Cybersecurity Threats

CYBR 4400/5400: Principles of Internet Policy, Lecture 6-1

Dr. David Reed, Technology, Cybersecurity, and Policy Program, CU Boulder

Today's Lecture

- Debate on Privacy Policy
  - Zuckerberg Calls for Stronger Regulation
  - Apple on Privacy
- Current Events
  - How is Your Broadband Holding Up?
- Unit 5 Wrap-up
- Cybersecurity Threats Lecture

Cybersecurity Threats

Definitions

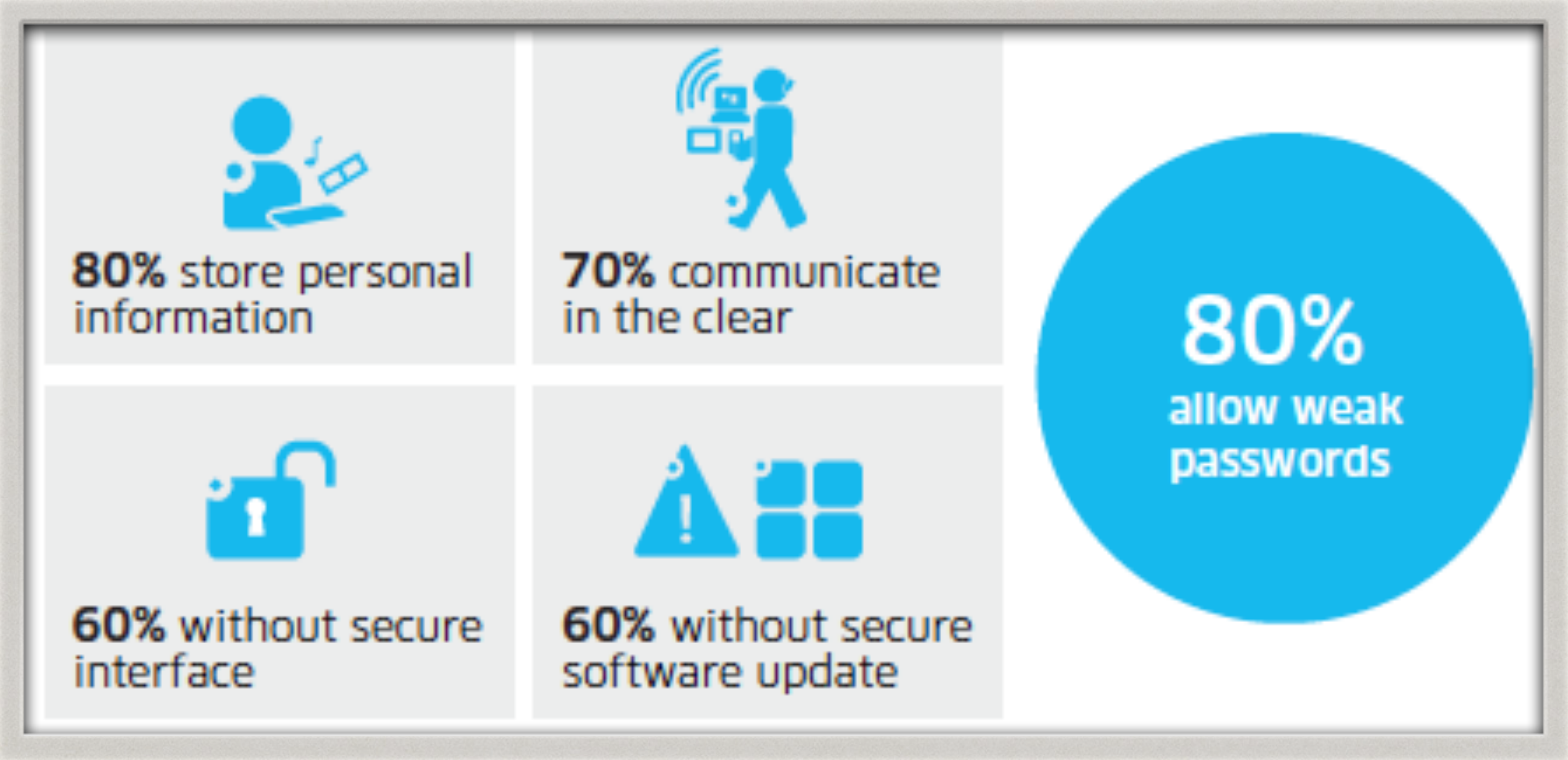
- Cyberspace
  - Artifacts based on, or dependent on, computing and communications technology,
  - Information these artifacts use, store, handle, or process,
  - and how these various elements are connected
- Cybersecurity (security in cyberspace) — technologies, processes, and policies that help to prevent or reduce negative impact of events in cyberspace
  - Result of deliberate actions against information technology by hostile or malevolent actor

Factors Creating Cybersecurity Issues

- Presence of malevolent actors in cyberspace
- Societal reliance on IT for many important functions
- Inevitable presence of vulnerabilities in IT systems that malevolent actors can exploit

Cybersecurity is a never-ending battle, and a permanently decisive solution to the problem will not be found in the foreseeable future

Security Concerns



80% store personal information

70% communicate in the clear

60% without secure interface

60% without secure software update

80% allow weak passwords

- Fast growing "Attack Surface" to valuable information
  - Smartphones
  - Cloud data
  - 50-60B Internet of Things devices by 2020

Source: The Future X Network, A Bell Labs Perspective, Chapter 3, 2016

Problems Cannot Be Solved Only With Technical Solutions

- Improvements can considerably reduce damage due to cybersecurity breaches
  - Efforts to more widely use what is known about improving cybersecurity
  - Efforts to develop new knowledge about cybersecurity
- Publicly available info and policy actions insufficient to motivate adequate sense of urgency
- Tradeoffs to improve cybersecurity inevitable, have to be accepted through political and policy-making processes

Key Tradeoffs

- Economics
- Innovation
- Civil liberties
- International relations and national security

Why Should Society Care About Cybersecurity?

- What are effective approaches to state-of-the-art cybersecurity challenges?
- What are the essential cyber vulnerabilities and threats upon which Society requires awareness?
  - Requirements for cyber hygiene?
  - Requirements for cybersecurity user education?
- Why such little progress despite significant policy responses?

Public Policy Concerns

- Cybercrime
- Loss of privacy
- Activism
- Misappropriation of intellectual property
- Espionage
- Denials of service
- Destruction of cyberphysical systems, critical infrastructure, public confidence
- Threats to national security and cyber war

Computing Technologies

"Computers do what the program tells them to do…"

- A fundamental concern:

  "although it may be possible to show that the program does what it is supposed to do … it is impossible to show that it will never do what it is not supposed to do with all possible inputs"

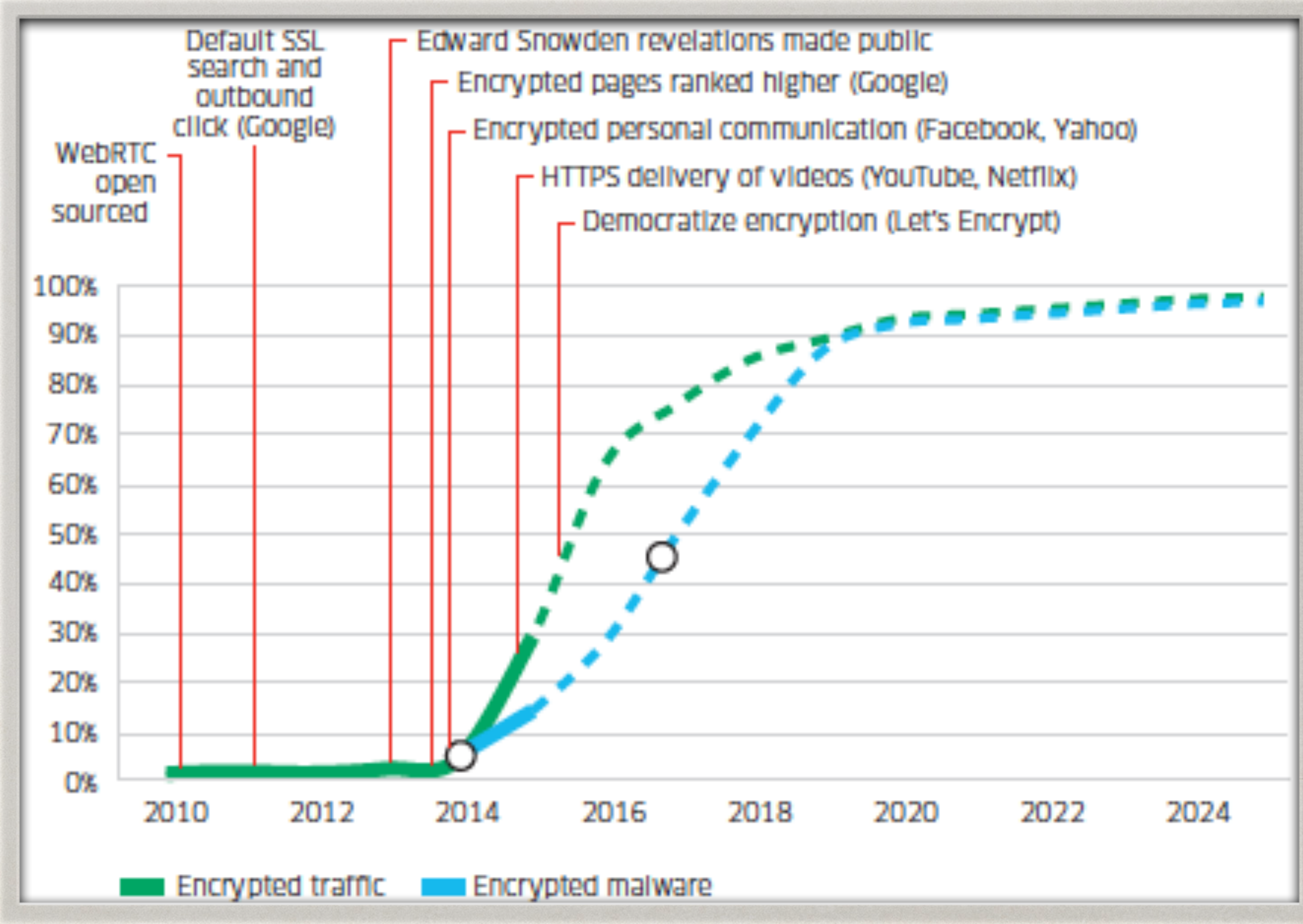
Eddie Tipton sentenced to 25 years in 2017 for rigging lottery system to win more than $2M. He designed code that predicted winning numbers in some games on three days of the year.

Digital Representation of Information

- Information is inherently anonymous
  - Activist/Hacktivist/white hat/black hat
  - Authentication associations can always be separated from data in principle
- How to distinguish sequence of bits between program and data?
- Enables cryptographic methods

Encrypted Traffic Paradox

Rise of encrypted traffic decreases effectiveness of security analytics



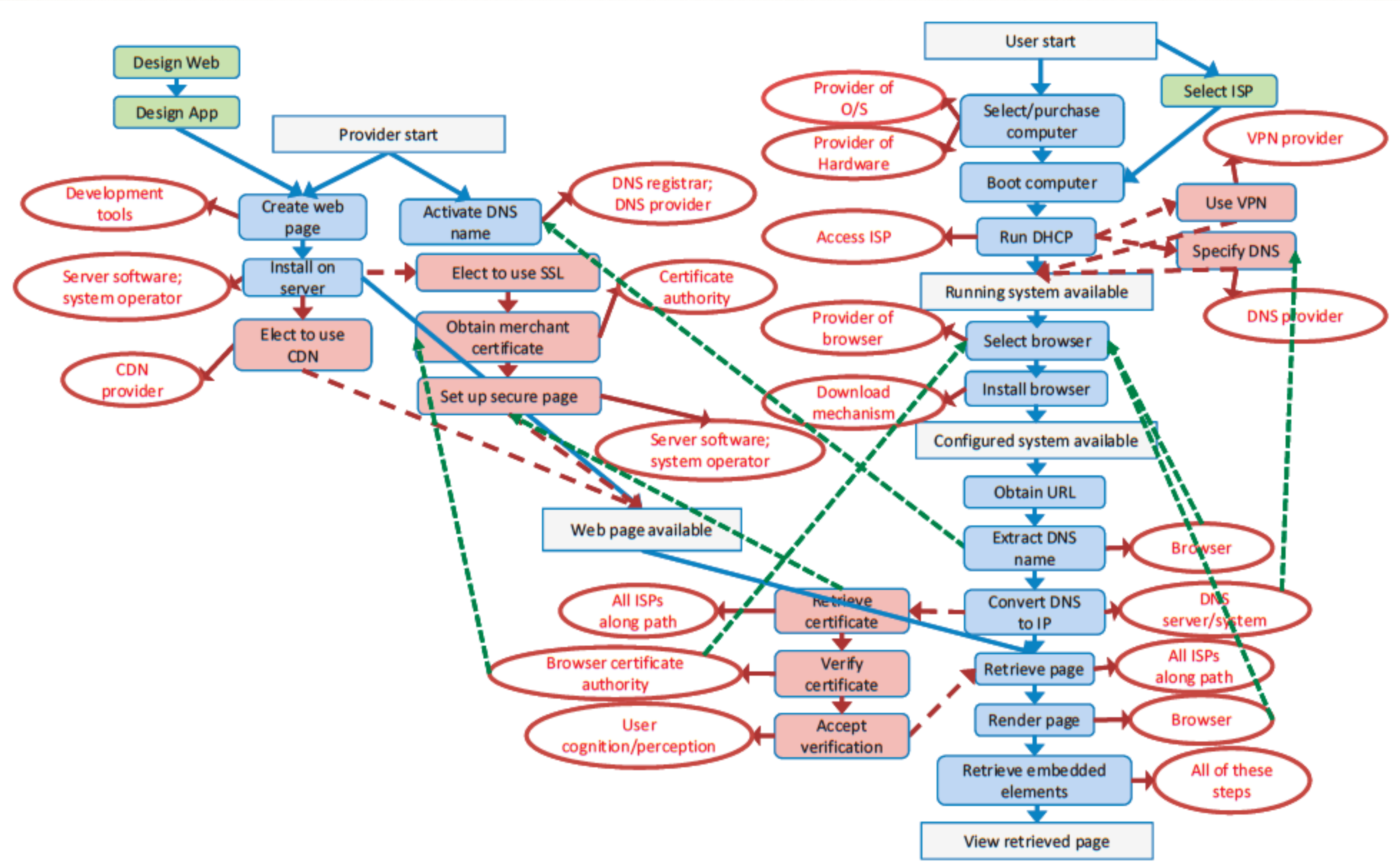
Source: The Future X Network, A Bell Labs Perspective, Chapter 3, 2016

Vocabulary

- Data exfiltration: unauthorized transfer of data from a computer
- Cyber Exploitation: Action to exfiltrate digitally stored information to unauthorized parties
- Cyberattack: action intended to cause denial of service or damage/destruction of stored/transiting info
    - DDOS, botnets

A Simple Web Page Viewing

"Each actor must carry out correctly the role it plays in overall process"



Design Web

Design App

Provider start

Development tools

Create web page

Activate DNS name

DNS registrar; DNS provider

Server software; system operator

Install on server

Elect to use SSL

Certificate authority

Elect to use CDN

Obtain merchant certificate

CDN provider

Set up secure page

Server software; system operator

Web page available

All ISPs along path

Retrieve certificate

Browser certificate authority

Verify certificate

User cognition/perception

Accept verification

User start

Select ISP

Provider of O/S

Provider of Hardware

Select/purchase computer

VPN provider

Boot computer

Use VPN

Access ISP

Run DHCP

Specify DNS

Running system available

DNS provider

Provider of browser

Select browser

Download mechanism

Install browser

Configured system available

Obtain URL

Extract DNS name

Browser

Convert DNS to IP

DNS server/system

Retrieve page

All ISPs along path

Render page

Browser

Retrieve embedded elements

All of these steps

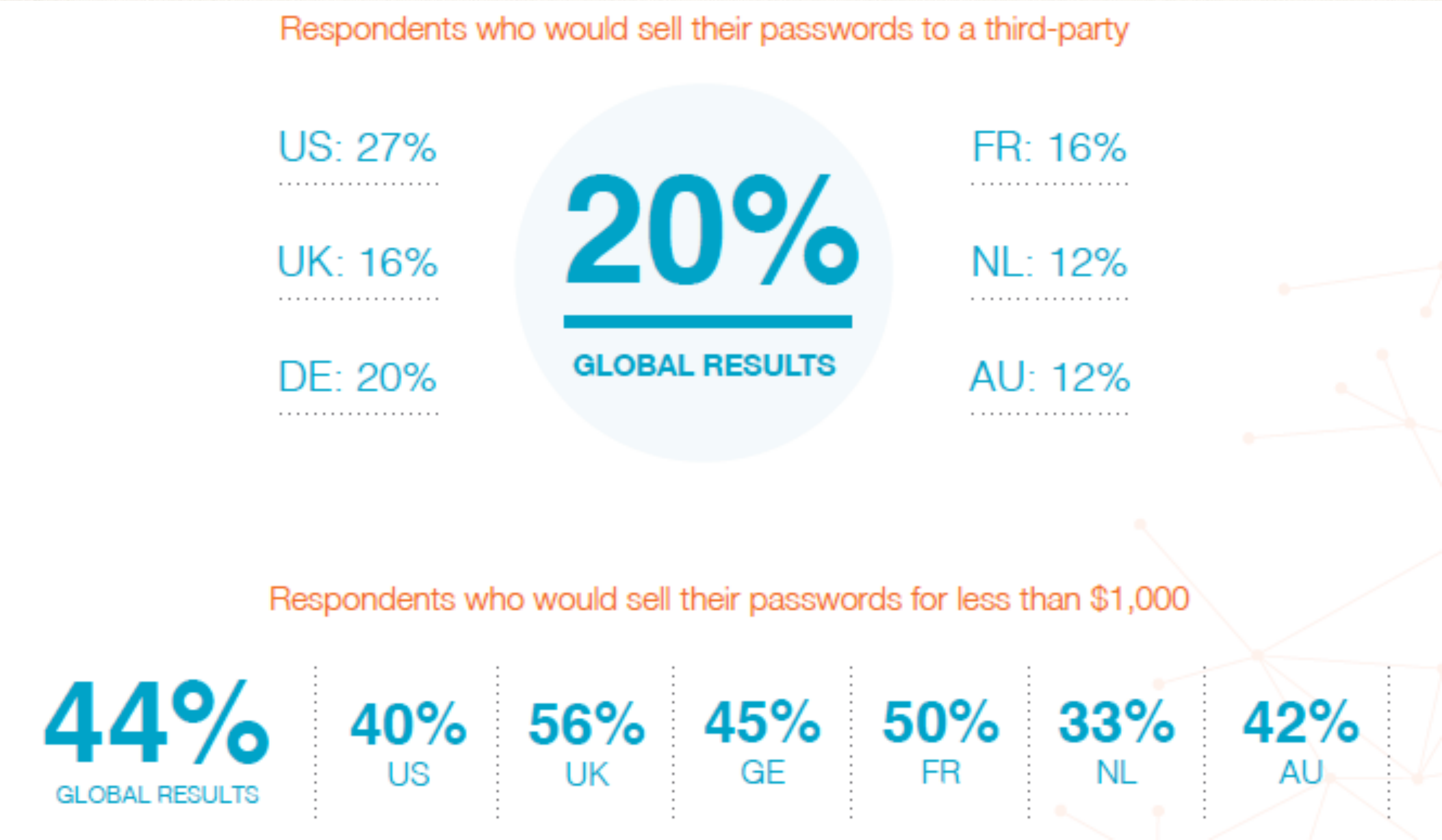
View retrieved page

Cyber Penetration

- Access
  - Remote access/close access (e.g. part of supply chain)/ social access
- Vulnerability
  - Accidental flaws/intentional flaws/configuration errors
  - “Zero day” vulnerability

Poor Password Hygiene

```
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
```



Respondents who would sell their passwords to a third-party

US: 27%

UK: 16%

DE: 20%

20%

GLOBAL RESULTS

FR: 16%

NL: 12%

AU: 12%

Respondents who would sell their passwords for less than $1,000

44% GLOBAL RESULTS	40% US	56% UK	45% GE	50% FR	33% NL	42% AU

Source: 2016 Market Pulse Survey, Sailpoint

Characterizing Threats

- Advanced Persistent Threats (APTs)
  - Focused target/customized to specific security configuration/difficult detection
- Malevolent actors
  - Keep trying/use deception/persuasion good option/will not go away

- GhostNet, 2009
- Stuxnet, 2010
- Deep Panda, 2015
- APT41 , 2020

Some APT examples

What About Antivirus Software?

- Protects against known attacks
- Cybercriminals can now quickly change attack signatures (e.g., using polymorphism malware with small changes)
- Antivirus and firewalls not enough to prevent users from installing malware on their devices

Future Trends

Generating a record of all network events that can identify suspicious activity using security analytics

Monitors OS, memory, processes and network interfaces, reporting activities to centralized security analytics engine

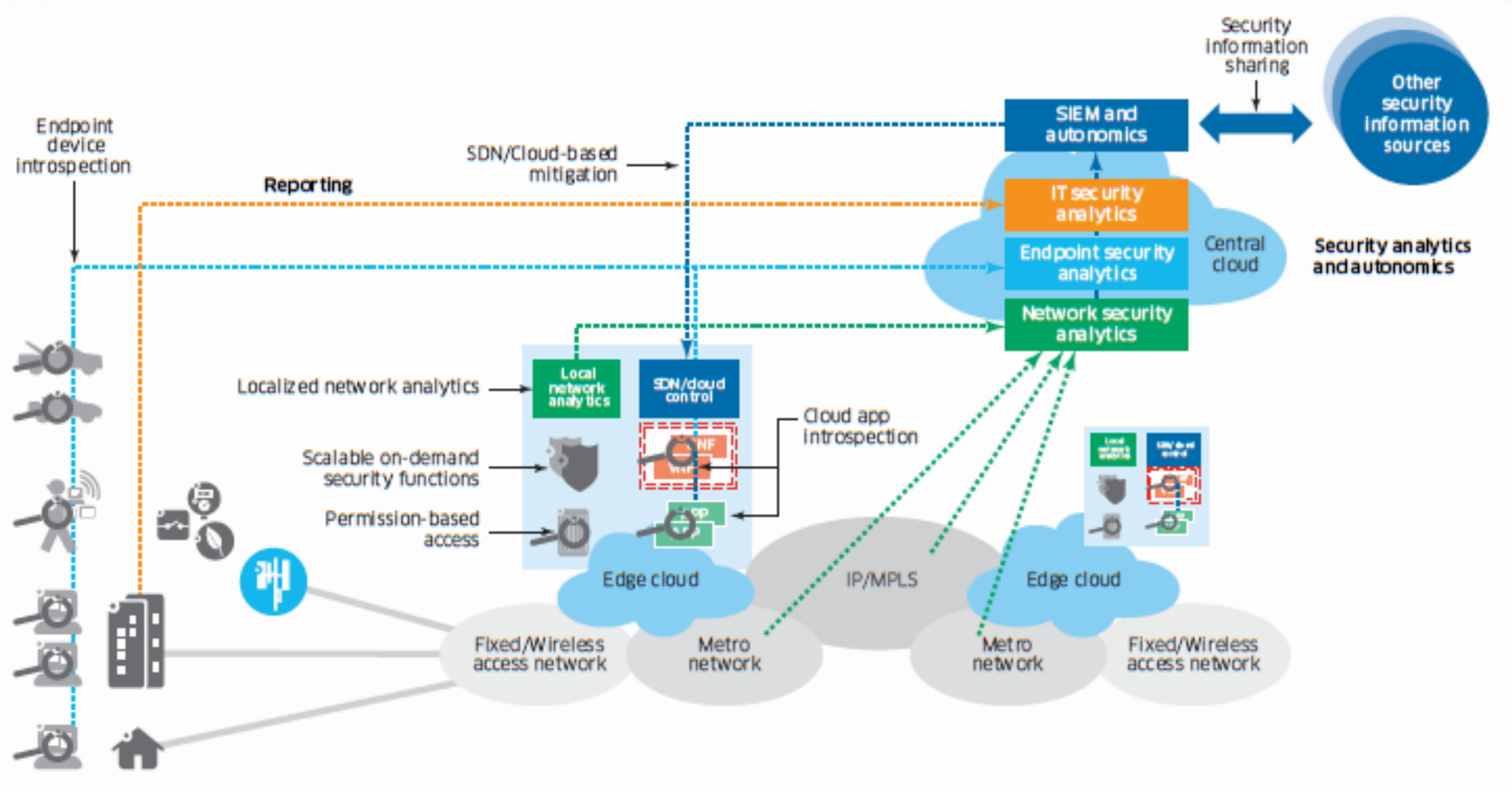
- Combination of perimeter-based, endpoint and network-based security
  - Cloud-based endpoint detection and response (EDR)
  - Perimeter and network security algorithms will run as virtual applications in cloud to find and prevent APTs

Source: The Future X Network, A Bell Labs Perspective, Chapter 3, 2016

2020 End-to-End Security

- Endpoint introspection on qualifying devices
- Permission-based access using biometrics and flexible encryption levels
- Security analytics for real-time APT detection and mitigation
- Security information and event management
- Software defined networking
- Collaborative threat intelligence and sharing

End-to-End Security Architecture


Security information sharing
SIEM and autonomics
Other security information sources
Endpoint device introspection
SDN/Cloud-based mitigation
Reporting
IT security analytics
Endpoint security analytics
Central cloud
Security analytics and autonomics
Network security analytics
Localized network analytics
Local network analytics
SDN/cloud control
Cloud app introspection
Scalable on-demand security functions
VNF
VNF
Permission-based access
App
App
Edge cloud
IP/MPLS
Edge cloud
Fixed/Wireless access network
Metro network
Metro network
Fixed/Wireless access network

Source: The Future X Network, A Bell Labs Perspective, Chapter 3, 2016

End-to-End Principle Debate Over Security in Core

End-to-End Preservationists

- More testing and validation needed against inadvertent disruptions to QoE (speed)
- Security services responsibility of individual applications

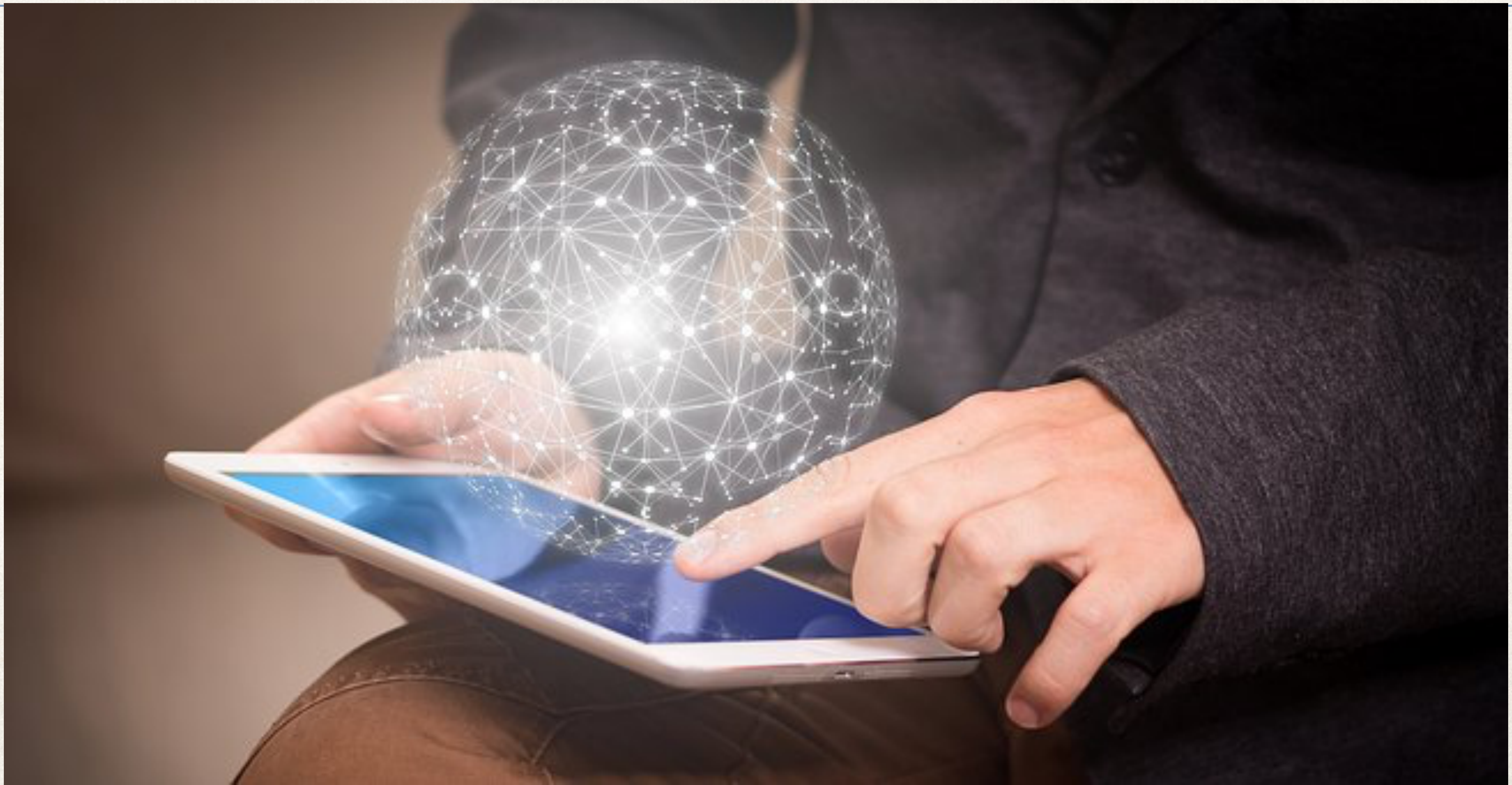
Favor Security in Core

- Embed security services into protocols and active in packet-switching layer (e.g., monitoring and remedy)
- Applications-based security is burden on end users

Discussion Concept: Consider your position on the question of whether to violate the end-to-end principle in the name of security

2019 U.S. State of Cybercrime

Enhancing Cybersecurity



Approaches to Improving Security

- Reducing reliance on IT - balancing advantages vs. security risks
- Knowing that security has been penetrated
  - Detection - Signature checks (morphing and zero-day concerns), behavioral signatures (false positives)
  - Assessment - scale of attack, targets, damage, foreign involvement, attribution

Approaches to Improving Security (cont'd)

- Defending a System or Network
  - Reducing number of vulnerabilities (patching, design)
  - Eliminating/blocking unnecessary access paths
  - Whitelisting software
- Potential conflicts with performance and functionality (e.g., backward compatibility bundles known vulnerabilities)

Technical Sidebar: Saltzer and Schroeder Design Principles

- Economy of mechanism: Keep it simple and small
- Fail-safe defaults: Access based on permission rather than exclusion
- Complete mediation: All access checked for authority
- Open design: design not secret
- Separation of privilege: where feasible, two keys to unlock
- Least privilege: user operations with least set of privileges necessary
- Least common mechanism: minimize common mechanisms for users
- Psychological acceptability: ease of use human interface

Ensuring Accountability

- Individual Authentication and Access Control
  - Ensuring only authorized parties perform certain actions
  - Facilitating accountability
  - Authentication process relies on something you know (password), have (two-factor), or are (biometrics)
- Organizational Authentication
  - Certificate authorities - secret decryption/public encryption keys
- Forensics
  - Examine computer hardware, audits of system logs, statistical/historical analysis of message traffic, interviews with system users

Building Capacity for Containment, Recovery, and Resilience

- Containment - limiting effects of cyber attack (sandboxes, heterogeneous computing systems)
- Recover - repair by system restoration to earlier point in time
- Resilience - performance degrades gradually rather than catastrophically (redundancy)

Employing Active Defenses

- Cyber deception for defensive purposes (honeypots)
- Disruption - reduce damage by affecting operation of computer systems causing attack (disabling botnet)
- Preemption - anticipatory self defense

Cybersecurity Policy Concerns

Economic Approaches to Enhancing Cybersecurity

- Use existing market mechanisms but with improved flow of info (e.g., better info about threats and vulnerabilities)

- Insurance (incentives for lower premiums)

- Liability accountability

- Direct regulation (e.g., adoption of best practices)

Other Policy Concerns

- Innovation
  - Reducing time to market vs. security by design
  - Ease of use, interoperability, and backward compatibility vs. security
- Civil liberties
  - Privacy/free expression (concerns for strong packet authentication)/due process

International Relations and National Security

- Internet governance = management/coordination of technical elements of Internet (e.g., DNS)

- Cybersecurity vs. surveillance tradeoffs - managing incompatible objectives

  - Communications Assistance for Law Enforcement Act (CALEA) of 1994 — Telecom industry must design, develop, and deploy systems that support law enforcement requirements for electronic surveillance

    - "the Athens Affair"

- Norms of cyberspace behavior

  - Collecting national security/foreign policy info = espionage (permitted)

  - Collecting economic/business interests = theft of intellectual property/trade secrets

International Relations and National Security (cont'd)

- Arms control in cyberspace unlikely to be feasible (due to verification challenges, legitimate uses to improve defenses, etc.)
    - Banning cyber exploitation goes beyond current international laws
- Confidence building measures for ICT to provide stability and mutual understanding
- Managing a global supply chain
- Role of offensive operations in cyberspace
    - U.S. would respond using all available means (diplomatic, military, economic…)
    - Laws of war apply, though no published military doctrine
    - Requires presidential approval due to significant consequences