FARSIGHT SECURITY

Managing Security Risks In Today's Complex Internet Landscape

Merike Kaeo, CTO Farsight Security
merike@fsi.io

FARSIGHT SECURITY

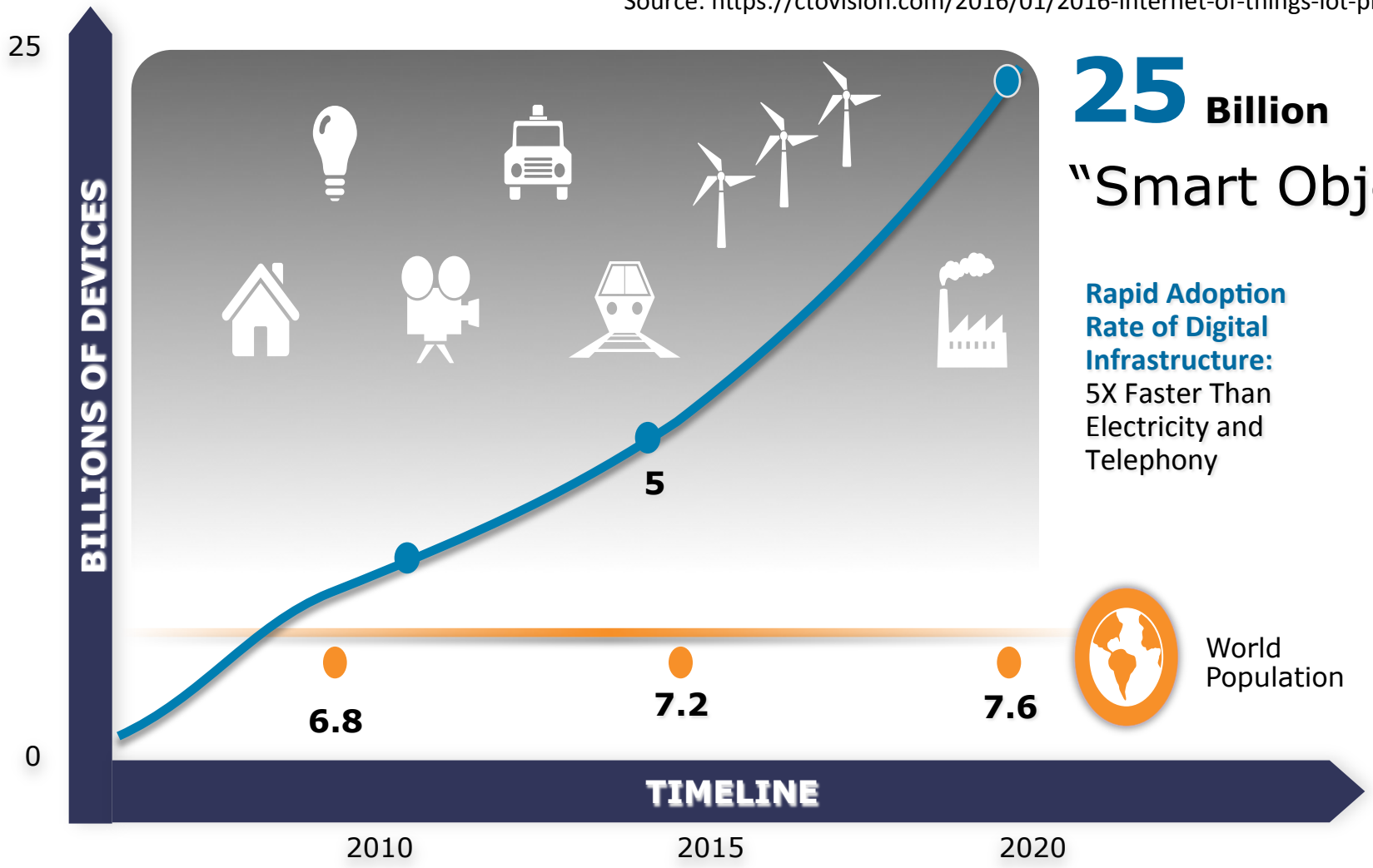
Goals For Today

- Understand the complexity we are creating
- Knowing the right questions to ask
- Admitting that we all need to take more action
- Working together to reduce risks in our infrastructures

FORESIGHT SECURITY

IoT Predictions

Source: https://ctovision.com/2016/01/2016-internet-of-things-iot-predictions/



25 Billion

"Smart Objects"

Rapid Adoption Rate of Digital Infrastructure:
5X Faster Than Electricity and Telephony

FORSIGHT SECURITY

We Are in a Period of Rapid Change

- Intelligent, interconnected devices are continuing to be connected to the global Internet
- Governments, businesses and individuals are moving their resources to the Internet with blind trust
- Data is accumulating faster than it can be organized or protected
- The complexity of the Internet ecosystem creates a rich environment exploitable by activists, criminals, and nation states
- Data will continue be stolen or modified using subtle, persistent, directed attacks

FARSIGHT SECURITY

Current and Future Concerns

- Greater data privacy issues will be exposed
- Implementations will have flaws but no upgrade path
- Security compliance often does NOT translate to realities of operational security
- Security continues to be an exercise in blind trust
  - Vendor implementations
  - Operational deployments
  - Technical standards

FARSIGHT SECURITY

Security Goals

- Controlling Data Access
- Controlling Network Access
- Ensuring Network Availability
- Protecting Information In Transit
- Preventing Intrusions
- Responding To Security Breaches

FORSIGHT SECURITY

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)

FARSIGHT SECURITY

Security Controls

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

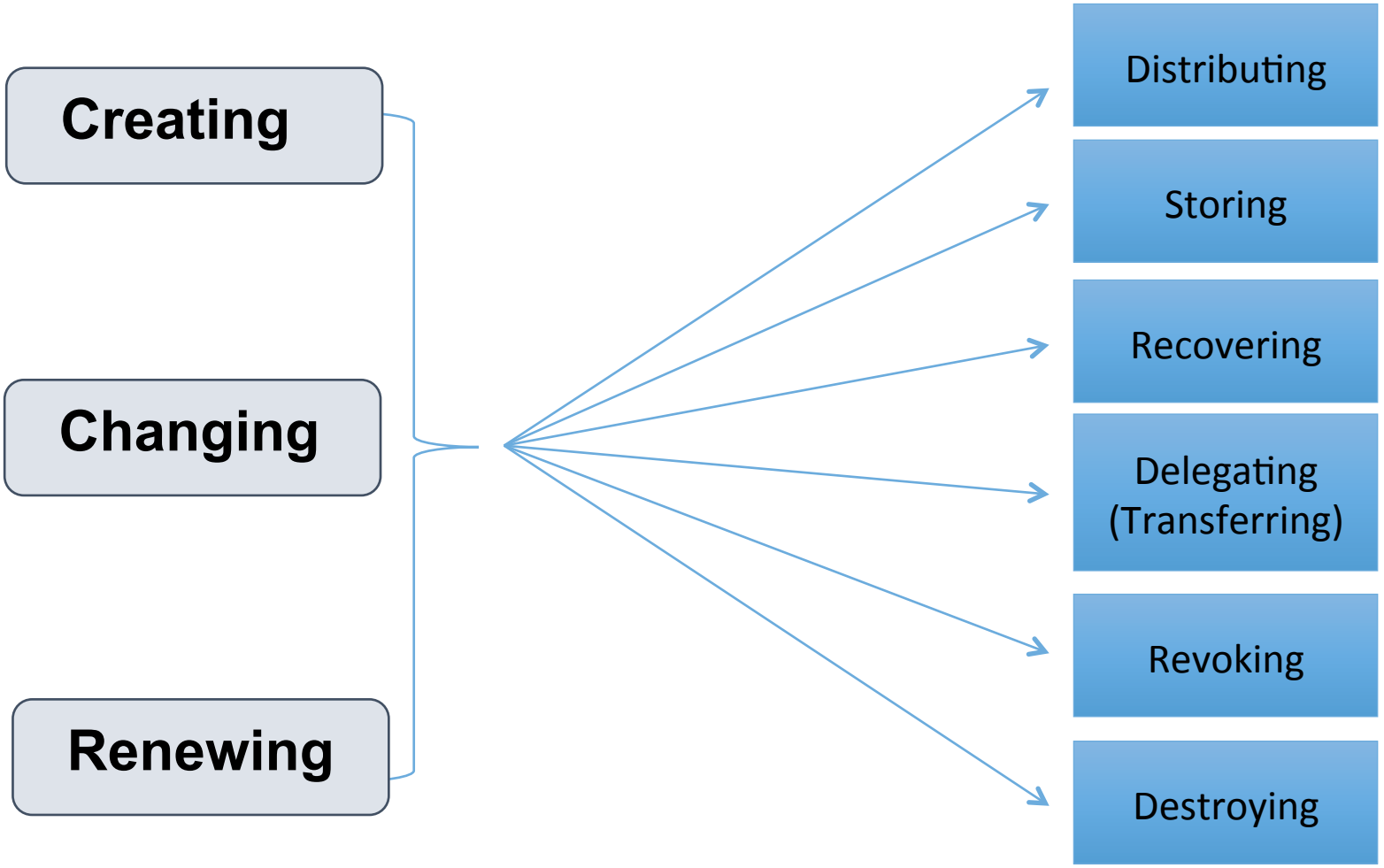
FARSIGHT SECURITY

Big Issue: Credential Compromise

- 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
- Using simple to guess password
- Unpatched security vulnerabilities are exploited

FARSIGHT SECURITY

Credential Management Process



FORSIGHT SECURITY

Improving Credential Management

- Know ALL credentials that are utilized in your environment
- Encourage the use of 2-factor authentication
- Create specific process to address ENTIRE credential management lifecycle
- Assess specific risks in your operational procedures and create a plan for improvement

FARSIGHT SECURITY

Keeping Up With Vulnerabilities

- Know Your Operating Systems and Application Versions
  - For TLS/SSL can use publicly available tests
  - https://www.ssllabs.com/ssltest/
- Get On Mailing Lists For Vendor Security Announcements
- Subscribe to National CERT Alert Lists
- Follow Security Industry Blogs
  - http://ccnso.icann.org/resources/cybercrime-resources.htm

FARSIGHT SECURITY

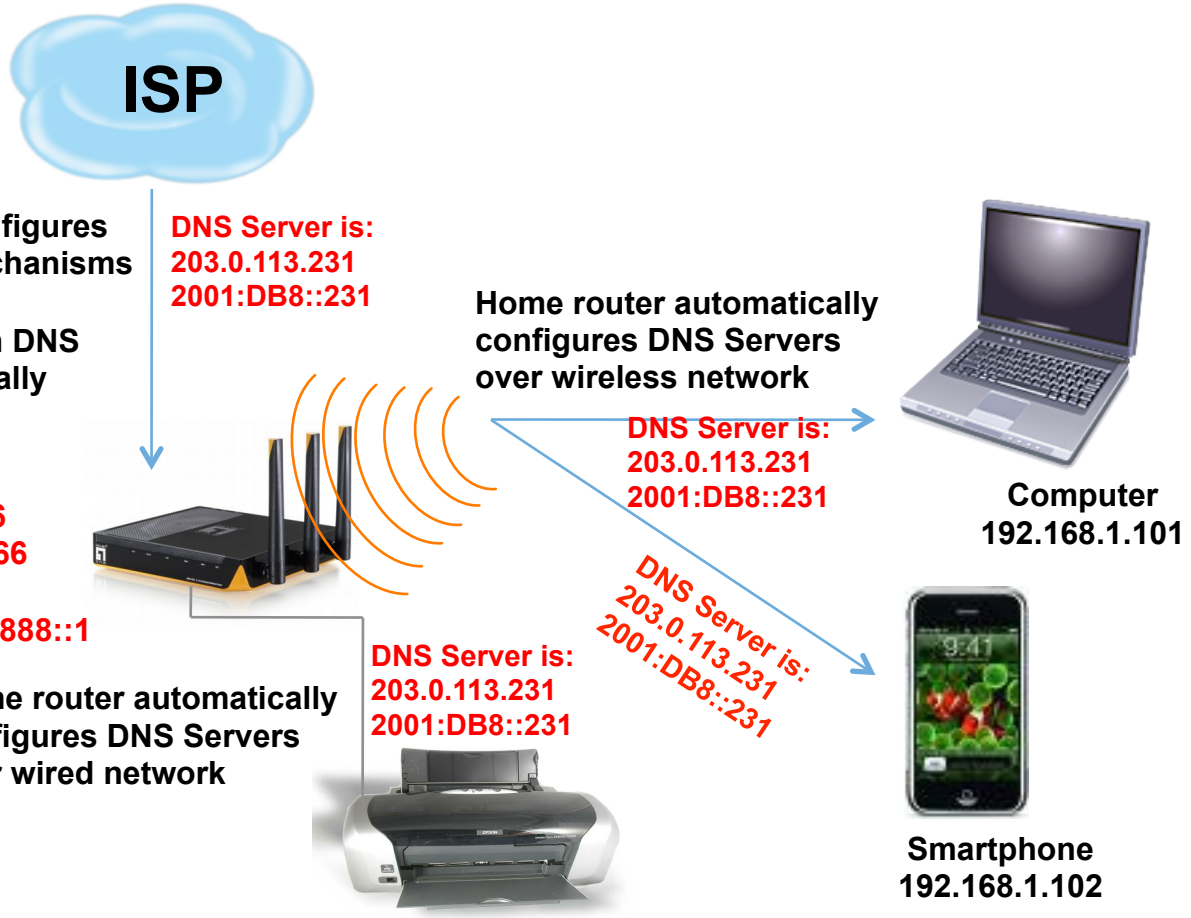
Exploitable Protocols

- IPv6
  - You are using it even if you think you are not
  - It is similar to IPv4 but different
  - Can vendor products detect and protect against attacks and malware utilizing this protocol?
- DNS
  - Do you know where your DNS traffic is going?
  - How would you detect when users going to malware sites?
  - How would you protect from amplification attacks?
  - Do you know how many domains you own?
  - Do you know who your registrar is?

FORSIGHT SECURITY

Recursive DNS Server Configurations

- Service provider automatically configures DNS Servers using automated mechanisms
  OR
- Service provider provides you with DNS Server IP addresses that get statically configured



FARSIGHT SECURITY

DNS Amplification Attack Example

Compromised User Devices

Recursive DNS Servers send legitimate questions to authoritative servers

Recursive DNS Servers

1

Forged information is used to make it look like intended victim sent legitimate questions to Recursive DNS Servers.

2

3

Authoritative servers send back legitimate replies

4

Legitimate responses from Recursive DNS Servers create large DDoS attack to victim.

Authoritative DNS Servers

Victim

FARSIGHT SECURITY

Some DNS Statistics

278 Million *Current Domain Names*

100+ Million *ccTLD Domains*

10+ Billion *Current Hostnames*

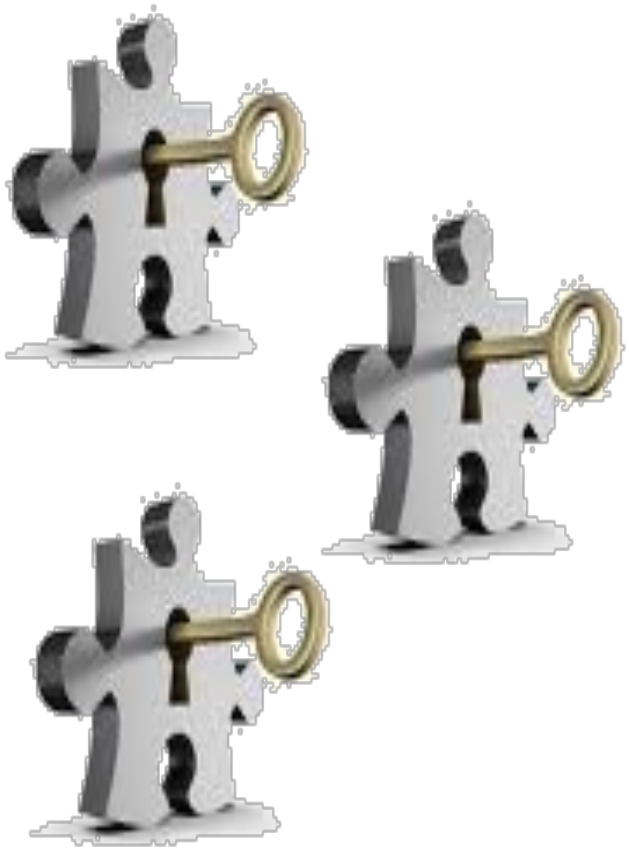
Questions That Can Be Answered Using Passive DNS

- Where did this domain name point to in the past?
- What domain names are hosted by a given nameserver?
- What domain names point into a given IP network?
- What subdomains exist below a certain domain name?
- What new names are hosted in ccTLDs?

FARSIGHT SECURITY

Sharing Security Related Data

- Everyone knows sharing is fundamentally good
- Many discussions around ***wanting*** to share
- Government, private sector and public sector alliance efforts have been ongoing
- Most issues relate to liability concerns and regulatory environments
- More action is needed



FARSIGHT SECURITY

Criminals Really Good At Sharing

- Websites advertise Botnets and Malware for hire
- Vulnerabilities and Exploits are traded on an 'open market'
- There are no enforceable rules for NOT sharing
- Utilizing social media is making sharing much more efficient

Choose Custom Botnet
- Number of Hosts
- Geographic Region
- Bandwidth
- Duration
- etc

FORSIGHT SECURITY

We Also Need To Start Sharing

- Initial Step – Build Trust Thru Networking
- Start by sharing for specific use cases that don't impact privacy and personally identifiable information (PII)
  - SSH Brute Force Attack
  - DNS/SNMP/NTP Amplification Attack
  - Passive DNS Information
- Investigate how to share data that may impact privacy/PII and what can be anonymised but still be useful
  - SPAM / Phishing details

FARSIGHT SECURITY

Do You Have A CIRT ?

- You should have a Computer Incident Response Team established
  - Who is part of this?
  - What are their responsibilities?
- Important – define a single individual to be in charge of final decisions (also have a backup for this individual)
- Know who you need to contact
  - Legal / regulatory responsibility
  - Upstream ISPs who may help filter on DDoS attacks
  - Impacted individuals

FORSIGHT SECURITY

Concluding Thoughts

- Business Risk Tolerance Weighs Into Security Decisions
- Play An Active Role In Managing Security Controls
  - Cannot hand off all security liability to cloud providers
- Perform Basic Security Hygiene
  - Create Effective Credential Management Processes
  - Restrict Access to Applications, Hosts and Network Segments
  - Perform Regularly Scheduled Firmware / Software Upgrades
  - Disable Unused Applications and Services
  - Configure Logging with Regularly Scheduled Log Reviews
  - Use Cryptographic Protection to Transfer and Store Data