RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PDSC-W09**

Too Much of Good Thing? The Cost of Overusing Encryption

Karen Reinhardt

Principal Engineer, Encryption & PKI
The Home Depot
@Farrside42

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

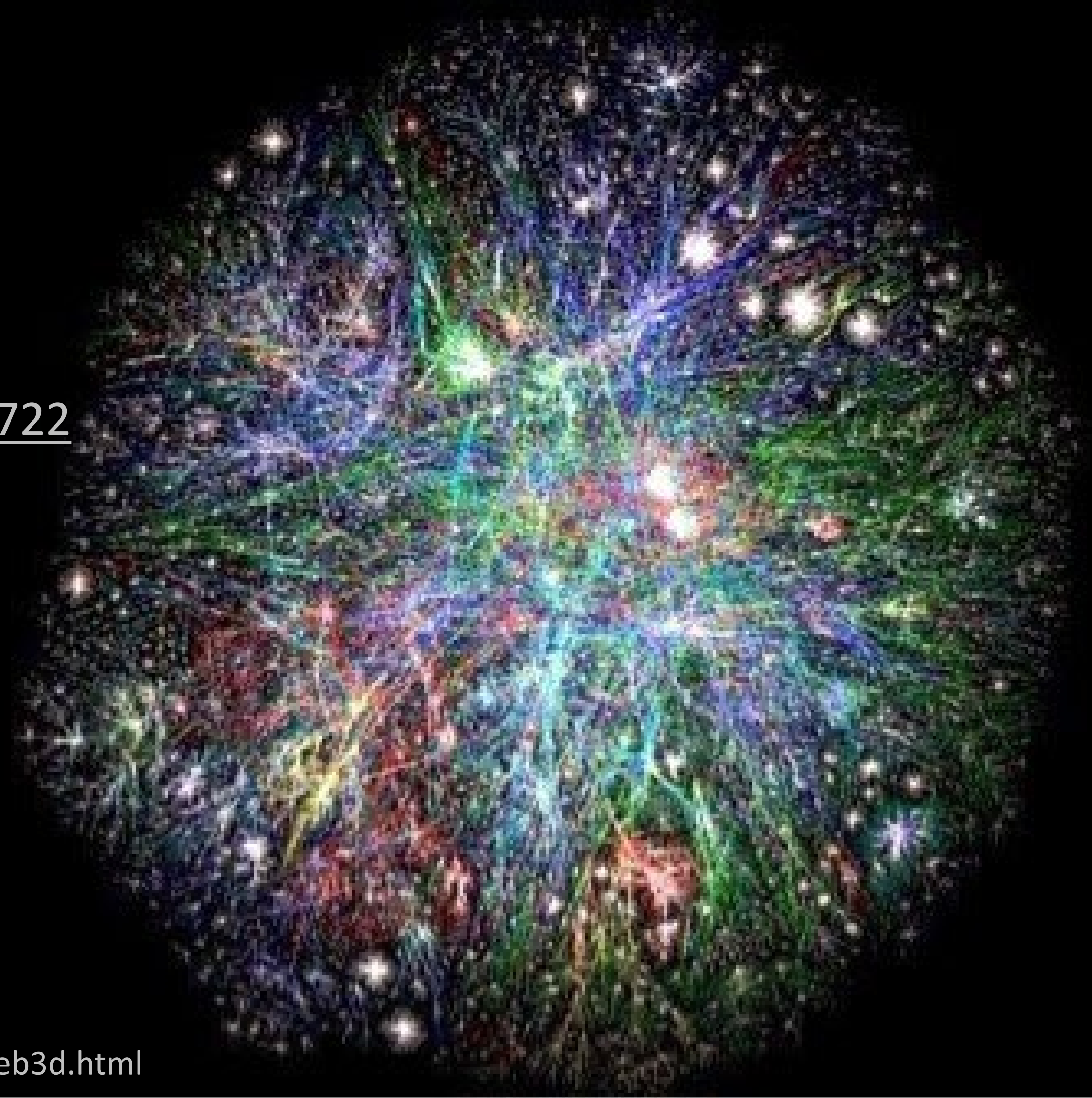
Introduction

Karen Reinhardt

- As per bio

Contacts:

- Karen.Reinhardt@badgersecurity.net
- www.linkedin.com/in/karen-reinhardt-farr-9825722
- Twitter: @Farrside42



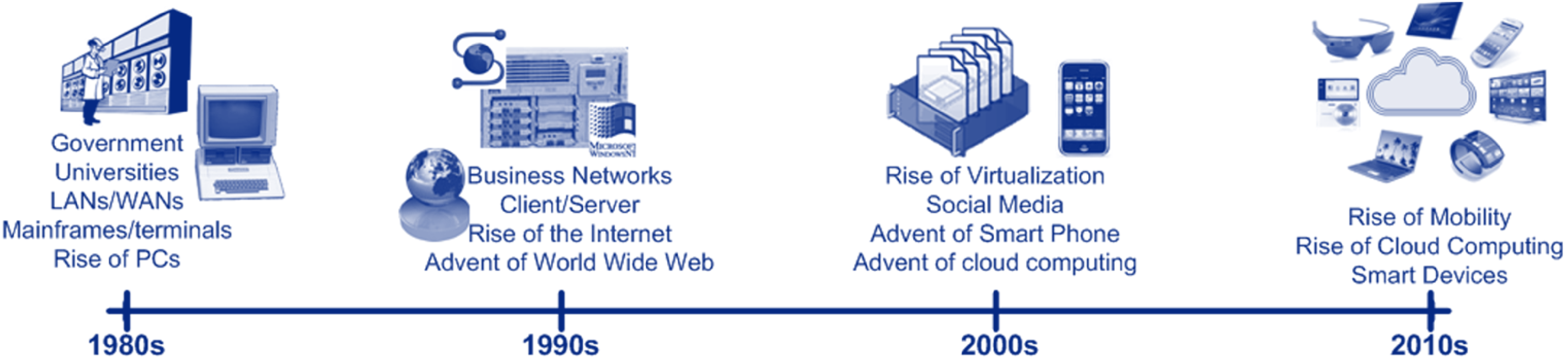
http://www.vlib.us/web/worldwideweb3d.html

The Call to Encrypt

The Rise of Internet Usage, Data, and Cyber-crime

A Very Brief History of the Internet

- Rise of Internet usage and data
  - Personal Computers, WWW, and E-commerce
  - Distributed computing for home and business pushing WAN adoption
  - Advent of broadband Internet Access
- Early Cybersecurity
  - Physical Access Controls – limited wired access (LANs), no wireless
  - limited Controls



Government
Universities
LANs/WANs
Mainframes/terminals
Rise of PCs

Business Networks
Client/Server
Rise of the Internet
Advent of World Wide Web

Rise of Virtualization
Social Media
Advent of Smart Phone
Advent of cloud computing

Rise of Mobility
Rise of Cloud Computing
Smart Devices

1980s
1990s
2000s
2010s

ARPANET → **NSFNET/CSNET/EUNET + WWW** → **Modern Internet**

Military
(d.1990)

Gov+University
(d.1995)

Berners-Lee
(b.1990)

Commercial (AT&T, Sprint, MCI, etc.)
(b1995)

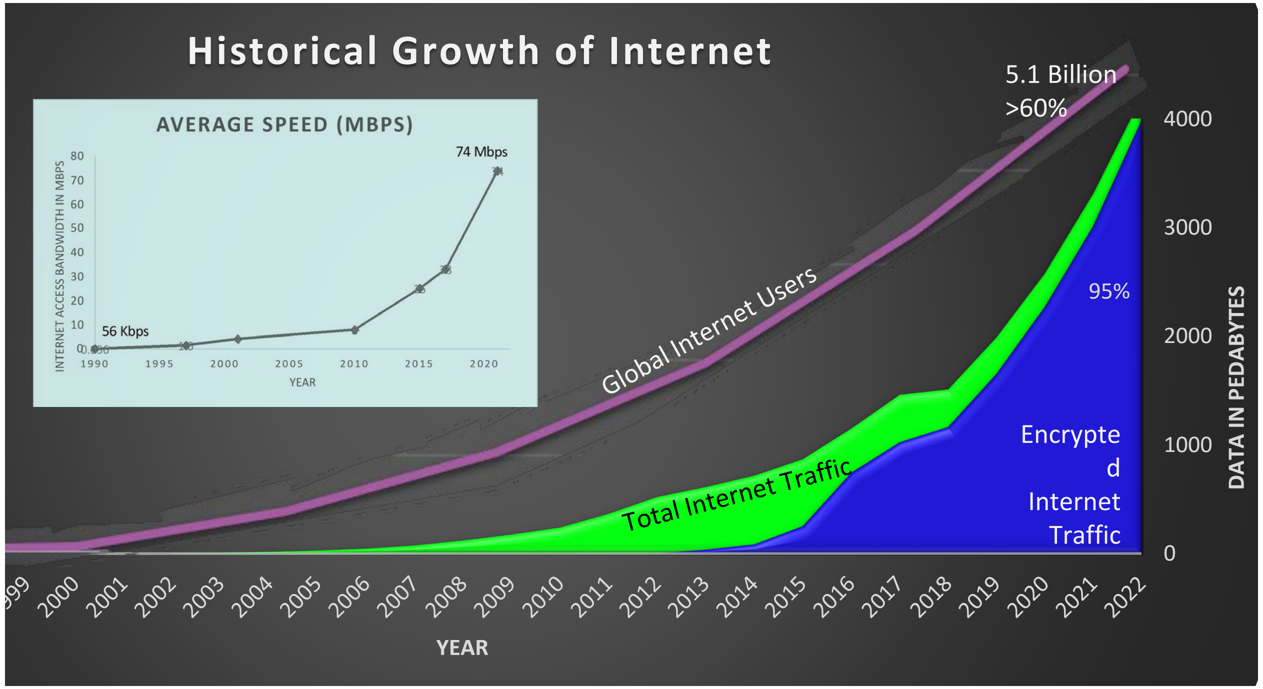
❖ Edholm’s Law (Internet bandwidth - doubling every 18 months)* [

❖ Moore’s Law (Processing power – doubling every 2 years**

*Expected to slow, but also fueled by wireless, **No transistors, current rate of improvement is debatable

Phenomenal Growth – DotCom to Cloud

- Personal Computers to Laptops to IOT and Mobile
  - Anywhere computing
- World Wide Web (Dotcom & beyond)
  - 100,000 web sites in 1995 to 1 Billions in 2014, nearing 2 Billion today (1.94) [~200 Million active]
- Graphics & Videos
  - Streaming (YouTube & Netflix)
- Faster, faster, faster
  - 1992: 56 Kbps → 2021:74Mbps average today
- Social Media, Mobile/IOT & Cloud
  - Computers integrated with life



©Akamai

The Evolution of Cybercrime

"Do you want to play a game?"

1980s

PCs, Smart kids, and Dial-up

Phreaking to Hacking

('98) 1st National Bank of Chicago - $70 mil

1990s

The Rise of the Web

The Rise of the Script Kiddies

('94) Citibank Hack - $10 mil
('98) Chernobyl Virus
('98) Melissa Virus

2000s

Faster Trojans, Toolz, Warez, More Identity Fraud

Network, DDOS Attacks,

('01) Code Red ('07-08) TJX & Heartland, ('08)Buckshot Yankee

2010s

IOT, Breaches, Misinformation, & Beyond:

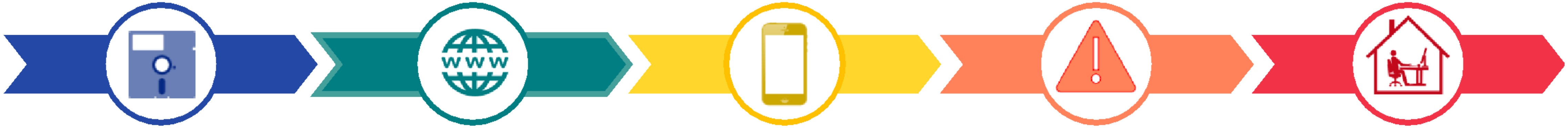
Bears, Pandas & More, Oh My!

('10) Stuxnet, ('11-) RSA,
('13- '19) Target, Adobe, Ebay,
Eqiifax, Marriott, Facebook,

2020s

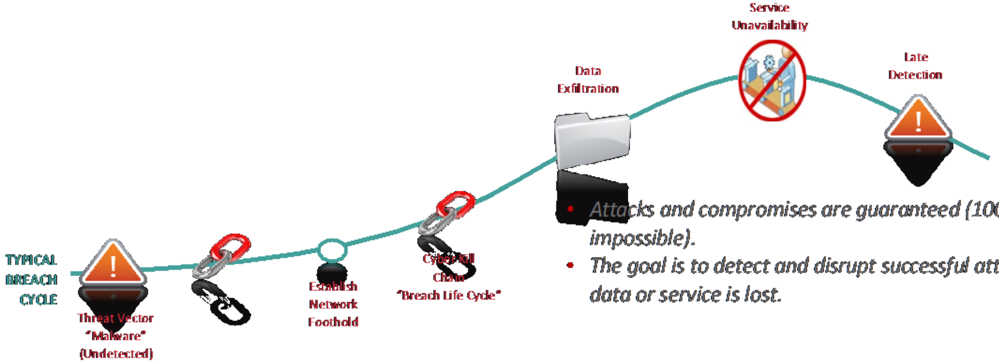
Ransomware, Mobile Workforce, Cloud, & Zero Trust

(.20) Solarwinds, ('21) Cardinal Pipeline, ('21,'22) Microsoft, ('22) Crypto.com



2022 Fun Facts

- **2,244 attacks** per day (every 39 seconds)
- **20,995,371 records breached** since 3/21
- **300,000 thousand new** pieces of **malware** are created daily


TYPICAL BREACH CYCLE
Threat Vector "Malware" (Undetected)
Establish Network Foothold
Cyber Kill Chain "Breach Life Cycle"
Data Exfiltration
Service Unavailability
Late Detection

- Attacks and compromises are guaranteed (100% prevention is impossible).
- The goal is to detect and disrupt successful attacks before critical data or service is lost.

So, What’s To Be Done?

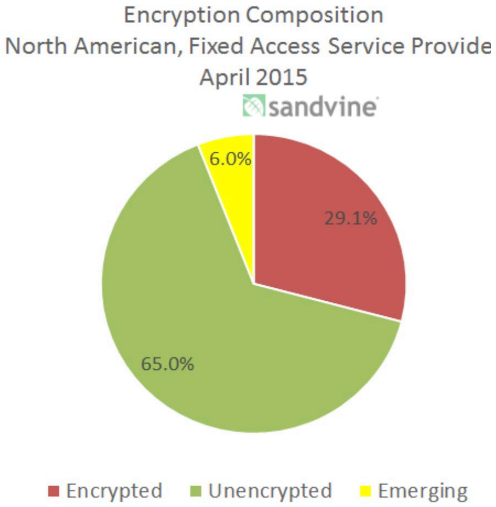
ENCRYPT EVERYTHING!!!

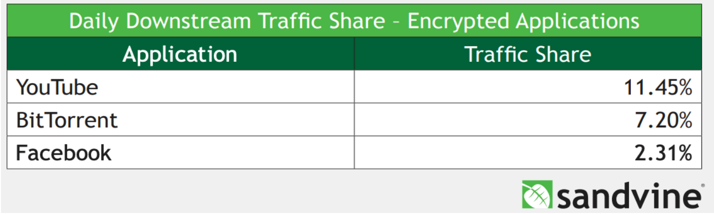
Encrypt Everything!!!

- Encrypt data stores
  - Hard Drives, Virtual Disks, Virtual Machines, Databases, etc.
- Encrypt sensitive data @Rest
  - Protects the data from unauthorized access even if a hacker gains user or system level access
  - Encrypt/decrypt keys must be kept safe
- Encrypt data in transit (TLS, IPSec, etc.)
  - Encryption key archival not required
- Layer @Rest & Transit Encryption
- HTTPS for Everything

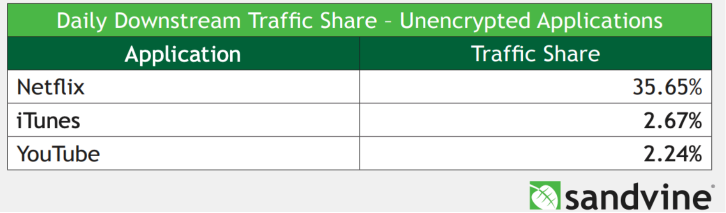
Progress on Encrypting Everything

- 2 of the largest data generators on the Internet: *Youtube and Netflix*
  - In 2015, YouTube : 11.43 percent. → 2016, Netflix: 64.7%

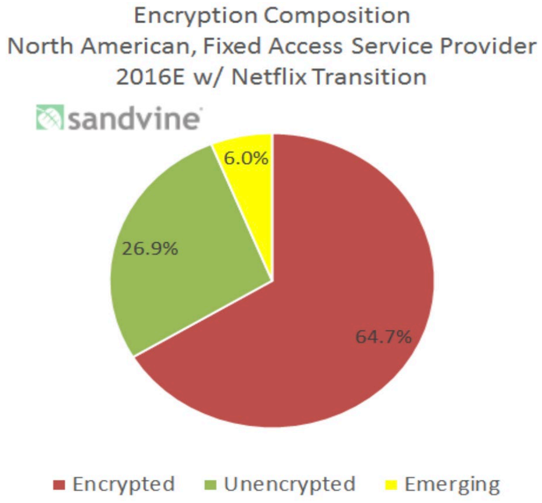

Encryption Composition
North American, Fixed Access Service Provide
April 2015



Daily Downstream Traffic Share - Encrypted Applications	
Application	Traffic Share
YouTube	11.45%
BitTorrent	7.20%
Facebook	2.31%



Daily Downstream Traffic Share - Unencrypted Applications	
Application	Traffic Share
Netflix	35.65%
iTunes	2.67%
YouTube	2.24%


Encryption Composition
North American, Fixed Access Service Provider
2016E w/ Netflix Transition

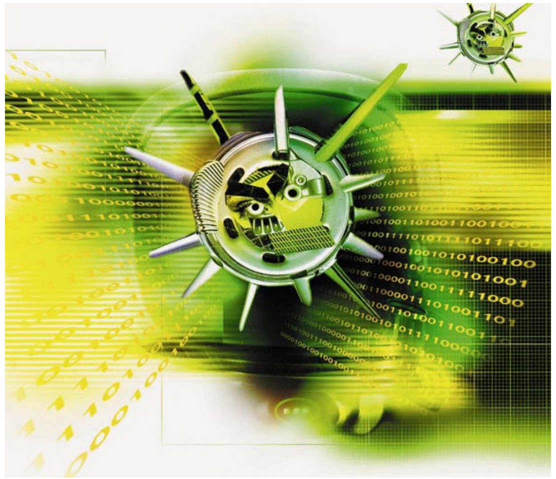
- So how much more secure are things today?
  - “We Encrypted the Web: 2021 Year in Review”: EFF declares over 90% of web traffic encrypted
- *BUT* …
  - “More Than 90% of Q2 Malware Was Hidden in Encrypted Traffic” - Dark Reading (2021)
  - “314 Percent Spike in HTTPS Threats” – Zscalar’s 2021 Report

The Truth About Encryption

- Confidentiality depends on the security of the keys
  - Failure to protect keys results in unauthorized access, data exfiltration, and data unavailability
- Data store encryption alone does not fully protect
  - Only prevents general access (all authorized users have access*)
  - Sensitive data still needs to be encrypted within the store
  - Data still needs to be encrypted in transit
- Uncontrolled encryption @rest can be used against you
  - Hiding in the shadows: hiding nefarious intent/content
  - No access: Ransomware

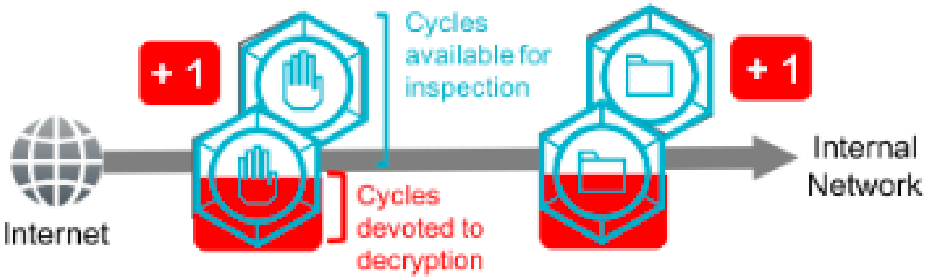
*Dependent on Access Control

Use Cases where Encryption can be Detrimental



©Silicon Republic

- Energy Sector – SCADA
  - Highly controlled networks, highly segmented
  - High Assurance Command & Control
- Integrity / Non-repudiation
  - Identifying source and destination
  - A high degree of integrity requires transparency to analyze data but often does not need to be secret
- Network Traffic Monitoring
  - Attackers routinely use encryption to hide
  - Non-repudiation impact
  - Central access point(s) for data, "eggs in one basket"
  - Can we monitor all traffic; is it worth the cost?



©Adaptera

HTTPS For Everything

A decade Later and over 90% Encrypted, Are we more secure?

HTTPS for Everything

Security professionals, government, and others recommend HTTPS for all Web Traffic. Why?

- Unencrypted traffic as reconnaissance
- Helps privacy over public networks (coffee shop, hotel)
- “Safety net” for sensitive data that is not otherwise encrypted
- Establishes minimal controls (TLS)
- Authenticates identity

Alignment of public and private organizations:

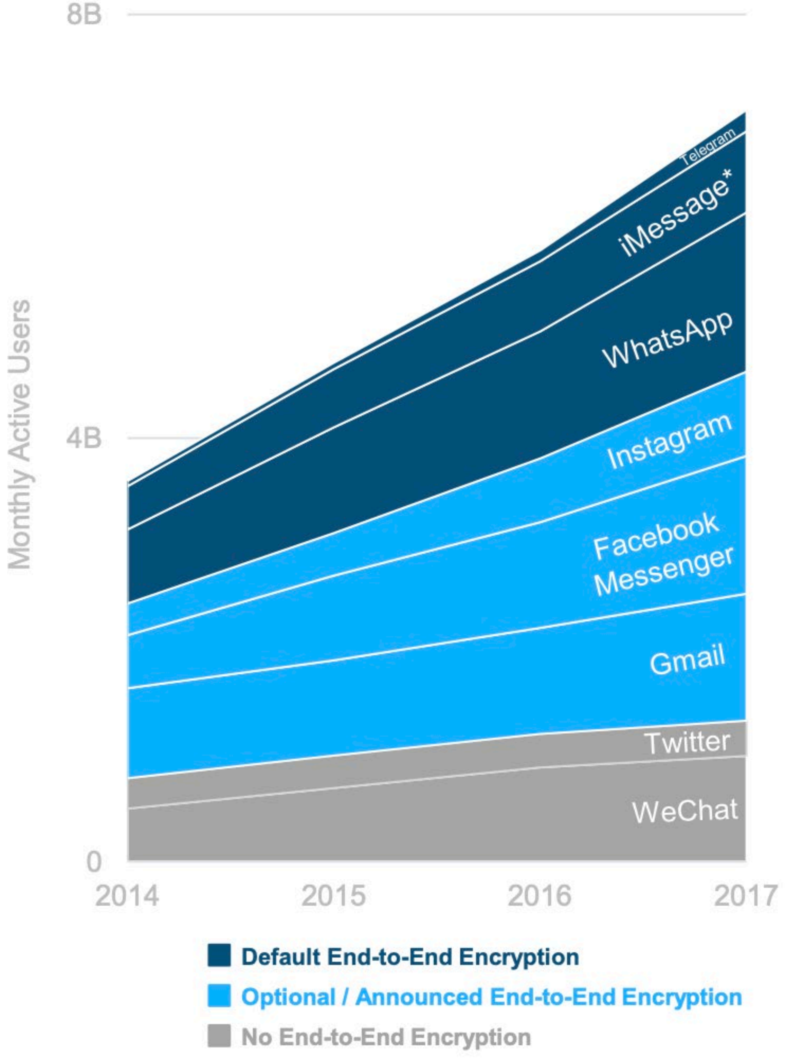
- “We Encrypted the Web” – EFF (2021)
- “Privacy and integrity by default” - HTTPS.CIO.Gov (2013, based on OMB M-13-15)

Privacy for everyone?

HTTPS for Privacy: Social Media Some Proof Encryption Works

- Social Media apps with encryption sell better
- HTTPS does help provide protection from social engineering resulting from data-mining social media

Select Messenger MAUs



https://www.bondcap.com/report/it19/#view/1

How Much Do You Trust HTTPS?

Do you trust:

- The Source?
- The Messenger?
  - ”Traffic cops” and agents
  - Depends on how important the message is and how secret it needs to be.

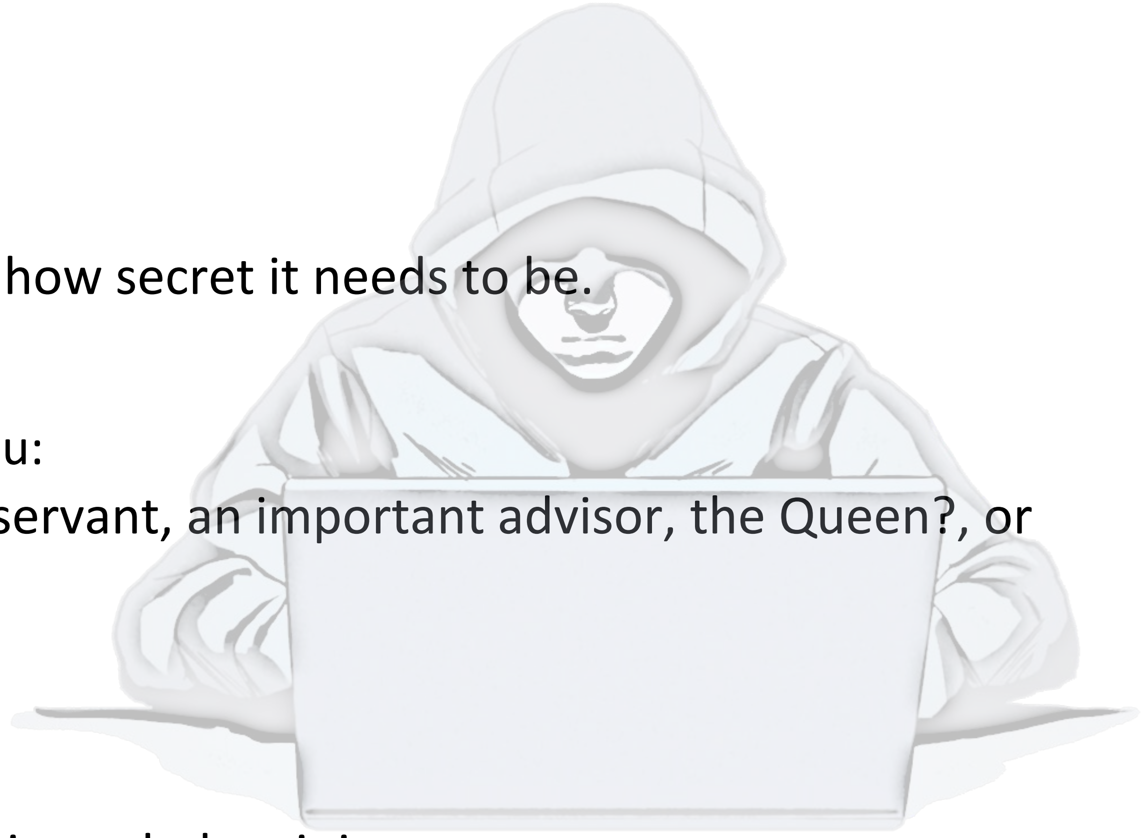
Metaphorical Use Case:

You have an urgent secret message for the King. Do you:

- Hand it off to another to deliver to the King? A servant, an important advisor, the Queen?, or
- Do you deliver it directly to the King?

Think About It:

- Most *assume* that the traffic is secure.
- Most *assume* the message is getting only to it’s intended recipient.
- If the message is about our bank accounts, we care a bit more.



©Iron Cloud Comics

The Reality of HTTPS

- The good news: No data loss if you lose a key (retry)
- The bad news: You still must protect your keys.
- **Weak key protection = weak identity = weak integrity**
- Session keys protect the session, not the system
- Not all traffic is encrypted, nor can it be
  - Network routing, handshake data is still readable
- Integrity is based on identity
  - Trusting a certificate with 100 names
  - The impossibility of non-repudiation over HTTPS

CNN: A Case Study in Encrypting Public Data

- http://www.cnn.com redirects to https://www.cnn.com
- Why does a web site sharing articles for public consumption want or need HTTPS?
  - Reader privacy
  - Publisher identity
- How Much Privacy is really needed?
  - What can be determined from sniffing traffic?
  - What assurance of integrity of articles?

✓ Publisher identity confirmed

✗ Tamper evidence for articles?

? Are CNN keys safe?

? Who can decrypt my traffic?

©National Association for Biomedical Research

©The Daily Beast

What’s To Be Done?

Integrity Independent of Encryption?

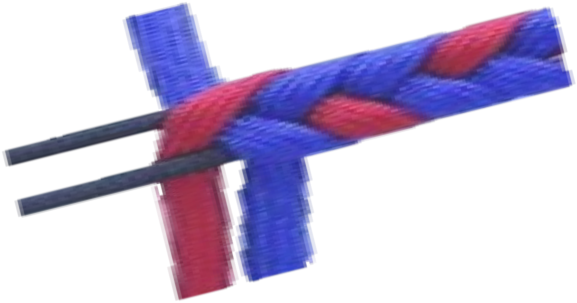
Integrity vs Confidentiality

- Can integrity exist without confidentiality?
  - Transparency and tamper-proofing
  - Digital signing
- Can confidentiality exist without integrity?
  - Why would we want it to?
  - Confidential lies and mis-information
- Does encryption provide integrity?
  - Tamper-proofing (all things must equal)

▶ Encryption relies on integrity for security

▶ Encryption support integrity as a control

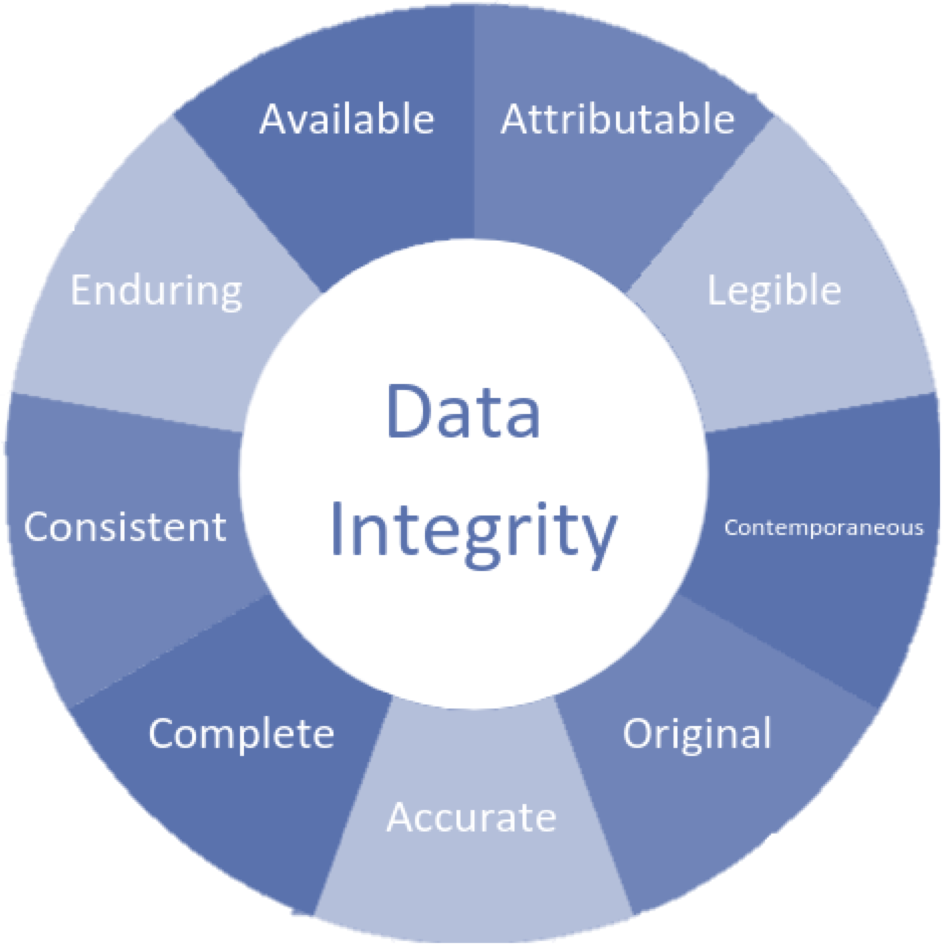
▶ Separate strands that can be woven



Creating a Framework for Integrity

Moving Beyond Privacy to Integrity

- Trust Domains
- Ensuring source and destination
  - Where did it come from?
  - Did it get to where it was intended?
- Tamper evidence
  - Did it arrive as sent?
- Validity and Quality
  - Can we verify the content?
  - What is the level of quality?
- Transparency
  - Are we valuing confidentiality over integrity?
  - What are the implications of focusing on secrecy over transparency?



Moving Beyond Assumptions

Is it time to change HTTPS?

- Separating identity & integrity from transport encryption
  - Identity ensured outside encrypted session
  - Tamper evidence vs encryption
  - Non-repudiation
  - Quality and reliability of data
- Assuring the path
  - Maintaining and demonstrating control end-to-end
  - Alerting to interruption
- Encryption as an option?
  - Updating TLS to off Server Identification without full session encryption
  - Using TLS Symmetric keys for specific field encryption between client and server
- Encryption management
  - Integrating with backend encryption systems (server-side) for stronger controls
  - Improved key storage and management

Parting Thoughts & Take Aways

Applying What We've Learned

For Today:

- Think beyond confidentiality
  - Security is Confidentiality, Integrity, and Availability and NOT necessarily in order
- Don't Assume Security
  - Trust but VERIFY (Zero Trust)
  - Encryption does NOT verify integrity of data
  - Are you talking to who you think you are talking to; Who has access to your data?
- ***Protect your keys!!!***

Thinking about the future:

- Is it time for new protocols? Web 3.0?
- Your ideas here ...

Thank You

Sources

IBISWorld, “Internet Traffic Volume”, IBISWorld August 9, 2021, https://www.ibisworld.com/us/bed/internet-traffic-volume/88089/

Jeff Desjardins, “How much data is generated each day?”, World Economic Forum, April 17, 2019, https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

Mary Meeker, ”Internet Trends 2019”, Bond Capital, June 11, 2019, https://www.bondcap.com/report/it19/#internettrends

Chad Skipper, “The Relevance of Network Security in an Encrypted World”, VMWare, Sept. 29, 2020, https://blogs.vmware.com/security/2020/09/network-security-encrypted.html#:~:text=The%20Rise%20of%20Encrypted%20Data&text=For%20example%2C%20the%20Google%20Transparency,100%20sites%20defaulting%20to%20HTTPS.

Google, “Google Transparency Report: HTTPS Encryption on the Web”, Google (2022), https://transparencyreport.google.com/https/overview?hl=en

Wang, Yahyavi, Kemme, He, “I know what you did on your smartphone: Inferring app usage over encrypted data traffic”, IEEE (2015), https://ieeexplore.ieee.org/abstract/document/7346855

Wikipedia, “Internet Traffic:Internet Backbone Traffic in th United States”, Wikipedia (2022), https://en.wikipedia.org/wiki/Internet_traffic#Internet_backbone_traffic_in_the_United_States

Lewis, Zheng, Carter, The Effect of Encryption on Lawful Access to Communications and Data, Center for Strategic and International Studies (2017), https://books.google.com/books?hl=en&lr=&id=_oknDgAAQBAJ&oi=fnd&pg=PR3&dq=Internet+statistics+worldwide+encrypted+data&ots=9MS-71FPa6&sig=CU63rpg67oxAIiq4RerkjtlIoY8#v=onepage&q=Internet%20statistics%20worldwide%20encrypted%20data&f=false

Adam Estes, “How to Encrypt Everything”,Gizmodo, June 5, 2015, https://gizmodo.com/how-to-encrypt-everything-1586619248

Sources continued

Tony Scott, “Memorandum: Policy to Require Secure Connections across Federal Websites and Web Services”, Office of Management and Budget (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf

Wikipedia, “History of the Internet”,Wikipedia (2022), https://en.wikipedia.org/wiki/History_of_the_Internet

Jacquelyn Bulao, “How Many Cyber Attacks per Day?”, Tachjury. May 2, 2022, https://techjury.net/blog/how-many-cyber-attacks-per-day/

Jal Vijayan, “More Than 90% of Q2 Malware Was Hidden in Encrypted Traffic”, Dark Reading, September 30, 2021, https://www.darkreading.com/perimeter/more-than-90-of-q2-malware-was-hidden-in-encrypted-traffic

Zscalar, “Zscaler’s 2021 Encrypted Attacks Report Reveals 314 Percent Spike in HTTPS Threats”, Zscalar, October 28, 2021, https://www.globenewswire.com/news-release/2021/10/28/2322370/0/en/Zscaler-s-2021-Encrypted-Attacks-Report-Reveals-314-Percent-Spike-in-HTTPS-Threats.html

The HTTPS-Only Standard, https://https.cio.gov/

Alex Hancock, “We Encrypted the Web: 2021 Year in Review”, Electronic Frontier Foundation, December 27, 2021, https://www.eff.org/deeplinks/2021/12/we-encrypted-web-2021-year-review

Kennedy, “It could be lights out as USB worm Stuxnet attacks networks”, Silicon Republic, July 21, 2010, https://www.siliconrepublic.com/enterprise/it-could-be-lights-out-as-usb-worm-stuxnet-attacks-networks

Adaptera, “Reduce the Cost of Tool Sprawl with Smarter Network Monitoring”, Adaptera, 2022, https://adaptera.gr/reduce-the-cost-of-tool-sprawl-with-smarter-network-monitoring/