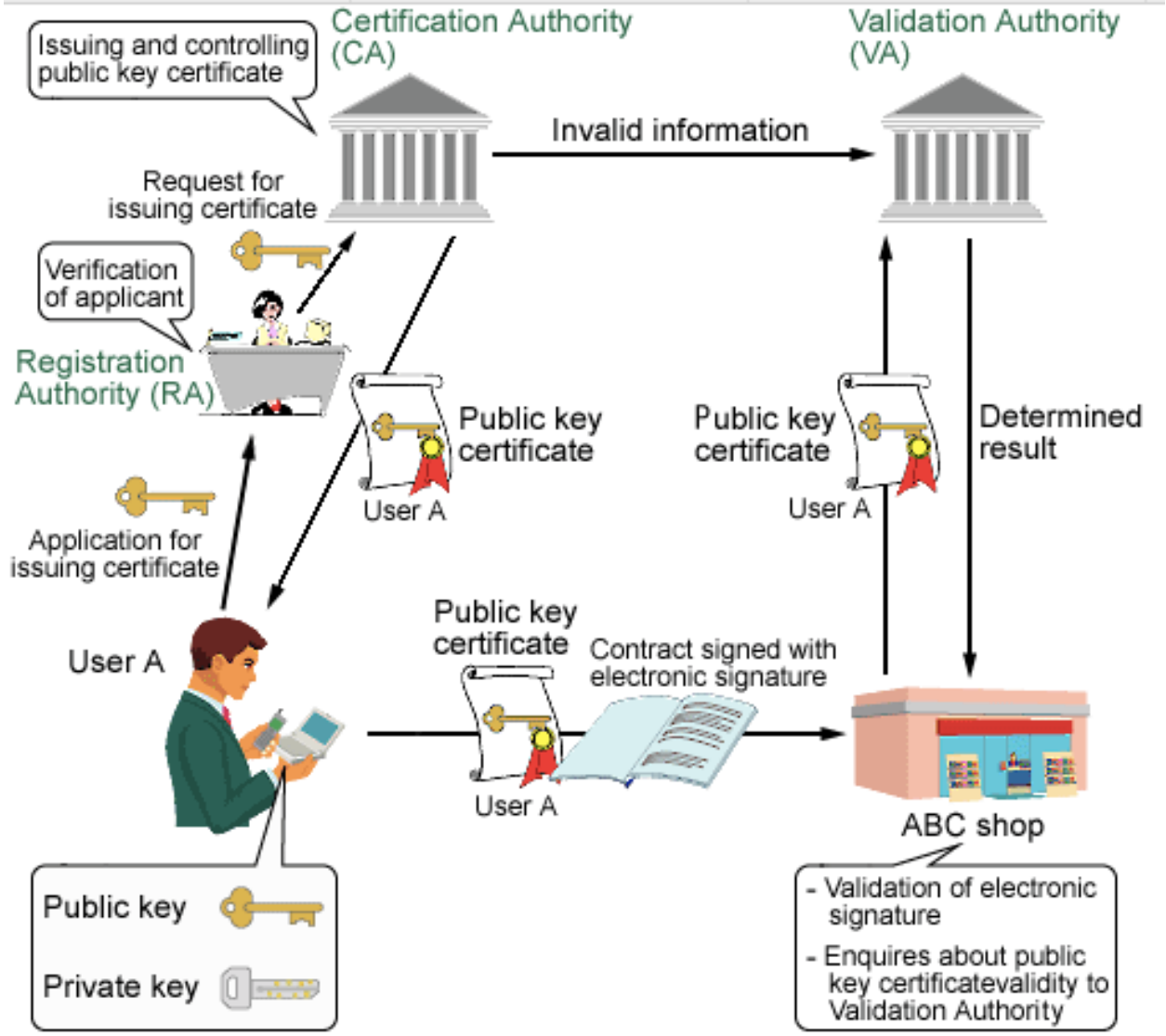
- Multi-factor authentication provides added layer of protection
- Varying types of MFA
  - Universal 2nd Factor (U2F)
  - Time based onetime passwords (TOTP)
  - HMAC-based onetime passwords (HOTP)
  - SMS Passcode
  - Phone Based Verification

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

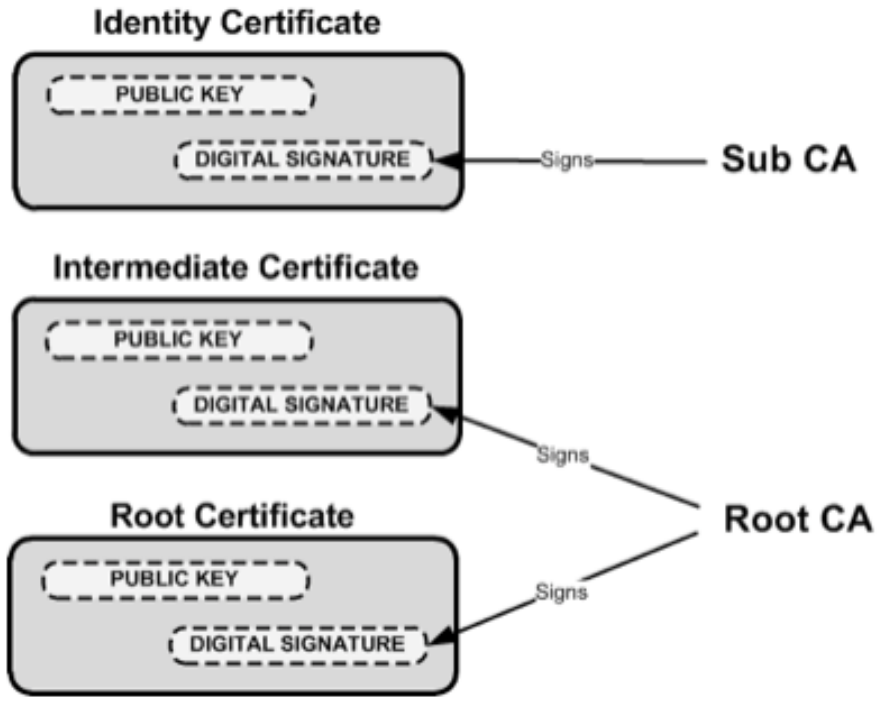
PKI ARCHITECTURE

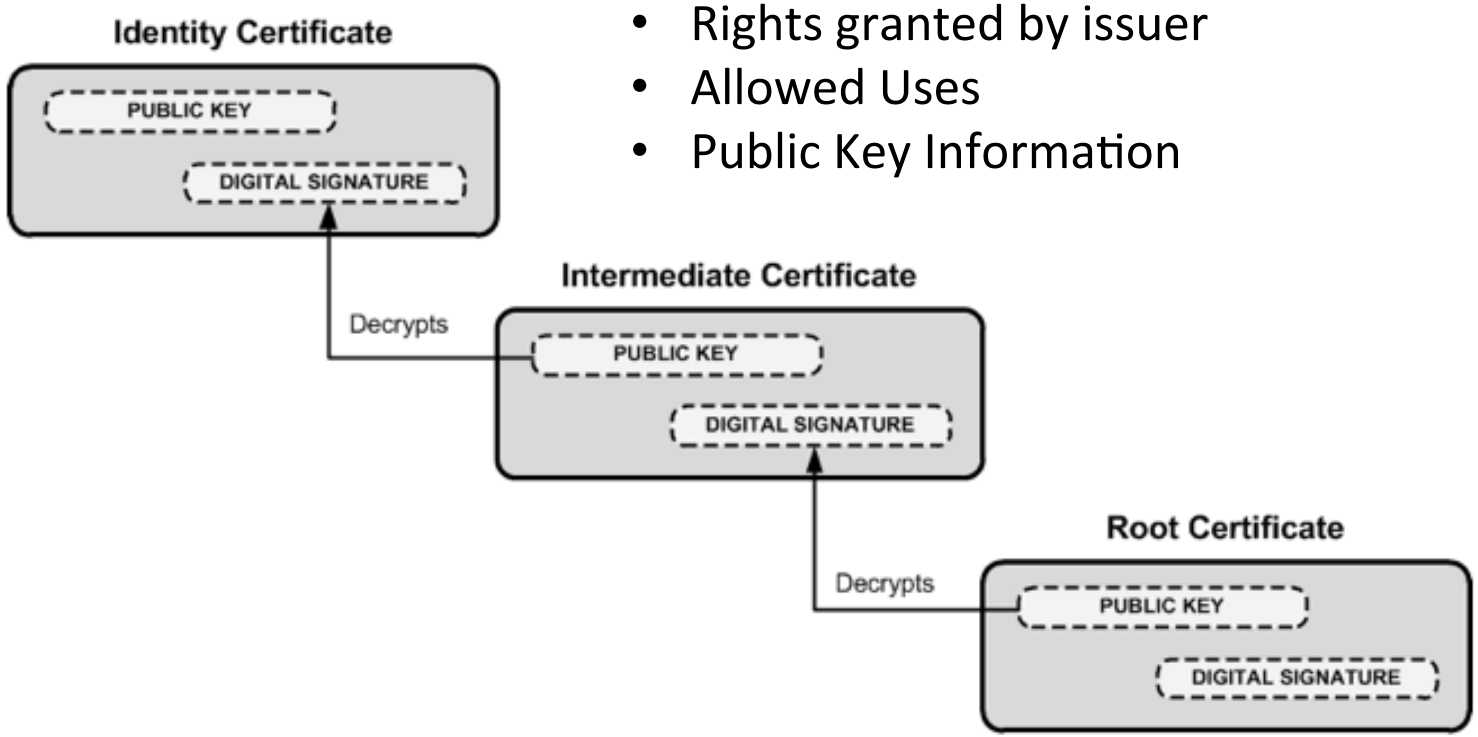
- Certification Authority
  - Issues digital certificates & CRLs
- Registration Authority
  - Trusted by the CA to vouch for the identity of users to a CA
  - Generally relies on operational controls and cryptographic security rather than physical security
- Validation Authority
  - An electronic site that holds certificates and certificate status information
  - Accessed via LDAP, HTTP, FTP or email



CERTIFICATE CHAIN OF TRUST

- Organization certificate is issued to
- Organization that issued certificate
- Hostnames certificate is valid for
- Validity period
- Rights granted by issuer
- Allowed Uses
- Public Key Information

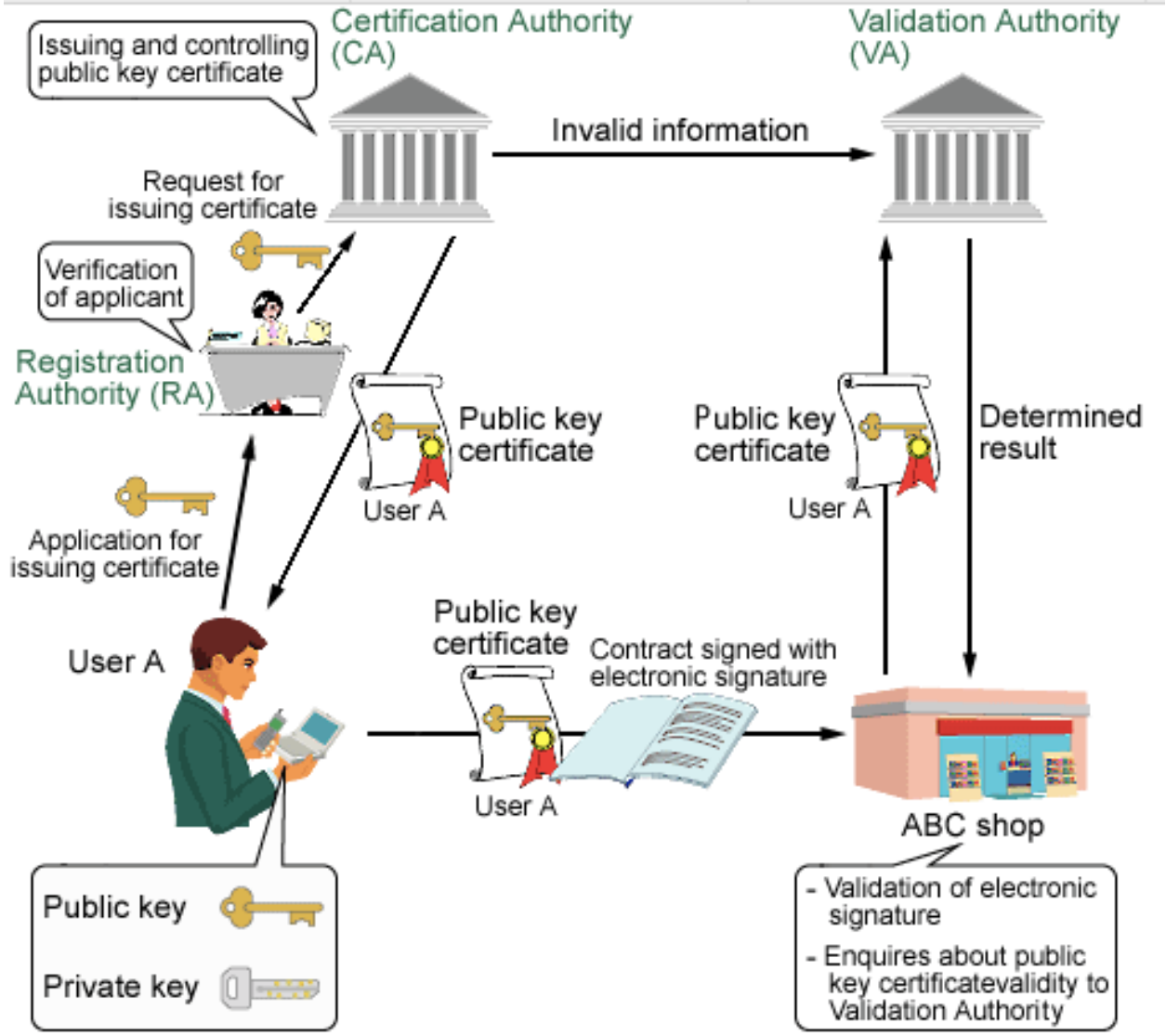




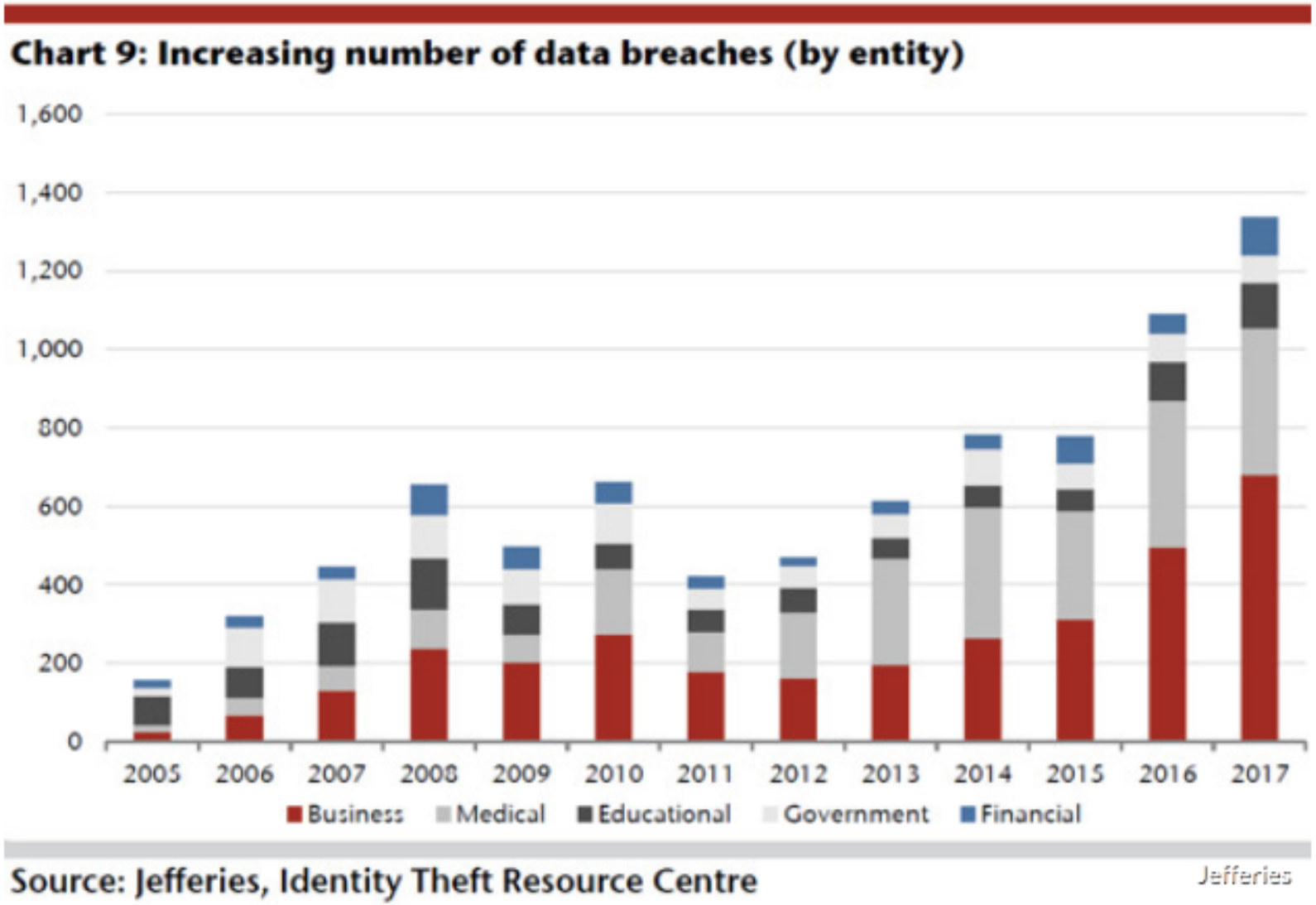
PKI SECURITY

Fundamental Security

- Server Access
  - Physical and Logical
- Integrity of Data
- Confidentiality of Data
- Availability of Data
- Validation of Data
  - Certificate Transparency



WHY FUNDAMENTAL SECURITY MATTERS



Privacy Violated

- Extortion
- Bullying
- Embarrassment
- Financial Ruin
- Identity Theft
- Fraud
- Loss of Life

WE NEED TO GET BACK TO BASICS

- 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**

BUILDING TRUST IN PEOPLE

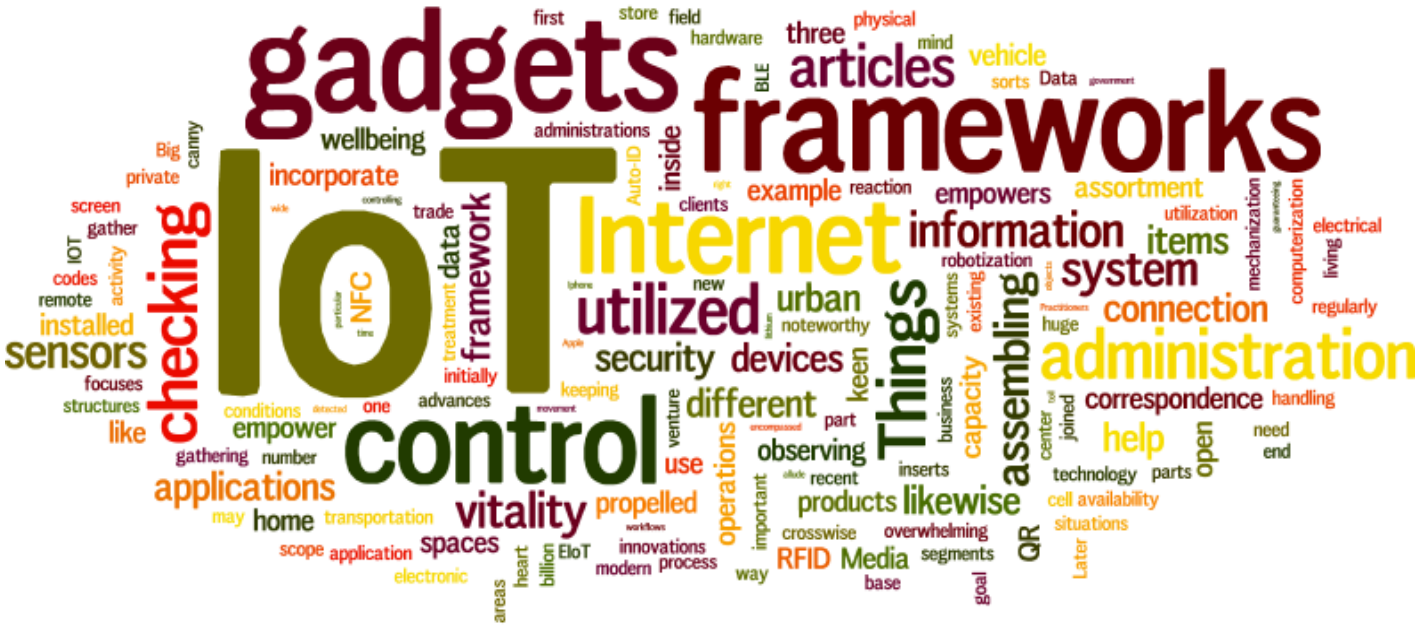
- Academia
- Technology Innovators
- Software Engineers
- Network Operators
- Business Executives
- Law Enforcement
- Lawyers
- Policy Makers
- Government

- Build culture that builds and maintains trust
- Accept most people are trustworthy
- Create values centered around integrity and trust
- Develop culture of commitment
- Challenge a culture of blame
- Learn from incidents

TRUST IS EARNED BUT MUST BE VERIFIED

TRUST BUT VERIFY

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



HOW DO YOU MEASURE EFFECTIVENESS OVER TIME ?